ribbon

Secure Real-Time Communications

Diameter Edge

Controlling the Diameter Edge Ensures 4G LTE Network Viability

Contents

Introduction

Long-Term Evolution (LTE) is the fastest developing mobile system technology ever according to GSMA1. The network's growth—fueled by subscribers' desire to have broadband connectivity anywhere, at any time, from any device and to any data source—is driving a significant rise in LTE subscriptions. Due to the mobile nature of subscribers, LTE networks cannot be deployed as islands; they must either be interconnected bilaterally or through Internetwork Packet Exchange (IPX)/hub providers, and these interconnections have internetwork technology and roaming agreement ramifications. This white paper discusses the challenges and opportunities that service providers encounter at the edge of LTE/Evolved Packet Core (EPC)/Diameter networks where interconnection between networks takes place.

Business Challenges / Drivers

With the number of LTE and VoLTE subscribers growing rapidly, and the number of VoLTE subscribers expected to reach 5.5bn by 2023, it is no wonder that service providers expect to make significant investments in LTE networks as well as seeing significant revenue opportunities. In order for mobile service providers to realize their share of the rapidly increasing 4G LTE/EPC/Diameter–based mobile revenue, the following technical and architectural challenges need to be addressed:

- Internetwork security
  - Diameter transport security
  - Topology hiding
  - Network admission control
- Protocol interworking
  - Diameter to Diameter
  - Diameter to SS7 and vice versa
- Segmentation of routing between interconnected networks

Addressing these issues will help operators optimize roaming revenues by providing subscribers with the best quality of service (QoS), thus reducing subscriber churn due to bad roaming experiences.

Internetwork Security

Network security is one of the most important issues to be addressed moving forward. Many of the challenges facing the internet today are applicable to the LTE/EPC/Diameter networks.

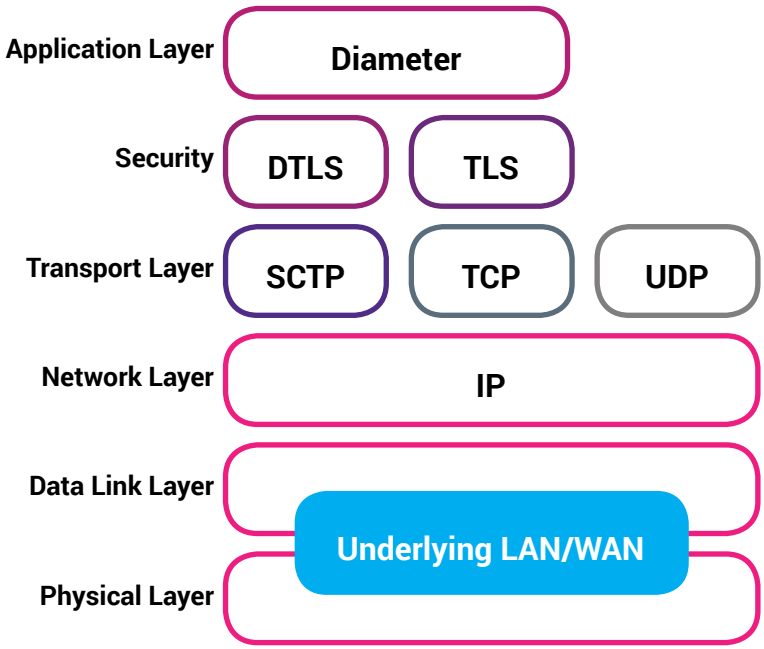
Discussion of internetwork security should include:

- Diameter transport security to help guarantee the integrity of transmitted and received Diameter messages
- Topology hiding to stop the exportation of network configuration information
- Admission control to apply access control at the Diameter application level

(1) Source: www.gsma.com

Transport Security

To address the transport security needs of the Diameter protocol, the IETF Diameter Specification (RFC 6733) states, "The Diameter protocol MUST NOT be used without one of TLS, DTLS, or IPsec." These security protocols ae Transport Layer Security (TLS) when using TCP, and Datagram Transport Layer Security (DTLS) when using Stream Control Transmission Protocol (SCTP). Optionally, IP Security (IPSec) can also be used. This discussion is not meant to be an exhaustive commentary on transport protocols and security, but rather an overview providing a basis for understanding the Diameter concepts that utilize these transport and security capabilities, both inter and intra network. (See the figure right for the relationship between protocol layers.)



Transport Layer Security (TLS)

TLS is the protocol used to provide private, reliable and secure communications over TCP. It ensures that sensitive data is safe from malicious attacks. The TLS protocol provides capabilities to perform client authentication, server authentication, data encryption and data integrity. RFC 5246 is the current TLS specification defining TLS version 1.2.

Datagram Transport Layer Security (DTLS)

Some may wonder "Why not use TLS as a security protocol for SCTP, especially when both TCP and SCTP are both connection-oriented protocols and TLS is used for TCP?" The reason is that there are serious limitations of TLS related to SCTP, including:

- TLS does not support unordered delivery of SCTP user messages
- TLS would only support the same number of data streams in both directions
- TLS would have a connection for every bidirectional stream; this would cause a large resource impact when a large quantity of SCTP is used.

DTLS over SCTP overcomes the issues by:

- Preserving SCTP message boundaries
- Supporting a large quantity of either unidirectional or bidirectional streams
- Allowing ordered and unordered delivery of SCTP messages.

For the reasons listed above, DTLS was selected by the IETF as the security protocol to be used for the Diameter protocol when SCTP is used as a transport protocol.

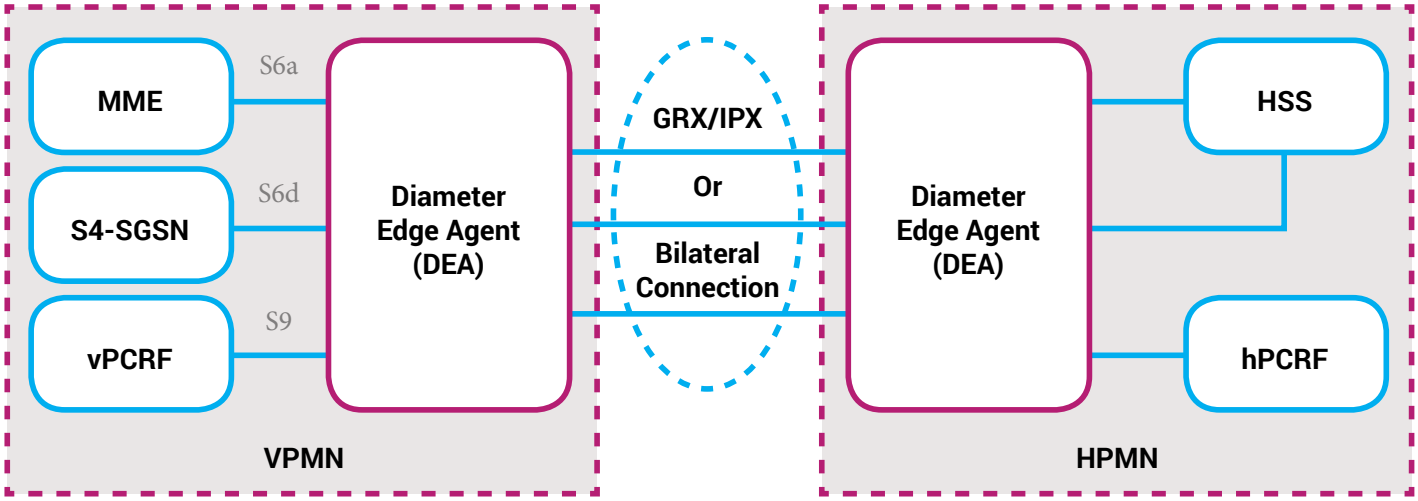
IP Security (IPSec)

The original Diameter Base Protocol specification (RFC 3588) stated, "In order to provide universal support for transmission-level security, and enable both intra and inter domain AAA deployments, IPsec support is mandatory in Diameter, and TLS support is optional." However, the subsequent release of the new Diameter Base Protocol specification (RFC 6733) states, "The use of a secured transport for exchanging Diameter messages remains mandatory. TLS/TCP and DTLS/SCTP have become the primary methods of securing Diameter with IPsec as a secondary alternative."

Reliable, secure transmission capabilities are of the utmost importance to the Diameter Base Protocol and the applications built on it. Great efforts have been made to ensure that the selected transport and security protocols address these needs. Both TCP/TLS and SCTP/DTLS can provide these solutions; however, great care must be exercised in selecting the proper protocol and security mechanisms based on specific network requirements, especially at the edges of the network.

Network Security – Topology Hiding

Since the beginning releases of the GSMA PRD IR.88, there have been recommendations for all network-to-network interconnections to be via a Diameter Edge Agent (DEA) to provide efficient connection methodologies and network security in the form of topology hiding. In the earlier releases of IR.88 (release 9 and earlier), DEA recommendations mentioned the implementation of DEAs "to provide topology hiding." However, there was no mention of how topology hiding was to be implemented—this was the crux of the problem. Topology hiding recommendations were not provided until the release of GSMA PRD IR.88, Version 10.0, 10 July 2013. With release IR.88 version 10.0, there were concrete recommendations for how the GSMA thought topology hiding should be implemented.



GSMA Topology Hiding Guide Lines IR.88 V10.0

GSMA recommendations for topology are contained in GSMA IR.88 V10.0, Section 6.5.1.3. These recommendations are segmented into the responsibilities of either the service provider, the Global Roaming Exchange (GRX), IP Packet Exchange (IPX), or a combination. These recommendations can be divided into the following categories:

- To ensure the network being communicated with is acceptable, i.e., there is an existing roaming agreement
- To ensure that Diameter messages are received in order, i.e., no answer can be received if no request has been issued
- No messages transmitted carry the true identification of nodes within the network—rather they use generic names

- To ensure numbers of Home Subscriber Servers (HSSs) or Mobile Management Entities (MMEs) are not exposed to a foreign network by not transmitting the true identification of MMEs or HSSs
- Only static entries of peers to be used between networks
- Service provider networks must ensure that messages received are destined for their network, i.e., no message received from an external network can be routed to another external network. Only GRX/IPX providers can perform this function.

Adherence to these rules and recommendations will help to secure and maintain LTE/EPC Diameter signaling networks at the application level.

Network Security – Diameter Screening
In addition to providing topology hiding recommendations, GSMA IR.88 V10.0 Section 6.5.1.3 also lists recommendations for admission control. IR.88 states that either the GRX or service provider is required to "Filter Diameter messages to accept only supported Application IDs, Command Codes and AVPs. Custom AVPs are not allowed by default. If custom AVPs are needed, they need to be bilaterally agreed to." The admission control provides a firewall between networks at the Diameter application level.

Interworking

Diameter to Diameter Interworking
As more and more network operators sign and implement LTE roaming agreements, the dialogue about network interconnections is becoming increasingly important. When reading the Diameter specifications or other related Diameter information, you typically see Diameter interworking defined in terms such as:

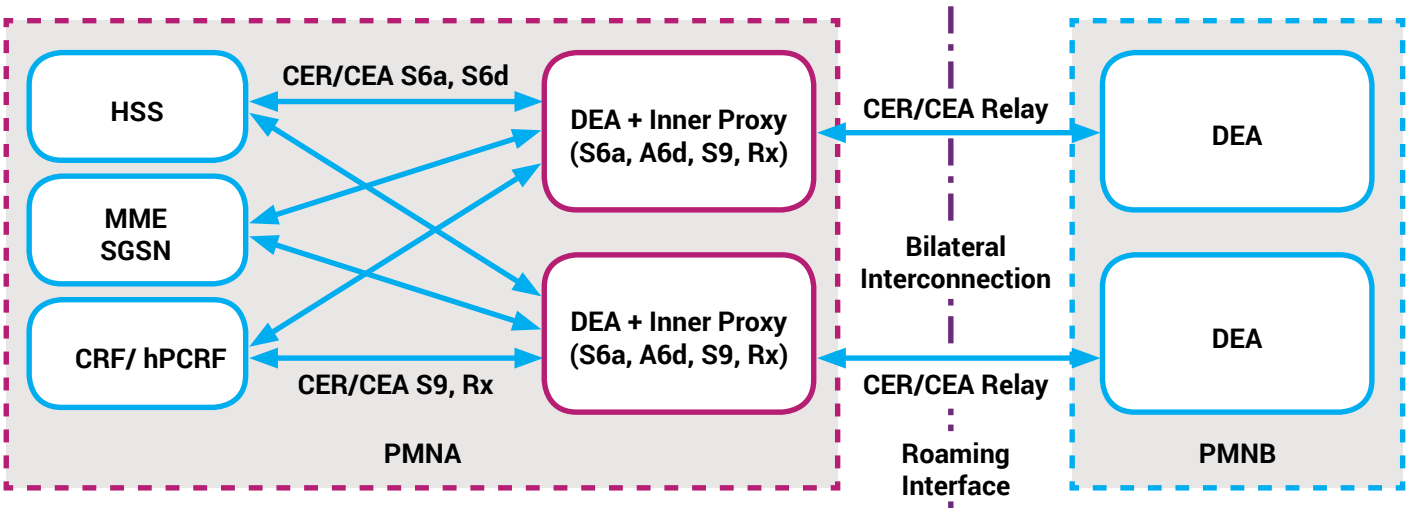
1. Diameter to RADIUS interworking
2. Diameter to SS7 MAP interworking

Both of these are important; however, these two topics are only a piece of the Diameter interworking puzzle. Any discussion around Diameter interworking at the edge of the network should also include **Diameter to Diameter interworking.**

In today's environment there are many different specifications for the Diameter protocol, including both Internet Engineering Task Force (IETF) and 3rd Generation Partnership Project (3GPP). The 3GPP has different release levels. With these varying specifications and releases, vendors may interpret the Diameter specifications differently, yielding Diameter implementations that are incompatible with each other. This problem is exacerbated at the network edge, where multiple networks converge. Service providers have little knowledge of the equipment and its software version in the foreign interconnected network.

Given these issues, a Diameter Routing Device, also called a Diameter Edge Agent (DEA), placed at the network edge is the perfect place for the protocol mitigation to take place.

Some might say that this has already been addressed by the GSMA in IR.88 with definition of the Diameter Edge Agent (DEA). However, as stated in IR.88, interconnected networks should view the DEA as a Diameter Relay Agent. When the device is defined as a relay agent, the device does not have the authority to modify any portion of the Diameter message outside of routing information; this is the responsibility of a Diameter Proxy Agent.



To keep the terminology and implementations consistent, the answer might be to route the conflicting messages off to a Diameter Proxy Agent (maybe in the same physical device) that advertises support for the application in question for AVP/message manipulation. After the protocol inconsistencies' mitigations take place, the message would be routed as originally required. Subsequent answer messages would have to be routed back to this proxy agent for translations back to the original format prior to being sent to the interconnected network. Even if the interconnected devices in both networks are from the same vendor, there is no guarantee that they are of the same revision or same software version and therefore the protocol differences can still occur.

Diameter to SS7 Interworking

As previously stated in the Business Challenges / Drivers section of this paper, while the number of LTE & VoLTE subscribers continues to grow at a high rate, the remaining mobile connections will still be 2G, 2.5G, or 3G (all SS7 based) for a number of years to come.

Given these facts, it is important to allow customers' LTE/EPC/Diameter subscribers and 2G, 2.5G and 3G SS7–based subscribers to roam into networks regardless of the core technologies. This enhanced quality of experience (QoE) for subscribers can be accomplished by providing a Diameter/SS7-Map interworking function, typically located in the LTE/EPC/Diameter network.

The Diameter to MAP interworking capability is specified by 3GPP TS 29.305 v12.1.0 (2013-12). TS 29.305 describes four scenarios for interworking:

- S6a/S6d – Pre Rel8 Gr interworking scenario with one IWF
- S6a/S6d – Rel8 Gr interworking scenario with one IWF
- S6a/S6d – S6a/S6d interworking scenario with two IWFs
- S13/S13 – Gf interworking scenario with one IWF

In today's evolving network, it is important to understand both the legacy SS7 network and the LTE/EPC/Diameter network and the interactions between these two networks. This understanding will allow the most effective network designs to meet the needs of mobile subscribers.

Diameter Routing Segmentation

Intranetwork connections—whether bilateral or through an IPX/GRX provider—pose a unique set of problems to mobile service providers. The combination of a complex LTE/EPC network, numerous interconnected networks, and the vendors' wide diversity of equipment and software releases presents service providers and hub providers with the challenge of setting up routing rules, shaping traffic, and handling Diameter protocol inconsistencies on an interconnected network basis. The deployment of separate Diameter routing entities is possible; however, this type of deployment significantly increases both the operations and capital costs.

Another solution is to consolidate routing rules for both intranetwork and internetwork traffic. This massive routing configuration leads to complexity and increases the chances of errors when making routing/traffic rules changes. A DEA providing routing segmentation (routing segmented on a per-interconnected network basis) can provide an efficient routing mechanism. This capability allows multiple virtual DEAs to be configured within a single network entity. Each of these virtual DEAs has its own separate routing and screening rules that include the ability to shape traffic on a per-peer basis. This shaping includes traffic flow control, throttling and congestion on a per-peer basis. This flexible routing concept provides increased control as well as ease of implementation, and helps open the door to increased service provider revenues.

Summary of Business Drivers

Today's network operators can be characterized by their desire to:

- Build a flat IP-based network architecture
- Have a high level of network security
- Have a flexible, robust QoS framework
- Lower capital expenditures (CapEx) long-term
- Lower operational expenditures (OpEx) near-term
- Provide subscribers with enhanced QoE

This, coupled with the mobile nature of subscribers and the uptick in LTE subscriptions, has increased the need to focus on the critical issues and concerns at the edges of the LTE/EPC/Diameter networks. Addressing these requirements now will help network operators:

- Design the most efficient networks
- Increase revenues
- Reduce costs
- Reduce risks

What to Look for in a DEA Solution

Extensive Diameter Security Mechanisms

Internet Protocol (IP) methodologies used in LTE/EPC/Diameter networks are increasing the importance of adhering to the latest specifications for network security. Additional capabilities such as the ability to screen (block or allow) on Diameter messages, AVPs and applications enables the building of efficient firewalls at the entry points of the network. The specification adherence and efficient firewalls are essential tools for network security.

Consistent Routing Engine

An important architectural issue to be considered in the selection of a Diameter Signaling Controller with Diameter Edge Agent capabilities is whether or not the internal software design is based on universal protocol switching and routing concepts. The use of a consistent routing engine across legacy and next-generation protocols such as Diameter and SS7 enables efficient network migration and proven routing concepts.

Routing Segmentation

The DEA should include the ability to segment the routing rules on a per interconnected network basis. This segmentation would provide the ability to administer routing rules, traffic shaping, Diameter to interworking, and Diameter to SS7 interworking on a roaming partner or interconnected network basis. This capability allows increased control, reduces administrative risks and provides the flexibility required in network design.

SDN and NFV

The DEA should include multiple deployment capabilities, including private cloud to meet network operators' desire to reduce costs and use commercial-off-the-shelf (COTS) servers.

Experience in Telecommunications Signaling SS7 and Diameter

In order to provide solutions that span the evolutionary stages of telecommunications signaling (SS7 to Diameter), it is imperative that the solutions vendor has experience in the concepts of both SS7 and Diameter Signaling. The experience in the legacy SS7 protocol and its associated network provides the STP/DSC vendor with the unique knowledge of issues and concerns that occurred within legacy networks. This knowledge allows the vendor to provide solutions that mitigate these issues in new networks and protocols such as LTE/EPC/Diameter.

Independence – Specializing in Network Signaling & Routing

There will always be differences in the implementation and interpretation of specifications when any network or protocol is deployed. These differences can cause catastrophic problems within networks and across the boundaries between different networks. A network equipment vendor that specializes in protocols and routing can provide mediation capabilities that solve the protocol inconsistencies and thus eliminate network impact.

The Ribbon DSC Advantage

Diameter Security

The Ribbon DSC 8000 adheres to IETF and 3GPP specifications for security, including the implementation of Datagram Transport Layer Security (DTLS), Transport Layer Security (TLS) and optionally IP Security (IPsec). Additionally, the DSC 8000 gives network operators the ability to route or screen on any AVP or message. This screening capability gives network operators unparalleled control of information entering their network, including messages, AVPs and applications.

Distributed Routing Engine

The internal design of the DSC 8000 utilizes Ribbon's advanced Distributed Routing Engine (DRE). The DRE concept provides instances of the DRE on each routing processor and intercommunications between these instances. The DRE's centralized point of provisioning, coupled with its distributed architecture, delivers the reliability and scalability required in today's network design. An additional advantage of the DRE is its registration capabilities, supporting both SS7 and Diameter.

Ribbon DSC 8000 "Virtual Instances"

The DSC 8000 enables the definition of separate DEAs within a single DSC 8000 platform. Each of these virtual DEAs has its own separate routing and screening rules that include the ability to shape traffic on a per-peer basis. This shaping includes traffic flow control, throttling and congestion per-peer. Architected for extensibility and straightforward evolution to future Diameter applications, this high-powered platform makes the DSC 8000 ideal for LTE/EPC and IMS networks.

Ribbon DSC SWe (Software Edition)

The DSC SWe delivers the same advanced features and functionality of Ribbon's hardware-based Diameter Signaling Controller in a virtualized platform, providing greater deployment flexibility for network operators. Software-defined networking (SDN) and NFV play an increasingly critical role in today's next-generation and cloud networks. Building upon its strategy to virtualize the field-proven code base of its industry-leading hardware platforms, Ribbon separated its Diameter software from the DSC 8000 hardware and architected it to operate on industry-standard COTS servers. For customers looking to leverage new and existing platforms to support NFV functionality, the DSC SWe allows customers to deploy a fully featured DSC co-resident with other applications.

A Rich History in Telecom Signaling

Ribbon is uniquely positioned to provide independent signaling and routing solutions to the telecommunications industry. Ribbon's extensive history of delivering Session Initiation Protocol (SIP) solutions enables Ribbon to expand and diversify its portfolio to both SS7 and Diameter products/solutions. This vast experience in all aspects of telecommunications signaling, SS7 to SIP to Diameter, enables Ribbon to deliver solutions over the broad spectrum of telecommunications signaling, resulting in more efficient, scalable, secure and cost-effective networks.

Specializing in Telecommunications Signaling and Routing Solutions

Ribbon's focus on signaling and routing solutions, combined with its expertise in SS7, SIP and Diameter protocols, provides the objectivity required to deliver the most efficient SS7, SIP and Diameter interworking capabilities in the industry. These interworking functions ensure that multivendor networks perform at their peak, and that the need to constantly upgrade network elements due to protocol inconsistencies is removed.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit **rbbn.com**.

Contact Us Contact us to learn more about Ribbon solutions.