

# 云计算赋能政企通信网络升级的路径探索

李雪婧

中国移动通信集团吉林有限公司 吉林长春 130103

**摘要:** 数字经济时代政企通信网络是数字化转型的基础设施,但是存在着带宽不足、运维复杂、安全风险高这些瓶颈。本文根据云计算技术特性,研究云计算如何赋能政企通信网络升级的核心逻辑,从云网协同架构重构、智能运维体系搭建、安全能力内生融合、多元技术协同赋能四个方面梳理出升级路径,用典型案例来验证路径的可行性,为政企单位依靠云计算实现通信网络高质量升级提供实践参考。

**关键词:** 云计算; 政企通信网络; 云网协同; 智能运维; 网络安全

## 引言

目前全球数字化转型的浪潮不可阻挡,政企单位的数字化业务规模越来越大,远程协同办公、物联网终端接入、多云应用部署等新的需求不断涌现出来,传统的以硬件为中心、边界固定的通信网络架构已经不能满足这些需求。从政策角度来说,我国东数西算工程、双千兆网络协同发展计划等政策不断加大投入,政企通信基础设施升级。但是政企通信网络在实践中存在资源调度僵化、运维成本高企、安全防护滞后等问题。云计算依靠弹性伸缩、资源池化、按需服务等优势,给破解以上难题赋予了有效的支撑。本文主要从云计算促进政企通信网络升级的路径入手进行研究,有理论价值和实践意义。

## 一、云计算赋能政企通信网络升级的核心逻辑

### 1. 打破传统网络架构桎梏

传统的政企通信网络大多采取分布式硬件部署的方式,核心路由、防火墙等设备要逐点配置,存在资源利用率低、扩展能力弱的缺点。传统政企网络带宽利用率一般在30%以下,新分支的上线需要数周的时间才能完成设备的部署和调试。云计算通过资源池化技术把网络硬件资源抽象成虚拟资源池,实现计算、存储、网络资源的集中调度与弹性分配,消除了传统网络“烟囱式”架构的资源壁垒。利用云平台可以将分散的企业和政府分支机构资源聚合起来,按照业务需求动态分配带宽和算力,提高资源利用率<sup>[1]</sup>。

### 2. 重构网络服务交付模式

云计算使政企通信网络由原来的硬件交付方式转变为现在的服务交付方式。传统网络服务要依靠物理设备的采购和部署,服务开通时间长、定制化能力差;云计

算支持网络功能虚拟化(NFV),把防火墙、路由器等传统硬件功能转变成虚拟网络功能(VNF),依靠云平台达成分钟级的部署以及灵活的迭代。同时云计算按需付费的方式也降低了政企单位网络建设的初始投入,避免了资源过多造成的浪费,适合于中小企业轻量化、低成本的网络升级需求。

## 3. 强化网络安全与运维能力

数字化转型背景之下,政企通信网络所面对的网络攻击手段越来越复杂,数据安全合规的压力也越来越大。云计算平台有规模化安全资源的整合能力,可以利用云安全网关、下一代防火墙、零信任网络访问(ZTNA)等技术来搭建起全链路的安全防护体系。另外,基于云计算的智能运维(AIOps)技术可以对网络流量、性能指标等大量的数据进行实时的采集和分析,从而实现对故障的准确预测和快速定位,大大降低运维难度和人力成本,提高网络运行的稳定性。

## 二、云计算赋能政企通信网络升级的关键路径

### 1. 架构重构: 构建云网协同一体化体系

云网协同是云计算赋能政企通信网络升级的主要途径,即云计算和通信网络深度融合、协同调度。一方面推进网络功能云化改造,采用软件定义广域网(SD-WAN)技术代替传统的MPLS专线,用云平台实现广域链路的智能选路和动态调度,提高跨区域、跨云端的网络连接效率。跨国集团可以利用SD-WAN技术整合互联网、专线等各种链路资源,实现海外分支和国内核心系统低时延互联,把网络时延从500ms降低到80ms左右。另一方面,创建统一云网管理平台,对物理网络、虚拟网络、云资源实施集中管理,支持业务需求同网络资源的智能对接,达成“云随需动,网随云调”。运营商主导

的云网融合方案已经形成了成熟的模式。中国移动移动云采用网云一体的架构，在变电站、配电房等重要节点部署微型云节点，对电力物联网的数据进行就地处理，故障定位时间由原来的4小时缩短到现在的1.2小时，效率提高了70%。政府部门可以依靠政务云平台，创建起覆盖省市县三级的政务云网体系，促使跨部门的数据共享以及业务协同，进而改善政务服务“一网通办”的效率<sup>[2]</sup>。

## 2. 运维升级：搭建智能运维与自动化管理体系

传统的政企通信网络运维主要依靠人工操作，存在着响应慢、误差大、成本高的弊端。以云计算为基础的智能运维体系，可以使得运维模式由原来的被动响应转变为现在的主动预判。首先创建全域数据采集分析平台，把网络设备、服务器、云应用等各部分的数据融合在一起，并用AI和ML算法来找出数据间的关联性，准确找到网络异常行为和潜在的故障风险。第二推进运维流程自动化，用脚本编排、智能调度等方式来实现网络配置、故障修复、性能优化等操作的自动化执行，减少人工干预<sup>[3]</sup>。犀思云智能WAN方案依托全链路智能化运维能力，将故障定位时间从小时级精准压缩至分钟级，核心业务保障水平可达99.99%。大型政企单位可以搭建自己的智能运维平台，中小企业可以采用云服务商提供的轻量级运维服务，从而降低运维成本。同时建立标准化运维管理规范，确定云网资源运维的职责分工、操作流程、安全规范，保证智能运维体系的正常运转。

## 3. 安全融合：构建内生安全防护体系

依靠云计算创建内生安全防护体系，就要达成安全能力同网络架构的深度整合，而不是传统的“事后补丁”式防护。一是采用零信任安全架构，以永不信任、始终验证为原则，用身份认证、权限控制、行为审计等方式对网络访问进行精细化的控制，适合远程办公、多终端接入等场景的安全需求<sup>[4]</sup>。某省电子政务云平台用自研的棱镜安全管理系统实现数据访问全程留痕、异常操作实时阻断，符合等保2.0三级要求，运行两年来没有发生数据泄露事件。二是利用云安全服务的规模化优势，采用安全即服务（SECaaS）模式，根据需要调用云服务商提供的病毒查杀、漏洞扫描、数据加密等安全服务，降低安全建设与运维成本。除此之外，对金融、政务等高敏感度的领域要建立国产化的信创云安全体系。全国性银行与移动云深度合作，依托鲲鹏芯片、昇腾算力搭建全栈国产化云计算平台，通过12项创新技术完成核心系统从X86到ARM架构的迁移，不仅实现业务连续性达99.999%、交易处理峰值提升35%的优异成效，更顺

利满足国产化替代要求，保障了核心业务稳定运行。

## 4. 技术协同：推动多元新兴技术融合赋能

云计算需与5G、边缘计算、量子通信等新兴技术深度协同发展，才能充分释放技术叠加效应，精准匹配政企通信网络多样化升级需求。其一，5G与云计算深度融合，依托5G大带宽、低时延、广连接的核心特性，结合边缘云节点部署模式，可精准适配工业互联网、智慧交管等低时延场景的技术支撑需求。例如，某省会城市依托5G网络与边缘云计算技术构建视频流AI分析体系，将违法驾驶行为识别时长从5秒压缩至0.3秒，主干道通行效率提升25%，显著提升交通管理智能化水平。其二，边缘计算与云计算协同联动，通过边缘节点承担实时数据处理、本地业务响应等即时性任务，云计算平台聚焦大规模数据存储、复杂数据分析等核心工作，形成“边缘响应、云端决策”的协同架构，有效满足工业制造、物联网等场景对低时延、高可靠的核心诉求。同时，需积极探索量子通信等前沿技术与云计算的融合应用路径，其中量子密钥分发（QKD）技术可大幅提升云平台数据传输的加密等级。据Gartner预测，截至2030年，65%的跨国企业将采用混合量子-经典加密方案，进而全面强化政企通信网络的安全防护能力。此外，IPv6规模化部署、分段路由（SRv6）等新型协议的落地应用，能够显著提升云网融合架构的扩展性与灵活性，为后续网络升级迭代预留充足空间。

## 三、案例分析：云计算赋能政企通信网络升级的实践成效

### 1. 金融行业：信创云驱动核心交易系统升级

全国性银行核心交易系统依靠国外的芯片及操作系统进行，不能完成国产化替换。依托与移动云的合作创建起全栈国产信创云平台，用鲲鹏芯片和昇腾算力来无感迁移核心交易系统到ARM架构。项目实施之后，核心系统的交易处理峰值由原来的每秒8000笔提高到现在的10800笔，性能提高了35%，业务连续性保证达到99.999%，每年的停机时间不超过5分钟。依靠云平台搭建起来的零信任安全体系，符合金融行业严格的数据安全合规标准，给其他金融机构网络升级赋予了可复制的信创解决办法。

### 2. 制造业：云网协同支撑智能化生产

大型汽车工厂实施生产线智能化改造的时候，车间设备互联、实时数据传输、AI质检等场景的网络支撑问题就成为要解决的问题。采用SD-WAN+边缘云的云网协同方案，在车间部署边缘云节点，实现设备数据的就

近采集和分析,用SD-WAN技术实现边缘云和企业私有云的高速互联,保证生产数据和AI模型的实时同步。方案实施以后,缺陷识别模型的迭代周期由原来的2周缩短到现在的3天,检测准确率由原来的82%提高到现在的99.7%,并且通过算力动态调度,在白天保证在线检测算力供给,夜间集中资源进行模型训练,算力资源利用率由原来的50%提高到现在的85%,大大降低了生产成本。

### 3. 政务领域:电子政务云网体系提升服务效能

推进一网通办改革的时候要破解跨部门数据壁垒、政务系统响应速度慢等难题。依靠移动云创建省级电子政务云网一体化平台,把全省300多个政务系统整合起来,达成政务数据的集中存储和共享,用SD-WAN技术实现省市县三级政务部门的高速互联,改善网络传输路径。平台运行之后,跨部门审批时间从5天缩短到2小时,政务服务效率得到很大的提高;平台自身的网络安全防护系统可以满足等保2.0三级的要求,保证政务数据的安全可控,为数字政府的网络支撑打下良好的基础。

## 四、云计算赋能政企通信网络升级的挑战与应对

### 1. 核心技术自主化不足风险

目前我国政企通信网络升级依靠的很多高端芯片、操作系统等核心技术都存在“卡脖子”的风险。由于受到国际地缘政治冲突和技术封锁的影响,核心硬件供应链稳定性会面临严峻考验,进而影响到升级进程的连续性以及安全性<sup>[5]</sup>。应对措施,一方面加大信创产业专项投入,鼓励企业同科研院所协同攻关,推进芯片、操作系统、数据库等核心技术的自主研发和产业化落地,创建全栈国产化云网生态;另一方面创建多元化供应链体系,积极拓展国内外优质供应商资源,削减对单一技术或者供应商的依靠,加强关键软硬件备品备件的战略储备,创建供应链应急响应机制,保证网络升级和运行的连续性。

### 2. 安全合规与数据治理难题

云网融合场景中,数据跨云端、跨区域、跨部门的传输越来越频繁,数据流转链路变长,参与主体变多,造成数据主权界定不清,隐私泄露风险增大,跨境数据合规难度增加等问题突出。应对措施有完善数据安全治理体系,建立政企全业务场景的数据分类分级标准,创建数据全生命周期安全管理流程,即从数据采集、传输、存储到销毁的全流程安全管控,利用数据加密、联邦学习、可信执行环境等技术手段,达到数据可用不可见的目的,在保证数据安全的前提下,高效推进跨主体数据

共享,加强与监管部门的常态化协同,提前开展合规评估,保证云网升级方案全面符合《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的要求。

### 3. 技术融合与人才短缺问题

云计算同政企通信网络的深度结合,既要有对云计算、云网协同等前沿技术了如指掌的人才,也要有对政企行业业务流程了如指掌、对行业监管要求了如指掌的人才。此类人才匮乏严重,现有的运维团队的技术储备不能满足云网融合升级的要求,也成了影响其更新进程的重要因素。应对措施:政企单位主动同高校、职业院校开展产教融合,共建特色专业或者实训基地,定向培养适合岗位需求的复合型人才;联合云服务商开展定制化的技术培训,搭建内部技能提升平台,全面提升现有运维人员的云网融合技术应用和故障处理能力;通过优化薪酬福利、搭建职业发展通道等人才引进政策,精准吸引行业高端人才,组建专业的云网升级与运维核心团队。

## 结语

云计算给政企通信网络的升级提供了革命性的技术支撑,网络架构从以前硬件集中式变成了现在的云网协同式,网络运维方式从以前的手工被动应对变成智能主动预测。由于5G、边缘计算、量子通信等技术的不断发展,云计算赋能政企通信网络升级将会越来越智能、越来越安全、越来越开放。政企单位要立足于自身的业务需求,把握云网协同的主要方向,冲破技术、安全、人才等瓶颈,促使通信网络由“成本中心”变为“业务引擎”,为数字化转型赋予有力支撑。并要加强产业协同,推进核心技术的自主研发,创建安全可控的云网生态,促进数字经济高质量发展。

## 参考文献

- [1]徐以蒙,董春辉,万昕.通信运营商政企网络安全能力技术架构[J].网络安全技术与应用,2025,(12):118-120.
- [2]李秋萍.通信运营商企业政企用户欠费管理策略[J].财讯,2024,(16):83-85.
- [3]边海涛.基于云计算的移动通讯电子信息存储与共享平台设计[J].软件,2024,45(08):102-104.
- [4]李欣然.云计算背景下中兴通讯公司财务共享模式研究[J].中阿科技论坛(中英文),2023,(06):66-70.
- [5]张崇术.基于政企客户融合通信应用的RCS标准化建议[J].数字通信世界,2020,(03):277.