Why does 5G need a service mesh?

Web-scale providers use service meshes in cloud native deployments to solve critical problems, including scaling, interworking, and fault isolation. For the 5G service-based architecture, service meshes bring a new and fresh approach. Service meshes address the challenge of how to automate, secure, scale, optimize, as well as simplify the communications layer between 5G network functions, also known as services. These services must be deployed across a multi-cloud infrastructure distributed over the core, region, as well as the edge of the network to provide users and applications with the connectivity they need. This paper introduces the concepts, capabilities, and implementations of service meshes along with the underlying network technologies needed to answer the question: Why does 5G need a service mesh?
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Service meshes and 5G signaling</td>
<td>4</td>
</tr>
<tr>
<td>Security</td>
<td>6</td>
</tr>
<tr>
<td>Traffic controls</td>
<td>6</td>
</tr>
<tr>
<td>Observability</td>
<td>7</td>
</tr>
<tr>
<td>Failure handling and injection</td>
<td>7</td>
</tr>
<tr>
<td>Service discovery and exposure</td>
<td>7</td>
</tr>
<tr>
<td>5G core Binding Support Function (BSF)</td>
<td>7</td>
</tr>
<tr>
<td>5G core Security Edge Protection Proxy (SEPP)</td>
<td>8</td>
</tr>
<tr>
<td>Transport network protocols</td>
<td>8</td>
</tr>
<tr>
<td>Quick UDP Internet Connections (QUIC)</td>
<td>9</td>
</tr>
<tr>
<td>Summary</td>
<td>10</td>
</tr>
<tr>
<td>Further reading</td>
<td>11</td>
</tr>
<tr>
<td>References</td>
<td>11</td>
</tr>
<tr>
<td>Acronyms</td>
<td>11</td>
</tr>
</tbody>
</table>
Introduction

The software industry is undergoing rapid growth and experiencing changes on a scale not seen since the birth of the Internet. Today, these changes are usually described with words, such as “cloud computing,” “web scale,” and “software defined networks,” and they are pushing applications to a maturity level typically described as “cloud native.” In the telecom industry, this means, among other things, stateless micro-services with a high degree of modularity, such that applications are composed from easily managed and deployed services across a multitude of infrastructures with flexible and minimal coupling. Indeed, the principles of a micro-services-based architecture are essential in meeting a cloud native maturity level that delivers on the promise of assuring continuous innovation and software deployments in order to maintain a competitive edge.

Figure 1 illustrates the transformation of the telecom industry from a network element (NE)-centric view to a modern cloud native architecture — one in which the VNF(s) are refactored into individual services and the solution is composed of a diverse group of micro-services. The services can be dynamically deployed throughout the network to meet the scale, KPI, and SLA requirements of an end-to-end service. In some respects, the complexity of a distributed service-based architecture is further increased with micro-services. This is due to incompatible interactions and varying degradations, as well as unpredictable failure modes. These challenges are the primary reason why a service mesh is needed. A service mesh delivers a secure, reliable, and resilient communications layer that can handle the delivery of signaling requests through the complex, dynamic, and ever-changing topology of services that comprise a modern, cloud native 5G deployment.

Figure 1. Migration of network elements to cloud native micro-services

Automating, securing, scaling, optimizing, and simplifying the signaling communication for 5G services across a multitude of less reliable infrastructures is a significant challenge. The Nokia Software business group addresses this issue. Not only does Nokia offer a complete, end-to-end, 5G next-generation core, it also brings the experience and expertise acquired through building large-scale, distributed signaling systems to provide service-based and web-scale solutions critical to the success of multi-cloud and multi-vendor 5G networks.

2 The Twelve-Factor App (https://12factor.net/)
Nokia delivers on the digital network’s architectural vision of openness and freedom to encourage single responsibility NFs and network automation. This includes a multitude of NF services from a diverse group of vendors – or the service provider itself. As a result, the service-based architecture, using service compositions, is capable of performing the business logic designed to meet the operator’s unique needs. All of this is done while liberating the micro-services from any concerns about inter-service communication. Consequently, the operator can introduce the functionality needed for its 5G rollout and evolution — even as the standards solidify. Moreover, the operator’s vendor ecosystem can deliver key services without waiting for the features required by other markets or migration scenarios.

Service meshes and 5G signaling

“A service mesh is a dedicated infrastructure layer for making service-to-service communication safe, fast, and reliable. If you're building a cloud native application, you need a service mesh.” Popular open-source examples of service meshes include Istio-Envoy and Linkerd (Conduit).

The primary role of a service mesh is the management of service communications for east-west traffic flows. East-west traffic refers to the transfer of packets between services (or servers) within an administrative domain. Similarly, north-south traffic is client-to-server traffic and crosses an administrative domain. Within the 5G core signaling plane, the service level communication is categorized as east-west. In contrast, an API gateway (for example, Kong) is typically concerned with north-south interactions, which are first-order service level communications designed and implemented for API management and monetization. In this context, a service mesh is capable of serving as an API gateway, but it is not a first-order concern for the 5G core signaling mesh.

Two main components comprise a service mesh. A service mesh is split between a signaling plane and a mesh control plane. All 5G core signaling traverses a signaling plane composed of lightweight service proxies. The centralized mesh control plane is tasked with the coordination and application of management, operations, and policies to all service proxies. Nokia calls the signaling plane’s instances a Network Function Proxy (NFP). Envoy, an edge and service proxy designed for web-scale, cloud native applications, is an example of an NFP.

The NFP is a lightweight, transparent proxy with support for HTTP/2 and gRPC 5G core signaling terminations. One of its primary roles is to abstract the network by providing a common feature set necessary for every 5G core NF service in order to communicate safely, rapidly, and reliably. In a cloud native approach, the NFP is “built to do one thing and do it well.”

---

4 Kong [https://getkong.org/about/]
5 Envoy [https://www.envoyproxy.io/]
6 Unix philosophy [https://en.wikipedia.org/wiki/Unix_philosophy]
In a modern web-scale, cloud native infrastructure, such as Kubernetes, each of the NFPs is autonomously injected as a sidecar\(^7\) container alongside the instance (or pod) of an NF service. In scenarios where a 5G core signaling network comprises physical or virtualized NPs, the NFP is deployed as a shared proxy NF to provide the same capabilities offered by a cloud native service mesh deployment. Once an NFP has been deployed, it interacts with the mesh control plane over its APIs to implement and apply the necessary policies — observability and security, for example — to the 5G core signaling traffic flows.

This interaction is illustrated in Figure 2, with a simplified view of the Nokia Cloud Signaling Director (CSD) service mesh.

**Figure 2. A service mesh of NFPs with the Nokia CSD control plane**

In the context of 5G core signaling, the service-to-service communication layer is fully distributed messaging. It is composed of JSON payloads over HTTP/2, which are exchanged between NF service instances in the 5G core network. This can also be conceived as a networking model that sits at the layer of abstraction above the IP transport layer, such as TCP/IP. Emerging protocols, such as QUIC,\(^8\) optimize and improve the 5G core signaling security and transport. One of the many advantages of a service mesh, with its collections of sidecar proxies, is that QUIC can be leveraged at the transport layer without having to wait for each NF service to implement, test, and deploy it. The management of the end-to-end service communications includes the ability to optimize the IP transport used independently and transparently of what each NF service is doing. In a robust cloud native architecture, service level communications are most efficiently developed, tested, and delivered by a signaling solution used by all, instead of each NF undertaking independent and variable implementations. The specifics of these protocols are explained in more detail later.

---

\(^7\) Sidecar pattern (http://blog.kubernetes.io/2015/06/the-distributed-system-toolkit-patterns.html)

\(^8\) QUIC (https://tools.ietf.org/html/draft-ietf-quic-transport-09)
While the rationale of the software industry for a service mesh resulted from the adoption by web-scale applications of cloud native micro-service architectures, the pain points addressed by service meshes were already familiar to traditional scalable telecom applications. Indeed, ONAP’s micro-services bus calls for the inclusion of a mesh within the ONAP architecture to facilitate transparent communications among application services. In the same vein, AT&T’s Direct Messaging Engine can be viewed as another early attempt to address these same concerns.

Security

Inter-service secure communications are mandatory for any control plane environment. By default, security is enforced by the service mesh for NF services. These communicate, using mutual TLS connections with automated and secured certificate management.

The Nokia CSD provides the necessary APIs and integration needed to offer closed-loop control of the implementation, compliance, and oversight of the security methods applied across the service-to-service communications layer.

Traffic controls

In a traditional approach, it is typical for application logic to implement, establish, and control the flow of communications traffic based on the topology of established connections with the peer entities that form a group or cluster. With a service mesh, such as Istio, the traffic flows can be decoupled from the infrastructure topology and provide a variety of traffic management features and use cases. Istio describes it “as dynamic request routing for A/B testing, gradual rollouts, and canary releases. These capabilities are all realized through the Envoy sidecars/proxies deployed across the service mesh.”

One example of a use case applied to 5G core signaling is the implementation of a traffic-shadowing pattern. In this case, a portion of the 5G core signaling traffic is mirrored asynchronously and in a controlled manner out of band from the rest of the 5G core signaling network. The mirrored traffic is then redirected to a test cluster where advanced observability and validation takes place with no impact on the production or live network. New software versions of an NF service or a complete network slice are validated against the existing network signaling before initiating an upgrade or new deployment within the live network. All of this is accomplished without impacting or involving the NF.

In addition to traffic-shadowing, more functionality such as load balancing, including automatic retries, circuit breaking, and rate limiting are provided by the Nokia CSD in concert with the NFPS. The Nokia CSD builds on the existing open source service mesh infrastructure to provide enriched capabilities. These capabilities include pro-active isolation of degraded services, as well as selective traffic discard in light of overload scenarios. These, and many other signaling needs, are directly fulfilled by the Nokia CSD, which incorporates depth of experience gained from deployments in 3G and 4G networks.

9 ONAP Microservices Bus Project (https://wiki.onap.org/display/DW/Microservices+Bus+Project)
10 Direct Messaging Engine (https://github.com/att/DME)
11 Istio traffic management (https://istio.io/docs/concepts/traffic-management/overview.html)
12 Advanced traffic-shadowing patterns (http://blog.christianposta.com/microservices/advanced-traffic-shadowing-patterns-for-microservices-with-istio-service-mesh/)
Observability

Troubleshooting a distributed application is one of the more challenging activities of a production deployment. With the advent of cloud native applications, these activities have become more complex and labor intensive. As a result, it is nearly impossible to use traditional techniques for capturing and monitoring traffic as it traverses the network. In the context of service-to-service interactions, the Layer 7 traffic is secured and headers get modified, deleted, and added. This makes it difficult to compose a full picture of end-to-end, 5G signaling.

To address these challenges, the control plane of the Nokia CSD collects and presents a number of use cases related to observability across the network of deployed signaling plane NFPs. A single pane of contextual observability is provided to the human operator to assist in operational proficiency. In addition, raw data can be analyzed and processed by machine learning, analytics, and network automation systems. This further optimizes, secures, and improves service level communications within the 5G core.

Failure handling and injection

The NFP is capable of failure recovery features such as timeouts, active health checks, bounded retries, and others. These capabilities are runtime controlled from the Nokia CSD to provide the flexibility and independent controls based on the overall status of NF services across the service mesh.

Several capabilities already mentioned as part of traffic control enhance the ability of the service mesh to avoid some common failure pitfalls. For example, based on the overall view of the traffic flows and the observability between NF services, a rate limiting policy profile can be applied to avoid the imbalance in service capacity while some components of the system NFs scale or recover to meet the immediate network demand.

The ability to apply circuit breakers is a common pattern for classifying service instances as healthy or not based on health checks. Similarly, the service mesh can be used for fault injection at the application level independent of faulting a service at the IP transport layer. This provides the ability to exercise the resilience of the NF services during service diagnostics, testing, or pre-deployment phases.

Service discovery and exposure

The Nokia CSD provides the necessary service discovery for the pool of NFPs to perform traffic control and update their own dynamic view of the service mesh topology. As NF services scale or recover from service failures, the NFPs are kept abreast of these changes.

The Nokia CSD in a 5G core signaling network builds the needed mesh topology based on the information accessed from the 5G NFs. It is used to register all 5G core NF services and provides service discovery information using the Network Repository Function (NRF).

5G core Binding Support Function (BSF)

In terms of 3GPP standards, a 5G core NF named BSF is needed when multiple and separately addressable Policy Control Functions (PCFs) are deployed in a network. (The PCFs could be multi-vendor or per region/zone.) For its part, the BSF ensures that an Application Function (AF) can reach the PCF holding the session information.
With a 5G core service mesh providing a secure, service-to-service communications layer for all NFs, the Nokia CSD can transparently glean and build the binding support required, or it obtains this information from the host PCF as sessions are established and torn down. In addition, the Nokia CSD tool sets can also conduct BSF audits to ensure that the sessions created by the Session Management Function (SMF) are present and known to the PCFs. The BSF can also obtain session lists from different PCFs to ensure that its own list of sessions is up to date. This can be configured for sessions meeting selected criteria, and not for others. In the case of a transparent BSF buildout, a PCF session establishment request is looked at, the necessary information is extracted from it, and then it is stored in the geo-replicated data store repositories of the Nokia CSD.

5G core Security Edge Protection Proxy (SEPP)

The 3GPP standards call for an entity to provide non-transparent proxy protection for all signaling interactions at the edge of the network’s administrative domain. These are sometimes called trust boundaries. This protection applies to any 5G core signaling that must take place between it and untrusted PLMNs or untrusted 5G slices. The SEPP functions include topology hiding, message filtering, and confidentiality protection of parameters, (such as SUPI), among others.

SEPP shares strong parallels with 4G’s Diameter Edge Agent and Diameter Firewall systems. All control plane messages traversing the network edge must flow through the SEPP. As they do, the messages are inspected, and passed along as is, modified, or discarded. Additionally, SEPP provides complete topology hiding. Any requests to the NRF in its own PLMN do not result in service references being passed to another PLMN’s NF. Instead, all NRF discovery requests are swapped with placeholder NFPs to conduct the SEPP-protected interactions with the other PLMN. In addition, all access flows can be validated, rate limited, and restricted to mirror any business relationships between the PLMNs.

Transport network protocols

The 3GPP standards body has chosen HTTP/2 as the protocol for transporting the various service level signaling messages, as well as events across the 5G core control plane network. The payload for HTTP/2 is JSON, which is one of the most widespread formats used in web-scale applications. 5G adoption of these popular protocols gives the telecom sector access to a vast ecosystem of tools and knowledge not unlike the IT, enterprise, and cloud industries.

By providing optimization for the stringent demands of 5G NFs, HTTP/2 is considered an improvement over the standard web HTTP/1.1. For the initial 3GPP Release 15 specifications, HTTP/2 leverages TLS over TCP/IP for the security requirements, as well as point-to-point connectivity. The initial selection of the security and transport protocols have been considered sub-optimal and suffer from several shortcomings. This issue is expected to be addressed in 3GPP Release 16 or later. As a result, TLS and TCP/IP are expected to be replaced by QUIC and UDP/IP.
Quick UDP Internet Connections (QUIC)

The Internet Engineering Task Force (IETF) describes the Quick UDP Internet Connections protocol as follows:

“QUIC is a multiplexed and secure transport protocol that runs on top of UDP. QUIC aims to provide a flexible set of features that allow it to be a general-purpose transport for multiple applications. QUIC implements techniques learned from experience with TCP, SCTP and other transport protocols. QUIC uses UDP as substrate so as to not require changes to legacy client operating systems and middle boxes to be deployable. QUIC authenticates all of its headers and encrypts most of the data it exchanges, including its signaling. This allows the protocol to evolve without incurring a dependency on upgrades to middle boxes. This document describes the core QUIC protocol, including the conceptual design, wire format, and mechanisms of the QUIC protocol for connection establishment, stream multiplexing, stream and connection-level flow control, and data reliability.”

It is important to note that QUIC is built on years of experience of using internet protocols that originally did not account for a zero-trust security posture. In today’s environment, it is no longer optional for security not to be part of the protocol.

From a latency standpoint, QUIC helps the protocol stack for 5G core networking to be further optimized by allowing the transport layer to offer zero Round Trip Time (0-RTT) resumption for establishment of a session. As illustrated in Figure 3, QUIC’s 0-RTT is critical when low latency applications need to communicate across networks.

In addition, QUIC allows for complete multiplexing of protocols, such as HTTP/2, which benefits from multiple streams at the transport layer. This ability to operate on multiple streams is one of the key benefits of moving to HTTP/2, but using TCP/IP as the transport negates this benefit due to the head of line blocking (HOLB) effect that occurs during periods of congestion or retransmissions at the transport layer.

---

Summary

The Nokia Cloud Signaling Director provides the ability to move 5G core service level communications “into the role of first-class member of the ecosystem – where it can be monitored, maintained, secured, and controlled independently of the infrastructure topology and service level network functions.” Having built large-scale signaling systems, the Nokia Software business group has the depth and experience to give service providers the know-how to address operational challenges in unforeseen ways. In addition, the ability to look into the wire protocols and conduct transparent and NF service-independent monitoring can enhance the operational efficiency of a services-based deployment when a zero-trust security model is considered. The end-to-end visibility of communications at the service level is an indispensable benefit for the operator.

---

15 QUIC connection details (https://jacobianengineering.com/blog/2016/11/1543/)
Further reading

Nokia product information: Cloud Signaling Director (CSD)
Nokia white paper: Anatomy of a microservice
Nokia white paper: Cloud-native core

References

1. CT4 Study Core Internal, TR 29.891 (http://www.3gpp.org/ftp//Specs/archive/29_series/29.891/)

Acronyms

0-RTT Zero Round Trip Time
BSF Binding Support Function
CNCF Cloud Native Computing Foundation
gRPC Remote Procedure Call
HOLB Head Of Line Blocking
IP Internet Protocol
JSON JavaScript Object Notation
KPI Key Performance Indicator
NE Network Element
NF Network Function
NFP Network Function Proxy
NRF Network Repository Function
ONAP Open Network Automation Platform
PCF Policy Control Function
PLMN Public Land Mobile Network
QUIC Quick UDP Internet Connections
SCTP Stream Control Transmission Protocol
SDN Software Defined Networks
SEPP Security Edge Protection Proxy
SLA Service Level Agreement
About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2018 Nokia

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR1803023161EN (March)