IPv6安全白皮书

中国移动通信集团有限公司

中国移动物联网联盟

2018 年 12 月

目 录

1 概述

IPv6（Internet Protocol Version 6，因特网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPNG（IP Next Generation，下一代因特网），它是 IETF 设计的一套规范，是 IPv4 的升级版本。随着移动互联网、物联网的发展，IPv4 的地址空间不足、不易进行自动配置等问题日益凸显，逐步向 IPv6 转型是发展的趋势。

2017 年 11 月，中办、国办下发了关于《推进 IPv6 规模部署行动计划》（以下简称“《计划》”），明确提出到 2018 年末实现 IPv6 活跃用户达 2 亿，2020 年末达 5 亿，2025 年 IPv6 网络规模、用户规模、流量规模居世界第一位。《计划》同时提出：“IPv6 规模应用为解决网络安全问题提供了新平台，为提高网络安全管理效率和创新网络安全机制提供了新思路。”

为贯彻落实中办、国办的要求，我公司已启动全网 IPv6 改造工作，并下发《中国移动 2018 年推进 IPv6 规模部署网络改造实施方案》（以下简称“《中国移动实施方案》”），计划在 2018 年实现网络可支持 IPv6 终端用户的接入及业务访问，2020 年之后新增网络地址不再使用私有 IPv4 地址的刚性管控要求。在积极推动 IPv6 规模部署的过

程中，中国移动也要充分考虑 IPv6 规模部署引入的新风险，保障 IPv6 环境下的网络信息安全。

本白皮书分析中国移动 IPv6 规模部署下的应用场景与安全影响，指出当前阶段所面临的主要安全问题，提出了 IPv6 安全技术需求和安全架构，以期推动产业链在相关方面达成一致，尽快攻克核心技术难题，从而促进 IPv6 网络安全可靠、健康发展。

2 IPv6 安全性分析

2.1 IPv6 对安全的增强

与 IPv4 相比，IPv6 的安全增强源于两个方面：一是地址空间的大幅增加对安全形成了增强，二是 IPv6 协议簇中增加了多项安全特性。

（1）反黑客嗅探与扫描能力大大提高

IPv6 地址长达 128 位，其地址空间的容量是 IPv4 的 2^{96} 倍，这意味着除非指定较小的 IP 段，广泛的 IPv6 地址扫描不可行，使得业务系统被互联网探测引擎扫描发现的可能性降低。

（2）网络信息的可溯源性显著提升

IPv6 巨大的地址空间可为每个网络设备分配唯一的地址，可保证路由器转发的每个数据包都有真实的源地址。因此，设备发出的数据包与设备地址对应，具备事后追查回溯能力。

（3）协议自身安全能力增强

IPv6 协议缺省支持 IPSec 协议，与 IPv4 环境下相比，无需另行部署加密手段（如 IPsec VPN 等）即可实现数据加密传输。

（4）部分 IPv4 中常见的攻击风险得以避免或缓解

IPv6 中无“广播”机制，因此 IPv4 网络中的“广播风暴”风险已不存在；而且 IPv6 不允许碎片重叠，IPv4 中常见的碎片攻击将得以缓解；由于 IPv6 海量的地址空间，针对 DHCP 协议的攻击难度也将增大。

2.2 IPv6 存在的安全风险

虽然 IPv6 协议进行了安全增强，但仍在三个方面存在安全风险：一是 IPv6 沿袭了 IPv4 存在的安全风险；二是 IPv4 与 IPv6 实施的双栈配置等过渡期机制引入的安全风险；三是新协议使用中形成的新安全风险。

2.2.1 协议安全风险

（1）继承自 IPv4 的安全威胁

IPv6 中协议和报文结构虽有变化，一些存在于 IPv4 网络中的攻击类型仍然存在。将在 IPv6 网络中继续存在的攻击类型包括：DoS 攻击、路由选择攻击、应用层攻击等。

（2）IPv6 特有的安全威胁

IPv6 报文结构中引入的新字段（如流标签、RH0、路由头等）、IPv6 协议族中引入的新协议（如邻居发现协议等）可能存在漏洞，被用于发起嗅探、DoS 等攻击。IPv6 特有的攻击风险包括：逐跳扩展头攻击、邻居发现协议攻击等。

不同类型设备在实现 IPv6 协议栈时，存在因编码、实施造成的安全风险。目前在 CVE 漏洞库中已有 300 余个与 IPv6 相关的安全漏洞被发布。

（3）IPv4/IPv6 过渡机制安全风险

在从 IPv4 向 IPv6 过渡的过程中，“双栈”、“隧道”、“翻译”是三种可能采用的方案，均可能引入新的安全威胁。

a）双栈机制安全风险

一是过渡期间双栈部署的网络中同时运行着 IPv4、IPv6 两个逻辑通道，增加了设备/系统的暴露面，也意味着防火墙、安全网关等防护

设备需同时配置双栈策略，导致策略管理复杂度加倍，防护被穿透的机会加倍。

二是在 IPv4 网络中，部分操作系统缺省启动了 IPv6 自动地址配置功能，使得 IPv4 网络中存在隐蔽的 IPv6 通道；由于该 IPv6 通道并没有进行防护配置，攻击者可以利用 IPv6 通道实施攻击。

三是双栈系统的复杂性也会增加网络节点的数据转发负担，导致网络节点的故障率增加。

b）隧道机制安全风险

隧道机制对任何来源的数据包只进行简单的封装和解封，所以各种隧道机制的引入，为网络环境增添了安全隐患。

一是不对 IPv4 和 IPv6 地址的关系做检查。利用隧道机制，可将 IPv6 报文封装成 IPv4 报文进行传输，由于 IPv4 网络无法验证源地址的真实性，攻击者可以伪造隧道报文注入到目的网络中。

二是不对隧道封装的内容进行检查，通过隧道封装攻击报文。例如对于以隧道形式传输的 IPv6 流量，很多网络设备直接转发或者只做简单的检查；因此，攻击者配置 IPv4 over IPv6，将 IPv4 流量承载在 IPv6 报文中，导致原来 IPv4 网络的攻击流量经由 IPv6 的“掩护”后穿越防护造成威胁。

c）翻译机制安全风险

翻译机制（协议转换）是为 IPv6 网络节点与 IPv4 网络节点相互通信提供透明的路由。翻译设备作为 IPv6 与 IPv4 互连节点，易成为安全瓶颈，一旦被攻击可能导致网络瘫痪。

2.2.2 安全设备风险

IPv6 对安全设备的主要影响包括：IPv6 环境下 NAT 机制可能缺失、IPv4/IPv6 双栈对安全设备的配置管理要求更高；IPv6、IPv4 双栈对扫描、分析设备的性能要求更高。

（1）网络层防护设备

a）IPv6 环境下所有设备均可使用全球单播地址，不需要使用 NAT 即可实现互通，同时也可能缺少 NAT 设备形成的防护。因此，防火墙（或其他安全防护设备）的安全域划分与访问控制策略需要更加严格管理，一旦出现如“可以访问任意目标 IP 与端口”的错误配置将会造成更大风险。

b）在 IPv6 与 IPv4 混合网络中，防火墙/安全网关等防护设备需要同时配置双栈策略保障安全性，对设备的功能、性能的要求更高，出现单点故障的概率增加。

（2）应用层安全防护设备

WAF、IPS、IDS 等应用层安全防护设备的 IPv6 报文解析能力、IPv6 地址格式配置（如黑白名单等）功能可能不完善；包含安全功能的网络系统（如流量控制系统等）也可能存在类似风险。

（3）网络扫描类设备

在 IPv4 环境下，系统漏洞扫描、WEB 漏洞扫描等设备一般按照 C 段/B 段地址进行扫描，目前主流的网络扫描设备可对外网或内网 IPv4 资产进行全面扫描。但 IPv6 地址长达 128 位，是 IPv4 的 2^{96} 倍，即使按 IPv6 默认的最小前缀划分区域（2^{64} 个地址）进行扫描，也难以实施。

2.2.3 业务安全风险

IPv6 对业务的影响主要存在于对 IPv6 地址格式的支持方面。

（1）DPI 类系统

部分 DPI 设备可能存在对 IPv6 报文的解析和输出不完备的风险；同时，DPI 识别规则库（如 IP 地址归属等）在 IPv6 场景下存在缺失。

（2）上网日志留存系统

上网日志留存系统在进行日志生成的过程中，需将 Radius 等设备的用户上网认证记录和防火墙 NAT 日志进行关联，可能存在不同系统间 IPv4、IPv6 匹配不一致的情况，导致日志缺失。

（3）其他业务平台

CDN、网站等业务平台存在 2.2.1 中引入过渡技术后形成的安全风险。

2.2.4 安全管理风险

由于目前还缺少相配套的安全管理措施，IPv6 的部署实施将对现网的资产监控、信息安全管控系统会产生影响，并对现有安全管理工作提出挑战。

（1）暴露面资产安全管理

当前互联网暴露面资产以“IP 地址+端口”作为标识，IPv6 规模部署后暴露面资产的标识发生变化，相关的情报获取及分析工作将受到影响，包括如下方面：

a)暴露面资产的探测稽核：目前的资产稽核主要是通过扫描工具对 IPv4 地址段进行逐个扫描，在 IPv6 环境下广泛的地址扫描已不可行。当业务系统采用 IPv6 部署时，暴露面资产的远程探测稽核要求对自有 IP 与客户 IP、已启用 IP 与未启用 IP 进行明确的区分。

b)暴露面资产指纹的获取：IPv6 条件下，需要资产指纹扫描工具具备对 IPv6 的支持，部分设备与系统需改造升级。

c)基础威胁情报的缺失：IP 地址的物理位置是当前互联网暴露面资产威胁情报分析中用到的最基本的情报之一。在 IPv4 条件下，这类

情报易得、准确率高。在 IPv6 规模部署过程中，IPv6 地址的物理位置等信息需重新积累；这类信息的缺失将影响情报分析、可视化展现。

（2）安全管理系统

4A、ISMS 等安全管理系统目前均运行在 IPv4 网络环境中，需针对 IPv6 环境进行改造。

（3）信息安全管控系统

在 IPv6 规模部署过程中，信息安全管控系统（如不良网站管控系统、手机恶意软件管控系统）需及时升级支持 IPv6，否则将存在业务系统提前改造而无法进行安全监管的风险。

3 IPv6 的安全要求

3.1 总体架构

针对过渡期间面临的各种安全风险，应构建积极的安全风险防御体系，落实安全三同步流程，将安全防护措施贯穿于 IPv6 规划、建设、运行阶段。

IPv6 安全架构如图 1 所示，在规划、实施、运营三个阶段均引入安全防护措施，并划分安全层。安全层包括协议安全、安全设备、业务安全和安全管理，在每个安全层和阶段采用多种技术手段管控，实现全流程端到端安全。

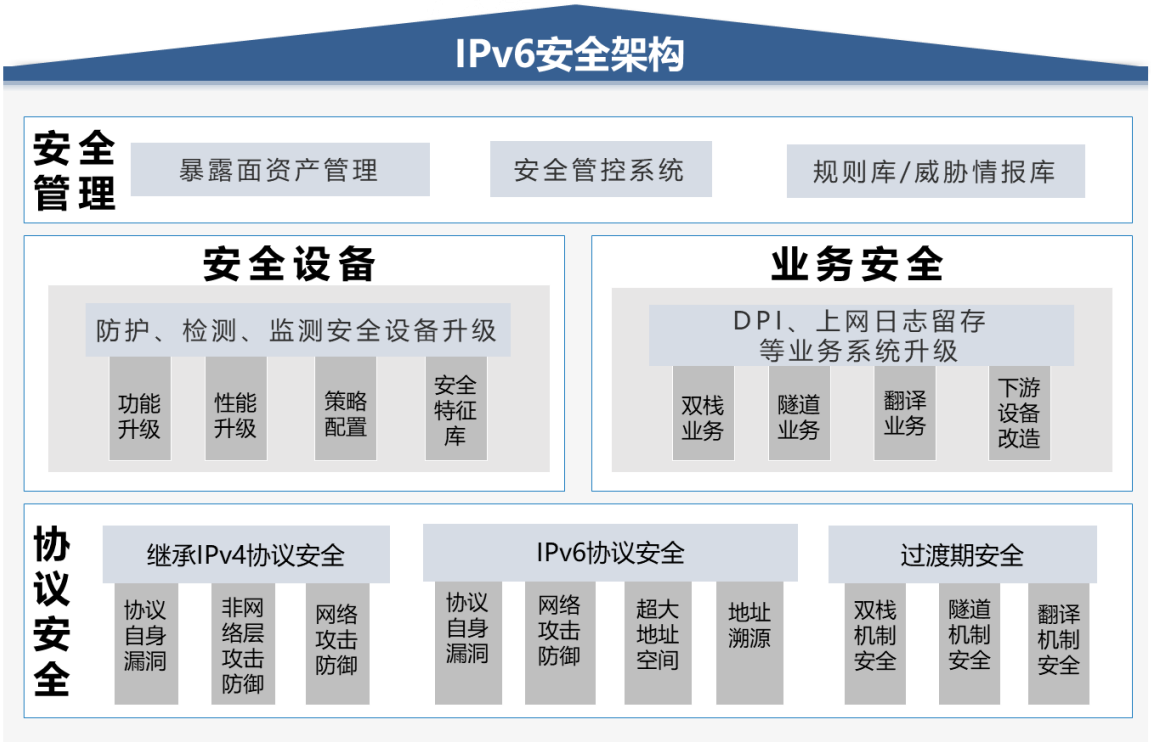

图 1 IPv6 安全架构

各层主要内容如下：

a) 协议安全：从继承 IPv4 协议安全、IPv6 协议安全、过渡机制安全三个方面，全面分析安全问题、提出应对方案；

b) 安全设备：对防护、检测、监测设备的升级改造需求进行分析，提出匹配 IPv6 环境的改造要求；

c)业务安全：对业务类型进行典型划分，如 DPI 类、上网日志类、一般业务类等，提出业务安全改造要求、测评要求；

d)安全管理：从暴露面资产、信息安全管控、威胁情报分析等方面，分析安全风险并提出安全管理措施。

3.2 能力要求

为保障 IPv6 全面部署安全，从基础安全、安全设备、业务安全、安全管理四方面构建 IPv6 安全体系。

3.2.1 基础安全能力

在基础安全方面，一方面关注协议自身安全，另一方面确保过渡机制安全。

（1）协议自身安全。针对已有的 IPv6 协议攻击手段和 IPv4 攻击的变种，设计检测手段与工具进行严格测试，保障入网设备不使用缺陷协议，安全设备能防范新增攻击手段。

（2）过渡机制安全。确定过渡机制中的双栈、隧道等机制的安全要求及实施方案，形成过渡期间的标准方案；研究并设计检测手段，保障过渡改造期间的安全。

3.2.2 安全设备能力

（1）安全防护设备

现有的网络安全防护设备（如防火墙、IPS、抗 DDoS、WAF 等）在 IPv6 相关功能上仍缺乏充分的检验和验证。IPv6 规模部署后，网络安全防护设备需从以下三部分进行升级。

a)**功能要求。**安全防护设备需支持纯 IPv6 环境下、过渡期间 IPv4/IPv6 双栈部署等场景的功能需求。例如，下一代防火墙设备需要支持 IPv4/IPv6 双栈协议及过渡时期的常用隧道技术，同时其集成的应用层网关需支持 IPv6 解析，应用识别、病毒检测、入侵防御等功能所需的规则库均需要升级，以支持 IPv6 或 IPv4/IPv6 双栈场景。

b)**性能要求。**IPv6 报文结构中支持任意数量的“扩展头”，防火墙等设备在解析报文时往往需要处理整个 IPv6 头信息链，需要细致地处理包含多个扩展头信息的数据包，甚至是含有异常扩展头的数据包。这些对防护设备提出了更高的性能要求。

c)**策略配置要求。**在 IPv6 与 IPv4 混合网络中，防火墙等安全防护设备需要同时支持双栈策略配置与管理，并应充分考虑 IPv4 和 IPv6 两个逻辑通道的安全需求，具备对安全策略配置进行一致性检查等能力。

（2）安全检测设备

通用安全检测工具（如系统漏扫、WEB 漏扫等）在 IPv6 网络中难以按网段进行扫描，上述工具的能力、使用调度策略均需研究与优化。同时，定制的专项检测工具也需要支持对指定 IPv6 地址的检测。

（3）互联网监测设备

防病毒、恶意软件、僵木蠕、DDoS 等互联网安全监测与处置设备需支持将恶意域名、数据报文特征与 IPv6 地址进行关联，形成新的威胁规则/特征库，用于网络安全检测与防护。例如，防病毒系统需将使用 IPv6 地址的病毒域名入库，并对所有使用该 IP 的域名进行排查，形成关联规则库。

3.2.3 业务安全能力

IPv6 规模部署后，各类面向用户的业务平台均需支持 IPv6 用户的访问。依据业务系统 IPv6 改造的不同实现方式，需在业务升级中按具体实施方法进行安全能力评估，并增加对应的防护手段。

a）对于采用“双栈”模式部署的业务系统，需对双栈部署导致的业务系统暴露面增加、脆弱性和威胁加倍等问题进行重点评估，增强安全防护手段。

b）对于采用“隧道”模式部署的业务系统，需重点评估隧道报文被伪造、用户身份被冒充等风险。

c）对于采用“翻译”模式部署的业务系统，需重点对翻译设备的安全防护措施进行评估，防范拒绝服务攻击等可能导致翻译设备宕机继而危及整个业务系统的风险。

d）对数据来源多样、且需要进行关联处理的安全业务系统（如日志留存等），需待下游设备改造支持 IPv6 完毕后再进行改造，防止业务数据缺失。

3.2.4 安全管理能力

（1）互联网暴露面资产管理

一是研究互联网暴露面资产稽核新手段。针对暴露面资产远程稽核在 IPv6 网络中难以进行全量或大范围地址扫描的情况，研究新的远程探测手段来发现未报备资产。

二是互联网暴露面资产报备机制需相应调整。依据现行报备工作规范、工作流程，增加对 IPv6 网络中的互联网暴露面资产管理的上报要求。同时，针对采用双栈方式部署的设备，制定暴露面资产的管理与报备要求。

（2）安全管控系统

不良网站监控、手机恶意软件监控等支持通过 IP 地址进行管控与封堵的系统需具备配置 IPv6 黑名单/白名单的能力，并能基于 IPv6 地址黑名单实现识别与封堵。

在 IPv6 规模部署后，4A、ISMS 等安全管理系统需支持 IPv6 地址解析与管理等能力。

流控系统、日志留存系统在升级支持 IPv6 的同时，需针对流量控制、域名管控、异常流量检测、文本图片还原等安全功能进行专项测试。

（3）规则库/威胁情报库

防病毒、恶意软件、僵木蠕、DDoS 等安全管控系统中各规则库（如恶意 URL、涉黄网站、恶意攻击 IP 等）关联的 IP 地址信息需及时更新。

IPv6 黑白名单地址等 IPv6 相关的威胁情报信息需及时收集整理。

3.3 安全三同步要求

IPv6 的全面推广，应遵循安全三同步要求，将 IPv6 安全要求贯穿到系统建设全过程，包括安全同步规划、建设、运行。

3.3.1 安全规划

规划阶段，应制定具体实施方案和推进工作计划，明确涉及的关键产品、网络及业务范畴，按照优先级分步骤实施。结合相关网络与系

统的建设需求，全面梳理 IPv6 带来的安全风险。同时系统规划和设计方案中，应包含整体 IPv6 安全方案,加强工程项目交付管理，确保系统现场施工严格按照设计实施，按照设计交付。

3.3.2 安全建设

建设阶段，开展 IPv6 安全测试工作，及时发现设备脆弱性等安全问题，避免设备“带病”入网。对于新业务上线前严格开展安全风险评估，根据评估结果进行整改复核，未经评估不得上线。构建安全态势感知和重点业务安全保障两方面能力，通过构建态势感知、威胁情报分析能力，开展主动防御。

3.3.3 安全运行

运行阶段，开展周期性风险评估检查、监测和审计，保证安全能力持续符合国家及内部安全管理要求；加强对设备退网环节的安全管理，对退网设备进行数据清理并及时下线。

4 中国移动推进建议

按国家《推进 IPv6 规模部署行动计划》总体部署，中国移动已全面启动 IPv6 规模部署网络改造实施工作，并计划 2018 年底前实现网络可支持 IPv6 终端用户的接入及业务访问。在 IPv4 到 IPv6 过渡期间以及 IPv6 的全面普及期间，我公司将在如下方面积极构建和完善网络

信息安全管理体系，并期望与产业链各方一起，强化技术攻关、知识共享、生态共建，共同确保 IPv6 网络信息安全可管可控。

1）研究 IPv6 地址/地址段的安全管理机制与流程。依据监管部门、公司内部（包括业务需求、IP 地址管理等）的要求，结合业内的先进安全管控经验，确定 IPv6 地址/地址段的分配、使用、报备的管理规定，保障 IPv6 地址的安全使用与管理。

2）构建 IPv6 防护体系与技术标准。与运营商、设备商、安全厂商一起，共同分析 IPv6 地址的分级保护需求，研究多层次防护、地址隐藏等机制，确保重要系统的地址安全防护；进一步完善国家、行业安全标准体系，积极推动国际标准制定。

3）加快安全设备的升级改造。结合上级监管部门的要求，与设备商、安全厂商共同研究设备与产品升级计划、升级方案，形成标准化管理机制、技术标准，确保安全改造先于业务改造完成。

4）开展 IPv6 安全测评技术攻关。目前业内针对 IPv6 协议安全的测评技术还不成熟，缺乏专项测试工具；我公司将与安全厂商一起尽快推进安全测评手段标准化、成熟化。

5）加快研究 IPv6 地址安全扫描技术。现有的安全扫描设备还难以在 IPv6 环境下进行高效扫描，需与安全厂商共同研究高效扫描机制以适应 IPv6 网络的超大规模地址空间。

6）研究 IPv6 的互联网暴露面资产管控机制。结合 IPv6 地址分配、管理、使用的制度要求，制定互联网暴露面资产报备相关制度规范；与安全厂商一起，研究改进 IPv6 网络中的远程稽核手段和威胁情报体系，适应 IPv6 环境下暴露面资产管控需求。