



推进IPv6规模部署专家委员会
国家电子政务外网管理中心办公室

IPv6演进路线图和实施技术指南

政务外网





CONTENTS

目录

01	前言	01
02	总体目标	02
03	演进路线图	03
3.1	总体演进原则	03
3.2	IPv6统计监测指标框架	07
04	实施技术指南	09
4.1	数据中心	10
4.2	广域网/城域网	13
4.3	部门政务外网	14
4.4	支撑系统	15
4.5	运维管理系统	15
05	缩略语	17

01 前言

互联网协议第六版（Internet Protocol Version 6，IPv6）是互联网升级演进的必然趋势、网络技术创新的重要方向、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。近四年来，各地区、各部门认真贯彻落实《推进互联网协议第六版（IPv6）规模部署行动计划》，推动IPv6规模部署取得显著进展。“十四五”时期是加快数字化发展、建设网络强国和数字中国的重要战略机遇期，我国IPv6发展处于攻坚克难、跨越拐点的关键阶段，面临不进则退、缓进亦退的风险挑战。2021年，中央网信办牵头下发《深入推进IPv6规模部署和应用2021年工作安排》（中网办发文〔2021〕12号）和《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），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。

为深入贯彻落实党中央决策部署，有效应对数字时代的业务挑战，加速推动政务外网IPv6发展，国家电子政务外网管理中心于2021年7月30日发布《政务外网IPv6演进技术白皮书（2021）》，给出了政务外网向IPv6演进思路。

政务外网向IPv6演进，是一个长期、系统化的工程。本指南为各地方各部门政务外网向IPv6演进提供技术指导。



02

总体目标

到2023年末，完成政务外网网络基础设施IPv6改造。各级政务外网广域网、城域网、数据中心出口支持IPv6，探索积累数据中心IPv6资源池建设和运维经验。

到2025年末，完成政务云和部门政务外网IPv6改造。各级政务外网数据中心完成IPv6资源池建设；新建应用及基础设施规模部署IPv6单栈。

到2030年末，完成政务外网向IPv6单栈演进。

03

演进路线图

3.1 总体演进原则

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、地市级三级网络平台，各级网络平台包含广域网、城域网、数据中心、互联网出口等部分。县（区）接入市级网络平台，作为市级网络平台组成部分。具备条件的区县，可以参考市级网络平台单独建设网络平台。

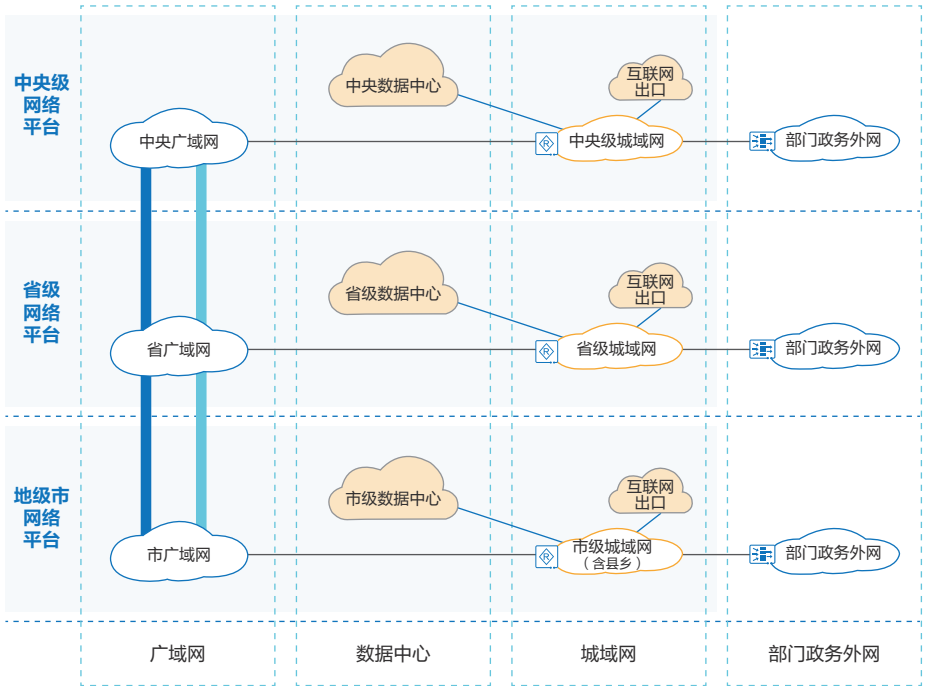


图3-1 电子政务外网架构

政务外网IPv6演进主要涉及数据中心（包括应用）、广域网/城域网、部门政务外网、支撑系统、运维管理系统五个方面，整体遵循统一规划、因地制宜、分步实施、安全稳妥的原则，基础设施先行，终端和应用逐步改造。

演进过程中瞄准IPv6单栈目标，数据中心建议采用新建IPv6资源池进行改造，具备条件的应用优先采用IPv6单栈方案，广域网/城域网优先采用IPv6+（Internet Protocol Version 6 Plus，基于IPv6下一代互联网的升级）技术，部门政务外网和终端采用IPv4（Internet Protocol version 4，互联网协议第四版）/IPv6双栈方案，随应用IPv6改造逐步向IPv6单栈演进。

► 阶段一 网络基础设施改造（到2023年末）

- 完成政务外网IPv6地址规划与管理规范发布，研究制定政务外网IPv6部署要求国家标准。到2023年末，政务外网原则上不再新分配IPv4地址。
- 完成政务外网IPv6统计监测指标框架制定，建设国家和省两级监测平台，定期开展政务外网IPv6发展情况监测与通报，督促落实进度。
- 各级政务外网广域网、城域网完成IPv6部署，可在原有网络进行升级，开启IPv4/IPv6双栈，建议采用IPv6+技术；具备条件的可新建IPv6单栈网络承载IPv6业务。
- 数据中心完成 NAT（Network Address Translation，网络地址转换）互访转换区建设，探索积累IPv6资源池建设和运维经验，具备条件的应用建议采用IPv6单栈方式进行部署。
- 网络运维系统、支撑系统、物联网平台完成IPv6改造，运维系统支持IPv6业务开通、故障排查等能力。
- 部门政务外网进行IPv4/IPv6双栈改造；具备条件的可新建IPv6单栈网络承载IPv6业务。
- 办公终端、物联终端进行IPv4/IPv6双栈改造，默认采用IPv6访问应用、平台和网站。
- 安全防护设备和安全监测平台与数据中心、广





域网/城域网、部门政务外网IPv6改造同步完成，IPv6防护能力不低于IPv4，满足网络安全等级保护三级要求。

- 开展IPv6+网络应用创新，扩大SRv6（Segment Routing over IPv6，IPv6分段路由）、网络切片、IFIT随流检测等新技术规模示范应用。

► 阶段二 政务云和部门政务外网改造 （到2025年末）

- 各级政务云完成IPv6资源池建设，新建应用规模采用IPv6单栈方案部署。
- 完成部门政务外网IPv6改造，新建办公终端规模采用IPv6单栈方案部署。
- 深化IPv6+应用创新，采用SRv6、网络切片、IFIT（In-situ Flow Information Telemetry，随流检测）、无损以太网等技术，推动APN6（Application-aware IPv6 Networking，应用感知的IPv6网络）等新技术发展，加快网络和应用融合。

► 阶段三 应用迁移（到2030年末）

- 各级政务外网应用完成向IPv6单栈迁移。
- 各级政务外网完成向IPv6单栈演进，关闭IPv4通道，不再提供IPv4访问。

3.2 IPv6统计监测指标框架

为全面掌握并及时发布政务外网IPv6发展数据，根据政务外网业务特点，结合国家IPv6监测平台，按照活跃用户、IPv6流量、网络就绪度、云端就绪度、数字资产、IPv6+创新应用六个维度进行统计监测，按照省市分开进行统计。

表3-1 IPv6统计监测指标框架

维度	指标	指标说明
活跃用户	IPv6物联网终端活跃连接数和占比	已经获得IPv6地址，且在30天内具备有效IPv6流量记录的物联网终端数和占比
	IPv6办公终端活跃连接数和占比	已经获得IPv6地址，且在30天内具备有效IPv6流量记录（不含Ping和域名解析流量）的办公终端数量和占比
IPv6流量	城域网IPv6流量和占比	城域网每天平均的IPv6流量和占比
	数据中心IPv6流量和占比	数据中心每天平均的IPv6流量和占比，包括公共区和互联网区
网络就绪度	IPv6网络时延	部门政务外网到数据中心入口，发送测试报文，计算多个报文平均时延
	IPv6平均丢包率	部门政务外网到数据中心入口，发送测试报文，计算报文丢包率
	IPv6网络抖动	部门政务外网到数据中心入口，发送测试报文，计算多个报文平均抖动
	广域网IPv6单栈能力	广域网采用新建IPv6单栈网络承载IPv6业务
	城域网IPv6单栈能力	城域网采用新建IPv6单栈网络承载IPv6业务
	数据中心网络IPv6单栈能力	数据中心网络采用新建IPv6单栈网络承载IPv6应用



维度	指标	指标说明
云端就绪度	云主机IPv6网络时延	终端到云主机发送测试报文，计算多个报文平均时延
	云主机IPv6平均丢包率	终端到云主机发送测试报文，计算报文丢包率
	云主机IPv6网络抖动	终端到云主机发送测试报文，计算多个报文平均抖动
	云资源池IPv6单栈能力	政务云采用新建IPv6资源池承载IPv6应用
	互联网区政务应用支持IPv6访问数量和占比	支持IPv6访问的互联网区应用数量/占比
	公共区政务应用支持IPv6访问数量和占比	支持IPv6访问的公共区应用数量/占比
	政务应用IPv6单栈能力	政务应用采用IPv6单栈数量
数字资产	IPv6数字资产	已配置IPv6地址的终端、服务器、网络设备、安全设备等资产数量和占比
IPv6+创新应用	IPv6+应用阶段	根据《“IPv6+”技术创新愿景与展望白皮书》定义“IPv6+”发展三个阶段，包括“IPv6+” 1.0、“IPv6+” 2.0、“IPv6+” 3.0，对各地方政务外网进行评估，定义网络所处阶段

04

实施技术指南

实施技术指南在政务外网IPv6演进路线图基础上针对数据中心、广域网/城域网、部门政务外网、支撑系统、运维管理系统五个部分展开描述。

4.1 数据中心

目前，政务外网数据中心已经为公众提供IPv6访问，主要是在互联网出口通过NAT翻译技术实现IPv6访问，业务系统、内部网络和安全设备大多数仍然采用IPv4地址，这种方式是在IPv6用户相对较少情况下的过渡方案。

随着国家IPv6规模部署的持续推进，IPv6和IPv4用户数和流量对比将会迎来拐点，根据《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，运营商移动网络IPv6流量占比在2023年将达到50%，IPv6将取代IPv4成为主流，数据中心要进行端到端IPv6改造。

在数据中心向IPv6改造的过程中，需要遵循“网络先行，安全同步改造”、“目标IPv6单栈，兼容IPv4”、“高可用性，平滑演进”三大原则。



网络先行，安全同步改造

网络设备是用户和应用之间的通道，必须先打通网络，应用和用户才能通信，因此建议先进行网络设备改造；在网络部署同时，需要对安全进行同步设计，同步改造。



目标IPv6单栈，兼容IPv4

终端会长期存在IPv4单栈、IPv4/IPv6双栈、IPv6单栈三种形态，演进方案需要考虑三种场景兼容。此外，要考虑目标是IPv6单栈，尽量避免二次改造。



高可用性，平滑演进

简化方案，减少日常运维和操作的负担，在演进过程中，尽量避免对运行中业务、设备进行操作，保证演进过程数据不丢失、业务不中断，将业务影响降低到最小，实现平滑过渡。

数据中心IPv6演进方案

以互联网区为例，涉及互联网接入区、应用区改造。数据中心IPv6演进方案有两种，第一种是新建资源池部署IPv4/IPv6双栈，应用部署双栈；第二种是新建IPv6资源池，承载IPv6单栈应用，通过NAT翻译实现IPv4访问。公共区改造可参考互联网区改造方案。

第一种，新建资源池部署IPv4/IPv6双栈，应用部署双栈

该方案通过端到端部署双栈，实现IPv4用户访问IPv4应用，IPv6用户访问IPv6应用，在安全防护上部署双栈检测，可以实现IPv6业务和IPv4同等防护能力，但存在以下不足：

- 双栈操作维护复杂，应用、服务器、网络设备、数据库等端到端部件都要配置双份地址，安全设备要配置双份策略，在实际部署中容易出现漏配置、错配置情况，引入运维和安全隐患。
- 设备/系统采用双协议栈运行，对外暴露的接口、漏洞加倍，需要承受来自IPv4和IPv6双重威胁和攻击，被攻破的风险增多。
- 设备和系统双栈运行，对网络、安全和系统的性能占用多，对整体性能要求提高，在增加建网成本的同时，系统复杂度的提升会导致设备、系统故障率增加。
- 向IPv6单栈演进需要进行二次改造，在实际操作过程中容易出现改造不彻底、配置遗留问题，进而增加安全风险和运维难度。

第二种，新建IPv6资源池，部署IPv6单栈应用，通过NAT翻译技术实现IPv4/IPv6互访

新建IPv6资源池，包括互联网接入区、IPv6应用区。IPv4和IPv6资源池采用不同的互联网出口链路 with 运营商对接，随IPv4和IPv6流量此消彼长，逐渐减小IPv4出口带宽，直至退网。

考虑到在互联网出口做NAT无法进行完整的安全防护检测，攻击溯源、流量审计困难，建议在IPv4资源池和IPv6资源池之间设置互访转换区，通过NAT翻译技术，供IPv4用户访问IPv6应用、IPv6用户访问IPv4应用，以及IPv4应用和IPv6应用互访，随IPv4用户和应用逐渐完成改造，将IPv4资源池和互访转换区退网，即可完成数据中心端到端IPv6单栈演进。IPv6资源池采用IPv6单栈路由协议，业务网络采用VXLANv6技术，业务网络和存储网络均采用IPv6+智能无损技术。

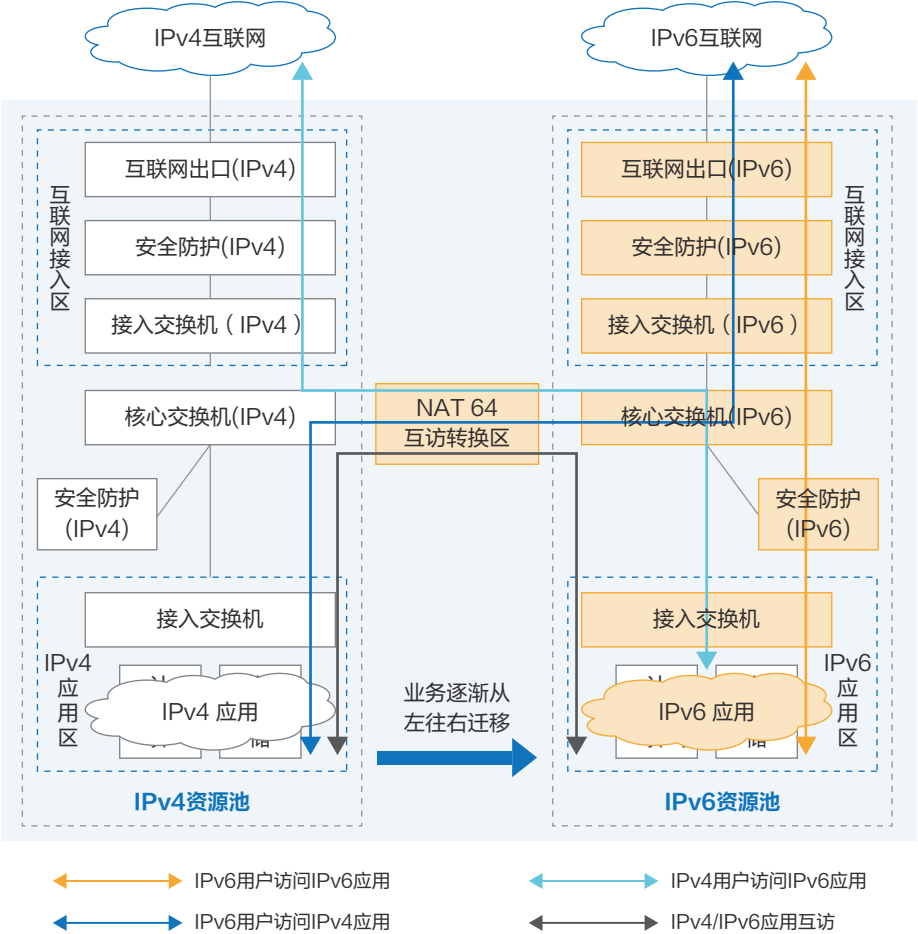


图4-1 新建IPv6资源池方案

从运维、安全、性能、向IPv6单栈平滑演进的难易度、积累IPv6单栈部署经验等方面考虑，建议采用第二种方案，通过新建IPv6资源池方式进行改造。该方案在IPv6单栈应用的基础上实现对IPv4终端的兼容，同时对现网业务影响小，可实现向IPv6单栈的平滑演进。

未实现IPv6访问的存量应用，先利用NAT翻译技术实现IPv6访问，通过监控应用的IPv6业务流量或者用户数，当超过50%时，适时启动IPv6改造迁移，部署在IPv6资源池里，原有IPv4应用可逐渐退网。

已通过NAT翻译技术实现了IPv6访问的应用，可采用监控数据中心流量的方式，当访问应用的IPv6业务流量或者用户数超过50%，适时启动IPv6改造迁移，部署在IPv6资源池里，原有IPv4应用可逐渐退网。

新建应用，可参考同类已实现IPv6访问的应用，建议优先在IPv6资源池部署，通过NAT翻译技术实现IPv4访问。

4.2 广域网/城域网

推进广域网/城域网双栈改造，为部门政务外网和政务云提供IPv6互联互通的网络支撑。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、再管理面”的改造思路，循序渐进，平滑演进。

广域网/城域网改造难点

在向IPv6的演进过程中，由于广域网/城域网分级建设、分层管理的模式决定了IPv6演进是一个长期、分地域的过程，在演进过程中存在上下级网络由于改造进度不同步导致的对接、互通问题。

广域网/城域网改造方案

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，保证现有IPv4业务不受影响。具备条件的，可采用新建IPv6单栈网络方案，IPv4业务在原有网络上运行，IPv6运行在新建网络上。

存量设备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设备的可用资源，如路由表项、上线用户数等。

城域网互联网出口采用IPv4/IPv6双栈方案，出口通过NAT66（Network Address Translation IPv6-to-IPv6，IPv6到IPv6的地址转换协议）将终端IPv6地址转换成运营商公网地址。

城域网的准入认证系统，需要同时支持IPv4和IPv6用户接入。

城域网/广域网边界安全设备开启双栈功能，确保在IPv6环境下，防护能力不低于IPv4；部署统一采集和分发系统，支持将IPv4/IPv6流量分发给监测平台进行威胁检测，在发现威胁时，结合网安协同机制，快速在网络设备上阻断，实现近源处置。

考虑到未来向IPv6单栈平滑演进，广域网/城域网IPv6改造建议采用IPv6+方案，先实现Underlay网络IPv6单栈，基于SRv6技术承载IPv4/IPv6双栈业务，通过网络编程能力，实现网络带宽、时延算路调优，提升网络专线利用率；通过网络切片能力，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；结合IFIT随流检测能力全面实现网络和业务的可视、可管、可控、可维，满足平滑演进要求。



4.3 部门政务外网

部门政务外网IPv6改造难点

部门政务外网由网络、安全设备和终端组成，目前大部分终端已经具备IPv6能力，只是还没有分配IPv6地址。部门政务外网IPv6改造难点在于保证不影响业务前提下，对安全和网络设备进行IPv6改造，对终端设备进行IPv6地址分配、监控和溯源。

部门政务外网IPv6改造思路 and 方案

部门政务外网的网络改造时，网络设备、安全设备部署IPv4/IPv6双栈；具备条件的可以新建IPv6单栈网络，承载IPv6业务；部门政务外网与城域网进行IPv6对接时，不需要NAT转换。

终端采用IPv4/IPv6双栈方案，建议通过DHCP系统分配地址，支持根据MAC（Media Access Control，媒体接入控制）地址分配固定IP地址；网络管理系统需要支持对DHCPv6（Dynamic Host Configuration Protocol version 6，动态主机配置协议版本6）、ND（Neighbor Discovery，邻居发现）等IPv6协议进行故障回放，支持对用户和IPv6地址进行监控和溯源。

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区和公共区。在部门政务外网内可通过VXLAN（Virtual Extensible Local Area Network，虚拟扩展局域网）、IPv6+网络切片等技术对网络进行隔离。

4.4 支撑系统

支撑系统包括DNS（Domain Name Server，域名服务）系统、DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）系统、AAA（Authentication, Authorization, and Accounting，认证、授权和计费）系统，在IPv6的改造过程中，应优先完成IPv6改造。

支撑系统向IPv6演进的难点在于存量系统不支持IPv6，需要进行软件升级或者新建系统支持。

- DHCP系统：支持用户动态获取IPv4/IPv6地址，可基于用户MAC地址分配固定IPv6地址。
- DNS系统：支持域名的IPv4/IPv6地址解析功能。
- AAA系统：支持IPv4/IPv6用户认证、授权、管理。

4.5 运维管理系统

运维管理系统按照国家电子政务外网“统筹协调、分级负责、属地管理”的原则，实现中央级运维管理系统与各地区各部门运维管理系统对接。

运维管理系统IPv6改造难点

在IPv4向IPv6演进的过程中，运维管理系统存在如何管理IPv6网络、如何进行IPv6的流量监控以及中央、省、地市运维管理系统之间的级联对接难点。

运维管理系统IPv6改造思路 and 方案

政务外网通过升级运维管理系统管理IPv4/IPv6网络，在新建IPv6单栈网络情况下，通过新建IPv6运维管理系统管理IPv6网络，运维管理系统应具备：



可视化能力

运维管理系统支持通过Telemetry协议实现网络拓扑、带宽、时延以及IPv4/IPv6业务质量数据（丢包、时延、抖动等）实时呈现；支持统计并呈现接入政务外网的单位数量、接入IPv6终端数量等能力；支持IPv6地址资源管理可视化。



智能化能力

支持通过Netconf/YANG协议实现业务自动化配置，支持业务配置仿真校验、配置回滚等功能，保障操作正确性；支持根据业务时延、带宽需求联合设备SRv6能力进行路径计算，提升业务体验；同时能够根据网络带宽使用率进行负载分担调整，减少网络局部拥塞情况，提升整个网络利用率；可借助网络设备IFIT随流检测能力，实现故障跨管理域的快速定界和域内快速定位；支持网络切片端到端部署，支持切片拓扑、带宽可视、带宽调整，支持切片回收；支持网络健康度评估，流量预测等能力。



级联协同能力

运维管理系统需支持中央、省、市系统的级联对接，对接数据包括但不限于节点信息、拓扑关系数据、资源类、告警类、运维协同流程类等数据，并能支持中央、省、市的多级联动故障定位。由于各省、市运维管理系统向IPv6演进的节奏并不一致，运维管理系统之间的级联对接，可以先通过IPv4对接，再逐步向IPv6对接演进。

05

缩略语

缩略语	英文全称	中文全称
AAA	Authentication, Authorization, and Accounting	认证、授权和计费
APN6	Application-aware IPv6 Networking	应用感知的IPv6网络
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
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
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
IPv6+	Internet Protocol Version 6 Plus	基于IPv6下一代互联网的升级，内涵参考《“IPv6+”技术创新愿景与展望白皮书》
MAC	Media Access Control	媒体接入控制
NAT	Network Address Translation	网络地址转换
NAT66	Network Address Translation IPv6-to-IPv6	IPv6到IPv6的地址转换协议
ND	Neighbor Discovery	邻居发现
SRv6	Segment Routing over IPv6	IPv6分段路由
IFIT	In-situ Flow Information Telemetry	随流检测
VXLAN	Virtual Extensible Local Area Network	虚拟扩展局域网





版权所有 © 推进IPv6规模部署专家委员会、国家电子政务外网管理中心办公室2021。保留一切权利。

本指南中所涉及的图片、表格及文字内容的版权归推进IPv6规模部署专家委员会、国家电子政务外网管理中心办公室所有。其中部分数据在标注有来源的情况下，版权归属原数据公司所有。本指南取得的部分数据来源于公开资料，如有涉及版权纠纷问题，请及时联络我们。

任何机构、个人在引用本指南的数据或相关内容时，需注明来源。