浅谈 IPv6 规模部署对网络安全带来的影响

（ 中国证券登记结算有限责任公司供稿）

当前，基于互联网的各种应用发展如火如荼，然而第四代互联网协议（IPv4）受协议设计限制，其网络地址资源规模存在瓶颈，严重制约了互联网应用的发展，新一代互联网协议（IPv6）应运而生。

IPv6 的产生有助于解决 IPv4 地址短缺，提升网络安全防御能力，但也同时带来了新的网络安全挑战。本文对 IPv6 协议栈进行了梳理，总结了 IPv6 对网络安全防御能力的提升，从 IPv4 协议继承的安全问题、IPv6 新协议暴露的安全问题、以及 IPv4/IPv6 过渡技术带来的安全风险三个角度系统分析了 IPv6 给网络安全带来的新挑战并提出了解决措施，希望本文可为 IPv6 规模部署中的安全体系建设提供有益的参考。

一、IPv6 协议栈简介

IPv6 全称 Internet Protocol Version 6，即“互联网协议第六版”。IPv6 是旨在解决 IPv4 服务质量难以保证、网络地址消耗殆尽等制约性问题的新技术，除此之外，它还具备有效和分级的寻址及路由基础结构、可扩展性、支持无状态和控制状态的地址分配等许多优势。

（一）IPv6 应用背景

1992 年，互联网工程任务组（IETF）成立了 IPNG 工作组，专门研究下一代互联网协议；1994 年，IPNG 工作

组正式推出下一代互联网协议 IPv6；1999 年，IETF 开始正式分配 IPv6 地址，IPv6 的协议文本成为标准草案。

2003 年，国家发展和改革委员会等八部委开展“中国下一代互联网示范工程 CNGI”的建设，第一期建设工作花费了 5 年的时间，基本达到了预期战略目标。2017 年，党中央、国务院发布了《推进互联网协议第六版（IPv6）规模部署行动计划》(以下简称《行动计划》), 我国全面进入 IPv6 发展快车道。此后，各地区、各部门深入贯彻落实党中央决策部署，进一步完善政策环境，加快推动重点领域部署，积极构建产业生态体系。

（二）IPv6 协议栈技术特点

IPv6 协议的地址结构中有 128 位（16 字节）。历经十多年的发展, IPv6 协议的设计和整体框架已经基本完善, 其技术优势包括如下几点：一是地址充裕, IPv6 的设计初衷就是为了解决 IPv4 地址空间枯竭问题, IPv6 提供了 2128 个地址空间, 与 IPv4 的 32 位地址空间相比, 其地址空间增加了 2128-232 个;二是扩展报头,根据不同协议的需求,IPv6 不仅增加了扩展头种类，并且按照协议的处理顺序合理分配扩展头的顺序；三是层次划分，用户可对 IPv6 地址进行层次性的地址规划，其目的主要是加快路由的查找速度，同时降低网络地址规划的难度。

二、IPv6 对网络安全防御能力的提升

IPv6 协议从设计之初就加大了安全问题的考虑，通过将一些安全机制固化到协议本身，增强了安全性设计，能解决

IPv4 网络中存在的部分安全问题。

（一）简化固定报头，降低攻击可能性

IPv6 协议的报文格式与 IPv4 完全不同，其主要特点是简化了固定报头并引入多种可选的扩展报头。从安全性角度看，通过简化固定报头，并规定中间路由器不必处理扩展报头（逐跳选项扩展报头除外），降低了利用异常报文头进行攻击的可能性。

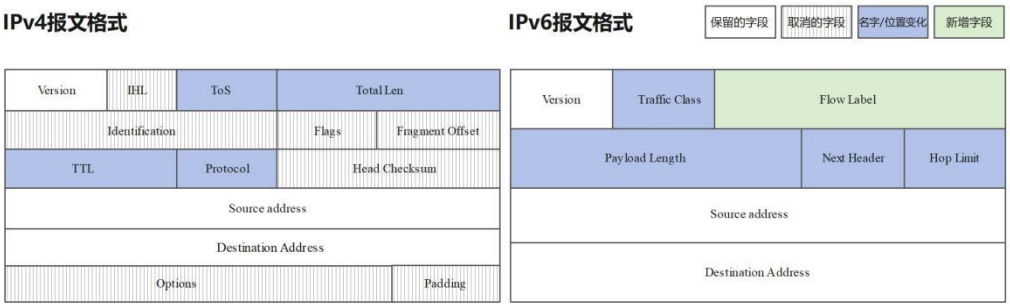

图 1　IPv6 和 IPv4 报文结构对比

（二）地址空间扩大，提升网络溯源性

在 IPv4 网络中，采用网络地址转换（NAT）技术缓解可用的地址空间枯竭问题。然而，采用这种技术不仅会破坏互联网端到端通信的特性，还隐藏了用户的真实 IP 地址，致使难以进行事后追踪溯源。从安全性角度看，由于 IPv6 网络地址空间富裕，无需进行 NAT 操作，每一台联网设备都有自己唯一的公网 IP 地址标识，且能绑定个人信息。这种特性简化了网络结构，进一步提升了网络可溯源能力。

此外，由于 IPv6 地址空间资源丰富，可以实现可聚合的层次化地址分配，使得下游的接入设备到上游的骨干设备能够层层汇聚，其优点一方面有利于在入口实现过滤，另一

方面能有效地防止源地址欺骗攻击。

站在攻击者的角度，黑客攻击的第一步通常是预攻击探测，即对目标主机及网络进行漏洞扫描并搜集有关目标主机或网络的数据，以此推断出目标主机或网络的操作系统类型、存在的漏洞、开放的服务、端口等信息，从而进行针对性地攻击。而在IPv6网络中，由于其地址空间为128位，假设网络前缀使用64位,最终目标网络中会有264个子网地址，这使得网络侦察的难度和代价都大大增加，从而进一步防范了攻击。

（三）重构编址模式，实现通信私密性

IPv6的编址可分为三类：单播、任播（泛播）和多播（组播）地址，其中单播和多播地址与IPv4地址类似，并增加了任播地址，取消了广播地址。IPv6以多播地址的方式实现原有的广播功能，以提高网络通信中一对多的效率。

IPv6单播地址包括可聚合全球单播地址、链路本地地址、唯一本地地址等。链路本地地址（FE80::/10）和唯一本地地址(FC00::/7)都属于本地单播地址，一般用于本地通信。若某服务仅局限于内部用户使用，可只给内部用户分配一个本地网络地址，其目的在于防止外部的任何人访问，从而提升安全性。另外为了进一步降低非法访问的成功率，用户即可启动自动配置，本地地址定期更新且随机配置。

（四）内嵌安全协议，提升防护安全性

当前大部分网络数据流没有加密和验证，黑客能轻易对交互报文进行篡改，主要有两方面原因：一是IPv4协议并

没有包含相关的安全机制，二是作为网络通信的加密技术，IPSec 不属于 IP 协议族。为了引入 IPSec 协议，IPv6 重新定义了 AH 和 ESP 两个扩展头，在一定程度上，IPv6 内置 IPSec 实现了端到端的机密性、完整性和抗重放攻击保护。

三、IPv6 给网络安全带来的新挑战

IPv6 网络面临的安全挑战包括从 IPv4 协议继承的安全问题、IPv6 新协议暴露的安全问题、以及 IPv4/IPv6 过渡技术带来的安全风险。

（一）协议继承的安全风险

虽然 IPv6 协议采用了不同的地址结构，在 IP 协议层进行了协议更替，实际无论是网络架构、上层协议还是应用上，IPv6 与 IPv4 并无本质上的区别，因此 IPv6 协议的推出仍无法从根本上降低 IP 协议本身的安全风险。

如表 1 所示，除了 DNS 以外，IPv6 的变化主要集中在网络层，因此安全风险和应对措施变化也都集中在网络层，传输层和应用层的安全风险与 IPv4 相比并无太大区别。因此我们需要重点考虑 IPv6 协议、ICMPv6 协议、邻居发现 ND 协议（Neighbor Discovery）以及 IPv6 路由协议的安全威胁。

网络层次	**IPv6** 变化	说明

网络层次	IPv6 变化	说明
应用层	由于 IPv6 地址长度增加，原有的 DNS 协议已不满足要求,所以 DNS 协议做了新的扩展以支持 IPv6 地址翻译。其他应用层协议都运行在 TCP/UDP 之上，协议不需要任何改变即可适应 IPv6。	例如：HTTP、FTP、DNS
传输层	得益于 TCP/IP 良好的分层设计,传输层的协议从安全角度看没有任何变化。	例如：TCP、UDP、RTP、SCTP
网络层	变化全部发生在这一层：地址长度从 32 位升级为 128 位；RIPng 代替了 RIP；OSPFv3 代替了 OSPFv2；ICMPv6(包括 ND)代替了 ICMP 和 ARP；MLD 代替了 IGMP。	例如：IP、ARP、ICMP、IGMP、IS-IS、RIP、BGP、OSPF
链路层	位于 IP 协议层以下，不受上层变动影响。	例如：以太网、Wi-Fi、MPLS 等

表 1　IPv6 在 TCP/IP 各层次变化说明

（二）新协议自有的安全风险

以 IPv6 扩展头和 ND 协议为例，二者均可能引起网络 DDoS 攻击，DDoS 攻击通过利用网络上的很多“僵尸主机”向受害主机持续发送报文，导致服务器充斥各种需回复的报文，消耗网络带宽等资源，从而无法正常提供服务。DDoS 曾在证券期货行业历史上造成过多次事故，例如 2020 年 8

月底，新西兰证券交易所网站曾连续一周遭到境外严重的DDoS攻击。

1.增扩展头引入攻击风险

IPv6相比IPv4报文格式的一个重要变化就是引入了扩展头，而协议本身不对扩展头的数量做限制，即同种类型的扩展头可使用多次。黑客可通过构造带有大量扩展头的恶意报文对目标防火墙或主机进行分布式拒绝攻击，目标防火墙或主机在解析恶意报文时会占据网络带宽等资源，从而影响设备正常的响应功能。

2.新增ND协议引入攻击风险

IPv6采用ND协议实现了IPv4中ARP协议的功能，虽然ND协议和ARP协议的协议层次不同但原理类似。所以对于IPv6协议而言，针对ARP协议的攻击如ARP欺骗、ARP泛洪攻击和中间人攻击依然有效。目前ND协议引入的风险主要分为ND欺骗和ND泛洪攻击两种。

（三）网络过渡技术安全风险

根据“IPv6行动计划”的演进步骤，IPv4与IPv6在很多业务场景下会长期存在，此时解决IPv4与IPv6网络资源的互访就必须依赖网络过渡技术。目前，IPv4与IPv6主要有3种过渡技术，双栈、隧道、地址翻译。

1.双栈机制安全风险

双栈技术指的是在网络中同时启用IPv4和IPv6两套协议栈，分别支持IPv4和IPv6网络通信。

双栈部署的网络中同时承载着IPv4、IPv6两个逻辑通

道，增加了设备的风险暴露面，极易由于IPv6的管理漏洞导致主机受到IPv6的攻击。

2.隧道机制安全风险

隧道机制指的是将IPv6数据包封装在IPv4数据包中，通过自动、手动等多种隧道配置方式保证不直连的局部IPv6网络间的相互通信。

由于隧道机制对任何数据包只进行简单的封装和解封处理，所以从安全性角度看，各种隧道机制的引入为网络通信增加了安全风险。例如使用隧道机制传输的IPv6数据包，大多数防火墙直接转发或仅做简单的检查。因此，黑客利用这一点特性将将IPv4流量封装在IPv6报文中，导致原本针对IPv4协议的攻击流量可经由IPv6封装后绕过网络防护设备造成攻击。

目前由于大多数隧道机制不内置认证、完整性和加密等安全新功能，黑客可任意拦截隧道数据包，并以仿照内外层地址的方式伪装成白名单用户向隧道内进行例如仿冒、篡改泛洪等攻击。

3.地址翻译机制安全风险

地址翻译机制（Network Address Translator，NAT）指在IPv4/IPv6网络边界处部署地址翻译网关，当有数据包经过时，对数据包头进行IPv4/IPv6地址转换和协议翻译，从而满足不同协议网络之间的相互通信，地址翻译机制主要可以分为NAT-PT和NAT64两种，但早期的NAT-PT，由于各种缺陷，已被IETF废止。由于该机制不需要进行IPv4和

IPv6 阶段的升级，具备改造周期短、成本低、部署灵活等优势，因此当前较主流的方式就是使用 NAT64 实现地址翻译。

翻译机制是为 IPv6 网络节点与 IPv4 网络节点相互通信提供对上层应用透明的路由。翻译网关作为 IPv6 与 IPv4 之间的连接设备，易成为黑客的攻击目标，一旦遭受攻击可能导致大面积网络故障。

另外，引入地址翻译机制会破坏 IPv6 协议设计中的严格的地址溯源设计。在 IPv4 与 IPv6 相互翻译中，可以实现“多对一、多对多”的灵活地址映射，从而难以对网络进行可靠的溯源和原地址验证，增加了对网络的滥用风险。

四、应对措施

针对 IPv6 从 IPv4 协议继承的安全问题、IPv6 新协议暴露的安全问题、以及 IPv4/IPv6 过渡技术带来的安全风险，主要可以采用下述措施进行应对。

（一）内外结合抵御继承风险

IPv6 从 IPv4 继承的诸多风险中，威胁最大的就是 DDoS 攻击和数据泄露，会给投资者带来巨大的经济和信誉损失。针对这些风险的应对措施总结起来主要为内部解决信任问题、外部解决威胁问题。

内部解决信任问题主要包含设备连接信任和数据互访信任两方面。而设备连接信任又可以分为三点：针对办公电脑、手机、摄像头等终端和物联接入设备的身份合法性验证，主要手段包括：一是针对固网接入的 802.1X 认证、针对移动接入的 Portal 认证、以及针对哑设备的 MAC 校验；二是

针对 OSPF、BGP 等网络协议的邻居和报文合法性以及完整性验证，主要手段包括密码验证、报文加密等；三是针对广域互联的可信验证，主要手段为 IPSsec、MACSec 等加密协议。数据互访信任主要是不同安全等级设备的互访，通常的做法为将不同安全等级的设备按区域进行隔离，区域内访问为了效率考虑通常不做管控，区域间互访则通过防火墙进行白名单管控。

解决外部威胁问题的方式主要是借助专用安全设备针对外部攻击和威胁进行防控，比如针对 DDoS 攻击，主要防护手段为在外网入口处部署 DDoS 检测和清洗；针对身份仿冒、网站挂马、恶意软件等攻击主要防护手段为在外网入口部署防火墙，基于病毒特征库对流量进行检测从而对威胁流量进行及时阻断。外部威胁还有很多防护手段，比如沙箱、恶意流量诱捕等，本文不再展开描述。

（二）安全配置抵御自有风险

在新增扩展头引入的风险防护方面，对于这种带有大量扩展头的 DDoS 攻击，可通过在防火墙上限制扩展头的数量和同一类型扩展头实例数目来进行防护。

在 ND 协议引入的风险防护方面，针对 ND 欺骗的防护可参考现有 ARP 的防御措施，通过 ND Snooping 和 DHCP Snooping 得到主机 IP 地址、MAC 地址和端口的绑定关系，根据绑定关系对恶意 ND 报文进行过滤；针对 ND 泛洪攻击的防护目前可通过配置端口的最大 ND 表项学习数量来进行防御。

（三）分类施策抵御过渡风险

过渡技术不同，对应的安全策略也会有所区别，需要根据具体选择的过渡技术来分类施策。

双栈机制下，其部署的网络中同时承载着 IPv4、IPv6 两个逻辑通道，因此在支持双栈的网络环境中，部署的网络设备和安全设备需要同步升级，尤其是相关安全特性要支持双栈，即同时支持对 IPv4 的网络安全防御和对 IPv6 的网络安全防御。

隧道机制下，面临的网络威胁主要依赖 IPsec 加密隧道来解决，IPsec 是一个对 IP 包进行加密和认证的协议包，用于保护 IP 协议的网络传输协议族(相互关联的协议的集合)。IPsec 协议集成了各种安全技术，从而建立了安全可靠的隧道。IPsec 安全架构包括三个基本协议:AH(认证头)协议为 IP 包提供信息源验证和完整性保证；ESP(封装安全载荷)协议提供加密保证；密钥管理协议(ISAKMP)在双方通信时提供共享的安全信息。ESP 和 AH 协议都有一系列的支持文档，这些文档规定了加密和认证算法。

地址翻译机制下，为了避免破坏 IPv6 地址设计中的可靠地址溯源与原地址验证机制，引入未知威胁，应该防止在标准的 IPv6 Network Prefix Translation 协议（RFC6296）之外，实现新的 NAT64 映射和翻译功能，并提供专门的安全特性作防御，主要包括：NAT64 会话数限制、用户建流速率限制、配置 NAT64 表项老化时间、过滤危险的端口号或端口段等。

五、思考与展望

IPv6 新的协议特征克服了 IPv4 一些固有的安全问题，但由于 IP 协议的开放性，IPv6 仍然继承了较多 IPv4 的安全问题，同时也引入了新的安全漏洞。IPv6 安全是个系统工程，仍需进一步进行系统考虑，为此我们建议：

一是加强 IPv6 安全产品演进和部署。为应对 IPv6 大规模推广带来的安全问题，可以通过与产业机构之间的积极协作，及时更新支持 IPv6 安全的网络产品与设备。根据《行动计划》的要求，各种安全产品应增强 IPv6 地址精准定位、侦查打击和快速处置能力，对现有网络安全保障系统进行升级改造，提升对 IPv6 地址和网络环境的支持能力。同时，为了保证 IPv6 的安全性和稳定性，在部署之前需要对 IPv6 相关的设备、网络、技术进行全面的测试，并根据其特点制订相应的测试计划，保障顺利部署。

二是促进 IPv6 安全特征库的积累。IPv6 的规模部署是一项长期工作，通过对 IPv6 安全特征库的积累，尽早实现对 IPv6 安全威胁和防护技术前瞻部署，可以有效避免重复试错的问题。通过建立公司级立体化、多维度的联防联控机制，实现“整体防控”，对 IPv6 部署过程中可能遇到的安全问题，做到早研究、早发现、早解决，防患于未然。

三是加强 IPv6 安全人才的培育。相对于 IPv6 部署的快速推进，公司在 IPv6 安全方面面临着一定的人才紧缺，需进一步优化完善安全人才数量及结构。公司可以通过积极开展与核心机构、市场机构的人才交流，实现与高等院校、

科研院所以及行业企业协同育人，通过理论知识培训、网络攻防演习、网络安全竞赛等多种方式有机结合，尽快提升人员素质，提高人才技术水平，维护公司网络安全环境，保障IPv6部署工作行稳致远。