NSP

Network Services Platform

NSP EDGE（Edge Network Services）

边缘网络服务

云杉网络

目录

1 边缘网络服务需求分析 3
1.1 边缘云 3
1.2 增值服务 4
1.3 应用加速 4
1.4 试验创新 5
2 技术方案 6
2.1 整体架构 7
2.2 网络服务编排 8
2.3 网络服务模版 9
2.4 网络功能虚拟化 10
2.5 流量工程 10
2.6 多租户管理 11
3 产品功能 12
3.1 网络服务编排 12
3.2 网络服务模板 12
3.3 网络功能虚拟化 13
3.4 系统管理功能 14
4 客户案例 15
4.1 某省边缘云建设 15
4.2 某运营商安全增值服务 17
4.3 某省游戏加速 18
4.4 某国家实验室大规模网络仿真平台 19

1 边缘网络服务需求分析

边缘计算（Edge Computing）强调应用、服务和内容可以实现本地化、近距离、分布式部署，从而在一定程度上解决了高带宽、低时延、高可靠以及大规模机器通信类终端连接等场景的业务需求。随着云计算、5G、物联网等技术的到来，边缘计算的应用也呈现出指数级的增长态势，包括游戏加速、AR/VR、MEC 等面向用户端的边缘计算应用，边缘层视频监控分析、边缘层视频会议加速、边缘层机器学习等面向企业端的边缘计算应用，以及物联网边缘计算、车联网等面向设备端的边缘计算应用。这些种类繁多、形态各异的边缘计算应用给边缘网络带来了更高的挑战：要求能够为应用提供端到端的自动化网络服务，要求能够满足应用的容量/带宽/时延/安全等差异化需求，边缘网络的复杂度也相应增加了 4~6 个数量级。

1.1 边缘云

边缘云是基于云计算技术的核心和边缘计算能力、构建在边缘基础设施之上、形成边缘位置的计算、网络、存储、安全等全面能力的弹性云平台，并与中心云形成“云边协同”的技术构架，通过把网络转发、存储、计算、 智能化数据分析等工作放在边缘处理，降低响应时延，减轻云端压力、降低带宽成本，并能够提供全网调度、算力分发等云服务。

边缘云网络具有多样性和复杂性，可以就近提供服务，来提供低延迟、高带宽、低成本的网络服务。边缘云对网络服务的具体需求包括如下四个方面：

- **网络功能虚拟化**：边缘云节点以云资源池的方式提供网络服务，网络服务的运行环境多为虚拟机或 Kubernetes 容器，因此就要求能够将所需的网络功能以虚拟化形式来提供。
- **网络服务编排**：参考公有云 VPC 模型做边缘云网络编排并不能满足边缘应用场景。例如边缘业务要与跨地域站点业务打通，一部分由 Kubernetes 集群提供，另一部分由 OpenStack 集群提供，还要访问传统的数据库和存储，那么公有云的 VPC 模型就无法满足上述需求。究其原因，一方面边缘云应用有大量的内部共享服务，需要“大内网”来保障各个应用对共享服务的有效访问；另一方面，边缘应用架构又有微服务化的趋势，需要对微服务进行有效的网络隔离。因此，边缘云需要的是面向业务而非面向资源（如 VPC）的网络编排。
- **设备商解耦**：如果网络功能和设备不解耦，那么网络服务就无法形成统一的抽象，进而无法实现面向业务的复杂网络编排。由于多数部署边缘云的企业都采用多家设备供应商以降低技术和成本风险，异构网络设备的统一纳管成为一种常见的需求。统一的网络功能抽象和异构网络设备纳管，都需要边缘云网络管理系统具有网络功能与设备解耦的能力，以此避免设备商锁定、 提升管理运营效率。

- **多租户管理**：边缘云节点以及运行于边缘云节点之上的边缘网络服务面向的是各种不同的用户，而且这些用户对边缘设备以及网络服务的使用、管理、运维权限也不尽相同，这就要求边缘云网络管理系统必须具备多租户管理的能力，能够对需求不同的用户分权分域、并进行有效的管理。

1.2 增值服务

增值服务主要针对运营商在 5G 和边缘计算场景下，为客户提供的创新网络服务。边缘计算与 5G、大数据、AI 等技术融合后有着广泛的行业场景，为产业带来了巨大的价值，相应的也产生了 AI 加速、边缘网络安全、互联网 CDN、AR/VR 等增值服务。这些增值服务普遍具有高带宽、低延时、高安全性、终端云化等特点，对边缘网络服务提出了多方面的要求，主要包括如下三个方面：

- **虚实混合编排**：AI 加速、边缘网络安全、互联网 CDN 等服务在提供的过程中，支撑服务提供的网络设备不仅包括虚拟化的网络设备，还包括一些传统的物理网络设备或者服务设备，为满足业务需求，这些物理实体设备需要与云资源池中的虚拟网元之间进行灵活组网，这就要求边缘网络服务平台能够支持虚实混合组网、将物理设备、物理网络与边缘云资源池中的虚拟环境进行协同编排与统一纳管、满足用户业务场景的需求。
- **服务链模板**：增值服务在对外提供的过程中，支撑服务提供的网元类型与网元位置相对固定，比如某增值业务流量从互联网 ISP 先进入 IDP、再经过虚拟防火墙、然后经过 WAF、最后进入 WEB Server 端，类似这种相对固定的业务模型如果能通过服务链的方式进行组网编排并形成服务链模板保存下来，就可以规模复制到其它用户相同的应用中去，从而可高效地提供网络服务、并避免人工配置错误导致业务受阻。
- **高性能虚拟网元**：互联网 CDN、AR/VR 等增值服务要求网络高带宽、低时延，这些增值服务需要边缘网络服务平台能够为运行增值业务的 OpenStack 集群或 Kubernetes 集群提供基于硬件的高性能虚拟化网元，避免由网络设备虚拟化带来的集群内部性能瓶颈。同时，OpenStack 集群和 Kubernetes 集群的虚拟网络与外部网络互联，也需要高性能的防火墙和负载均衡服务，避免集群间的性能瓶颈。

1.3 应用加速

在边缘计算应用场景下，用户终端设备是数据的生产者，云端是数据的消费者。例如物联网传感器数据通过边缘计算上传到云端进行消费。这也就意味着，云计算处理的是大数据，而边缘计算处理的是传感器或者用户产生的实时数据。通常情况下，传感器或者用户产生的实时数据对数据处理的时延要求比较高，一般都需要采用基于应用的加速技术来助推数据的实时处理。诸如游戏加速、视频加速、传感器数据实时处理、车联网等都属于这个范畴。

这类应用加速的场景对边缘网络服务的要求主要包括如下两个方面：

- **应用识别**：在边缘侧需要部署 DPI 引擎或者能识别 IP 五元组的边缘网络设备对要加速的应用流量进行及时准确的有效识别，识别出来后才能进行有针对性的加速处理、降低应用时延、提升业务体验。
- **流量工程**：应用识别出来以后，需要对这些高价值的、需要优先保障体验的应用进行全网视角或者 VIP 用户视角的流量调度和网络选路，确保这些应用的传输时延能够明显降低、用户体验得到有效提升，这就要求边缘网络服务管理系统具备流量工程的处理能力。

1.4 试验创新

在科技快速发展的当今时代，迫切需要一大批新一代的网络及安全人才，然而这些人才的产生和培养又严重缺乏有效的试验创新平台。对大专院校来说，需要进行场景实训、工程实践，培养合格的毕业生；对大型企业来说，需要对现网优化并进行安全攻防演练和网络靶场等实践，培养适应企业发展所需的工程师；对科研单位来说，也需要孕育出创新的网络协议和网络应用，培养科学家。所有的这些需求，都需要一个能够提供试验模板能力、支持异构网元集成、且支持多租户管理和用户配置自服务的试验创新平台。具体体现在：

- **试验模板**：网络及安全的实践和创新有一个复杂且充满变数的阶段，唯有基于场景快速编排设计并生成相应的试验模板，才能满足不断变化的需求和场景，并针对不同的试验人员进行快速复制，提升试验效率。
- **异构网元集成**：场景实训、网络攻防、网络靶场、科研创新的过程中，需要的是诸多厂商、形态各异的边缘网络设备，要求边缘网络服务平台能够具备异构网元集成、多厂商设备纳管的能力。
- **多租户及配置自服务**：不论是高校、企业还是科研单位，试验创新平台的运维管理和使用者有多种角色、多种类别，同时人才培养和技术创新离不开能够动手实践的环境，试验创新平台必须具备多租户以及配置自服务的功能。

综上所述，边缘计算各类应用场景下对边缘网络服务产生了几大类的需求，包括：网络服务编排，网络服务模版，网络功能虚拟化，流量工程和多租户管理等。下文第二章主要介绍基于 NSP 产品来满足这几类需求的技术方案。第三章重点描述 NSP 产品的功能。本文最后一章将分享一系列客户案例作为技术方案有效性的印证。

2 技术方案

NSP（Network Services Platform）包含一系列软件组件，主要有编排器（orchestrator）、控制器（controller）和各类插件（plugin）。针对每一个数据中心部署一组控制器，该组控制器用于该数据中心的配置管理和状态维护。多组控制器由一套编排器统一管理。

编排器主要负责北向对接 OSS (Operation Support Systems 操作支持系统), 提供统一抽象的 API 供 OSS 调用，同时南向对接控制器提供统一的资源调度和业务网络编排能力。编排器包含网络服务编排、统一策略配置、业务网络模板三个模块，通过与 OSS 对接为网络运维和网络安全团队提供面向应用的网络、安全服务编排。

- 网络服务编排：通过自动化解决方案，可支持多厂商、多种类型的物理或虚拟网元之间的网络编排，支持 PNF、VNF 网元进行协同异构组网编排。
- 统一策略配置：通过编排器的 WEB 界面以 API 调用的方式对各类虚拟网元、物理网元的网元策略进行自动化配置，并进行统一的策略状态监控，可减少人工干预、避免人工配置错误、并进行快速排障。
- 业务网络模板：通过 TOSCA 编排模型提供面向上层应用的、场景化、高度自动化、可批量复制的模板化编排能力。

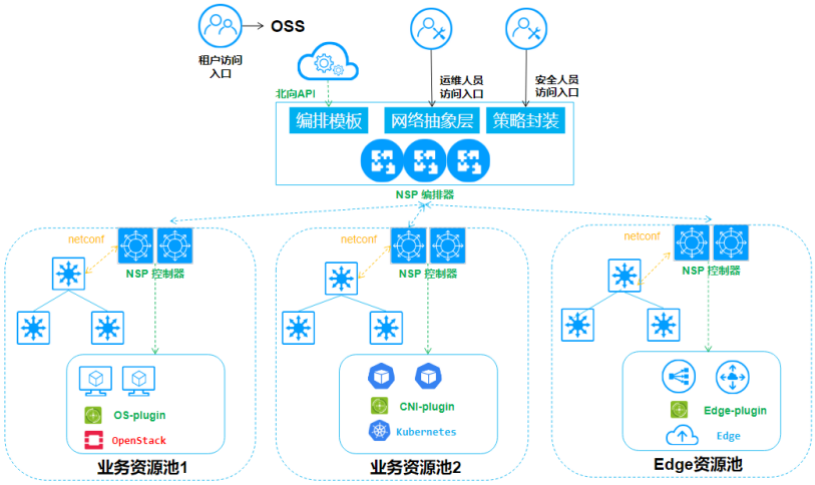
控制器主要负责南向对接硬件网元以及云资源池内的虚拟网元，提供面向网元的配置管理、策略管理、状态维护等能力。基于转控分离 SDN 架构的网络控制器用于执行编排器下发的策略，并自动维护被控网元的状态与预期状态一致。

- 南向对接网元：实现对多厂商、多类型的网络设备的统一管控，包括控制多厂商 Leaf 交换机、控制多厂家的物理网关设备并进行统一的抽象和管理、对基于 X86 服务器构建的 VNF 网元进行统一抽象的管理和控制。
- 北向对接编排器：对基于控制器控制的物理及虚拟网络设备进行统一的逻辑抽象，并以 Restful API 方式提供统一的北向接口供编排器进行调用。
- 运维管理：可提供基于业务的实时路径可视，基于设备配置、设备表项的查询比对，基于 VRF 粒度的运维诊断工具，以及资源检索等运维管理能力。

NSP-Plugin 是运行于各类云资源池（如 Kubernetes 集群、OpenStack 集群）服务器之上的软件，其主要目标是为了资源池能够使用 NSP 所提供的各种网络服务。NSP-Plugin 可为多数据中心、边缘云、安全资源池等提供网络服务的接入，例如面向 Kubernetes 的 CNI plugin，面向 OpenStack 的 Neutron plugin 以及提供各类网络服务的 Edge plugin。

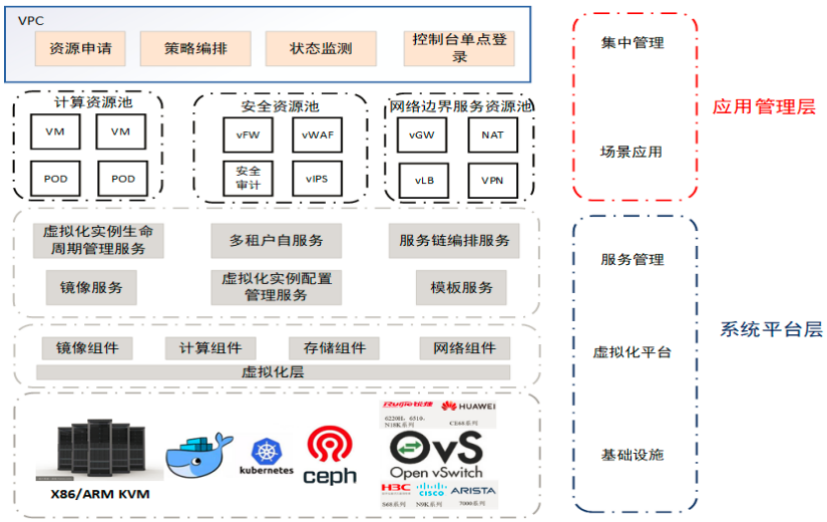
- CNI plugin：实现了基于 Kubernetes 集群架构，为 Kubernetes 资源池提供跨资源池扩容、跨异构资源池组网以及跨数据中心互联等网络能力。

- OpenStack Neutron Plugin：实现了基于数据中心 Fabric 架构，为 OpenStack 资源池提供高性能的，自动化的二三层虚拟网络的能力。
- vSphere Plugin：实现了基于数据中心 Fabric 架构，为 vSphere 云资源池提供高性能的，自动化的二层虚拟网络的能力。
- Edge Plugin：实现了基于数据中心 x86 集群架构，为各类物理/云资源池提供高性能，自动化的边界网络服务，包括网关服务，负载均衡服务，VPN 服务，防火墙服务等。



NSP 产品组件与整体架构

2.1 整体架构



NSP 边缘网络服务技术方案整体架构

如上图所示，整个边缘网络服务平台以层级方式设计规划，分为系统平台层和应用管理层。

系统平台层：包括基础设施、物理/虚拟化平台以及服务管理。

- 基础设施：由成熟的商品化硬件和开源软件组成，向上提供可靠的基础资源服务。
- 物理/虚拟化平台：提供镜像管理，模板管理，存储管理，网络虚拟化，网络功能虚拟化等功能。

- 服务管理：提供虚拟化实例生命周期管理、虚拟化实例配置管理、服务链编排管理以及多租户自服务等功能。

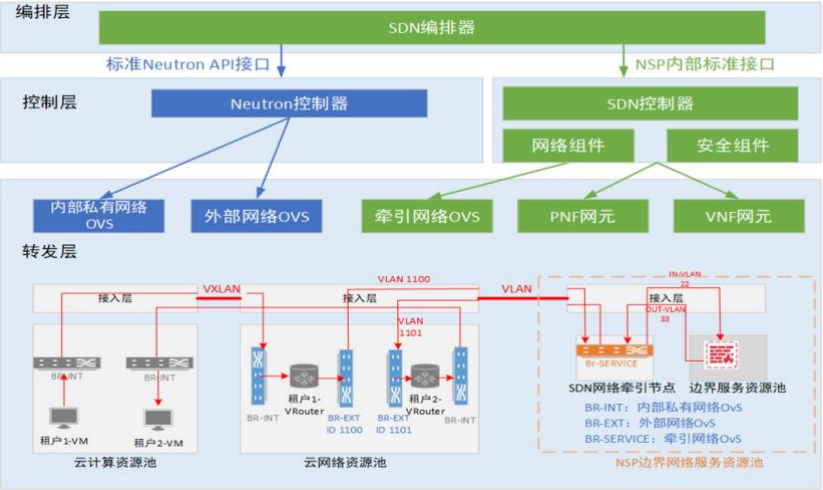
应用管理层：包括场景应用和集中管理。

- 场景应用：提供计算资源池中的 VM、POD，安全资源池中的 vFW、vWAF、vIPS、漏洞扫描、堡垒机、态势感知、安全审计，网络边界服务资源池的 vGW、vLB、NAT、VPN 等；
- 集中管理：提供基于 VPC 的资源申请、策略编排、状态检测以及控制台单点登录等管理功能。

2.2 网络服务编排

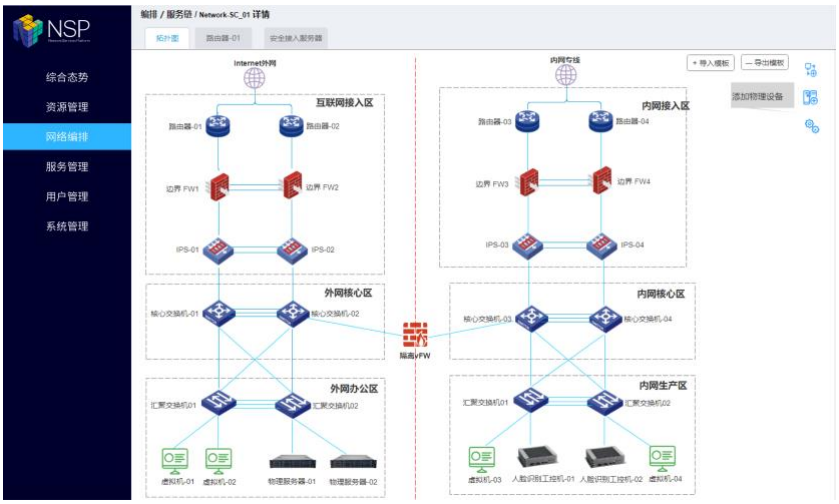
SDN 以其控制转发分离的特性，通过对基础网络的虚拟化和逻辑抽象，通过网络的集中控制部件--网络控制器的控制，可以引导转发流量自动穿过网络服务节点，从而实现拓扑无关的、灵活、便捷、高效、安全地调配转发流量到服务节点上并进行网络业务的处理，从而形成 SDN 定义的 Overlay 虚拟网络中的服务链（Service Function Chaining）。

由 NSP 控制器负责将 Overlay 网络中流量牵引至网络服务资源池，然后控制器能够通过精细流表控制旁路流量（同时支持串联/单臂路由、串联透明和旁路部署等多种方式），从而实现高效的调配转发流量在网络服务资源池内不同服务节点上的业务处理、实现南北向流量和东西向流量的按需网络、安全服务。



网络服务编排-流量牵引功能

在网络仿真、网络靶场、增值服务等应用场景中，客户网络中的物理实体设备需要与 Edge 资源池中的虚拟化网元进行灵活组网，这就需要 NSP 支持虚实混合组网、将物理设备、物理网络与 Edge 资源池中的虚拟环境进行协同编排与统一纳管、满足客户业务场景的需要。



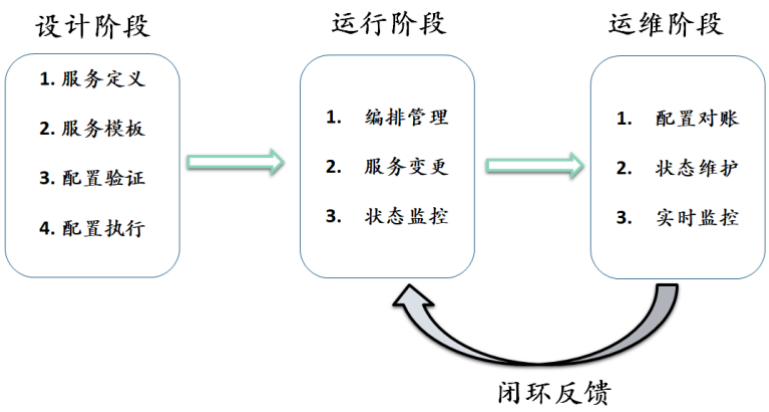
网络服务编排-虚实混合编排产品效果图

如上图所示，NSP 资源池在虚实混合编排场景中可提供如下核心产品能力：

- 提供统一图形化的画布、并通过拖拽连线等简易操作对客户网络中的 PNF、VNF 网元进行协同异构组网编排；
- NSP 的 Web 界面通过 API 统一自动化配置网元，减少人工干预，避免人工配置错误；
- 对物理实体设备，可通过 Web 界面提供统一的远程管理通道，用户可直接对物理设备进行远程管理及配置、提高配置管理和运维管理的效率；
- 通过自动化解决方案，支持多厂商、多种类型的物理或虚拟化网元；
- 支持通过 SDN 技术及拖拽组网方式实现虚拟设备与虚拟设备之间、虚拟设备与物理设备之间、物理设备与物理设备之间的网络编排应用场景。

2.3 网络服务模版

NSP 边缘网络服务平台中的服务模板是用来定义完成特定功能目标的 TOSCA 网络服务模板，它能够定义网络服务的类型、规格参数、拓扑、基本配置，可帮助快速生成网络服务实例。



网络服务模板生命周期各阶段

如上图所示，网络服务模板的生命周期可分为三个阶段：

- 设计阶段：该阶段主要进行服务的定义（图形化方式）、服务模板的生成以及基于模板化编排时 TOSCA 配置脚本的验证和执行。
- 运行阶段：该阶段可进行编排实例和网络连接的管理、服务的变更操作，并将对整个服务实例的运行状态进行图形化的监控呈现。
- 运维阶段：该阶段用户可通过对模板生成实例状态的实时监控、实例状态的维护操作以及配置对账等运维操作来对设计阶段和运行阶段进行闭环反馈，从而更高效地支撑业务部署和运行保障。

综上，用户可通过定义面向客户应用的 TOSCA 网络服务模板来实现面向应用的服务编排，同时网络服务模板可帮助用户实现：

- 以可视化方式固化业务使用场景；
- 快速构建网络服务实例；
- 实现业务场景批量复制；
- 使得运维监控、运维诊断更加直观高效。

2.4 网络功能虚拟化

- 多厂商、设备商解耦：NSP 面向 VNF 集成遵循 ETSI 标准框架、基础平台提供开放管理能力、可集成用户业务所需的各种第三方厂商 VNF（包括且不限于虚拟计算类、虚拟网络类、虚拟安全类），NSP 基于 NFV+SDN 技术可提供以下多厂商 VNF 能力：（1）提供对云网络基本纳管能力，可实现与云网络无缝衔接；（2）提供虚拟防火墙、网关、负载均衡、VPN 等云基础设施网络服务；（3）提供等保要求的安全能力如 WAF、IPS、网页防篡改、抗 DDOS、入侵检测、漏洞扫描、数据库审计、堡垒机、态势感知等安全能力；（4）实现高性能链路负载均衡能力。
- 高性能：NSP 可提供高性能虚拟网元并基于 OVS-DPDK 等性能加速技术提供基础二层网络服务功能，网络性能优化后虚拟机单网卡的吞吐可达 8Gbps 至 10Gbps。
- 弹性扩展：Edge 资源池基础平台层面可通过虚拟化技术实现资源池跨地域部署以及计算、网络、存储的横向弹性扩展；同时在虚拟化网元层面支持负载均衡能力，可对同类型的服务网元可按需横向扩缩容。

2.5 流量工程

NSP 边缘网络服务平台可通过集成对接第三方 DPI 引擎对业务流量进行特征识别，或者通过

自研的网络服务设备对业务流量通过 IP 五元组进行识别，达到首先识别出高价值应用的目的。然后，NSP 编排器和控制器协同工作，实时感知并计算得到应用传输路径中各个可用网络切片的时延、带宽、丢包率等性能指标，并将高价值的应用流量映射到性能指标最优的网络切片、将低价值的应用流量映射到性能指标次优或者性能指标较差的网络切片，从而可以控制不同的业务流走不同的路径，关键的业务走可靠的路径并保证服务质量，并且在某段网络拥塞的情况下，动态调整路由，整个网络如同一个“可控的城市交通系统”。

2.6 多租户管理

- RBAC 的多租户管理体系： NSP 边缘网络服务平台的多租户管理遵从基于角色的访问控制（RBAC）体系。对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限。这样做的好处是，不必在每次创建用户时都进行分配权限的操作，只要分配用户相应的角色即可，而且角色的权限变更比用户的权限变更要少得多，这样将简化用户的权限管理，减少系统的开销。
- 配置自服务：NSP 边缘网络服务平台通过基于业务的模板、自动化服务链编排以及统一的南向 API 调用等手段实现了用户配置自服务，用户可根据自身实际需求并结合 NSP 简单明了的 WEB 界面完成业务的自服务开通。

3 产品功能

3.1 网络服务编排

类别	子功能	功能描述
服务链编排	服务链创建-VNF 网元部署模式	针对 VNF 网元的部署方式支持三种: 1.串联路由模式 2.串联透明模式 3.独立部署模式
	服务链删除-VNF 网元摘链	支持两种 VNF 摘链方式：a.支持对指定 SF 手动摘链；b.支持对整体服务链自动摘链。 VNF 网元基于分类规则摘链
	服务链删除-网元链删除	基于分类规则删除服务链
	服务链恢复-VNF 网元恢复	与 VNF 网元摘链相对应，支持某个或某些（包括所有）网元恢复时手动加入服务链
	服务链恢复-SF 高可用切换	SF 所在的 VNF 网元发生高可用切换（网元异常或者网元软件版本升级）时，系统能够感知并自动更新 SFP 服务功能转发路径
	网元链状态恢复	系统自治性状态恢复，配置一致性检查（以控制面 CMDB 系统为主）
虚实混合编排	物理设备接入交换机管理	支持手动录入物理实体设备上联的接入交换机，并批量获取接入交换机接口信息、对交换机接口信息进行编辑操作
	物理设备管理	支持手动录入物理实体设备并指定物理实体设备连接的接入交换机端口信息、远程访问方式等
	虚实混合组网	支持通过编排画布 WEB 页面将物理实体设备和虚拟网元进行编排组网、解除组网、组网连接信息查看等

3.2 网络服务模板

类别	子功能	功能描述
网络服务模板	模板导出	支持通过应用实例导出网络服务模板
	列表展示	可展示模板名称、模板描述、导出时间，并支持通过列表查看详情、预览、生成实例和删除操作
	查看详情	查看服务模板对应的 TOSCA 文件
	模板预览	以图形化方式展示模板对应的拓扑概况
	生成实例	通过服务模板生成一个服务链应用实例

	模板删除	删除当前网络服务模板
	异常处理	支持 TOSCA 模板生成实例出现异常时手动清理异常及 Retry 功能
应用实例生命周期管理	实例新建	新建实例并填写应用实例基本信息，如实例名称、实例描述等
	填写实例参数	通过服务模板生成实例时需要指定实例详细参数，包括：外部网络类型、外部网络 IP、外部网络 VLAN、内部网络 IP 网段等
	配置检查	展示 TOSCA 配置模板文件，里面包括实例化的具体参数，方便用户进行核对
	部署检查	对网元是否能构建以及网络连接是否能配置进行可行性检查
	配置提交	整体编排内容下发做实例化创建
	实例修改	对实例名称、实例描述、接入 IP 等进行修改
	实时动态模板生成	支持对应用实例实时生成动态服务模板
	实例删除	对已经创建完成的应用实例进行一键式删除

3.3 网络功能虚拟化

类别	子功能	功能描述
VNF 镜像管理	上传	上传 VNF 网元的 KVM 镜像文件。必填参数包括：名称，网元类型，网元所属厂商；选填参数包括：描述、网元版本号。上传时间自动生成
	下载	可下载指定网元镜像文件，支持批量下载
	修改	修改录入的网元镜像。所有上传子功能参数均可修改
	删除	删除指定网元镜像，支持批量删除
	查看	1.查看所有镜像文件的名称、类型、厂商，支持列表项排序。 2.查看指定镜像文件时，呈现名称、类型、厂商、版本号、上传时间
VNF 模板管理	创建	对 CPU\内存\存储\网卡规格做定义和管理，包括：名称、描述（选填）、CPU 核数、内存、磁盘（系统:50G，不支持扩容、数据：缺省 100G，支持扩容）、网卡数量（1<= vNICs <= 10）。注：考虑 EPA 特性（CPU affinity、NUMA）提高网元计算能力
	修改	只支持修改名称和描述
	删除	没有被网元引用的模板可被删除，支持批量删除
	查看	支持模板列表查看，包括名称、CPU、内存、存储、网卡
VNF 生命周期管理	创建	对指定的网元做实例化，包括：名称、描述、模板名称、要加入的网络
	修改	修改名称时无需检查网元状态
	删除	删除网元时需要用户确认，支持批量删除
VNF 配置管理	平台初始化配置	在创建并启动网元实例时，通过控制平面配置网元的基础信息，包括：用户

		名、初始密码、管理 IP 和管理路由
	配置导入	除了平台初始化配置信息外，用户配置的其他信息可导入并覆盖指定 VNF 网元
	配置导出	用户可对指定 VNF 网元配置信息到导出备份，注：不包含平台自动配置的初始化信息（用户名/密码/管理 IP 和路由信息）
控制台访问	VNF 控制台访问	支持从 Edge 界面跳转访问网元的 portal 页面，通过管理网络平面 https 加密访问
设备管理	计算资源使用率统计	展现 CPU/内存/系统盘计算资源的使用率
	接口统计	展现网元所有接口的名称、类型、IP 地址、状态以及接收和发送字节数、包数、丢包和错误包数量

3.4 系统管理功能

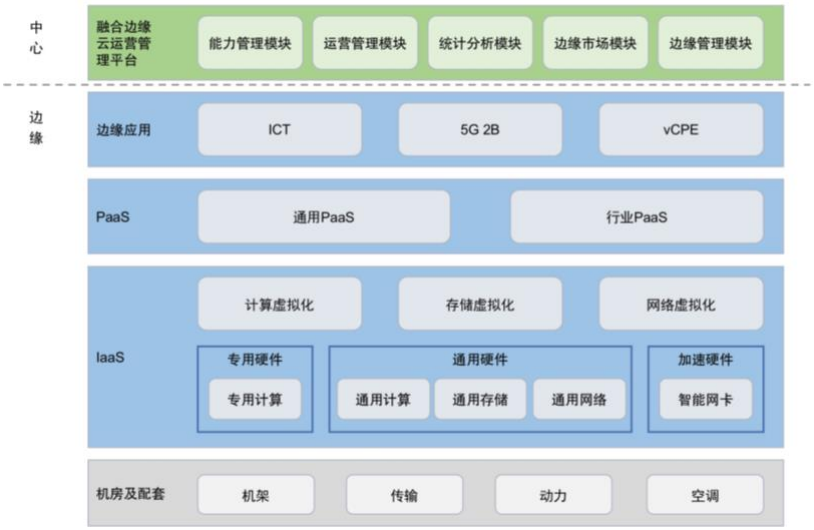
类别	功能	备注
SDN 控制器	OC 分离	编排面与控制面分离
	高可用	控制器异常不影响数据面转发；
DashBoard	自定义展示窗口	支持用户灵活自定义 Dashboard 展示窗口内容
	Edge 使用状态	支持展示 Edge 资源池的 CPU、内存、存储使用状态
	VNF 服务实例状态	支持展示 Edge 资源池集成的防火墙、WAF、vRouter 等 VNF 实例的状态
资源管理	资源录入	支持 Web 录入路由器、接入交换机、物理实体设备； 支持 Web 录入 Edge 资源池以及资源池内的 VLAN 资源池、管理 IP 资源池、接入线路、接入 IP、互联 IP 地址池；
	资源展示	支持以列表方式展示 Edge 服务器信息，包括 Edge 服务器名称、管理 IP、所属 Edge 资源池、CPU 使用情况、内存使用情况、存储使用情况以及 Edge 服务器状态
用户管理	管理员角色管理	支持超管用户对普通管理员用户的创建、修改和删除
	租户角色管理	支持管理员用户对租户的创建、修改、删除、锁定、解锁操作
	多租户权限控制	支持多租户，可按照租户粒度隔离展示对应的资源、服务信息
	配置自服务	支持租户登录 NSP Web 界面进行配置自服务
系统日志	日志展示	支持展示平台相关的用户登录及用户操作日志
	日志查询	支持查询最近 1 小时、最近 6 小时、最近 1 天、最近 1 周、最近 1 个月、最近 1 年的日志信息

4 客户案例

4.1 某省边缘云建设

概述：

中国移动某省公司结合省内各类业务需求，先行先试在各地市建设融合边缘云，与 5G MEC 共址建设，分层解耦建设 IaaS、PaaS 和融合边缘云运营管理平台，满足地市 ICT 项目、5G 2B、vCPE 业务等各类业务需求。整体架构如下：



案例 1-图

- 边缘 IaaS 层：充分利旧现有硬件，补齐通用硬件，试点边缘加速，引入 2 家云平台厂商打造异构技术栈，提供丰富的云服务能力。
- 边缘 PaaS 层：通过引入+自研方式构建通用+行业 PaaS 能力。
- 边缘运营层：升级边缘云运营管理平台为“融合边缘云运营管理平台”，满足云网融合产品的统一运营需求，运营层建设待需求进一步明确后在下阶段项目中考虑。

面向业务的网络服务编排：

边缘网络服务平台实现数据中心 Multi-Fabric 网络统一管理和编排交付，具备灵活的网络编排能力，以满足多种业务场景角网络需求：

- 支持裸金属服务器、虚拟机、容器等计算对象的混合组网构建 VPC；
- 支持裸金属服务器、虚拟机、容器等计算对象的统一安全策略配置；
- 支持跨 Fabric 二层、三层网络互通；
- 支持跨数据中心租户业务三层互通；
- 支持跨数据中心网络编排时同时接入物理设备 PNF 和虚拟网络服务 VNF；
- 支持独立的网络服务资源池构建，以提供东西向和南北向网络服务；网络服务资源池既

可以是盒式硬件设备也可以是 X86 服务器，以满足同时接入多类网络服务的能力（包括防火墙、负载均和器、VPN 等）。

多厂商网络服务支持能力：

数据中心根据区域业务规划分为多个网络安全域，安全域内和各安全域之间南北向和东西向网络访问需根据业务需求进行安全策略管理，S 融合云 SDN 控制器将实现租户粒度 L4-L7 网络服务编排和服务，包括物理防火墙、虚拟防火墙、物理负载均衡器、虚拟负载均衡器等。

高性能网络虚拟化：

部署 OpenStack 以及裸机 Kubernetes 资源池，由 Fabric 提供网络虚拟化能力，SDN 控制器统一纳管并由编排器构建混合云网络。

4.2 某运营商安全增值服务

概述：

该运营商建设的云网融合安全服务支撑平台的定位是面向集团客户领域 DC 托管、移动云、ICT 合作建设托管、互联网专线接入用户的统一营销与服务支撑门户。主要功能是提供安全服务产品的展示、线上解决方案咨询定制、产品订购、服务报告、态势感知呈现及底层安全服务设备资源池节点的管理策略配置、分析查询、集中认证、安全域划分、统一维护、日志合规留存等。

案例 2-图

多厂商安全设备集成：

该云网融合安全服务支撑平台在建设的过程中所采用的安全设备（如防火墙、WAF、IPS、抗 DDOS、IDS、堡垒机等）由多家设备厂商提供，且设备形态包括物理和虚拟化两种，通过 NSP 边缘网络服务平台提供的网络功能虚拟化、以及多厂商&设备商解耦能力，用户可达到节省投资、防止厂商绑定之目的。

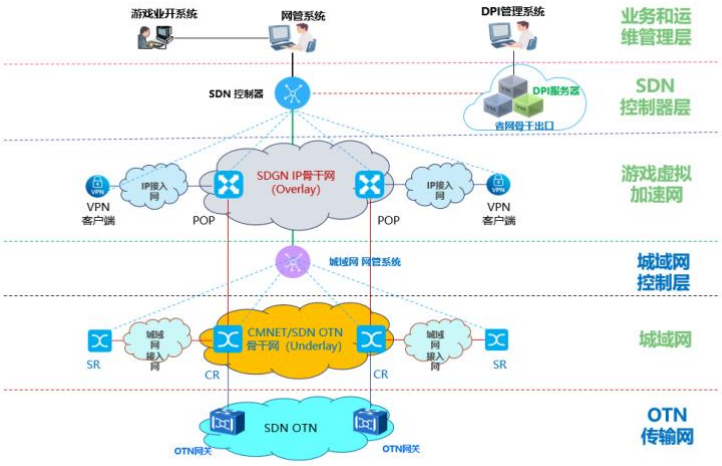
面向安全业务的网络服务编排：

边缘网络服务平台具备灵活的网络服务编排能力，由边缘网络服务平台中的 SDN 控制器负责将 Overlay 网络中的流量牵引至安全业务资源池，然后控制器通过精细流表控制旁路流量，从而实现高效的调配转发流量在安全资源池内不同安全服务节点上的业务处理，实现南北向和东西向流量的按需安全服务。

4.3 某省游戏加速

概述：

该游戏加速项目的目标是为了整体提高家宽用户访问内地游戏平台的网络质量，使得用户能够获得全省最优秀可靠的网络体验，并通过 SDN 控制器实现指定游戏转发路径的自动调整，以将游戏应用流量转发到更可靠的链路上。



案例 3-图

面向应用的流量工程：

通过 DPI 引擎识别出对网络有超低时延要求的网络游戏类业务，然后通过 NSP 边缘网络服务平台的流量工程能力将这些高价值的游戏业务映射到性能指标最优的传输链路上进行传输，从而达到对游戏业务有效加速的目的。

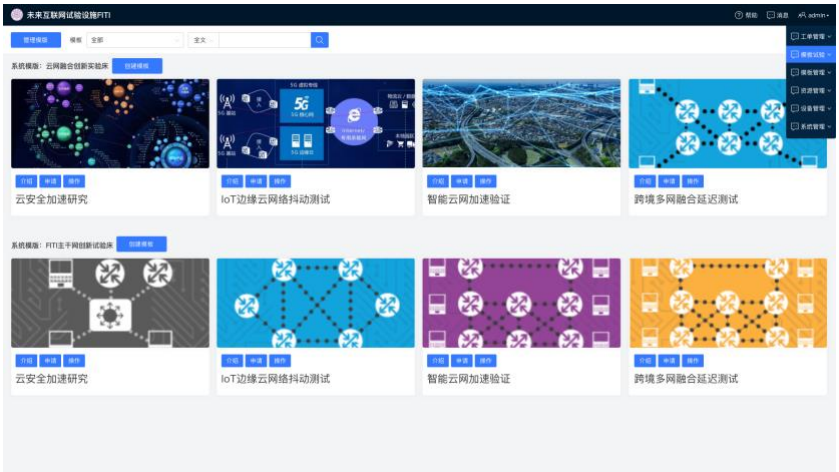
网络功能虚拟化：

通过 NSP 边缘网络服务平台提供的虚拟路由器网元来实现游戏业务在边缘节点的用户面转发，从而实现软硬件解耦、避免厂商绑定的业务诉求。

4.4 某国家实验室大规模网络仿真平台

概述：

某国家未来网络试验基础设施平台，是我国信息领域第一个国家重大科技基础设施项目“未来网络试验设施”，覆盖全国 40 个高校的边缘站点，服务于未来互联网科研技术人员，该试验床用于网络空间安全、可编程网络、物联网等业务场景的新技术、新协议验证。NSP 边缘网络服务平台帮助用户构建未来互联网孵化平台，通过试验平台孵化出一个未来互联网，用户拥有真实的 IP 地址和真实的自治域号码，让用户拥有完全的操控权。与互联网连接，引入真实流量，逐步拥有真实的用户，提供真实互联网服务，成长演进为一个真正的“未来互联网”。



案例 4-图

面向科研创新的网络服务模板：

该试验创新平台的建立和使用以模板为中心，将所有的科研创新场景固化为系统模板和个人模板两种类型的网络服务模板，科研人员可通过 WEB 界面查看到相应的模板并进行模板申请、试验等操作。这些模板均由 NSP 边缘网络服务平台提供的标准的 TOSCA 模板文件生成，并通过 NSP 边缘网络服务平台提供的自动化编排能力将模板转化成试验实例。

基于 RBAC 的多租户管理：

该试验创新平台的用户共分为三类：管理员、VIP 用户（科研人员）以及普通用户（助教），NSP 边缘网络服务平台针对每类用户分别赋予不同的操作维护权限，管理员在创建具体用户时只需将该用户划分到相应的用户类别中，即可完成对该用户的授权和认证管理操作，可显著提高平台运维效率。

更多信息

专业的售前技术支持及商务合作，协助您选择最合适的解决方案

详询：400-9696-121

网址：www.yunshan.net

北京云杉世纪网络科技有限公司

北京市海淀区成府路 28 号优盛大厦 A 座 1209

版权所有 © 2022 YUNSHAN Networks 保留所有权利。 本资料中的文字内容和产品相关图片未经北京云杉世纪网络科技有限公司书面许可禁止擅自摘抄、复制部分和全部内容，并不能以任何形式传播。