

基于服务通信代理的 5G 信令和控制面流量

2021-12-15



概要

随着 5G SA 网络在 2021 年底和 2022 年大规模部署，信令网络将发生巨大变化。在 5G 网络中，信令不再像 SS7 和 Diameter 那样是一个单独的网络。5G 信令与所有使用 HTTPS 或 HTTP/2 协议的网络功能共享控制面。

3GPP R16 中定义了服务通信代理 (Service Communication Proxy)。作为路由控制节点，SCP 能够转发核心网控制面的所有消息。另外，SCP 还负责路由服务发现请求到网络存储功能 (Network Repository Function)，在负载均衡、流量优先级管理和消息管理方面也发挥着重要作用。5G SA 网络的信令至少会增长两个数量级。而 SCP 可以将控制面处理效率提升 30%。通信服务提供商才刚刚开始意识到 SCP 在使能动态路由和管理数百万同步的控制面消息流与信令交互方面发挥的关键作用，这些消息与信令对确保服务性能和盈利能力至关重要。

I. 信令网概述..... 3

II. 5G 信令和 3GPP R16..... 4

信令演进 4

NRF 在 5G 信令中的关键作用..... 4

5G 信令网络备选模型 6

SCP 路由、负载优化和传输保障的优势 7

III. SCP 在 5G SA 网络中的关键作用..... 8

SCP 帮助解决 5G SA 网络面临的主要挑战 8

1. 信令容量的高度扩展性..... 8

2. 多代网络业务支持 9

3. 跨域端到端业务交付..... 10

4. 信令网安全..... 12

IV. 5G 信令网络现状和部署进展..... 14

5G SCP 将随着 5G SA 网络加速部署..... 14

SCP 部署..... 14

V. SCP 的领先供应商..... 16

领先的 5G 信令系统供应商..... 16

VI. 总结 18

SCP 带来的价值 18

分析师联系方式..... 18

I. 信令网概述

随着 5G SA 网络的大规模部署，信令网络将会发生巨大变化。在 3GPP R16 中，5G SA 信令不再像 Diameter 和 SS7 那样有单独的信令传输网络。

在 5G 网络中，网络信令与所有其他事件触发的交互及使用标准 HTTPS/HTTP/2（最终将演进至 HTTP/3）协议的功能间通信共享控制平面。在引入扁平化的服务化架构（Service Based Architecture）之后，信令流量也急剧增加。除了许多其他信令，控制面还要处理服务发现请求和 NRF 响应，以及 IP 地址查询请求来实时查找可用的 NF 实例。

在传统的 SS7 网络上，信令转接点（Signaling Transfer Point）是信令路由节点。在 4G 网络中，Diameter 路由代理（Diameter Routing Agent）和 Diameter 中继代理（Diameter Relay Agent）负责控制 Diameter 信令，它们对 Diameter 信令流量进行路由和负载管理。

3GPP R15 中定义 5G 信令网元可直接发送服务发现请求给 NRF。这种通信模式仅适用于试验和小型网络。

3GPP R16 引入了服务通信代理（Service Communication Proxy）。通过 SCP，控制面可以实时处理大量请求消息并对这些消息划分优先级。SCP 成为核心网中转发所有信令和控制面消息的控制节点，负责路由数百万并发的请求和响应消息，为实现网络切片、微服务实例化和边缘计算访问做出了突出贡献。另外，它还能提升服务发现请求路由效率，帮助控制面实现负载均衡，在流量优先级管理和消息管理方面也发挥着重要作用。

5G SA 网络的控制面会产生大量信令，预计至少比 Diameter 时代的信令量大两个数量级。此外，5G 信令网络还必须同时与传统的 SS7 和 Diameter 网络进行互通，以确保 4G、3G 和 2G 业务的无缝互操作。

通信服务提供商才开始认识到 SCP 在对数百万并发的业务流以及网元间交互进行动态管理时发挥的重要作用，这些业务量与交互将决定 5G 网络的性能和盈利能力。

本白皮书主要阐述了 5G 信令的要求、SCP 部署的一些关键驱动因素、基于 3GPP Model D 组网的 NRF 间接通信以及部署 SCP 的优点。另外，还总结了爱立信、华为、诺基亚和甲骨文四大领先供应商在信令网部署上的优势。

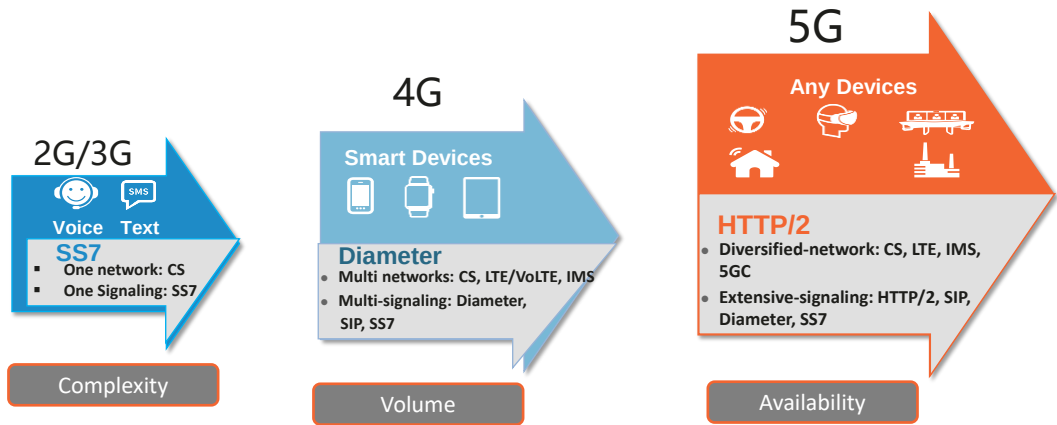
II. 5G 信令和 3GPP R16

随着网络演进，信令的性质也发生了重大变化。

信令演进

2G/3G 网络采用的是 SS7 信令，是以语音和文本为中心的网络。2G/3G 网络最需要优先保证的是业务的可靠性。到了 4G，网络变成以数据和媒体为中心，信令网需要支持智能手机和多样的业务应用，信令业务量也进入了快速增长阶段。进入 5G 时代，网络不仅需要支持传统的业务，还要支持新的高带宽、低时延应用和大规模机器通信，以及进行复杂的跨域互通。当前形势下，如何降低网络复杂度和处理激增的信令业务量是运营商的首要任务。

图 1 信令演进适应运营商业务转型



在 2021 和 2022 年，随着 3GPP R16 发布，基于 SBA 架构的 5G 网络已能够完全商用。鉴于 5G 信令与所有网络功能或应用功能共享控制面，我们预计控制面流量将呈指数上升。

NRF 在 5G 信令中的关键作用

在 5G 网络中，NF 服务消费者通过 NRF 发现可用的 NF 服务生产者实例。3GPP 提出了多种 NRF 通信模式，如下图所示。

图 2 3GPP R15 和 R16 中定义的信令通信模型

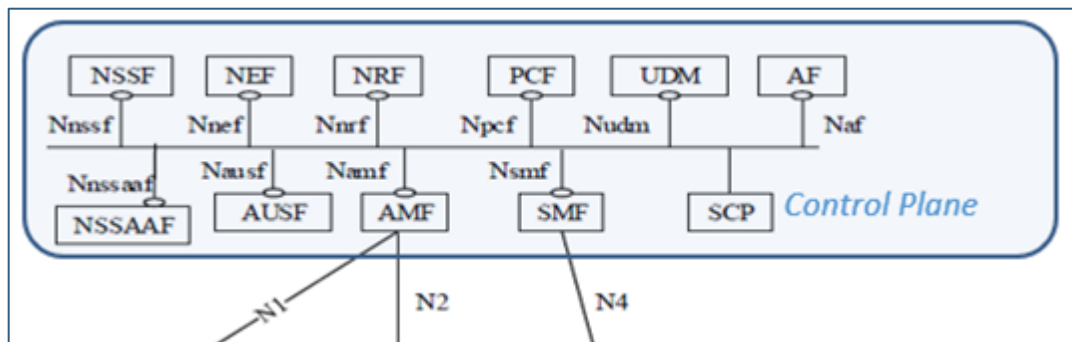
3GPP Release	Model	Communications Flow	NRF and SCP Roles
Release 15	Model A	Direct Communication between NFs without NRF interaction	No NRF requests
	Model B	Direct Communication between NFs with NRF interaction	NF consumer interacts with NRF for Service Discovery and to support Discovery Result Caching and Selection.
Release 16	Model C	Indirect Communication without Delegated Discovery	Adds SCP in the communications path for Service Discovery from NRF
	Model D	Indirect Communication with Delegated Discovery	SCP takes over all Service Discovery and Selection on behalf of NF consumers to monitor and optimize traffic load and routing etc.

来源：3GPP 和 Strategy Analytics

上图展示的四种通信模式中，只有 Model B 和 Model D 被广泛应用。在 3GPP R15 定义的 Model B 通信模式下，NF 服务消费者可直接与 NRF 通信进行服务发现。在这个“扁平化”的网络中，NF 服务消费者通过控制面与 NF 服务生产者互通。运营商通常将 Model B 用于试验和早期的小型 5G 网络。

3GPP R16 定义了 Model C 和 Model D。Model C 和 Model D 通过一个新的网络功能——服务通信代理（SCP）来实现间接通信。这两种通信模式适用于规模较大的网络。

图 3 3GPP 引入新的控制面网元——SCP



来源: [ETSI TS 123 501 V16.9.0 – 5G System architecture for the 5G System](#) – 2021 年 7 月

在上图中，除了标准的控制面网元，包括网络切片选择功能（Network Slice Selection Function），网络能力开放功能实体（Network Exposure Function）和网络存储功能（Network Repository Function）等，还新增了一个网络功能——服务通信代理（Service Communication Proxy）。正如我们前面提到的，在 5G 网络中，所有可用的 NF 实例都需要通过 NRF 进行发现。NRF 记录着每个 NF 可以提供的服务和当前可用的 NF 实例。NF 之间能进行服务发现，NRF 起到至关重要的作用。另外，如果部署了 NEF（Network Exposure Function），NF 的服务能力还能开放给其他 AF。通过 NRF，NF 还能发现其他厂商的 NF 实例，以实现跨域互通。

不同优先级的流量共享控制面

5G 网络的控制面本质上是一条虚拟的“网络总线”。网络功能、服务功能甚至第三方应用都通过这条“总线”来发送请求和响应消息。由此看来，是这条“逻辑总线”在处理 5G 网络的所有控制面流量。与传统网络不同的是，5G 信令与其他流量共享这条“总线”。所有流量都通过无优先级区分的 HTTPS 或 HTTP/2 消息流运行。

NRF 或成为网络通信中的潜在瓶颈

由于每个 NF 都需要与 NRF 进行实时通信，NRF 请求和响应消息数会迅速攀升。由此一来，NRF 可能会成为影响控制面流量处理的“瓶颈”。例如，非信令相关的 NF 服务消费者发往服务生产者的请求消息，或其他 NF 和 AF 之间的请求消息可能会激增，与发往 NRF 的高优先级的服务发现请求发生冲突。

集中路由是大势所趋

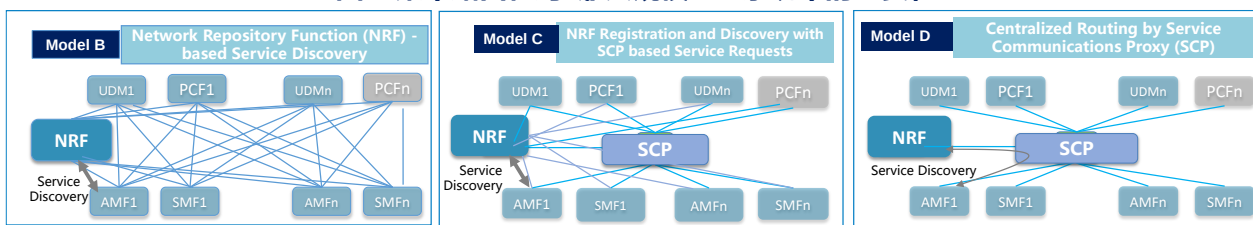
面对上述问题，运营商需要一种机制来优化路由优先级（根据策略规定），并最大化减轻拥塞。为此，3GPP 在 R16 中规定了 Model D 间接通信模式，并定义 SCP 来扮演“交通警察”的角色，由其提供路由、重定向、负载管理和流量优化等功能。

5G 信令网络备选模型

那么，不同通信模式的优缺点分别是什么呢？

下图展示了 Model B（直接 NRF 通信）和 Model C（无代理服务发现的间接通信）带来的弊端，以及 Model D（间接通信和集中路由）是如何从网络简化、流量管理和跨域性能这几方面化解这些弊端的。

图 4 集中路由在跨域/大规模 5G 系统中的重要性



来源：5G 信令产业线上研讨会《信令，5G 网络至关重要的神经中枢》2021 年 10 月

在 Model B 通信模式下，如果 5G 网络中同类型网元有多个，例如多个 UDM、PCF 和 AMF，那发往 NRF 的服务发现请求数量会呈指数增长。这种直接通信模式可能会导致严重的后果，包括：

- NF 服务消费者可能无法实时接收信令消息
- NF 的负载均衡策略可能无法统一
- NF 服务生产者之间的负载不均衡

Model C 也仍在一些运营商的考虑之中。在 Model C 通信模式下，NF 直接与 NRF 通信进行服务注册和发现，同时 NF 也与 SCP 互通，由 SCP 来路由业务请求。然而，Model C 也与 Model B 一样会产生大量的消息流，以及大量额外的服务发现和订阅通知流量。

在引入 Model D 之后，所有的流量通过 SCP 进行集中路由，这解决了 Model C 和 Model B 带来的弊端，也极大地简化了网络操作。具体来说，Model D 具有以下优点：

- SCP 集中路由
- 统一的负载均衡
- 实时发送和接收请求和响应消息
- 控制面流量容量提升

部署 SCP 后，即使面对大量服务发现和查询请求，NRF 也不会成为 5G 控制面信令处理的阻塞点。

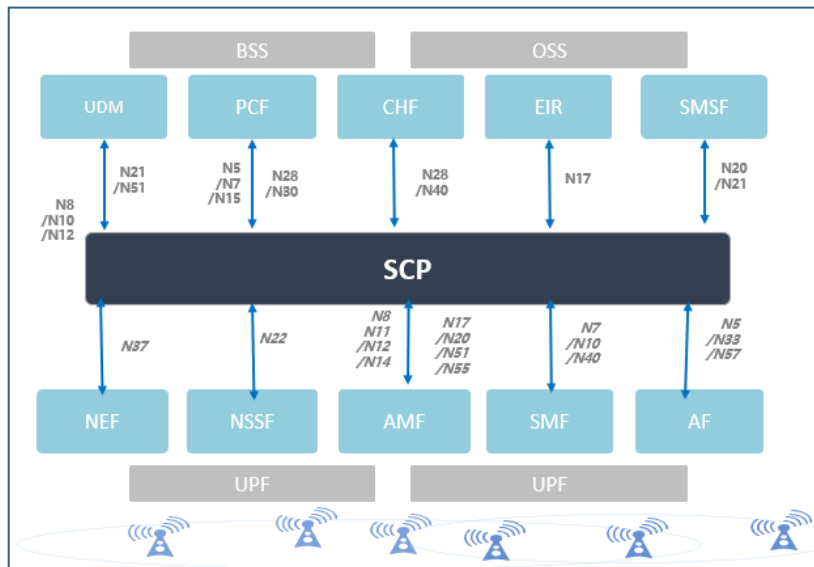
高优先级信令也不会受到低优先级 NF 请求的影响。

Model D 提供的间接路由模式使 5G 商用网络具备可扩展性，也为信令传输提供了保证，提升了网络性能。

SCP 路由、负载优化和传输保障的优势

首先我们要了解 SCP 路由和流量优化是如何提升网络性能的。

图 5 SCP 简化控制面路由和管理



如上图所示，SCP 作为路由中介，管理 5G 核心网中所有 NF 间的请求和响应消息。图上还列出了每个 NF 的参考点接口。

在 5G 网络上，NEF 和 PCF 会限制哪些 NF 之间能相互通信。如果每个 NF 都直接与其他授权的 NF 进行通信，那网络上的交互消息数量就会非常大。

但是，如果 NF 都通过 SCP 进行互通，如上图所示，则仅需分配和管理 10 个动态共享的通信路径。基于策略控制的优先级，不同的消息类型可以共享到同一 NF 或 NRF 的公共路径。在高度分布的云原生环境中，无论 NF 微服务实例在不在同一个容器中运行，SCP 都能极大地简化消息流管理，并高效汇聚流量。

因此，逻辑上集中的 SCP 与规定访问优先级的策略规则相结合，可以规模、有效地调度资源并路由所有的控制平面流量负载。

注意：这里是把 SCP 的集中路由与几家供应商提供的 4G DRA 以及更早的 SS7 集中路由相比较。

III. SCP 在 5G SA 网络中的关键作用

当 R15 首次推出 5G 时，3GPP 还未引入 SCP。几个早期建设的 5G SA 网络不得不耗费大量投资来改造其信令网络，因为随着用户数的增长，信令网络已不堪重负。事实证明，延迟部署 SCP 耗费的成本是建网初期就部署 SCP 所需成本的 3 倍。3GPP R16 发布之后，运营商可以在网络建设初期就部署 SCP，从而避免后期的网络改造和投资。更重要的一点是，SCP 能够帮助解决 5G SA 面临的许多挑战，为通信服务提供商节省大量成本。我们将在下文讨论 SCP 是如何应对这些挑战的。

SCP 帮助解决 5G SA 网络面临的主要挑战

除了优化控制面信令路由外，SCP 还有助于运营商解决在部署 5G SA 业务时遇到的几个关键挑战，帮助他们做到以下几个方面：

1. 信令容量的高度扩展性：

- 流量负荷
- 信令风暴

2. 多代网络业务支持：

- 2G、3G、4G 和 IP 业务，SS7 和 Diameter 仍将长期存在
- 4G 和 5G 融合业务的无缝交付

3. 跨域端到端业务互通：

- 多业务域组网
- 跨运营商业务域的信令互通

4. 信令网安全

- 漫游信令攻击
- 网络边缘安全

下面我们将详细介绍 SCP 如何在上述各个领域做出贡献，并为其带来关键收益。。

1. 信令容量的高度扩展性

SCP 对 5G SA 业务的第一项重大贡献是信令容量的高度扩展性。

控制面的流量负荷将非常高，与信令风暴相当，而且是突发性的。

如前文所述，5G 网络基于扁平化的服务化架构，固有地会产生更多的信令流量。Strategy Analytics 最近的一份基于美国早期经验的[报告](#)中写到，“3GPP 采用 HTTPS 和 HTTP/2，引入了新的基于文本的协议，这引发了行业对网络性能的担忧，因为 5G 控制面上的流量可能（至少）是目前 Diameter 信令量的 10 倍到 20 倍”。根据中国部署的更为成熟的大型 5G SA 网络来看，显然这个预测已经远远低于实际情况。

与 4G Diameter 信令相比，一些中国运营商网络在 5G 控制面上的流量高达 100 倍甚至更多。在 5G SA 网络上，运营商需要应对至少两个数量级的信令流量增长。

综合使用流量汇聚、优化到 NRF 的路由以及在整个控制面上实施基于智能策略的流量优先级等手段，可以从容应对突增的信令流量，SCP 在这一过程中发挥着关键作用。

信令风暴影响控制面业务

近日，东亚某 4G 运营商网络因数据库升级引发大面积网络故障，导致了大规模信令风暴，语音和数据业务中断长达 12 小时。在 5G SA 网络中，即使升级失败后系统可以实现自动回滚，并且实时会话状态能从非结构化数据存储功能（Unstructured Data Storage Function）中恢复，但控制面的信令风暴仍难以避免，因为系统回滚会触发大量服务发现请求同时发往 NRF，同时还会产生大量可用实例查询请求。

对于最大限度减少控制面“信令风暴”的影响，SCP 的作用也至关重要。。

2. 多代网络业务支持

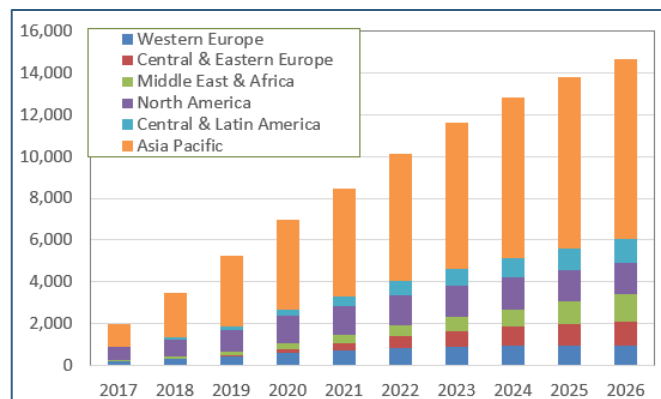
SCP 的第二大贡献是使能多代网络互操作和推动网络向 5G 演进。

支持 2G、3G、4G 和 IP 业务，SS7 和 Diameter 信令将长期共存

即使 5G 用户在迅速增加，仍有许多用户在继续使用传统的网络基础设施。尽管 3G 网络面临关停，运营商会重耕 3G 频谱，但年长的用户可能会继续使用传统的 3G 手机，甚至 2G 网络也将在未来几年内会继续服务一些低端市场或物联网市场。因此，运营商需要为这些用户继续运营 SS7 信令网络。尽管 5G 已经商用，但 4G 用户数仍在增加。在全球范围内，至少到 2026 年，4G 用户数仍是超过 5G 用户数的。

与此同时，运营商亟需实现 VoIP、VoLTE 和 VoWiFi 业务的互操作，以提供完善的语音和视频呼叫业务——IP 会话既可终止于 4G/5G NSA 网络，也可连接到 5G SA 网络。IP 语音、交互式视频通话以及 VoWiFi 业务的互通需要 Diameter 信令的支持。如图所示，在未来几年内，数十亿呼叫将继续依赖 Diameter 信令。

图 6 数十亿语音呼叫 (VoIMS、VoLTE 和 VoWiFi) 将继续依赖 Diameter 信令



来源: Strategy Analytics, Service Provider Strategies

SCP 与信令网关相互配合，使能网络互操作，缩短通话时延，并确保计费的正确性。

4G 和 5G 融合业务的无缝交付

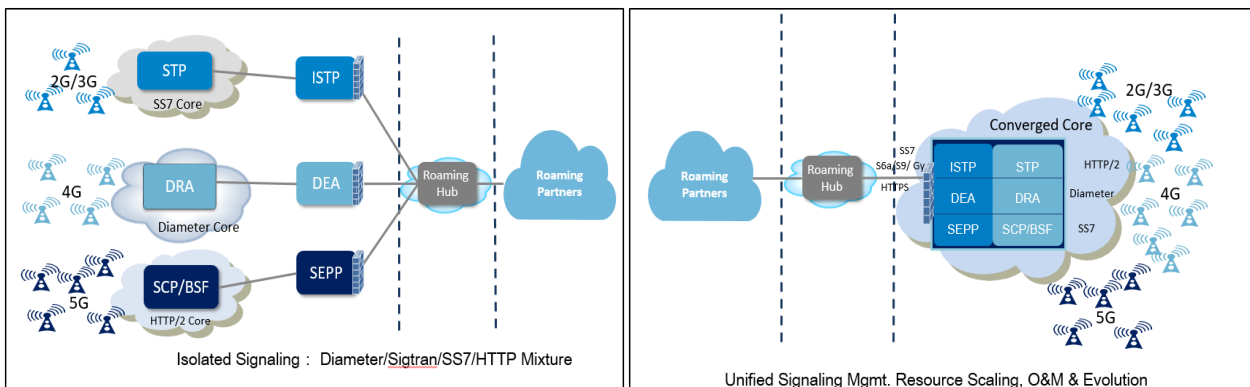
展望未来，包含有 SS7、Diameter 和 5G 信令的完全融合信令解决方案将助力实现高质量的混合业务连续性以及总体较低的运营成本，SCP 是其中不可或缺的一部分。

随着信令网络逐步融合，成本也会进一步降低。

下一阶段是从互操作演进到全融合的信令网络。

如下方左图所示，如果运营商同时维护老旧的 SS7 和 Diameter 网络以及新的 5G 信令网络，那么运维将会变得十分复杂。如果如下方右图所示，采用融合信令解决方案把多个信令网融合成一张网，那网络结构会变得简化，运营成本也会降低。

图 7 独立信令网 vs 融合信令网



来源：5G 信令产业线上研讨会《信令，5G 网络至关重要的神经中枢》2021 年 10 月

在运营商寻求合适的方案来演进他们的 3G 和 4G 网络时，5G 融合信令解决方案在实现无缝演进方面发挥重要作用。统一的信令解决方案使运营商能够在所有网络中充分利用动态资源分配的能力，并确保为传统用户和 5G 用户都提供无缝服务。总结有以下几点：

- 2G、3G、4G 和 5G 网络将长期共存，但传统业务的设备平台面临 EOS 问题。
- 融合信令解决方案降低了多网络运营的成本。
- 2G、3G、4G 和 5G 网络之间需要互操作和动态资源分配，确保传统业务的连续性以及投资回报。

随着网络演进到 5G SA，网络间的互操作成为提供业务的必备条件，而 SCP 在实现网络互操作和传统网络持续运营方面发挥着关键作用。

3. 跨域端到端业务交付

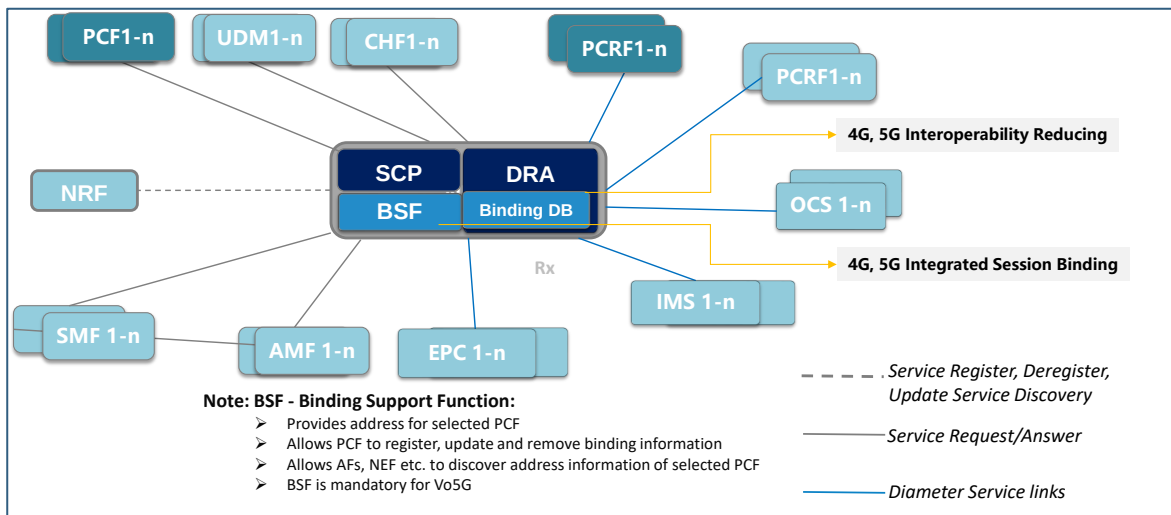
SCP 的第三大贡献是帮助 5G SA 网络实现跨域互通，包括有线和无线网络、公共和私有网络。5G SA 网络不仅需要与传统网络进行互通，还要与多样化的运营商和非运营商网络域以及信令系统进行互通。

多业务域组网

如下图所示，SCP 融合 DRA 及其绑定数据库（Binding DB），与绑定支持功能（Binding Support Function）配合来提供跨域业务。注意：在下图中，运行在不同网络上的网络功能用 1-n 表示。

网络功能	4G 网络	5G 网络
策略控制功能	PCRF 1-n	PCF 1-n
计费功能	OCS 1-n	CHF 1-n

图 8 多 PCF 处理机制



来源：5G 信令产业线上研讨会《信令，5G 网络至关重要的神经中枢》2021 年 10 月

标准的 5G 网络必须支持 4G/5G 互操作。上图展示了 SCP 与 DRA 的共部署场景。在该场景中，SCP 和 DRA 虽然各自继续管理自己的策略域，但运营商能无缝跨 4G 和 5G 策略域来提供呼叫和会话。通过融合信令解决方案，SCP 和 DRA 可以基于优先级协调各域的策略控制功能。

上图中的一个关键网络功能是 BSF，它使网络可以跨 4G 和 5G 来提供端到端的语音和其他业务。在这个过程中，SCP 可以从 NRF 获取多个域内的服务发现信息，进一步确保跨域业务顺利进行。综上所述，当网络上部署了多个 UDM、PCF/PCRF 以及 CHF/OCS 时，SCP/BSF 和 DRA/Binding DB 对于处理 4G/5G 跨域业务至关重要。它们既能各自负责各自域中的策略控制功能，也可以简化 4G/5G 融合业务的操作流程。

跨运营商业务域的信令互通

当不同域由不同的通信服务提供商运营时，每个通信服务提供商会部署各自的 UDM、PCF、CHF 等，就会出现运营商网络间的信令互通问题。因此，必须部署漫游中心（如图 7 所示）来确保运营商域间能够进行互通。

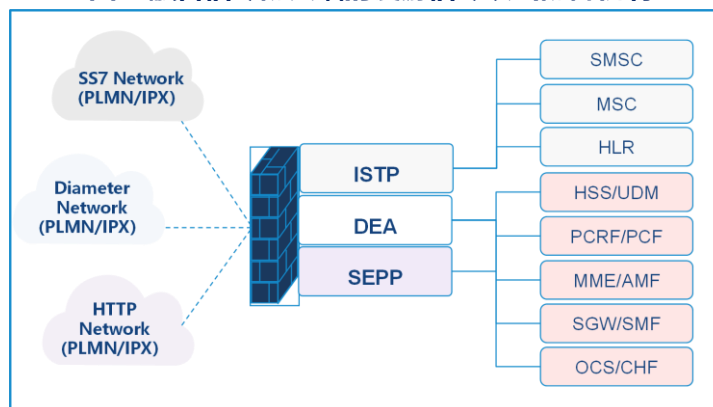
SCP 对于同一运营商的不同域之间以及不同运营商之间的多域业务交付至关重要。

4. 信令网安全

SCP 的第四个贡献是确保信令网络自身安全。

在 5G SA 网络中，信令网安全对于控制面至关重要。如下图所示，5G 安全边缘保护代理（Security Edge Protection Proxy）与国际信令转接点（International Signaling Transfer Point）、Diameter 边缘代理（Diameter Edge Agent）以及防火墙相互配合，以保护所有信令网络（包括 SS7、Diameter 以及 HTTP 信令）。

图 9 融合信令防火墙的漫游信令攻击防御机制



近年来，信令网络频遭安全攻击——主要是来自其他国家不受信任的运营商。最容易受到攻击的目标之一是运营商网络信令汇聚点：信令网关。目前，许多运营商都引入了信令防火墙（如图 9 所示）。在 5G 网络中（如图 7 所示），5G 漫游中心负责安全地转发不同运营商网络间的信令，降低归属地信令网络被攻击的风险。

对于分布式拒绝服务攻击（DDoS）之类的控制面攻击，另一个潜在的“攻击面”是网络边缘。目前，由于多接入边缘计算（Multi-access Edge Computing）业务的开通，运营商需要将安全攻击抵御在信令防火墙之外，防止其靠近数据中心。5G 网络中，运营商可以通过嵌入 SEPP，提供会话前安全协商，端到端应用安全加密，HTTP/2 核心信令封装，以及运营商漫游安全监控等措施，将信令攻击抵挡在数据中心之外。为确保运营安全，SCP 必须与 SEPP 配合，作为安全信令网络的一部分。安全信令网络可以提供如下功能：

网络互通安全：

- 网络拓扑隐藏
- 黑白名单
- 信令屏蔽
- 信令防火墙
- 传输层加密 (IPSec、TLS 和 DTLS)

多网络交叉分析：

- 跨时间位置验证
- 多网络安全分析

因此，即使没有额外的信令网关或防火墙，5G SA 网络固有的安全机制与 SCP 融合，也可以确保控制面信令安全。

IV. 5G 信令网络现状和部署进展

5G SCP 将随着 5G SA 网络加速部署

5G SA 网络部署现状决定 SCP 是否被采用

早在 2019 年到 2020 年间，中国运营商率先将网络从 4G 直接演进到 5G SA。当时，3GPP R16 版本尚未发布，他们采用的是 R15 版本推出的 Model B 组网，因此未部署 SCP。随着 3GPP R16 版本发布，他们计划将原来的 Model B 改造为 Model D 组网，但这需要一些时间才能完成。

一些运营商基于 R15 版本部署了 5G NSA 网络，即采用 4G Diameter 信令和 5G 无线接入。到 2021 年底，全球运营商都在加速部署商用 5G SA 网络。

截至 2021 年 11 月中旬，全球共有 26 家运营商提供 5G SA 公网业务，其中 9 家还为企业、公用事业和政府提供专网解决方案。还有 7 家运营商计划在不久的将来推出商用 5G SA 网络。随着 5G SA 在许多国家成为标准组网，5G SA 网络部署将在 2022 年进一步加速。

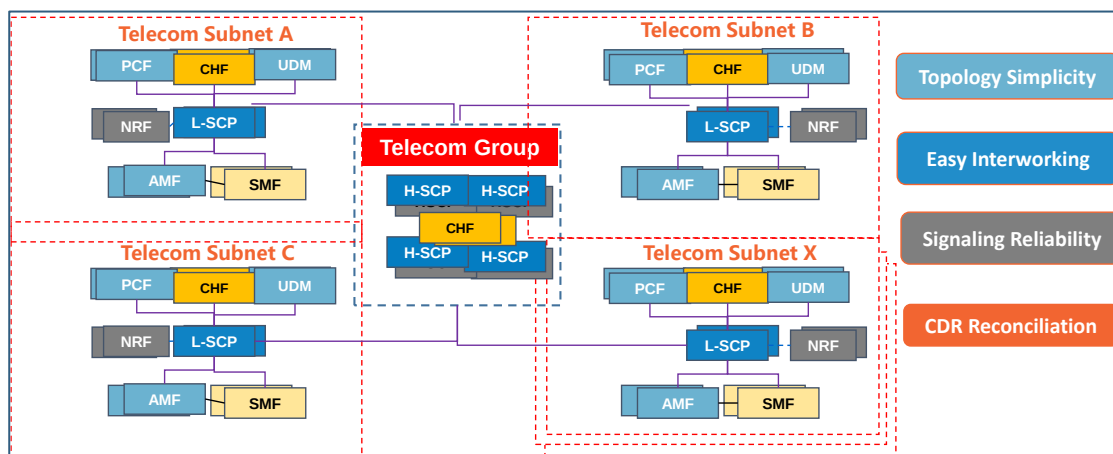
SCP 部署

目前，法国的 Orange、英国的沃达丰、西班牙的 Telefonica、韩国的 SK 电讯、泰国的 AIS、瑞士的 Sunrise 以及中国的三大运营商都在准备全面实施 3GPP R16 版本，并将 SCP 纳入 5G SA 网络部署计划。AIS、中国电信、Sunrise 和 SK 电讯已经商用了 SCP。其他新加入 5G SA 阵营的运营商也已经就他们的信令网络做出了规划并进行了小规模的 5G SA 网络试点运营。随着 3GPP R16 版本发布，SCP 已成为 5G SA 网络中不可或缺的一部分。

中国电信已商用 SCP

SCP 帮助运营商以更佳途径使能 5G SA 现网业务，助力商业成功。中国电信利用 SCP 来管理跨子网漫游用户的话单（如下图所示），将漫游话单的生成时间从几周缩短到了几天。

图 10 中国电信通过部署 SCP 来减少链路，缩短 TTM，并帮助生成漫游话单



韩国 SK 电讯利用 SCP 提升 5G SA 网络控制面效率

2020 年 11 月，SK 电讯在韩国第一个推出商用 5G SA 数据业务，其后又基于 3GPP R16 版本完成了下一代 5G 核心网部署。

SK 电讯与其供应商合作开发了基于云原生技术的 SCP 来更高效地管理 5G 控制面。SKT 采用 SCP 根据流量状态和行为智能调控 NF 间的通信。， SCP 使 NF 能够根据网络流量状态，仅在必要时相互通信，这极大地提高了信令效率。据 SK 电讯估算，SCP 使 NF 间的通信效率提高了 30%。

提前部署 SCP 软件，为 5G SA 信令融合做准备

一些运营商已经在提前部署 SCP 软件，以优化 Diameter 和 SS7 路由，实现安全融合信令。SCP 软件即使在 5G SA 未正式推出之前也可以支持 VoIP、VoWiFi 和 VoLTE 互通，从而在短期内为运营商带来投资回报。另外，SCP 还能确保 5G SA 网络一经推出即可提供一体化的 4G/5G/VoIMS/VoIP 业务。

SCP 正在为运营商创造投资回报

随着 5G 网络的发展，SCP 的商用价值不断提升，成为 5G 网络中必不可少的机制，它不仅可以确保 5G 网络的实时性能和可扩展性，还帮助提升业务处理效率，降低运营成本，提高链路利用率，增加端到端业务收入。

V. SCP 的领先供应商

领先的 5G 信令系统供应商

Strategy Analytics 利用公共渠道比较了四大领先供应商的 SCP 产品：

- 爱立信
- 华为
- 诺基亚
- 甲骨文

爱立信、华为和诺基亚都提供 SCP 产品作为其 5G 核心网产品的一部分。

华为

华为是目前业界唯一——一个提供融合信令解决方案全集的供应商。华为推出的融合信令控制器 ([Unified Signaling Controller](#)) 适用于 5G 核心网，不仅融合了 SS7 和 Diameter 信令，还能提供 SEPP 功能，在跨域业务处理、信令路由优化和负载管理等方面都具有独特优势。SCP 的关键能力包括：

- 基于业务和用户的智能流控
- 控制面负载管理和可靠的抗信令风暴能力
- 2G/3G/4G/5G 融合的信令网络
- BSF 与 4G/5G 业务互通
- 统一的路由数据库和路由控制
- 多层安全防护，支持 5G SEPP
- 信令网络的统一运营和管理（专为自动化而设计）

爱立信和诺基亚提供如下 5G SCP 特性：

爱立信

爱立信的[云化信令解决方案](#)包括 3GPP R15 和 R16 版本中定义的网元——SCP、SEPP 和 BSF 以及其基于云原生的传统 Diameter 信令控制器 (Diameter Signaling Controller)。该解决方案被统称为[信令控制器](#)。它支持静态和动态的过载控制，利用算法高效处理忙时信令，帮助提升网络吞吐量。

然而，爱立信对[SCP 间接通信模式 \(Model D\)](#) 持谨慎态度。他们认为“根据 SCP 的部署方式（包括地理位置）以及信令如何通过 SCP 从 NF 消费者路由到 NF 生产者，信令可能沿途经过多个 SCP.....考虑到 NF 之间的距离很长并且需要经过几个 SCP，一些时延敏感型业务的 KPI 可能会受到影响”。而 Strategy Analytics 认为，具有高吞吐量连接的，良好的分布式 SCP 网络架构应该可以避免这一问题。

诺基亚

诺基亚和爱立信一样，将 SCP、SEPP 和 BSF 三大网元功能融合在一起，推出了云化信令管理器（[Cloud Signaling Director](#)）。它负责处理信令面流量，管理网络拓扑，确保控制面 4G/5G 互操作，保护漫游基础设施，并“通过在控制面中定义行为，提高运营效率、可扩展性和性能”。

诺基亚的 CSD 在 [5G 建设初期可提供基于 SCP 的信令解决方案](#)，其最终会提供 5G SCP 网元功能，用于传输网络内部和网络之间的信令。它的功能包括：

- 智能路由，提高控制面的安全性和可扩展性
- 规则引擎，应对信令和云化流量增长

诺基亚提供特定的模块用于信令风暴防护、信令互通、信令安全、智能路由、负载均衡、过载保护及防欺诈。它还提供与第三方系统集成的接口，包括“敏捷”策略规则创建和修改的增强功能。。

甲骨文

甲骨文推出了基于云原生技术的 [SCP 产品](#)。它提供的功能包括负载均衡、交替路由、基于 5G 的流量分级、NF 服务生产者发现和选择、5G 路由中介、Canary 测试、混合部署、5G 用户位置功能（SLF）和 NRF 协同。甲骨文认为 SCP 可以帮助减少 NF 连接，减轻网络拥塞，平衡网络负载，控制路由，增强路由韧性，提供故障熔断机制和关键指标等，并简化 NF 上线流程。

尽管甲骨文没有提供一整套 5G 核心网产品，但它近来在信令产品部门（前身为 Tekelec）投入了大量资金，以此增强 [SCP](#) 为基础，开发了完全云原生的 5G SA 信令解决方案。

随着新型 SCP 产品的推出，甲骨文未来可能成为几大领先供应商强有力的竞争者。

供应商面临的潜在威胁

除领先的几家供应商外，一些小型的独立信令软件供应商也提供 SCP 软件，包括 Casa Systems、NetNumber 和 Tieto。

这种充分的竞争水平预示着 SCP 能力的重要性和未来创新增强的可能性。

VI. 总结

通信服务提供商已经开始体会到 Model D 作为 5G SA 网络早期部署组成部分的价值，并开始利用 SCP 来动态扩展和管理数百万并发的业务流以及 5G NF 间的交互，以在包括 5G 和传统部分的整个网络中确保高性能和业务盈利能力。

SCP 带来的价值

随着通信服务提供商逐步部署 5G SA 网络并采用 Model D 组网，他们发现了部署 SCP 的诸多优势。下面分别总结了单独部署 SCP 和部署含有 SCP 的融合信令解决方案给网络运营带来的运营优势：

- **Model D 和 SCP 的运营优势：**
 - 服务化架构可延展
 - NF 和 NRF 配置无需更改
 - 端到端服务通信简化
 - 自动化管理
 - NF 路由优化
 - 统一负载均衡和过载控制
 - 业务可编排，满足 5G 业务的低时延和可靠性要求
 - 网络韧性提高，可应对潜在的信令风暴、DDoS 攻击等
 - 操作和维护效率提高，包括网络互操作、故障隔离、路由管理、流量预测、嵌入式安全保护等。
- **含有 SCP 的融合信令解决方案的优势：**
 - 多网络运营简化
 - 资源利用率提高，运营成本降低
 - 支持 SS7 和 Diameter 向 5G 信令无缝演进
 - 支持与 2G、3G 和 4G 业务的无缝互操作
 - 支持跨域业务（包括公共和私有网络、固定无线接入网、WiFi 和移动网络等）
 - 网元间的统一协调，包括 UDM、PCF 和 CHF 等

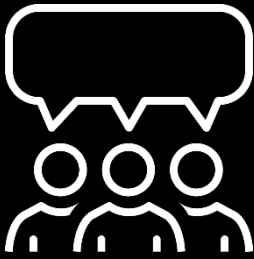
基于 SCP 的 5G 信令解决方案能够确保控制面性能，保证传统和 5G 业务的互通以及端到端无缝交付，保护信令网络免受攻击（包括来自不受信任的运营商的信令攻击），并为新型 5G 业务搭建起面向未来的网络架构。

分析师联系方式

本文作者：[Sue Rudd](#)；邮箱地址：srudd@strategyanalytics.com

Get help from Strategy Analytics

Working with Strategy Analytics gives you the knowledge you need to succeed.



| Understand your customer

Business opportunities abound. But which ones are right for you and your customers? Which will give you the advantage?



| Optimize your user experience

Optimize your product to give your users the best experience and you the market advantage.



| Analyze the market

Understand the size of the opportunity and where your product fits using our unrivalled knowledge and world class data analysis techniques.



| Explore your future

Working with us will focus you. With our insight and forecasting expertise you'll make confident strategic decisions that drive success.

Please contact us at custom@strategyanalytics.com with any questions and for further details and solutions on how we can work with you on creating a custom solution to address your specific needs.