Session Border Control in IMS-based Converged Networks
Executive Summary

Session Border Controllers (SBCs) that can be physically separated into signalling and media elements are an essential part of building converged networks based on an IMS core. Between access and core networks, SBCs provide signalling security, Lawful Interception, Emergency Call Handling and, where required, NAPT, firewalling and traffic policing at the media layer. Additionally, they can direct users to the correct home network. SBCs have the advantage that, unlike most elements in this newly defined architecture, the functionality is deployable today.

It has become evident in recent years that a number of forces were leading operators towards convergence. Services can be accessed from a range of devices and users were rightly questioning why they could not have uniform access to services regardless of the type of access network being used. Upon seeing declining revenues, wireline providers started to consider ways to access wireless revenues. Wireless operators, in turn, have seen handset sales peak and must now consider ways to expand their markets as well; the most obvious area being converged business services.

The IP Multimedia Subsystem (IMS) defined by 3GPP provides an enabling architecture that is access independent. This is central in the move towards convergence. Now each access type is being ‘enabled’ to work with an IMS core, be it DSL, WLAN, GPRS or any emerging technology, such as WiMAX.

This white paper provides an overview of the different strands of standardization that are providing the base for converged networks to become a reality and describes some of the key functional elements. It then shows how the Newport Networks 1460 SignallingProxy™ and MediaProxy™ can be used to provide practical, secure and reliable access to an IMS core for wireless and wireline services.

Background: A Convergence of Standards

As a result of IMS becoming the convergence architecture of choice, a number of standards bodies are involved in defining converged architectures in both fixed and wireless networks. This section reviews the main players in this arena.

3GPP

3GPP (Third Generation Partnership Project) is really an amalgam of existing standards bodies, brought together to drive the specification and standardization of 3rd generation mobile. Standards bodies from Europe, USA, Japan, China and South Korea are all involved. It was at Release 5 that 3GPP introduced the IP Multimedia Subsystem, having previously defined the wireless access infrastructure, UMTS Terrestrial Radio Access Network (UTRAN).

IMS is basically an overlay to the packet-switched domain using Session Initiation Protocol (SIP) to provide multimedia services over IP. It re-uses much of the IETF definition of SIP, adding customizations for the requirements of mobility. It is important to note that the 3GPP IMS does not provide service equivalence to the circuit-switched domain. Hence, the migration towards an IMS only network, replacing a circuit-switched core, can be seen only as a long-term vision currently.

An important point of principle in the 3GPP Release 6 standards is that the IMS core is independent of access technology. This means that any specific requirements for mobile access should be dealt with by the access network, for example, compression requirements to optimize bandwidth usage. Practically, the IMS’s access independence is still not a reality for fixed network access and this is where TISPAN comes in.

ETSI TISPAN

The role of TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks) in ETSI is to standardize converged networks using IMS as its core architecture. This means adding the ability for fixed network access to interface to IMS and also requesting 3GPP to enhance the IMS specification where it has been found to be wireless specific. With the objective of moving existing PSTN functionality onto an IP core, IMS is now being focused on to provide PSTN emulation; this is effectively PSTN equivalence services. PSTN simulation services provide a definition of what must be provided as a minimum, for example, malicious call trace, but also allow for multimedia to provide additional enhancements to the service.
3GPP

The 3GPP2 group is using the IMS as a base for their Multimedia Domain (MMD) solution. This will allow CDMA2000-based access networks to provide third generation mobile services. The 3GPP2 core definition follows the IMS definition closely but there are differences to allow for the differences in radio technology. Interestingly, 3GPP2 has also allowed the use of IPv4 and the separation of GGSN and P-CSCF [see later].

TISPAN / IMS Structure

In Release 6 of the 3GPP specifications, the IMS has been specified to be access independent. This means that the access technology used to transport user SIP messages to the IMS network does not impact the functionality of the IMS network itself. Consequently, any access can be used, examples being DSL, Cable, WLAN, GPRS, etc. This is obviously a key step in the move towards converged network architectures.

The IP Multimedia Subsystem itself is made up of a number of component ‘blocks’ as shown below.

To simplify matters, items in Figure 1 shown in green are associated with PSTN egress and ingress and items in burgundy are associated with IP to IP SIP calls. The key functions are as follows:

**P-CSCF: Proxy Call Session Control Function.** This is the first point of contact within the IMS for a User Element (UE). The P-CSCF may be located in the home or visited network. In the context of fixed networks, the home network may be a wholesale network and the visited network may be a retail network that uses the wholesale network. The P-CSCF ensures that registration of the user is passed to the correct home network and that SIP session messages are passed to the correct Serving CSCF (S-CSCF) once registration has occurred. Contact with the home network during registration is through the home network I-CSCF and initial SIP session setup is through called party I-CSCF.

The P-CSCF is an important function as it is in the position to detect services, which should be hosted by the visitor’s network. This is important not only in terms of content services but also in the provision of Emergency Call Handling and Lawful Intercept. It also can provide defence against SIP signalling attacks.

**PDF: Policy Decision Function.** (Also known as Service-based Policy Decision Function in TISPAN). This function takes a service level policy request from the application layer (for example P-CSCF) and translates it into IP QoS parameters. For example, a G.711 call would be translated into real-time priority with 80 kbps IP bandwidth requirement. The access network is then asked if it can provide this QoS. What happens next will depend on the type of access network used. In GPRS networks, the PDF will use the ‘Go’ interface to set the policing policy for that session in the GGSN. In TISPAN-based networks, the PDF contacts the Border Gateway Function (BGF) to enforce the policy. There is an important difference here: GGSNs are not SIP session aware and hence they can only police on PDP sessions. SIP expects sessions to be able to handle multiple media simultaneously and this is not the case here. It means that 3GPP has had to define an additional parameter, which forces the session to set up a new PDP context for each new media stream in the session. Border Gateway Functions, however, are controlled from the application layer to enable a new media pinhole to be opened for each media component. Policing can therefore occur on a per-media component basis. This will allow the operator to ensure that the users’ media traffic is throttled or discarded if it exceeds the policy negotiated at the SIP layer.

**IBCF: Interconnect Border Control Function.** This function was introduced by TISPAN to formalize interconnect between networks. Its roles include the provision of NAPT and firewall functions for signalling, policing of signalling, topology hiding and conversion between IPv4 and IPv6. Whilst 3GPP networks are IPv6 only, 3GPP2 and wireline evolutions are likely to be a mixture of IPv4 and IPv6. The standard is also likely to specify the detection of failure of interconnect points. Through the control of a Border Gateway Function, the IBCF also controls the media exchanged across the operator boundary, controlling media pinhole establishment, policing, and dynamic NAPT and firewall functions.
ICSCF: Interrogating Call Session Control Function. This is the function that is able to determine the S-CSCF (Serving Call Session Control Function) with which a user should register. This is achieved by querying the Home Subscriber Server (HSS), which checks that the user is allowed to register in the originating network and returns an S-CSCF name and capability if this is the case. The ICSCF is then able to contact the S-CSCF with the register. The ICSCF function can be removed from the signalling path once it has been used to establish which S-CSCF is in use. The exception to this is if the THIG (Topology Hiding Inter-network Gateway) function of the ICSCF is being used.

S-CSCF: Serving Call Session Control Function. The S-CSCF is the function that registers the user and provides service to them (even though these services may be on separate application platforms). It performs routing and translation, provides billing information to mediation systems, maintains session timers, and interrogates the HSS to retrieve authorization, service triggering information and user profile. In short, it is the brain of the IMS.

HSS: Home Subscriber Server. The HSS is the database of all subscriber and service data. Parameters include user identity, allocated S-CSCF name, roaming profile, authentication parameters and service information. The HSS also provides the traditional Home Location Register (HLR) and Authentication Centre (AUC) functions. This allows the user to access the packet and circuit domains of the network initially, via IMSI authentication.

PSTN Ingress/Egress Functions. The PSTN ingress and egress functions allow interworking with the PSTN. Media Gateways provide the physical conversion between TDM and IP for media. Signalling Gateways provide translation at the transport layer between SS7 on MTP (TDM networks) and SS7 on SCTP (IP networks). The Breakout Gateway Control Function (BGCf) decides whether PSTN breakout will occur in the current network, or whether the SIP-I (ISUP over SIP) must first be sent to another IP network before breaking out. If it is the former case, then the signalling is passed to a Media Gateway Controller to then allocate a port on a Media Gateway for breakout. If it is the latter, the signalling is passed across the IBCF to another BGCf in the breakout network.

In the descriptions above, only the main functions of interest have been covered. For more complete subject coverage, the reader is referred to reference [1].

Roles of Session Border Control within a Converged Network

It is clear from the preferences of operators and the standards themselves that wireless networks require a signalling proxy function and wireline networks require both signalling and media proxies. Session border controllers are a good match for this functionality as we will see in this section but must be architected to allow physical separation of media and signalling, thus complying with standards requirements and allowing maximum flexibility of deployment with independent scaling of signalling and media.

It will also have become clear to the reader of the previous section that functions within converged networks and IMS definitions currently have considerable overlap. It is therefore important to consider the functional requirements at any particular point in the network rather than generate products to meet a functional block.

The Newport Networks 1460 has been designed to be carrier scale and capable of delivering signalling and media functions in physically separate devices. As such, the Newport Networks 1460 is well placed to perform the following functions.

SignallingProxy: Visited Network

In this position, the SignallingProxy provides the first point of contact for signalling from the User Element and can locate the Home Network via DNS. Services destined for the visited network can also be directed at this point. Where required, Lawful Intercept of signalling and Instant Messaging can be provided, and Emergency Call Handling can be done in the local network, nearest to the emergency. At the interconnection towards the home network,
the 1460 SignallingProxy can resolve issues with overlapping IP address spaces between the networks and also provide topology hiding. The signalling can be policed to prevent DoS attacks at the IP, UDP/TCP and SIP signalling level. A media device can be controlled to ensure that QoS negotiated at the signalling layer is not exceeded at the media layer. In contrast to the GGSN, this feature is provided on a per-media flow level. Billing records can be provided to record user SIP session activity in the visited network.

In summary, the Newport Networks 1460 SignallingProxy provides the P-CSCF, PDF, IBCF and THIG functions. These functions may reside in the same system or may be distributed as scaling demands.

**SignallingProxy: Home Network**

Within the home network, the SignallingProxy again provides the network boundary function. It provides the first point of contact from visited networks and all functionality described in the visited networks section above. For example, traffic management, topology hiding and signalling policing are still likely to be key requirements. In addition, the I-CSCF provides a Diameter interface to retrieve the S-CSCF that should serve the user. Conversion between IPv4 and IPv6 could occur in either visited or home network, or tunnelling could be used through the visited network.

In standards terms, the SignallingProxy provides the P-CSCF, IBCF, and THIG functions and is well placed to provide the I-CSCF functions in the future. These functions may reside in the same system or may be distributed as scaling demands.

**MediaProxy**

Mobile standards for IMS currently address signalling only, which leaves the packet network to deal with media. Consequently, the GGSN must police traffic within these networks. The disadvantages of this have already been covered. The GGSN is not available in access networks, other than GPRS, and therefore it makes sense to control the policing of media directly from the SignallingProxy. This means that sessions can be policed on a per-flow basis. This prevents the user from performing different actions in the media layer to that negotiated in the signalling layer. The MediaProxy can also provide NAPT and firewall functions for media crossing IP boundaries. This architecture is extremely robust in preventing unauthorized access at the media layer, as all ports on the MediaProxy are opened and closed under the control of the SignallingProxy.

This function equates to the Core Border Gateway Function (C-BGF) when deployed in the visited network toward the user and to the Interconnect Border Gateway Function (I-BGF) when deployed between networks. Again, these functions can be co-located or distributed as required.
Conclusions

Carrier-class session border controllers, such as the Newport Networks 1460, that can be deployed as a signalling proxy and media proxy can meet and exceed the requirements of next generation IMS-based networks. This gives the carrier the ability to deploy signalling proxies and media proxies today to meet existing network requirements, such as NAT traversal, Lawful Intercept and policing, in the full knowledge that investment in hardware and software will be reusable as their networks migrate towards a converged architecture.

References

TIPSPAN: NGN Release 1: Functional architecture for PSTN/ISDN Emulation
TISPAN: NGN Functional Architecture Release 1
TISPAN: IP Multimedia Subsystem IMS
TISPAN: NGN Functional Architecture; Network Attachment Subsystem Release 1
NGN Functional Architecture; Resource and Admission Control Subsystem (RACS)
The IMS: IP Multimedia Concepts and Services in the Mobile Domain (Mikka Poikselka, Georg Mayer, Hisham Khartabil, Aki Niemi)

Glossary

3GPP 3rd Generation Partnership Project
AUC Authentication Centre
BGCF Breakout Gateway Control Function
CBGF Core Border Gateway Function
CSCF Call Session Control Function
ECH Emergency Call Handling
GGSN Gateway GPRS Support Node
GPRS General Packet Radio System
HLR Home Location Register
HSS Home Subscriber Server
I-BCF Interconnect Border Control Function
IBGF Interconnect Border Gateway Function
I-CSCF Interrogating-Call Session Control Function
IETF Internet Engineering Task Force
IMS IP Multimedia Subsystem
IMSI International Mobile Station Identity
LI Lawful Interception
MG Media Gateway
MGCF Media Gateway Control Function
MTP Message Transfer Part
NAPT Network Address and Port Translation
P-CSCF Proxy-Call Session Control Function
PDF Policy Decision Function
PDP Packet Data Protocol
PSTN Public Switched Telephone Network
QoS Quality of Service
SCTP Stream Control Transmission Protocol
S-CSCF Serving-Call Session Control Function
SIP Session Initiation Protocol
THIG Topology Hiding Inter-network Gateway
TISPAN Telecoms & Internet converged Services & Protocols for Advanced Networks
UE User Element
UMTS Universal Mobile Telecommunications Service
UTRAN UMTS Terrestrial Radio Access Network
WiMAX Worldwide Interoperability for Microwave Access
WLAN Wireless Local Area Network