



双栈家庭网关接入安全机制研究

陈仲华

(中国电信股份有限公司上海研究院 上海 200122)

摘要:当前 Internet 正面临 IPv4 地址耗尽,网络向 IPv6 演进的过程中。重点分析固定网络向 IPv6 演进过程中,用户侧家庭网关设备在双栈接入场景下面临的 3 个新的安全问题,包括 IPoE 业务通道防护、双栈用户地址溯源、管理口双栈地址防护。针对性地提出了 3 个安全防护技术方案,并给出了相应的实现方案和验证结果,可以提升家庭网关设备在双栈接入环境下的安全防护能力。

关键词:家庭网关;双栈接入;地址溯源;接口地址;地址跳变

doi: 10.3969/j.issn.1000-0801.2014.12.016

Security Mechanism for Dual Stack Network Accessing of Home Gateway

Chen Zhonghua

(Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: With the exhaust of IPv4 address, internet is transferring to IPv6. Firstly, security problems of home gateway in the dual stack accessing scene were analyzed, including IPoE service channel protection, dual stack address pool tracing, and manage port address protection. Secondly, three methods were given to solve the security problems. At last, a realization and experiment result was given.

Key words: home gateway, dual stack accessing, address tracing, interface ID, address hopping

1 引言

随着 IPv4 地址逐渐耗尽,近年来 Internet 开始逐步向 IPv6 演进。在网络的 IPv6 改造中,负责用户接入的家庭网关设备是一个改造的重点。虽然从目前家庭网关的硬件设备实现来看,大部分网关只需要进行 IPv6 协议栈的升级就可以支持双栈功能,但是由于在原有的网关设备中加载了新的协议栈,同时也引入了新的地址分配、管理流程和设备维护管理功能。因此,有可能带来新的安全风险。

2 双栈家庭网关接入的安全风险

2.1 双栈家庭网关接入模型的差异

在固定网络的 IPv6 改造中,很重要的改造内容就是

升级用户侧的家庭网关支持双栈,从而将 IPv6 真正引入商用网络中。在实际网络中,考虑到运营的要求,双栈家庭网关接入的基本模型与 IPv4 家庭网关的网络接入模型不会有很大差异,但是由于需要支持 IPv6 的特性,如新的地址格式、分配方式等,会给家庭网关原有的设备形态和 workflow 带来一些变化。

首先,如图 1 所示,虽然双栈家庭网关的硬件设备形态与 IPv4 家庭网关相同。但是由于 IPv6 协议本身对 IPv4 协议中的一部分工作机制进行了改动,例如引入了 NDP (neighbor discovery protocol) 替代地址解析协议 (address resolution protocol, ARP)/反向地址解析协议 (reverse address resolution protocol, RARP),引入无状态地址分配方式为家庭网关分配 IPv6 地址。这些改变会在网络中引入

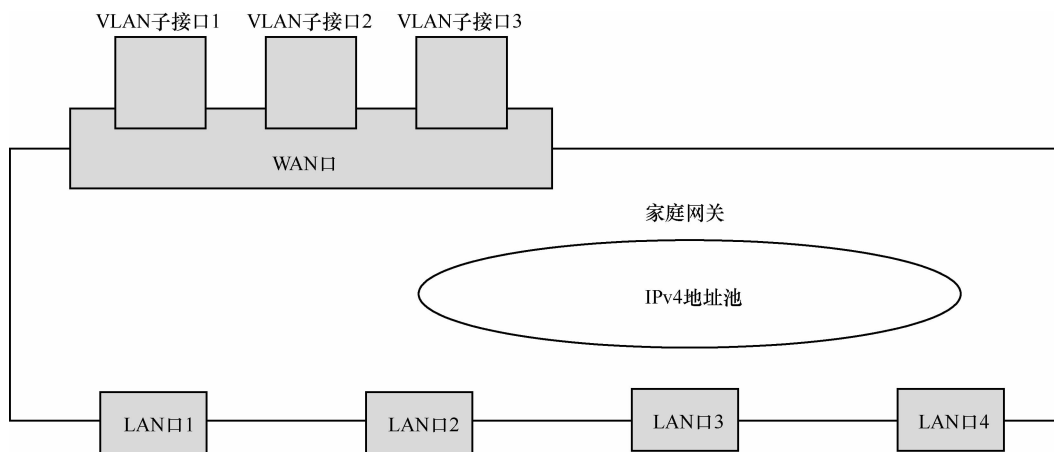


图1 双栈家庭网关的设备形态

新的安全风险。

家庭网关一般有5个物理以太网端口,其中一个连接网络侧的WAN(wide area network,广域网)口,4个是连接家庭网络的LAN(local area network,局域网)口。LAN口可以配置成连接普通个人电脑,并采用PPPoE拨号方式连接到城域网的逻辑端口,也可以配置成连接IPTV机顶盒、VoIP、WLAN AP设备,并采用IPoE方式连接到逻辑端口。不同的LAN端口的数据分组在通过WAN口发送到网络之前,会打上不同的VLAN标记,城域网边缘的业务网关设备通过识别不同的VLAN标记将这些流量转发到不同

业务网。

家庭网关WAN口的物理端口只有一个,通过VLAN子接口方式将不同LAN口的流量分组到不同的VLAN中。从现状来看,WAN口一般有3个VLAN子接口,一个是承载PPPoE流量的通道,一个是承载IPoE流量的通道,还有一个是承载家庭网关本身的远程管理流量的通道。

其次,双栈家庭网关接入IPv6网络时,认证过程和地址分配的过程与IPv4网络有诸多不同之处,如图2所示。

在双栈家庭网关接入场景中,由于网络侧要为家庭网

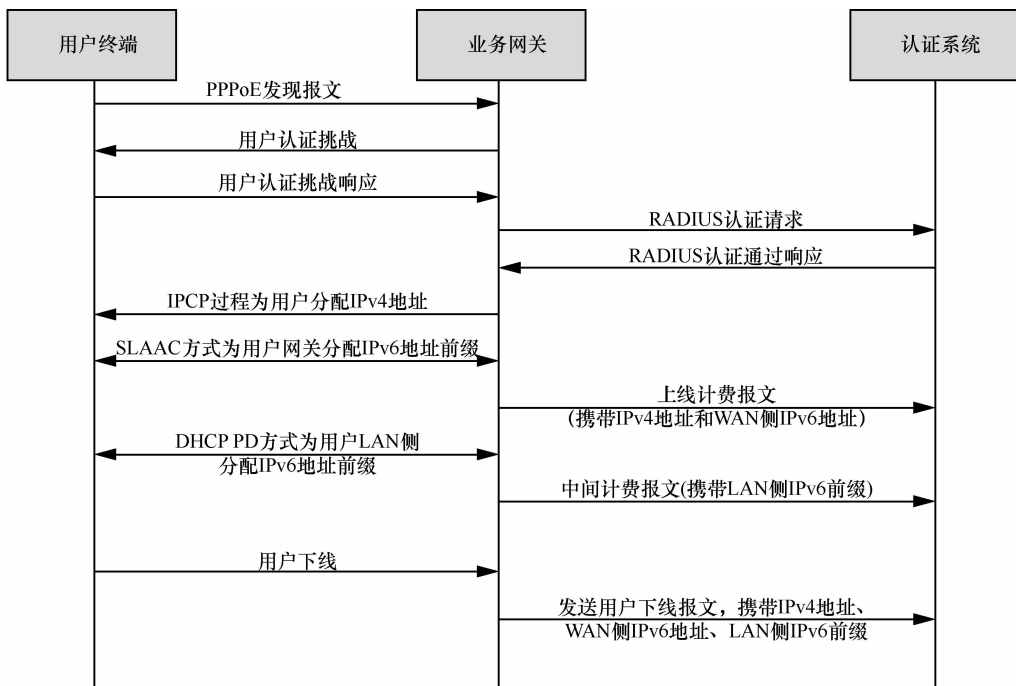


图2 家庭网关双栈接入流程

关分配双栈地址,导致分配过程复杂化,需要通过多个协议报文的交互才能够完成。同时,记录用户地址的过程分为多个 RADIUS 报文,给用户地址记录与处理带来差异。

最后,双栈家庭网关的远程管理端口一般都配置有独立的 VLAN,可以实现与业务 VLAN 端口流量的隔离。在 IPv4 网络中,为管理口分配私网 IPv4 地址,并在网络侧进行 NAT(network address translation,网络地址转换),远程主机在不知道 NAT 信息时是无法主动发起对家庭网关管理口的访问的。但是在双栈网络中则不同,如果为管理口分配 IPv6 地址,IPv6 地址都是公网可路由的地址,因此远程主机有可能访问到双栈家庭网关的管理口。

2.2 双栈家庭网关接入安全

从实际引入 IPv6 的过程来看,家庭网关接入双栈网络主要面临 3 个方面的安全问题:其一是 IPoE 接入通道中,不同家庭网关之间的 NDP 安全问题;其二是用户地址分配方式改变导致的对家庭网关的用户地址溯源的问题;其三是管理口 IPv6 地址的防护问题。

在 IPoE 场景下,由于 IPoE 不具备 PPPoE 的天然用户隔离的特性,因此同一接入业务网关下的所有家庭网关彼此都能够互相访问,虽然在部署上可以通过为所有终端分配独立的 VLAN 来进行二层隔离,但是依然存在实际部署中配置困难、VLAN 数量的 4 096 限制等问题,导致实际部署的效果不佳。目前业内针对 IPv6 NDP 的安全防护措施主要采用 SEND(secure neighbor discovery)技术来对 NDP 交互过程中的双方 IPv6 地址进行加密和验证,以防止伪造通信主机身份的攻击。但是 SEND 技术的部署存在不少问题,首先 SEND 技术基于 RSA 公一私密钥算法,需要在终端和网络侧设备的协议栈中嵌入这一密钥算法才能够实现 SEND 认证的过程。对于网络侧而言,网络设备的升级相对简单,但是对于终端侧而言,大量存在的老旧终端或者计算能力较差的终端并不能很好地部署 SEND 技术。其次,SEND 技术的兼容性并不理想,在 SEND 技术描述的场景下,在一个接入网关下,所有的终端都必须支持 SEND 的验证,如果部分终端不能够支持,从严格意义上来说将不能接入网络,否则将导致整个 SEND 机制失效。由于 SEND 技术存在以上两个实际应用上的难点,导致在实际网络中部署 SEND 技术困难,同时现有主流的终端设备支持 SEND 技术的也并不多见。

与 IPv4 网络类似,家庭网关接入 IPv6 网络时也存在用户地址溯源的要求,在 IPv4 网络中,用户地址溯源的实

现依赖于对用户拨号时的 RADIUS 上线计费报文携带的地址信息的记录。IPv6 地址分配过程与 IPv4 不同,由于 IPv4 接入时家庭网关可以实现 NAT 功能,家庭网络内部是不需要网络为其分配 IPv4 地址的,通常家庭网络内部由家庭网关自动为其分配私网 IPv4 地址。但是在 IPv6 网络中,由于不存在 NAT 技术,网络侧除了需要为家庭网关分配 WAN 口地址外,还需要为家庭网络内部分配公网 IPv6 地址段,并由家庭网关维护这个地址段的使用。由于多个地址/地址段的分配存在时间上的差异,例如在一些极限情况下存在 IPv4 地址先协商成功,间隔数十秒再协商成功 WAN 口的 IPv6 地址,再间隔数十秒协商成功 LAN 口的前缀地址段。由于上线报文关系到用户拨号成功后,能否正常使用网络,如此长时间的等待上线计费报文,将导致家庭网关被迫下线。因此,这样的地址分配过程使上线报文无法携带所有的地址分配信息,后续协商成功的地址必须通过扩展的中间(interim)更新 RADIUS 报文携带。由于目前认证系统并不具备处理这样报文的能力,因此需要对现有系统进行升级改造,才能完成对双栈地址的获取和记录,才能实现对用户双栈地址的溯源。

除此之外,在网络向 IPv6 演进过程中,由于要解决 IPv4 地址耗尽的问题,还可能应用到多种过渡技术。这些过渡技术主要依赖于使用私有 IPv4 地址,并通过在网络侧使用 NAT(地址转换)技术,通过端口号来复用公网 IPv4 地址,从而延缓地址耗尽的发生。因此,在地址溯源过程中,在网络侧捕获的公网 IPv4 地址并不能直接对应到用户账号,必须通过查询 NAT 的映射信息,实现对应关系的查询。但是传统 NAT 是动态发生的,其转换的信息量巨大,如何处理私网地址的转换信息,也是用户溯源中必须解决的问题。

对于双栈家庭网关的管理口,由于使用了 IPv6 公网地址,也存在一定的安全风险。在 IPv4 网络中,对于家庭网关的管理需要网关启动以后,主动在管理平台上进行注册,然后平台侧才能实现对其访问。因此,从第三方角度来看,由于无法猜测这个私网地址在 NAT 网关上映射的公网地址和端口号,针对家庭网关管理口的远程主动攻击是不可行的。但是,在 IPv6 网络环境下由于管理口地址前缀是网络规划的,而接口地址根据硬件 MAC 地址生成且与业务端口的接口地址一致,因此第三方攻击者很容易猜测或者扫描到家庭网关的管理口 IPv6 地址,并从远程发动攻击。



3 安全防护技术与实现

3.1 IPoE 业务通道的防护

3.1.1 SEND 技术简述

SEND 协议是一个由 IETF 定义的、在 IPv6 节点之间运行的、验证节点身份信息(主要是 MAC 地址与 IPv6 地址映射关系)的协议。该协议通过在 NDP 可选项功能中扩展 CGA(cryptographically generated address)选项和公私密钥机制,实现对地址映射关系的验证,可以在开放的 IPv6 网络中,防止恶意节点盗用正常节点 IPv6 地址,从而防止类似网关重定向攻击、邻居不可达检测攻击和二层地址解析攻击等攻击行为,提升 IPv6 网络的安全性。

SEND 技术应用的场景主要有以下 3 种:

- 企业内部局域网络场景;
- 运营商网络场景;
- Ad Hoc 网络场景。

这 3 种场景从安全需求角度和实现安全防护的难度来说是递增的。在企业内部局域网中,由于网络存在统一的管理员,所有接入网络的节点和网络的出口网关设备是可以受到管理员控制的,其安全性可以通过统一的管理得到保证。运营商网络中,整个网络有一个统一的接入点,一般是运营商网络的业务网关路由器设备,这个设备由运营商统一管理,可以视为可信任的设备。整个运营商网络中所有的用户接入设备均视为不可信任的设备,只有通过验证才能够认为是可信设备。同时,用户接入设备在无线网络状态下,也可以进行互相通信,但一般这种通信的数据报文都需要经过业务网关路由器的转发。在 Ad Hoc 网络中,没有一个类似于运营商网络的中心业务网关路由器,接入节点都是随机与周边节点进行通信的。因此,在 Ad Hoc 场景下,需要节点自身能够进行身份的加密,同时还需要周边其他节点能够根据一定的加密规则,对节点的身份信息进行验证。

SEND 技术应用在实际网络中存在一定的缺陷,主要有以下两方面。

- 由于公一私密钥对是由发送节点自身产生的,本身没有经过安全认证。因此,这个密钥对信息本身存在伪造的问题。
- 节点地址生成。节点地址通过 CGA 算法生成完毕之后,需要进行地址冲突检测,此时恶意节点有机会通过不断发送地址冲突响应来干扰正常节点的 CGA 地址生成,最终迫使被攻击终端无法生成有效

地址连接进网络。

造成这两个缺陷的本质原因是 SEND 技术中使用的验证 IPv6 地址有效性的公一私密钥对,这一机制本身需要解决安全问题。通常情况下,SEND 技术需要配合一套密钥分发和验证的证书机制,保证密钥不被攻击者伪造。但是一般基于证书认证机制的密钥分发技术过于复杂,且需要建设独立的第三方验证平台,例如在互联网上常用的基于 PKI 的公用证书认证机构。但是,对于二层接入网络的验证来说,由于每一个局域网终端接入都需要证书集中验证和管理,这样的验证机制显然将造成很大的浪费。因此,在实际网络中引入 SEND 机制时需要考虑进行改进。

3.1.2 基于 SEND 技术的改进

首先,从家庭网关接入 IPv6 网络的拓扑情况来看,一般接入网络属于逻辑星型或树型连接。所有用户终端接入网络的设备通过有线或无线链路接入运营商提供的接入业务路由器设备。在没有进行身份验证和绑定之前,所有用户终端都属于不可信任设备,网络中心的接入业务路由器设备,由于是运营商提供的,可以视为可信任设备,所有用户终端设备必须无条件地信任中心设备。这一安全模型如图 3 所示。

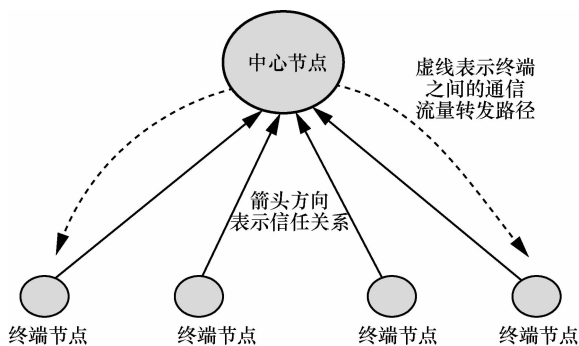


图 3 SEND 技术改进安全模型

在这个模型中,有如下两个假设前提:

- 所有节点必须无条件信任中心节点,中心节点不能被假冒;
- 所有接入的终端节点的通信流量,无论是二层还是三层数据报文,都必须经过中心节点转发,包括二层广播报文,也必须由中心节点转发。

从实际家庭网关接入网络的拓扑来看,这样的假设是合理的。一般网络中心节点的角色由网络边缘的业务路由器承担,负责对接入用户终端最初的身份绑定信息进行验证,并对终端与终端之间的安全争议和身份冲突进行仲裁。由于被攻击终端通常先于攻击者连接到网络内,其相

关的地址验证信息将先于攻击者被业务路由器缓存下来,随后发生的攻击报文在经过中心的业务路由器时,由于地址信息与缓存中的地址信息无法匹配将被丢弃,攻击者的攻击行为将不能够实施。这一方法的一个典型的实现过程如图 4 所示。

图 4 中终端身份缓冲表是这一改进技术方案的核心。这一缓冲表一般属于中心路由器中的一个模块,该模块的作用就是存放当前已正常接入中心路由器的终端的 IPv6 地址、MAC 地址、CGA 选项、终端家庭网关的接入线路信息参数等信息。当一个正常的家庭网关接入网络时,其发送的 NDP 报文将首先判断是否携带 CGA 选项,如果携带则证明这是一个支持 SEND 技术的终端,需要使用 CGA 算法对其地址进行验证,如果 CGA 验证不通过则判为攻击,静默丢弃该报文;如果 CGA 验证通过,则中心路由器将到身份缓冲表中进行下一步的验证。如果终端不支持 SEND

技术,则直接进入身份缓冲表的验证过程。

一个进入身份缓冲表进行验证的报文,可能遇到以下两种情况:

- 如果地址及相关信息没有在身份缓冲表中,那么这个报文不会是一个攻击报文或者即使是一个攻击报文也没有具体的攻击目标;
- 如果报文的地址信息已经存在于缓冲表中,那么需要将报文中的信息与缓冲表中的信息进行核对,比如与缓冲表中记录的 CGA 信息是否一致,与缓冲表中的终端 MAC 地址是否一致,与缓冲表中的接入线路信息是否一致等,如果一致则证明是一个合法的 NDP 报文。如果不一致则判断为一个攻击报文,并丢弃。

3.2 用户地址溯源

3.2.1 双栈家庭网关地址溯源需求

与 IPv4 网络中的地址溯源相似,在 IPv6 网络中地址

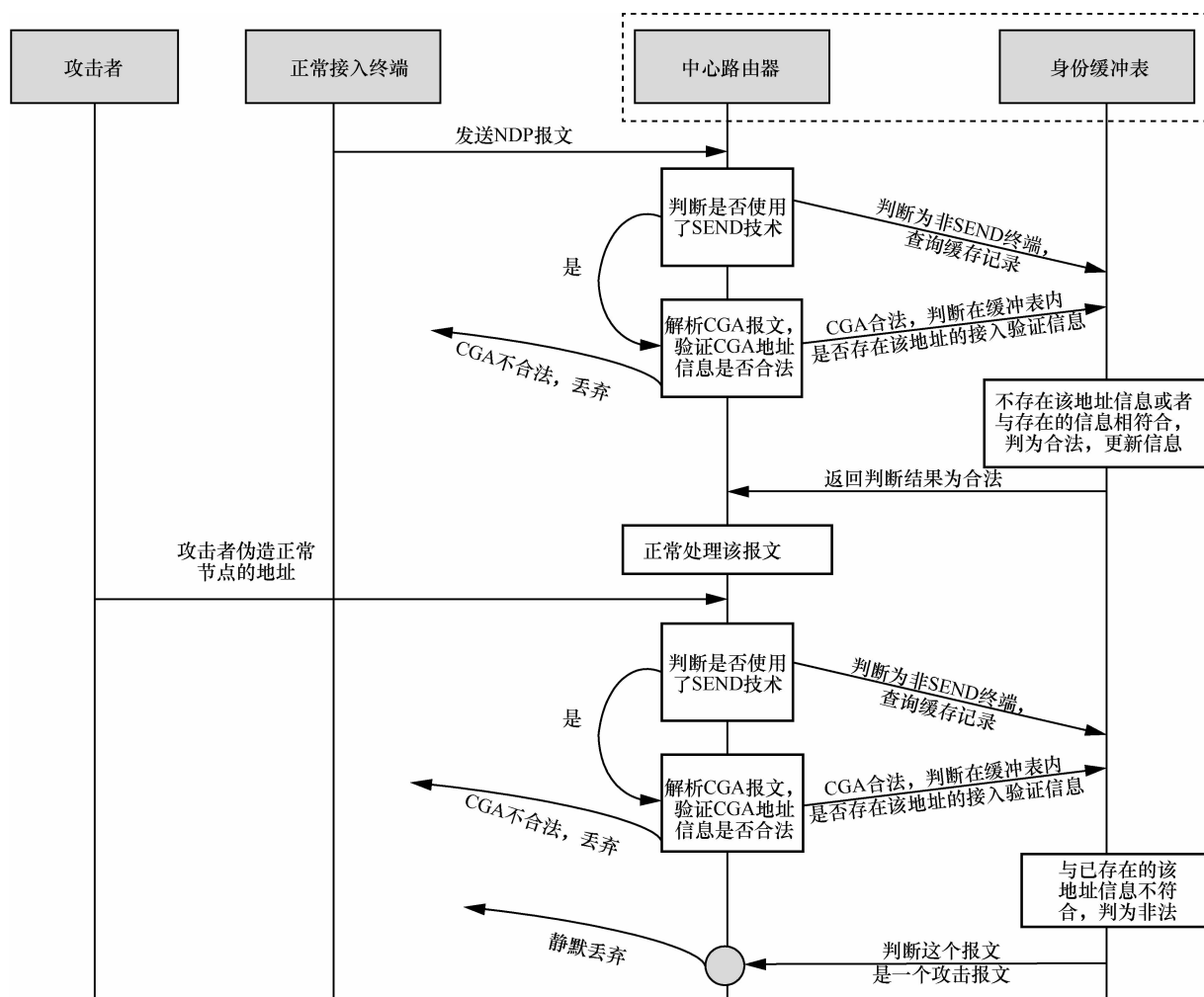


图 4 SEND 改进技术实现流程



溯源也要求网络管理者能够通过 IPv6 报文中的源 IPv6 地址信息来找到对应发送报文者的用户身份信息。但是由于 IPv6 网络的地址分配方式与 IPv4 网络不同,因此其溯源的方式也有 IPv4 网络有一定的差异。

在 IPv6 网络中对用户地址进行溯源需要考虑多种场景,其与 IPv4 网络的不同点见表 1。

由于账号与地址匹配信息的差异,IPv6 地址或前缀对应的账号信息可能需要经过多次的匹配查询,才能够实现溯源。这对溯源查询系统的性能有一定的要求。因此,在实现 IPv6 地址溯源时需要采用逐次查询的方式,才能够高效地实现基于地址信息的账号匹配查询。首先,在获得一个需要查询对应账号的 IPv6 地址后,根据网络中规划的地址前缀信息,从小到大在认证系统的在线信息表或者日志中进行查询。例如网络中规划使用了 56 bit 的前缀和 64 bit 前缀,则需要先匹配查询 56 bit 前缀,再从 56 bit 前缀的匹配结果中查询 64 bit 前缀对应的信息,最后再尝试精确匹配到 128 bit 的 IPv6 地址。这样可以逐步缩小匹配的数据集,避免反复在所有记录中查询结果,导致系统性能下降。

在 IPv6 过渡时期,网络中通常还需要部署各种过渡技术,而过渡技术的引入一般都会引入新的地址溯源问题,例如目前比较常用的私网双栈过渡方式中,网络中同时部署 IPv4 协议栈和 IPv6 协议栈,但是 IPv4 协议栈为用户分配的是私网 IPv4 地址,当用户上网访问时通过 NAT 技术将一个公网 IPv4 地址和 TCP/UDP 端口号动态地映射给一个私网地址用户使用,这样在同一时间多个私网地址用户可以共享同一个公网 IPv4 地址,以达到节约 IPv4 公网地址的目的。但是,这种方法将引入 IPv4 私网地址和 IPv4 公网地址+端口号的动态映射关系,用户访问的网站上获得的用户公网 IPv4 地址并不能直接对应到网络分配给用户的私网地址和用户的账号,这使得原本的 IPv4 地址溯源流程无法进行。此外,另外一些过渡技术,例如 NAT64、DS-Lite 等也会引入类似的技术问题,因此,在 IPv6 过渡场景中需要对现有的溯源流程进行修改,引入对地址转换信息的保存和映射处理,才能够满足过渡场景的溯源要求。

3.2.2 双栈家庭网关地址溯源方案

首先,对于 IPv6 地址的溯源其原理与 IPv4 地址的溯源相同。但是,家庭网关接入双栈网络采用的是单 PPPoE 会话承载双栈通信,也就是在一个 PPPoE 会话内实现双栈地址的分配和管理,同时要求 IPv4 和 IPv6 两个协议栈不互相干扰。因此,家庭网关拨号接入网络时在 PPPoE 的 LCP 阶段与现有 IPv4 接入一致,完成用户账号认证。但是在 IPCP 阶段与 IPv4 不同,除了要完成 IPCPv4 的地址协商过程之外,还要实现基于 SLAAC (stateless address autoconfiguration, 无状态地址自动配置) 的家庭网关 WAN 口地址分配和基于 DHCP PD 的家庭网络 LAN 口地址段的分配。这一地址分配方式将导致在用户上线过程中除了 RADIUS 上线报文之外,还存在多个用户在线地址更新的 RADIUS 更新报文。因此溯源系统需要支持对多个 RADIUS 报文分别携带部分地址分配信息的处理与整合。

其次,对于 IPv6 过渡技术中的私网地址溯源,一般网络中私网地址到公网地址的转换的功能由 NAT 网关(CGN 设备)承担,由于 NAT 表项的建立和拆除是动态的、随机的,如果要记录用户所有的转换信息的新建和删除,则日志信息的数量非常巨大。为了应对私网地址转换的海量日志信息,采用了基于地址段管理的 NAT 设备转换算法。当用户建立第一个 TCP/UDP 会话时,在 NAT 网关设备上将为用户分配一个指定的端口段区域,如端口 1000~3999。这一端口号区域内的所有端口都将为这个用户保留,用户以后需要建立地址映射时直接选用该区域内的端口即可。通过这一方法,NAT 的日志信息只需要在用户建立端口区域的时候发送即可,以后用户使用端口区域内的端口映射将不再发送日志信息,同时 NAT 系统处理老化的日志信息,也只需要在端口范围内所有的 NAT 会话信息都老化后,系统回收所有 NAT 资源时才发送。因此,NAT 网关上原来针对 4 000 个端口的日志信息被合并成 1 个信息,即使不考虑每个端口因为老化和再分配引起的重复日志发送信息,对于日志信息的压缩比例也将达到 4 000:1。相当于日志处理系统每秒只需要处理 360 KB 日志信息,而后台

表 1 IPv6 溯源与 IPv4 溯源信息的异同点比较

地址分配方式	IPv4		IPv6		
	DHCPv4	IPCP	DHCPv6	DHCP PD	SLAAC
账号对应	IPv4 地址 (32 bit)	IPv4 地址 (32 bit)	IPv6 地址 (128 bit)	IPv6 地址前缀 (小于 64 bit)	IPv6 地址前缀 (等于 64 bit)

缓冲存储 1 年的日志信息数量也仅有 11.4 TB, 如不采用压缩方法, 相同规模的网络中日志量将达到 45 PB/年。

在实现 RADIUS 地址分配报文的收集和 NAT 日志的收集后, 将这两方面的信息进行整合就能够实现对分配给双栈家庭网关的双栈地址的溯源, 其总体流程如图 5 所示。

3.3 管理口 IPv6 地址的防护

3.3.1 基于地址跳变的防护方法

地址跳变通信, 是一种在 IP 通信过程中隐藏通信双方 IP 地址的技术。其基本原理是在实际通信中, 通信双方按照一定的算法任意改变通信连接的 socket (套接字) 的 IP 地址参数进行通信。这个算法可以是按通信时间的不同、报文大小不同或者实现商定的随机码的不同进行地址的变换, 只需要通信双方在通信开始时, 进行协商, 达成算法的一致即可。同时, 由于 IPv6 地址划分的特性, 地址前缀部分是由网络分配, 用于 IPv6 的路由, 这部分一般不能随意变动, 否则将影响网络的路由, 同时也会导致网络的路由收敛震荡。而接口地址部分一般不参与网络的路由, 因此这部分的地址可以通过实现本文提及的地址跳变算法, 达到通信保密的目的。

3.3.2 形式化证明

基于 IPv6 接口地址的跳变, 可以有效地提升系统的安全性。基于网络安全领域常用的攻击图, 分析其对于安全性能的加强, 如图 6 所示。

其中 S_n 表示攻击者需要完成的攻击行为, 例如 S_0 可以表示攻击者获得目标的 IPv6 地址。在攻击图中攻击者的最终目标是到达 S_9 状态, 这意味着攻击者成功获得目标主机的控制权或者是目标瘫痪, 在本文中代表攻击者获得双栈家庭网关的管理控制权或者使家庭网关瘫痪。在攻击者从 S_0 状态到达 S_9 状态过程中, 有多个路径可以选择, 每个不同的 S_n 节点代表了攻击者需要完成的不同的攻击行为, 这些行为的组合最终能够使攻击者达成攻击的目标。例如 $S_0 \rightarrow S_1 \rightarrow S_3 \rightarrow S_7 \rightarrow S_9$ 可以表示攻击者扫描发现 IPv6 地址 (S_0) $\rightarrow$ 对端口进行扫描, 发现打开的监听端口 (S_1) $\rightarrow$ 采用 TCP 半开连接进行攻击测试 (S_3) $\rightarrow$ 启用 TCP SYN flood 攻击 (S_7) $\rightarrow$ 导致家庭网关瘫痪 (S_9)。

图 6 中, P_n 表示攻击者在该节点成功的概率, q_n 表示在该节点攻击失败的概率。 P_{mn} 表示攻击成功之后, 攻击者选择从 m 到 n 的攻击路径的概率。由此可见攻击者通过 $S_0 \rightarrow S_1 \rightarrow S_3 \rightarrow S_7 \rightarrow S_9$ 攻击成功的概率为: $P_0 \times P_{01} \times P_1 \times P_{13} \times P_3 \times$

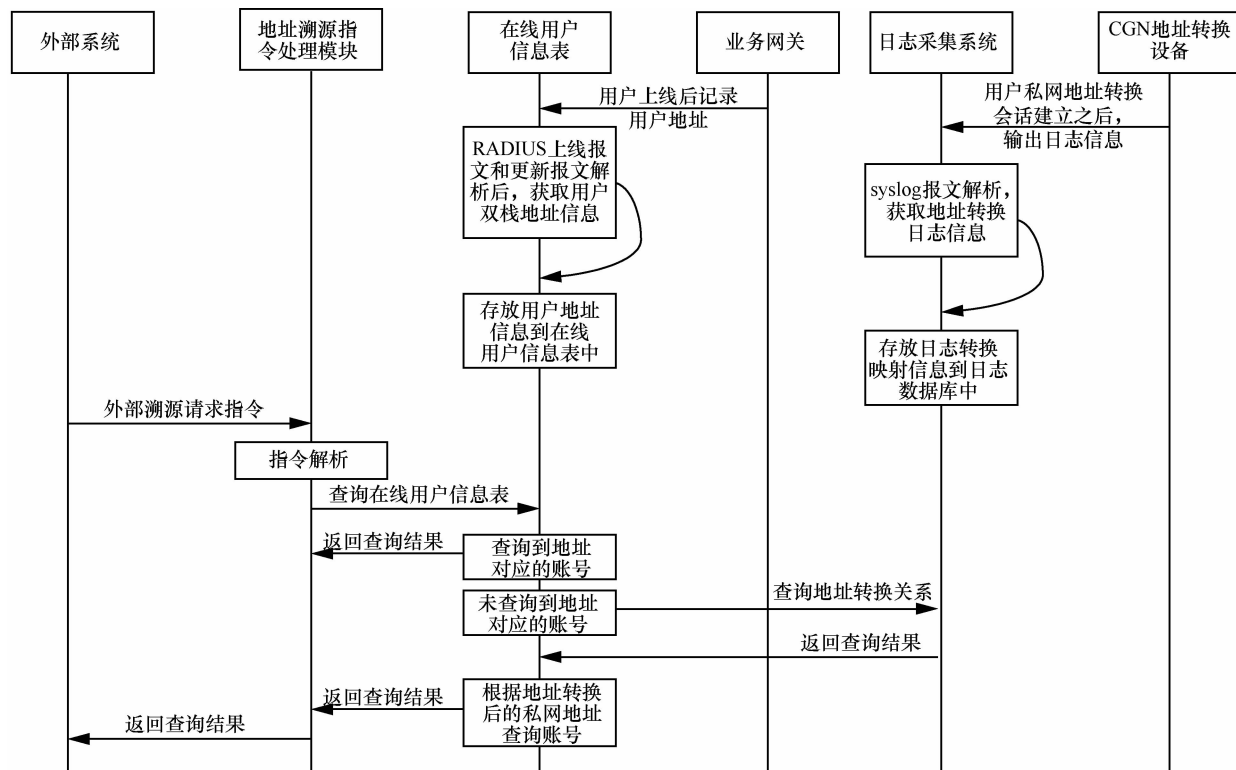


图 5 溯源系统总体流程示意



$P_{37} \times P_{77} \times P_{79}$, 以此类推, 可以得到图 6 的各个攻击路径成功的概率方程组:

$$P(S_0 \rightarrow S_1 \rightarrow S_3 \rightarrow S_7 \rightarrow S_9) = P_0 \times P_{01} \times P_1 \times P_{13} \times P_3 \times P_{37} \times P_7 \times P_{79}$$

$$P(S_0 \rightarrow S_1 \rightarrow S_5 \rightarrow S_7 \rightarrow S_9) = P_0 \times P_{01} \times P_1 \times P_{15} \times P_5 \times P_{57} \times P_7 \times P_{79}$$

$$P(S_0 \rightarrow S_2 \rightarrow S_4 \rightarrow S_8 \rightarrow S_9) = P_0 \times P_{02} \times P_2 \times P_{24} \times P_4 \times P_{48} \times P_8 \times P_{89}$$

$$P(S_0 \rightarrow S_2 \rightarrow S_6 \rightarrow S_8 \rightarrow S_9) = P_0 \times P_{02} \times P_2 \times P_{26} \times P_6 \times P_{68} \times P_8 \times P_{89}$$

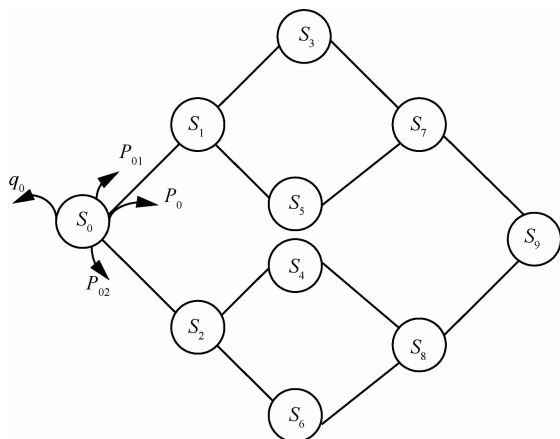


图 6 地址跳变技术的攻击

攻击者攻击成功的总概率可以看作以上所有攻击路径成功的概率之和。由此可知, 要减小攻击者攻击成功的概率, 首先可以选择在可能的条件下减小所有节点被攻击成功的概率, 即减小所有 P_n 的值。其次, 在条件有限的情况下, 可以在一些关键节点上部署防御措施, 所谓关键节点也就是在所有攻击路径中都出现的节点, 一旦减小这个攻击节点的成功概率, 无疑将大幅减小攻击者攻击成功的总概率。

由于在 IP 网络中的攻击行为, 目标的 IP 地址是所有远程攻击的通信基础, 无疑在发动实质性攻击之前获取目标的 IP 地址是所有攻击的前提, 因此具有攻击图中的关键节点的特性。基于 IPv6 接口地址跳变的技术, 增加了目标地址获取的难度, 相当于减少了这一关键节点的成功概率, 因此可以提升整个系统的安全性能。此外, 由于 IPv6 目标地址的跳变, 使得部分需要反复尝试的攻击行为, 例如密码猜测、DDoS 攻击等的成功可能性降低, 也可以被认为降低了部分 P_n 的值。因此, 也有助于提升整个系统的安全性。

但是, 基于 IPv6 地址跳变的防护方法, 只能适用于封闭的通信系统, 这类系统不需要将自身的 IPv6 地址公开给所有人, 例如借助于 DNS, 使自身地址可以被全球访问, 而只需要供特定系统访问。

从双栈家庭网关的管理口功能来看, 其只需要提供给管理平台访问, 外部系统的访问是应该被积极拒绝的。因此, 这一方法可以适用于针对双栈家庭网关管理口的防护, 同时根据攻击图的分析, 这种防护也是有效的。

3.3.3 技术实现与验证

双栈家庭网关的管理口 IPv6 地址跳变子系统由两部分组成: 第一部分是部署在家庭网关上的地址跳变子系统客户端; 第二部分是部署在管理平台的地址跳变服务端, 两端程序在通信过程中将变换使用的 IPv6 地址, 在同步的情况下, 两端的通信报文将能够正常传输。地址跳变实现流程如图 7 所示。

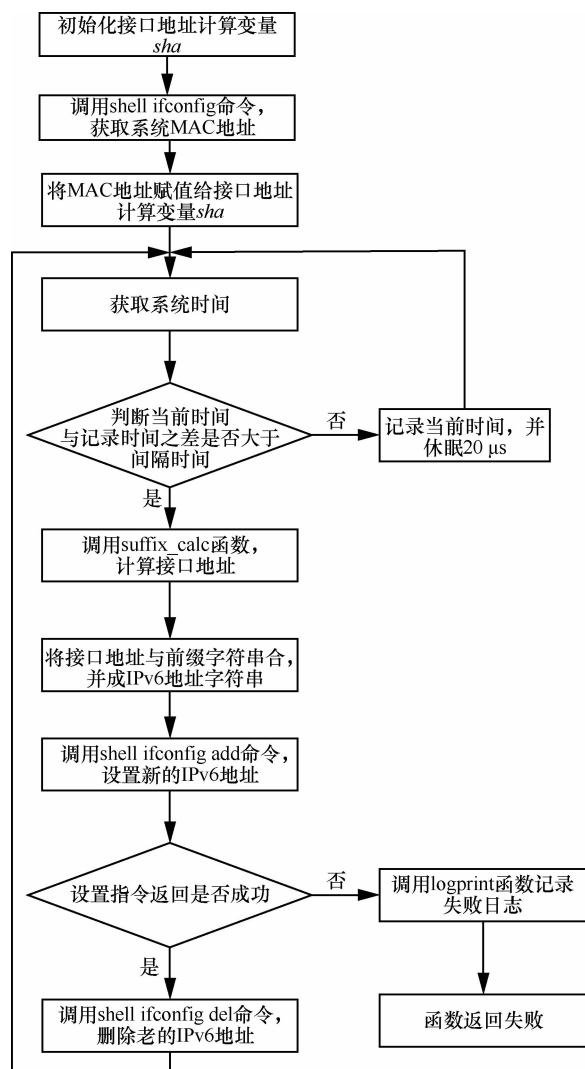


图 7 地址变换流程

由于基于地址跳变的防护技术, 最易干扰正常通信的情况就是出现大量分组丢失。因此需要进行相应的测试验证, 以证明地址跳变能够保证通信双方在通信过程中的分

组丢失情况在可接受的范围,对正常通信的干扰可以忽略。

实验采用虚拟机加载跳变程序原型进行,为了验证在不同情况下原型系统运行的效果,选择地址跳变时间间隔分别为不进行地址跳变(静态)、10 s 跳变周期、60 s 跳变周期和 300 s 跳变周期 4 种情况进行。获得的相关测试数据见表 2。

表 2 地址跳变机制试验结果

地址变换周期	静态	10 s	60 s	300 s
发送分组数/个	100 000	101 200	102 800	1 023 900
	100 000	101 200	102 400	1 019 700
	100 000	106 000	104 800	1 034 100
收到分组数/个	99 615	81 817	99 831	1 015 853
	99 716	80 441	99 646	1 013 329
	99 763	84 516	102 023	1 026 126
分组丢失率	0.39%	19.15%	2.89%	0.79%
	0.28%	20.51%	2.69%	0.62%
	0.24%	20.27%	2.65%	0.77%
均值	0.30%	19.98%	2.74%	0.73%

以上结果说明地址变换带来了更多的分组丢失,而分析其原因,主要有以下两个。

- C/S 架构的两台虚拟机时间不同步。虽然原则上都与宿主机时间实时同步,但同步精度不高。地址变换牵涉系统级的进程调用,难免会产生几十毫秒级甚至几百毫秒的时间不同步现象。
- 主要是实验过程中的操作问题,启动服务器端的地址变换进程和启动客户端的时间不一致导致的地址变换不同步现象,这种现象在极短时间内即变换一次的情况下会被明显放大。若牵涉实际应用,则可能是几百秒才变换一次地址,而且可以有较为成熟的时间同步机制,那么该操作问题的影响可以基本忽略不计。

结合以上原因分析测试结果,操作影响是 1~2 s,可能增加的分组丢失时间为 $1/\text{周期} \times 100\% \sim 2/\text{周期} \times 100\%$ 。可以认为虽然地址变换会带来一定的分组丢失,但总体影响并不致命且根据测试结果来看,随着地址变换周期的增长而明显减小,在变换周期为 300 s 时已经接近静态地址场景下的测试结果。因此基本可以认为该方法导致的分组丢失在可接受范围。

4 结束语

综上所述,在家庭网关向双栈演进过程中,将会面临新的安全风险。这些安全风险可能导致家庭网关的 IPv6 业务通道、原有的地址池溯源机制、管理口的 IPv6 地址面临被攻击或者功能缺失的风险。本文提出的 3 种安全改进防护措施能够针对性地起到加固家庭网关在这些方面的安全防护措施。但是由于目前 IPv6 正处于商用的初级阶段,本文所提及的安全防护技术还需要根据部署场景的不同进行优化,结合传统的一些安全防护技术,例如 VLAN、ACL、防火墙等,才能起到更好的安全防护效果。

参考文献

1 Stevens W R, Fenner B, Rudoff A M. UNIX Network Programming. 北京:人民邮电出版社,2009

2 Li Q, Jinmei T, Shima K. IPv6 Advanced Protocols Implementation. 北京:人民邮电出版社,2009

3 Li Q, Jinmei T, Shima K. IPv6 Core Protocols Implementation. 北京:人民邮电出版社,2009

4 Hogg S, Vyncke E. IPv6 Security. 北京:人民邮电出版社,2011

5 Deering S, Hinden R. Internet Protocol, Version 6. IETF RFC2460, 1998

6 Narten T, Nordmark E, Simpson W, et al. Neighbor Discovery for IP Version 6. IETF RFC4861, 2007

7 Rigney C, Willens S, Rubens A, et al. Remote Authentication Dial in User Service. IETF RFC2865, 2000

8 Arkko J, Kempf J, Zill B, et al. Secure Neighbor Discovery. IETF RFC3971, 2005

9 Davies E, Krishnan S, Savola P. IPv6 Transition/Coexistence Security Considerations. IETF RFC4942, 2007

10 Hinden R, Deering S. IP Version 6 Addressing Architecture. IETF RFC4291, 2006

11 Aura T. Cryptographically Generated Addresses. IETF RFC3972, 2005

[作者简介]



陈仲华,男,中国电信股份有限公司上海研究院高级研发工程师,多年从事 IP 网络技术研究和开发工作,主要研究方向为 IPv6、物联网、SDN/NFV、IP 安全等。

(收稿日期:2014-06-16)