Dialogic

White Paper

Beyond the Session Border Controller: Accelerating the Move to IP with Multimedia Border Elements

Executive Summary

For several years, service providers have been migrating from circuit-switched networks to more flexible network topologies based on IP. To increase flexibility and reduce costs, service providers initially kept existing circuit switches in place and used media gateways to convert to IP. However, service providers are now taking the next step and building services with all IP-based elements, typically using the SIP protocol. These emerging SIP-based networks offer enormous potential for generating new services and increasing revenue per subscriber, but the introduction of IP throughout the network also creates challenges.

Although service providers often use Session Border Controllers for signal translation and security, most do not include the hardware-based signal processing needed for media transcoding. For all-IP environments, new elements are required that can mediate signaling, transcode among different media formats, and handle basic security issues. Dialogic has developed the concept of the Multimedia Border Element (MMBE) to meet these needs, and its carrier-proven products, such as the Dialogic® BorderNet™ 2020 Session Border Controller, are exceptionally well-suited to serve as MMBEs.

Table of Contents

Introduction

Once service providers understand the significant cost advantages of IP, they are eager to adopt IP technology. The Session Initiation Protocol (SIP) is widely deployed in networks where gateways connect existing circuit-switched equipment and an IP network, but using SIP in an all-IP network is a more recent development — and more problematic.

Gateways handle a variety of issues for service providers, such as translating signaling protocols (e.g. ISDN and SS7 into SIP), converting circuit-based media to IP, and protecting the internal IP network from attack. Gateways also offer a de facto form of security since they normally connect to the Public Switched Telephone Network (PSTN), which is far more complicated to "hack" into than the internet. In addition, gateways provide a clear demarcation point between internal and external networks, allowing session monitoring and billing applications to be straightforward. However, when the edge of a network simply marks a connection to another IP network, service providers must use new techniques for functions such as signal translation, media transcoding, and basic security.

Platforms with session border controller functionality are well suited for IP-to-IP interworking applications, especially those with multimedia transcoding capabilities. For applications requiring IP-to-TDM interworking, service providers could deploy a combination of platforms to get the functionality they need. Alternatively, a border element that combines gateway functionality and multimedia transcoding with session border controller features, would rationalize the network border in a simpler fashion. A Multimedia Border Element (MMBE) combines gateway functionality, multimedia handling and session border controller features to provide connectivity, security, service assurance and border management. In many cases, a MMBE proves to be a more comprehensive, flexible and cost effective solution than a traditional gateway.

SIP: One Standard or Multiple Dialects?

The SIP protocol has been a major success in the telecom community, and most of the equipment and software used for voice and other multimedia communications has a SIP interface. But which SIP? The core SIP specification is RFC 3261 from the Internet Engineering Task Force (IETF), which replaced the earlier RFC 2543 version. Beyond that, there are at least 20 SIP RFCs that are commonly implemented and found in products offered by a host of vendors. Originally, SIP ran over the UDP protocol only. Now, it can also run over the TCP protocol, over Stream Control Transmission Protocol (SCTP) or in a secured version over Transport Layer Security (TLS). In addition, different user communities can specify different profiles of SIP, such as the SIP Connect profile used for SIP trunking or the profile indicated by Microsoft for integrating with its Lync unified communications. The Third Generation Partnership Project (3GPP) has its own standards that call out specific SIP specifications.

If you are an operator who has two devices that speak SIP but do not talk to each other, you can do either of the following:

- Make changes to the two implementations until they are compatible, a process that may take months or even years.
- Insert a third device that can mediate between the two flavors of SIP, a process called SIP Mediation. An MMBE is useful for SIP Mediation, because both the SIP signaling messages and the related media typically flow through the device.

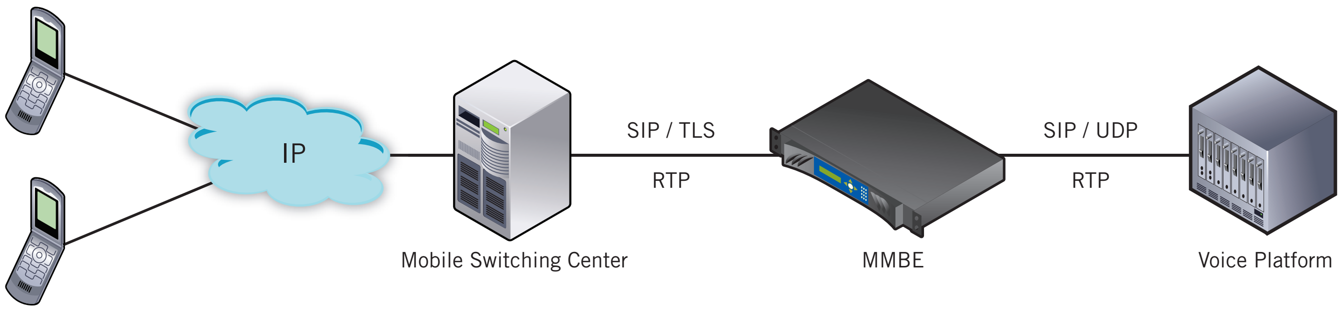

Figure 1. Using an MMBE for SIP Mediation

In this example, the MMBE performs SIP mediation between the different SIP header elements used in a Voice Platform and a Mobile Switching Center. The process of SIP Mediation is suitable for situations in which communication must be established among equipment from a variety of vendors that use different variations of SIP headers to convey message attributes. The MMBE can manipulate the headers generated by one vendor's endpoint to comply with the header structure understood by another vendor's endpoint.

SIP Mediation may also be required when two endpoints need to communicate but use different underlying transport protocols. In this case, the MMBE may perform transport layer conversion between different protocols such as UDP, TCP, and TLS. As service providers migrate their network layer infrastructure to IPV6 from IPV4, the MMBE's location at the network border makes it well suited to mediate between networks if both domains have not completely migrated to IPV6.

Media Translation

One of the most powerful aspects of voice communications via telephone networks has been its universality. With traditional PSTN-based telephony, any phone in the world could talk to any other phone over the PSTN, since voice was converted as needed to traverse a path from one user to another. When mobile phones became popular, new voice coding methods were introduced; however, interworking functions within the Public Land Mobile Network (PLMN) ensured that mobile and fixed line subscribers could still talk to each other.

As the phone network has become a hybrid between circuit switched technology and IP technology, media translation (transcoding) requirements have grown. To reduce bandwidth, most IP network voice traffic is compressed for its journey over long haul networks. Media gateways then translate the compressed voice back into its original form in order to reach the subscriber's handset. Similarly, fax is a standard way of sending documents over the PSTN, made possible by the universal adoption of the Group 3 fax protocol, and several approaches have been developed to enable fax transport over IP networks. In addition, many enhanced services, such as voicemail, depend upon clear and accurate transport of tones that result from the user pressing a keypad.

Adding an IP network into the mix makes the process of clear and accurate transport more complicated; since there are several different standards for compressing voice, fax, and tones. Just as SIP mediation is important for ensuring that two SIP devices can communicate correctly, transcoding is important to support on the network edge because it helps ensure successful end-to-end communication and supports related enhanced services such as voice mail and fax.

A recent development that is gaining in importance among service providers and consumers is high-definition (HD) voice. HD voice utilizes voice codecs that can support a voice experience that often exceeds the quality available on a fixed line network and far exceeds typical cellular voice quality. In order to take maximum advantage of the benefits of HD voice, service providers are using multiple strategies that include various forms of transcoder-free operation (enabling the use of the same voice coding from end-to-end on a call) and transcoding among different HD voice codecs. Customer demand and competitive forces are driving service providers to add HD voice to their mix of services. This will likely increase the need for additional transcoder-free signaling options as well as transcoding among HD voice codecs and the currently deployed narrowband voice codecs.

Standards for video transmission over IP networks are still at an early stage of deployment, but the principles described above for other types of media are likely to apply. A typical early stage requirement involves using a clear channel technique to detect the presence of a video stream in a circuit-based call via signaling, and then to package the media for transmission over IP. This technique preserves the video content so that it can be backhauled over IP for processing within another SIP device on the network. In addition, IP video utilizes several different standard encodings, so that service providers will want to be able to transform video between different encodings and resolutions for applications such as video voice mail and video telephony.

Media translation is an important function at the network border. An MMBE that has built-in media translation capabilities to handle voice, fax, and tones can address these requirements in a cost-effective manner. Going forward, similar capabilities for HD voice and video translation are likely to grow in importance as the market for applications such as HD voice and mobile video evolves.

Converting Other Signaling Protocols to SIP

SIP is the primary protocol used to support multimedia services in the new all-IP core; but there are often other protocols that come into play. Much of the existing circuit-switched infrastructure is based on protocols such as SS7, ISDN, or CAS. Media gateways convert these protocols to SIP, but sometimes other conversions take place as well. H.323 was the initial protocol used for Voice over IP, so there is often a need to convert between H.323 and SIP signaling.

Mobile networks are moving to IP, but at a much slower pace than circuit-switched networks. These mobile networks include a variety of important and popular services based on SS7; including functions like caller ID, roaming, message waiting, and local number portability. As a result, elements in the mobile core network, such as Mobile Switching Centers (MSCs), are implementing a version of SIP called SIP-I that can take the content of SS7 messages and include that content as an attachment to the SIP message. When operators want to communicate between an MSC and other SIP solutions, such as a voice mail system or call center, they must find a way to translate between SIP and SIP-I.

SIP-I encapsulates the SS7 ISDN User Part (ISUP), so it is important that the entity providing the translation between SIP-I and SIP supports the major ISUP standards developed by the International Telecommunications Union (ITU), European Technical Standards Institute (ETSI), and American National Standards Institute (ANSI). SIP-I specifications are designed by the ITU. The IETF has also developed a standard for ISUP encapsulation, which is referred to as SIP-T. Both SIP-I and SIP-T carry ISUP content as an attachment and are largely compatible. Translation between SIP and SIP-I/SIP-T is important to enable communication between VoIP and wireless networks that use these protocols.

Another way to convert the SS7 ISUP protocol to IP is to use one of the SIGTRAN adaption layers standardized by the IETF. Many would argue that a direct conversion from ISUP to SIP within a media gateway provides the best results when mapping between these different networks, but some operators prefer to distribute the signaling functions into a network entity separate from the media gateway. For the latter cases, there is a need to eventually convert the ISUP over SIGTRAN signaling into SIP, another important IP-to-IP network function.

Though SIP Mediation is an important function, operators often need to translate between SIP and other IP protocols such as H.323 and SS7 ISUP over SIGTRAN. Since there may also be a PSTN-to-IP protocol conversion required at the network edge, the integrated media gateway functionality of a MMBE offers a robust and flexible approach within a single network element.

Security Basics

When service providers move to having an all-IP network, they must consider security factors in the design of their network. Security is not a “one size fits all” proposition. Service providers need to understand potential threats and then design security strategies and mechanisms to address these threats. The following security considerations might apply to service providers moving to an all IP network:

- Protecting the network
- Crossing the NAT barrier
- Overload and denial-of-service (DoS) protection
- Privacy across the Internet

Protecting the Network

Many service providers have all of their IP operations running over their own closed network, in which case, it is likely they use firewalls to keep unauthorized parties from gaining access to the network. In addition, they may have IP peering arrangements with other service providers, typically through a structured approach, such as a multi-party peering fabric or bi-lateral agreements with other service providers. Peering arrangements are typically implemented on a private network instead of over the open Internet, so peering involves communication only between the two peer service providers.

Often, the peer service providers communicate with each other without using firewalls or Network Address Translation (NAT) devices, but they may want to hide their IP topologies from each other. In this case, it is useful to have a device on the network border that can act as a back-to-back user agent. The service provider will only see the IP address topology of the device and will not see the IP addresses of the other service provider's network. This function is called *topology hiding* and is frequently used as a lightweight way of protecting the service provider's infrastructure. If the MMBE uses a back-to-back user agent, topology hiding can be provided along with the border element's other features.

Crossing the NAT Barrier

NAT is often found at a network edge between a private IP network and the public Internet. NAT functions are often incorporated as part of a firewall device if service providers need to do either or both of the following:

- Cross the public Internet to connect to special capabilities, such as feature servers
- Extend SIP trunks out to an enterprise

In these situations, the NAT translates between the private IP addresses in the internal network topology and the public addresses on the Internet.

For SIP-based communications, crossing the NAT border requires adjusting IP addresses and possibly media port numbers. There are several different methods of achieving NAT traversal for media streams, and it is important that an MMBE support at least one of them in instances where NAT traversal is needed.

Overload and Denial-of-Service Protection

When a SIP device is located outside the firewall, it can be exposed to a variety of attacks. It is important that the SIP device is either able to deal directly with these attacks or that it is protected by a separate border element appliance. Denial-of-service (DoS) is a typical type of attack, which often involves overloading a network entity with a particular type of traffic, such as sending repeated TCP packets. A smart SIP device such as an MMBE discards IP packet traffic that does not pertain to the types of expected sessions. In this manner, an MMBE can help prevent congestion by not accepting and processing SIP traffic that exceeds a specified limit, thus helping to protect a service provider against overload and DoS attacks.

Privacy Across the Internet

There is a lot of discussion about the need to have privacy when sending sessions or media across the Internet for applications like SIP trunking, but the vast majority of SIP and related media traffic is not secured. However, extensions have been made to the SIP protocol to enable users to operate SIP in a secure manner. For example, running SIP over Transport Layer Security (TLS) provides authentication between the two end points and can be used to encrypt the SIP signaling itself after a public key exchange. Therefore, a standard way of securing SIP is to create an end-to-end TLS session when running SIP over the Internet.

TLS is typically not required over a private network, so running a SIP session over UDP or TCP might suffice for private networks. Ensuring the privacy of media transmitted over the Internet also typically involves an encryption step, although this type of security is still not in common use and is computationally intensive. A standard approach for securing media is the Secure Real Time Protocol (SRTP).

MMBE Examples

This section describes two scenarios where MMBEs can play a useful role:

- MMBEs between network elements
- MMBEs on the network edge

MMBEs between Network Elements

MMBEs are useful where there is a need to translate between the SIP variations used by different vendors in order to produce an enhanced service such as unified messaging. In the scenario shown in Figure 2, a SIP-based Softswitch supporting SIP over UDP needs to communicate with a hosted voice platform that uses SIP over TCP. The MMBE provides SIP mediation between the two platforms and media transcoding between the platforms for tones or voice.

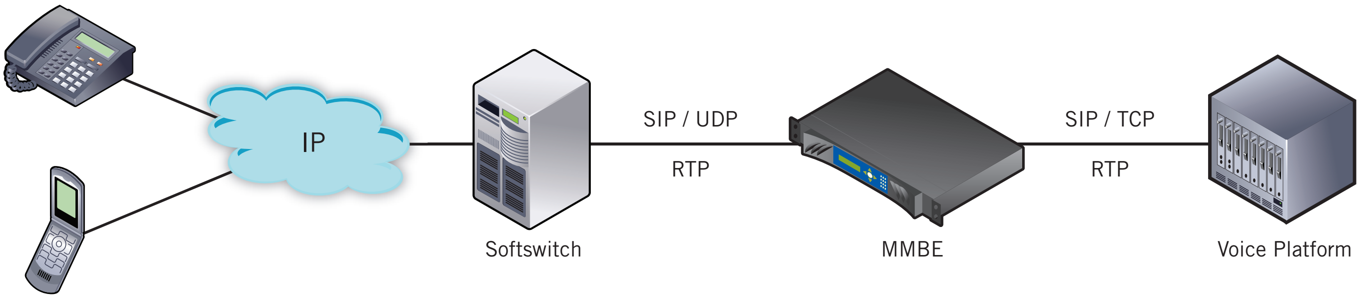

Figure 2. Using an MMBE between Network Elements

In this example, the MMBE plays a role much like a PSTN-to-IP media gateway, but the connections on both sides are IP-based. The MMBE provides value by reconciling the signaling and the media between the softswitch and the voice platform, and by performing these functions using a single device.

MMBEs on the Network Edge

Another role for the MMBE is to provide an intelligent link at the network edge between two different IP networks. Service providers have often used SBCs in this role, but in cases where there are requirements for media transcoding between the networks, an MMBE can offer a more comprehensive approach.

Figure 3 shows an example of using an MMBE on the network edge. In this example:

- A service provider must handle telephony traffic that is sent from a softswitch to the network edge, and then sent across a network boundary. The traffic needs to cross the network boundary in order to connect to a feature server controlled by a service provider who offers hosted services on the Internet.
- The service provider needs to use SIP to connect to the feature server, but also wants extra protection for the signaling, so it issues a request for SIP over TLS to the feature server.
- The service provider wants to conserve bandwidth, so it requests that the media be converted from uncompressed G.711 voice into compressed G.729.
- The service provider wants to mask its IP topology when communicating with another service provider, so it uses the back-to-back user agent of the MMBE to shield the internal IP addresses of the carrier from the service provider.

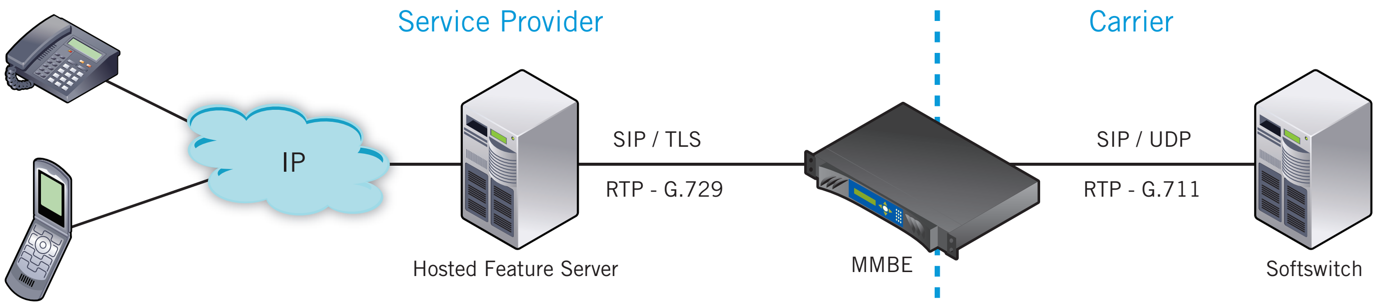

Figure 3. Using an MMBE on the Network Edge

In this example, the MMBE provides value to the carrier by securing the signaling for passage across the Internet, transcoding the voice media per the requirements of the service provider, and masking the carrier's IP topology.

Scenarios and Suitable Devices

The recent move to all-IP network deployments has complicated the choices at the edge of the network. Depending on the network scenario, service providers can choose among traditional gateways, SBCs or an MMBE that combines SBC and gateway functionality to meet their needs at the network edge. Table 1 summarizes some suitable device options:

Network Scenario	Suitable Device
Network edge involving a transition between the circuit-based PSTN and an IP network	Media gateway, which typically offers signaling and media translation between the circuit-based PSTN and IP networks
Network edge involving a transition between two IP networks and with a need for media transcoding	SBC which can support both signaling mediation and media transcoding with a single device
Network edge with a requirement for highly scalable IP-to-IP session management and with little or no need for media transcoding	SBC, which has a focus on IP-IP session management and related security aspects, with minimal manipulation of associated media
Network edge with a need for highly sophisticated session management, TDM to IP and IP-to-IP interworking and scalable media transcoding	An MMBE offers a flexible approach to meet service provider needs in this situation where gateway, media handling and SBC functionality is necessary

Table 1. Network Edge Device Choices

The Dialogic® Solution

Dialogic offers powerful, versatile session border element that provides the features of an MMBE in the BorderNet 2020 SBC. The BorderNet SBC integrates media and signaling gateway functionality and session border controller functionality along with voice and video transcoding in an efficient one rack unit (1 RU) appliance. The BorderNet 2020 SBC has the following functionality that makes it well suited to those situations that require an MMBE:

- Any-to-any signaling
- Any-to-any media for voice, fax, and tones
- IP address topology hiding
- SIP mediation (includes SIP, SIP-I, SIP-T)
- SIP lower layer protocol conversion (among UDP, TCP and TLS)
- SIP overload protection
- Secure SIP signaling and authentication (via TLS)

For help in choosing the right BorderNet solution for your needs, contact your local Dialogic sales representative.

Acronyms

3GPP	Third Generation Partnership Project
IETF	Internet Engineering Task Force
ETSI	European Technical Standards Institute
ISDN	Integrated Service Digital Network
ISUP	ISDN User Part
ITU	International Telecommunications Union
MMBE	Multimedia Border Element
MSC	Mobile Switching Center
NAT	Network Address Translation
OCS	Microsoft® Office Communication Server
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
SBC	Session Border Controller
SIP	Session Initiation Protocol
SIP-I	Session Initiation Protocol Interconnect
SIP-T	Session Initiation Protocol for Telephones
SRTP	Secure Real Time Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

For More Information

Dialogic® BorderNet™ 2020 Session Border Controller
http://www.dialogic.com/Products/session-border-controllers/bordernet-2020.aspx

Dialogic® IMG 1010 Integrated Media Gateway
http://www.dialogic.com/products/gateways/img_gateways/IMG1010.htm

Dialogic® IMG 1004 Integrated Media Gateway
http://www.dialogic.com/products/gateways/img_gateways/IMG1004.htm

IETF RFC 3261, "SIP: Session Initiation Protocol," June 2002 at
http://www.ietf.org/rfc/rfc3261.txt?number=3261

SIP Forum, "SIP PBX/Service Provider Interoperability: SIPconnect 1.1 Technical Recommendation" at
http://www.sipforum.org/component/option,com_docman/task,cat_view/gid,43/Itemid,75/

www.dialogic.com

Dialogic Inc
1504 McCarthy Boulevard
Milpitas, California 95035-7405
USA

05/12 11533-03