NFV 产业发展白皮书（2016）

SDN/NFV 产业联盟

2016 年 4 月

版权声明

前 言

过去一年，SDN/NFV 所倡导的网络开放化、虚拟化、智能化、融合化的技术理念得到了越来越广泛的认同，成为全球业界普遍看好的促进现网升级演进、未来网络技术创新的重要技术途径。NFV 技术通过硬件和软件解耦，以及软件功能的虚拟化，进一步细化和拉长产业链环节，促进产业重心将由硬向软快速调整，推动新一代信息通信技术产业生态的加速构建，将对今后 5-10 年全球信息通信技术创新、产业发展、网络升级产生深远的影响，成为技术产业发展的新焦点和新方向。

SDN/NFV 产业联盟秉承联盟“开放、创新、协同、落地”的宗旨，以引导国内 NFV 技术产业发展、加快构建 NFV 自主产业生态为目标，聚焦 NFV 技术、产业、部署等热点问题，组织国内主要网络运营商、典型互联网企业和相关科研机构，开展广泛而深入的调研与分析，编写完成了《NFV 产业发展白皮书（2016）》。白皮书分为”NFV 产生背景及发展驱动力、NFV 产业现状和发展趋势、NFV 关键技术问题和挑战、电信运营商对于 NFV 的技术需求、传统电信网络向 NFV 的演进策略、产业联盟的 NFV 推进策略及 2016 年重点工作“等六个章节，总结了过去一年全球 NFV 技术产业发展态势与特点，研判了未来几年国内 NFV 技术研发、网络部署的发展趋势与重点方向，以期对国内相关技术产业发展提供了必要的指导与支撑。

本白皮书的编制得到了中国电信、中国移动、中国联通、中国信息通信研究院、华为、中兴、华三、上海贝尔等企业的大力支持和配合，在此一并表示感谢。

目 录

NFV 产业发展白皮书

1 NFV 产生背景和价值

1.1 背景与驱动力

（一）现有相对封闭的网络架构以及粗放的网络建设与运维模式难以支撑网络可持续发展。

传统的电信网络架构是在 90 年代以电话业务为主的时代确立的，随着数据业务流量的爆炸式增长，现有网络架构暴露出难以克服的结构性问题，主要体现在以下几个方面：

（1）网络复杂且与业务强相关。每一种新业务的引入都需要新建一张承载网络，而且通常是由功能单一、价格昂贵、专用的硬件设备构成；

（2）网元设备使用软硬件一体化的封闭架构，导致设备日益臃肿、扩展性受限、功耗大、功能提升空间小、技术进步慢、价格昂贵、厂商锁定；

（3）网络和业务相互割裂，缺少协同，业务不了解网络的资源使用状况，网络无法适应业务动态的资源需求，造成资源不能共享、业务难以融合；

（4）成本居高不下，网络中存在大量不同厂商、不同功能的设备，在部署中需要实现多厂商设备的集成、互通、维护和升级，很难降低成本。

（二）新服务带来了降低网络建设与运维成本、提高网络资源利用效率、提升网络与业务部署速度的新需求。

未来将是数字化、全连接的世界，云计算、大数据、物联网、移动互联网、工业互联网以及高清视频、虚拟现实等将成为未来的热点业务，运营商面临流量/连接数快速增加、用户体验高要求和新业务不断涌现的需求。在流量方面，运营商网络的流量将会有爆炸式的增长，预计 2016 年全球将会产生高达 1.3 ZB 的网络流量(1ZB = 10^9TB)；在连接数方面，预计到 2020 年全球将有 2000 亿个物联网终端连入互联网。在用户体验方面，实时、按需定制、全时在线、自助服务以及社交分享成为用户的核心需求。

新服务带来了对网络敏捷、创新、安全、经济、开放的新需求，要求网络遵循开放标准体系，能够支撑业务多样化、弹性化，高效支持第三方业务创新，提供高安全性，支持自动化部署和运维。

1.2 NFV 带来的影响

NFV 和 SDN 所倡导的网络开放化、融合化、智能化和虚拟化的新理念，将驱动网络技术路线的深刻调整，推动网络建设、运维、业务创新和产业生态的根本性变革。

（一）NFV 将深刻改变基础网络运营商的网络建设、运维、业务创新和管理模式

在网络建设方面，NFV 利用通用化硬件构建统一的资源池，在大幅降低硬件成本的同时，还可以实现网络资源的动态按需分配，从而实现资源共享和资源利用率的显著提升。

在研发和运维方面，NFV 采用自动化集中管理模式，将推动硬件单元管理自动化、应用生命周期管理自动化，以及网络运维自动化。运维研发一体化（DevOps）成为可能。

在业务创新方面，基于 NFV 架构的网络中，业务部署只需申请云化资源（计算/存储/网络），加载软件即可，网络部署和业务创新变得更加简单。

在企业管理方面，为了应对 NFV 对运营商带来的一系列变化，基础网络运营商的组织关系、企业文化等都需要变革，运营商的企业文化在 NFV 引入之后将加速向软件文化转变。

（二）NFV 正在推动通信设备制造业的发展重心调整、产业升级与生态重构

NFV 拉长了整个通信产业链条，传统设备制造商面临严峻挑战。引入 NFV 以前，旧有产业链相对单一，核心成员主要包括设备制造商、芯片制造商等，而 NFV 引入后，新的产业链核心成员主要包括通用硬件设备制造商、芯片制造商、虚拟化软件提供商、网元功能软件提供商、管理设备提供商等。其中受冲击最大的是传统设备制造商，原本软硬件一体化设备销售模式被拆解为通用硬件、虚拟

化平台和网元功能软件三部分的销售模式，传统设备制造商除了在网元功能软件上具有强的技术壁垒外，在通用硬件和虚拟化平台软件方面将面临来自 IT 领域的强大竞争。

（三）NFV 将极大激发互联网企业与第三方业务服务商的业务创新活力

NFV 软件化、模块化实现方式可灵活的对网络能力进行定义、组合和管理，对外提供更为丰富的网络能力接口，促进第三方业务服务商与运营商的灵活对接，实现业务的快速集成和上线，激发第三方业务创新活力。

1.3 典型应用场景

NFV 将率先在五大应用场景落地，商用化发展路径进一步清晰。现阶段，虚拟化宽带远程接入服务器 BRAS（Broadband Remote Access Server）、虚拟化客户终端 CPE（Customer Premise Equipment）、虚拟化移动演进分组核心网 EPC（Evolved Packet Core）、虚拟化 IP 多媒体子系统 IMS（IP Multimedia Subsystem）以及虚拟化业务路由器 vSR（Virtual Service Router）是业界普遍认同的 NFV 率先应用领域。

（1）虚拟化 CPE

传统 CPE（客户驻地设备）在定制化家庭网关/企业网关应用中存在提供新业务能力差、升级周期长、三层配置复杂且故障率较高、网络演进困难等诸多问题。vCPE 是将传统 CPE 上的三层路由、网络翻译（NAT）、用户认证、组播控制、增值业务等功能上移到网络侧，客户端设备仅保留二层转发、L2TP 隧道封装及配置、基于二层信息的防火墙等功能。该方式简化了客户侧设备的配置难度，从而降低用户侧故障率，避免对网关频繁升级引起的故障以及硬件、软件成本增加，有利于网络演进。目前，vCPE 已在部分运营商网络中进行试点，产业链相对较为成熟，预计国内 2016~2017 年将会具备小规模商用的能力。

（2）虚拟化 BRAS

智能边缘是城域网的关键节点，是用户接入的终结点及基础服务的提供点。专业一体化设备在业务功能实现上与硬件强相关，给新业务部署带来很大难题。

vBRAS 是实现智能边缘虚拟化的代表技术，其以功能集为单元对设备控制平面进行重构，形成用户管理、组播、QoS 与路由等独立模块，每个模块可按需在虚拟机上部署，且可基于通用服务器的虚拟化资源提供能力实现灵活扩展。vBRAS 是当前业界认同的发展方向，国内运营商计划在 2016 年开展小规模的试点应用。

（3）虚拟化 EPC

传统 EPC 设备为专用的硬件设备（大多数为 ATCA 设备），设备通用性差导致研发、测试、入网和运维周期长，且成本难以下降。vEPC 通过通用硬件构建虚拟化的统一平台，支撑 EPC 网元（包括 ME、HSS、PCRF、SGW、PGW）的高效部署，从而降低建网和运维成本。引入虚拟化后，vEPC 网络架构、接口及协议依然遵循原有规范。目前，ETSI 组织了 vEPC 的 PoC 概念验证测试，相关运营商提出了相关的部署计划，初步预计国内运营商将在 2017 年前后小规模商用部署 vEPC 网络。

（4）虚拟化 IMS

vIMS 网络可以快速调配硬件资源池中的资源，可以快速搭建业务测试环境，可以对预上线的业务进行上线测试，将有助于运营商缩短业务上线时间，提升市场的竞争能力。预计国内运营商 2017 年将在 VoLTE 业务中小规模商用部署 vIMS 网络。

（5）虚拟化路由器 vSR

为了实现虚拟私有云与企业租户的内部网络互通，需要通过虚拟私有云网关在虚拟私有云与企业内部网络之间建立 VPN。虚拟路由器 vSR 运行在标准的服务器上，可提供路由、防火墙、虚拟专用网（VPN）、服务质量（QoS）等功能，帮助企业建立安全、统一、可扩展的智能分支，精简分支基础设施的数量和投入。目前，世界上主要的几大公有云服务器提供商，包括亚马逊、谷歌、微软，国内的阿里云、腾讯云等，都在虚拟私有云 VPC（Virtual Private Cloud）内部出口处，提供 VPN 网关业务。随着 VPC 应用的增加，vSR 的应用将越来越广泛。

2 NFV 产业现状和发展趋势

2.1 NFV 产业生态要素

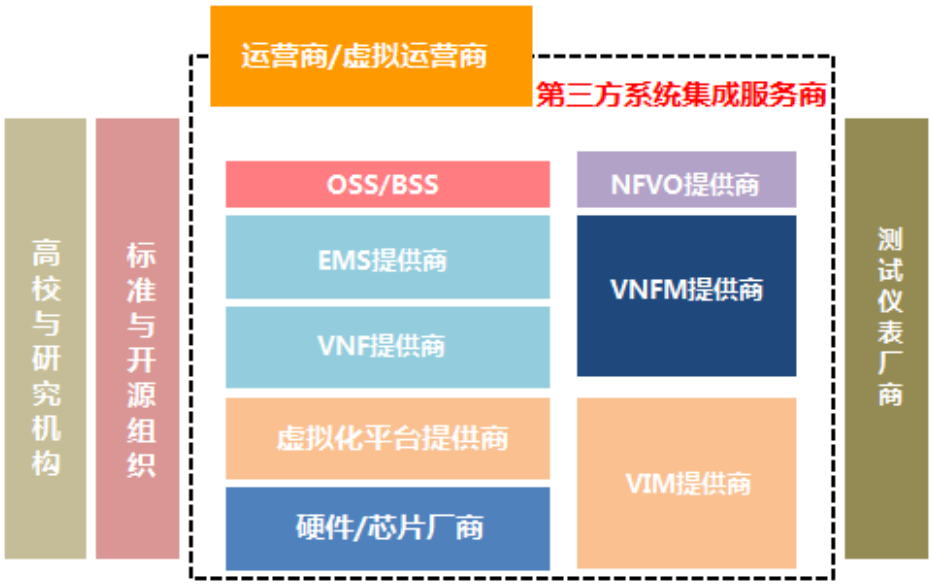

图1： NFV 产业生态要素

NFV 技术产业生态日益完善，产业重心加速调整。与传统软硬件封闭一体的架构相比，采用 NFV 技术将推动硬件和软件解耦，以及软件功能的分层解耦，进一步细化和拉长产业链环节，形成新的 NFV 产业生态要素（如图 1）。在这种新的产业生态体系下，产业重心将由硬向软调整，软件公司特别是第三方系统集成商的产业价值凸显。原先由单一厂商提供整套软硬件一体的系统，将分解成来自不同厂商的组件，如通用硬件、虚拟化平台、不同功能的 VNF 等。这一方面要求网络架构更加开放，接口统一并且标准化，另一方面第三方系统服务集成商将扮演更重要的角色，并要求具备更强的软件研发及系统集成能力。传统通信设备行业巨头需适应这种产业生态的变革，围绕自身平台积极打造产业生态系统，提供开放架构的产品及解决方案，集成源自不同服务提供商的组件。

2.2 趋势分析及市场预测

NFV 市场未来五年呈加速发展态势，产业规模效应初显。从 NFV 技术理念提出到 PoC 概念验证，到现场试验再到小规模商用试点，NFV 产业发展路径和目标

进一步清晰。大多数服务提供商都计划在未来 3~5 年随着产业成熟分场景逐步推进 NFV 的商用部署，期望实现业务灵活便捷部署，提升运维效率和降低投资成本等。根据联盟会员的调研，结合国际商业咨询机构的研究报告，可以将 NFV 产业发展划分为两个阶段。

（1）5 年内，以技术竞合、试点应用、理念培育为特征的发展初期阶段。这一阶段，重点是统一架构，标准化接口，推动符合电信级需求的产品成熟，逐步打破单厂商“独奏”的封闭架构，打造开放系统平台，推进多厂商的集成。运营商部分场景（如数据中心组网、数据中心互联、vCPE、vEPC 和 vIMS 等）从现场试验到小规模商用部署，奠定网络架构面向用户和业务的智能化转型基础，培育运维人员，积累运维经验。未来 5 年，SDN/NFV 的市场将会覆盖数据中心组网、数据中心互联、光网络、接入网、移动核心网、IMS 等领域，国内市场规模接近 2500 亿。

（2）5~10 年，以技术成熟、规模部署、运营变革为特征的融合应用阶段。这一阶段，开放网络目标架构更加清晰，平台和接口标准化程度更高；产品和解决方案日益成熟，不再是单厂商的“独奏”而是多厂商的“合唱”，合作共赢的产业生态初步形成；运营商网络将更大规模的部署 SDN/NFV 技术以期实现网络开放可编程、资源灵活调度、业务快速上线、运维高效的总体目标。

2.3 标准和开源项目进展

标准化组织在竞合中实现互补式发展，开源颠覆技术标准的研发模式。在 IT 领域，通过开源项目构建产业生态，以迭代开发模式加速产品应用并形成事实标准，影响技术和产品的发展方向。而传统电信领域的标准化更多是通过文稿制充分讨论后达成共识，再在产品中实现。两种不同开发模式的融合对传统电信领域的标准化流程产生了颠覆性的影响。

2.3.1 ETSI

主导 NFV 基础架构，推动 PoC 验证。2011 年 11 月，由运营商主导在 ETSI 成立 NFV ISG 工作组，成为推动 NFV 基础架构标准的主要国际标准组织之一，主要制定支持 NFV 硬件和软件的基础设施要求和架构规范，以及虚拟网络功能

的指南。目前已发布架构、需求、应用案例等多个技术文稿及一系列 PoC 文档。目前，该工作组的研究重点包括： IFA 组研究的 MANO 功能及接口、加速技术；REL 组研究的可靠性模型、故障检测及可靠性框架；TST 组研究的测试方法及开源组件等；EVE 组研究的 NFV 网络演进及生态体系建设；SEC 组研究的与安全相关的内容。2016 年，将重点研究 SDN 与 NFV 的结合、VNF 独立构建及管理的相关规范、基于 VNF 的端到端应用落地、无缝加载和混合部署，同时推进 VNF 产业化落地。

2.3.2 3GPP

面向移动核心网演进需求，聚焦网络资源切片。3GPP 中主要由 SA5 负责与 NFV 相关的标准化工作。SA5 侧重于制定虚拟化网络管理架构，云管理与网管协同，NFV 引入后的网络信息模型，以及故障、配置、性能、安全等管理流程，OSS/BSS 网管接口要求等方面的标准。预计 2016 年底将完成 NFV 网管标准化的制定工作。针对 NFV 的平台层，3GPP 主要还是依赖于 ETSI NFV ISG 和其他开源组织的工作。此外，3GPP 开始考虑基于 NFV/SDN 技术结合 5G 的发展来制定新一代的移动网络标准，重点研究如何利用 NFV 技术来提升 5G 网络的效率和灵活性。

2.3.3 IETF

完善 IP 协议体系，构建网络虚拟化能力。IETF 作为互联网领域的重要标准组织之一，也同步开展 NFV 相关标准化工作，涉及 2 个研究组和 9 个工作组，其中 NFV RG 主要关注固定和移动网络基础设施的虚拟化、基于虚拟化网络功能的新网络架构、家庭和企业网络环境的虚拟化、虚拟化和非虚拟化基础设施与服务的并存等问题研究；SDN RG 主要针对 SDN 模型进行定义和分类，网络描述语言（和相关的工具），抽象和接口，网络或节点功能的正确操作验证等。IETF 的 9 个工作组涉及 Internet、路由、传输、安全四个领域，包括 DMM、SFC、NVO3、I2RS、BESS、TEAS、VNFPOOL、IPPM、I2NSF 等，研究内容涵盖移动网络，数据中心内部网络虚拟化，用于网络安全控制和监控功能的新信息模型、

软件接口和数据模型等。其中 NVO3（Network Virtualization Overlays）主要关注架构、协议、数据面需求以及安全等；SFC（Service Function Chaining）重点关注在一个虚拟网络中流量的灵活调度并形成流经多个功能实体的业务链。

2.3.4 OPNFV

立足开源和集成，主导最佳实践。OPNFV 是 NFV 开放平台项目，由 AT&T、中国移动等电信运营商牵头发起的开源组织，于 2014 年 9 月 30 在 Linux 基金会下创建成立，该开源社区旨在提供运营商级的综合开源平台以加速新产品和服务的引入，实现由 ETSI 规定的 NFV 架构与接口，提供运营商级的高可靠、高性能、高可用的开源 NFV 平台。OPNFV 项目启动以来，已经得到 100 多个厂商关注，包括网络运营商、IT 厂商、设备制造商及解决方案提供商等。

2015 年 6 月，OPNFV 发布其第一个版本 Arno，这一版本将 Openstack、ODL、OVS、DPDK、KVM 等多个开源软件集成起来，旨在为 NFV 的实验室测试和 PoC 提供开源 NFV 平台。2016 年 3 月，OPNFV 发布第二个版本 Brahmaputra，提供包括 ODL、ONOS 和 Open Contrail 等多个 SDN 控制器的集成，超过 30 个项目贡献了规范和社区资源。

2.3.5 CCSA

立足国内需求，培育自主技术。中国通信标准化协会（CCSA）中与 NFV 技术相关的研究目前集中在 TC3、TC5 和 TC7。其中，TC3 成立软件化智能型通信网络（SVN）子工作组，聚焦 SDN /NFV 方面，重点研究核心网网元虚拟化一般性要求（虚拟化场景、架构、功能和接口等），主要针对网元虚拟化平台。截止到 2015 年底，共完成 13 个标准研究项目的立项。TC5 重点研究基于 SDN/NFV 演进的移动核心网网络需求场景、网络架构、网元功能和接口协议，以及基于新架构下的网络安全技术，共启动 6 项标准研究项目。TC7 作为网络管理与运营支撑工作组，重点研究引入 NFV 后网络管理相关的技术，启动 2 个标准研究项目。后续 CCSA 标准化研究重点将包括 VNF 软件架构、NFV 管理及编排、性能及可伸缩性、可靠性以及安全等方面。

2.4 NFV 产品及方案成熟度

2015 年，中国厂商加快战略布局，NFV 产品与解决方案日益成熟。中国厂商加快战略调整和产品研发，一方面不断提升自身技术创新与产业化能力，另一方面加快了与国际国内市场需求的紧密衔接，对于 NFV 技术与产业发展方向的掌控力进一步增强。

表 1：国内主要厂商的 NFV 发展战略

设备厂商	NFV 产业发展战略观点	未来 3-5 年的计划	典型应用
华为	以 SoftCOM 解决方案为总体框架，以分布式云数据中心为下一代电信级业务网络的核心，实现传统网络的分层解耦、功能虚拟化以及资源的弹性调度，实现运营商在网络、架构、业务以及运营上的快速转型，满足实时、按需定制、全在线、自助服务和社交分享的用户体验需求。	从技术可行性，商业价值，平滑演进，生命周期等多方面综合考虑，按以下步骤逐步实施 NFV 演进： 1.2016-2017 年，从低技术复杂度和新的的价值业务（如 MVNO,物联网 M2M/IoT core/Gi LAN 业务链等）开始引入，通过叠加网方式部署 NFV。 2.2017-2018 年，现网改造一般从控制面（IMS Core，SGSN/MME,PCRF）开始再到用户面(GGSN/SGW/PGW,SBC,BRAS，CPE 等)，通过混合组网方式（如 Pool 方式），实现现网和 NFV 网络共存共管，逐步平滑演进。 3.2018-2020 年，网络改造从集中网络向分布式网路演进，实现控制面（IMS core,HSS,PCRF,MME/SGSN 等）集中部署集中运维，用户面（GGSN/SGW/PGW,SBC,BRAS,CPE 等）分布式部署提升业务体验。	SoftCOM 解决方案包含 CloudOpera、Digital inCloud、CloudCore、CloudEdge、CloudBB、CloudDSL/OLT 等六类 ICT 基础云设施的 NFV 典型应用。 **CloudOpera**：定位是运营商下一代的运营系统； **Digital inCloud**：是运营商面向全球提供各种业务的开放云服务设施； **CloudCore**：是基于 NFV 和 SDN 重构核心网，包含各种可弹性扩展、灵活部署的核心网虚拟功能单元，以开放的方式提供敏捷的服务体验。 **CloudEdge**：在开放的 ICT 云设施上，使用 NFV/SDN 重构运营商的网络边缘，提供了虚拟化 EPC，虚拟化 BRAS,虚拟化 CPE 等。 **CloudDSL/OLT**：基于 NFV/SDN 重构的开放接入云设施，实现固网 DSL 以及 OLT 等有线方式的接入。 **CloudBB**：使用 NFV/SDN 重构运营商的无线接入网络，以开放的 ICT 云设施实现无线侧的业务接入。
中兴	□ 以 ElasticNet 弹性网络架构为总体目标，深度融合 NFV/SDN 技术，实现网络重构。	NFV 发展分四个阶段（IaaS 资源池化降低成本、PaaS 能力构建、网络开放可编程、全面开放及经营服务创新）：（1）推出全系列网元虚拟化	中兴通讯NFV领域的解决方案 Elastic Cloud Service 包括了 Elastic Cloud UniCore(核心网系列)，Elastic Cloud Uni-RAN(无线 RAN)，Elastic

设备厂商	NFV 产业发展战略观点	未来 3-5 年的计划	典型应用
	坚持标准化、开源、开放，在通用硬件可靠性基础上，通过多种优化手段和解决方案，打造高可靠的电信云网络，提升用户的体验。	产品，构建云化 IaaS 平台，资源池化降低成本，满足基本商用要求。 （2）网络核心及业务平滑演进，具备 PaaS 能力。 （3）增强组件化能力，网络切片，实现网络开放可编程，满足面向 5G 的网络与架构需求。 （4）实现网络全面开放和标准组件化，满足 5G 网络和 ElasticNet 目标架构要求。	Cloud Bearing（含 vCPE, vBRAS）和 IVAS（业务系列）等系列子方案。Elastic Cloud Platform 解决方案则包括多厂家计算和存储网络产品及其虚拟化组件的集成。在编排领域，提供 Elasitc Conductor 解决方案。
上海贝尔	上海贝尔将以 CloudBand NFV 云平台产品为主线，协同 Nuage VSP 虚拟网络业务产品，配合 Motive Dynamic Operations 产品，支持端到端的网络业务切片的分配与管理，支持多种 5G 业务，实现无线网络资源的虚拟化，提供完整开放的 NFV 运营蓝图架构，支持自动部署优化构建任意规模网络下虚拟化网络功能，实现网络服务的高效、可靠、动态、精益运营方案。	夯实 NFV 管理面：优化 CloudBand 功能架构，进一步提升系统的可靠性、安全性和互联互通能力，优化 SDN 技术集成及网络服务自动化功能的专业设计和验证。 2. 完善 NFV 运营面：优化 Motive Dynamic Operations 功能架构，进一步优化业务流程编排、操作和管理，推动标准的端到端服务流程和服务等级管理信息，支持扩展无缝虚拟网络功能业务流程编排模型。 3. 梯度迁移、推进 VNF 业务部署： Ÿ 2016 年，优先实现 vIMS、vSBC、vCPE 等应用的商用部署，推动 vEPC 规模商用部署和 vBNG、vRAN 小规模试商用，积累 NFV 部署与运维经验； Ÿ 2017 年，实现 vBNG、vRAN 规模商用部署，从而成为宽带接入的补充方式；	NFV 领域的解决方案包括： CloudBand：NFV 基础架构平台方案，通过提供运营商 PAAS 能力，提供虚拟网络功能自动部署、弹性伸缩和自治愈功能，满足运营商业务需要。 NuageVSP（虚拟网络业务平台）：支持网络自动化和抽象的 SDN 技术，提供完整的多租户云网络服务解决方案。 Motive Dynamic Operations 方案：增强 NFV 功能的 OSS/BSS 产品，实现零接触的业务流程编排、操作和管理，实现标准的端到端的服务流程和服务等级管理信息。 面向 NFV 的网络功能方案：涵盖接入、网络、应用等多组方案，如：vIMS、vEPC、vMG、vRAN、vPPCRF/DRA、vBNG 等。 典型应用场景包括：连续广域覆盖、超密集高容量热点组网、低功耗大连接 IoT 应用、低时延高可靠应用等
华三	NFV 利用传统的虚拟化技术，让网络功能和专用硬件解耦，实现了网络功能更灵活的部署，加速新业务的提供。NFV 解决专用硬件带来的存放空间、电力消耗问题，降低资本投入。同时，专用硬件生命周期短，NFV 使用标准	根据 NFV 目前特点，按照下面 3 个阶段点，逐步实现 NFV 在云计算和城域网的可持续性发展： （1）完成物理设备的虚拟化，实现业务功能全覆盖，支持设备级冗余备份 （2）实现 VXLAN 网络下的流量灵活调度以及资源池化。业务能自动化部署以及监	VSR 广泛应用于公有云的 VPC 网关，连接企业内部网络和 VPC 中企业资源，提供 IPsec、GRE 等 VPN 业务。 vBRAS 结合 VxLAN，已经应用于国内主要运营商。配合城域网扁平化架构演进，在提供传统 BRAS 业务基础上，在一个 POP 点中，融合 vCPE、vFW、vDPI 等网络功能，组成城域网

设备厂商	NFV 产业发展战略观点	未来 3-5 年的计划	典型应用
	COTS 硬件，操作维护人员也不需要熟悉、维护专用硬件，只需专注业务本身，运营成本也得到降低。网络功能虚拟化后，网络功能可以像云计算一样，按需提供服务（NaaS），例如：按需提供 VPN、网络速度智能提速等。	控。对于当前最适合部署 NFV 的大并发、小吞吐的场景，加速实现商用。 （3）实现资源池的动态调度，网络开放接口，打造一个开放的生态链。	的 vPOP 资源池。 vCPE 应用于运营商和企业用户，把用户终端的功能上收到统一的部署点集中控制。 vFW 应用于数据中心，提供专业的防火墙体验，保护数据中心不受到外部的入侵，保障数据安全。 vLB 提供数据中内部租户资源访问的负载均衡服务，保证租户业务的响应速度，提高业务的可靠性。 vAC 主要应用于本地转发的场景下，提供高容量的 AP 接入，适用于企业网、商贸市场等场合。

2.5 运营商 NFV 部署规划

2015 年，传统电信运营商加速战略转型，NFV 成为转型的重要技术支撑。电信业务和互联网业务的相互渗透与融合，电信运营商开始迈入信息服务转型的关键发展阶段，由此带来网络基础架构的深刻变革，构建一张“资源可全局调度、能力可全面开放、容量可弹性伸缩、架构可灵活调整”的新一代网络成为运营商网络演进发展的重要方向。国内三大运营商纷纷发布转型战略（如电信 B2I 战略、移动 NovoNet 2020 愿景和联通 CUBE-NET2.0 新一代网络架构等），寄期望于采用 SDN/NFV 技术推动网络架构的革命性变革。

在 NFV 领域，国内运营商积极参与国际标准/开源组织的标准化工作，相继成立开放实验室开展 NFV 相关专业的功能、性能和互通性测试验证工作，促进 NFV 生态系统构建，推动产业发展成熟。

在 NFV 商用化部署方面，将遵循以业务为驱动，从行业应用到公众应用，先局部后整体，先控制面后用户面的逐步演进、迭代升级的思路，新建网络在满足性能的前提下优先考虑以 NFV 形式部署。NFV 商用目标方案是硬件、虚拟资源层、上层网元功能三层全部解耦，但在商用初期，鉴于虚拟资源层和上层网元功

能解耦难度较大，可采用软硬件两层解耦的模式作为过渡。

表 2：国内运营商的 NFV 发展战略

运营商	NFV 产业发展战略观点	未来 3-5 年的计划	典型应用
电信	NFV 对网络架构演进产生深远的影响，与 SDN 配合，推动网络架构向“简洁、敏捷、开放、集约”的方向演进，提供“可视、随选、自管”的网络能力。	开展 NFV 实验室测试，推动分层解耦;开展 EPC 虚拟化、BRAS 虚拟化等现场实验，积累部署经验后，逐步推广 NFV 商用部署；虚拟化网元统一部署到 DC，推动 CO 向 DC 转型	EPC 虚拟化、IMS 虚拟化、BRAS 虚拟化、企业网关虚拟化等
移动	NFV 给中国移动带来的价值分为开源与节流两部分。开源方面，通过软硬件分离，加快了业务上线时间，增加了网络的灵活性，加速了网络的快速部署。节流方面，NFV 通过引入通用服务器，降低了硬件成本，并可以实现跨系统间的资源共享。	根据市场发展需求，在成熟性相对较高的前提下，优先考虑需要大规模新建的业务网络单元或大规模退网替换的业务网络单元，在时间进度上，优先迁徙虚拟化难度较低的网元，如信令面网元，再考虑虚拟化难度较大的网元，如用户面网元 SAE-GW 等。	主要有三大应用场景：（1）VoLTE/vIMS，VoLTE 面临大规模建设，使用 NFV 技术可以实现快速部署上线；（2）万物互联，随着物联网的发展，依托专用 EPC 实现虚拟化，满足快速部署和灵活应用的需求，中后期实现大网 EPC 的虚拟化；（3）固网接入，以 vCPE、vBRAS 为抓手，推动固网接入的虚拟化和灵活部署。
联通	联通提出了面向未来网络演进需求的新一代网络架构——CUBE-Net 2.0，利用 SDN/NFV 技术对网络进行重构和升级。通过引入 NFV 技术增强网络服务能力和降低网络运营成本，构建面向网络云化的集约型网络，提供网络弹性高效、灵活敏捷特性，真正意义上实现“网络及服务”的目标。	未来 3~5 年内联通将统筹考虑 SDN/NFV 网络发展目标与演进策略，技术研究与现网部署同步推进，加快 NFV 技术成熟，在核心网、业务链、固网接入、数据网等领域优先考虑 NFV 解决方案，升级传统服务产品。各专业从网络实际情况出发，以业务为驱动逐步引入 NFV 理念，走开源之路，聚合开发合作伙伴，研发 NFV 核心软件，推动网络向智能化、集约化方向发展。	核心网：以 VoLTE 业务和新兴物联网应用为切入点，在统一的云化平台下集成 vIMS/vEPC/业务链功能，提供完整的核心网云化解决方案，进行控制面集中部署，构建统一的资源管理系统。 固网接入：结合接入网络业务特性，满足企业网关基本功能和用户需求，体现 vCPE 功能简单，故障率低，软硬件分离，业务功能灵活部署等优点，实现容量弹性伸缩，业务软件化，新业务上线快等特点。 数据网：基于 SDN/NFV 技术重构 BRAS，实现 vBRAS 池组化及资源均衡，加速 vBRAS 业务创新，并通过 SDN 控制器统一调度 vBRAS 资源，达到资源均衡，最终实现城域网的 SDN/NFV。

3 NFV 关键技术问题和挑战

六大关键技术问题勾勒出 NFV 技术产业未来发展方向与重点。VNF 生命周期管理、性能、可靠性、安全、集成部署、开放互联是当前 NFV 技术发展的核心问题，也是未来 5 年牵引 NFV 技术产业发展的重要方向。

3.1 VNF 生命周期管理

NFV 要实现硬件资源与软件功能的解耦，需要通过标准的接口、通用的信息模型以及信息模型与数据模型之间的映射来实现，同时还需要一套新的管理和编排功能系统。NFV 引入了管理和编排功能 MANO，主要用于提供虚拟化资源、虚拟化网络功能和网络业务的统一管理，包含三类功能模块：NFV 编排器（NFVO）、VNF 管理器（VNFM）和虚拟化基础设施管理器（VIM）。

VNF 生命周期管理是 NFV 架构下实现自动化运维的关键环节，由 MANO 和 EMS 协同完成，包括 VNF 的实例化、终结、查询、扩容/缩容、自愈等功能，实现了自动化资源编排、智能部署编排、弹性扩缩容决策等。在具体部署时需根据业务的规格需求和基础设施的硬件属性完成自动化资源编排，根据亲和性/反亲和性策略、基础设施资源的负荷/可用状况等关键要素完成智能部署编排，基于网元的 CPU 占用率、用户容量门限、带宽使用率等关键要素进行扩缩容决策。上述算法的参考要素和具体实现需要业界共同研究和攻关。

3.2 性能

硬件通用化、网元功能的软件化导致网络 I/O 能力难以匹配电信网络的需求，计算能力难以满足特殊功能（如加解密、编解码、深度报文解析等）的需求。另一方面网络功能虚拟化引入中间件带来一定性能损耗。如何降低软件的开销并通过引入软硬件加速技术满足电信网络高速转发、密集计算的性能需求成为 NFV 需要解决的挑战之一。

3.3 可靠性

传统的电信网络设备需要 99.999%的高可靠性，而采用虚拟化技术的通用设备目前暂时还没达到该要求（一般 COTS 设备可靠性只能达到 99.9%）。为了满足电信级设备高可靠性的要求，NFV 的组件需在多个方面提供与传统电信设备相当的性能，包括故障率、检测时间、恢复时间以及检测和恢复的成功率。

引入 NFV 之后，原有软硬一体化设备分成了三层，同时还引入 MANO，而 MANO 也深度介入网元的自动伸缩等流程中，对整个网元的可靠性带来了深刻的影响。为了满足电信级设备 5 个 9 的高可靠性，硬件资源层、虚拟资源层、VNF 和 MANO 每层如何增强、三层如何协同、VNF 与 MANO 如何配合等都会影响到整个系统的可靠性。这需要建立一套完整的可靠性体系并对三层如何协同提出明确的要求。

3.4 安全

相比传统电信设备，软硬件分离的特点以及虚拟化网络的开放性给网络带来了新的潜在安全问题：一是引入新的高危区域——虚拟化管理层；二是弹性、虚拟网络使安全边界模糊，安全策略难于随网络调整而实时、动态迁移；三是用户失去对资源的完全控制以及多租户共享计算资源，带来的数据泄漏与攻击风险。

在 NFV 环境中，可能存在安全风险的关键组件包括 VNF 组件实例、绑定到 VNF 组件实例的本地网络资源、远程设备上对本地 VNF 组件实例的参考、VNF 组件实例占用的本地、远程以及交换存储等。在发生安全事故的情况下，如何保证这些关键组件所涉及的硬件、内存不被非法访问，如何保证 VNF 上应用的现有授权不被改变，本地和远程资源彻底清除崩溃的 VNF 资源及授权不被滥用，是 NFV 安全面临的关键技术挑战。

3.5 集成部署

NFV 本身解决的是业务网络的自动部署问题，从架构看也是一个巨大的 ICT 系统集成工程，包括 NFVI 的集成、VNF 的集成和业务网络的集成，涉及的系统、厂商、地域、接口都非常多。

引入 NFV 后，电信网络从传统一个厂商完成的软硬件集成转换为 NFV 下

多个厂商的软硬件集成，复杂度大大提升。现阶段，NFV 相关接口的标准化进度不一，部分接口将直接采用开源软件，部分 API 难以完全标准化。此外，开源软件和厂商定制化软件解决方案所采用的私有协议和接口，都将成为 NFV 系统集成和工程联调面临的挑战。

3.6 开放互联

NFV 通过标准 API 接口向第三方应用、中间软件供应商等开放电信网络能力，可以通过统一的基础服务平台快速集成第三方业务。当前，如何规范开放的 API 编程接口，如何基于敏捷开发方法构建统一的基础服务平台，从而动态适配不同的第三方应用是 NFV 发展面临的挑战。

4 电信运营商对 NFV 的技术需求

4.1 数据中心设计建设需求

4.1.1 分级原则

电信业务数据中心的建设需要根据用户和业务发展分布的具体情况来规划，可分为全国（中心/核心）、省级（区域）、接入三级数据中心。

全国（中心/核心）数据中心：主要承载集约化运营业务，如全国范围内的集中性业务 RCS(融合通信)等，主要涉及信令控制方面的网元。

省级（区域）数据中心：以承载有属地化需求的业务和需要区域集中流量的网元，如 IMS 的控制面网元、SAE（系统架构演进）的 MME 和 SAE-GW 网元等。

接入数据中心：部署对转发极度敏感的网元（时延要求极高），如用户面网元和接入网设备，可满足大量业务的本地分流和实施业务就近接入，满足用户业务的体验诉求。

4.1.2 覆盖范围

全国（中心/核心）数据中心：按照国家或者洲一级的区域进行划分，规划

一个或者多个，覆盖全球或全国；

省级（区域）数据中心：按照省一级的区域划分，也可以把多个相邻的省份划分到一个大区数据中心里面，覆盖半径在千公里级别；

接入数据中心：按照市县一级的区域根据业务的收敛半径划分，因业务需求不同覆盖半径可以在百公里级或十公里级别。

4.1.3 建设要求

4.1.3.1 机房

对于大中型数据中心（DC）机房，如全国（中心/核心）DC、省级（区域）DC、大中型本地 DC，侧重于机房的建设与维护成本，尤其需关注长期运维费用的降低。在建设方面，需重点考虑靠近资源、设备低功耗、高密度与集中管理等因素，同时机房选址还需要考虑容灾备份对承载网的要求，如承载网的网络拓扑、网络质量，不同 DC 之间交互信息的带宽和时延等。

对于小型数据中心（DC）机房，如小型本地 DC、边缘 DC，则更关注于机房改造成本，尤其是原有 PSTN 机房在改造过程中面临的电力、空调等问题。

4.1.3.2 设备

数据中心内采购的设备（包括计算、存储、网络等）必须符合电信级应用环境的要求，对于构建 NFV 基础设施的设备可靠性要求更高一些。

4.1.3.3 业务

对于电信业务，建议按管理域、业务域和 DMZ（Demilitarized Zone，不可信的外部网络和可信的内部网络之间的缓冲区）域三类功能域进行规划。

- 管理域主机部署管理软件及网络业务的 EMS/VNFM 软件等；
- 业务域主机部署网络业务的核心业务网元软件等；
- DMZ 域主机部署网络业务对外直接提供接入或访问服务的网元软件，如 IPsec VPN 网关。

在业务域内，不同的业务可以划分不同的 VPC（Virtual Private Cloud，虚拟

私有云），实现不同业务的逻辑资源隔离，避免不同业务之间相互影响或资源抢占。

4.2 电信业务对 NFV 的要求

4.2.1 计算处理能力

与传统电信设备相比，NFV 在物理硬件之上增加了虚拟化层，这会导致物理资源的损耗，需要采用性能提升技术来降低该损耗的影响。

- CPU 处理能力

多虚拟机对物理 CPU 资源的竞争和抢占，导致虚拟机的性能降低，尤其是转发面网元，在业务处理过程中，对表项的操作（增删改）非常密集。建议支持巨页内存，以减少内存访问带来的性能损耗。

- 内存访问性能

内存的访问性能将会直接影响到业务系统的处理性能，因此需要采用必要的机制来保证内存访问性能，（1）有效提升页表查询时命中虚拟寻址缓存的页表；（2）NFVI 应当支持预留连续内存资源池，以减少或消除虚拟机内存碎片；（3）NFVI 需支持将虚拟机的 CPU 和内存部署在同一个 NUMA(Non Uniform Memory Access，非一致性内存访问)内，从而降低内存访问的时延[1]。

- 内核处理实时性

传统的操作系统中，进程都是按照时间片来执行，一个具有更高优先级的用户任务也必须等待前一进程时间片到期后才能被执行。而电信网元要求应用进程的响应时间是确定的，可以通过对进程分配不同的优先级来指定或调整响应时间。因此，NFVI 应当能够支持内核实时性扩展技术，充分利用资源之间的亲和性关系实现计算处理能力的高效发挥，满足电信业务的实时性要求，重点可以考虑虚拟机 vCPU 核绑定、虚拟机 vCPU 超线程、虚拟机 OVS、虚拟机组互斥、虚拟

[1] NUMA 模式的 COTS 服务器通常具有多个 NUMA 节点，每个 NUMA 节点由多个物理 CPU 组成，且具有独立的本地内存、I/O 槽口等。NUMA 节点之间通过互联模块进行连接和信息交互，每个 CPU 均可以访问整个系统的内存，但 CPU 访问本地内存的速度远高于访问远程内存(系统内其它 NUMA 节点的内存)的速度。

机主机组亲和性等。

4.2.2 可靠性

NFV 的可靠性需要 NFVI 逐层支撑保证，并通过垂直集成增强整系统的可靠性。NFVI 通常通过以下几方面技术保证电信级可靠性。

- 故障检测

电信业务的故障检测时间一般要求在秒级，要求 NFVI 同样支持秒级的故障检测，支持在检测硬件故障后实现快速无缝切换受影响的虚拟机业务到状态正常的硬件，减少对电信业务的影响。

- 故障定界

在 NFV 软硬件解耦的架构下，电信业务软件需要结合 NFVI 基础设施平台信息进行故障定界。NFVI 需要具备定界 COTS 硬件或自身软件故障的能力，同时对受影响的虚拟化资源信息进行上报，以便电信业务软件统一运维管理。

- 虚拟机智能化部署

NFVI 应当支持智能化的虚拟机部署，满足电信业务无单点故障的需求，并支持电信业务软件的跨站点部署，可跨站点管理不同数据中心的物理资源,满足地理容灾要求。

- 虚拟机迁移

当物理机出现故障时，NFV 应支持虚拟机可快速迁移和恢复，至少应支持跨主机或跨机架的迁移。

- 冗余备份

NFVI 应具备硬件和软件的冗余备份能力。硬件方面，支持冗余电源接入、冗余网卡连接、冗余散热风扇等高可用性部件，避免由电源及网络接入等单点故障影响业务功能。交换模块需要支持冗余设计，任何一个部件故障不影响带宽和业务性能。软件方面，应支持虚拟机的快速恢复，对于管理软件需要实现组件级的备份。

- 硬件高可靠

服务器内存支持高级 ECC（Error Checking and Correcting，错误检查和

纠正）内存保护技术或内存镜像保护；磁盘支持 RAID 技术，保证磁盘系统的高可靠性，提高持续工作而不发生故障的能力；网络端口支持聚合或故障切换功能，满足系统对于网络可靠性的需求。

4.2.3 转发性能

电信业务存在高吞吐和实时性要求，尤其是针对需要进行编解码转换、协议转换的数据面网元，采用虚拟化技术基于通用硬件和虚拟层软件通常会存在性能瓶颈，无法满足数据面高吞吐量要求，为了在 NFVI 上减少报文调度次数，降低网络转发延迟，提高网络吞吐量，需要提供转发性能加速机制。现有的加速机制包括：

（1）Single root I/O virtualization (SR-IOV)：一种基于硬件的虚拟化通道技术。虚拟机直接连接到物理网卡上，获得等同于物理网卡的 I/O 性能和低时延，且多个虚拟机之间高效共享物理网卡。

（2）Data Plane Developers Kit (DPDK)：一种内核旁路机制。为了提高包处理的速度，允许虚拟交换机旁路内核并直接与兼容的网卡通信。

（3）超线程技术。要求 COTS 硬件支持超线程技术提高 CPU 的并发处理数，使得单个处理器可使用线程级并行计算，减少 CPU 的闲置时间。

（4）硬件加速机制。NFV 技术采用通用硬件来承载电信业务，对于某些特殊业务采用上述（1）至（3）的软件加速方式而不是专有硬件处理，会导致转发性能的显著下降，因此需要引入硬件加速技术来解决相关业务的转发性能问题。目前业界主流的专用硬件加速技术包括通用加速资源池、专用 PCI 加速卡或 CPU 内置加速芯片等，但具体采用何种专用硬件加速技术仍有待进一步研究评估。

4.2.4 组网

早期数据中心主要满足外部对数据中心的访问，因此流量以南北向为主。电信业务多为分布式部署，网元间的流量较多，随着 NFV 的部署，电信业务对数据中心的流量模型将产生巨大的冲击，数据中心流量将由南北向为主转变为东西向为主。组网上需要考虑如何保障电信业务的接入质量。

对于 NFV 而言，NFVI 需要加强接入质量的保障，确保用户在访问数据中心时带宽能够得到保证，因此首先要求 COTS 硬件提供足够数量的 40GE/100GE 以太网接口，并支持 JumboFrame 提升报文传输的效率，从而保障电信业务的南北向流量的 QoS。

电信业务的东西向流量在数据中心的 VNF 之间交互转发，将导致数据中心内的东西向流量相比南北向流量成倍增长。NFV 的内部组网同样要求大带宽的 QoS 保障，而数据中心的虚拟机之间一般采用二层组网以支持动态迁移，因此这将对承载数据中心内东西向流交换的交换机性能提出要求，其需要支持高达 40GE~400GE 每服务器节点的交换组网能力。

4.2.5 安全

NFVI 基础设施平台资源的安全，主要涉及到电信业务运行的物理硬件资源、虚拟化平台和网络的安全可靠。

对于物理硬件资源，需要保证 COTS 硬件的安全可信。COTS 硬件需要提供基于硬件芯片的可信环境，以便于虚拟层及业务软件层可基于硬件可信环境构筑信任根，实现安全启动和安全存储。目前通过使用可信赖的平台模块（Trusted Platform Module，TPM）来完成加密、签名、认证、密钥生成等功能。对于接口的访问，COTS 硬件需要进行访问控制和认证鉴权，防止非法访问。

对于虚拟化平台资源，要求提供租户、虚拟机以及不同业务的安全隔离，避免虚拟机之间的数据窃取或恶意攻击。对于虚拟化平台及其所管理的虚拟资源的访问，要求提供访问控制和认证鉴权，防止非法访问对系统的影响。在存储方面，对物理存储实体的直接访问具备禁止或限制的能力，提供虚拟存储数据清除、虚拟存储数据审计、虚拟存储数据访问控制和冗余备份功能；在计算方面，能利用加密算法协处理器，高效实现 VNF 内部的机密性和完整性保护。

对于网络资源，应具备对虚拟机的隔离和访问控制能力，虚拟机之间需要授权和鉴权后才能建立通信连接。通过在线的深度报文检测、虚拟防火墙技术以及基于 Netflow 采集的流量溯源与关联分析等综合技术，可以建立基本的 NFV 网络安全防护体系，能够支持抵御畸形报文攻击、DoS 攻击和仿冒攻击等。

4.2.6 环境适应性

国际标准组织对电信设备的环境适应性有正式的规定，例如：欧洲的 EN3000019 和 EN300318 系列要求、北美的 NEBS 系列要求等。电信业务的设备要求普遍高于目前 COTS 设备的工作指标。为了使 COTS 设备系统稳定可靠的运行，减少机器故障对电信业务的影响，COTS 设备需满足一系列的环境因素要求，包括工作的温度、湿度、散热方式、高度、供电模式等需求。

4.2.7 能耗

NFVI 中通用服务器功耗相较于传统电信设备功耗更大，需要提供相应的手段和措施尽量降低能耗，减少 NFVI 投资和运维管理费用，通常可以采用以下几种技术和措施。

- 功耗测量

支持连续测量系统功耗，并应能够根据系统负载控制 CPU 功耗状态，且不会造成性能损失。支持带外功耗实时监控能力，支撑主动策略型节能管理。

- 电源封顶技术

可以通过服务器的动态配置或功率封顶，有效地对每一台服务器能耗进行准确控制。

- 功耗控制

支持平台功耗控制，通过 IPMI 标准协议，将单台、多台服务系统或整个弹性计算平台功耗设置为限定目标功率，并能在该功耗限定下达到最佳性能。

- 功耗报警

支持功耗阀值警报，通过动态监控限定目标的功耗来监控平台的功耗，当无法维持限定目标功耗值时，系统能向管理平台发送警报。

5 传统电信网络向 NFV 的演进策略

5.1 NFV 部署策略

NFV 的部署将是一个渐进的过程，传统网络和 NFV 长期共存。在全网部署 NFV 前，运营商现网设备不可能全部立刻退网，因此 NFV 的部署将是一个渐进的长期过程。NFV 的部署范围将覆盖核心网、承载网、接入网等全领域，其典型部署场景包括：

- 基于 NFV 提供新业务，如基于蜂窝的窄带物联网 NB-IOT（Narrow Band Internet of Things）、Gi-LAN 等。通过部署 VNF 来提供新业务具有部署周期短、对现网影响小、业务创新快的优势。如图 2 是部署 vEPC 支持 NB-IOT 的示例。

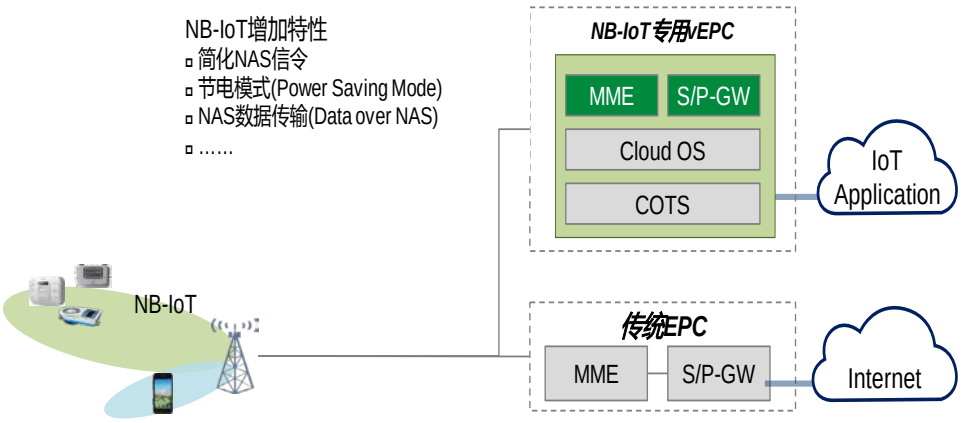

图2： NB-IoT 专用核心网示例

上述方案也能够基于传统架构实现，但存在组网复杂、业务上线慢、缺乏灵活性等问题。而利用 NFV 技术，可以实现业务功能快速上线和自动编排。

- 行业或企业应用，如公共安全(Pubilic Safety)，BYOD 等。这些应用对网络部署和功能有特殊要求，如公共安全一般要求资源隔离、安全增强和高优先级服务等，可以利用 NFV 的多实例/切片技术方便的为这些应用提供服务。

- 网络扩容，如通过 vEPC 扩容。面对快速的业务增长，运营商通过部署 VNF 来分担现网 PNF（Physical Network Funcation，物理网络功能）的负荷，同时逐步淘汰现网设备，实现网络的平滑演进。

- 网络升级替换。传统设备因为折旧或需要进行硬件替换时，通过引入

NFV 设备，可以加快未来网络的升级部署速度。

目前 NFV 还未完全成熟商用，各 VNF（Virtual Network Funcation，虚拟网络功能）的复杂度和技术要求也不相同，所以部署中要考虑各 VNF 的成熟度。偏重计算和存储类的 VNF（如 CSCF、AS、PCRF、HSS 等）相对成熟，偏重转发和媒体处理的 VNF（如 S/P-GW、SBC）成熟度低。所以通常的部署节奏是先业务(如 AS、RCS)和控制面网元(如 IMS、MME)，再转发和媒体层(如 EPC-GW、SBC)。图 3 是 VNF 成熟度的相对比较。

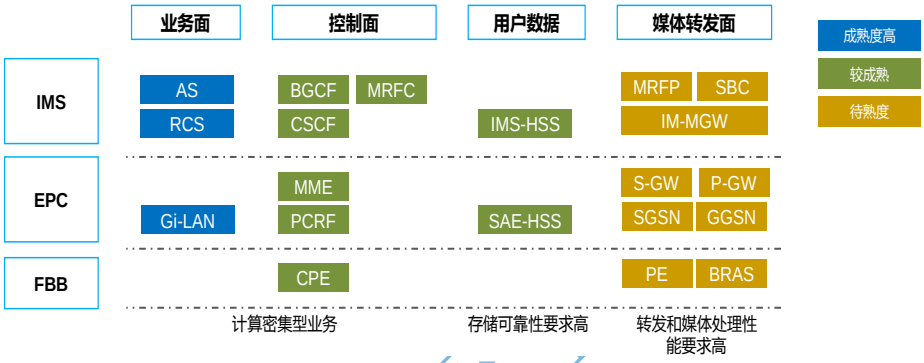

图3： 网元虚拟化成熟度比较

从业务和设备的生命周期角度考虑，一般新业务或成长期业务（如 Gi-LAN）涉及的功能优先虚拟化，衰退期业务(如 CS)涉及的功能虚拟化要慎重；存量设备也存在替换周期，一般即将退网设备优先考虑虚拟化。

总之，NFV 的部署一般原则是“需求导向，业务驱动，效率优先，从易到难”循序渐进的过程。

5.2 传统网络与 NFV 协调部署

5.2.1 PNF 和 VNF 共存部署场景

虚拟网络功能（VNF）和物理网络功能（PNF）共存部署的总体目标是：充分利用现网投资，最小化网络风险，实现业务平滑迁移。目前存在两种典型的共存部署场景：（1）在传统网络基础上采用 NFV 开展新业务；（2）对传统网络采用 NFV 扩容现有业务。

场景一：在传统网络基础上采用 NFV 开展新业务。

在现网基础上新建设 VNF，并由 VNF 提供新业务或服务特定用户群(如 MVNO 用户)。这种方式对现有网络不产生影响，资源和管理面独立，但业务互通，具有部署快、风险小特点，比较适合由 NFV 提供新业务或小规模商用场景。图 4 是在现有传统 EPC 网络基础上开展 Gi-LAN 的示例，运营商有两种选择，采用传统物理设备部署 Gi-LAN 业务，或者采用 NFV 部署 Gi-LAN 业务。

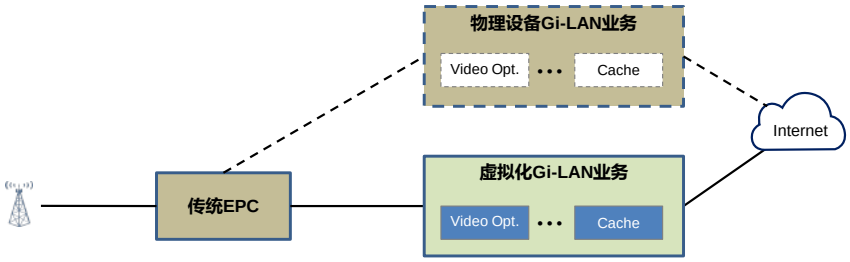

图4： NFV 部署新业务，加速新业务上线

场景二 ：对传统网络采用 NFV 扩容现有业务。

现网 PNF 池内增加 VNF 网元。图 5 是 vEPC 和现网 EPC 混合池部署示例。这种组网具有如下的优势：

（1）异构平台组池，互为备份，可靠性更高，可以避免全网故障的风险。

（2)用户和业务平滑迁移至 VNF，迁移过程可以随时终止和回退，最小化网络割接风险。

（3）充分利旧现网 PNF，保护现有投资，并可逐步淘汰 PNF，实现网络平滑演进。

（4）利用 VNF 实现池的弹性伸缩，当池内业务量增加时，VNF 自动扩容吸收话务，应对业务突发和信令风暴。

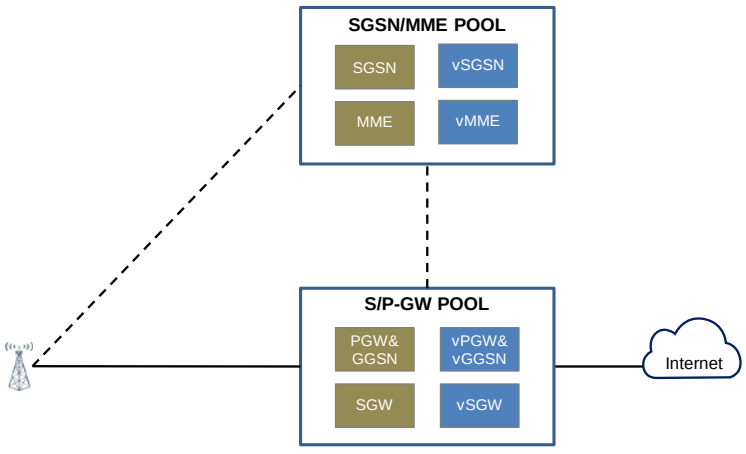

图5： NFV 扩容现有业务，共 Pool 部署

5.2.2 VNF 和 PNF 业务特性一致

为了使 VNF 能平滑承接现网业务，VNF 和现网 PNF 的特性对齐非常重要，原则上 VNF 应满足如下需求。

- VNF 的部署对终端和用户业务是完全透明的，即网络功能虚拟化不应该影响用户业务和体验。
- VNF 应该支持所有现网接口，并且可以与 PNF 互操作。
- 电信业务规范本身是平台无关的，理论上，只要 VNF 遵循相关规范并继承 PNF 的业务特性就可以承接现网业务，但实际部署中需要解决如下问题。
  - VNF 转发性能优化：虚拟化后，进出 VNF 报文的需经过虚拟层(如 vSwitch)复制和转发，影响转发性能，特别是时延/抖动，可能会影响用户的业务体验，需要优化方案。
  - VNF 基于通用 COTS，采用全 IP 接口，现网非 IP 接口(如 E1/ATM)需要提前考虑 IP 化或部署 IWF（Interworking Function，网络互联功能）进行转换。
  - VNF 可以灵活部署和迁移，业务流量不固定于某物理端口/线路。现网探针一般采用链路分光/端口镜像方式实现引流，该方案不再适用虚拟化场景，需重新考虑部署和组网方案。

5.2.3 VNF 和 PNF 网元协同管理

PNF 软件和硬件集成在一个设备中，设备生命周期、业务配合、日常维护等均通过 EMS 完成。

NFV 要求业务自动部署，软硬件分层运维。新增 MANO 负责网络业务(NS)和 VNF 的生命周期管理以及全局资源视图的管理。VNF 的业务配置、业务策略管理、日常维护等(FCAPS)仍然由 EMS 负责，MANO 和 EMS/OSS 通过运营商自定义的协同方式完成对 VNF 的全面管理。

在 PNF 和 VNF 混合组网情况下，网络侧应支持对 PNF 和 VNF 网元的协同管理，以实现端到端网络服务的管理。

5.2.4 垂直运维和分层运维模式共存

NFV 的出现，尤其是 PNF、VNF 混合网共存环境，对网络运维提出了较大挑战。传统网络软硬件一体化，按业务构建烟囱式运维团队；NFV 后软硬件解耦，网络运维团队面临转型，可能需要分层构建运维团队，同时需跨层协同运维，变化主要体现在以下两方面，一是各实体功能网元演变为以软件形态存在的虚拟网元，传统分业务领域的维护依然存在，而且网络业务和网元还可能分层运维，但是不再针对设备硬件进行维护；二是新增加 NFV 基础设施维护，管理和维护各数据中心的硬件和虚拟资源，如图 6 所示。

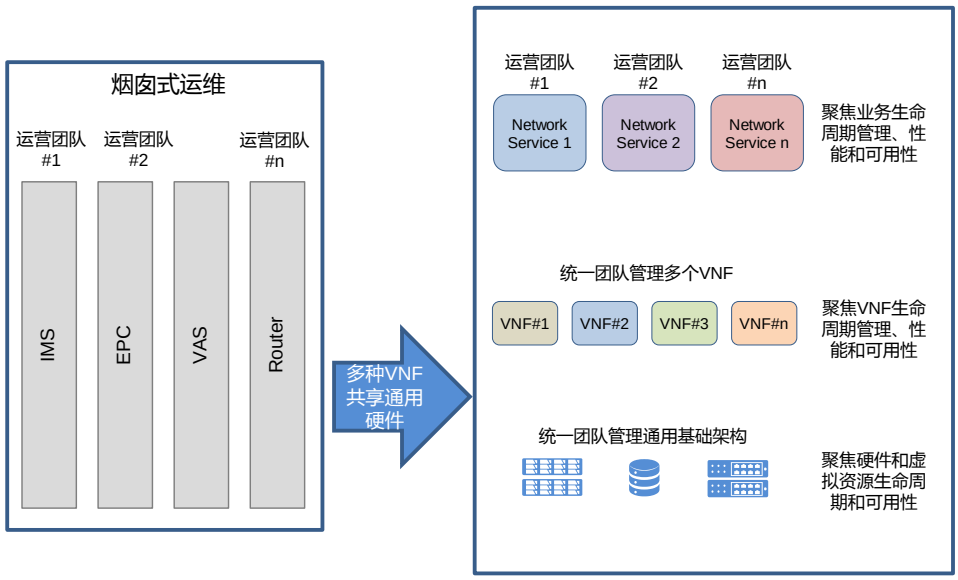

图6： 垂直运维向分层运维转型

另外，在技术上也面临如下挑战，包括：

- 混合组网场景下，业务涉及 PNF 和 VNF，这就要求跨 PNF/VNF、跨域、跨厂商的端到端业务编排和保障。

- 未来大流量将聚集在视频、重大事件/突发事件等场景，流量时空不均衡、潮汐效应显著，需研究如何利用 NFV，实现存量资源和虚拟化资源统一管理和调度，避免按峰值规划。

5.3 NFV 网络演进节奏和目标部署示例

运营商当前网络结构复杂，涉及到种类繁多的硬件和软件，因此从当前网络到 NFV 目标架构将是一个分步演进过程。

从运营商的角度来看如何引入 NFV 存在两种路线选择，颠覆性引入和逐步引入。颠覆性引入核心思想是直接在 DC 中新建全新的 NFV 网络并逐步替代现有的网络，而逐步引入则是在现有网络设备基础上逐点改造支持 NFV/SDN 等新技术。颠覆性引入对运营商要求高，在 NFV 引入初期就需要做好全局规划，并制定详细的实施步骤，在实施过程中要考虑业务的整体搬迁风险，初期实施代价大且存在一定风险；而逐步引入则对运营商要求相对较低，通过成熟一个改造一个的方式，最终形成大一统的 NFV 网络。具体演进路线每个运营商应结合企业自身的实际情况来制定，同时需要考虑以下几个方面的问题。

- 以数据中心为核心规划未来网络，建设基于云的统一基础设施；
- 根据业务驱动力、产品成熟度等，有序实施网元虚拟化，对于原有的非虚拟化设备，可以作为一个独立的业务节点存在，进行 VNF 和 PNF 混合组网。
- 运营系统增强(含 MANO)，实现自动化和智能化，从内部管控模式转变成外部用户服务模式；
- 从 IT 云、CT 云到 ICT 融合。

一个可能的 NFV 网络目标部署示例如图 7 所示。

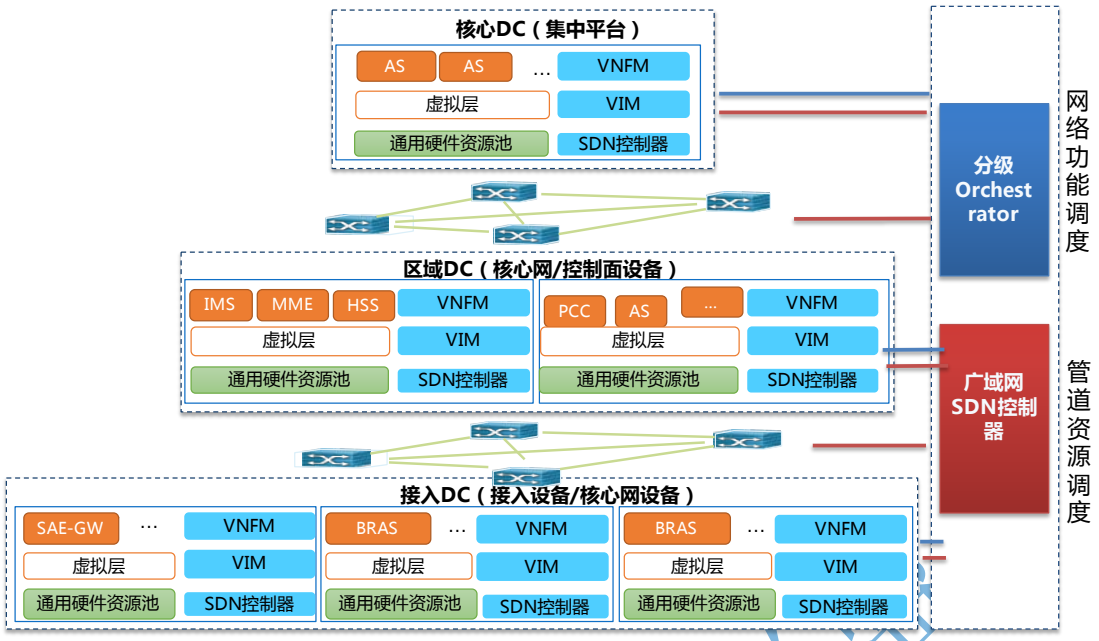

图7： NFV 网络目标部署示例

该示例中 NFV 网络目标部署是一个全虚拟化的三层 DC 架构。每个 DC 均采用标准化的设计，包括标准化的基础设施、组网和统一的编排管理体系。标准化的基础设施在硬件方面采用通用 COTS 硬件架构(如 x86)，并辅以增强型的硬件性能要求和电信级的管理要求；在虚拟层方面需满足标准统一的电信级要求，支持统一的虚拟层指标参数等。标准化的组网包括以电信标准为基准的更为严格的网段隔离和网络平面划分，数据中心内部业务、管理、存储平面相互独立。统一的管理编排体系包括以整合的 NFV 编排器和 SDN 编排/控制器作为统一管理编排体系，以电信级增强的 Openstack/VIM 实现云资源的管理和分配。

6 产业联盟的推进策略及 2016 年重点工作

围绕当前 NFV 技术和产业发展面临的主要问题，依托 SDN/NFV 产业联盟，秉承联盟“开放、创新、协同、落地”的宗旨，以构建 NFV 的产业生态为核心，以标准化和互通测试为工作重心，重点在关键技术、标准化、互操作以及测试等方面，发挥联盟的平台作用，促进 NFV 技术应用与业务创新，推进 NFV 标准化进程，实现开放的 NFV 解决方案，并通过互操作测试推动商用场景下多厂商解决方案的互通。在产业推进方面，可以考虑从以下几方面来着手。

第一，加快标准化工作，为 NFV 应用部署提供技术依据。重点围绕架构演进及各参考点的接口标准化，以及 MANO 与 OSS/BSS 协同管理、VNF 的可靠性和

可用性等，发挥产业联盟的平台作用，与相关标准组织合作推进 NFV 标准化工作，为 NFV 产业健康发展和规模应用部署提供必要的技术支撑。

第二，建设互通测试平台，推动解决方案的成熟落地。依托产业联盟，聚焦 NFV 商用场景，制定 NFV 基础设施平台层的基准测试规范，加快建设 NFV 互通测试平台，推动商用场景下多厂商解决方案的互联互通，为 NFV 大规模的商用部署奠定基础。

第三，强化应用与业务创新，积极打造自主开放的产业生态。以开放为核心，积极引导和鼓励联盟成员加强技术和产业合作，紧密围绕国内网络发展的实际需求，整合资源，形成合力，共同推动 NFV 技术研发与产业化进程，推动 NFV 产业生态的繁荣。鼓励和支持 NFV 开源生态建设，吸引全球智慧参与，形成以技术为纽带的创新模式，培育开放共享的开源社区。

在关键技术研究方面，2016 年计划推进 5 个重点项目的研究，包括：

（1）面向 VNF 的 MANO 要求：研究资源授权 direct 和 in-direct 模式的优缺点，形成统一需求，统一 MANO 与 OSS 的协同工作机制， 统一 NFVO 的基本功能要求；

（2）虚拟化层要求：研究满足电信级要求的 NFV 虚拟层特殊功能要求和性能指标；

（3）硬件要求：研究满足电信级需求的硬件资源（包括计算、存储、网络等）相关功能和指标要求；

（4）存储方案：研究用户数据类网元对存储的要求，分析对比本地存储、集中式 IP-SAN 存储、存储服务器三类存储方案的优缺点，统一存储方案及要求；

（5）可靠性：研究 NFV 引入后端到端高可靠性方案体系，明确 NFV 引入后各层的高可靠性方案要求。

附录 A 缩略语

3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
API	Application Program Interface	应用编程接口
ATCA	Advanced Telecom Computing Architecture	高级电信计算架构
BESS	BGP Enabled ServiceS	BGP 使能业务
BRAS	Broadband Remote Access Serve	宽带接入服务器
BSS	Business Support Systems	业务支撑系统
BYOD	Bring Your Own Device	自带设备
CCSA	China Communications Standards Association	中国通信标准化协会
COTS	Commercial Off-The-Shelf	商用成品
CPE	Customer Premise Equipment	用户端设备
CPU	Center Process Unit	中央处理单元
CT	Communication Technology	通信技术
DC	Data Center	数据中心
DoS	Denial of Service	拒绝服务
DPDK	Data Plane Development Kit	数据平面开发包
ECC	Error Checking and Correcting	错误检查和纠正
EMS	Element Management System	网元管理系统
EPC	Evolved Packet Core	移动演进分组核心网
ETSI	European Telecommunications Standards Institute	欧洲电信标准协会
FCAPS	Fault, Configuration, Account, Performance, Security	管理 5 大功能
HSS	Home Subscriber Server	属地用户服务器
I2NSF	Interface to Network Security Functions	网络安全功能接口
I2RS	Interface to the Routing System	路由系统接口
IETF	Internet Engineering Task Force	国际互联网工程任务组

IMS	IP Multimedia Subsystem	IP 多媒体子系统
IPPM	IP Performance Metrics	互联网性能指标
IT	Information Technology	信息技术
IWF	InterWorking Function	互通功能
MANO	NFV Management and Orchestration	NFV 管理和编排
MME	Mobility Management Entity	移动管理实体
NAT	Network Address Translation	网络地址翻译
NB-IoT	Narrow Band Internet of Things	窄带物联网
NFV	Network Function Virtualization	网络功能虚拟化
NFVO	NFV Orchestration	NFV 编排器
NUMA	Non Uniform Memory Access	非一致性内存访问
NVO3	Network Virtualisation Overlays	网络虚拟化叠加
L2TP	Layer 2 Tunneling Protocol	2 层隧道协议
OSS	Operations support systems	运营支撑系统
OPNFV	Open Platform for NFV	NFV 开放平台
PCI	Peripheral Component Interconnect	外围组件互连
PNF	Physical Network Funcation	物理网络功能
QoS	Quality of Service	服务质量
PCRF	Policy Control and Charging Rules Function	策略控制与计费规则功能
PGW	Packet data network Gateway	包数据网网关
PoC	Proof of Concept	概念验证
RCS	Rich Comunication Services，	富媒体通信业务
SAN	Storage Area Network	储存区域网络
SFC	Service Function Chaining	业务功能链
SGW	Serving Gateway	服务网关
SR-IOV	Single root I/O virtualization	单根 I/O 虚拟化

TEAS	Traffic Engineering Architecture and Signaling	流量工程架构与信令
TLB	translation lookaside buffer	翻译后备缓冲器
VIM	Virtualisation Infrastructure Management	虚拟化基础设施管理器
VNF	Virtual Network Function	虚拟网络功能
VNFM	VNF Manager	VNF 管理器
VoLTE	Voice on Long Term Evolution	LTE 语音
VPN	Virtual Private Network	虚拟专用网
VPC	Virtual Private Cloud	虚拟私有云
vSR	Virtual Service Router	虚拟业务路由器

附录 B. SDN/NFV 产业联盟相关介绍

B. 1 联盟的定位和目标

SDN/NFV 产业联盟旨在汇聚产业链力量，共建 SDN/NFV 产业生态，推动 SDN/NFV 商用化进程，解决现有网络如何向基于 SDN/NFV 技术架构的网络演进、网络如何支撑新型业务创新和灵活部署、超大规模网络如何运维等关键问题。

SDN/NFV 联盟宗旨：“开放、创新、协同、落地”。

SDN/NFV 产业联盟的愿景是：

（1）立足中国，面向全球，聚焦产业资源，共同推动 SDN/NFV 技术和产业发展；

（2）推动联盟成员广泛协作交流，力促 SDN/NFV 技术、标准、产品/解决方案及应用的成熟；

（3）围绕 SDN/NFV 技术开展不同应用场景的解决方案探索，组织和推动联盟成员共同协作，促进 SDN/NFV 产业生态健康发展，推动 SDN/NFV 产业生态繁荣。

B. 2 联盟的组织架构

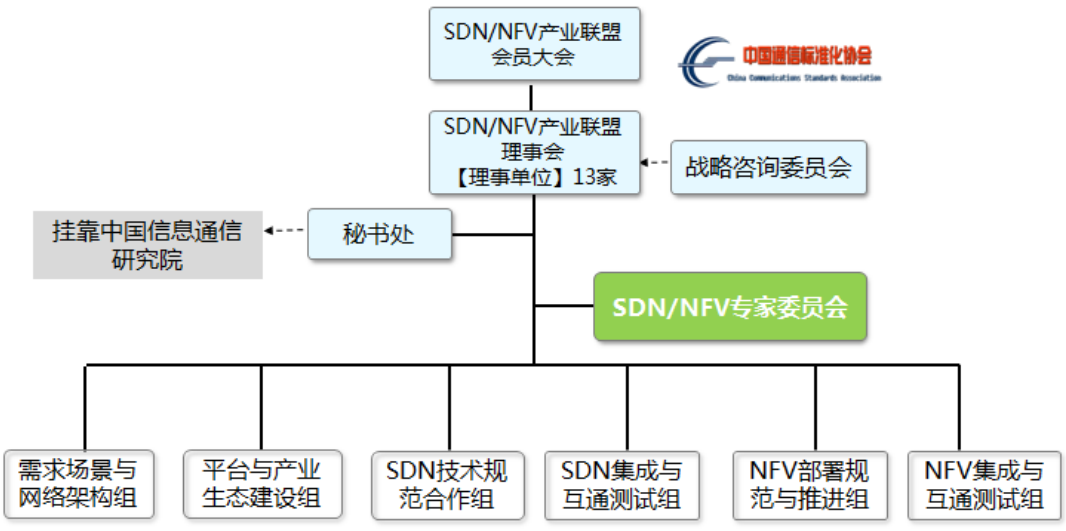

图 B.1　SDN/NFV 产业联盟组织架构

目前，SDN/NFV 产业联盟的组织架构如图 A.1 所示，其中：

（1）会员大会是联盟的最高权力机构，主要审议联盟章程、联盟发展规划和工作方针、理事会的工作报告等。

（2）理事会是会员大会的执行机构，领导本联盟开展日常工作，负责 SDN 联盟整体战略制定，及联盟运作重大事项决策。审议理事会年度工作报告、议案、年度财务预算和秘书处提交报告。

（3）战略咨询委员会作为顾问组织，由业界专家组成，向理事会提供发展战略咨询建议。

（4）秘书处主要是支撑联盟日常事务、运营及重大活动，负责联盟相关论坛会议活动的组织与品牌宣传造势。

（5）SDN/NFV 专家委员会：在技术层面上为各个工作组提供指导并协调各个工作组的工作。

（6）需求场景与网络架构组：负责汇总行业信息，开展所有 SDN 场景下的需求沟通事宜，把握方向梳理出行业关键需求；输出 SDN 技术架构，面向行业发布 SDN 解决方案。

（7）平台与产业生态建设组：负责协调联盟应用开发资源积极开展业务应用创新开发工作，打造开发平台，挖掘新机会和应用点，促成行业不断创新和发展。

（8）SDN 技术规范合作组：研究制定 SDN 技术规范，并负责同行业 SDN 标准组织之间的联系沟通工作，促进产业链各领域资源在技术标准制定中统一意见。

（9）SDN 集成与互通测试组：负责联盟各厂商间产品互通测试规范和标准制定，组织协调产业链资源积极参与对接测试活动。

（10）NFV 部署规范与推进组：基于需求和场景，研究制定 NFV 按需编排的网络顶层架构、关键部件的定义、业务流程和接口定义等；推动并完善相关 NFV 硬件认证标准；研究制定典型行业 NFV 解决方案；研究针对多种业务的服务加速、快速集成、开放创新技术等。

（11）NFV 集成与互通测试组 ：构建测试系统和平台，完成测试需求和测试场景的设计；组织开展 NFV 认证、NFV 互通测试、NFV 集成验证；推动 NFV 测试用例、工具仪器的研发。

结 束 页