

中国移动 5G行业专网技术 白皮书

目 录

1.	5G行业专网能力需求	5
1.1	组网需求	5
1.1.1	业务加速	5
1.1.2	业务隔离	5
1.1.3	本地业务保障	5
1.1.4	业务数据不出场	5
1.1.5	边缘计算	5
1.1.6	无线上行带宽增强	6
1.1.7	无线专用	6
1.1.8	接入控制	6
1.1.9	能力开放	6
1.2	运营及运维类需求	6
1.2.1	业务运营	6
1.2.2	网络运维	7
1.2.3	安全	7
1.2.4	计费	7
1.3	业务能力与网络技术能力的映射	7
2.	技术架构及技术要求	9
2.1	技术网络架构	9
2.2	技术要求	10
2.2.1	端到端 QoS优先调度	10
2.2.2	专用 DNN.....	11
2.2.3	网络切片	12
2.2.4	边缘计算	14
2.2.5	无线专网定制	15
2.2.6	无线专网增强	16
2.2.7	核心网定制	16
2.2.8	能力开放	16
2.2.9	开通	20
2.2.10	计费	21
2.2.11	安全	21
3.	产业及商用发展建议	23
4.	结束语	24
	缩略语列表	25

1. 5G行业专网能力需求

1.1 组网需求

行业客户基于不同的应用场景，业务需求众多且差异巨大，各类行业应用的差异化组网需求主要包括：业务质量保障、业务隔离、超低时延需求、数据不出场、边缘计算、超级上行、接入控制和能力开放。

1.1.1 业务加速

行业用户要求增强的数据业务质量保障，根据业务质量要求在带宽和时延方面提供差异性的服务质量保障，保证高优先级用户获得更好的业务加速体验。

1.1.2 业务隔离

行业客户要求专用网络资源与公众网隔离，通过专用的业务数据通道实现业务流量的定向汇聚传输和隔离，保证数据专用和安全。

1.1.3 本地业务保障

行业客户要求对时延敏感的业务（20-40ms）在靠近用户的位置进行卸载，就近处理。

1.1.4 业务数据不出场

行业客户要求超低时延保障（20ms），企业内部相关业务数据要在园区内分流卸载，不出园区，满足数据安全和本地数据快速处理的需求。

1.1.5 边缘计算

行业用户要求在网络边缘通过运营商提供的平台部署边缘业务以及超低时

延应用。

1.1.6 无线上行带宽增强

部分行业业务，例如高清视频监控，对无线上行带宽有非常高的需求，需要通过无线增强方案才能支持。

1.1.7 无线专用

行业客户在局域覆盖且对安全隔离或业务质量要求很高的场景下，要求使用专用的基站或者专用的频段，同时提供业务隔离和业务质量保障。

1.1.8 接入控制

当行业用户使用专用基站或者专用频段时，要求只允许特定用户接入，不允许其他用户接入，而且客户能够对哪些用户接入进行控制。

1.1.9 能力开放

行业用户对于 5G 网络有自主性需求，要求实现网络和行业平台等联动，满足行业系统对网络服务能力的调用需求。

1.2 运营及运维类需求

1.2.1 业务运营

行业客户需要通过运营商提供的业务订购入口发起行业专网业务的业务运营流程，包括业务订购、业务变更、业务退订、业务管理等流程。当业务开通涉及边缘计算资源时，客户需要能在开通行业专网业务时同时开通边缘计算网络资源。

行业客户对 5G 专网的生命周期管理有一定的自配置、自我管理需求。

行业客户需要能对其专网内的用户成员进行批量开通，并提供客户自我管理能

力，包括成员添加、成员删除、成员权限变更和成员状态查询等。

1.2.2 网络运维

行业用户对专网网络有运维需求，包括网络运行状态查询、切片指标查询、网络性能监控、网络监控报警等能力。

1.2.3 安全

行业客户要求 5G 专网在物理安全、接入安全、信息传输安全、数据防泄露安全、恶意攻击抵御等方面提供全方位安全防护能力，要求专网具有安全风险、安全事件监测、告警以及及时响应的能力，满足关键信息基础设施安全、等级保护等法律法规要求，确保重要基础设备自主可控，防止敏感信息泄露，防止业务滥用对公共安全带来风险和恶劣影响。

1.2.4 计费

行业用户要求多种模式的价格及灵活多样的计费模式，可根据给用户提供的网络资源情况为行业客户提供灵活可组合、定制化的计费方案

1.3 业务能力与网络技术能力的映射

从上述业务能力需求可以看出，垂直行业需求种类繁多，且与 SA 公众网客户需求差异比较大。为满足这些差异化需求，5G 网络引入多种网络技术能力，能够提供在网络组织和性能方面的差异化能力。

表 1 业务能力需求与网络技术能力的对应

业务能力需求	对应的网络技术能力
业务加速	端到端 QoS 优先调度
业务隔离	专用 DNN 网络切片，核心网定制
本地业务保障	用户面下沉，无线超低时延调度
数据不出场	用户面下沉园区，本地分流，核心网定制

边缘计算	本地分流，边缘计算，核心网定制
上行带宽增强	无线上行增强（专用覆盖场景），特殊时隙配比
无线专用	无线基站专用，无线频段专用
接入控制	专用小区无线接入控制
能力开放	网络能力开放
业务开通	业务开通，云网协同统一入口，业务开通自服务， 批量用户开通，专网成员管理
运维	网络运行状态查询，切片指标查询，网络性能监控， 网络监控报警
业务安全	网络切片，用户面下沉园区，核心网定制，网络安全机制
业务计费	多量纲计费

本白皮书将对这些网络技术能力的要求进行明确。

2. 技术架构及技术要求

2.1 技术网络架构

中国移动 5G行业专网核心网与面向大网用户的 SA网络相对独立，采用“核心网独立部署，无线共用为主按需专用，共用传输资源按需隔离”的方式组网。

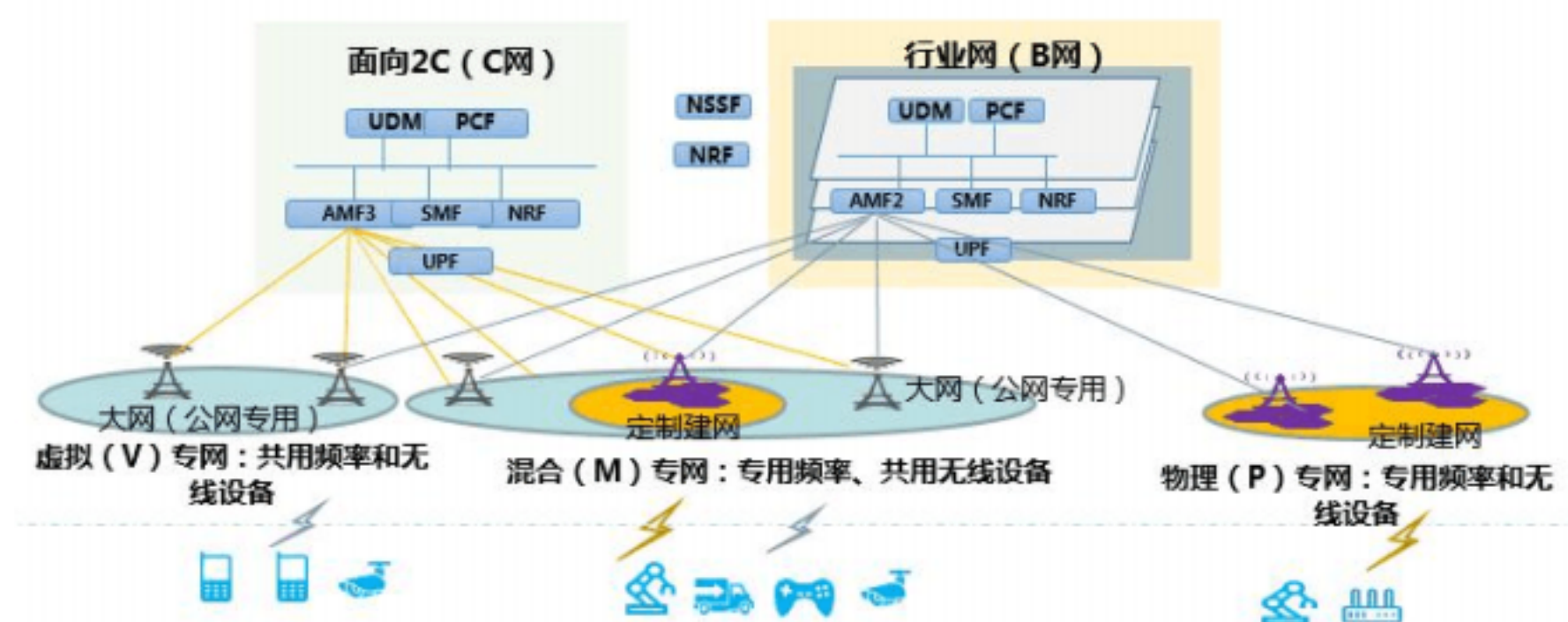


图 1 行业专网总体组网

ToB与 ToC各自独立建设 AMF/SMF/UDM/UP等网元；两张网络进行必要互通以满足切片重定向需求。

整体上 ToB与 ToC共用无线，仅在特定需求场景下通过专用基站或划分专用频段的方式提供专用无线资源。

ToB与 ToC共用传输网络，通过 SPN软、硬隔离手段为 ToB应用按需划分传输资源。

5G行业专网的逻辑网络架构如下图所示：

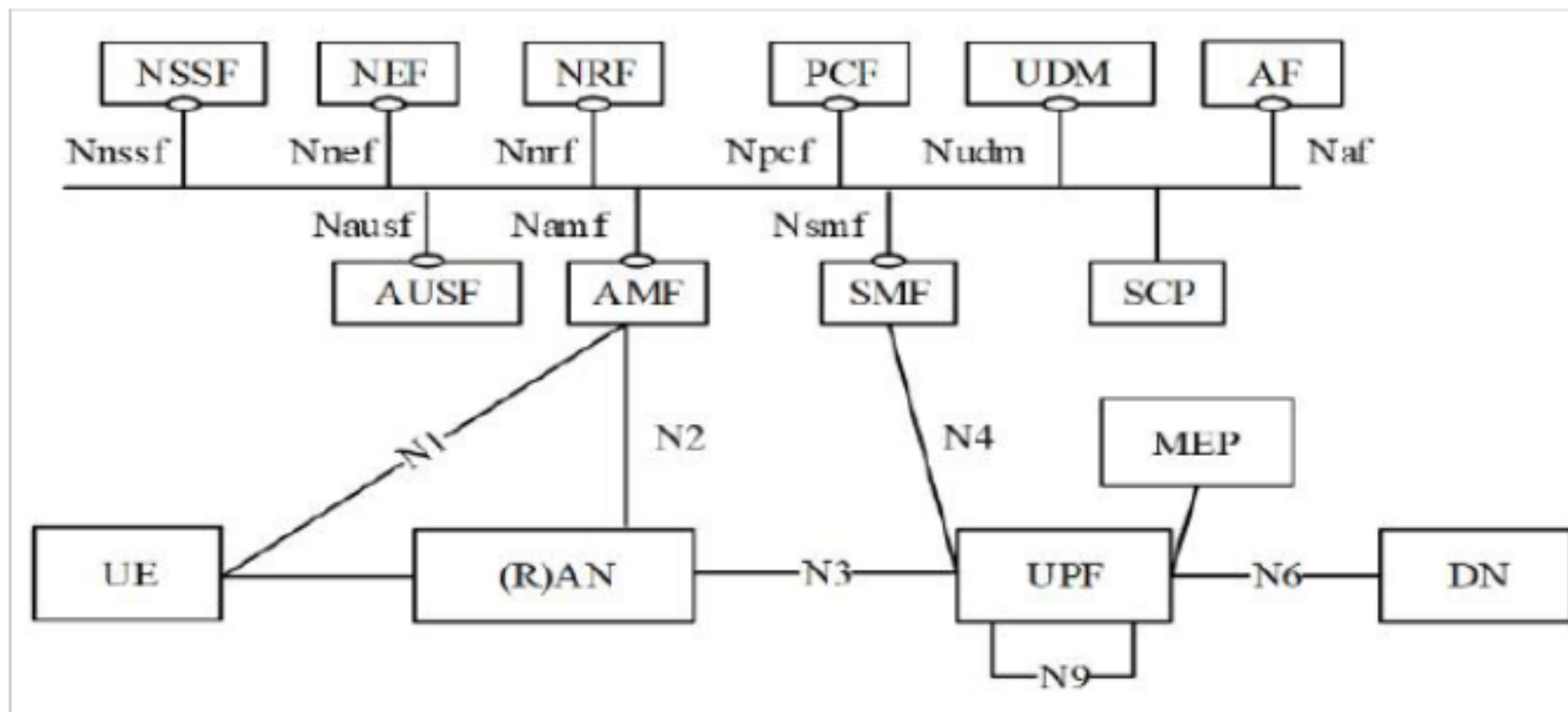


图 2 5G行业专网的逻辑网络架构

5G行业专网网络架构包含端到端的节点或网元，由终端、无线接入网、5GC核心网和边缘计算平台等部分组成。

无线接入网由5G基站组成，直接与5GC核心网连接，承载数据业务。

5GC核心网采用基于服务的架构，主要由AMF, SMF, NSSF, NRF, NEF, AUSF, PCF, BSF, NWDAF, UDM, UDR, UPF等控制面网络功能和UPF等用户面网络功能组成。

其中，PCF, SMF, UDR, AMF, NEF, BSF, NWDAF等网络功能组成策略控制及能力开放系统。UDM, UDR, AUSF等网络功能组成用户数据系统。

边缘计算平台MEP与UPF连接，处理UPF分流出的数据，提供边缘计算应用及应用管理。

2.2 技术要求

2.2.1 端到端 QoS优先调度

5G网络应支持端到端QoS机制，能够根据行业专网应用的业务质量要求，对业务数据流进行端到端优先级调度，保证业务指标的满足和差异化。

2.1.1.1 5GC核心网 QoS功能要求

5GC应支持4G/5G融合策略控制PCC架构，应支持会话级别和QoS流级

别的 QoS策略控制，包括门控、QoS 控制、流量控制、事件监控、用量监控、流量引导等能力；

5G核心网应支持 3GPP协议中定义的标准 5QI 以及自定义 5QI

5GQ应支持灵活的策略配置，支持向终端和无线下发相关策略

5GQ应支持 3GPP协议中规定的标准 ARP配置。

5GQ应支持 QoS参数到传输级参数（ VLANPriority 和 DSCP等）的映射

5GQ应支持下行业务流到 QoS Flow 的绑定

2.1.1.2 5G无线网 QoS功能要求

支持 QoS相关的参数配置，包括 MBR(MaximumBit Rate)、GBR(Guaranteed Bit Rate)、PBR (MinBR UE-AMBR5QI、用户等级等，用于基于 QoS参数的调度。

针对不同的切片与 QoS需求，无线网可通过调度优先级、预调度等参数 / 算法配置，保障空口速率、时延、可靠性等性能需求。

无线支持根据 ARP进行接纳控制。

支持 5QI 参数和 DSCP参数的灵活映射

2.1.1.3 5G传输承载网 QoS功能要求

IP 承载网应支持根据核心网、无线映射的 DSCP等参数进行 QoS调度。

SPN和 PTN传输网应支持根据核心网、无线映射的 VLANPriority、DSCP等参数进行 QoS调度。

针对同一 5QI，核心网支持为传输和承载配置不同 DSCP, 支持运营商自配置 5QI 与 DSCP VLAN Priority 的映射关系。

2.2.2 专用 DNN

5G网络支持为行业客户分配独立的 DNN 提供专用的业务数据通道，支持根据 DNN为行业用户选择特定的 UPF, 实现流量汇聚。

2.2.3 网络切片

网络切片是提供特定网络能力的、端到端的逻辑专用网络。网络切片建议基于 NFV/SDN的通用基础设施构建，实现低成本高效运营。

针对网络切片标识（ S-NSSAI）：

切片 / 服务类型（ SST）取值中， 0-12由标准定义， 128-255依据中国移动优/专/尊享不同模式进行自定义。

切片区分符号（ SD）取值针对公众网包含公众网切片能力等级信息，针对行业专网包含区域、行业、公司和业务等信息。

5G行业专网支持默认切片和专用切片

无线域 / 核心网域与传输域交互时应支持 S-NSSAI与 VLANID 的映射

无线域支持以原有 QoS机制为基础，增强基于切片用户组的资源预留无线资源分配机制，满足不同业务的不同 SLA需求。支持基于 QoS机制，从空口速率、时延、可靠性三个维度实现 QoS保障；支持为特定切片的用户预留资源，保障其业务体验。

核心网域支持网络功能和资源按需部署：

除 UPF网元外，核心网网元支持基于云化技术部署，根据实际需求实现自动部署、弹性伸缩、故障隔离和自愈等功能。

基于网络切片选择功能（ NSSF），支持在用户注册流程中，基于 NSSAI提供相应接入的网络切片选择信息。

核心网域网元支持 NSSAI的签约、传递、管理与更新、网元选择与接入等功能。

传输域支持基于 SPN提供子切片能力。 SPN支持基于切片以太网时隙交叉 TDM通道实现切片硬隔离，支持基于以太网包交换通道以及 QoS实现切片软隔离。

SPN物理网元支持虚拟化多个逻辑 vNode，物理链路支持虚拟化多个逻辑 vLink。

SPN的切片资源层支持将逻辑虚拟的 vNode和 vLink 组合成逻辑

网络 vNet。

SPN切片管控层支持提供北向接口开放网络切片能力。

5G终端各种形态，包括智能类手机终端和数据类终端（如通用模组、CPE等），应支持切片相关功能。

5G终端支持 S-NSSAI的处理：支持根据网络指示，对 NSSAIs（包括 Configured/Allowed/Rejected NSSAI）进行接收、存储和更新；支持根据 NSSAI inclusion modes指示，在空口 RRC层携带 NSSAI信息给 gNB；支持基于配置规则为各个业务选择相应的 S-NSSAI

5G终端应支持同时并发携带多个（2个）网络切片标识的能力。

5G终端应支持基本的预配置 URSI规则：支持由网络下发 URSI配置规则的接收、保存和更新；支持网络指示 URSI的动态更新；支持优先使用由网络指示的 URSI规则；支持根据 URSI规则，提供业务应用（APPID、IP3 元组，FQDN、DNN、ConnectionCapability）等描述信息，以及建立业务应用与对应的 S-NSSAI的映射绑定；支持根据 URSI相关信息发起相应的 PDU会话

5G网络应支持网络切片的管理，其中：

CSMF支持依据优 / 专 / 尊享不同模式下的不同用户需求，实现需求订购和处理，并支持将业务需求转换为对应网络需求。

NSMF支持基于从 CSMF下发的切片网络需求，将切片的 SLA需求分解为无线、传输和核心网各子域的 SLA需求，并下发至各子域 NSSMF

核心网 NSSMF支持将网络切片子网的网络需求转换为网络服务，向 NFV的 NFVO系统下发网络服务的部署请求。核心网 NSSMF能支持与 NFVO合设。

无线 NSSMF支持网络切片无线域业务参数的配置，支持与 OMC/EMS合设。

传输 NSSM支持依据 NSMF下发的传输域业务需求，识别出传输域服务类型，实现对应资源的分配，并调用 SC北向接口实现切片业务的下发，基于 SC实现跨 OMC/D的业务控制。

2.2.4 边缘计算

2.2.4.1 5G 核心网功能要求

5G核心网应支持数据本地卸载功能，实现方式包括：

UL CL方式，即 UPF根据目的 IP 地址将数据进行分流；

Branching Point 方式，即 UPF根据源 IP 地址将数据进行分流；

LADN(Local Area Data Network) 方式，即建立只在特定区域内容才能使用的 PDU会话，该会话的数据全部通过本地 UPF疏通；

DNN切片方式，即网络根据 UE访问的特定 DNN或切片或二者的组合选择特定的本地 UPF对全部数据进行本地疏通。

PCF/UDR支持数据本地卸载策略的生成，包括静态签约方式和通过能力开放动态生成方式。

UPF支持预配置本地分流策略

SMF支持分流点的动态插入、删除、变更。

SMF与 UPF之间应支持 N4接口开放，满足异厂家互操作要求。

2.2.4.2 边缘 IaaS 要求

统一运维：采用边缘计算 IaaS 云管理平台作为统一运维入口（省级或地市级），对辖区内所有边缘节点的 IaaS 进行运维管理，实现无人值守边缘节点的远程运维，并对管理编排组件收敛北向接口以节省网络开销；

自治性：边缘节点存在地市、区县、接入等多个位置，但每个位置的边缘计算 IaaS 都是可自治的云，不依赖其他边缘计算 IaaS；

承载多类型云平台：边缘计算应用和相关电信网元可能采用了不同的设计和承载方式，从云的角度需要支持虚拟机和容器两种资源，因此边缘

计算 IaaS 需要支持 OpenStack 云和 Kubernetes 云，两者的关系在后面论述；

管理轻量化：区县以及接入等位置的边缘节点资源受限，可采用融合节点、压缩管理组件资源占用等将管理开销轻量化的方式，使得业务可用资源最大化；

按需使用和计费：边缘计算 PaaS平台或业务可以按需申请使用边缘计算 IaaS 资源，边缘计算 IaaS 根据使用情况计费；

统一云资源视图：管理编排器应具备边缘计算 IaaS 资源的统一视图，以便对资源进行一致性的管理，并对边缘计算 PaaS平台或业务申请 IaaS 资源进行授权；

组网轻量化：区县以及接入等位置的边缘节点内组网需要扁平化设计；

支持 SDN: 边缘计算 IaaS 应按需支持 SDN, 以及基于 SDN的切片能力；

支持加速：UPF等用户面网元以及计算密度较高的边缘计算应用等对 CPU的压力较大，需要支持将加速功能卸载到硬件实现。

2.2.4.3 边缘 PaaS要求

业务部署，PaaS集中管理平台作为应用部署的统一入口，将应用部署在边缘计算数据中心里。

网络能力 API ,边缘 PaaS平台为边缘应用提供网络相关的能力开放 API , 如 QoS策略 API、数据分流策略 API 等

通用能力 API ,边缘 PaaS平台提供通用 IT 能力 API 供边缘应用调用

行业能力 API ,边缘 PaaS平台应能够面向不同行业应用提供与行业强相关的 API 能力

2.2.5 无线专网定制

5G无线应支持频率专用能力，在特定区域将部分频段资源通过专享基站或共享基站独立小区的方式分配给行业用户专用。

5G无线应支持通过多 PLMN Cell Bar、专用 TAC等方案实现专用小区的接入控制功能，并演进支持基于 CAG的目标方案。

2.2.6 无线专网增强

5G无线应支持根据客户需要新建或增补基站，按需实现基站专用。

5G无线应支持采用 4.9GHz 3U1D专属帧结构增强上行速率。

5G无线应支持通过皮站定位、蓝牙定位、UWB定位、基站定位等提供不同精度的室内外定位能力。

2.2.7 核心网定制

5G行业专网可以根据行业用户需求进行核心网定制，包括专用核心网切片、轻量型核心网下沉至园区、UPF/MEP 一体机模式。

5G行业专网支持为行业客户建设专用的独立核心网切片，每个切片设置专用的核心网控制面网元设备和用户面网元设备，按需部署在公共资源池服务器上或者行业用户专用的服务器上，实现网络物理隔离。

5G行业专网可为行业用户提供定制化轻量型核心网下沉园区技术，以轻量级边缘网关形态部署至用户侧，边缘网关兼有 AMF, SMF, UPF 基本功能，按需定制为 SMF+UP功能形态或 AMF+SMF+UP功能形态

5G行业专网支持一体机模式，使用 UPF增强支持 ME形态的一体化设备，在网络能力外同时提供边缘平台服务和第三方应用加载和管理的能力。

2.2.8 能力开放

结合 5G行业专网对外开放的能力以及行业专网特征，中国移动 5G行业专网能力开放的技术架构采用网络能力层、能力接入层和能力开放层 3层全解耦架构，如下图所示：

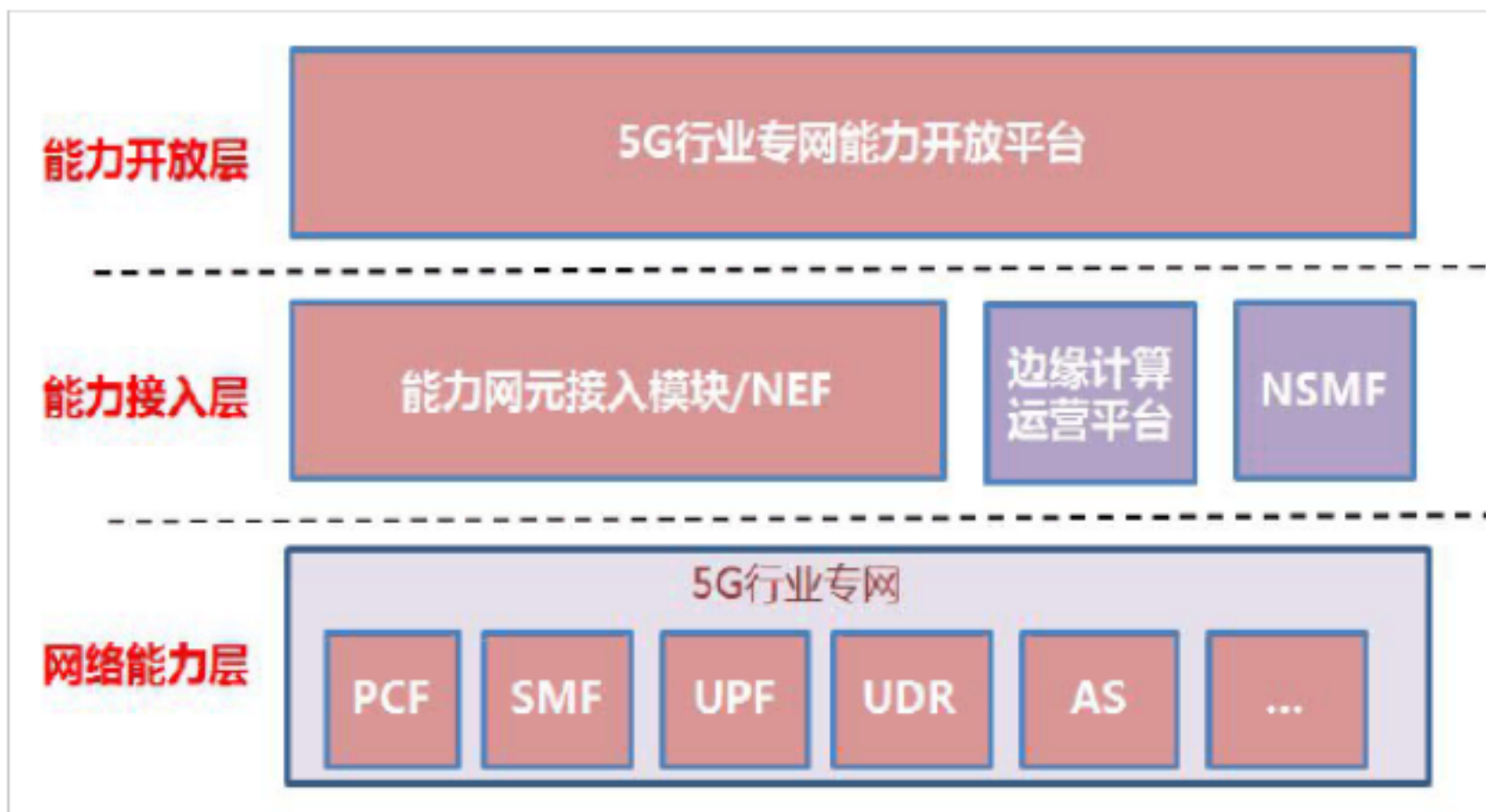


图 3 行业专网能力开放架构图

网络能力层：网络能力层为 5G 行业专网，支持通过服务化接口支持管道、网络数据、音视频、边缘计算和网络切片等网络能力的提供。

能力接入层：能力接入层包括能力网元接入模块 /NEF、边缘计算运营平台和切片管理器 NSMF 支持网络通信能力、边缘计算能力和网络切片能力的汇聚封装功能。

能力网元接入模块 /NEF：应支持音视频能力、消息能力、管道能力、网络数据能力、管道能力、网络数据能力、PFD 能力、URSP 能力。

边缘计算运营平台：应支持边缘计算能力。

切片管理器 NSMF 应支持网络切片能力。

能力开放层：能力开放层为 5G 行业专网能力开放平台，支持 5G 行业专网能力对外开放的统一运营管理，支持面向行业客户提供线上注册、能力产品订购、自助添加行业企业用户等在线服务功能。支持面向行业企业应用提供应用登记、能力 API 发现和 API 调用等功能。支持边缘计算平台（ECP）进行能力调用。

中国移动 5G 行业专网支持面向行业企业客户开放音视频、消息、管道、网络数据、DPI/PFD 边缘计算和网络切片等行业专网能力，支持行业企业应用通

过基于 IP/TCP/HTTP协议的标准 RESTful API 进行行业专网能力的调用，对开放能力的具体要求如下：

音视频能力：音视频能力包括呼叫控制、小号、点击拨号、IVR和录音等能力。主要由智能网 SCP/AS 和多号平台和双跨 Centrex AS等网元支持提供能力，

智能网 SCP/AS: 智能网 SCP/AS应支持针对行业专网用户的呼叫发起、振铃、接通和挂机等呼叫事件的通知上报，以及支持呼叫接续、拦截等呼叫控制和 IVR 放音收号功能。

和多号平台：和多号平台应支持通过中间号完成主 / 被叫号码的翻译，以实现号码隐藏功能。

双跨 Centrex AS: 双跨 Centrex AS应支持使用行业企业号码对行业企业用户进行外呼，并支持行业企业用户的点击拨号和通话录音功能。

消息能力：消息能力包括短消息、多媒体消息和 USSD消息的发送和接收递送报告等能力，主要由云 MAS行业网关和智能网 SCP/AS进行能力提供。

云 MAS行业网关：应支持短消息、多媒体消息的发送、接收和接收递送报告等能力。

智能网 SCP/AS: 应支持 USSD消息的推送能力。

管道能力：管道能力包括 QoS和流量引导能力，主要由 PCF UDR SMF 和 UPF 等网元完成能力提供。

PCF:应支持根据 NEF下发的请求进行 QoS资源和流量引导策略的更新并动态下发至 SMF的功能。

BSF: 应支持 UE会话绑定信息查询以及 PCF地址查询功能。

UDR: 针对不区分 UE地址的应用分流请求，UDR应支持用户分流策略等数据的创建更新删除、保存以及订阅通知等功能。

SMF:应支持根据 PCF下发的 QoS策略对指定数据流进行 QoS控制功能。应支持根据 PCF下发的分流策略完成 UPF的选择以及分流

策略的下发。

UPF: 应支持根据 SMF下发的策略执行用户数据分流操作。

网络数据能力：网络数据包括监控数据以及码号标识数据，主要由 UDM和 AMF网元完成能力提供。

UDM 应支持网络监控数据的查询及 3GPP协议中规定的事件订阅通知功能。

AMF: 应支持接收 UDM的位置查询请求，并返回 UE的位置信息。

DPI/PFD能力： DPI/PFD包括网络数据报文检测能力，主要由 UDR SMF和 UPF网元完成能力提供。

UDR: 应支持 PFD规则数据的创建、更新、保存、读取和删除等功能。

SMF: 应支持从 NEF获取 PFD规则实现网络数据报文检测功能。 应支持向 NEF发起 PFD规则订阅请求并根据下发的 PFD规则进行更新。

UPF:应支持根据 SMF下发的报文检测条件执行相应报文检测操作。

边缘计算能力： 边缘计算能力包括网络能力（ RNIS、 Location 、BWMUEI等）与垂直行业能力，主要由 RAN ECP和 ECA完成能力提供。

RAN: 应支持提供 RNIS无线信息与 Location 位置信息的查询、订阅、通知

ECP: 应支持提供应用 BWM带宽管理、 UEI用户标识管理、 ECA垂直行业能力（编解码）。

ECA: 应支持提供 ECA垂直行业能力（ AI能力等）。

网络切片能力： 网络切片能力包括切片生命周期管理（资源勘查、 创建、删除、激活、去激活等）和切片状态监控（查询、订阅、退订）等能力，主要由无线、传输和核心网子切片管理器 NSSM提供。

无线、传输和核心网 NSSMF 应支持提供各域子切片生命周期管理（资源勘查、创建、删除、激活、去激活等）和状态监控

供（查询、订阅、退订）。

URSF能力：URSF能力包括 URSF策略查询与 URSF策略更新能力，主要由 PCF/UDRAMF 和 UE等网元提供。

PCF/UDR: 应支持 URSF策略信息查询与 URSF策略下发。

AMF: 应支持将 URSF指令经 AMF下发给用户 UE,从而实现用户 UE 根据应用指示动态优选网络切片。

UE: 应支持接受并执行 URSF指令进行网络切片选择。

2.2.9 开通

5G行业专网支持网边云协同的统一运营入口，为专网业务所需要的网络资源、云资源、用户数据提供一站式开通。

统一运营入口接收到业务开通请求后，能够对其中针对云资源和网络资源的需求进行分解，对于网络资源的需求通过调用 CSM进行开通，对于云资源的需求通过对应的云管理平台实现开通。

CSM面向客户经理提供 5G行业专网订购入口，提供产品、订购、监控、计费 and 结算等功能，并通过 NSMF完成端到端切片的开通。

5G行业专网支持用户自服务，即用户可在业务受理门户上自行操作对业务进行自助业务订购和管理运维展示界面等功能。

统一运营入口支持分级部署，即省内业务可通过二级运营入口实现省内闭环开通；跨省业务或全国业务通过一级运营入口受理业务开通请求之后将相关资源开通需求分发给各省内业务开通系统。

5G行业专网支持 2B用户的卡号开通、用户签约、订购关系同步、计费和结算管理等功能。

5G行业专网支持 2B2C业务订购入口，支持 2B2C用户的业务开通，与各省 BOSS交互完成 2B2C用户业务开通和订购关系同步。各省 BOSS负责 2B2C用户的卡号开通、用户签约、计费和结算管理等功能。

2.2.10 计费

5G行业专网计费支持基于流量计费的模式，采用融合计费架构，并具备离线计费、在线计费、内容计费、策略计费能力。

SMF应支持计费触发功能，SMF通过 Nchf 接口与 CHF进行交互，CHF 支持离线计费话单生成，并通过 Nchf ' 接口将在线计费消息路由至 OCS

BOSS/OC支持采集并处理 CHF生成的离线计费话单和转发的在线计费消息，实现精准计费。

5G网络支持多种内容计费量纲，根据不同接入方式、流量、业务质量（QoS）、DNN 切片 ID、UPFID 及各种组合进行复杂计费的功能。内容计费由各业务平台、SMF UPF和 CHF网元共同完成，由 BOSS/OC完成综合计费。

2.2.11 安全

中国移动 5G行业专网支持定制化的安全，引入用户接入安全、数据传输安全、切片安全、服务化架构信令安全、NFV 及边缘计算安全、数字证书、网络设备安全保证等方式为行业用户提供覆盖网络的通用安全，通过制定组网安全域划分、部署安全防护设备、建设安全管控系统、搭建网络与业务系统间的安全通道、提供业务技术安全等多方面，针对不同行业用户对安全的需求提供端到端灵活的安全策略。

5G行业专网提供的安全能力如下：

提供切片级的安全保护措施，包括切片内部的安全，也包括接入安全、传输安全、以及管理安全等：

提供切片级的用户接入安全，进行双向认证，进一步对用户提供接入切片的认证，以及提供切片选择辅助信息的隐私保护；对空口传输的数据提供安全加密和完整性保护能力；

实施对切片的隔离，建立切片逻辑或物理隔离、将敏感网元部署在高安全级别的物理位置和设备上隔离以及专用无线网络隔离等三级立体化安全隔离体系。

针对切片管理，提供实时的切片安全监控能力，应急处置以及故障恢复能力，在企业网络受到攻击或非法入侵时探查到安全事故，切换服务节点，并恢复受攻击出现故障的网络单元。提供对切片管理操作的双向认证、授权、日志审计，切片管理操作指令传输的加密、完保、抗重放保护，以及切片配置的检查校验，和切片终止后的数据清除等。

提供切片级的安全服务能力。在面向垂直行业的网络切片中，存在三种安全能力提供方式：

在与垂直行业签约切片服务时，以 SLA的形式确定针对特定切片的安全配置参数，行业客户可按需向运营商申请调整安全配置及其参数；

运营商的网络和安全能力由网络开放功能 NEF提供给垂直行业应用开发者，应用开发者可在业务逻辑中按需调用。

在网络侧部署安全设备或者安全功能模块，通过流调度的方式让特定应用流量依次经过这些安全模块，提供纵深防御。

此外，对于在网络中引入边缘计算平台的情况，需支持使用 IPSec、TLS 等加密传输方式，防火墙、二层三层数据隔离等逻辑隔离通用安全手段，还应建立安全评估系统来评估安装在边缘计算系统中的应用安全以及应用接口与网络之间的安全。

3. 产业及商用发展建议

面向 2020 年 5G SA 初期商用，中国移动计划针对 5G 行业专网建设，实现 QoS 加速、切片、边缘计算、无线专网定制、能力开放 / 对外服务等关键技术，高效推进 5G 产业端到端技术拉通及产业成熟。建议产业提前考虑相关功能推出的测试验证时间。中国移动相关商用发展建议如下：

2020 年 10 月 5G 网络切片具备初期商用能力， 初期考虑基于无线和核心网打通跨厂家流程，支持核心网的自动编排和手动局数据配置，同时终端支持多切片并发。 后续实现无线+传输+核心网端到端拉通 ，完善全领域自动编排/配置，实现切片 SLA 质量保证。

2020 年 11 月 5G 边缘计算能力具备初期商用能力，初期提供数据分流、基本云服务；后续支持 N4 解耦 UPF, 网络能力调用，面向垂直行业的丰富能力调用。

2020 年 12 月 5G 网络支持网络通信相关能力的开放， 后续逐步引入边缘计算、网络切片和 URSP 等技术的能力开放。

4. 结束语

5G行业专网针对不同行业及应用场景，通过差异化的组网服务于行业用户的不同业务需求。本白皮书根据垂直行业多样化的业务场景，提炼出共性需求并映射为明确的5G网络需求，进而提出5G行业专网的组网需求、网络架构、以及网络端到端主要技术要求，希望和业界共同推进5G产业端到端技术拉通及产业成熟。

中国移动期望通过和各产业合作伙伴的通力合作，共同打造具备开放、灵活、安全可靠的面向垂直行业的5G行业专网服务能力，与垂直行业相互促进、协同发展。