



北京 2022 年冬奥会官方合作伙伴

中国联通 5G 政务外网 技术白皮书

China Unicom 5G Private Network for Government Affairs
Technical White Paper

中国联合网络通信有限公司

2022 年 01 月

目录

- 1 序言.....
- 2 政务外网需求洞察.....
 - 2.1 电子政务数字化转型诉求.....
 - 2.1.1 科技驱动政府业务创新.....
 - 2.1.2 数字化提升政府业务效率.....
 - 2.2 政务外网网络安全诉求.....
 - 2.3 政务外网网络建设诉求.....
 - 2.3.1 移动政务外网需求.....
 - 2.3.2 传统政务外网挑战.....
 - 2.3.3 5G 加速政务数字化发展.....
- 3 中国联通 5G 政务外网解决方案.....
 - 3.1 5G 政务外网规划.....
 - 3.2 园区内接入场景.....
 - 3.3 园区外漫游场景.....
 - 3.3.1 单业务漫游互通.....
 - 3.3.2 多业务智能分流.....
 - 3.4 方案差异化优势.....
 - 3.4.1 超越标准，跨省漫游灵活分流.....
 - 3.4.2 超越传统，低成本高安全体验.....
- 4 5G 政务外网案例.....
 - 4.1 山东联通 5G 政务外网案例.....
 - 4.1.1 案例背景.....
 - 4.1.2 解决方案.....
 - 4.1.3 应用成效.....

1 序言

国家电子政务外网（简称政务外网）是按照中办发[2002]17 号文件和[2006]18 号文件要求建设的我国电子政务重要公共基础设施，是政务机关通过统一门户对外发布信息和向社会提供信息服务、业务办理和管理监督等政务活动的公共信息网络。

截至目前，国家电子政务外网已实现区县级以上行政区域全覆盖，乡镇政务外网覆盖率达到 96.1%。中央级政务外网已连接党中央、全国人大、国务院、全国政协、最高人民法院、最高人民检察院、群众团体、民主党派中央、解放军武警总部等主要部门。政务外网全国接入部门共计 40 余万家，接入终端数 600 余万台，承载应用包括公共服务类（如行政审批、价格管理、信息公开等）、政务内部业务类（如协同办公、电子监察、应急指挥、信息报送等）和基础服务类（如视频会议、数据备份、电子邮件等）。目前全国一体化政务服务平台、全国信用信息共享交换平台、投资项目在线审批监管平台、国家数据共享交换平台、公共安全视频、图像共享交换平台等重要跨部门应用均依托政务外网部署和运行。

2021 年广东省人民政府发布《广东省数字政府改革建设“十四五”规划》，提出推动新一代无线政务网络应用要求。聚焦移动政务、公共安全、应急通信、社会管理、重大活动保障等应用场景，在现有政务外网基础上，探索融合 1.4GHz、700MHz、370MHz 专用通讯、5G 切片以及卫星通信技术，补充增强现有政务网络资源，提升政务外网无线服务能力。

2021 年深圳市政府发布《深圳市人民政府关于加快智慧城市和数字政府建设的若干意见》，制定了深圳加快智慧城市和数字政府建设的总体要求、重点任务和保障措施等。提出到 2025 年，

深圳将打造具有深度学习能力的城市智能体，成为全球新型智慧城市标杆和“数字中国”城市典范。

随着政务服务信息化进程的推进，跨地区、跨部门信息共享和业务协调逐渐成为现实，公务人员移动办公需求显著增加。如何不断提升支持服务能力，为推进数字政府建设提供有力信息基础设施支持，成为政务外网建设的最大挑战。

本白皮书针对公务人员移动办公场景的需求，提出 5G 政务外网解决方案，替代传统 VPN 方案，为政务外网移动设备提供随时随地安全访问政务系统的 5G 政务链接，满足政务网客户端在园区内、漫游地同时访问 Internet 和政务业务的诉求。

2

政务外网需求洞察

2.1 电子政务数字化转型诉求

“数字中国”是新时代国家释放信息化数字红利，实现现代化的新战略，“数字政府”是建设“数字中国”的有机组成部分，电子政务是建设“数字政府”的重要抓手，高效、便捷的政务系统建设可以推进政府管理和社会治理模式创新，实现政府决策的科学化、精准化和高效化。

电子政务是政府机构运用云计算、大数据、物联网、人工智能等技术，通过监测、整合、分析、智能响应，实现各职能部门的各种资源的高度整合，提高政府业务的办理和管理效率，同时加强职能监管，使政府更加廉洁、勤政、务实，提高政府的透明度，形成高效、敏捷、便民的新型政府，保证城市可持续发展，为企业和公众建立一个良好的城市生活环境。

电子政务以新一代信息技术为支撑，通过构建大数据驱动的政务新机制、新平台、新渠道，逐渐形成“用数据对话、用数据决策、用数据服务、用数据创新”的现代化治理和服务的新趋势。

2.1.1 科技驱动政府业务创新

科技发展是数字政府发展的基础和技术保障，并在相当程度上推动着数字政府服务能力与服务内容的创新。Gartner 将聊天机器人、区块链、数字孪生政府、数据市场、智能工作空间列为未来五到十年对政府机构影响最大的五项技术。结合中国市场实际，可以看到区块链、人工智能、大数据分析、数字孪生政府，以及持续演进的云服务，都在不断推动数字政府服务内容与形式的

创新。

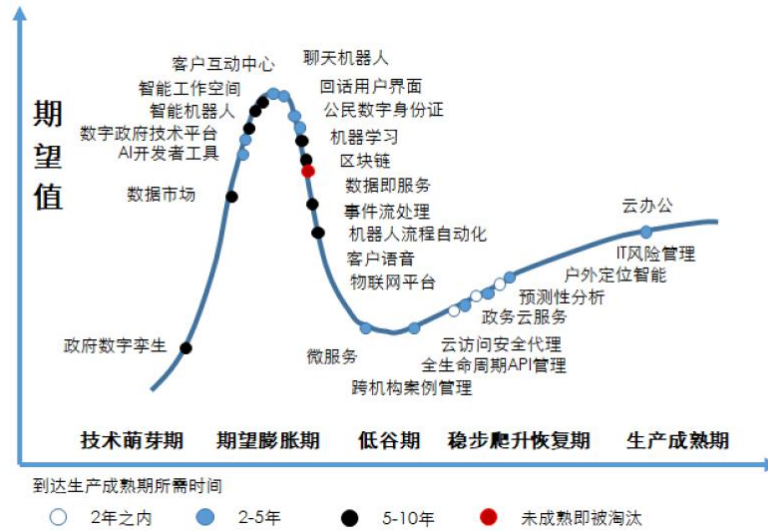


图1：Gartner 数字政府科技技术成熟度曲线

科技发展是数字政府发展的基础和技术保障，并在相当程度上推动着数字政府服务能力与服务内容的创新。Gartner 将聊天机器人、区块链、数字孪生政府、数据市场、智能工作空间列为未来五到十年对政府机构影响最大的五项技术。结合中国市场实际，可以看到区块链、人工智能、大数据分析、数字孪生政府，以及持续演进的云服务，都在不断推动数字政府服务内容与形式的创新。

区块链能够保障数据传输安全，在司法、财税等领域有较大应用前景。2019 年一季度区块链应用行业分布调查显示，金融和政务占比较高，分别为 36%和 34%。政务类应用主要集中在智慧城市数据协作，智慧商圈链上积分，区块链电子发票，商事登记，不动产登记，司法存证取证等方面。目前浙江已经创建了全国首个区块链电子票据平台，实现电子票据全过程“上链盖戳”，保证票据真实性和唯一性。

AI 在数字政府中已经有所应用，未来发展方向主要集中在两个方面：应用场景进一步扩大，

包括人脸识别、走失人口、稽查布控方面等；人工智能与政务大数据结合，赋能政府智能热线、政府决策支撑和公众个性化服务等，推动服务创新。

2.1.2 数字化提升政府业务效率

过往的政务信息化建设，目的都是为了实现既有政务服务的在线办理、自动处理等数字化功能，也就是政务服务的“服务数字化”。而现在，对于已经基本完成省级政务云统一平台建设和数据集中的中国政府，未来重要的发展方向是发挥数据的价值，基于数据融合提供各类智能服务，实现“数字服务化”。

■ 内部互通与融合应用

在引导政府各部门系统迁移至统一政务云平台基础上，进一步打破政府部门间数据孤岛，推动互联互通，强化数据分析、管理等 PaaS 层能力，围绕公众服务、内部管理、社会治理、营商环境等几个重要方向丰富政务应用。

■ 与智慧城市的融合

数字政府在建设过程中，与智慧城市建设趋于融合。两者在建设过程中，存在大量的业务交叉与数据交叉，地方政府中开始出现继承原有大数据基础平台功能与组件，再衍生出系列的通用数据处理能力。这更进一步发挥了数字政府的平台价值，推动智慧城市在各个领域的渗透。

随着政务集约化建设持续深入，政府对外提供政务服务的入口呈现由市级向省级上移趋势，建设类似“粤省事”的省级服务入口成为各省共识。与服务入口向省级上移并统一相对应的，是服务入口的多元化与功能一致化，即全渠道融合体验。政府自有网站、APP、热线、自助服务终端，

第三方流量入口微信（公众号、小程序）、支付宝等，可以看到，移动互联网丰富了政务服务入口，而数据融合与开放则保证了各渠道间功能的一致性，保障“一网通办”。这将成为所有地方政府服务入口建设的方向。

政务服务不再是单向的，完全由政府主导。移动互联网+社交直播+即时通信的飞速发展，对政府机构的反应与决策速度与效率，以及舆论应对能力提出严重挑战。但更重要的是，这为政府机构提供了听取建议与了解需求，吸引更多公众、企业参与数字政府建设的平台。同时，也有效推动政府政务公开、数据开放、组织效率、公关等方面能力的提升。

2.2 政务外网网络安全诉求

电子政务网络，是电子政务的核心基础设施和信息网络平台。电子政务网络由政务内网和政务外网构成，两网之间物理隔离，政务外网和互联网之间逻辑隔离。政务内网主要是政务部门的办公网，政务外网是政府的业务网，主要运行政务部门面向社会的专业性业务和不需要在内网上运行的业务。

根据政务外网所承载的业务和系统服务类型的不同，在逻辑上，将政务外网划分为专用网络区、公用网络区和互联网接入区三个功能域。其中，专用网络区用于实现不同部门或不同业务之间的虚拟专用网（VPN）相互隔离，公用网络区用于实现各部门、各地区互联互通，互联网接入区用于实现各级政务部门面向社会的公共服务需求。

政务外网承载各级政务部门业务协同、社会管理、公共服务、应急联动等面向社会服务的业务应用系统，主要满足中央和各级地方对口政务部门之间信息纵向传输、汇聚及各级政务部门之间、政务部门与公众、企业之间信息交换与共享的需求，与互联网安全联结，支持各级政务部门

面向社会的门户网站。政务外网能支撑多个业务系统的文件、数据、表格、图像、图片等多媒体数据的传输，能够支持视频会议、视频点播、话音等业务。

目前的电子政务外网包含了九个方面的政务支撑能力：

1. 支撑政务部门纵向业务应用：全国政务外网骨干网满足各部门纵向到县的业务应用(IP 电话、视频、数据等)。
2. 支撑跨部门业务应用：通过政务外网城域网实现跨部门的业务应。
3. 支撑构建部门虚拟专网：采用 VPN 等技术建立横向或纵向虚拟专网。
4. 支撑开展面向公众服务的互联网业务：通过政务外网统一互联网出口，支持政务部门开展业务受理、信息发布、视频点播及网上互动等业务。
5. 为已建专网部门提供互联互通网络支撑：已建专网部门间无法互通，若都与政务外网相连,可以使部门间互联互通、业务协同、信息共享。
6. 具备公共应用支撑服务：包括 DNS 系统、共享经济数据库和公务员范文库、邮箱和网络传真、即时通讯和短信、视频点播系统、文件传输与下载等；以及 IDC 托管服务等公共基础应用和服务。
7. 安全可靠的备用网络支撑：为已有专网部门实现备份网络功能，提高部门已建网络可靠性和安全性。
8. 正在构建信息交换与共享平台：目录服务、信息交换共享平台，实现跨地区跨部门业务系统互联互动。

9. 安全防护和应用安全需求的支撑：包括边界安全和终端安全防护、CA 认证、存储备份、应急响应支持等。

电子政务的网络安全与公民隐私、公共秩序以及国家安全等众多敏感信息紧密相关。在电子政务的运行过程中需要使用大量政府的保密信息或公民的隐私信息。

尽管中国电子政务所依赖的技术在持续创新发展，但电子政务的网络信息安全风险亦在不断扩大。网络安全风险主要包括页面遭篡改、数据被窃取、内网被侵入等多方面。政府网站的网络安全隐患层出不穷，容易导致公民信息、金融数据乃至国家安全信息等数据泄露。另外，在跨部门之间的协同共享过程，存在着数据泄露、暴露公众隐私等安全性问题。为了实现人们的远程办公，需要保证人员外出时可以安全访问组织内部网络进行日常操作，并同时确保数据的安全。结合客户的网络状况，有以下几个方面存在安全和可靠性风险：

1. 身份认证安全

现有采用的是较为单一的用户名密码认证方式，安全强度不高，极易遭到窃取、暴力破解造成重要应用系统的越权访问、强行攻破，导致核心数据的泄漏问题。尤其是领导中享有较高级权限的帐号若是遭到盗窃所造成的损失将更为严重。

2. 终端访问安全

一旦远程终端通过 VPN 接入到了总部的网络，总部的安全域延伸到了远程终端。虽然在总部网络中有防火墙、IPS、防毒墙等一系列安全防御设备，但需要接入到总部的远程用户所使用的终端主机普遍安全防御水平都较低，而总部的防护设备又往往不能抵御 VPN 隧道中的威胁。为了保证整体安全防御水平，就需要对接入的终端主机的安全水平采取一定的控制措施。

3. 权限划分安全

总部内网中有众多的应用系统，若是没有采用合理的访问权限控制机制，将重要服务器暴露在所有内网甚至外网用户面前，容易因密码爆破、越权访问等行为导致系统内重要数据的泄漏，同时，开放的权限环境也将给重要的服务器开放了攻击通道，一旦遭到攻击后果将难以估量。所以，对于不同的应用系统需要对访问人员做好细致的访问权限控制。

4. 应用访问审计安全

为了避免重要的信息系统的访问安全风险，做到有据可查，同时也为了了解应用系统的使用情况，需要对应用的访问采取必要的审计措施，了解何时何地何人访问了哪些应用系统。

5. 远程访问速度性问题

影响用户远程办公的最主要因素就是访问速度问题，拖滞的访问速度将大大影响用户的访问体验及办公效率，网络状况、传输数据量及应用的交互方式等等都将影响着速度质量。对于遍布各地远程接入用户而言，线路的运营商环境也多种多样，需要解决跨运营商高丢包导致的速度问题。

2.3 政务外网网络建设诉求

2.3.1 移动政务外网需求

随着电子政务向集约整合方向发展，政务外网的综合性平台效益不断增强，网络范围已从规划的四级覆盖开始向乡镇基层延伸，接入单位由政务部门为主加快向企事业单位和公共机构拓展，承载业务属性也从面向政务效能提升向更为注重有效支撑国家治理现代化演进，由此也涌现出多元化网络服务需求。

- 网络拓展：布线困难边远地区或大量分散机构接入
- 快速接入：需要快速响应的突发业务及临时性业务
- 线路备份：重点业务线路备份或专线中断应急保障
- 移动办公：办公地点不固定或出差人员的终端接入

鉴此，以运营商专线为主的政务外网建设模式面临创新挑战，移动通信技术的迅猛发展恰为有效满足上述需求并进一步强化政务外网公共基础设施作用提供了坚实保障，基于移动通信的无线接入模式以其部署便捷、安全稳定、计费灵活等优势，逐渐成为传统 VPN 专网之外政务外网重要的组网方式。

移动政务外网通过安全接入架构，满足相关机构和人员利用互联网、移动通信网接入政务外网的需求。其中，无线接入平台是利用无线网络、无线 VPDN 等基础网络，面向不具备有线接入条件的政务部门企事业单位公共机构和移动办公人员，提供安全接入政务外网网络或业务的服务平台。

通过服务网关，采用负载均衡技术分别实现 IPSec VPN、SSL VPN 及 L2TP（主要用于无线 VPDN 接入）等网关集群，为用户提供安全接入服务：

IPSec VPN：主要用于非专线接入政务外网的单位，采用网关对网关模式组网以及远程终端接入开展数据上报、视频、会议等非 web 方式访问的业务。专线接入单位发生线路故障时，也可采用网关对网关方式进行应急保障。

SSL VPN：主要用于接入终端以 Web 方式接入政务外网，实现业务系统访问、远程桌面管理、移动办公等。

无线 VPDN：既可用于网关对网关组网，也适用于终端接入。

移动政务外网的关键技术在于确保安全接入基础上，实现接入部门局域网与政务外网基于 MPLS VPN 技术划分的安全域有效对接。

2.3.2 传统政务外网挑战

从安全性来看，政务外网无论采用固定网络还是移动网络，均需经过 Internet 回传，政务网业务数据通过公网传输，存在信息被截取和攻击的安全性问题。

从成本上来看，政务外网采用应用层 VPN 技术，包含安装 VPN 设备、软件授权、维保等费用，成本较高。

从方案性能方面来看，VPN 方案对数据进行加解密处理，存在性能瓶颈，Internet 网络中的时延、网络丢包也导致业务访问速度急速下降，严重影响办公效率，而且不能根据客户的业务需求进行定制化的 QoS 配置，用户体验较差。

2.3.3 5G 加速政务数字化发展

5G 是最新一代蜂窝移动通信技术，是 4G 的升级，是新的无线接入技术和现有无线接入技术的高度融合。它的特点是超高频率，超高频宽，比 4G 的速率更快出一个数量级，对物联网做了优化，具有更低的时延，满足车联网，智能交通，高清视频，虚拟现实的需求。

业务可控性。业务需求的多样性同样为网络带来了巨大的挑战，基于这样的需求，网络切片技术应运而生，通过网络切片，使得运营商能够在—个通用的物理平台之上构建多个专用的、虚拟的、互相隔离的逻辑网络，来满足不同客户对网络能力的不同要求。由此，通过 5G 服务化架构

的网络切片技术，运营商将能够最大程度地提升网络对客户需求、业务场景的适应性，提升网络资源使用效率，优化网络建设投资，构建灵活和敏捷的 5G 网络。

网络安全性。5G 提供更全面的数据安全保护，相对 4G 网络，5G 不仅提供了对网络信令进行完整性保护，还增强了对用户数据的完整性保护。在认证机制方面，5G 网络不仅增强了归属网络对认证的控制，还具有更灵活的可扩展认证协议框架，支撑各种应用场景下的双向身份鉴权和新认证能力。更严密的用户隐私保护，5G 网络对永久用户标识进行加密，有效保护了用户隐私；网间信息保护，新增安全边界保护代理 SEPP，对传输信息进行机密性和完整性保护。

随着 5G 商用步伐的加快以及新基建对 5G 应用的大力推进，利用 5G 实现业务模式智能化、数字化转型的必要性愈发显著。传统专网技术难以满足企业网络的日新月异的信息业务需求。5G 技术凭借通信性能指标的大幅提升，将在工厂、能源、政府、电力、交通、医院、教育等领域，以专属网络的形态赋能行业数字化应用场景创新及信息化业务演进，推动生产要素的数字化智能化转型。在当前阶段，用户对行业网络的需求呈现差异化和碎片化，通用化的网络产品已经无法完全满足需求，需针对行业用户提供量身定制、灵活便捷的网络服务。

5G 专网是一款面向行业客户的一款定制化组网产品，基于 5G 组网、切片和边缘计算等技术，5G 专网为客户提供专属覆盖、网络定制、数据隔离、质量保证的基础连接网络，实现大带宽、低时延、安全可靠的数据传输，满足客户在生产、办公、管理等应用的通信服务需求。5G 专网具有大带宽、广连接、低时延、安全性高等诸多优势。同时，5G 专网具备适用部署区域化、网络需求个性化、行业应用场景化等特点：

- 所谓部署区域化，是指 5G 专网服务的部署范围可根据区域设计，可面向封闭式的使用场景，如制造业园区、港口、矿山等；

- 网络需求个性化，是指对时延要求严苛、可靠性要求高、上行速率需求高、数据安全和隔离要求严格等，5G 专网中的网络切片、边缘计算、NFV/SDN 实现园区网络灵活部署；

- 行业应用场景化，是指 5G 网络为不同行业场景就近部署算力并提供能力开放。

此外，5G 专网可与现有 IT 网络实现兼容互通，网络能力、网络技术也将不断演进升级。

5G 专网产品通过切片配置，提供不同等级的带宽、时延保障等网络能力及服务，此类专网部署模式具备以下特点及优势：

- 服务范围广：中国联通公众网络覆盖的地方均可提供业务切片服务。
- 可靠安全：通过 5G 切片技术，为用户提供逻辑隔离专网的专属管道，实现专网用户与公共用户的业务隔离，互不影响，保障用户业务安全。
- 高灵活性：灵活签约专属切片，可将专网自主管理，自主配置、告警提醒等能力权限开放给专网用户，为用户提供大屏监控、业务管理等灵活自服务能力。
- 可选业务应用：在基础连接能力之上，可为客户提供集群调度、AR 远程协作、5G 专网语音、安全网关等。

基于 5G 技术的政务外网解决方案可有效满足移动办公接入的用户实时连接政务外网的需要，极大提高了网络适用性与便捷程度，为政务外网进一步发挥电子政务公用网络平台综合效能提供了有力支撑。

3

中国联通 5G 政务外网解决方案

中国联通 5G 政务外网解决方案基于 3GPP 标准，通过 ULCL (Uplink Classifier) 本地分流，满足政务网用户在园区内同时访问 Internet 和本地业务的诉求。同时，在政务网用户远程办公场景下，5G 政务外网解决方案超越标准，在漫游场景下也能将园区业务数据分流回政府园区，实现政务网用户随时随地，免 VPN，通过 5G 安全接入政务网络的诉求。

3.1 5G 政务外网规划

用户在政府园区内接入政务外网的场景下，通过专享 UPF/MEC，在更贴近用户的地方提供高性能 5G 服务，保障政务业务永不卡顿。通过 ULCL 本地分流，可以满足用户同时访问互联网和政务外网的诉求。

漫游场景下，为提升政务网客户端远程接入园区网的业务体验，降低政务广域网承载压力，5G 政务外网解决方案实现了同省跨地市、跨省节点之间的互通，将漫游地业务数据直接通过 5G 政务外网回传至园区，实现政务网客户端在全国各地，随时访问园区业务的诉求；通过多业务智能分流，在终端设备侧或网络侧区分园区业务和 Internet 流量，满足政务网用户同时访问 Internet 和园区业务的诉求。

为保障政务外网业务、数据安全性，5G 政务外网不同地市节点之间通过智能城域网实现互联互通，与互联网安全隔离。智能城域网是由中国联通建设的主要用于承载移动业务、政企客户接入、云骨干业务、云网协同业务、物联网承载等业务的，架构简化的融合承载网络。

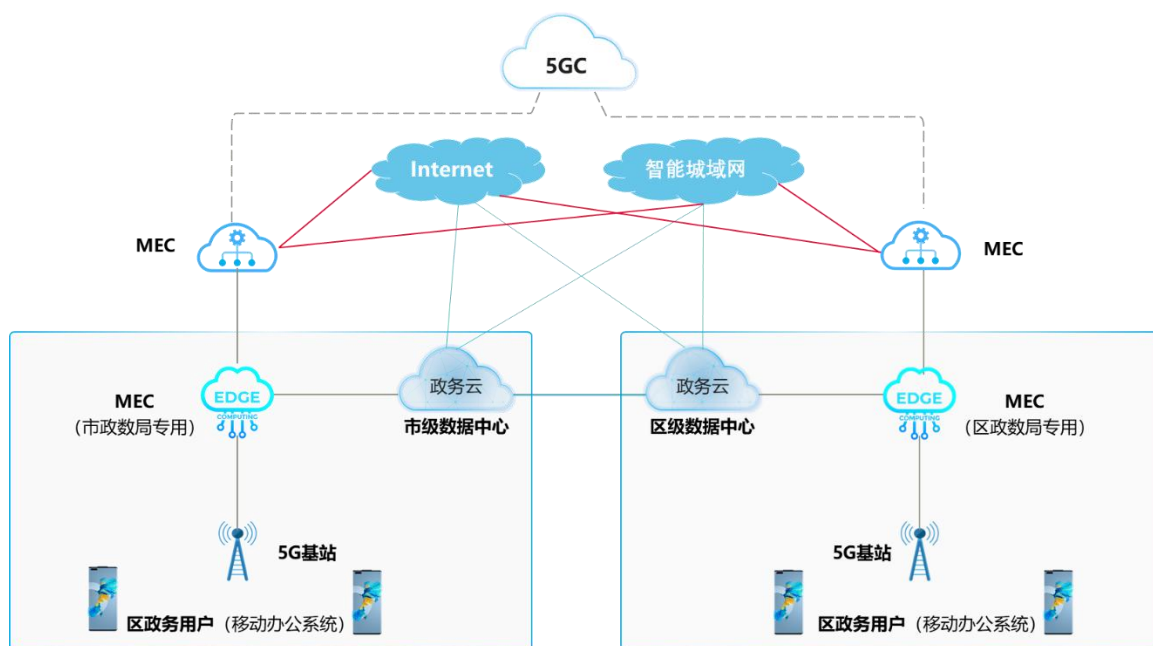


图 2: 5G 政务外网整体规划

政府部门仅需在园区内部署专享 UPF/MEC (Multi-access Edge Computing) , 即可实现政务用户园区内同时高速访问本地业务和互联网; 对于远程办公场景, 用户需要在家里, 或者在出差地安全访问园区业务的诉求, 政府用户无需额外部署 VPN 等设备, 而是基于运营商部署在地市的数据转发节点, 通过随行专线解决方案, 将漫游场景下的园区业务数据通过政务外网安全分流回政府园区, 实现远程用户安全、高速接入政务网络。

用户在园区外同时访问 Internet 和本地业务可以基于标准定义的 ULCL 功能实现本地分流, 根据用户业务流特征, 将访问本地网络的业务流分流到本地业务服务器, 缩短用户访问本地业务的端到端时延, 提升用户业务体验。

对于跨园区漫游、跨地市漫游、跨省漫游场景, 如何将园区业务数据分流回园区 3GPP 标准尚未定义, 为解决漫游场景下的分流难题, 本白皮书超越标准, 创新提出随行漫游解决方案, 将远程办公场景下的政务网客户业务访问流量与互联网业务流量区分开, 并通过中国联通建设的智

能城域网将业务流量安全送回企业园区，实现政务人员随时随地，安全办公。

3.2 园区内接入场景

针对政务外网用户在园区内通过 5G 政务外网接入的场景，部署进政府部门园区内的专享 UPF/MEC 与政务外网相连，同时对园区内的用户流量进行本地分流，实现园区业务与 Internet 业务分流，将访问政务业务的流量转发至政务外网；在园区内访问 Internet 的流量转发至中国联通部署在地市的 5G UPF/MEC，经由地市 UPF/MEC 进行数据转发，实现互联网访问。

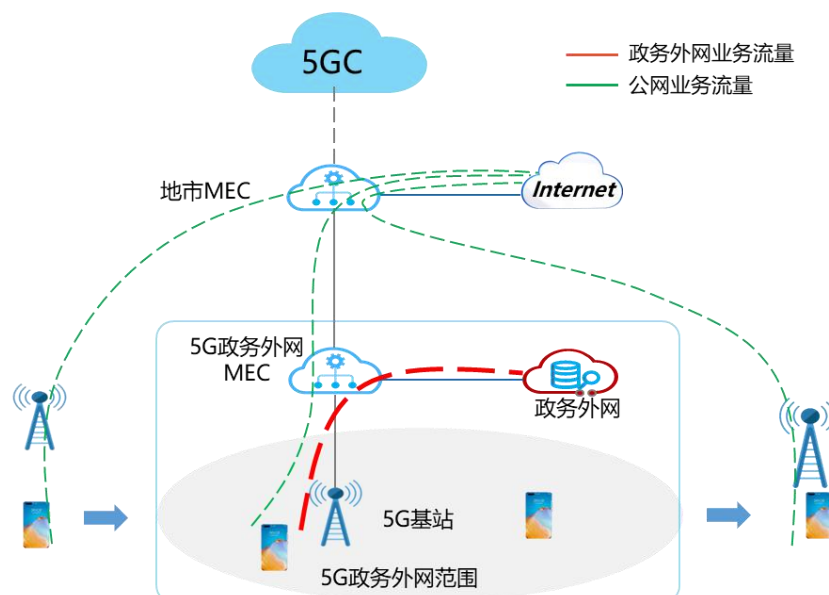


图 3：用户园区内数据业务分流方案

3GPP 针对 5G 用户面的数据分流定义了 ULCL(Uplink Classifier)功能，即上行分流器。该功能可将用户上行数据分流至靠近业务侧的本地数据网络或 Internet，同时还会将来自不同支流上的下行数据聚合后发送给用户。

政务 UPF/MEC 可以基于用户位置，对业务访问进行控制，实现政务外网用户在园区范围外时，仅能访问互联网，进入园区范围内时，通过 ULCL 对业务流量进行识别，Internet 业务分流至

运营商地市 UPF/MEC，访问政务外网的业务流量分流至本地业务服务器。当政务外网用户离开园区区域时，无法触发 ULCL 分流策略，数据流直接通过地市 UPF/MEC 转发到 Internet，无法接入政务外网。

政务外网业务规划方案：

- 政务外网区域：规划政务外网范围，ULCL 策略范围可以根据园区大小灵活进行划分，最大可覆盖整个市区
- 政务用户签约：接入外网的政务用户需要签约政务业务策略
- 政务 UPF/MEC 分流策略：可根据业务诉求灵活配置分流条件

3.3 园区外漫游场景

3GPP 标准尚未支持漫游场景下的 ULCL 分流功能，对于政务办公地点不固定或出差人员的终端接入场景，本白皮书创新提出随行漫游解决方案，实现政务办公人员随时随地安全接入政务网络。

以下章节将 5G 政务外网解决方案分为单业务和多业务两种场景，分别进行介绍。政务场景下，一些移动设备，如警务执法仪，只需要访问园区业务，没有 Internet 访问诉求，此类场景为单业务场景。而公务人员出差、远程办公使用的办公设备，如手机、平板电脑等通用终端，既需要访问园区业务，又需要访问 Internet 的多业务场景，这类场景成为多业务场景。

3.3.1 单业务漫游互通

针对只有单一园区业务的场景，例如警务执法仪等移动设备，超级漫游方案可实现终端设备

全国范围内的漫游互通。终端漫游出归属地后访问园区业务时，接入漫游地由运营商部署的地市 UPF/MEC，业务流量由漫游地 UPF/MEC 直接回传至归属地地市 UPF/MEC，经由地市 UPF/MEC 转发至园区专享 UPF/MEC，地市间 UPF/MEC 通过智能城域网实现互通，实现业务流量不出内网，无需经过 Internet 回传。

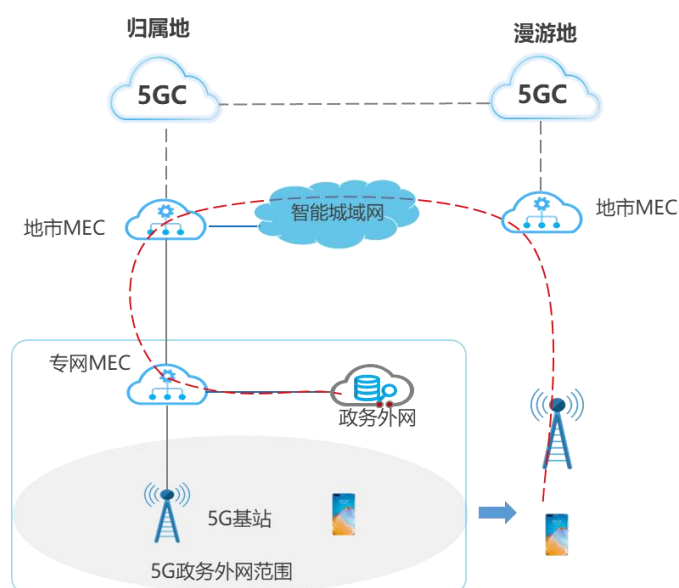


图 4：单业务场景漫游方案

3.3.2 多业务智能分流

对于政务用户办公使用的手机、平板电脑等通用终端，既需要访问园区业务，又需要访问 internet 的多业务场景，随行漫游方案提出终端侧分流和网络侧分流的方案，实现园区内、省内、跨省同时访问园区业务和 Internet 业务的便捷体验。

3.3.2.1 终端侧分流

终端侧分流方案 UE (User Equipment) 在应用程序侧就对业务流做出识别，进行业务区分，简化网络配置。但终端侧分流方案需要为园区业务定制应用程序，在应用程序侧进行配置，以实

漫游地政务用户访问互联网和政务外网的业务流量在漫游地网络侧进行识别，由运营商部署在漫游地的 UPF/MEC 作为 ULCL 分流锚点，对不同业务流量进行识别、分流处理，访问互联网的流量直接在漫游地接入互联网；访问政务内网的流量转发至归属地 UPF/MEC，由归属地 UPF/MEC 回传至园区内专享 UPF/MEC，实现政务业务访问。

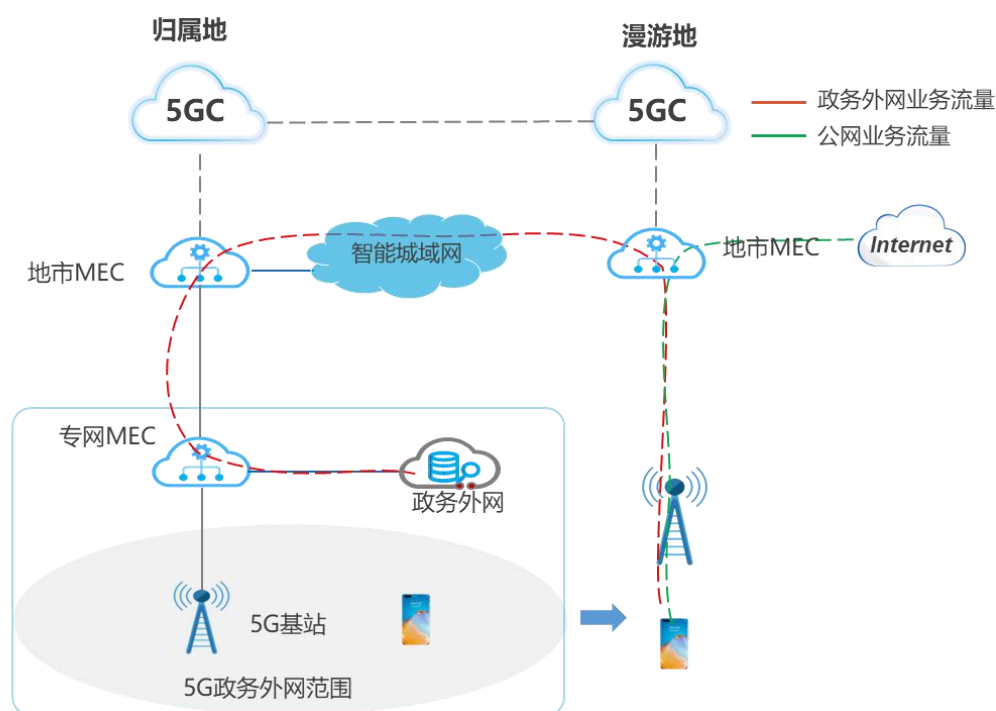


图 6：多业务场景网络侧分流-Internet 流量本地卸载

网络侧分流方案将互联网业务访问直接在漫游地接入互联网，实现 Internet 流量本地卸载，减少互联网业务流量的传输路径，提升政务用户在漫游地访问互联网时的体验。

从方案具体实施层面来看，实现 Internet 本地卸载需要在漫游地为用户进行网络地址转换，需要漫游地运营商与归属地运营商进行协调，在漫游地核心网侧做相应配置，因此运营商在建网时需提前考虑跨地市、跨省网络部署、协调问题。

3.4 方案差异化优势

3.4.1 超越标准，跨省漫游灵活分流

多业务场景下，用户在园区接入同时访问 Internet 和本地业务可以基于标准定义的 ULCL 功能实现本地分流。但是对于跨园区漫游、跨地市漫游、跨省漫游场景，如何将园区业务数据分流回园区标准尚未定义。5G 政务外网超越标准，替代传统 VPN 方案，为政务外网移动设备提供随时随地安全访问政务系统的 5G 政务外网，满足政务网客户在园区内、漫游地同时访问 Internet 和政务业务的诉求。

3.4.2 超越传统，低成本高安全体验

从安全性来看，5G 政务外网方案通过 5G 政务外网实现漫游地业务流量无需经过 Internet 回传，实现政务网业务数据不出私网，提供更高安全性的解决方案。

从成本上来看，5G 政务外网方案替代应用层 VPN，节省 VPN 设备、软件授权、维保费用。

从方案性能方面来看，VPN 方案对数据进行加解密处理，存在性能瓶颈，Internet 网络中的时延、网络丢包也导致业务访问速度急速，严重影响办公效率。超级漫游方案提供的 5G 政务外网可通过 QoS，提升业务体验，在某项目的实测数据中，5G 外网对比应用层 VPN 方案，达到下载速率近 2 倍提升的效果。

对比项	VPN 方案	5G 政务外网方案
安全	园区业务数据经过	数据不出私网

		Internet	
成本		硬件+软件授权+维保	节省 VPN 投资
用户 体验	用户登录	5s	无需单独输入账户密码
	下载速率	100+Mbps	200+Mbps

表 1: VPN 方案与 5G 政务外网方案对比

4

5G 政务外网案例

4.1 山东联通 5G 政务外网案例

4.1.1 案例背景

山东省政务外网是政务办公的统一平台，纵向覆盖省、市、县（区）、乡、村，实现贯通政府业务部门的四级信息通道。横向连接各级政府部门，及各级党委、人大、政协、法院和检察院等政务部门的办公平台，满足各级政务部门经济调节、市场监管、社会管理和公共服务等需求，实现各级政务部门的互联互通、信息共享、数据交换和业务互动。

传统的政务移动办公是使用的 4G VPDN 技术，随着用户数量的增加，业务场景的丰富，出现了文件下载速度慢、系统反应时间长、观看视频不流畅等多种问题。随着 5G 网络建设的不断加快，5G 终端在移动办公中的占比越来越高，政务办公人员希望能够在移动办公中感受到 5G 带来的高速、便捷和优质的服务。山东联通发挥网络和技术优势，基于政务外网，为山东省各级政务部门建设了一个方便好用、技术先进、安全可靠的 5G 政务外网。

山东联通 5G 政务外网分为两期建设。一期实现覆盖地市的场景，将整个济南市定义为办公区，满足了公务人员在工作地、会议场所、宿舍区等多个场景的移动办公需求。开通 5G 政务外网手机套餐后，不论在办公区内，还是办公区外，公务人员都不需要在移动终端上修改任何配置，就可以在访问政务外网时，同时关注微信、微博、钉钉等互联网应用。二期将实现 5G 政务外网覆盖全省，满足全省公务人员移动办公诉求。

4.1.2 解决方案

山东联通发挥网络优势，基于政务外网的行政服务域，为山东省各级政务部门建设了一个方便好用、技术先进、安全可靠的一体化移动办公平台（简称“山东通”平台）。“山东通”平台满足了全省范围内跨层级、跨部门的互联互通、数据共享、协同治理、一体化服务的移动办公需求。

山东联通 5G 政务外网通过在客户的机房部署两套 5G 政务外网的专用 UPF/MEC（实现业务容灾），与“山东通”平台对接，通过“山东通”平台接入政务外网。公务人员开通 5G 政务外网手机套餐，签约公用接入点，配置 5G 政务外网业务规则，实现不换卡不换号同时访问政务外网和互联网。

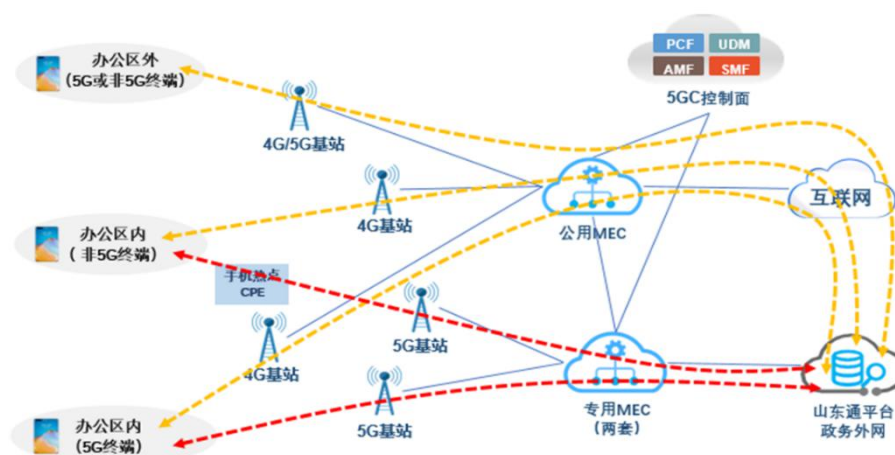


图 7：山东政务外网示意

1. 办公区内使用 5G 终端

在 5G 覆盖区，通过专用 UPF/MEC 访问政务外网。在 4G 覆盖区，通过公用 UPF/MEC 访问互联网，再通过互联网访问政务外网。

2. 办公区内使用非 5G 终端

在 5G 覆盖区，利用 5G 手机热点或 CPE 接入 5G 网络，通过专用 UPF/MEC 访问政务外网。在 4G 覆盖区，通过公用 UPF/MEC 访问互联网，再通过互联网访问政务外网。

3. 办公区外使用 5G 或非 5G 终端

在 4G 或 5G 覆盖区，通过公用 UPF/MEC 访问互联网，再通过互联网访问政务外网。

4.1.3 应用成效

基于 5G 政务外网，为全省政务部门打造了一张网、一平台、多应用、全服务的云网边端业一体化的移动办公服务。一张 5G 政务网，实现办公、会议、通信、学习等应用的一点接入，办公区域全覆盖；一个山东通平台，实现全省范围内跨层级、跨部门的互联互通、数据共享、协同治理、一体化服务的移动办公需求；多种应用包括公文批阅、视频会议、学习培训、指挥调度、视频监控、数据管理等应用；全场景服务包括全天候网络监控和故障处理，全终端接入安全管理，全业务通信安全隔离，全方位满足客户需求。

5G 政务外网带来了三大提升。第一，工作效率的提升，操作简单，使用便捷，政务办公效率提高了 20%；第二，使用感知的提升，实现了工作学习两不误，视频应用更流畅，公务人员更愿意使用。第三，数字政府建设的提升，将六大机关事项实现数字化办公，提升了机关运行效能和数字化水平。

该案例受到业界广泛关注与认可。2021 年获得第四届“绽放杯”5G 应用征集大赛总决赛优秀奖。

《中国联通 5G 政务外网技术白皮书》编写委员会

总策划:

薛吉平、冯兰晓、刘北阳、王睿

主编:

王楠、陈丹、赫罡、胡广金、张勇

编委会成员:

卢志燕、肖羽、郝晶、高功应、张小勇、王勇、张欣、侯海敬、潘峰、尹鹏军、马钦德、陈坚光、陈沁茗、傅成龙、钱昊、马春燕、郭传光、张亮