The F5 LTE Roaming Reference Architecture

When deploying LTE networks, service providers must deliver a robust messaging infrastructure, implement advanced roaming policies, and adhere to regulations—all while managing costs.
Introduction

Global travel and communications are normal in today’s society, and consumers want to be able to make calls and connect to the Internet with minimal, if any, configuration changes no matter where in the world they are. In addition, an explosion of different devices such as smartphones, laptops, tablets, and embedded computer systems have created a new landscape for data usage and availability. LTE networks are becoming the standard for 4G wireless networks because they deliver the high-speed data access required and help fill consumer demand for faster downloads and ubiquitous Internet availability.

![LTE Roaming Functionality](image)

Core functionality required to deliver consistent roaming services in an LTE network

LTE network architecture represents a major shift in how voice and data services are delivered and managed, from circuit-switched voice communications to a packet-based, IP network infrastructure. To be successful in serving roaming subscribers from these new networks, communications service providers (CSPs) must deploy a dynamic Diameter framework that can effectively manage policies for connectivity and keep costs under control, while making use of advanced capabilities and adhering to the telecommunications regulations now being implemented.

Technology Solutions

CSPs must equip their LTE networks with a dynamic Diameter framework as well as the core functionality that will make voice and data services always available and delivered reliably, securely, and in a scalable fashion.
Core Functions

A rich set of functions is the foundation of an infrastructure for delivering consistent services in an LTE network. When signaling protocol communications enter the LTE network, the various network components must be able to effectively process the messaging information, whether this means applying security policies or routing the session to a specific destination based on the context. Advanced context-based services provide value by expanding the network’s message-handling capabilities.

These core functions can be broken down into broad categories:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Load Balancing</td>
<td>Managing the distribution of sessions through different signaling components such as MMEs and HSSs with context-aware session analysis for unlimited scalability</td>
</tr>
<tr>
<td>Message Steering</td>
<td>Encrypting and decrypting application traffic for security, inspection, and routing session messages to different networks or components based on origin, customer profile, or session details such as application, IMSI, or time of day</td>
</tr>
<tr>
<td>Security</td>
<td>Analyzing content to validate messages and delivering IP-based network security for a clean and secure LTE network infrastructure</td>
</tr>
<tr>
<td>DNS</td>
<td>Using advanced DNS services to enhance cloud services and deliver global availability</td>
</tr>
<tr>
<td>DRA and DEA</td>
<td>Providing support for the Diameter routing agent (DRA) and Diameter edge agent (DEA), along with full 3GPP support, including the inter-working function (IWF)</td>
</tr>
<tr>
<td>Message Normalization</td>
<td>Parsing and manipulating message content to standardize the content across all platforms</td>
</tr>
<tr>
<td>Analytics</td>
<td>Offering advanced and high-performance logging with customized data and reports to enable proper management of the LTE signaling infrastructure</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Delivering session awareness and message content inspection, with content manipulation that enables voice communications management based on custom scenarios such as local breakout</td>
</tr>
</tbody>
</table>

Diameter: Not Just for Geometry Class

Diameter is an enhanced signaling protocol designed to replace RADIUS and has become the standard authentication, authorization, and accounting (AAA) signaling protocol in the 3GPP IP Multimedia Subsystem (IMS) infrastructure in LTE networks. Without Diameter, voice and data services cannot connect, policies cannot be applied, and revenue cannot be realized.
LTE Roaming Architecture

When designing and deploying roaming solutions for LTE networks, a DEA or IP exchange (IPX) is essential to scale the connectivity to multiple roaming partners. The DEA offers an added advantage, since it can provide message normalization and advanced message steering through content analysis and manipulation. These inter-gateway functions need to seamlessly interact with the core LTE components such as the PGW, home subscriber services (HSS), or online charging systems (OCS).

The DEA should act as the intermediary between the core IMS components to determine AAA via Diameter, which in turn delivers roaming services to the remote subscriber. This function is also critical to deliver proper records for billing to generate revenue for the CSP and make the subscriber aware of the costs associated with their roaming services. The network must perform flawlessly to generate a significant proportion of the CSP's revenue. How the services are made available to the roaming subscriber will greatly affect the subscriber’s quality of experience (QoE). If the Diameter infrastructure is compromised or disabled, wireless services become unavailable to all subscribers.

Scalability

Data services rely on Diameter signaling to properly connect and to enable the application of provider and subscriber policies. These tasks can require large numbers of signaling messages to key LTE network elements such as HSS, OCS, and the policy and charging rules function (PCRF). These services must scale to meet network demands in a highly reliable and efficient manner.
Market-leading technology from F5 Networks provides advanced Application Delivery Controllers (ADCs) to make resources available and interact with an orchestration system utilizing software defined networking (SDN) and network functions virtualization (NFV) models.

Advanced DNS technologies enable services to become independent of geographical and physical location. Using DNS to inspect and route messages to the most appropriate service location (based on multiple dynamics) makes it possible to scale beyond the data center and virtualize the core IMS infrastructure in a cloud-like environment.

When connecting to roaming partners, one or more DEAs must be used to manage the signaling from the CSP home network to the roaming partners and IPXs, and vice versa. Clustering technologies and the ability to scale solutions enable CSPs to use their DEAs and IPXs as a point of control for almost infinite scaling of signaling services.

**Availability**

When things break, sessions must still connect and the service must maintain operational status. Redundancy in the data center ensures that when a resource fails, messages are automatically directed to backup facilities. Advanced load balancing technologies within the ADC and Diameter agents ensure that messages are routed to available services.

While the ADC and Diameter agent can provide session synchronization and high-availability technologies, CSPs can also maintain sessions even when there is a failure within the LTE infrastructure—if DNS services can monitor the availability of resources tied to the DNS query and only deliver DNS responses based on service availability.

Beyond the data center, orchestration and NFV also enable the CSP to engineer an architecture that makes all resources available, at all times, on a global scale. Monitors and intelligent routing based on service availability and resource demand ensure that the data and control messages always connect to the intended destinations.

**Flexibility**

With intelligent protocol inspection and the ability to inspect the content within Diameter signaling messages, CSPs can steer content based on subscriber profiles and implement custom policies based on fields within the control messages. For example, any parameter in the Diameter signal—such as origin, destination, connection information, or application—can be identified, and the message can be routed based on that content in conjunction with subscriber and provider policies.
This functionality becomes critical to LTE roaming if the CSP and customer want to manage the roaming partner the customer connects to based on the cost and availability of services through the partner network. Such functionality, which can be defined as intelligent roaming (IR), manages the remote network customers can connect to. Services such as local breakout (LBO)—when the roaming network provider delivers local Internet services instead of tunneling the subscriber traffic all the way back to the home network—can reduce customer costs while maximizing CSP revenue through the use of optimal roaming partners. But they require the roaming network provider to establish a mechanism for sharing usage and billing information with the home network.

Security

Security is very different in an IP-based network than in the past’s circuit-switched voice networks. Critical infrastructure must be protected from malicious attacks as well as inadvertent floods and compromises caused by bad applications or untested network models. The S/Gi portion of the network also must be protected, with the quality of the connection maintained throughout the LTE network infrastructure.

Specifically, all border points that connect to core IMS services must be secure. This means that the infrastructure beyond the GGSN/PGW must be protected from subscribers’ equipment, and core IMS databases such as the HSS, PCRF, and OCS also need protection when communicating via the DEA with roaming partner networks.

Security solutions built into Diameter routing products can normalize traffic spikes and use message inspection to validate the Diameter signaling messages sent and received from external components. IPSec encryption is being mandated by regulatory bodies and can be utilized to protect the communications and ensure privacy. In addition, advanced security gateways can enhance protections by applying full-proxy, stateful security policies from a high-performance platform.

Conclusion

By using the components of the F5® LTE Roaming reference architecture, CSPs can optimize the benefits of the LTE architecture to gain capital and operational efficiencies.

- Improve quality.
- Maintain availability.
- Retain credibility.
- Reduce cost.
- Increase revenue opportunities.
- Expand service coverage.
F5 delivers a complete solution to help CSPs meet all of the new infrastructure requirements and optimize the data capabilities of LTE roaming agreements with key partners. The unified solution ensures quality customer experiences while maximizing mobile revenues.