SESSION BORDER CONTROL IN IMS

AN ANALYSIS OF THE REQUIREMENTS FOR SESSION BORDER CONTROL IN IMS NETWORKS

Metaswitch Networks

CONTENTS

EXECUTIVE SUMMARY

THE IP MULTIMEDIA SUBSYSTEM (IMS), WITH ITS MULTITUDE OF STANDARDIZED FUNCTIONS AND VARIANTS, PROVIDES A BLUEPRINT FOR NEXT GENERATION NETWORKS (NGNS). SESSION BORDER CONTROLLERS (SBCS), ON THE OTHER HAND, HAVE A REPUTATION FOR BEING NON-STANDARD "BLACK BOXES". BOTH PROMISE A MANAGED IP NETWORK THAT SUPPORTS RELIABLE, SECURE, REVENUE-GENERATING REAL-TIME SERVICES FOR AUTHORIZED USERS, BUT THE STANDARDS BODIES HAVE YET TO FULLY CLARIFY HOW THESE CONCEPTS FIT TOGETHER.

This white paper explores how far the capabilities offered by SBCs can be explained in terms of IMS functions, and notes where the IMS standards are insufficient to describe all of the required real-world features. It also explains what an SBC designed for deployment in an IMS network should look like, and how this requirement is likely to evolve.

This white paper is aimed at equipment manufacturers looking at building SBC functionality and IMS capabilities into their product range, and at carriers and consultants looking to understand how an SBC fits into an NGN.

ABOUT THE AUTHOR

Jonathan Cumming is Director of VoIP Product Management for the Network Protocols Division at Metaswitch Networks. During his 10 years in the company, he has held a range of development, marketing and product management roles.

Jonathan has over 20 years' experience in the communications software industry. He holds an MBA from INSEAD and an Engineering degree from Cambridge University.

INTRODUCTION

IN RECENT YEARS, THE VISION OF IMS AS THE MODEL FOR A UBIQUITOUS QOS-ENABLED NETWORK FOR MULTIMEDIA SERVICES HAS EVOLVED. TODAY'S REALITY IS A HETEROGENEOUS WORLD CONTAINING BOTH IMS AND NON-IMS MANAGED NETWORKS, WITH LINKS TO A LARGE RANGE OF UNMANAGED AND LEGACY NETWORKS, AND DISPARATE ACCESS TECHNOLOGIES AND USER REQUIREMENTS.

Session Border Controllers (SBCs) are now established as a cornerstone of this multi-media network environment: controlling and adapting the signaling and media flows as they cross network borders. In response, the IMS standards have expanded to incorporate many of the features that SBCs offer and the different requirements of fixed-line, mobile and cable operators.

1.1 Scope

This white paper describes how SBC function is standardized in the IMS standards, and explores how SBC function can be deployed in different network environment to provide QoS and enable interworking between different types of network.

This section provides a brief overview of Session Border Control and IMS.

Sections 2 and 3 cover how Session Border Controllers fit into the IMS architecture and the SBC features that are not contained in IMS standards.

Section 4 considers what a Session Border Controller targeted at an IMS market should look like.

Section 5 provides some examples of how SBCs can be deployed in IMS-based networks.

Sections 6 and 7 discuss how this market is likely to change in the future, and what conclusions can be drawn.

Section 8 provides a list of references to additional information, a glossary of the acronyms used throughout this document, and information on Metaswitch Networks and its products.

1.2 Session Border Controllers

Session Border Controllers were developed to address the wide range of issues that arise when sessionbased voice and multi-media services are overlaid on IP infrastructure. These include

Security

- enforcing call admission control policies at the network border to ensure Quality of Service (QoS)
- preventing service abuse and maintain privacy of carrier and user information

Extending reach

- resolving VoIP protocol problems arising from the widespread use of firewalls and network
- address translation (NAT), and the vast array of different protocols and dialects used in VoIP networks

Other services

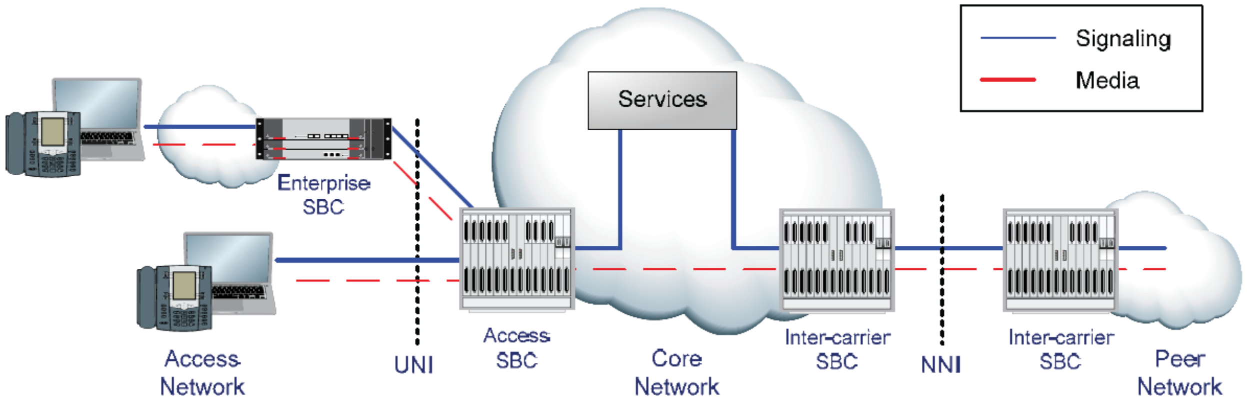
- monitoring for regulatory compliance, billing, and service assurance.

Session Border Controllers were traditionally deployed as discrete devices at the edge of the managed network, where they could control both the signaling and media streams, as shown in the diagram below.

However, actual SBC deployments have required much greater flexibility in how the Session Border Controllers are deployed. For example:

- The Session Border Controller may be decomposed with selected functions deployed in specific areas of the network, such as Denial of Service protection within the access network.
- The Session Border Controller may be integrated into existing devices that already have an accepted role in the network, such as an edge router.
- Modularity of functions is needed to allow à la carte selection of capabilities for each user group and on each interface, for example, to provide custom H.323 interworking for a particular enterprise.

IMS provides a single model for a managed network, and this white paper explores how it handles Session Border Controllers. For a more detailed description of Session Border Controllers, see our white paper, "Session Border Controllers: Enabling the VoIP revolution", which is available on our website: (www.metaswitch.com).



1.3 The IP Multi-media Subsystem (IMS)

IMS is the control plane of the 3rd Generation Partnership Project (3GPP) architecture for its nextgeneration telecommunications network (NGN). This architecture has been designed to enable carriers to provide a wide range of real-time, packet-based services and to track their use in a way that allows both traditional time-based charging as well as packet and service-based charging.

IMS provides a framework for the deployment of both basic calling services and enhanced services, including

- mixed voice and video calls
- multimedia messaging
- web integration
- presence-based services
- push-to-talk
- IPTV and Video-on-Demand.

At the same time, it draws on the traditional telecommunications experience of

- guaranteed QoS
- flexible charging mechanisms (time-based, call-collect, premium rates)
- mobility, including roaming to competitive networks
- lawful intercept legislation compliance.

Carriers are deploying IMS to cut their CapEx and OpEx through the use of a converged IP backbone and standardized components with standardized interfaces. They expect IMS to provide the following advantages.

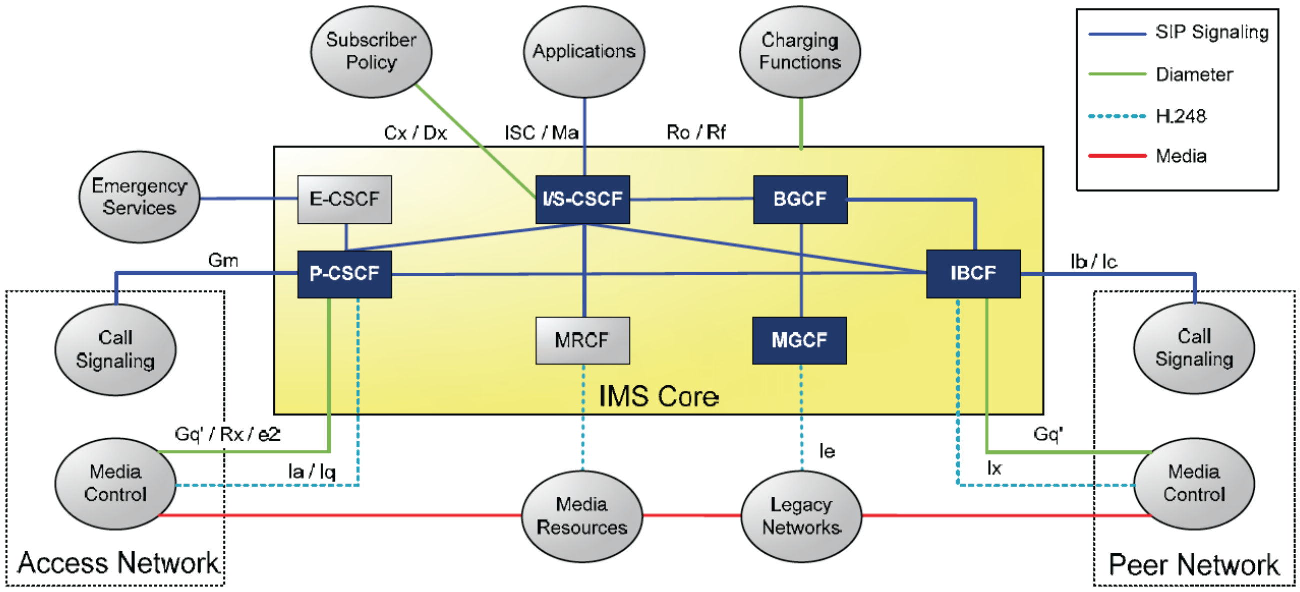
- A single converged network that provides voice and data service over many mobile and fixed access technologies.
- Standardized common components, including user authentication, call control, and configuration storage, to reduce the development work required to create each new service and promote a more consistent user experience.
- Standardized interfaces to increase competition between equipment vendors by preventing carriers from being tied to a single supplier's proprietary solution.

IMS promises to enable new services to be rolled out more quickly and cheaply than the traditional monolithic design of telephony services. It also simplifies the delivery of combined voice and data services, e.g. integrated voicemail and email, which are becoming increasingly popular.

The IMS model has been adopted by many standards bodies as the basis of their NGN architectures. In each case, the architecture has been extended to match the differing service requirements and installed equipment. This process risked undermining the standard by creating incompatible variants, so to maximize interoperability the standards bodies split the IMS model into "IMS Core" and "Access and Applications".

1.3.1 IMS Core

The "IMS Core" contains the core switching functions, as shown in the diagram below. These functions are standardized by 3GPP.



1.3.2 Access and Applications

The other components comprise the “Access and Application” functions. These functions are defined by separate standards bodies that cater to specific service provider industries. The result is disparate “IMSbased” architectures that share common core functions.

- 3GPP continues to standardize “3GPP Access”, which covers the requirements of the mobile carriers (2G, 3G, 4G, LTE, WiMax and WiFi access).
- ETSI TISPAN covers the requirements of fixed-line carriers (DSL and enterprise access).
- PacketCable covers the requirements of cable carriers (DOCSIS).

The differences between Access and Application standards are driven by the different physical and commercial environments of the carriers, in particular the capabilities of their existing infrastructure and their need to support legacy features. Although the standards bodies have made little progress in a unified or even compatible architecture, real-world requirements of system vendors demand that SBCs include the flexibility to address the disparate standards. This approach is covered in section 4.5.1.

When any feature requires a change to the IMS Core, the requirement is passed to the 3GPP standards process for inclusion in the next IMS release. This approach means that the IMS Core functions have, in the main, only a single way to provide each feature, although not all features are available in every environment.

In this white paper, we discuss how Session Border Controllers fit into the access architectures covered by the 3GPP, TISPAN and PacketCable standards. These provide a representative selection of possible approaches and address the majority of issues faced by service providers.

For a more detailed introduction to IMS, see our white paper, “An Introduction to IMS: The Technology and The Motivation”, which is available on our website (www.metaswitch.com), and the other references that are listed in Section 8.

IMS FEATURES PROVIDED BY SBCS

IMS DEFINES A SET OF EXTERNAL BORDERS AND THE FUNCTIONS TO CONTROL ACCESS THROUGH THEM. THESE INCLUDE INTERFACES THROUGH GATEWAYS TO CIRCUIT-SWITCHED AND LEGACY NETWORKS, AS WELL AS INTERFACES TO IP-BASED NETWORKS RUNNING BOTH COMPATIBLE AND INCOMPATIBLE SIGNALING AND MEDIA PROTOCOLS. IT IS THE INTERFACES TO IP-BASED NETWORKS THAT REQUIRE THE PROTECTION OF SESSION BORDER CONTROLLERS, AS SHOWN IN THE DIAGRAM BELOW.

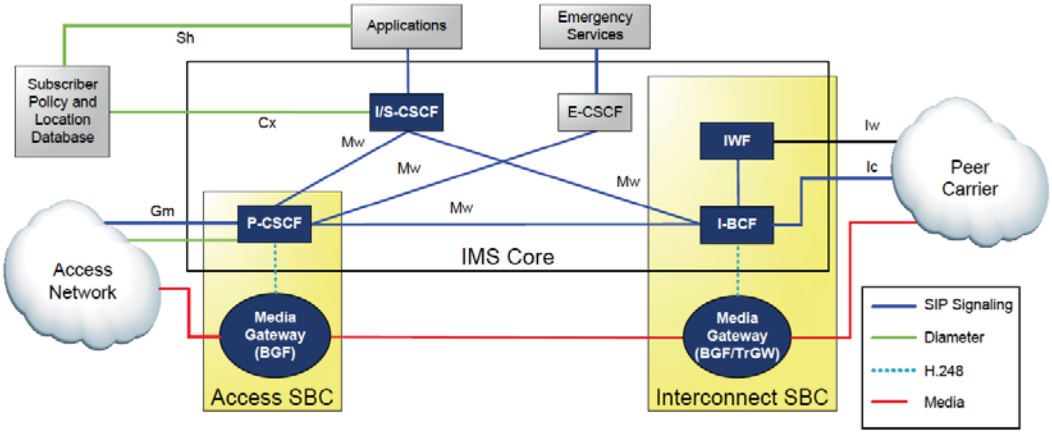
IMS defines two functions to police the signaling flows from IP-based networks entering the network core.

- On the access side, signaling between users and the IMS core is controlled by a P-CSCF.
- On inter-carrier links, signaling is controlled by an IBCF.

The primary distinction between P-CSCF and IBCF is that devices that attach through a P-CSCF use SIP signaling to register their presence and subscribe for service (client-server), whereas the IBCF uses statically configured routing (peer-peer), such as DNS or ENUM. A single device may support both PCSCF and IBCF modes, as both behaviors may be required, even over the same physical interface.

These standardized border functions form the signaling core of the Access and Interconnect SBCs. They provide routing and authentication of the signaling, and communicate with devices within the IMS core over the standardized Mw (SIP) interface. SBCs are also required to support functions outside the IMS standards, such as Denial-of-Service protection and interworking with non-IMS devices.

The rest of this section describes how IMS has standardized many of the features provided by SBCs. Section 3 describes how non-standard SBC features fit into the IMS architecture.



2.1 IMS Core Features

2.1.1 Network Address Translation (NAT)

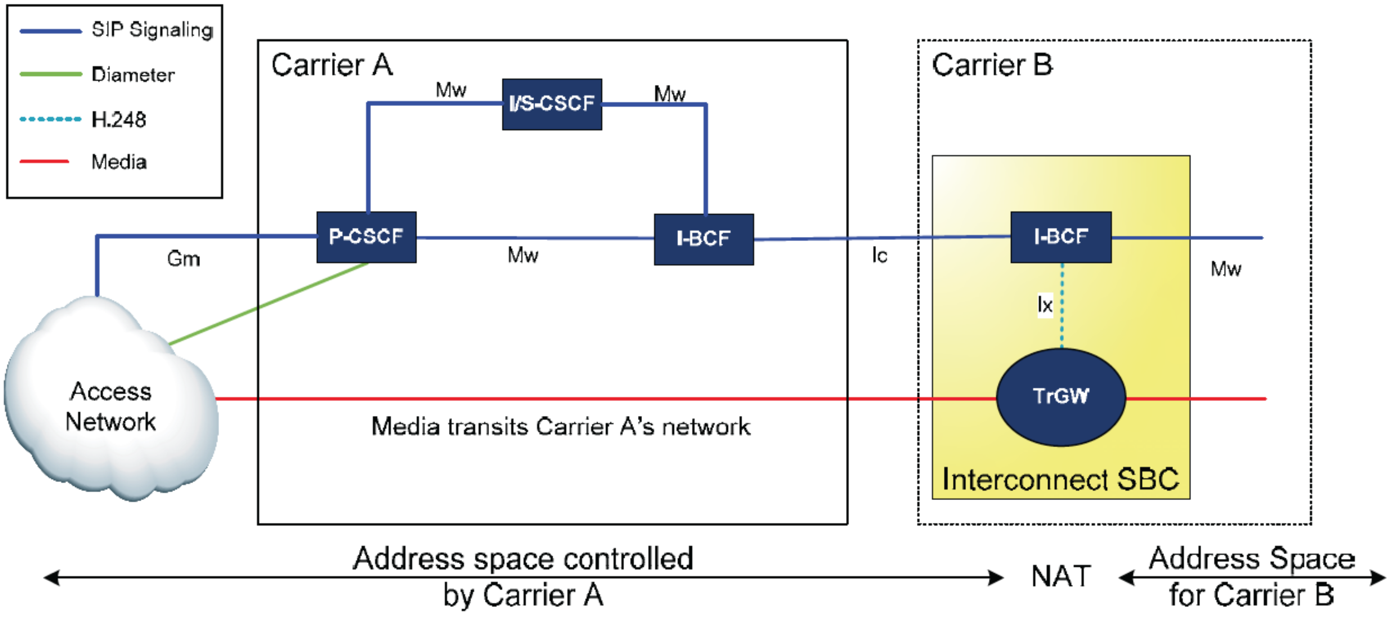
Network Address Translation is required when devices using private IP addresses wish to communicate outside of their domain. For example, a NAT is required to route between carriers if either is using a private address spaces.

Because call signaling messages carry the media addresses, changes to these addresses due to the NAT must be reflected in the call signaling. This means that the NAT function must pre-allocate mappings between “internal” and “external” addresses and ports before any media actually flows, so that these mapping can update the signaling that establishes the call.

This is different from a simple NAT, which automatically allocates external ports when forwarding outgoing media, and only routes media received on external ports to internal addresses when there is an existing mapping.

In the IMS architecture, the BGF (TISPAN) or TrGW (3GPP) provide this NAT function under the control of SIP-ALG (SIP back-to-back User Agent) functionality in the P-CSCF or IBCF. The control mechanism (Ix reference point) is not standardized in 3GPP release 8, although it is expected to be very similar to the TISPAN-defined Ia reference point (ETSI ES 283 018).

The diagram below shows the routing of the media and the signaling for a call where there is a NAT (TrGW) between two carrier networks.



2.1.2 NAT and Firewall Traversal

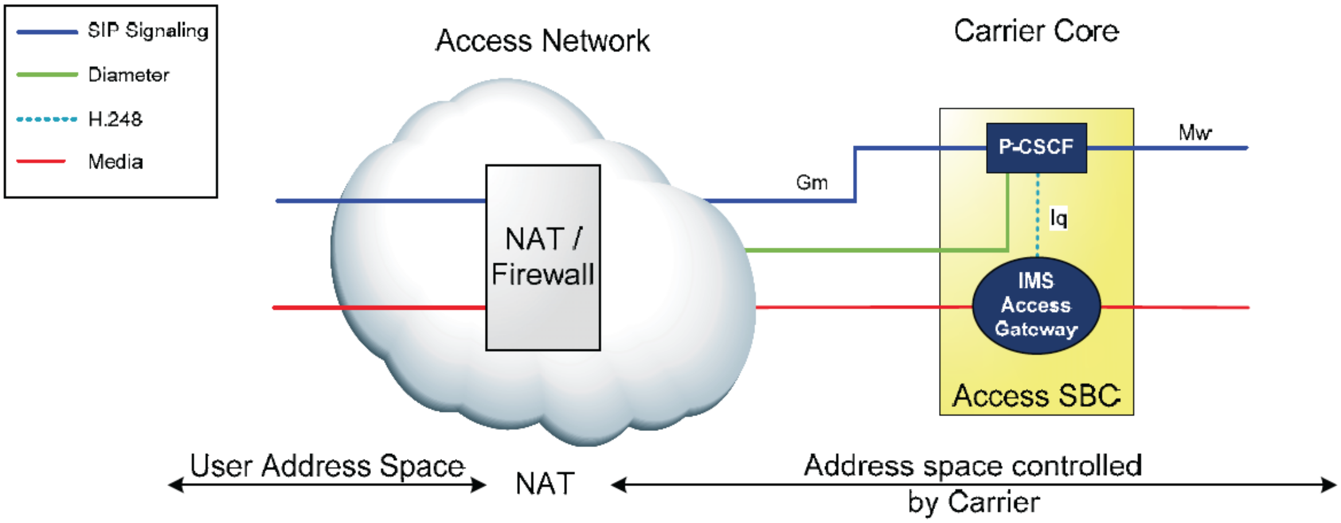
Where there is a NAT or firewall between the endpoint and the IMS core, the border controller must route the call signaling and media through pinholes[1] for the endpoint.

IMS describes two alternative solutions for NAT and firewall traversal.

- The use of the IETF "STUN", "SIP Outbound" and "ICE" standards: RFCs 5389, 5626 and 5245. In this mode, the User Equipment (or endpoint) maintains pinholes in the firewall / NAT, determines an IP address (or set of alternative addresses) at which it can be contacted and inserts these in the call signaling.
- Where the endpoints do not support NAT traversal, the IMS core is required to fix-up the signaling and override the routing. In the 3GPP architecture, SIP-ALG functionality within the PCSCF fixes up the signaling and an IMS Access Gateway controls the media routing. These two devices communicate over the Iq reference point.

As for the Ix reference point, the control mechanism (Iq reference point) is not standardized in 3GPP release 8, although the protocol is expected to be very similar to the TISPAN-defined Ia reference point (ETSI ES 283 018).

The diagram below shows the routing of the media and the signaling for a call where there is a NAT or firewall in the access network. The P-CSCF has no control over any NAT or firewall, so may require traversal techniques described above to operate in this environment.



[1] A pinhole controls whether external traffic reaches devices within a protected address space. It is a mapping maintained by a NAT between a private address and port and a public address and port. The NAT forwards traffic received on the public address to the private address. Traffic received by the NAT that does not correspond to an active pinhole is discarded. A pinhole in a firewall is similar, but, as there is no NAT, the public and private addresses are the same.

Pinholes may be established dynamically when the internal device sends traffic through the NAT to an external address. They may also be created by signaling from the endpoint or statically configured.

2.1.3 Privacy of User Identity and Network Topology

Privacy is achieved by the removal of identifiable information from both signaling and media messages sent to untrusted parties, which may be end users or other carriers.

IMS standardizes the hiding of the user location and network topology information in the call signaling in the border gateway (P-CSCF, I-CSCF or IBCF), for example, to enable anonymous calling.

IMS also allows the border gateway to hide the address of signaling entities within the network core (topology hiding). For example, the IP address of the S-CSCF may reveal the number of S-CSCFs and simplify direct attacks.

2.1.4 Routing of Signaling entering the IMS Core

IMS standardizes control of routing SIP messages entering the IMS core. These controls are enforced by the P-CSCF, which overwrites any routing headers provided by untrusted endpoints. This prevents external devices from directly accessing servers within the IMS core, so helps protect against DoS attacks. The P-CSCF routes:

- registration messages to the relevant I/S-CSCF based on the domain of the subscriber that is registering
- out-of-dialog requests (new calls) based on the Service-Route for the subscriber that was established during registration
- in-dialog requests over the Route set established for the dialog.

In this way, the P-CSCF ensures that signaling entering the IMS core traverses the servers that are required to provide the contracted features for that subscriber, and protects other servers from malicious traffic.

2.1.5 Monitoring, including Lawful Intercept

To comply with government regulations and commercial requirements, usage monitoring and interception of calls may be needed. IMS provides a complete framework for Lawful Intercept and usage monitoring in 3GPP TS 33.107, although the details are still being refined to ensure that they meet the requirements of each national regulator.

IMS allows extremely flexible reporting of traffic flows across the network border, as the usage statistics required are configured as part of access policy. IMS also defines the use of charging identifiers in the signaling messages to correlate billing records for each call, see 3GPP TS 23.203. This enables any device in the network to record its usage for the call.

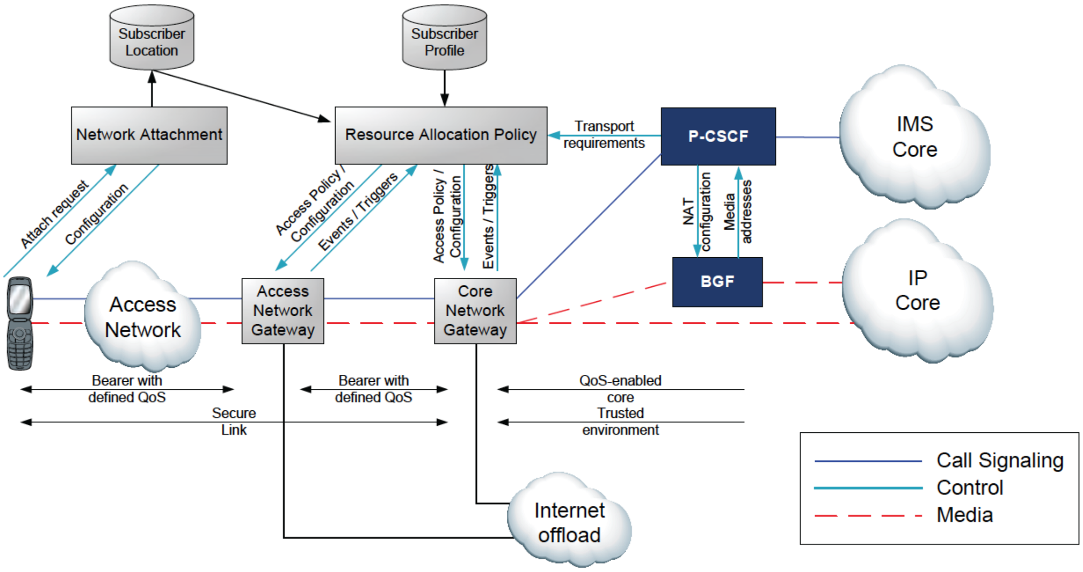
The statistics are sent to centralized charging functions, which combine the billing records from different devices to create a consolidated record for each call. This provides a comprehensive and flexible solution, which integrates border control with resource management throughout the network.

2.2 Access Network Controls

Session Border Controllers use information contained in the signaling flows to configure routers in the access network and media gateways that allow media traffic to enter the carrier's IP core. Although each IMS-based network has its own access network architecture, function names and interfaces, the access control architecture for all IMS-based networks is similar.

The algorithms used, the differences between the access network architectures, and the functions defined by each standards body are covered in section 4.4.

The diagram below shows the high-level architecture that is used for access network control.



The IMS architecture defines two stages of user identification.

- An initial attachment process allows the User Equipment (UE) to request access to the network and obtain configuration, including an address and a default set of access rights, such as access to the Internet. This does not involve any IMS (SIP) signaling.
- A secondary registration process (not shown) registers the UE with the IMS core and enables access to services in the IMS core.

The UE requests services from the network using either call signaling (e.g. SIP) or requesting access to the media directly.

- Call-signaled services use a "push" resource reservation model. The P-CSCF analyzes the call signaling and signals the session's transport requirements to the resource allocation layer. The resource allocation layer decides the physical resources to use for the call and "pushes" the policy to be applied to the media for the call onto the devices handling the media.
- The media gateways can also request authorization for additional bandwidth or services, for example, on receipt of IGMP or RSVP requests. This is referred to as policy "pull" and is used when the media resources are not explicitly signaled, for example, when joining a well-known IPTV multicast stream.

The resource allocation layer uses many inputs to calculate the appropriate resources for a call. These include the access technology, the current utilization rates, the subscriber's location, subscription profile, the service requested, details of other services already being used by the subscriber, and the call's priority.

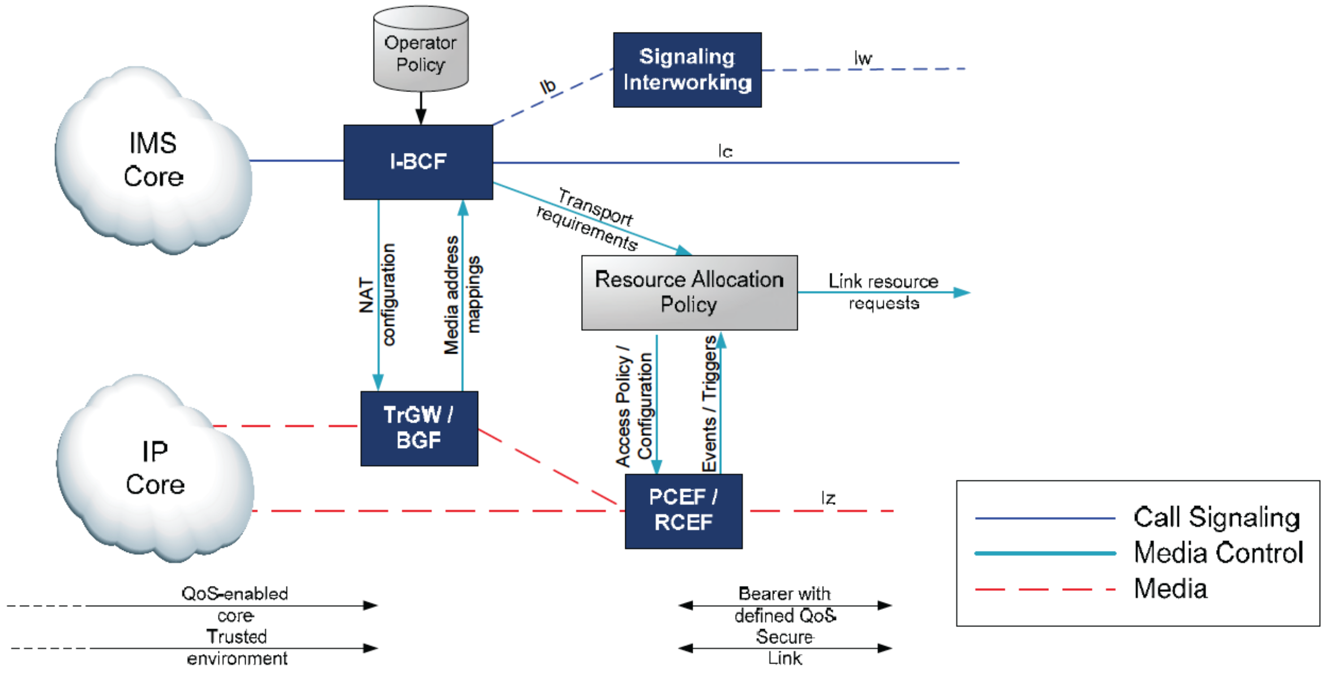
2.3 Peer Interconnects

The control architecture on interconnect links is similar to that on access links. However, the Interconnect SBC does not authenticate each user individually, so cannot apply subscriber-based policy to individual media requests. Instead, the Interconnect SBC monitors aggregate capacity on the link to ensure QoS and SLA compliance, prioritizing calls as necessary to maintain performance.

It also provides the other SBC protection and interoperability features that are not covered by any standards.

The diagram below shows the high-level architecture that is used for control over peering links. It is similar to that on the access network, but does not include a subscriber location database or network attachment function, as these responsibilities have been delegated to the peer network.

The Signaling Interworking function supports peering with non-IMS networks. It provides interworking between the IMS-standardized Ib reference point and the nonstandard Iw interface.

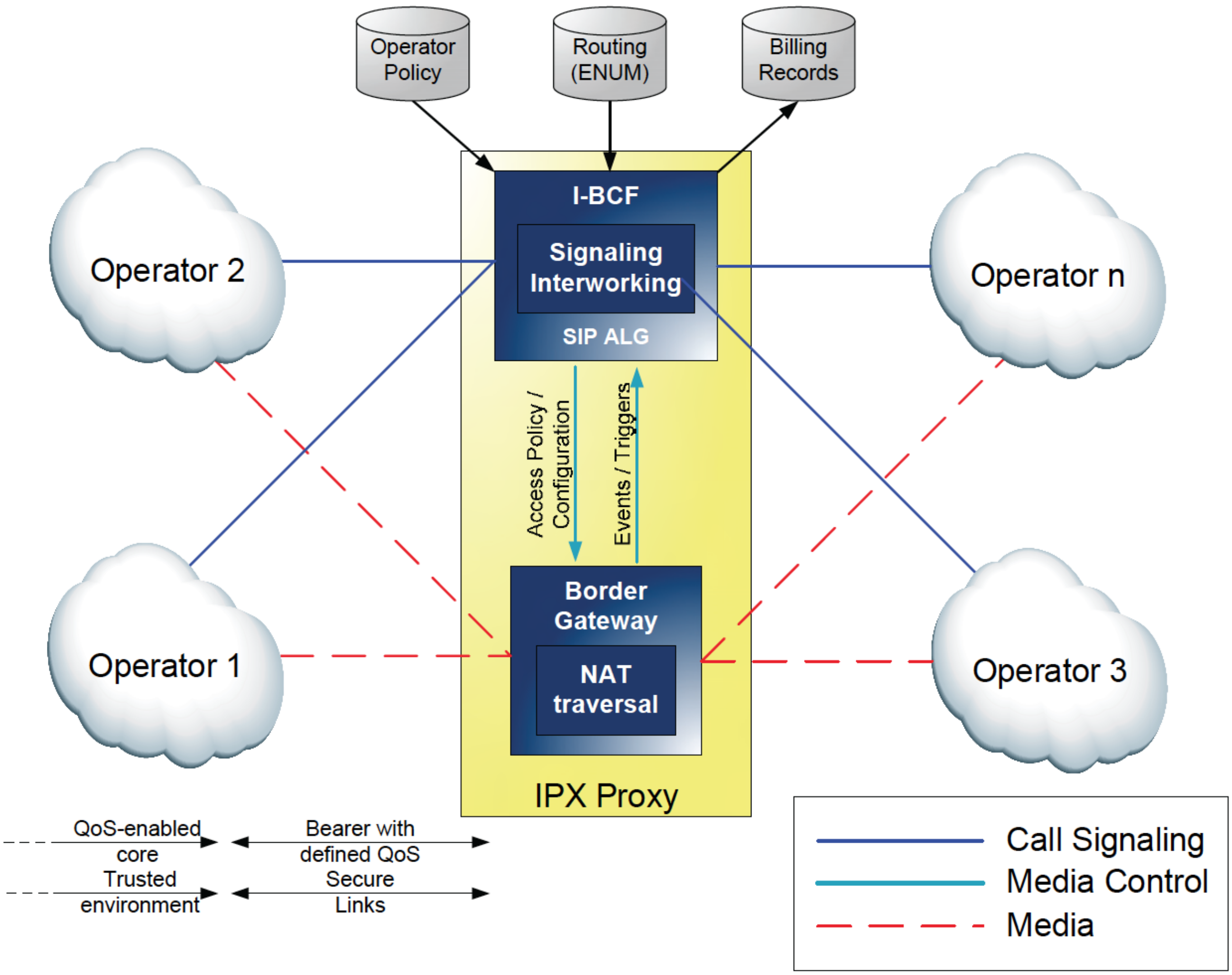


2.3.1 IPX Proxy

The GSM Association (GSMA) identified the need for a centralized interconnection of multiple IMS carriers through an inter-carrier carrier that provides both IP connectivity and a clearinghouse for intercarrier charges. This mimics the existing inter-GSM carrier (GRX) networks and removes the need for bilateral agreements between all interconnected carriers. This inter-carrier IP network is known as an IPX network.

In addition to simple connectivity, the IPX network provider can also protect and monitor the inter-carrier links by providing a centralized SBC service within the IPX network. An SBC in this role is known as an IPX proxy.

The work of the GSMA has fed into the 3GPP and TISPAN standards, in particular into the IBCF requirements. See *Advanced requirements for IP interconnect (3GPP TR 22.893) and Infrastructure ENUM Options for a TISPAN IPX (ETSI TR 184 008).*



2.4 Support for Enterprise Customers

The interface that the carrier presents to an enterprise customer does not always conveniently fit into the Access or Interconnect models described earlier.

ETSI TISPAN uses the following definitions[2] for the types of service that a carrier may offer to its enterprise customers.

A **Transport Service Provider** provides an IP pipe to the Internet or between enterprise sites (VPN-service). The carrier is not session-aware, so does not deploy a Session Border Controller.

A **Session Service Provider** acts as a transit network for calls. The carrier provides session control through processing of the call signaling, which may include the following services: guaranteed QoS for signaled media, call routing, and NAT traversal. It does not provide any intelligent call processing as it does not manage individual user identities. This is a peering relationship, so the carrier may deploy an Interconnect SBC.

An **Application Service Provider** provides higher-level applications, such as intelligent call routing, voicemail, presence, and conferencing. Individual applications can be hosted by either the enterprise or the carrier. For example, the enterprise may provide its own PBX, but use a carrier-hosted voicemail service. Many variants are possible and an "Application Service Provider" may interface to an enterprise using a subscription-based arrangement (Access SBC), where the enterprise appears to the carrier as multiple separate phones, or a peering arrangement (Interconnect SBC).

It is envisaged that each enterprise will combine services from different carriers to create its particular corporate solution.

To support enterprise customers, a carrier SBC may need to provide different behavior for different customers, depending on their contracted services, and even differentiate between "internal" inter-site traffic and "external" traffic to/from third parties. For example, "internal" signaling may pass unchecked so that the enterprise can implement proprietary features, but these same proprietary features may be removed from external traffic to prevent interoperability and security issues.

The carrier SBC may also need to interwork with non-IMS networks. For example, the SIP Forum's "SIP Connect" initiative offers an alternative SIP-based standard for interconnection between enterprises and carriers.

2.4.1 Enterprise SBCs

On the enterprise-side of the interface, the enterprise may deploy a Session Border Controller to

- police and monitor the traffic entering and leaving its network
- control traffic across otherwise unmonitored links, such as those provided by a Transport Service Provider
- protect traffic traversing insecure links, such as connections across the Internet, by encrypting the media and signaling flows.

Alternatively, a carrier may also offer an Enterprise SBC service, either physically located at the enterprise site or hosted by the carrier, where it could be part of the carrier's border router. In this case, the carrier could extend its managed network to include the enterprise so as to ensure QoS for the media streams across the enterprise LAN.

The enterprise environment and Enterprise SBC function are not currently covered by the TISPAN or 3GPP standards. However, the standards are likely to expand into this area to ensure that carrier-hosted services can be provided to devices within the enterprise

[2] TISPAN work on enterprise requirements is covered by the following documents.

- Business Communication Requirements (ETSI TS 181 019).
  - Core and enterprise NGN interaction scenarios; Architecture and functional description (ETSI TS 182 023)
  - Hosted Enterprise Services; Architecture, functional description and signaling (ETSI TS 182 024)
  - Business trunking; Architecture and functional description (ETSI TS 182 025)

2.5 IPTV Support

Video is viewed as one of the killer applications for carriers, so NGNs must support IPTV, as well as voice and data services. However, its high bandwidth and low latency requirements can place huge demands on network resources.

A scalable solution capable of delivering mass-market IPTV services requires network optimizations, and all of the following are being considered.

- Broadcast or multicast routing for streams to multiple viewers, e.g. for live shows. These reduce the resources required throughout the network. Broadcast and multicast streams can be provisioned in access routers using the same mechanisms as unicast streams[3].
- A parallel "content network" to the main core network for video with local caching of popular content. This improves responsiveness and reduces load on the main core.
- Where there is spare access network capacity, peer-to-peer solutions can reduce load in the core of the network and on the media source. This approach is more appropriate to fixed than to mobile environments and is discussed in TISPAN; Peer-to-peer for content delivery for IPTV services: analysis of mechanisms and NGN impacts (ETSI TR 182 010).
- IPTV delivery can be controlled by a dedicated non-IMS control plane. This approach allows greater reuse of existing TV investments and greater control of the customer's TV experience due to limitations in the current IMS standards. See IPTV Architecture; Dedicated subsystem for IPTV functions (ETSI TS 182 028).

Session Border Controllers supporting IPTV may need to control IGMP/MLD requests to restrict multicast streams to authorized subscribers and distribution of encryption keys for the selected media streams.

The Session Border Controller may itself act as a multicast router and replicate multicast packets, or may act as an IGMP proxy and pass authorized IGMP requests to an upstream router. The standards leave flexibility in exactly where multicast functionality is implemented, as this decision depends on the availability of resources to hold the required multicast state and to replicate packets.

ADDITIONAL BENEFITS OF SESSION BORDER CONTROLLERS

THE IMS MODEL PROVIDES A SOLID FRAMEWORK FOR NETWORK PROTECTION, BUT IT DOES NOT STANDARDIZE ALL VULNERABLE AREAS AND IT ASSUMES A CERTAIN LEVEL OF STANDARDS COMPLIANCE BY DEVICES ACCESSING THE SERVICE.

In the real world, the carrier network must be protected against concerted malicious attack, as well as misbehaving devices. Session Border Controllers offer extensions to the IMS-defined behavior to provide more customizable operation to deal with the complexities of real-world deployment.

3.1 DoS protection

The flow-based policing that IMS defines allows the carrier to configure bandwidth limits for signaling flows, as well as media flows, in the access gateways. These can be used to control simple DoS attacks from misbehaving endpoints.

An SBC can provide more intelligent protection from malicious endpoints through analysis of the signaling messages and correlation between flows to detect Distributed Denial of Service (DDoS).

Once identified, malicious traffic is blocked as close to the source as possible.

3.2 Enhanced privacy

IMS standardizes manipulation of fields in the SIP signaling in the border gateway (P-CSCF, I-CSCF or IBCF). Removal of some identifiable fields, such as the Call-Id or dialog tags, requires the gateway to operate as a SIP Back-to-Back User Agent (B2BUA). This is one of the reasons that most SBCs are implemented as B2BUAs rather than as pure SIP proxies.

The IP address of the endpoint may identify the user. For calls that are marked as "private", any identifiable endpoint IP address in the media or the signaling must be removed, for example, by using a media relay or NAT to hide the real IP address.

In the IMS architecture, identifiable media addresses are not expected to be an issue. Endpoint addresses used within the carrier core are normally dynamically allocated by the carrier so they cannot be resolved by a third-party to identify the user. Where the media address is required to be hidden, the SBC must control a TrGW (see 2.1.1).

[3] 3GPP defines the Multimedia Broadcast/Multicast Service (MBMS) in 3GPP TS 23.246. ETSI TISPAN defines similar extensions to allow flow descriptions to represent a multicast stream.

3.3 Interworking

The Access SBC typically handles a large number of separate connections from individual users and a wide range of equipment, so it has to deal with a wide variety of protocol variants and network topologies, which makes interworking a major challenge. To make this issue more manageable, the carrier is often forced to limit the range of devices that it is prepared to support.

The Interconnect SBC typically handles a smaller number of high-volume connections with peer carriers. Each interconnect agreement typically specifies the supported capabilities in great detail, so one of the Interconnect SBC's roles is to adapt the signaling and media flows to match the agreement with the selected peer.

3.3.1 Signaling Interworking

The TISPAN-defined Interworking Function (IWF) provides interworking between SIP variants and to other signaling protocols, such as H.323. Its role is to allow the IMS core to work with non-standard devices without requiring the core devices to support multiple signaling variants. The work required depends on the external protocol variant being handled; therefore it can only be achieved in a non-standard way.

The architecture currently only includes an IWF on the peering interface, as the devices attached to the access network are assumed to fully conform to the specifications. In reality, interworking is also required on the access side to handle non-compliant and legacy devices like PBXs. This can be provided by adding interworking features to the Access SBC.

3.3.2 Media Interworking

For commercial or technical reasons, a carrier may allow only a specified set of codecs or a limited number of media streams across its network. Equally, it may wish to support calls between devices with incompatible codecs. A Session Border Controller can help by filtering the requested media capabilities (SDP) to allow only permitted codecs through, or by redirecting the media through a transcoder.

However, IMS does not expect this functionality to be provided through border policy. Instead, it is expected be provided through S-CSCF / Application function in the core of the network.

The limitation of the IMS approach is that it requires the network core to know the access network capabilities and subscriber policy for both the caller and the callee. Without this information, it cannot proactively determine whether a transcoder is required, and must instead rely on the initial call setup attempt failing, before retrying with a transcoded call.

If, instead, the destination P-CSCF does the filtering, it can know which codecs are acceptable so it can proactively filter on behalf of the destination access network, and set up transcoding proactively.

The limitation of the border approach is that the call must be re-signaled if the capabilities of the access network change, as this may change codec policy.

Another limitation is that transcoding may be performed at the border of either the caller or callee's network, or of a visited network if either party is roaming. When viewed as a chargeable service provided to a subscriber, this requires more complex authorization and reconciliation between the network providers.

Session Border Controllers can support both approaches and, in principle, an IMS network could use either one, as IMS forces the endpoint to re-signal the call when it detects an access network change. However, the border approach is not currently covered by the standards, but it is an area of ongoing discussions in the standards bodies.

SBC DESIGN REQUIREMENTS

SESSION BORDER CONTROLLERS HAVE A WIDE RANGE OF CAPABILITIES, NOT ALL OF WHICH ARE RELEVANT TO EVERY ENVIRONMENT. THEREFORE THE ABILITY TO SPLIT THESE CAPABILITIES INTO SEPARATE FUNCTIONAL COMPONENTS IS REQUIRED. THE IMS ARCHITECTURAL MODEL IS ONE SUCH EXAMPLE. HOWEVER, IMS DOES NOT DICTATE HOW THESE FUNCTIONS SHOULD BE MAPPED ONTO PHYSICAL DEVICES, SO SESSION BORDER CONTROLLERS NEED A MODULAR DESIGN THAT MATCHES THE DIFFERENT DISTRIBUTION OPTIONS.

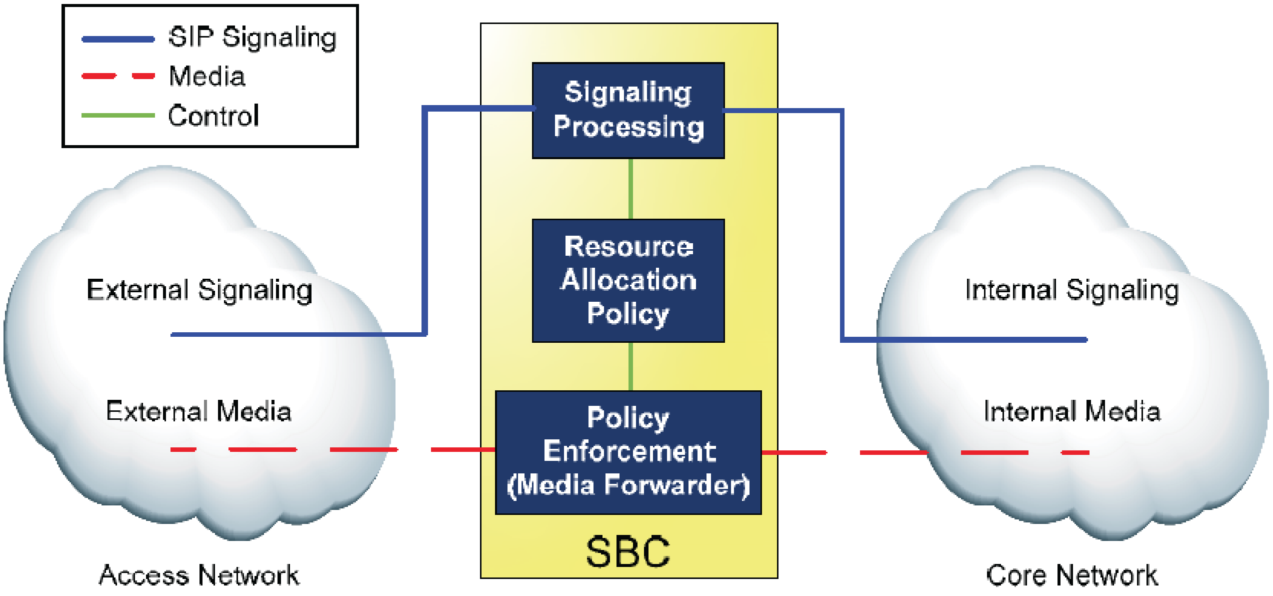
This section discusses how SBC function can be packaged into deployable products that suit the scale and operational requirements of each environment.

4.1 Integrated SBC

An integrated SBC is implemented as a single standalone device that is placed in front of existing equipment in the path of all the signaling and media traffic on an interface. This one box includes the media and signaling processing, as well as the media resource control.

The advantage of a standalone SBC is that it provides clear delineation of function, so the effect of interworking and protection controls can be isolated when diagnosing problems. It can also be the only practical solution when the existing deployment is old and heterogeneous so existing devices are difficult to extend, or when the SBC feature set is only required for a minority of customers, so upgrading existing devices would risk significant destabilization.

However, this architecture adds another device into the network, increasing the network's complexity and latency, and introducing another point of failure.

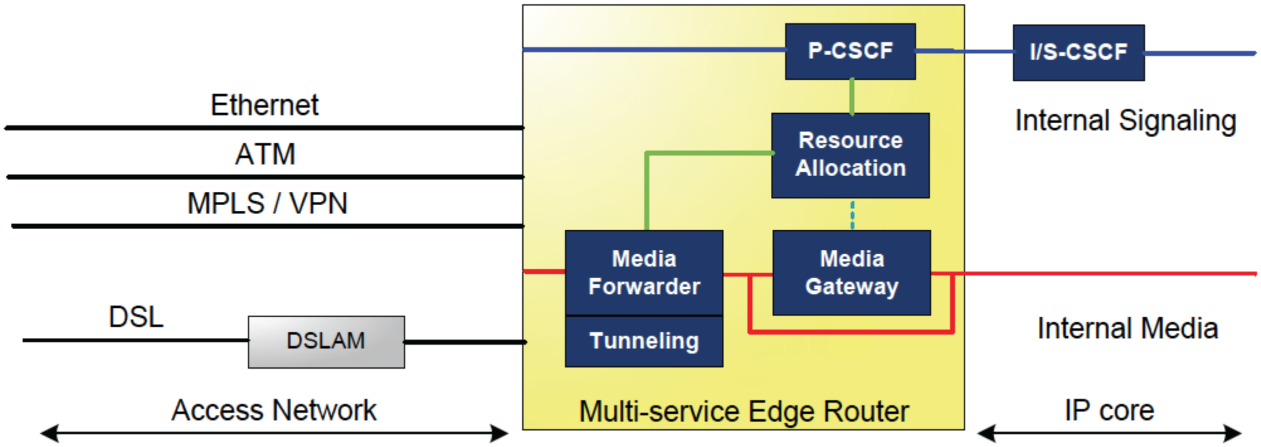


4.2 Integration into Existing Devices

Session Border Controllers are increasingly deployed as part of existing network elements, such as edge routers, rather than separate devices in the architecture. For example, the proportion of operators using SBC features embedded in a router is expected to rise from 5% in 2009 to 32% by 2011[4].

One example is the Multi-Service Edge Router, which provides a single-box access solution for multiple types of access network, including tunnel-termination, authentication, access controls, and trafficshaping. Multi-Service Edge Routers are widely used by carriers migrating to a converged network, as they support a wide range of legacy access services in a single device.

By adding signaling processing, an intelligent edge router can provide an integrated SBC for multiple access networks, including signaling interworking, NAT traversal, and topology hiding. In this scenario, the service provider does not have to purchase, install and manage a separate physical platform. Rather the SBC function is often served on a single or small number of line cards.



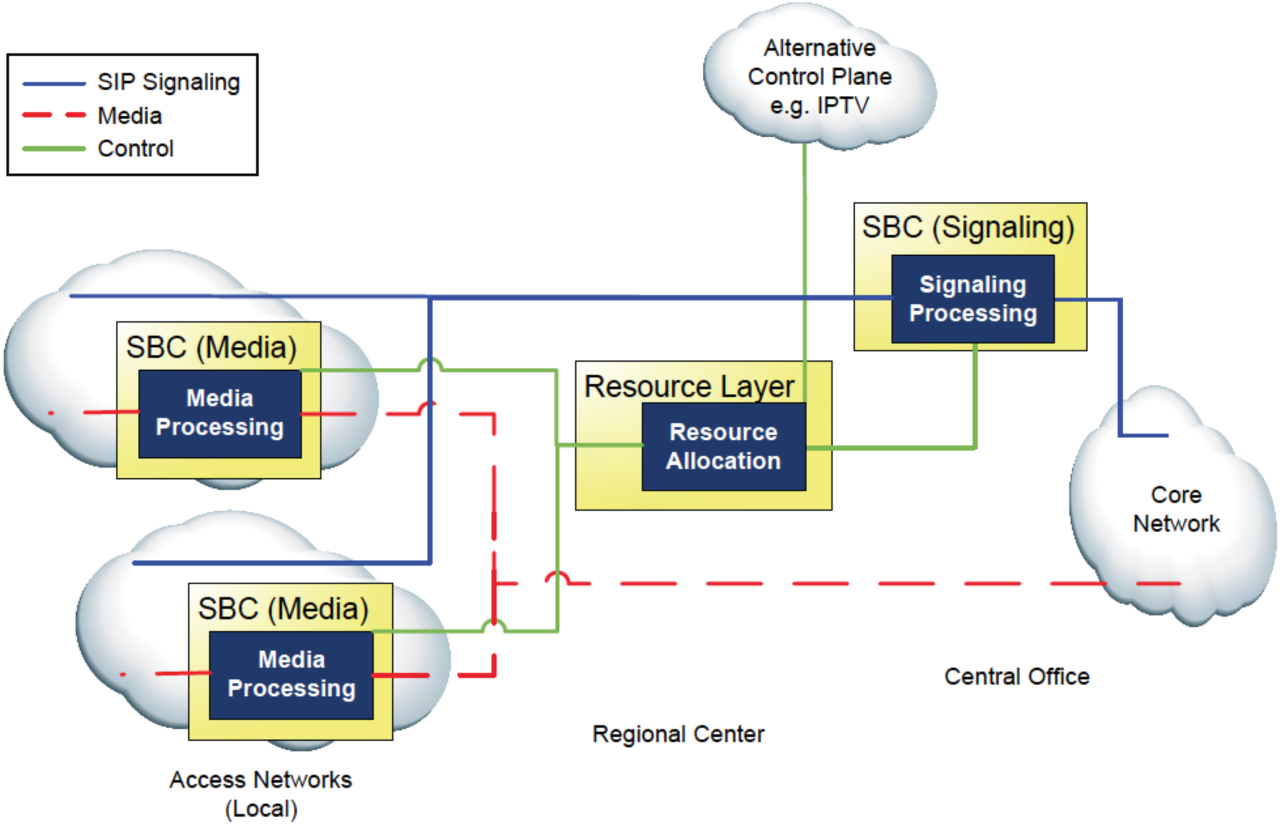
[4] SBC Deployment Strategies: Global Service Provider Survey 2009, Infonetics Research, Inc.

4.3 Plane Separation

Although in small-scale applications it can make sense to include media and signaling processing in a single device, this solution does not scale well to the requirements of larger service providers. For these applications, the media, signaling and policy processing will often be split into separate devices, with the signaling processing clustered into regional server farms, and the media processing distributed closer to the user. This provides economies of scale on the signaling processing, whilst maintaining direct media routing to minimize network transit delays.

The hardware requirements for signaling and media processing are very different: media processing often requires specialized hardware to achieve the necessary media QoS, but standard COTS components give better signaling performance. Plane separation allows the use of separate hardware platforms to match these different requirements and ensure that expensive media processors are only used for their specialized purpose.

This arrangement also enables the use of multiple control planes to share the same media resources, for example, as used by the dedicated IPTV control plane described in section 2.5.

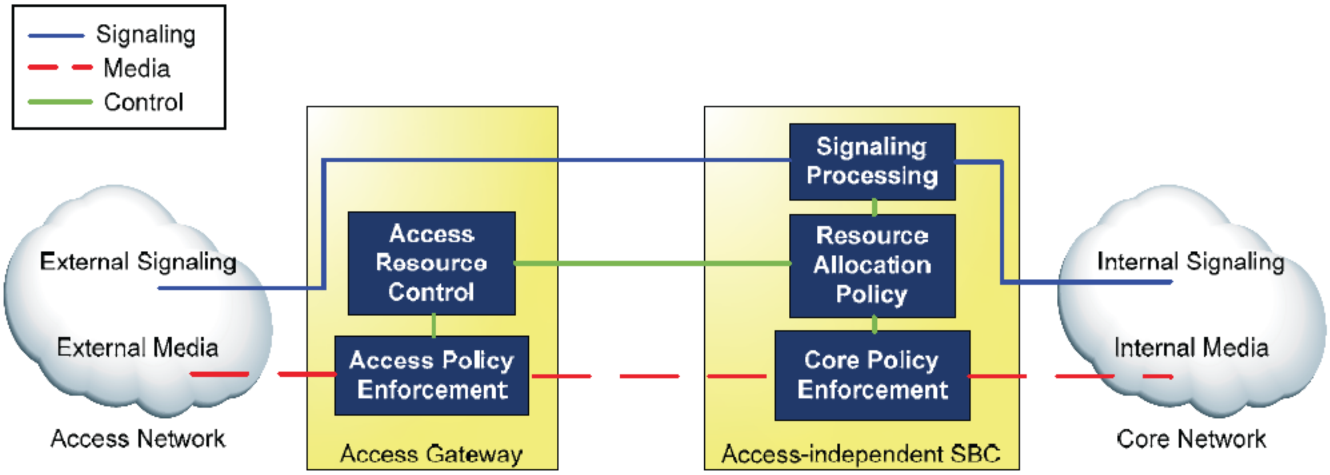


4.4 Access Network Control

Control of the access network resources can also be partitioned to a separate device. Each access technology requires different resource control processing, so this split enables the deployment of access resource control devices that are tailored for each access technology.

This arrangement also enables a carrier to control several different access networks using a single set of policies, which simplifies the provision of a consistent user experience as a subscriber roams between devices and access media.

Different standards bodies have defined their own functions and interfaces to control the access technologies used by their members. The following sections explore the different access architectures defined by each standards body, and how the access SBC maps on to these environments.



4.4.1 TISPAN

The TISPAN architecture is designed to meet the requirements of fixed-line (DSL-based) carriers. In these environments, the subscriber is tied to the physical connection and a single subscriber may have multiple devices sharing the connection.

The access architecture contains the following main functions.

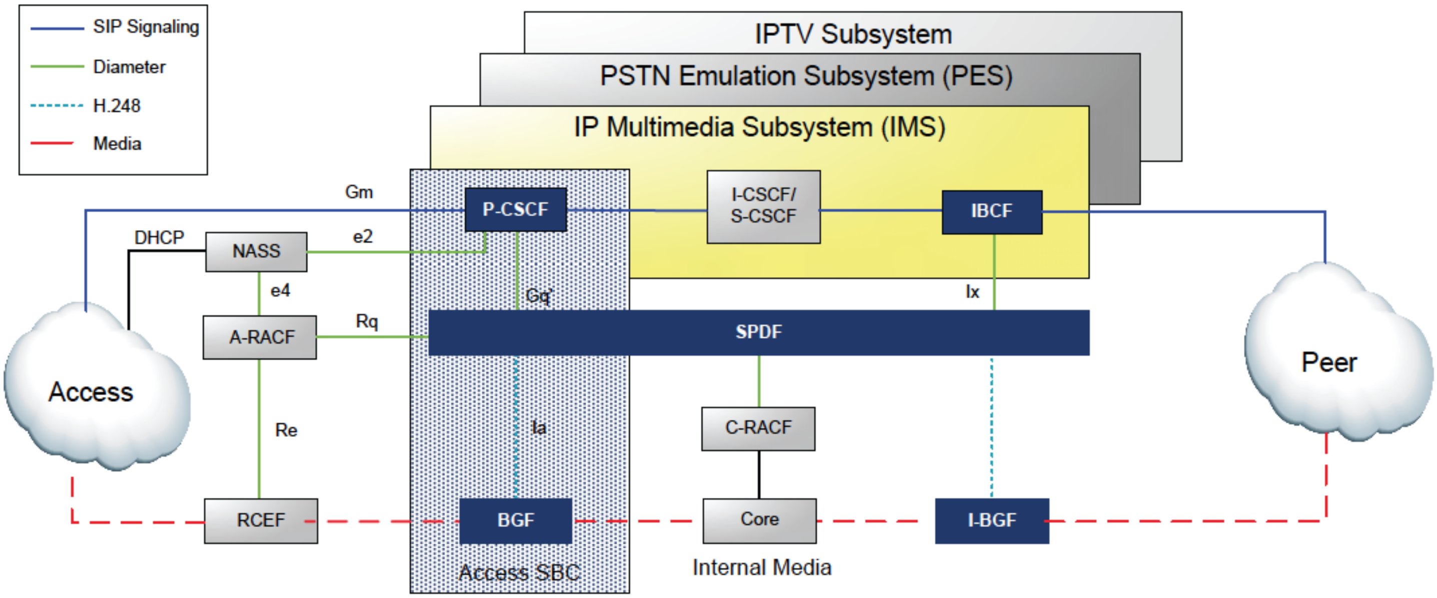
- The Network Attachment Subsystem (NASS) provides network connectivity to users on the access network. It authenticates user equipment, assigns its IP address (DHCP), and programs the ARACF with the initial set of services, for example, to provide Internet access.
- The A-RACF controls the access network resources and installs bandwidth controls and routing policy on the access routers (RCEF). The A-RACF receives requests for session-based QoS resources from the SPDF. It compares them against carrier-configured policy and available network resources, and tells the SPDF whether or not a request is granted.
- The SPDF mediates between application-level media resource requests (media descriptors) and the available network resources. TISPAN has defined several alternative control planes that can make requests on the SPDF. IMS is one of these control planes. Others are PSTN Emulation Subsystem (ETSI ES 282 002) and IPTV Subsystem (ETSI TS 182 028).

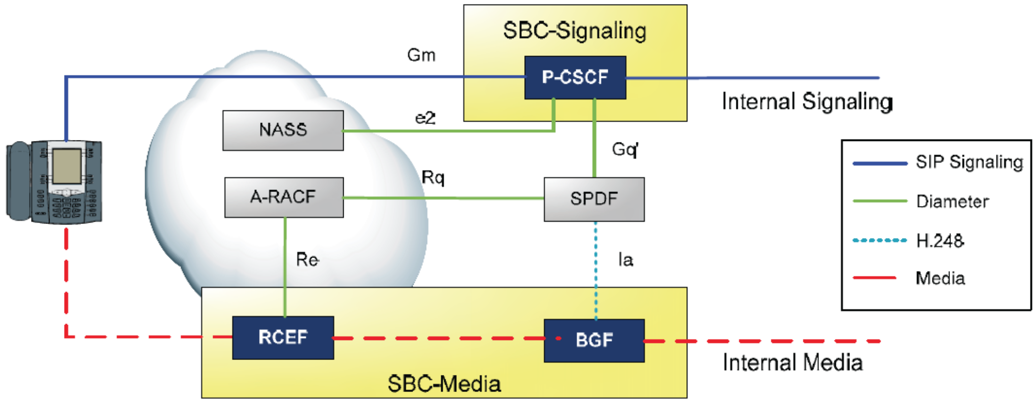
In the TISPAN architecture, the Access SBC comprises the P-CSCF together with the SPDF and BGF. It may export the

- Rq interface to one or more A-RACFs to reserve access network resources
- e2 interface to obtain user location information from the NASS, which is used to identify the SPDF that is managing the access resources and for emergency call routing.

If the SBC is split into media and signaling devices, it exports the

- Ia interface to control the BGF at the core network border, which applies QoS attributes, NAT, NAT traversal, and bandwidth controls to the media.





The SBC may also be deployed with a separate SPDF. In this case, it exports the Gq' interface to the SPDF to communicate media requests.

The BGF may also be integrated with the access routers (RCEF). In this case, the media device exposes the

- Re interface to program the media flows
- Ia interface to control NAT and interworking features.

4.4.2 3GPP

The 3GPP access architecture is designed for mobile access, which includes

- roaming subscribers, where policy and billing are coordinated with another carrier
- pre-pay subscribers, where subscribers may be cut-off when they run out of credit.

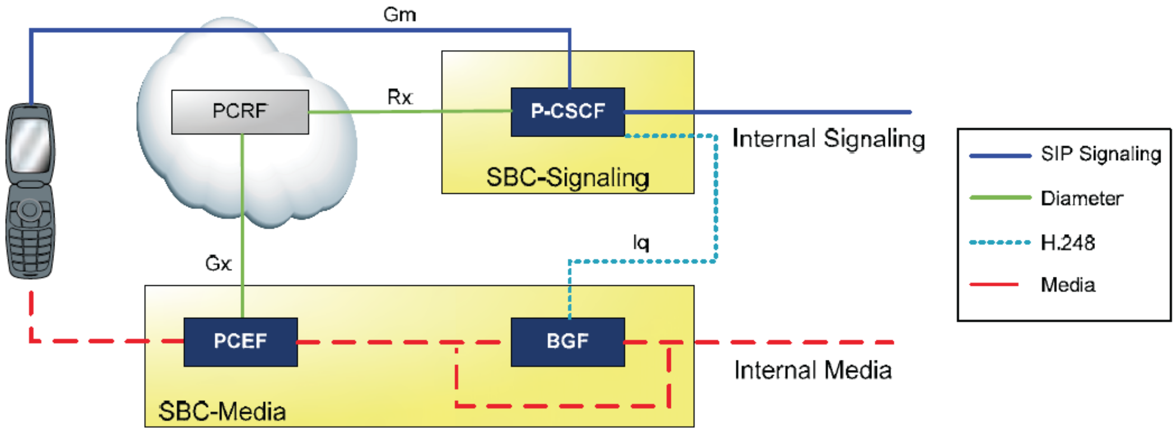
These require a dynamic registration and location tracking process that enables authentication and policy to be delegated to a peer carrier, and for authorization to be withdrawn when credit runs out.

Users are identified by a Subscriber Identity Module (SIM) in every handset, wherever it attaches to the network. All policy is tied to the subscriber identity and is held in the Subscriber Policy Repository (SPR). The PCRF coordinates access resource policy with input from the SPR and carrier-configured rules, and installs routing policy in the access routers (BBERF and PCEF).

A 3GPP Access SBC exports the

- Rx interface to the PCRF to specify the media resources required within the access network and report location information.
- Iq interface to a BGF, but this is only required for media services that are not provided by the PCEF, such as NAT-related functionality, transcoding, and DTMF interworking.

In most scenarios, a BGF is not required in the media path, as the User Equipment is an approved phone that does not need media interworking.



4.4.3 PacketCable

Cable carriers have similar requirements to fixed-line carriers in that subscriber identity is tied to a physical connection. They also run multiple services over the same network, using different control architectures.

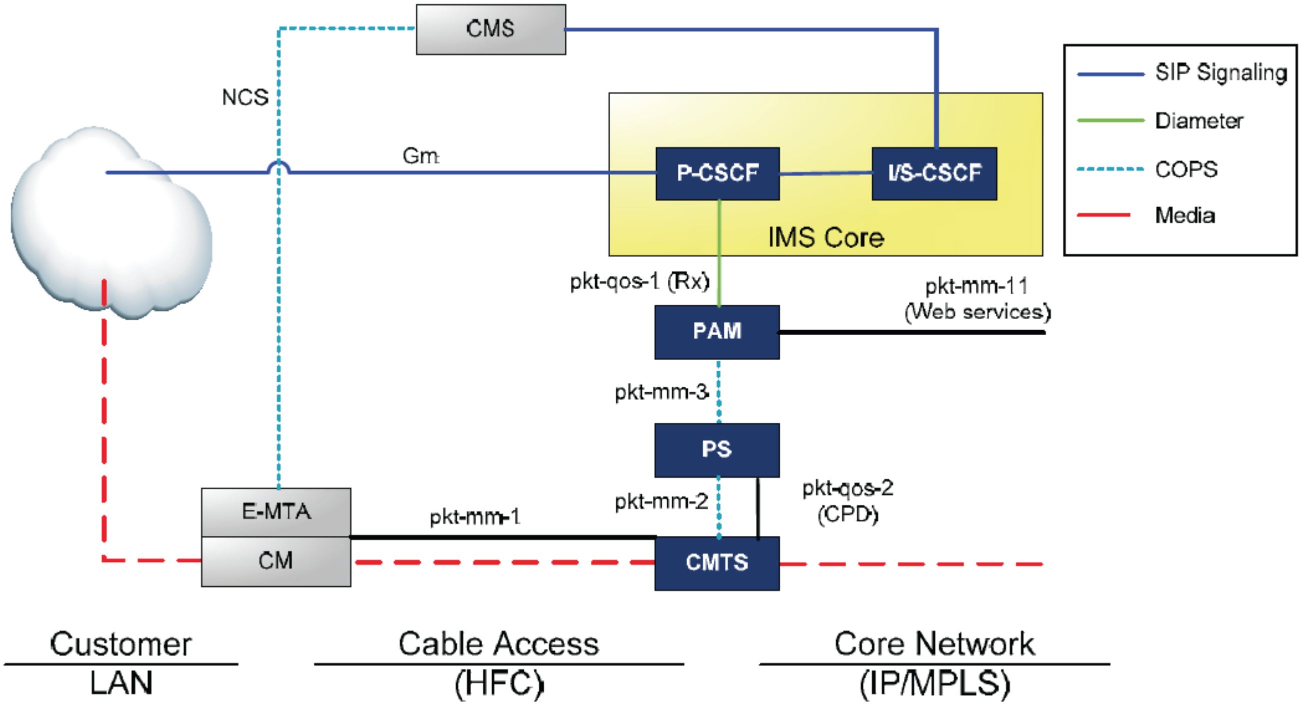
In the PacketCable architecture, the 3GPP-defined PCRF is split into a PacketCable Application Manager (PAM) and a Policy Server (PS). This split enables multiple Application Managers to control the same network resources over the pkt-mm-3 interface. A PAM is an example of an Application Manager.

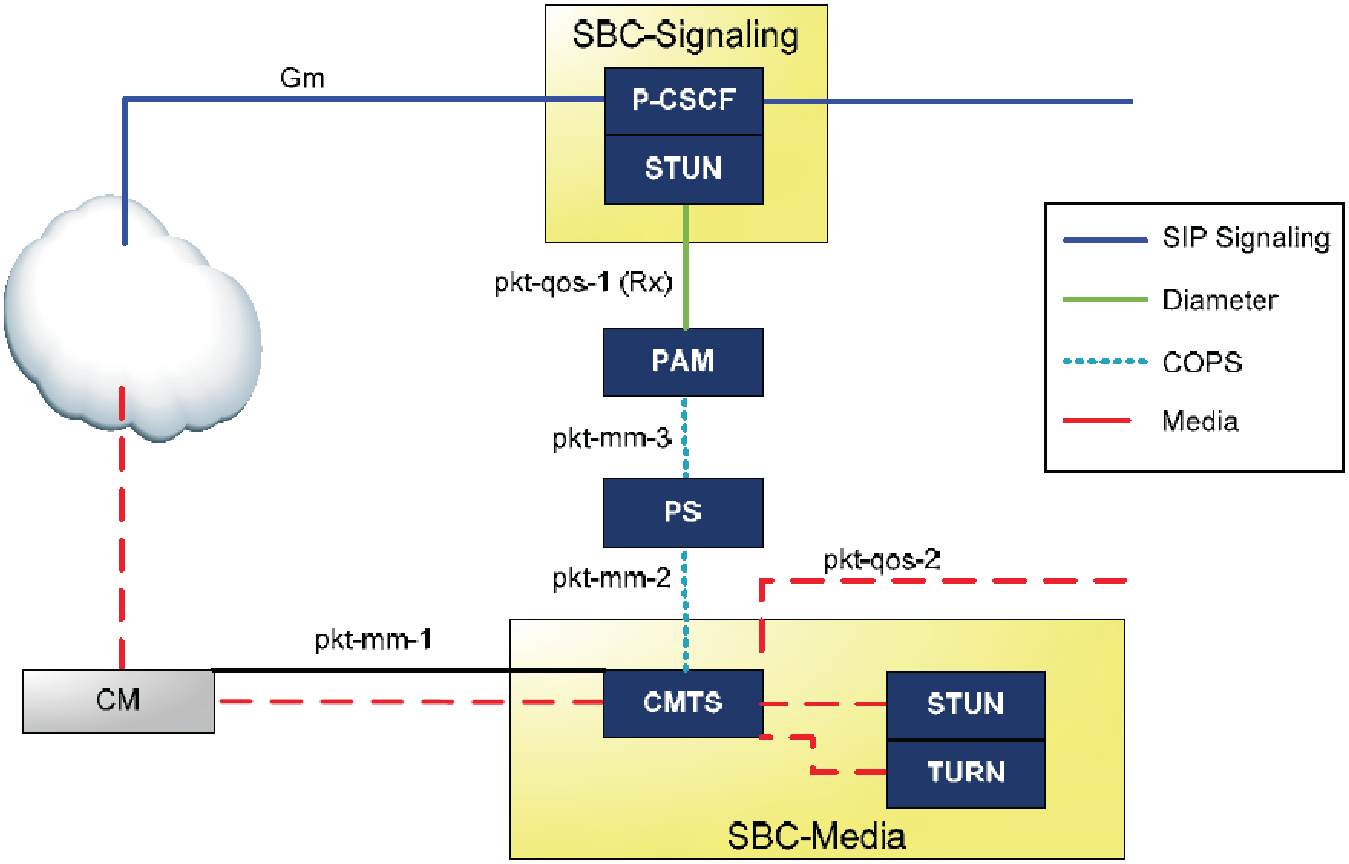
- The PAM determines the QoS requirements for application-specific resource requests (media descriptors) and translates them into PacketCable Multi-media (PCMM) requests, which it forwards to the PS.
- The PS ensures that resource requests meet the configured network policy and installs QoS policy on the Cable Modem Termination System (CMTS).
- The CMTS classifies traffic to the end user and routes it over the appropriate bearer. It also pushes filters to the Cable Modem (CM) for classification of traffic from the end user. On attachment, the CMTS assigns the user's IP address and primary flows. The primary flows are used for non-QoS flows, such as Internet connectivity.

The PacketCable network must also continue to support legacy access from NCS-compliant endpoints. These can be supported through an interface between the Call Management Server (CMS), which acts as a gateway between the Embedded Multi-media Terminal Adaptors (E-MTA), and the IMS core.

A PacketCable Access SBC exports the Rx interface to the PAM, like the 3GPP Access SBC. This interface specifies the media resources required within the access network and reports location information.

There is no BGF in the PacketCable architecture. Instead, the PacketCable standards advocate using STUN and TURN together with endpoint functionality to provide NAT and Firewall traversal: SIP outbound (RFC 5626) and ICE (RFC 5245), instead of SBC modification of the signaling and media flows.





4.5 Convergence of Access Network Architectures

As discussed above, each IMS-based NGN has its own access network control architecture.

- The PacketCable and 3GPP standards hide their differences behind a common Rx interface, so a single SBC could control either access network over this interface.
- The ETSI TISPAN architecture is significantly different from the others. It uses the Gq' and e2 interfaces in place of the Rx interface, and allows preliminary reservation of resources earlier in the call establishment process[5].

The sets of requirements and the resulting architectures have become more similar with each release, and TISPAN and 3GPP have formally attempted to merge the Rx and Gq' interfaces (3GPP work item SP- 070822). However, there is little political motivation to fully converge the approaches, and this effort was abandoned in March 2009 due to lack of contributions.

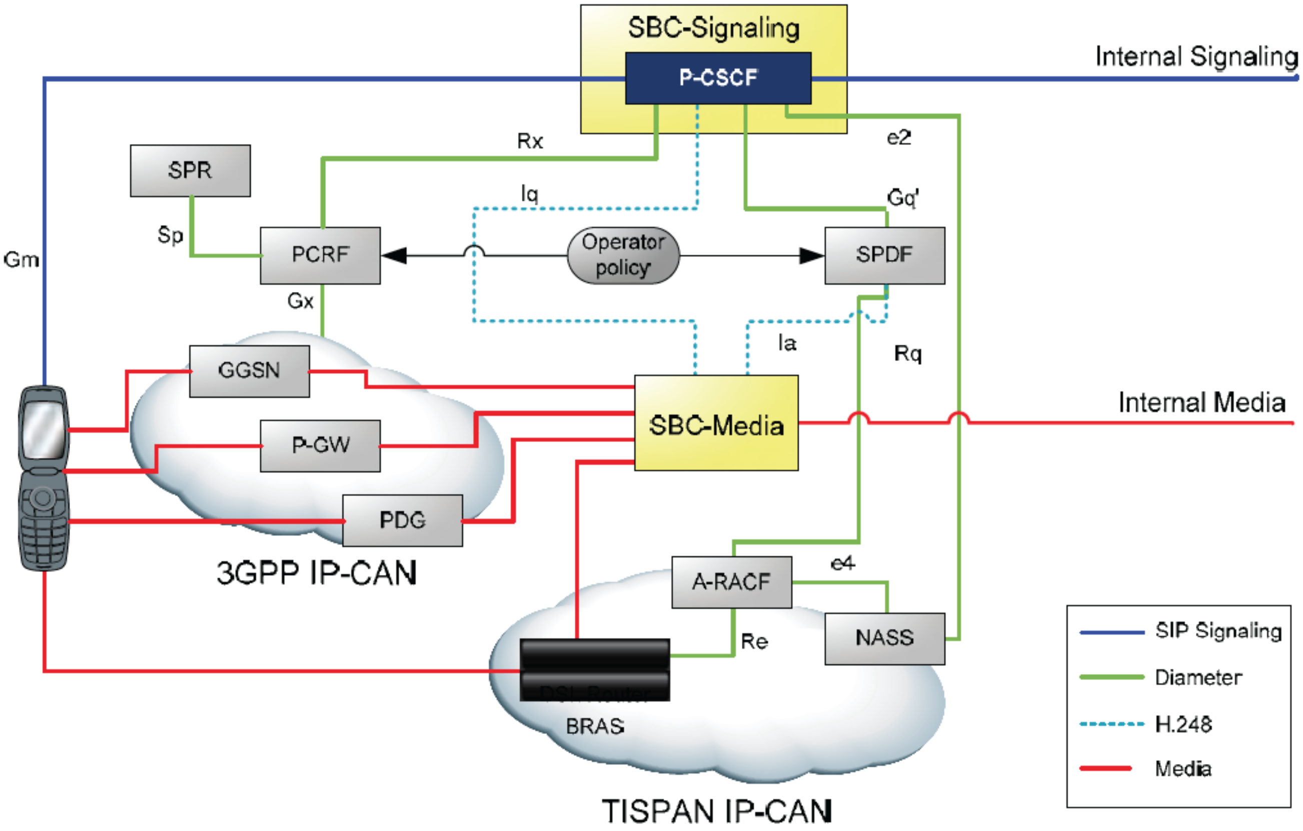
[5] The TISPAN interface includes the "Service-State". This field allows the resource allocation layer to differentiate between resource reservation resulting from processing an INVITE request, and those from processing an INVITE response. For example, the maximum level of overcommitted resources may be higher when processing requests to allow for rejected calls.

4.5.1 P-CSCF supporting both fixed-line and mobile access

Without a single resource control architecture, a P-CSCF can still provide the border gateway for both fixed and mobile networks, and a single media gateway can enforce the core policy / NAT functionality.

To support this environment, the P-CSCF supports both the Rx and Gq' interfaces, plus the Iq interface if NAT functionality is required on the mobile side.

- The advantage of this approach is that existing devices in the access networks do not have to be changed, which minimizes cost and risk of disruption.
- The disadvantage is that policy is stored and processed separately by each access technology and there is no coordination between them to ensure a smooth transfer of roaming calls. This segmented approach makes it more difficult to provide a consistent user experience as the user moves between fixed and mobile access.



4.5.2 Fully converged architecture

The standards bodies have found it difficult to agree on how to converge their access network architectures, and continue to take different approaches when extending their installed equipment. For example, both the SPDF and the PCRF have evolved from the Policy Decision Function (PDF) defined in 3GPP Release 5, but in incompatible ways.

- TISPAN added media routing decisions and NAT control (Ia) to its PDF and a separate A-RACF to control the media resources within a geographical area.
- 3GPP added charging rules and subscriber-based policy to its PDF, and have put NAT control (Iq) in the P-CSCF.

One converged architecture could be based on the TISPAN architecture, as shown below.

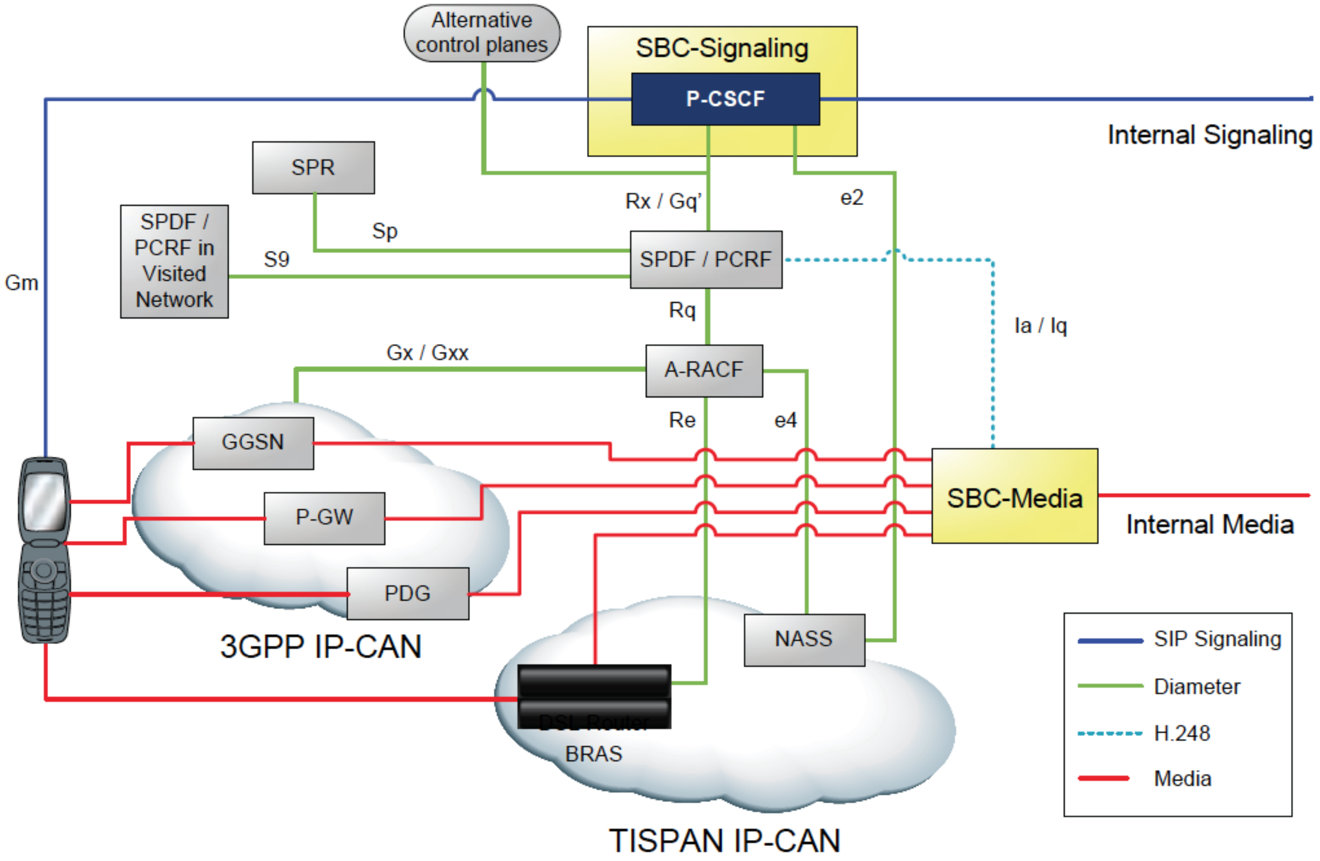
The SPDF

- is extended with the subscriber policy and charging rules from the PCRF
- exports the S9 interface that allows media resource requirements to be forwarded to an equivalent function in a visited network
- provides media routing and NAT control, which is removed from the P-CSCF.

The e2 interface remains to enable the P-CSCF to determine the SPDF to use, as this may depend on the location of the user – information that may not be reliably available from the call signaling.

The A-RACF incorporates the resource control function from the PCRF and exports the Gx and Gxx interfaces to control the 3GPP access network devices.

Given the level of upheaval that this would cause to 3GPP-based equipment and the lack of political will, it is likely that incompatible TISPAN and 3GPP-based access network (i.e. wireline and wireless access networks) will exist for the foreseeable future.



SBC DEPLOYMENT SCENARIOS

ALMOST ALL CARRIERS, WHETHER OR NOT THEY ARE IMPLEMENTING AN IMS-BASED NETWORK, REQUIRE SOME FORM OF SESSION BORDER CONTROLLER TO PROTECT THEIR NETWORK. THIS SECTION LOOKS AT THE TYPICAL DEPLOYMENT SCENARIOS FACED BY FIXED AND MOBILE CARRIERS.

5.1 VoIP access to a packet-switched core

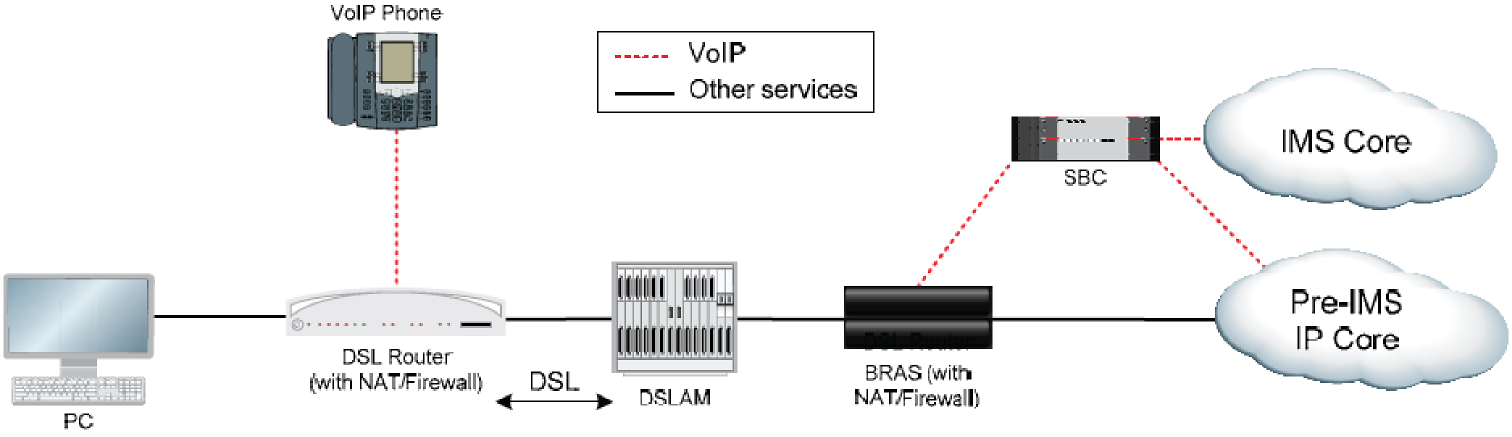
One of the most advanced areas of carrier SBC deployment is for a VoIP service from traditional fixed-line carriers.

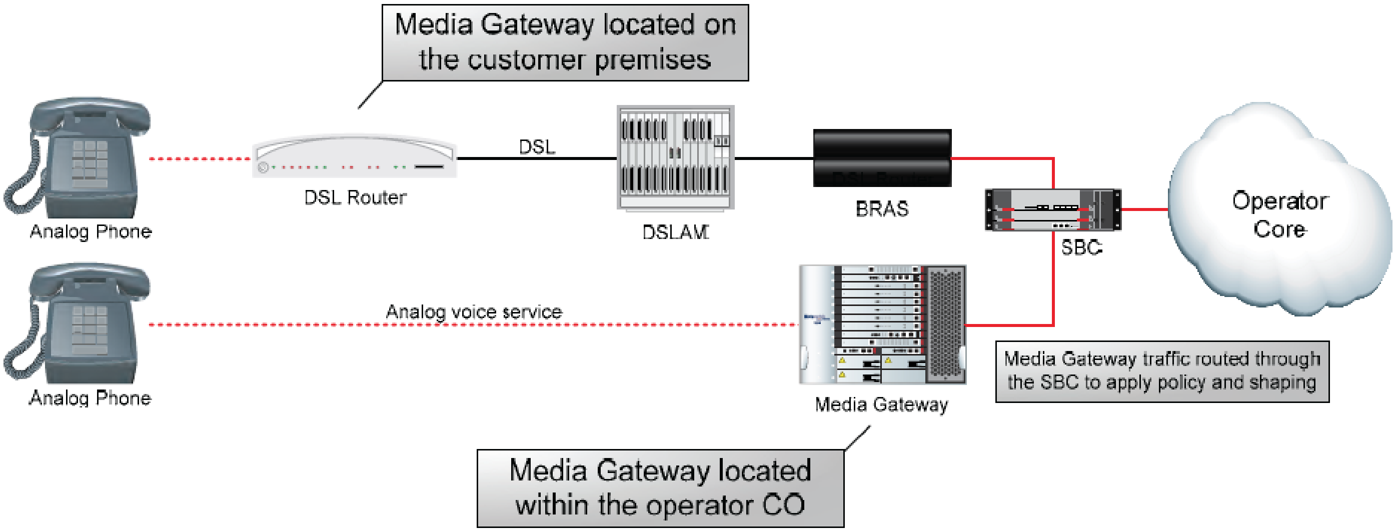
The SBC protects the carrier's IP core and ensures QoS over the access network, resolving the competing demands of voice, data and – increasingly – video.

It also can be used to provide a consistent service as the carrier evolves its core network.

- Initially SBC can protect the carrier's IP-backbone when adding a VoIP service to its broadband offering.
- Then, when the core network migrates to IMS, the same SBC can hide the internal changes from existing users and provide interworking between the existing broadband VoIP customers and the IMS core.

Depending on the scale of the deployment, the SBC may be deployed as a part of the edge router (BRAS), or as a distributed solution with centralized signaling processing and distributed media control, as discussed in Section 4.



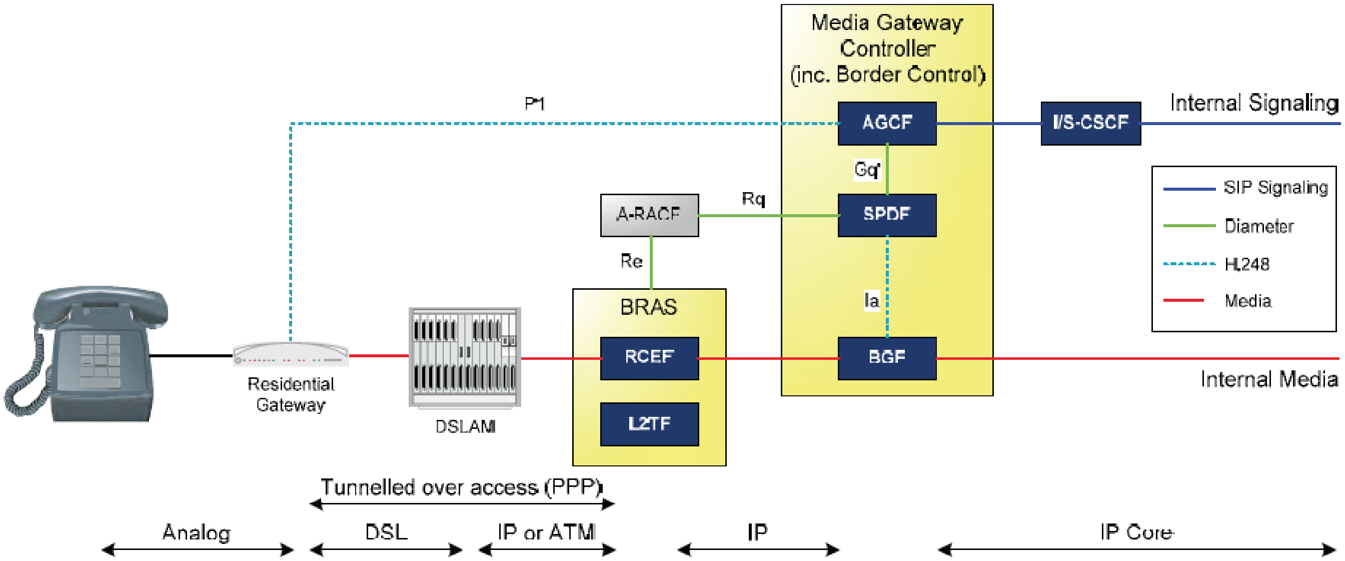

Media Gateway located on the customer premises
DSL
DSL Router
DSLAM
BRAS
SBC
Operator Core
Analog Phone
Analog voice service
Analog Phone
Media Gateway
Media Gateway traffic routed through the SBC to apply policy and shaping
Media Gateway located within the operator CO

5.1.1 Supporting legacy voice access

Even once the carrier has upgraded their core network to a converged packet-switched network, they must continue to provide voice service to their existing customers and their legacy equipment. The conversion between the analog telephony and packet-switched voice is provided by a media gateway. This gateway can be located anywhere from the customer premises to the central office (CO) at the edge of the core network, for example, it may be part of the customer's DSL router.

Where the media gateway is within the customer's premises, the interface to the media gateway (residential gateway) cannot be trusted as it passes across an open connection. The carrier can apply additional controls through the use of Session Border Control function within the media gateway controller to enforce bandwidth controls on the media traffic through the access network.

In this case, the Session Border Controller also provides interworking between the H.248 interface to the user and the internal SIP interface.



5.2 Mobile Networks

Mobile carriers have significant installed infrastructure to handle the requirements of their existing circuit-switched voice traffic, data traffic, and GPRS. With the evolution to a converged packet-switched core and improved radio access, enhanced mobile access gateways are required to control packet-based media services to the endpoints and circuit-switched access into the packet-based core.

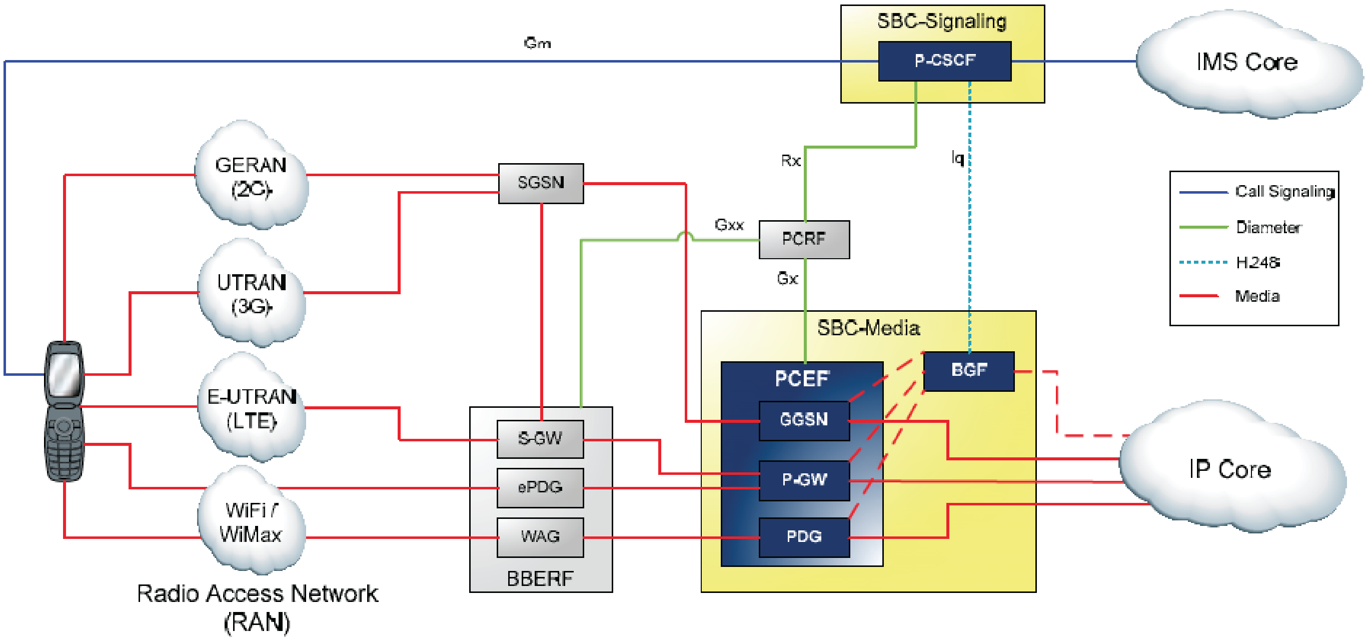
For mobile deployment, the Access SBC has to support a wide range of access technologies and tunneling techniques. This range is continuing to increase with the introduction of new radio technologies (WiFi, WiMax, LTE) and base station equipment, such as Femtocells.

5.2.1 Femtocells and WiFi Access Points

Femtocells and WiFi Access Points provide competing solutions for extending mobile access using thirdparty fixed broadband links at low cost for the mobile carrier. Both provide mobile coverage within a small area (< 100m) and are particularly suitable for high-bandwidth indoor applications, where traditional mobile coverage is difficult and expensive to provide.

The approaches differ in terms of the radio technology that they use (Femtocells use licensed spectrum, whereas WiFi uses unlicensed spectrum) and their compatibility with existing devices (handsets, access points and core components), and this affects where new functionality is required in the network.

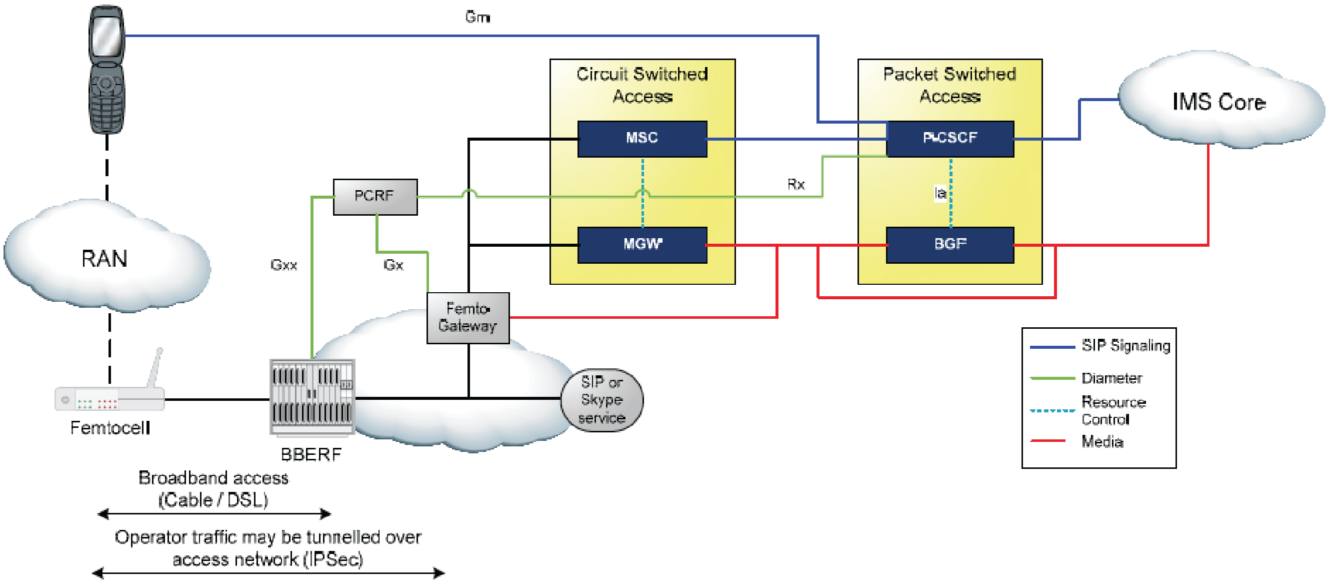
- Femtocells extend reach with minimal change for the end user, both in terms of handset technology and experience. The existing signaling and media protocols are tunneled over the access network through secure tunnels into the carrier core. Femtocell access is available from a number of carriers, although the technology is not yet widely deployed.
- WiFi access may follow a similar model with access tied to authentication by the mobile carrier and all traffic tunneled through to the carrier's network, or a more open model that allows the handset to contact alternative telecommunications service providers, for example, using a SIP or Skype-based client. WiFi access is widely available, but is less user-friendly due to its higherpower consumption and lack of integration with most handset clients and carrier services.



Legacy circuit-switched (CS) handset can also be supported. The CS media and signaling is tunneled over the IP access, then via gateways (MSC and MGW in the diagram below) into the IMS core.

Depending on the chosen architecture, the Access SBC may be able to rely on the Femtocell to provide authentication and packet filtering on behalf of the carrier, or control a BGF to handle NAT traversal of media.

A flexible Session Border Controller is fundamental to successful deployment in these complex cases, to handle both the standards-based behavior and the non-standard variants required to support real customers and their specific requirements.



THE FUTURE

SESSION BORDER CONTROLLERS ARE ALREADY WIDELY DEPLOYED IN ENTERPRISE AND CARRIER NETWORKS, PROVIDING SECURITY, EXTENDING REACH AND OFFERING A RANGE OF OTHER SERVICES. THIS SECTION LOOKS AT SOME OF THE FACTORS DRIVING THEIR EVOLUTION AND THE CHANGING OPERATING ENVIRONMENT IN THE YEARS AHEAD.

6.1 Evolution of IMS-based NGN Standards

As IMS has moved from a theoretical model to a deployed architecture, it has expanded to handle the inevitable complexities and extended requirements of real-world deployment. As a result, the IMS architecture now includes many common Session Border Controller features, such as NAT control and prioritization of emergency calls, which were missing in the early releases.

This process will continue as carriers attempt to codify the operation of their NGNs. However, strict adherence to the standards will matter less because the observed behavior of equipment in the large carrier networks will determine the commercial success of a product.

Session Border Controllers will maintain their vital role protecting the core network. They will need to support multiple access networks and several releases of the standards, plus the inevitable customizations made by each carrier. Interoperability and flexibility will be the key capabilities of the most successful products.

6.2 Government Regulation

Government regulations will have a number of effects on the market and the features that SBCs will provide.

Government action to require lawful intercept (wire tapping), mandatory quality levels and emergency services support may force all telephony service providers (including those providing pure VoIP services) to deploy managed networks with SBCs. However, unless governments make it illegal to communicate over P2P VoIP services (as they have in China), the effect of this sort of legislation just increases the cost of providing a traditional telephony service and increases the use of less regulated P2P solutions.

Arguments abound about the exact meaning of net neutrality, but as communications networks are, in most environments, natural monopolies, consumer protection will continue to be important. Regulations will be required to ensure that customers are able to choose their carrier, or combine services from a selection of carriers, even if the service is provided over a limited number of physical networks. These regulations will affect how far carriers are allowed to use the capability offered by SBCs to prioritize traffic and how they charge for their services.

The effect on deployed devices, such as SBCs, will be the increasing use of shared equipment, where a single device appears as multiple virtual devices, each controlled by a different carrier. This shared equipment may be at any level in the architecture, from media resources through to signaling processing. The interfaces between these virtual devices will continue to be those standardized by 3GPP and the other bodies.

6.3 QoS on the Customer Premises

The network on the customer premises is also handling a mixture of media, so it must also be QoSenabled to ensure suitable prioritization of real-time services. This is a concern for carriers that need to guarantee service quality end-to-end.

There are two options.

- The carrier takes responsibility for ensuring QoS within the customer network. This effectively extends their domain of control to include to the customer premises.
- The carrier only guarantees the performance to the entry to the customer premises. This is equivalent to today’s analog phone service. The issue with this option is that, as networks and devices become more complex, customers become less able to identify who is responsible for any problems they see and will blame the carrier anyway.

Both models will evolve, and carriers will increasingly offer a chargeable managed service that covers the customer premises; they will have to deal with all of the privacy and technical challenges that raises.

In terms of SBC function, the customer premises becomes part of the access network, so will be subject to the carrier policy exported over the Rq (or equivalent) interface. A carrier-managed router on the customer premises will enforce the policy.

For larger customers, the Enterprise SBC marks the boundary between the carrier and enterprise networks. It plays an important role as a QoS demarcation point – it can reliably report the QoS on each side, so allow areas of degradation to be identified and resolved by the party responsible.

As the carrier and enterprise networks become more sophisticated, the enterprise SBC may combine policy requests from the carrier with local configuration to determine resource allocation and media routing within the local network and across the access links.

6.4 Integration with Core Bandwidth Reservation

For enterprise use in particular, very high bandwidth services may be required on demand, for example, to support a new product launch or particularly successful media campaign.

In extreme situations, the increased demand may require the carrier to reconfigure their network core to satisfy the bandwidth requirement.

To allow these situations to be handled in an automated way, the SBC could provide intelligent media routing through its knowledge of the media requirements of all existing flows and, where necessary, request additional core network capacity through integration with the MPLS control plane of the network core.

6.5 Increasing Scale

The demand for Session Border Controllers of increased scale will be driven by

- high-bandwidth, mass-market IP services, e.g. IPTV
- carrier-hosted services, such as interworking of video conferencing between incompatible devices, and Unified Communications systems
- SPIT detection
- DPI for monitor and interworking.

Addressing this demand will require SBCs that are designed to distribute their processing and are able to take advantage of multi-core processors, multi-processor cards, multi-card chassis, and, where appropriate, cloud-based technology.

6.6 Continued Importance of Interworking

IMS has now been adopted by most standards bodies as the basis for their next generation network architecture, although deployment of IMS-based networks is in its early stages. Most current deployments are pre-standard and limited in scope, but are providing a valuable proving ground for the technology.

As IMS-based networks become more widely deployed, the devices developed to target this space will become more mature, and this will aid interoperability. However, there are other pressures that will increase, rather than decrease, the need for interworking, as provided by SBCs.

- The number of different devices and versions of each that are being used will increase. Each will have its own interpretation of the standards.
- The complexity of the services being offered will increase. This will introduce new interactions between the devices and use less mature areas of function.
- Not all carriers and users will adopt IMS, and interworking will be required on these interfaces.

Overall, Session Border Controllers will need to provide a wider range of interworking options, with each being required for a smaller set of flows. The requirement for SBCs will certainly not go away.

7. Conclusions

Early Session Border Controllers provided a stand-alone device on the network border to make VoIP work reliably, but they were viewed as a necessary evil. IMS has transformed the SBC into an integral part of a managed multi-media network and standardized much of its functionality and its interfaces.

The role of SBCs will continue to expand with newly standardized function being implemented as well as the proprietary features that are required for real-world deployment, such as interworking between protocol variants and countering new forms of cyber attack.

Their design needs to be modular, scalable and flexible to handle the huge range of potential deployments. Much of their function will be common to all environments, but they will offer different distribution models, external interfaces, and customized configuration options to match their target market.

At the top end, Session Border Controllers targeting Tier 1 carriers are becoming part of an integrated equipment vendor offering. Their function is distributed across the core and access network devices, and managed by legacy systems. This trend will continue with Session Border Controllers becoming less identifiable as a specific network device, but with their function remaining a fundamental part of all access gateways.

At the bottom end, Session Border Controllers will increasingly appear within residential equipment to ensure QoS all the way from the customer premises. They will be offered by service providers as part of a simple and reliable carrier-managed service that includes the customer's own network. The growth of femtocells provides a good indication of how this market may develop.

In between, Session Border Controllers will continue to exist as a stand-alone dedicated device, but will increasingly be deployed as a value-added service within an existing router.

Behind these targeted solutions, the underlying SBC functionality will become increasingly powerful, flexible, and extensible to address the disparate needs of each market, support new services, and handle new threats. For example, to address the needs of TISPAN and 3GPP access networks, carrier SBCs will support both the Rx and Gq' interfaces, although in many deployments only one of these interfaces will be exposed.

Metaswitch Networks developed DC-SBC, its carrier-grade solution for equipment manufacturers to meet the ongoing need for a comprehensive SBC solution. For more information on DC-SBC, please visit **www.metaswitch.com/sbc-session-border-controller/**.

8.1 Sources

CableLabs	http://www.cablelabs.com
ETSI TISPAN	http://portal.etsi.org/tispan
GSM Association	http://www.gsmworld.com
IETF	http://www.ietf.org
SIP Forum	http://www.sipforum.org
3rd Generation Partnership Project	http://www.3gpp.org

8.2 References

IP Multimedia Subsystem (IMS)

3GPP	TS 23.228 v9.0.0	Group Services and System Aspects: IP Multimedia Subsystem (IMS)
3GPP	TS 23.203 v9.0.0	Technical Specification Group Services and System Aspects; Policy and charging control architecture
CableLabs	PKT-TR-ARCH-FRMV06-090528	PacketCable™ 2.0 Architecture Framework Technical Report
GSM Association	IR.65	IMS Roaming and Interworking Guidelines
Metaswitch Networks	An Introduction to IMS: The Technology and The Motivation	

SBC

Metaswitch Networks	Session Border Controllers: Enabling the VoIP Revolution

SIP

Metaswitch Networks	SIP Market Overview	
IETF	RFC 3261	Session Initiation Protocol (SIP)
IETF	RFC 5389	Session Traversal Utilities for NAT (STUN)

8.3 Glossary of Acronyms

3GPP	Third Generation Partnership Program
ALG	Application Level Gateway
A-RACF	Access – Resource and Admission Control Function
B2BUA	Back-to-Back User Agent
BAS	Broadband Access Server
BBERF	Bearer Binding and Event Reporting Function
BCF	Border Control Function
BGCF	Breakout Gateway Control Function
BGF	Border Gateway Function
BRAS	Broadband Remote Access Server
CSCF	Call Session Control Function
CM	Cable Modem
CMTS	Cable Modem Termination System
COPS	Common Open Policy Service
DoS	Denial of Service
DSLAM	Digital Subscriber Line Access Multiplexer
E-CSCF	Emergency CSCF
GGSN	Gateway GPRS Support Node
IBCF	Interconnect Border Control Function
I-BGF	Interconnect – Border Gateway Function
ICE	Interactive Connectivity Establishment (RFC 5245)
I-CSCF	Interrogating CSCF
IMS	IP Multimedia Subsystem
IWF	Interworking Function
L2TF	Layer 2 Tunneling Function
MGCF	Media Gateway Control Function
MGW	Media Gateway
MRCF	Media Resource Control Function
MSC	Mobile Switching Center
NAPT	Network Address and Port Translation
NASS	Network Attach Subsystem
NAT	Network Address Translation
NNI	Network-Network Interface
P-CSCF	Proxy CSCF
P2P	Peer-to-Peer
PAM	PacketCable Application Manager
PCMM	PacketCable Multi-media
PDF	Policy Decision Function

PDG	Packet Data Gateway
PLMN	Public Land Mobile Network
PoC	Push-to-Talk over Cellular
PS	Policy Server
QoS	Quality of Service
RACS	Resource and Access Control Subsystem
RAN	Radio Access Network
RCEF	Resource Control Enforcement Function
S-CSCF	Serving CSCF
SBC	Session Border Controller
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOHO	Small Office Home Office
SPDF	Service-based Policy Decision Function
SPR	Subscriber Profile Repository
STUN	Session Traversal Utilities for NAT (RFC 5389)
THIG	Topology Hiding Inter-network Gateway
TrGW	Transition Gateway
TURN	Traversal using Relay NAT
UE	User Equipment
UNI	User-Network Interface
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAG	Wireless Access Gateway
WLAN	Wireless Local Area Network

8.4 About Metaswitch Networks

Metaswitch Networks is a leading provider of the technologies and solutions that are powering the migration of communications networks to open, next-generation architectures. Hundreds of network operators worldwide depend on its reliable, scalable carrier systems solutions, while its high performance, fault-tolerant software technologies are licensed by all the world's leading communications equipment manufacturers. For more information, please visit **www.metaswitch.com**.

8.5 About DC-SBC and IMS

Drawing from technology and experience from multiple divisions of Metaswitch Networks the Network Protocols Division has developed a fully portable Session Border Controller (DC-SBC) software solution designed specifically for system vendors. Metaswitch Networks' extensive VoIP and IP routing heritage provides equipment vendors with a field-hardened SBC solution that is deployable immediately, delivering dramatic cost and time to market savings.

Along with traditional session border controller functionality, DC-SBC also supports many of the vital functions required in IMS networks including P-CSCF, IBCF, SPDF, and BGF/I-BGF roles. Furthermore, Metaswitch Networks offers a full range of VoIP and IMS protocols stacks (DC-SIP, DC-Megaco/H.248 and DC-Diameter) that support the required interfaces and enhancements to fully operate in standards-based IMS environments.

For more information on Metaswitch Networks' VoIP and IMS stacks and solutions, please see **www.metaswitch.com**.

Metaswitch Networks is a trademark of Data Connection Limited and Data Connection Corporation. All other trademarks and registered trademarks are the property of their respective owners.