政务外网IPv6
演进技术白皮书(2021)

国家电子政务外网管理中心办公室

前言
FOREWORD

IPv6（Internet Protocol Version 6，互联网协议第六版）是互联网升级演进的必然趋势、是网络技术创新的重要方向、是网络强国建设的基础支撑。2017年，以习近平同志为核心的党中央作出推进IPv6规模部署行动的战略决策。按照中央网信办、国务院办公厅的工作部署，国家电子政务外网已开始启动IPv6改造工作。“十四五”时期，我国将加快数字化发展，大力推进数字政府建设。政务大数据、城市治理、专网融合、移动办公等来自制度、技术、场景的变革要素正在加速涌现，持续挑战政务外网IPv4服务能力。为贯彻落实党中央决策部署，有效应对数字时代的业务挑战，需要加快政务外网IPv6演进。

本白皮书旨在为政务外网全面向IPv6演进提供分析和指导，给出基于IPv6的新一代政务外网建设思路和演进路径，为地方政务外网IPv6改造提供参考。

本白皮书由国家电子政务外网管理中心办公室和华为技术有限公司联合编写，白皮书中的广西、广东、中山案例材料，分别由广西壮族自治区信息中心、广东省政务服务数据管理局、中山市政务服务数据管理局提供。

目录 CONTENTS

01 政务外网发展现状

国家电子政务外网是按照《国家信息化领导小组关于我国电子政务建设的指导意见》（中办发［2002］17号）、《国家信息化领导小组关于推进国家电子政务网络建设的意见》（中办发［2006］18号）等中央文件要求建设的我国电子政务公共基础设施，主要承载各级政务部门经济调节、市场监管、社会管理、公共服务、生态保护、协同办公等非涉密的业务应用，支撑跨部门、跨层级、跨区域数据共享和业务协同。国家电子政务外网为非涉密网络，与互联网逻辑隔离。

1.1 建设历程

2005年8月，国家电子政务外网一期工程开始启动；2006年9月开始承载业务；2010年10月，国家信息中心加挂“国家电子政务外网管理中心”的牌子，政务外网正式开始承载业务；2014年底，全国县级以上行政区域基本实现全覆盖。目前，国家电子政务外网二期工程建设已经基本完成。

1.2 承载业务

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。

1.3 技术路线

网络架构

国家电子政务外网由网络平台和部门电子政务外网构成，网络平台分为中央级、省级、市级、县级四级，各级网络平台包含广域网、城域网、数据中心等部分。网络平台采用统一规划、分级负责的原则进行建设，中央级网络平台由国家电子政务外网管理中心负责建设，省级及省以下网络平台由地方政府相关部门负责建设。部门电子政务外网按照要求接入本级网络平台。

网络平台分为公用网络区和互联网接入区。公用网络区提供跨部门业务互通功能；互联网接入区向互联网用户提供服务。

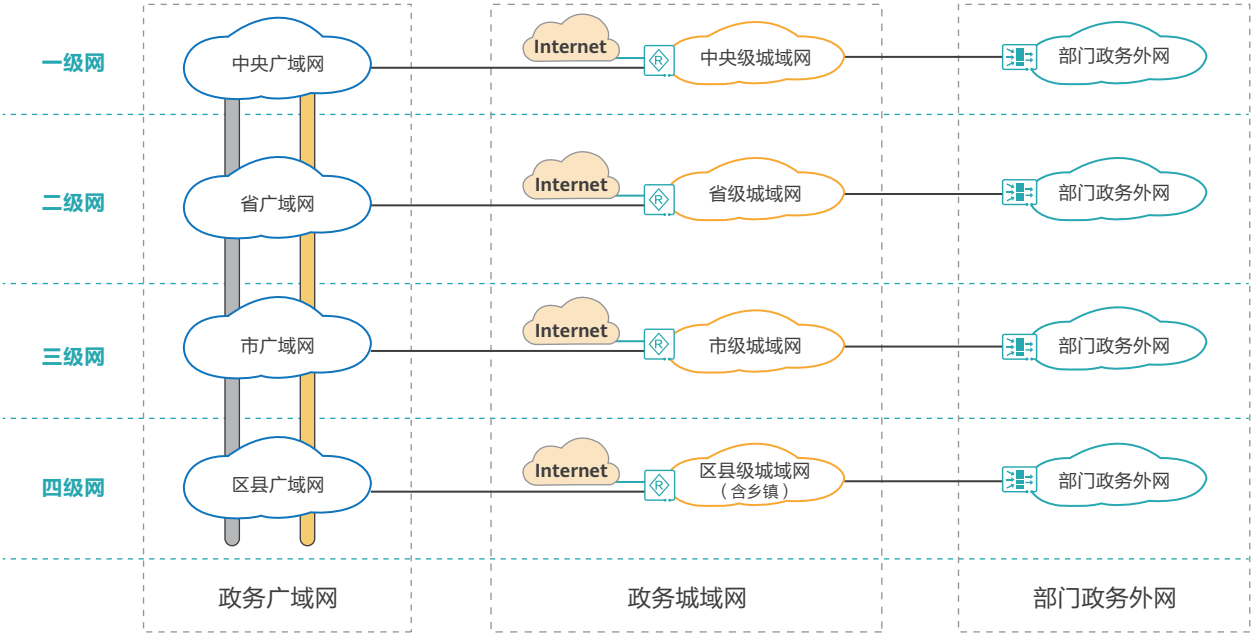


图1-1 电子政务外网基础网络架构

地址分配

政务外网IPv4地址分为全局地址、地方地址，全局地址用于中央级网络，以及地方网络的跨省访问；地方地址用于地方网络。国家电子政务外网管理中心统一申请64个B类公有地址，用于政务外网全局地址。全局地址在全网范围内通告，路由可达。地方地址在省网范围内通告，不向省外通告，仅在本省内路由可达。地方终端出省访问需转换为全局地址。

2015年，国家电子政务外网管理中心发布《国家电子政务外网IPv4地址规划》，指导各级电子政务外网地址规划。政务外网地址规划采取“全局地址统筹规划、地方地址分省复用”的混合组网原则。国家电子政务外网管理中心负责政务外网全局地址总体规划和管理。省级政务外网建设运维单位负责全省（区、市）全局地址段的具体分配工作，同时负责地方地址的规划和管理。

网络安全

政务外网安全等级保护的目标是通过推进安全等级保护工作，加强政务外网整体的安全防护能力，确保国家电子政务外网全网的安全性、可靠性和一致性，保证所承载的各级政务部门电子政务业务的畅通和安全。

中央、省、地（市）政务外网均应达到安全等级保护2.0(GB/T 22239-2019)第三级要求，并每年开展等保测评工作。

政务外网安全等级保护首先是网络防护，保证所承载各级政务部门信息系统的网络畅通，抵御病

毒和人为的攻击。在所管辖的网络边界范围内，管理好统一的互联网出入口、安全接入平台，并做好各部门政务外网接入边界的访问控制，具备跨区域数据安全交换能力，确保跨部门数据在安全的前提下进行共享交换。

另外，政务外网还需要具备统一的安全监测、分析和预警能力。统一安全监测依托安全监测平台，平台采用中央、省二级架构，每级单位单独建设安全监测平台，具备完整的数据采集预处理、数据分析、展示与应用等功能，各级平台可按照本级安全监测需求来建设专项监测。

1.4 政策环境

1.4.1 IPv6相关政策环境

IPv6为我国网络设施升级、技术产业创新、经济社会发展提供了重大契机，加快推进IPv6规模部署是我国新一代信息基础设施升级的必然要求，也是下一代互联网发展的必由之路。为进一步推进国内IPv6下一代互联网发展，2017年11月，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》（厅字〔2017〕47号，简称《行动计划》），明确提出了未来5到10年我国基于IPv6的下一代互联网发展的总体目标、路线图、时间表和重点任务。《行动计划》是加快推进我国IPv6规模部署，促进互联网演进升级和健康创新发展的行动指南。

2021年，《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》再次强调，全面推进互联网协议第六版（IPv6）商用部署。

2021年7月，中央网信办、国家发展改革委、工信部联合印发《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》（中网办发文〔2021〕15号），要求推动国家电子政务外网、地方政务外网、政务专网等IPv6改造。推动政务数据中心、政务云平台、智慧城市平台IPv6改造。推动新建政务网络及应用基础设施全面部署IPv6，探索开展政务网络及应用IPv6单栈化试点。

1.4.2 政务外网相关政策环境

党中央、国务院高度重视数字政府建设，并将其作为实现国家治理体系和治理能力现代化的战略支撑，提出以电子政务为抓手，推进政府管理和社会治理模式创新，实现政府决策科学化、社会治理精准化、公共服务高效化，并陆续发布了相关政策法规，为电子政务发展提供了良好的政策环境。

为了统筹国家政务信息化工程建设，推动政务信息系统整合共享，2017年5月，国务院办公厅印发《政务信息系统整合共享实施方案的通知》（国办发〔2017〕39号），明确要求完善国家电子政务外网，拓展网络覆盖范围，具备跨层级、跨地域、跨系统、跨部门、跨业务的支撑服务能力，满足业务量大、实时性高的网络应用诉求，构建“大平台、大数据、大系统”，形成覆盖全国、统筹利用、统一接入的数据共享大平台，除极少数特殊情况外，政府各类业务专网都要向国家电子政务内网或外网整合。

为深化“放管服”改革，进一步优化政务服务，2018年7月，国务院印发《关于加快推进全国一体化在线政务服务平台建设的指导意见》（国发〔2018〕27号），强调各级政务服务平台原则上统一依托国家电子政务外网构建，要拓展国家电子政务外网覆盖范围，加强网络安全保障，满足业务量大、实时性高的政务服务应用需求。推动各地区和国务院有关部门非涉密业务专网与电子政务外网对接整合。2020年9月，国务院办公厅印发的《关于加快推进政务服务“跨省通办”的指导意见》（国办发〔2020〕35号）强调，加强全国一体化政务服务平台“跨省通办”服务能力，进一步加强市县政务服务平台建设，加快实现网上政务服务省、市、县、乡镇（街道）、村（社区）全覆盖。通过全国一体化政务服务平台，垂直业务系统与地方政务服务平台互联互通、协同办理。深化“全程网办”，拓展“异地代收代办”，优化“多地联办”，实现申请人“单点登录、全国漫游、无感切换”。

为进一步推动政务数据的整合共享，全面提高数字化政务服务效能，《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》进一步强调，推动政务信息化基础设施共建共享，提高数字化政务服务效能；推进新型智慧城市建设，将物联网（Internet of Things，IoT）感知设施、通信系统等纳入公共基础设施统一规划建设，推进市政公用设施、建筑等物联网应用和智能化改造；推进“上云用数赋智”行动，集约建设政务云平台和数据中心体系，推进政务信息系统云迁移；加快构建全国一体化大数据中心，建设E级和10E级超级计算中心；建立健全国家公共数据资源体系，推进数据跨部门、跨层级、跨地区汇聚融合和深度利用。

十四五规划和相关政策的颁布指明了电子政务的发展方向，政务外网作为支撑数字政府的基础设施，是政务数据流通的大动脉，未来需要进一步扩大覆盖范围、服务范围，提升服务质量，为数字政府的发展提供有力的支撑。

02 政务外网面临的业务挑战

新的业务场景的出现，对政务外网的网络覆盖、安全防御、体验保障均提出了新的要求，IPv4地址不足、运营管理难度大、安全防护不全面等问题成为制约政务外网发展的瓶颈，随着IPv6产业的成熟，通过IPv6赋能政务外网已经成为必选项。

2.1 IPv4地址不足，制约政务业务发展

国家信息中心于2015年向CNNIC（China Internet Network Information Center，中国互联网络信息中心）申请64个B类IPv4公有地址，用于政务外网建设，主要解决各部门、各地方政务外网地址冲突的问题。划分网段后，地址空间利用率30%左右，可用IP（Internet Protocol，互联网协议）地址大约为130万个，以全网接入的部门数量40万计算，每个部门平均可使用的全局IP地址小于4个。据估计，目前尚有30%-40%的政务部门未接入政务外网，IP地址量严重制约政务部门开展信息系统建设和数据共享。

IP网络的发展是由业务和应用驱动的，随着新的业务模式的不断出现，全局地址的需求量不断增加，同时精细化运营和精准溯源要求每个终端具备唯一可寻址的IP地址，全局地址短缺严重影响了政务业务持续创新。

2.1.1 数据大集中架构难以扁平化

2020年4月，《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》（简称《意见》）正式公布，数据作为一种新型生产要素被写入中央文件，《意见》指出“要加快培育数据要素市场，推进政府数据开放共享、提升社会数据资源价值”。

2020年12月，国家发展改革委、中央网信办、工业和信息化部、国家能源局等四部门联合印发《关于加快构建全国一体化大数据中心协同创新体系的指导意见》（发改高技〔2020〕1922号），提出了创新大数据中心体系、推动算力资源服务化、深化大数据应用创新、强化大数据安全防护等要求和举措。

人口、法人、自然资源与空间地理数据库等基础库已经实现数据大集中，与地方政务部门数据双向交互。以某部委一体化平台为例，需要全国2万多家部门集中使用国家级平台，过程数据双向交互，要求原本封闭的网络融合互通，需要使用全局IP地址，IP地址的需求量大大增加。

数据大集中后，如果地方终端仍然采用地方地址部署，多级NAT之后，会导致双向互访场景支持受限，不利于应用的灵活部署。

2.1.2 跨层级视频会议缺乏灵活性

政务外网已经承载国家民委、司法部、商务部、退役军人事务部、应急管理部、中国气象局、国家邮政局、台盟中央、中国科协等多个部门纵向视频会议业务。

随着部门之间协同的不断加深，跨部门、跨层级视频互联需求持续增加。目前政务外网的视频会议服务器采用分布式级联架构，各地分建，省级视频会议服务器使用公网地址，市县乡视频服务器采

用省内地方地址。市、县视频会议终端能够主动与国家的视频会议终端建立连接；但是国家级视频会议终端主动向市、县的视频终端发起连接时，由于国家级视频会议服务器没有到市、县视频服务器地址的路由，无法主动与跨层级如地市、乡镇视频会议服务器建立连接，跨部门、跨层级视频会议缺乏灵活性。为了灵活支持视频会议的各类应用场景，省内视频会议服务器需要采用全省集中架构，或者全部视频服务器都采用全局地址，才能满足视频会议的要求。

2.1.3 行业专网迁移对接带来增量IP地址诉求

根据要求，政府部门非涉密业务统一通过政务外网承载，目前由于各种原因，部分政府部门的非涉密业务采用专网承载，还没有与政务外网融合。行业专网对接或者整合到政务外网后，跨省互通或者访问国家业务平台时，部分业务需要采用政务外网统一规划的全局地址进行业务交互。政府部门一般涉及到部、省、市、县等多级单位，每一级单位都涉及到全局地址的使用诉求。随着政府部门业务的发展和专网整合的进一步推进，政务外网IPv4地址不足的问题会进一步加剧。

2.1.4 智慧城市治理带来IP地址数量指数级增加

城市治理在向智能化、精细化方向发展，物联网通过各类传感器将城市运行数据汇聚起来进行分析，实现对城市的全维实时感知，支撑城市策略制定和决策。当前各个政务部门烟囱式建设物联网，物联系统之间相互隔离，数据相互调用难、共享难，例如：供水、应急、环保等多个部门需要调用水务数据，在实际操作中，数据非标准化，没有统一的共享对接机制，导致数据对接共享的时效性难以满足业务需求，甚至存在无法对接的情况。

国家“十四五规划”中提到，要将物联网感知设施纳入公共基础设施，统一规划建设，推进市政公用设施、建筑等物联网应用和智能化改造。将海量的物联终端进行统筹管理，数据开放共享，需要给每一个终端分配唯一的IP地址进行标识。此外，物联终端类型多，覆盖范围广，管理难度较大，终端容易成为被攻击的对象，在终端出现异常时需要精准定位溯源，进行阻断处理，这也需要为每个终端分配单独的IP地址。

2.1.5 移动办公带来终端数量显著增长

随着4G（4th Generation，第四代移动通信系统）、5G（5th Generation，第五代移动通信系统）网络的逐步完善，移动网络可以支撑高清视频类及时通讯。各部委采用移动政务平台支撑移动执法、移动办公、应急指挥等业务，提升政务办公效率，解决信息化“最后一公里”问题。在移动执法过程中，从现场检查到调查取证、立案查处等，通过移动执法系统做到办案全过程留痕，全面提升办案质量，增强执法透明度，确保公开、公正。在移动办公场景下，个人或车辆配备多种智能化终端，包括车载电脑、智能手机和智能对讲等，人均配备终端数量不断增加，整体终端数量也呈现快速增长趋势。为了实现高效的通信，需要为每个终端分配IP地址，进行数据通信和业务管理。

2.2 网络运营管理难度大

2.2.1 IPv4地址可读性差，管理难度大

政府部门通常采用条块化管理模式，纵向按行业接受上级部门业务指导，横向按属地接受地方政府管理。地方电子政务外网和上级业务部门都有识别用户、业务进行管理的诉求。

由于IPv4地址长度有限，无法通过IP地址字段区分业务、区域、部门等信息，只能按照网络结构进行规划，无法通过IP地址同时区分两类信息，不能进行直观的管理。

2.2.2 私有地址使用，导致难以实现用户级管理

由于IPv4地址不够用，部门政务外网通常会采用私有地址，通过NAT转换后接入政务外网，多个用户共享IP地址，会带来以下问题：

1. 通过IP地址无法区分具体用户和业务，进行端到端的业务保障，管理复杂度高。

2. 无法进行安全方便的认证，采用Portal认证会带来一定的安全风险，一个终端认证通过，会放行使用同一个IP地址的其他终端。L2TP（Layer 2 Tunneling Protocol，二层隧道协议）认证方式可以解决这个问题，但使用较为复杂。

3. 当在政务外网上发现异常用户时，需要对用户进行阻断下线，而多个终端共享使用同一个IP地址，无法进行精细化控制。

2.2.3 网络故障定位复杂度高

基于IPv4的政务外网出现故障后，定位流程复杂，主要体现在以下两个方面：

1. 各级部门内采用私网地址，通过NAT转换成公网地址进行互通，导致问题定位困难。例如某个用户出现故障，需要综合查询同一时刻，路径上所有防火墙设备的NAT用户表项日志，并在各台防火墙时间同步的前提下，才有可能找到具体用户，找到用户后，还需要对设备上的NAT表项进行分析，寻找故障根因，给定位工作带来了很大的不便。

2. 视频会议业务对网络丢包、时延较为敏感，丢包率要小于千分之一才不会出现花屏，而传统IPv4网络难以对丢包、时延等影响用户体验的故障进行定位。

2.2.4 网络负载调整不方便，带宽利用率低

政务外网当前主要依靠路由开销进行选路，大部分情况下，业务会优选一条链路，容易出现一条链路负载很高，另一条链路流量较少的情况，可能会导致瞬间拥塞，影响业务体验。基于路由开销的选路方式，不能基于用户体验对业务路径进行优化，影响用户体验的同时，也造成高昂的专线资源不能被充分利用，从而变相提高专线成本。

2.2.5 网络差异化保障能力不足

基于IPv4的政务外网，缺乏对业务的差异化保障能力，主要体现在两个方面：

1. 政务外网需要为部分政务业务提供实时性、高质量的服务，不能中断，例如部分地方政务外网承载了医保结算类业务，当网络出现丢包，可能导致医保卡刷卡反复失败，进而导致医院排队人员增多，可能引发群众性事件。根据《全国医疗保障系统核心业务区骨干网络建设指南》要求，医保结算类业务要求误码率为10E-7，抖动小于等于2ms。基于IPv4的政务外网，由于IPv4扩展受限，无法为高质量业务提供专有带宽保障。

2. 由于业务需要，运维人员经常需要针对重保业务进行保障，目前常用的手段是手工在经过的所有设备上配置QoS（Quality of Service，服务质量），为重保业务分配高优先级，保障业务体验，当会议结束后，再逐跳删除业务配置，工作量大而且容易出错。

2.3 网络安全防护难度增大

2.3.1 私有地址重复，安全监测和溯源难度大

对于政务公共业务，政务部门经过NAT后进入政务外网，或者各省的流量经过NAT后进入中央级政务外网，由于多个用户共用一个IP地址，当安全监测平台监测到攻击后，并不能精准定位到是具体哪台主机进行取证。

在政务外网承载政务部门专网VPN（Virtual Private Network，虚拟专用网）的场景下，由于VPN内私有地址重叠，针对同一个IP地址，安全监测平台可能监测到大量重复IP地址的告警，由于安全监测平台按照五元组进行呈现，不能监测到具体是哪个业务，哪个政务部门的哪台终端出了问题，造成溯源排查困难，难以实施进一步的阻断策略。

2.3.2 公网地址错误私用，存在数据泄漏风险

随着虚拟化和物联网技术的发展，网络规模越来越大，子网数量激增，政务业务对全局地址和地方地址需求量越来越大。IPv4地址不足时，有些地方可能会把其他组织已申请，但未启用或非私网的IP地址，作为私有地址使用，例如172.0.0.0/8网段。这些地址一旦后续在公网重新启用，由于内网已经使用该地址，导致内网用户根据私网路由无法正常访问公网启用的相应服务；同时，当内网业务路由发生变化（不可达等），可能将数据包按照默认路由转发到外网，造成内部信息泄漏。

03 IPv6在政务外网的应用实践

随着政务业务的发展，IPv4地址短缺问题日益加剧，从IPv4迁移到IPv6已经成为当前的工作重点。2013年开始，国家电子政务外网管理中心开始组织开展IPv6应用试点，国家和地方电子政务外网相继进行IPv6改造，在IPv6改造上积累了丰富的经验。

3.1 IPv6技术特点

3.1.1 IPv6优势1：地址充足，支撑海量覆盖和连接

IPv6巨大的地址空间，支撑新一代政务外网的海量连接。IPv6地址采用128比特标识，总体空间有2^{128}，能很好地解决IPv4地址短缺，以及专网整合时私网地址冲突的问题，支撑物联感知网络的海量连接需求。

IPv6地址可管理性好，支撑新一代政务外网的高效管理。巨大的地址空间使得IPv6地址不同的字段可以代表丰富的语义，可以按照纵横两个维度分配地址段，方便路由聚合，可高效支撑新一代政务外网的基础管理。

IPv6所提供的巨大地址空间，正是实现数字政府乃至数字社会万物智联，促进生产生活数字化、网络化、智能化发展的关键基础。

3.1.2 IPv6优势2：扩展性佳，提供差异化的用户体验

IPv6报文的灵活扩展性为新型政务应用创造了优异的条件。IPv6报文和IPv4报文相比，去除了IHL（Internet Header Length，首部长度）、Identifier、Flag、Fragment Offset、Header Checksum、Option和Padding域，只增加了流标签域，因此IPv6报文处理较IPv4报文更为简化，提高了处理效率。IPv6扩展头新增选项时不必修改现有结构，理论上可以无限扩展。如IPv6分段路由技术SRv6（Segment Routing over IPv6，IPv6分段路由），通过在IPv6的扩展头Routing Header中定义SRH（Segment Routing Header，分段路由扩展头）实现，SRv6将一些IPv6地址定义成实例化的SID（Segment ID，段ID标签），通过不同的SID操作，实现简化的VPN，以及灵活的政务业务路径规划，体现了优异的灵活性和网络可编程能力，也为未来网络加载新的应用提供了充分的支持。

以SRv6为基础的IPv6+（Internet Protocol Version 6 Plus，基于IPv6下一代互联网的升级）**技术体系，为高品质的业务体验保驾护航。**IPv6+是基于IPv6、AI的协议技术创新，如IPv6+网络切片技术，为各类政务业务提供专网级的体验；IPv6+随流检测技术，实现网络质量可视、业务质量实时监测，在业务出现异常时，快速定位故障。IPv6+应用感知技术，基于应用自动导航，选择最佳路径，提供智能化的政务服务。

基于IPv6的灵活扩展以及协议技术创新，可以为政务业务的差异化质量保障、自动化、智能化保驾护航。

3.1.3 IPv6优势3：安全性高，提升网络自主权

我国IPv6/IPv6+协议的自主化能力强。我国企业、高校和科研机构的IETF（Internet Engineering Task Force，因特网工程任务组）影响力日益增长，中国主导完成的RFC（Requirement For Comments，征求意见稿）数量和工作组文稿数量的增幅均保持全球前列，目前已经主导完成了百余项IETF的各类RFC，主要集中在IPv6+领域，我们也拥有了IPv6+时代的自主权。

IPv6可以方便实现网络实名制。IPv6庞大的地址空间可以从技术上解决网络实名制和用户身份溯源问题，实现网络精准管理，有利于事后追查回溯，提高安全保障能力。

IPv6与生俱来的安全优势，可进一步提升政务办公、政务服务、社会治理的安全性，更好地保障政务业务的安全运行。

3.2 IPv6/“IPv6+”产业正在加速升级

3.2.1 IPv6发展现状

全球IPv6发展呈加速态势。随着物联网、工业互联网和人工智能等产业飞速发展，IPv4地址资源日益枯竭，世界主要的互联网大国已充分认识到现阶段部署IPv6的紧迫性和重要性。各国政府纷纷出台国家发展战略，制定明确的发展路线图和时间表来积极推进IPv6的商用部署。

IPv6产业链已经基本成熟。根据《2020全球IPv6支持度白皮书》中的信息，以及IPv6监测平台相关数据，截至2020年7月，从操作系统、网络/安全设备、应用软件、云平台等成熟度情况判断，目前行业组织信息化基础设施向IPv6演进已具备成熟的基础条件。

根据从下一代互联网国家工程中心、全球IPv6测试中心，以及IPv6监测平台官方获得的数据，从操作系统、网络/安全设备、应用软件、云平台四个维度对IPv6支持情况总结如下。

操作系统

移动终端、固定终端和信创终端，都支持IPv6，虽然具体实现上有些差异，但是当业务服务器具有双栈地址时，都优选IPv6，如果IPv6地址不可达，则可以切换到IPv4。

表3-1 主流操作系统IPv6支持情况

分类	操作系统	是否默认安装IPv6协议	是否支持DHCPv6	是否支持SLACC
移动终端	Android	是	否	是
	IOS	是	是	是
固定终端	Win XP	否	安装插件支持	是
	Win 7	是	是	是
	Win 10	是	是	是
	Win 2008	是	是	是
	ubuntu	是	是	是
	Redhat	是	是	是
信创终端	中标麒麟	是	是	是
	统信UOS	是	是	是

信息来源：

- 移动终端/固定终端：根据全球IPv6测试中心，以及下一代互联网国家工程中心发布的《2018-2019全球IPv6支持度白皮书》、《2018 IPv6支持度报告》整理。
- 信创终端：中标麒麟、统信UOS分别基于Linux2.6内核和Linux5.3内核（百度百科），结合《2018 IPv6 支持度报告》中Linux版本对IPv6的支持度整理。

网络/安全设备

主流路由器、交换机已支持IPv6，安全产品已具备基本IPv6防护能力、检测能力、审计能力和大数据分析能力，能够满足基本商用部署需求。

表3-2 主流网络/安全设备IPv6支持情况

网络基础设施	产品类别	设备名称	是否支持IPv6
网络类	交换机	园区交换机、数据中心交换机	是
	路由器	接入路由器、骨干路由器	是
安全类	安全防护类	防火墙、入侵防御系统、Web应用防火墙、Anti-DDoS、防病毒网关、VPN网关	是
	检测类	入侵检测系统	是
	安全审计类	日志审计、数据库审计、上网行为审计、网络综合审计、堡垒机运维审计	是
	大数据分析管控类	态势感知平台、安全策略管理、安全运营中心、漏洞扫描	是

信息来源：根据下一代互联网国家工程中心、全球IPv6测试中心发布的《2020全球IPv6支持度白皮书》，以及主流安全厂商官方数据整理。

应用软件

当前主流的数据库、中间件、程序开发软件和办公软件已具备了IPv6基础支撑能力。

表3-3 主流应用软件IPv6支持情况

软件类别	软件名称	是否支持IPv6
数据库	人大金仓	是
	达梦	是
	神州通用	是
	瀚高	是

数据库	MySQL 5.7.17	是
	Oracle Database 12.1.0.2.0	是
中间件	东方通中间件	是
	普元中间件	是
	宝兰德中间件	是
	Kafka	是
	zookeeper	是
程序开发软件	Apache	是
	Ruby	是
	Python	是
	Java	是
	PHP	是
办公软件	IE系列浏览器	是
	Chrome浏览器	是
	Firefox浏览器	是
	Opera浏览器	是
	360安全浏览器	是
	QQ浏览器	是
	FileZilla3文件传输软件	是
	SmartFTP4文件传输软件	是
	Outlook邮件软件	是
	Lotus Notes邮件软件	是

信息来源：根据下一代互联网国家工程中心、全球IPv6测试中心发布的《2018-2019全球IPv6支持度白皮书》，以及厂商官方数据整理。

云平台

主流云平台已具备IPv6服务能力。在“2020中国IPv6发展论坛”上，中国信息通信研究院为腾讯云、阿里云、华为云以及移动云颁发了云服务IPv6支持能力测评证书。同时从国家IPv6监测平台上可以看到，截至2021年7月，已有11家云服务商的全部云服务产品100%支持IPv6。

表3-4 主流云服务IPv6支持情况

云服务商	云服务名称	是否支持IPv6
阿里云	云服务器ECS、容器服务、SLB、DNS、对象存储、云数据库、API网关、Web应用防火墙、DDoS基础防护等	是
华为云	弹性云服务器ECS、弹性负载均衡SLB、对象存储服务OBS、API网关APIG、云解析服务DNS、云数据库RDS、WEB应用防火墙WAF、云容器引擎CCE等	是
腾讯云	云服务器、负载均衡、对象储存、云数据库MySQL、Web应用防火墙、DDoS等	是
移动云	云主机、弹性负载均衡、对象储存、Web应用防护、抗DDoS服务等	是

信息来源：中国信息通信研究院和下一代互联网国家工程中心发布的云服务IPv6支持能力评测结果。

综上可以看出，主流的操作系统、网络/安全设备、应用软件、云平台已经具备IPv6能力，行业基础信息化设施已经具备向IPv6演进的条件。

3.2.2 “IPv6+”产业现状

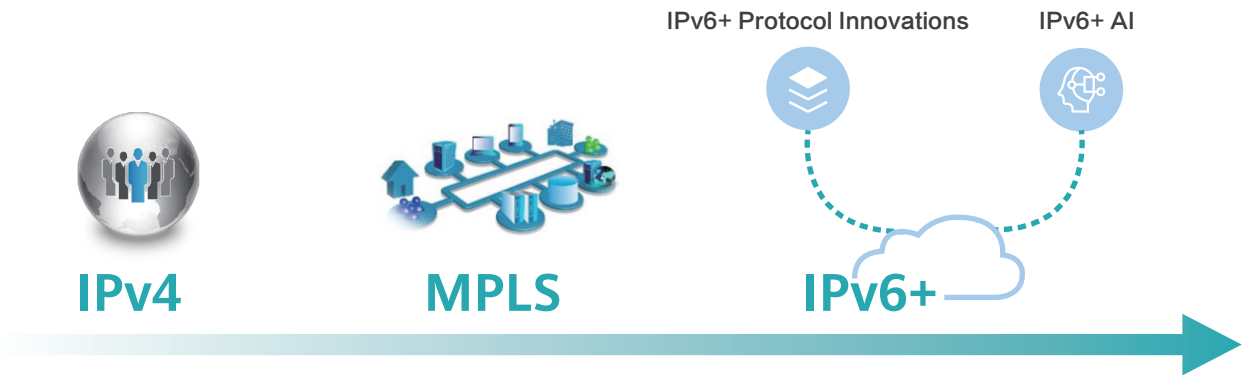
“IPv6+”技术体系

业界普遍认为IPv6不是下一代互联网的全部，而是下一代互联网创新的起点和平台。在IPv6部署过程中，业界认识到IPv6的部署不仅是增加地址空间，解决IPv4地址瓶颈，身份可溯源，更好实现安全管理等问题，还可以进一步开发IPv6技术与应用，为用户创造更大价值，增强发展IPv6的内生动力。为此，国家推进IPv6规模部署专家委员会在2019年底正式成立了“IPv6+创新推进组”，构建“IPv6+”技术创新工作体系。

“IPv6+”是基于IPv6下一代互联网的升级，包含两方面：

- **由万物互联向万物智联的升级**
  IPv6海量地址构建了万物互联的网络基础，“IPv6+”全面升级IPv6技术体系，推动IPv6走向万物智联，满足多元化应用承载需求，释放产业效能。
- **由消费互联网向产业互联网升级**
  “IPv6+”进入千行百业，赋能行业数字化、网络化和智能化，全面支撑数字政府、数字社会、数字经济的网络基础设施建设。

1980年代，IPv4成为互联网的基础协议，推动了IP网络的发展。2000年代，MPLS技术诞生，增强了语音和视频等业务的综合承载能力。2020年，5G和云时代驱动新一代IP网络，以IPv6海量地址为基础，以协议创新和网络智能化技术创新为核心的“IPv6+”应运而生。



来源：ETSI White Paper No. 35

图3-1 IP网络代际规划

“IPv6+”包括：一是以SRv6分段路由、网络编程、网络切片、确定性转发、随流检测、新型组播、应用感知、无损网络等为代表的网络技术体系的创新；二是以实时健康感知、网络故障主动发现、故障快速识别、网络智能自愈、系统自动调优等为代表的智能运维体系的创新；三是以5G toB、云间互联、用户上云、网安联动等为代表的网络商业模式的创新。“IPv6+”在广联接、超宽、安全、自动化、确定性和低时延6个维度全面提升IP网络能力，可以满足业务快速开通、用户体验优化、差异化保障、网络运维等需求。

IPv6与网络切片技术结合，可以打造前瞻性、全覆盖的“一网多平面”电子政务外网，为各类业务提供专网级的体验。IPv6与随流检测技术相结合，可以实现电子政务外网网络质量可视、业务质量监测和故障快速定界。与APN6（Application-aware IPv6 Networking，应用感知网络）结合，可以将应用信息及其需求携带进入电子政务外网，使得网络能够有效且低成本地感知应用的差异化需求，并提供相应的网络服务。基于“IPv6+”的网络应用与政务外网业务需求相结合，可以反向促进IPv6的规模化部署，加速国家信息化进程、助力经济社会发展，逐步形成全球领先的下一代互联网技术和产业体系。

“IPv6+”应用情况

2020年初，我国提出了加快新型基础设施建设的目标，IPv6作为新基建高质量发展的基石，迎来了新的重大发展机遇，“IPv6+”是新基建场景下IPv6持续演进的方向，也将成为实现数字经济转型的重要基础之一。目前，我国已逐步迈入“IPv6+”商用部署阶段。“IPv6+”创新分为三个阶段，从基于SRv6的网络编程能力，到有条件自治网络的用户体验保障，最终目标是根据应用驱动网络技术实现应用感知、高度自治的网络。“IPv6+”技术在国内部署和应用得到快速发展，多个运营商及行业用户已相继进行了部署。在数字政府领域，国内不少省市积极采用先进的“IPv6+”建网理念和网络架构来建设新一代电子政务外网。

3.3 政务外网IPv6实践案例

3.3.1 国家电子政务外网IPv6地址规划

国家电子政务外网管理中心向CNNIC申请/21网段IPv6全球单播地址用于政务外网建设，并编制《国家电子政务外网IPv6地址规划》（2019版），指导部门、地方IPv6网络试点建设。IPv6地址规划遵循如下原则：

渐进规划原则

国家电子政务外网管理中心已为政务外网申请了/21网段的全球单播地址用于政务外网的IPv6建设，并制定了地址规划标准。按照标准对整网IPv6地址进行统一规划，标准里没有提到的内容，可向国家电子政务外网管理中心征求意见，逐步完善标准。

分级管理原则

IPv6地址采用中央、省、市、县政务外网建设单位分级管理的基本原则，地方在省内业务及本地业务地址的规划使用方面拥有自主权。

易于识别原则

按照国际惯例，IPv6地址采用16进制方式表示。规划力求在行政区划、行业条线特征位上保持一定的可读性，以便于网络管理人员的使用和识别，并保证路由可聚合的策略。

基于如上规划原则，IPv6地址基于如下思路进行规划：

- **支撑信息共享和区域性横向协同业务，兼顾中央、省级部分的纵向统筹。**

  为各级部门全网横向协同业务、中央部门纵向业务、省级部门纵向业务分别预留独立的地址空间，做到一般性业务在本地申请地址，纵向业务由上级部门统一规划地址。一方面尊重地方在横向协同业务部署方面的自主性；另一方面强化中央部门和省级部门对纵向业务系统的统筹建设和运维管理。

- **充分尊重地方在新技术发展和业务系统建设上的自主权。**

  为地方纵向业务及各级地方横向业务预留独立的地址空间，由地方自行管理和分配，保障地方在新技术发展和业务系统建设方面的自主权。

- **通过区分地址类型优化对网络流量的分类管理。**

  用顶级路由前缀类型域表示地址类型，以便于路由的发布和聚合。地址类型由国家电子政务外网管理中心统一定义。每发布一个地址类型，各级政务外网建设运维单位结合区域获得本地相应的地址段。

3.3.2 中央级政务外网IPv6双栈改造与部门应用试点

依托政务外网二期工程，对中央城域网、广域骨干网进行双栈改造。2020年底，作为政务外网中央部门的IPv6应用试点，金审三期IPv6试点省份完成部署。

中央级政务外网IPv6改造完成情况

截至2020年底，中央城域网支持IPv4/IPv6双栈协议，对部分有互联网业务的部委接入设备进行了替换，可根据部委业务的部署需求提供IPv6接入能力。具体如下：

- **中央城域网完成IPv6改造升级**

  通过政务外网二期工程实施，完成中央城域网核心层、汇聚层的网络设备，以及13个有互联网业务的中央政务部门接入设备的升级替换，支持IPv4/IPv6双栈协议，可根据部委业务的部署需求提供IPv6接入能力。

- **中央广域网完成IPv6改造升级**

  通过政务外网二期工程实施，完成广域网核心设备的升级替换，广域网支持IPv4/IPv6双栈协议，可根据地方业务的部署需求提供IPv6接入能力。

金审三期IPv6应用试点

按照金审工程三期项目（以下简称金审三期）规划安排，审计署办公厅和国家电子政务外网管理中心在天津市和山东省，联合开展第一批金审三期IPv6试点工作。

具体来说，审计署本级、国家电子政务外网先行改造，并制定IPv6专项设计方案、部署实施、地址规划等规范文档，用于指导全国审计机关IPv6部署实施工作开展；同时选取山东审计厅和天津审计局、以及山东省和天津市电子政务外网作为IPv6试点，完成试点审计厅（局）IPv6网络建设以及应用系统的IPv6接入，完成试点省（市）电子政务外网IPv6升级改造，以及试点审计机关接入省（市）政务外网，并实现与审计署本级IPv6互联互通。

IPv6试点部署充分考虑《行动计划》要求、业务连续性及网络的可演进性。在IPv6地址使用上，统一根据国家电子政务外网管理中心印发的“电子政务外网IPv6地址规划”，按照行政区划、部门、业务系统等进行审计机关网络系统的统一规划和分配，地址语义化，所见即所得，为电子政务外网和金审三期的建设运维人员带来了管理上的便利；在演进技术上，电子政务外网采用“双栈模式”完成IPv6部署，金审三期建设的“审计专网”、“数据分析网”以及各个系统、终端也全面采用了双栈技术部署，从而使审计署部省审计机关依托电子政务外网，基于IPv6实现了真正的纵横贯通，使审计工作跨部门、跨地区、跨层级协同更便利。

截至2020年底，天津、山东两个试点省市，已完成省-市-县三级政务外网IPv6双栈改造，各级审计机关分级接入政务外网，并实现与审计署本级IPv6互联互通。目前，已迁移部分审计业务系统至IPv6环境下运行，支撑审计机关业务系统部署，为电子政务外网IPv6规模部署积累了经验，为全国推广部署奠定了基础。

3.3.3 国家电子政务外网互联网区IPv6改造

按照《关于推进国家电子政务外网互联网协议第六版（IPv6）改造工作的通知》（国办电政函〔2018〕70号）要求，对互联网区IPv6改造，为公众提供IPv6业务访问。2018年12月，中央级和省级政务外网互联网区IPv6改造完成，中央、省级政务部门门户网站支持IPv6访问。国家电子政务外网互联网区IPv6改造不仅涉及网络、系统、安全基础设施的升级改造，还包含应用、云平台、管控系统的协同。国家电子政务外网互联网区IPv6改造方案如下：

- 网络设备、安全设备、云平台具备IPv6能力，采用双栈方案部署，基础设施改造一步到位，同时具备IPv4/IPv6业务承载能力。
- 由于业务应用暂未改造支持IPv6，在互联网区出口通过地址转换技术，对公众提供IPv6业务访问。
- 申请运营商IPv6专线，终端用户的IPv6访问数据流在互联网出口地址转换设备上转换为内部应用对应的IPv4地址。

中央级政务外网互联网区IPv6改造完成情况

通过国家电子政务外网平台二期工程（以下简称“外网二期”）实施，新建互联网出口，链路支持IPv6接入，完成互联网出口涉及的路由器、交换机、负载均衡、DNS等设备的IPv6替换升级。通过在互联网出口部署的负载均衡设备上采用IPv4/IPv6地址翻译技术，使互联网IPv6用户可以通过域名访问数据中心现有业务。

2018年12月底，中央级政务外网互联网出口已完成IPv6改造，实现了全国公共资源交易平台网站、投资在线审批监管平台的IPv6接入服务；中央城域网支持IPv4/IPv6双栈协议，对部分有互联网业务的部委接入设备进行了替换，可根据部委业务的部署需求提供IPv6接入能力。

省级政务外网互联网区IPv6改造完成情况

国家电子政务外网管理中心对天津、河北、山西等27个省（区、市）以及新疆生产建设兵团报送的IPv6改造方案进行了审核，提出了针对性的修改意见；组织开展了全国IPv6改造工作技术培训会，指导各省改造工作。北京、上海、重庆、黑龙江4个省（市）政务外网无互联网区，不涉及本次IPv6改造任务。

截至2020年底，31个省（区、市）以及新疆生产建设兵团政务外网已完成IPv6改造工作。其中，辽宁、浙江、安徽等17个省（区、市）及新疆兵团政务外网承载了政务部门的IPv6门户网站业务，已按要求完成政务外网互联网区的IPv6改造。通过中国信通院网站的IPv6支撑度测评平台对其IPv6门户网站域名进行测试，已全部通过验证，具备支持IPv6用户访问能力。

3.3.4 广西壮族自治区政务外网IPv6+改造

广西壮族自治区电子政务外网按照国家发展改革委、中央综治办关于印发《公共安全视频监控建设联网应用“十三五”规划方案》的要求，建设覆盖自治区、市、县、乡、村各级的公共安全视频图像共享交换体系和应用支撑体系，提高社会治理的社会化、法制化、智能化、专业化水平。当前电子政务外网存在如下挑战，难以满足视频图像等新业务的要求。

- 现有网络带宽不足，难以承载大量视频业务。视频数据并发交互约为1000路，需要考虑如何实现多条专线的负载均衡，保证视频业务质量的同时，提升专线带宽利用率。
- 办公、视频调阅、视频会议等多业务承载，如何保障关键和敏感业务的质量。
- 政务业务端到端路径长，涉及网络多，对于质量要求较高的视频等业务，如何实时感知业务状态，业务出现异常后，如何快速定位故障，恢复业务。

广西壮族自治区电子政务外网基于“一网通达、一云承载、一池共享、一事通办、一体安全”五个一的建设理念，采用IPv6+技术构建新一代电子政务外网，具体方案如下：

- 在现有的广西电子政务外网基础上，新建图像网平面，图像网平面主要承载视频业务，现有数据网平面主要承载办公等业务，两个网络平面互为备份。采用SRv6技术，实现专线带宽资源化管理，按照业务质量要求，选择最优网络路径，同时实现专线负载均衡，充分利用带宽资源。
- 对于重保视频会议、重要视频调阅等业务，采用网络切片技术，提供独立的带宽资源，保障业务质量。
- 通过SDN控制器，实现网络和业务的可视化运维。通过iFIT（In-situ Flow Information Telemetry，随流检测）技术，实现业务质量的实时检测和快速定界，结合故障聚类、AI人工智能等技术，实现根因自动分析，故障快速定位和恢复。

3.3.5 广东省政务外网IPv6+改造

广东省作为改革开放的前沿阵地，紧抓中国特色社会主义先行示范区与粤港澳大湾区“双区驱动”的重大历史机遇，推动政府治理体系和治理能力现代化、再创营商环境新优势，为实现“四个走在全国前列”、当好“两个重要窗口”提供有力支撑。政务外网作为数字政府的重要基础设施，广东省已实现省、市、区县、镇街全面覆盖。但因网络建设时间较早，网络设备老旧，在广东“数字政府”推动省域治理“一网统管”的新形势下，存在对视频会议、大规模视频感知数据共享交换等网络质量敏感类业务网络差异化保障能力不强，对财政、司法等专业用网隔离性需求保障能力不足、厅局委办业务上云网络开通响应慢，用户反馈式被动运维、网络故障定位复杂度高等问题，亟需对广东省电子政务外网升级改造，进一步夯实数字政府基础能力。

广东省积极贯彻落实《中共中央办公厅国务院办公厅关于印发（推进互联网协议第六版（IPv6）规模部署行动计划）的通知》，同时结合自身发展需要，秉承“全省一张网”的统筹规划思路，在网络升级改造过程中采用SDN、SRv6、FlexE网络切片、iFIT随流检测等先进的IPv6+技术，打造了一张广覆盖、多元化、有韧性、富能力的新一代电子政务外网，并于2020年9月印发了《广东省电子政务外网IPv6改造指南》，为全省加快推进IPv6改造工作提供指导。

在技术应用方面，广东省新一代电子政务外网采用SDN+SRv6 Policy技术可基于带宽、时延进行选路，当某条路出现拥堵时，就自动切换到另外一条路上，保障带宽均衡，体验最优，满足业务质量保障和安全隔离的要求；采用SRv6 VPN和FlexE网络切片技术，将政务外网划分为2+M个网络业务平面，固定部署政务外网和视频业务2个公共业务平面，按需部署M个专用业务平面，网络业务平面之间安全隔离，保证业务高质量承载。在运维管理方面，综合使用流量回溯分析、网络质量拨测和iFIT随流检测技术，实现业务质量可视，故障快速定界，提升运维管理效率。

2021年初，广东省新一代电子政务外网正式上线。升级改造后的电子政务外网，将进一步实现1200余家省级财政预算单位全覆盖。通过对IPv6+技术的应用，同时满足省级政务应用视频、数据一网承载的诉求，为推动政务网络集约化建设打下基础，同时有效解决原有电子政务网络业务开通慢、体验差、运维难等问题，进一步夯实了数字政府的基础底座的支撑能力，为实现广东省政务服务“一网通办”、政府治理“一网统管”、政府运行“一网协同”提供了强有力的网络保障。

3.3.6 中山城市综合治理一张网改造

中山市地处粤港澳大湾区几何中心，全力抓住粤港澳大湾区“双区驱动”的重大历史机遇，立足“打赢经济翻身仗，重振虎威，加快高质量崛起”，打造中型智慧城市样板点。依托“中山城市大脑”、“数字孪生底座”等核心平台，构建智能化治理体系，强化数字技术在城市规划管理和服务等领域的应用，建立统一指挥、实时调度、上下联动、横向协同的中山智慧化城市运行体系，逐步实现“六个一流”的总体目标，打造“四个一体”，创建“四个示范区”，建成国内先进、可持续运营的新型智慧城市“中山样板”，推动城市更加聪明，更加智慧。

在智慧城市的建设中，网络是底座，也是基础。要致富，先修路；要智能，网先行。政务外网作为智慧中山城市联接核心承载网络，应具备广覆盖、高质量、强安全、易运维的能力。但是原有政务外网核心定位是服务于政府部门，存在网络只覆盖市、镇两级一百余家单位，承载业务只包括政务服务和办公业务，相较于智慧城市市、镇、乡村基层全覆盖，政务、视频、物联等城市业务综合承载，还存在较大差距。同时，原有政务外网故障定位和运维能力不足、安全不满足等保要求限制了政务信息化共建共享的发展。

新一代网络基础设施建设全面考虑智慧城市业务需求，形成了城市网络和安全顶层设计。通过与20多家委办局、镇区政府进行深度调研，从有线无线全覆盖，城市物联感知体系，集约共享视频和数据网络，全市网络安全运维平台等方面进行了规划和定义。2020年11月20日，全市政务外网网络实现全新升级，网络能力得到全面提升：

- 网络带宽十倍提升，提升我市政务网络使用体验。骨干网带宽由千兆升万兆、接入终端带宽由百兆升千兆。
- 实现“纵向到村居、横向到边缘”的全市覆盖。纵向延伸到25个镇区、277个村居节点，横向接入全市各政府部门、相关市直属单位、医院、学校及运营商等1300多个单位。
- 采用“一网多平面”方式承载政务业务、城市物联网、视频专网业务。基于领先的IPv6+网络技术架构，实现业务自动化开通，全网流量智能调优，保证委办局-镇区汇聚-市核心-政务云/省外网出口一跳上云。为财政专网整合划分单独虚拟专网承载。 正在规划视频和物联网平面，未来连接城市万路高清视频，数十万级物联终端及传感器。

新一代政务外网建成后，数字政府集约化建设规模效应显现，“数据壁垒”进一步打破，政务服务关键环节被打通，平台使用体验强：

- 政务服务“再提速”，实现电子证照向镇街、村居延伸，近100种证照“免提交”，真正打通服务基层“最后一米”。
- 线下服务“持续优”。推动政务服务向基层延伸，全市277个村居、313个党群服务中心均设立政务服务专区。

- “数据壁垒”进一步打破。政务服务关键环节被打通，平台使用体验强。建立市、镇、村三级政务服务中心，25个镇区建成行政服务中心，277个村居建成公共服务站，实现“进一扇门办千件事”。

此外，全市建成安全运营中心，制定安全运营体系，实现全市安全管控，符合等保合规要求。要求各单位应充分依托一体化网络和安全基础设施、网络安全防护平台资源开展网络安全体系建设。

2021年，重点推进和落实全市专网整合工作，各单位建设的非涉密系统应接入或建在政务外网上。同时，在政务外网IPv6深化应用、政务5G无线和政务外网协同、城市物联网方面将会持续开展顶层设计、标准制定、先行先试等积极探索，为推动政务信息化共建共用，提高数字政府建设水平提供实践经验。

04 基于IPv6构建下一代电子政务外网

政务外网IPv6演进的目标是在完成业务、网络IPv6升级改造的基础上，解决当前制约业务发展的问题，同步完成网络架构优化，进一步提升政务外网的可持续服务能力。

4.1 政务外网IPv6演进思路

政务外网采用统一规划、分级负责的模式建设，IPv6演进是一个长期、分地域、分系统逐步升级的过程，演进过程遵循应用驱动、规划先行、分级分域、保障安全的原则统筹推进。各层级单位需要密切配合，充分利用沟通协调工作机制加强对接，合力破解具体困难和问题。

政务外网IPv6改造以部门业务需求为切入点和突破口，驱动网络演进，应用、网络互相促进，形成IPv6改造正循环。推进IPv6特色应用创新示范，尤其是对IP地址需求量大的应用，对存量应用实施分批分步的IPv6改造，改造一个，应用一个，最终实现IPv6规模部署。

政务外网IPv6演进要规范化、制度化推进。国家立足全局，制定IPv6改造规划，完善IPv6相关规范，指导地方进行改造实施。《国家电子政务外网IPv6地址规划（试行版）》经过地方、行业专网IPv6改造实践，已经具备正式发布推广条件。

政务外网IPv6改造在统筹规划的基础上，遵循分级分域负责的原则。国家将IPv6改造规划分解到各级网络平台和各部门，各级网络管理单位应把握IPv6演进升级机会，立足本级网络平台现状，充分考虑技术的先进性，制定切实可行的演进方案和路径，因地制宜，分步骤、分阶段推进实施，避免网络再造，重复投资。

演进过程中必须保障业务的可持续性及网络安全性，实现“业务不断，安全不乱”。在进行IPv6替换或者演进时，兼顾国产化战略，优选国产化产品或系统。尽快完善IPv6相关的等保测评体系，维护业务系统的安全运行。

各级政务外网IPv6演进需要政务云、网络平台、部门政务外网三方面协同发展，优先进行政务云互联网接入区改造，满足政策要求，应用逐步迁移到IPv6；公用业务区按照“网络先行、应用逐步改造”策略，优先进行基础设施改造，打通政务外网IPv6访问通路，为IPv6应用上线奠定基础。

4.1.1 政务云：互联网区优先改造，应用逐步迁移

目前，政务云互联网区已经为公众提供IPv6访问服务，方案以NAT翻译技术为主，业务系统大多数仍然采用IPv4地址。政务云IPv6改造遵循“先对外，后对内”，“先基础，后应用”，“先业务面，后管控面”的原则，优先改造提供对外公众业务的互联网区；网络、安全、云平台等基础设施优先部署IPv6能力；业务面优先进行IPv6改造，并探索开展IPv6单栈（IPv6-only）应用试点。

互联网区改造

互联网区的云平台、数据库、应用监测系统、身份认证管理系统、网络设备、安全设备等基础设施改造支持IPv4、IPv6双栈，具备双栈业务承载能力，过渡期内不支持IPv6的应用，通过NAT64（Network Address Translation IPv6-to-IPv4，IPv6到IPv4的地址转换协议）的方式支持IPv6用户访问。升级互联网区DNS（Domain Name Server，域名服务器）系统，具备IPv4/IPv6域名递归解析能力。

应用系统需要支持IPv4和IPv6用户同时访问。对于网页中的外链（网页包含其它网站内容的链接），需要通过代理等方式解决，避免出现“天窗”问题（用户访问网站时出现响应缓慢，部分内容无法显示，部分功能无法使用等情况）。随着IPv6改造的逐步深入，“天窗”问题会逐渐消失。

互联网出口与运营商对接，对外的IPv6业务地址建议采用运营商地址，政务外网地址和运营商地址解耦，避免相互影响。

公用网络区改造

公用网络区的云平台、数据库、应用监测系统、身份认证管理系统、网络设备、安全设备等基础设施改造支持IPv4、IPv6双栈，具备双栈业务承载能力。升级公用网络区DNS系统，具备IPv4/IPv6域名递归解析能力。

新建的应用系统，需要做好系统平台的架构规划，充分考虑系统对IPv6的支持，建议部署双栈，同时支持IPv4和IPv6用户的访问。存量应用系统根据业务需要逐步进行改造。

4.1.2 广域网/城域网：先核心，再边缘，循序渐进

推进广域网/城域网双栈改造，为部门政务外网和政务云奠定IPv6互联基础。广域网/城域网IPv6改造整体按照“先评估，再规划”，“先试点，再推广”，“先核心，再边缘”，“先业务面，再管控面”的改造思路，循序渐进，平滑演进。

由于电子政务外网国家、省、市采用分级建设的模式，改造计划、进度存在差异，建议采用双栈方案改造，兼容IPv4和IPv6两种协议，对于未完成IPv6改造的网络，使用IPv4协议进行对接，保障现有IPv4业务不受影响。

存量设备改造时，改造前需要评估确认设备的升级、替换策略，关注开启双栈后性能变化，双栈功能可能会降低某些设备的可用资源，如路由表项，上线用户数等。

城域网的边界安全和准入认证系统，需要同时支持IPv4和IPv6用户和业务。网络管理运维系统，仅涉及内部管理，不涉及业务，可优先改造完业务面后，再进行改造。

考虑到持续演进，广域网/城域网IPv6改造建议采用IPv6+方案，基于SRv6技术承载IPv4、IPv6业务，提升网络可编程能力，同步提升业务体验，全面实现网络和业务的可视、可管、可控、可维，满足持续演进要求。

4.1.3 部门政务外网：按需改造，逐步演进

部门政务外网的网络和终端根据各部门需要进行改造。改造时，网络设备、安全设备、终端部署双栈。部门政务外网与城域网对接时，不需要NAT转换。终端访问政务外网时，采用终端准入控制机制，不允许终端同时访问互联网和政务外网，避免跳板攻击。

4.2 基于IPv6构建集约化、高品质、智安全的下一代电子政务外网

IPv6规模部署和应用是互联网演进升级的必然趋势，是网络技术创新的重要方向，是网络强国建设的关键支撑。在政务外网持续推进IPv6规模部署，积极开展基于IPv6技术的应用创新，对政务外网业务发展、网络安全提升具有重要意义。下一代电子政务外网将以IPv6为基础，在基础设施集约化建设、业务高品质承载、安全精准管控方面深耕优化，提升政务治理的现代化水平。

4.2.1 基于IPv6，构建集约高效的政务基础设施

- **统一承载，集约化建设**

  在数字社会从信息化走向智能化的新时代，智慧城市、移动办公等政务业务快速发展。通过为全网业务系统的服务器、终端等分配唯一的IPv6地址，实现政务非涉密业务通过统一的政务云、政务外网来承载，促进新业务的快速发展，实现政务资源的集约化。

- **数据大集中，提升政务业务效率**

  在每个服务器和终端具有唯一的IPv6地址后，对于数据大集中系统，以及跨层级、跨部门的视频会议等系统，可以实现扁平化的架构，不同层级的服务器和终端等可以直接通信，有效提升政务业务的处理效率。

4.2.2 通过IPv6+，实现高品质的政务体验

- **网络切片保障重保业务质量**

  随着专网整合的进一步深化，政务外网将承载越来越多的业务，不同的业务对网络质量要求不一样，传统IP网络尽力而为转发，不同业务之间难免会互相影响，通过基于FlexE/信道化子接口的网络切片技术，在一张物理网络上实现资源隔离的专网，可以为重保业务提供独立的带宽资源，在其他业务出现拥塞时，不影响重保业务的质量，实现高品质的体验。同时，结合SRv6 VTN ID（Virtual Transport NetworkID，切片ID）技术，多个网络切片平面可以共用一套接口IP地址和IGP（Interior Gateway Protocol，内部网关协议）路由协议，降低网络协议的复杂性。

- **SRv6提高专线利用率**

  政务外网广域网和部分城域网通过租用专线的方式进行承载，专线带宽资源有限。基于SRv6 Policy技术和SDN架构，可实时采集整网链路的时延、丢包等质量信息，根据不同业务的要求，选择最佳的网络路径进行承载，并自动进行优化。在存在多条专线链路路径时，优先选择轻载的链路进行承载，实现专线链路负载均衡，提升专线带宽利用率，降低运营成本。

- **随流检测提升管理运维效率**

  政务外网层级多，在业务出现异常时，故障定位困难，业务恢复慢。通过iFIT随流检测技术，可以实时检测业务的质量，可视化呈现；在业务出现异常时，自动在业务路径上逐跳收集业务质量信息，定界故障位置，恢复业务，保障政务业务的连续性。同时结合APN6技术，可将视频会议等终端与网络深度协同，实现应用端到端可视和运维。

4.2.3 依托IPv6安全优势，提供精准的安全管控和溯源

- **攻击精准溯源和阻断**

  政务外网接入的终端类型和数量在不断增加，在出现威胁时，需要做到精准的溯源和阻断。全网终端具有唯一的IPv6地址，通过安全监测分析平台，实时检测网络威胁，当发现威胁后，可以通过IPv6地址精准溯源到终端位置，对异常终端进行阻断。结合网安协同机制，可以同时在网络设备上阻断威胁，实现近源阻断，杜绝异常外联及跨网攻击的发生。

- **灵活高效的准入认证**

  政务外网需要对接入的终端进行准入认证，认证通过的用户才可以访问政务外网。为部门政务外网的终端统一分配唯一的IPv6地址，接入政务外网时不需要进行NAT转换，不需要考虑NAT穿越的问题，可以通过免客户端的Portal认证方式进行准入认证，增加了认证的灵活性和便捷性。利用IPv6地址丰富的扩展字段，可以携带用户ID等信息，网络和安全设备通过用户ID等信息，对用户进行精准的认证和威胁防护。

05 缩略语

缩略语	英文全称	中文全称
4G	4th Generation	第四代移动通信系统
5G	5th Generation	第五代移动通信系统
AI	Artificial Intelligence	人工智能
Anti-DDoS	Anti-Distributed Denial of Service	防御分布式拒绝服务
APN6	Application-aware IPv6 Networking	应用感知的IPv6网络
CNNIC	China Internet Network Information Center	中国互联网络信息中心
DCN	Data Center Network	数据中心网络
DHCPv6	Dynamic Host Configuration Protocol Version 6	动态主机配置协议版本6
DNS	Domain Name Server	域名服务器
FlexE	Flexible Ethernet	灵活以太
IETF	Internet Engineering Task Force	因特网工程任务组
iFIT	in-situ Flow Information Telemetry	随流检测
IGP	Interior Gateway Protocol	内部网关协议
IHL	Internet Header Length	首部长度
IoT	Internet of Things	物联网
IP	Internet Protocol	互联网协议
IPv4	Internet Protocol version 4	互联网协议第四版
IPv6	Internet Protocol Version 6	互联网协议第六版

缩略语	英文全称	中文全称
IPv6+	Internet Protocol Version 6 Plus	基于IPv6下一代互联网的升级
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
NAT	Network Address Translation	网络地址转换
NAT64	Network Address Translation IPv6-to-IPv4	IPv6到IPv4的地址转换协议
QoS	Quality of Service	服务质量
RFC	Requirement For Comments	征求意见稿
SDN	Software Defined Network	软件定义网络
SID	Segment ID	段ID标签
SRH	Segment Routing Header	段路由扩展头
SRv6	Segment Routing over IPv6	IPv6分段路由
VPN	Virtual Private Network	虚拟专用网
VTN ID	Virtual Transport Network ID	切片ID