

doi:10.14132/j.cnki.1673-5439.2020.06.004

IPv6 多出口解决方案应用研究

崔北亮

(南京工业大学 信息中心, 江苏 南京 210009)

摘要: 由于 IPv6 地址的多样性、IPv6 源地址选择的复杂性和 IPv6 的 NAT 不推荐性,如何合理分配和使用多条 IPv6 线路,达到负载均衡和冗余的效果,是一个突出的现实问题。众多有多运营商接入或多链路接入的单位,因没有好的 IPv6 多出口解决方案,而只开通了单一的 IPv6 链路。随着 IPv6 的规模部署,单一 IPv6 链路将严重制约网络的发展。文中首先阐述 IPv6 多出口的必要性,然后剖析 IPv6 多出口的复杂性,接着给出三种 IPv6 多出口的解决方案,最后对三种解决方案的特点进行比较和总结分析,用户可根据不同需求,选择某种方案实施。

关键词: IPv6 多出口; IPv6 地址; NAT66; IPv6 前缀转换

中图分类号: TN915 **文献标志码:** A **文章编号:** 1673-5439(2020)06-0020-08

Research on IPv6 multi-export solution

CUI Beiliang

(Network Information Center, Nanjing Tech University, Nanjing 210009, China)

Abstract: How to reasonably allocate and use multiple IPv6 lines to achieve the effect of load balancing and redundancy has become a prominent practical problem due to the diversity of IPv6 addresses, the complexity of IPv6 source address selection and the non recommendation of IPv6 NAT. Numerous enterprises and institutions with multi-operator or multi-link access only open a single IPv6 link for the lack of an effective IPv6 multi-export solution. With the scale deployment of IPv6, a single IPv6 link will seriously restrict the development of the internet. Firstly, the necessity of IPv6 multi-exports is expounds. Secondly, the complexity of IPv6 multi-exports is analyzed. Then, three solutions to IPv6 multi-exports are provided. Finally, the characteristics of the three solutions are compared and summarized. Therefore, users can choose different solutions to meet their varied needs.

Keywords: IPv6 multiple exits; IPv6 address; NAT66; IPv6 prefix conversion

从中共中央办公厅、国务院办公厅印发《推进互联网协议第六版(IPv6)规模部署行动计划》以来,IPv6网络得到大面积部署,IPv6网络商用化也逐步普及。随着IPv6网络商用化和大规模部署,国内几大运营商(中国电信、中国移动、中国教育科研网等)都开通了IPv6支持,一个单位接入多家运营商或多链路就可能会有多个IPv6出口。产生接入

多运营商或多链路的主要原因有:

(1) 受制于一些特殊需求,比如国内的高校一般都有 edu.cn 的域名,要拥有这样的域名,必须要接入中国教育科研网(以下简称教育网)。

(2) 对于单位接入多家运营商网络主要是因多运营商的现状,比如某个公司的网站要服务全国的用户,由于用户分散在多家运营商的网络中,为了更

好的用户体验,该公司可能会申请接入多家运营商,给服务器分配多个运营商的 IPv4/IPv6 地址,根据来访用户的 IPv4/IPv6 地址,由 DNS 服务器返回对应运营商的 IPv4/IPv6 地址。此外,考虑到网络的稳定,有些单位也会接入多运营商,避免单一运营商网络故障造成网络中断。

(3) 部分单位也会通过多条链路接入同一家运营商,比如某家运营商只提供千兆的接入,而用户却需要多条千兆接入。也有可能出于资费考虑,用户觉得千兆接入太贵,而采用几条百兆链路的叠加。

综上所述,国内多运营商链路接入的情况普遍存在。现阶段一般单位只开通了单一链路的 IPv6,随着 IPv6 的普及,单 IPv6 链路承载的流量将越来越大,单 IPv6 链路也缺乏冗余,开通多 IPv6 出口势在必行。

1 IPv4 多出口与 IPv6 多出口比较

通过 IPv6 接入多家运营商后,配置哪家运营商的 IPv6 地址、依据什么负载分担、某条链路故障后如何冗余,加之 IPv6 地址的多样性和 IPv6 源地址选择的复杂性等,这些问题综合在一起,使 IPv6 多出口变得异常复杂。

1.1 IPv4 出口选择的简单性

IPv4 中很少遇到源地址选择的原因是上网设备一般只会会有一个 IPv4 地址,这个地址可能是公网地址,更可能是私网地址。IPv4 环境中有下列几种场景:

场景一:单出口环境,且公网地址充足。此时直接给设备配置公网地址;

场景二:单出口环境,但公网地址不足。此时给上网设备配置私网地址,上网设备与外界通信时,由边界防火墙或路由器等设备做 NAT,将内部私网源地址转换成公网地址;

场景三:多出口环境,公网地址足够。这在国内不多见,主要以一些大公司,比如百度、腾讯、阿里等,它们申请了独立的 AS 号,有足够的公网 IPv4 地址,然后与各家运营商以 BGP 协议进行互联;

场景四:多出口环境,公网地址有限。这种情况在国内也很常见,内部上网设备配置私网 IPv4 地址,由边界防火墙或路由器根据各种策略的路由去选路,然后做 NAT,使用任何出口都能正常通信。

从以上分析可以看出,IPv4 中普遍公网地址不足,主要依赖 NAT。

1.2 IPv6 地址的多样性

IPv6 地址与 IPv4 地址除格式不同外,IPv6 地址的多样性也远超 IPv4。IPv4 地址可以通过手工静态配置和 DHCP 分配来进行,二者只能选其一。IPv6 的地址可以是手工静态配置、无状态地址自动配置^[1] (Stateless Address AutoConfiguration, SLAAC)。可能还存在公用地址、临时地址和 DHCP,同时还存在链路本地地址,这些类型的 IPv6 地址可以在一台 IPv6 设备上同时存在。因此,一台 IPv6 设备最多会同时存在 5 种类型的 IPv6 地址,由于临时 IPv6 地址还存在生命周期的问题,同一台 IPv6 设备可能会同时存在多个临时 IPv6 地址。这还只是在单一 IPv6 前缀的情况下,如果网关设备分配了多个 IPv6 前缀(比如分配多个运营商的 IPv6 前缀),同一台 IPv6 设备可能存在多达 10 个以上的 IPv6 地址^[2]。

1.3 IPv6 源地址选择的复杂性

当有多个地址的主机需要与外界主动通信时,就需要对源地址或目的地址进行选择。RFC6724 中源地址选择的规则有 8 条^[3],这些规则也是按顺序排列,当前面的规则选不出源地址时,执行下一条规则。其中规则 7 是使用临时地址,主要是考虑到私密性;规则 8 是使用最长前缀匹配的源地址,可以将源地址和目的地址都转成二进制数,从首位开始,依次比较两个地址对应位置二进制数是否相同,相同的话,则匹配的长度值就加 1,再比较下一位,直至二进制数不同为止,此时就能得出匹配的长度值,源地址与目的地址匹配的长度值越大,源地址越优先。

当这 8 条规则都无法选择出源地址时,源地址选择就存在很大的不确定性。比如网关设备通告了 2 个 IPv6 前缀,IPv6 设备上生成了 2 个前缀的 IPv6 临时地址,RFC6724 执行到规则 8,如果 2 个临时 IPv6 地址与目的 IPv6 地址前缀匹配的长度相同,此时就选不出源 IPv6 地址,RFC6724 只提了一下这需要由具体情况来决定,这就存在很大的不确定性。

1.4 IPv6 多出口的复杂性

IPv6 地址数量足够多,因此,IPv6 单出口类似于 IPv4 环境中的场景一,此时没必要使用 NAT^[4]。

IPv6 多出口类似于 IPv4 环境中的场景三,可以去申请独立的 AS 号和独立的 IPv6 地址段,然后与多家运营商 BGP 互联,这虽然是最理想的方案,但真正实施起来却很困难。首先,全球可用的 AS 号

数量有限,申请难度很大;其次,出于安全和稳定考虑,运营商与用户 BGP 互联的意愿并不强烈;最后,BGP 互联对网络设备的性能和网络管理人员的技术要求都非常高,一般单位很难满足,通过 BGP 互联的可能性不大。

如果 IPv6 多出口借鉴 IPv4 环境中的场景四,即内网配置私有的 IPv6 地址,在出口设备上进行 NAT66 转换,转换成运营商出口对应的 IPv6 地址,本文认为该方案有一定的可行性,只是 NAT 会导致网络性能下降、影响端到端的可达性、存在安全上隐患,该技术并不被推崇。

IPv6 多出口环境下,源 IPv6 地址的选择由 IPv6 终端设备完成,当数据包到达 IPv6 多出口设备时(防火墙或路由器),出口设备根据数据包特征(比如:源 IPv6、目的 IPv6、数据包大小等)选择相应的出口。源 IPv6 地址和出口确定后,还要判断这样的组合是否需要进一步处理,比如教育网的源 IPv6 地址选择了中国电信(以下简称电信)的出口,这样的源 IPv6 地址将会被判定为不合法,出口设备需要对这样的源 IPv6 地址进行 NAT66 转换。

对于 IPv4 多出口场景,由于 IPv4 公网地址普遍不足,不论选择哪个运营商出口,私有的 IPv4 地址都会转换成该运营商出口对应的公网 IPv4 地址,配置起来比较简单。鉴于 IPv6 地址的多样性、IPv6 源和目的地址选择的复杂性、IPv6 多地址下寻址和路由的不确定性^[5]、链路故障的冗余性等因素,IPv6 多出口配置起来,将更加复杂。

2 IPv6 多出口的方案

由于很多网管人员对 IPv6 多出口的复杂性认知不足,以至于现阶段很少有单位使用 IPv6 多出口。本文假设某单位通过教育网和电信网接入了 IPv6,然后给出三种 IPv6 多出口的解决方案。

2.1 仅配置某个运营商的 IPv6 地址

终端设备仅分配了某个运营商(比如教育网)的 IPv6 地址,终端设备使用教育网分配的 IPv6 地址访问互联网。互联网也可以通过教育网分配的 IPv6 地址从教育网链路访问到该终端,实现了端到端的可达性。但这会导致电信线路的完全浪费,尤其是在教育网链路故障时,内部终端不能通过电信链路访问互联网。

解决的办法可以是在终端仅配置教育网的 IPv6 地址,在出口防火墙上根据目的地址路由,比如配置目的是教育网地址的选择教育网,除此之外

的配置默认路由,选择电信出口。目前,教育网的 IPv6 地址块有 33 条,电信网的 IPv6 地址块有 39 条^[6],条目都不多,配置静态路由比较方便。因终端设备配置的是教育网的 IPv6 地址,选择电信网出口时,需进行 NAT66 地址转换,转换成电信网分配的 IPv6 地址,如果可以简单地做一个前缀替换(比如电信网分配了 2401:da8:0::/48 的 IPv6 地址,教育网分配了 2001:da8:0::/48 的 IPv6 地址,数据包从电信线路发出时,把源 IPv6 地址前缀 2001:da8:0::/48 替换成 2401:da8:0::/48,IPv6 地址的其余 80 位保持不变。数据包从电信线路进入时,把目的 IPv6 地址前缀 2401:da8:0::/48 替换成 2001:da8:0::/48),即实现 IPv6 地址的一对一转换,这样从互联网访问电信网的 IPv6 地址流量到达防火墙后,转换成教育网的 IPv6 地址,也实现了端到端的可达性。NAT66 前缀的转换,多数防火墙并不支持,这样就不能自动实现电信网 IPv6 地址到教育网 IPv6 地址的自动转换,但访问互联网没有问题,如果要实现端到端的可达,需要配置静态的 NAT66 条目,这只限于少量的静态条目,无法应对大面积的使用^[7]。在本人的建议下,“山石网科”已着手防火墙对 NAT66 前缀转换支持的开发,2021 年前可以面市。

对于异常处理,若某条链路故障,假如教育网链路故障,在防火墙上再配置教育网链路监控,使静态路由失效,把所有的流量都切换到电信出口;假如电信网链路故障,在防火墙上再配置电信网链路监控,使默认路由失效,配置管理距离大的默认路由,指向教育网出口,把所有流量都切换到教育网出口,当电信链路恢复时,管理距离小的默认路由重新生效,管理距离大的默认路由失效,默认流量重新切换回电信网出口。3.1 节将对此方案进行验证。

2.2 分别配置每个运营商的 IPv6 地址(NAT66 容灾)

这里仍以有教育网和电信网两个 IPv6 出口为例,终端设备分别分配教育网和电信网的 IPv6 地址。终端设备访问互联网,目的 IPv6 确定后,将根据 RFC6724 选择源 IPv6 地址,默认将采用最长匹配,由于每家运营商 IPv6 地址块比较接近,终端设备最终实现用电信网分配的 IPv6 地址访问电信网资源,用教育网分配的 IPv6 地址访问教育网资源,对于既不是教育网,也不是电信网的目的 IPv6 地址,仍然采用最长匹配的原则,有可能选择电信网分配的 IPv6 地址,也有可能选择教育网分配的 IPv6 地址。源和目的 IPv6 地址确定后,还要考虑防火墙

上的路由配置,如果防火墙配置了 2.1 节的路由条目,默认路由选择的是电信出口,这里存在一个问题,比如互联网上非教育网和非电信网的源 IPv6 访问内网终端教育网分配的 IPv6 地址,数据包从内网返回时,根据默认路由,防火墙选择了电信出口,教育网分配的源 IPv6 地址从电信网出口发出时,会被电信网认为是非法来源的 IPv6 流量,很可能被丢弃。同样,如果内网终端主动访问互联网上非教育网和非电信网的资源时,根据最长匹配,假如选择了教育网的 IPv6 地址,由于出口选择的是电信出口,电信网同样会认为这是非法来源的 IPv6 流量。

解决的办法可以是删除配置的静态和默认路由,在出口防火墙上配置源路由,即根据源 IPv6 地址选择路由,教育网的源 IPv6 地址选择教育网的出口,电信网的源 IPv6 地址选择电信网的出口。这样双链路都得到了利用,链路的使用情况取决于要访问目的的 IPv6 地址与源 IPv6 地址的最长匹配情况。

对于异常的处理方法,为防火墙的两条源路由分别配置链路监控,监控对应的教育网和电信网,当链路故障时,源路由失效。同时在防火墙上再配置两条默认路由分别指向教育网和电信网出口,默认路由也设置与教育网和电信网的链路监控有关,若链路故障,对应的默认路由也失效。假如教育网故障,教育网的源路由和默认路由都失效,教育网分配

的源 IPv6 地址将选择电信出口,在防火墙上再配置 NAT66,对教育网分配的源 IPv6 地址进行转换,转换成电信网的 IPv6 地址。同样,为了避免电信网链路故障,也要对电信网分配的源 IPv6 地址配置 NAT66,转换成教育网的 IPv6 地址。3.2 节将对此方案进行验证。

2.3 分别配置每个运营商的 IPv6 地址(完全无 NAT66)

该方案和 2.2 类似,但是在异常处理的方法上不同。此时,需要让终端的网关设备(一般是三层交换机或路由器)探测每条运营商链路,当运营商链路故障时,网关设备通知 IPv6 终端设备,分配的该运营商 IPv6 前缀的首选寿命和有效寿命的时间都是 0,IPv6 终端弃用该运营商的 IPv6 地址。这种方法不论在网络正常或异常的情况下,都没有使用 NAT66,该方案可提升网络性能、解决端到端的可达性和安全性,值得推荐。3.3 节将对此方案进行验证。

3 IPv6 多出口方案验证

本节通过实验验证 IPv6 多出口的三种解决方案。图 1 中,某单位通过防火墙接入教育网和电信网,教育网给该单位分配了 2001:da8:0::/48 的 IPv6 前缀,电信网给该单位分配了 2401:da8:0::/48 的 IPv6 前缀。

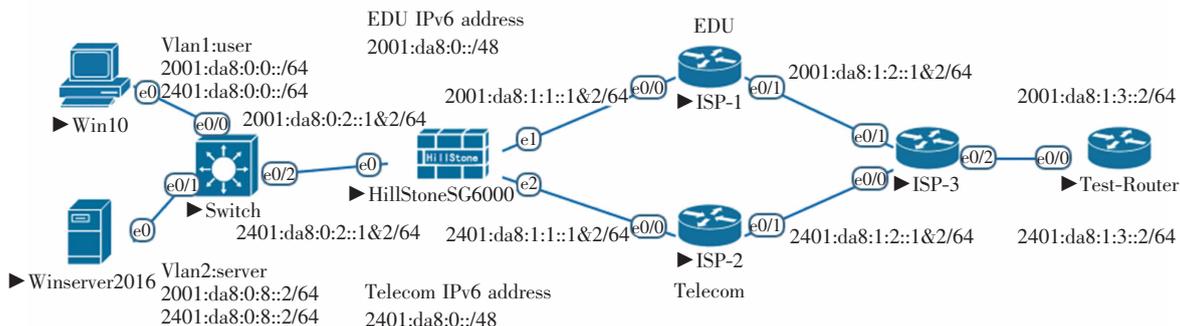


图 1 IPv6 多出口拓扑

该实验环境基于 EVE-NG^[8],本文准备了完整的实验平台,可从笔者的个人主页处下载: <http://blcui.njtech.edu.cn/eve-ng-v2.rar>,完整实验配置脚本也可从笔者的个人主页处下载: <http://blcui.njtech.edu.cn/IPv6-multi-out.rar>。为了便于读者测试,笔者搭建好了一个网上在线实验平台,访问的网址是 <http://210.28.203.12>,登录的用户名是 admin,密码是 eve@135,登录时请选择“Html5 console”。

3.1 IPv6 多出口解决方案一(配单运营商 IPv6 地址 + NAT66)

该方案配置的关键部分和测试如下:

(1) 设备配置。配置图中的内网核心交换机 Switch、出口防火墙 HillstoneSG6000、教育网运营商路由器 ISP-1、电信网运营商路由器 ISP-2、互联网路由器 ISP-3 和测试路由器 Test-Router。其中: Switch、ISP-1、ISP-2、ISP-3 和 Test-Router 涉及的是常规的接口 IPv6 地址和路由配置,这里不再列出,具

体请参考 IPv6-multi-out.rar 文件, 防火墙 HillstoneSG6000 的接口 IPv6 地址配置和策略配置, 这里也不再列出, 同样请参考 IPv6-multi-out.rar 文件. HillstoneSG6000 的关键配置如下(其中斜体部分为注释):

```
SG-6000(config)# ip vrouter "trust-vr"
```

```
SG-6000(config-vrouter)# snatrule id 1 from "2001:da8::/48" to
"::0" service "Any" eif ethernet0/2 trans-to 2401:da8:0:1::/120
mode dynamicport
```

这时配置的是源 IPv6 的 NAT66, 把符合 2001:da8::/48 前缀且外出接口是 ethernet0/2, 去往任何目的地址任何服务的源 IPv6 地址转换成 2401:da8:0:1::/120 前缀的 IPv6 地址。若防火墙可以把 2001:da8::/48 前缀一一对应地转换成 2401:da8::/48 前缀, 防火墙就可以是无状态的防火墙了, 且从互联网可以通过电信网的 IPv6 地址端到端的访问到内网的 IPv6 上网设备。遗憾的是山石防火墙暂不支持 IPv6 前缀直接转换的功能, 且 NAT66 中目的 IPv6 地址条目受限, 所以这里使用了电信网 IPv6 地址段中的部分地址 2401:da8:0:1::/120, 由于使用的是基于端口的转换, 这里提供的 2⁸ 个 IPv6 地址足够了。

```
SG-6000(config-vrouter)# ipv6 route 2001:da8:0::/48 2001:da8:0:2::1
```

去往内网教育网地址的路由

```
SG-6000(config-vrouter)# ipv6 route 2401:da8:0::/48 2001:da8:0:2::1
```

去往内网电信网地址的路由

```
SG-6000(config-vrouter)# ipv6 route 2000::/8 2001:da8:1:1::2
```

去往外网教育网地址段的路由

```
SG-6000(config-vrouter)# ipv6 route ::/0 2401:da8:1:1::2
```

去往外网的默认路由

```
SG-6000(config-vrouter)# ipv6 route source 2001:da8:0:8::/64 2001:da8:1:1::2
```

这里配置的是源路由, 也称基于源地址的路由, 源路由优先于正常的路由。2001:da8:0:8::/64 是内网中使用教育网地址对外提供服务的地址段, 所以出口只能是教育网出口

```
SG-6000(config-vrouter)# ipv6 route source 2401:da8:0:8::/64 2401:da8:1:1::2
```

(2) 测试。在 Win10 计算机上追踪去往教育网和电信网流量的路由, 显示如图 2 所示。

```

C:\Users\Administrator>tracert -d 2001:da8:1:3::2
通过最多 30 个跃点跟踪到 2001:da8:1:3::2 的路由

 1  1 ms  1 ms  1 ms  2001:da8::1
 2  2 ms  1 ms  1 ms  2001:da8:0:2::2
 3  12 ms 2 ms  2 ms  2001:da8:1:1:2
 4  40 ms 3 ms  3 ms  2001:da8:1:1:2
 5  40 ms 4 ms  3 ms  2001:da8:1:3:2

跟踪完成。

C:\Users\Administrator>tracert -d 2401:da8:1:3::2
通过最多 30 个跃点跟踪到 2401:da8:1:3::2 的路由

 1  1 ms  <1 毫秒  1 ms  2001:da8::1
 2  3 ms  2 ms  2 ms  2001:da8:0:2::2
 3  3 ms  3 ms  3 ms  2401:da8:1:1:2
 4  4 ms  3 ms  4 ms  2401:da8:1:1:2
 5  22 ms 4 ms  4 ms  2401:da8:1:3:2

跟踪完成。
C:\Users\Administrator>

```

图 2 Tracert 路由

从图 2 中, 可以看到 Win10 去往教育网 2001:da8:1:3::2 的数据包, 第一跳是网关, 第二跳是防火墙内网接口, 第三跳是 ISP-1 的 e0/0 接口, 第四跳是 ISP-3 的 e0/1 接口, 第五跳到达测试路由器。

继续追踪 Win10 去往电信网 2401:da8:1:3::2 的数据包, 第一跳是网关, 第二跳是防火墙内网接口, 第三跳是 ISP-2 的 e0/0 接口, 第四跳是 ISP-3 的 e0/0 接口, 第五跳到达测试路由器。从输出中可以看到, 出口防火墙根据目的地址做了分流, 两条运营商链路都用了起来。

在 Win10 上打开一个 DOS 命令行窗口 telnet 连接 2001:da8:1:3::2, 再另外打开一个 DOS 命令行窗口, telnet 连接 2401:da8:1:3::2, 然后在该窗口中使用 show users 查看登录的用户, 显示如图 3 所示。

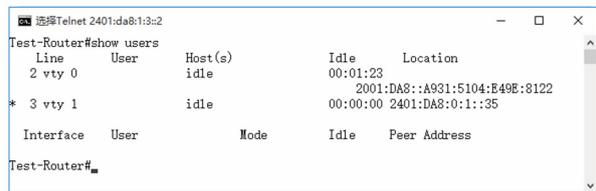


图 3 查看 telnet 用户

从图 3 中, 可以看到当前登录的是 2401:da8:1:3::2 地址, 源地址是 2401:da8:0:1:35, 这个源 IPv6 地址不是 Win10 计算机上的 IPv6 地址, 是被防火墙转换后的电信网分配的一个 IPv6 地址。从图中也可以看到另一个用户 2001:da8::A931:5104:E49E:8122, 可以验证这个用户就是 Win10 计算机上的教育网 IPv6 地址。此时, Win10 计算机从两家运营商都可以访问互联网, 但只支持从教育网访问该 Win10 设备, 除非电信网配置静态的 NAT。

按图 1 所示给 Winserver2016 服务器手工配置两个 IPv6 地址, 使用 Win10 同样的测试方法测试, 可以验证 Winserver2016 分别使用教育网和电信网分配的 IPv6 地址访问对应的教育网和电信网互联网资源, 也可以分别从教育网和电信网访问到服务器。

(3) 异常处理。前面测试了教育网和电信网出口都正常情况下的网络访问, 接下来分别讨论教育网和电信网出口故障的解决办法。

① 教育网故障: 关闭 ISP-1 路由器的 e0/0 接口, 模拟教育网故障。经测试可以发现, Win10 和 Winserver2016 都不能访问互联网的教育网资源, 但访问其他网资源正常。这里配置防火墙的链路检测, 从防火墙 e0/1 接口探测互联的教育网对端 IPv6 地址, 若地址不可达, 则认为链路故障, 使防火墙 e0/1 接口的协议失效。防火墙 e0/1 接口失效后, 基于该接口的目的路由 2000::/8 和源路由 2001:

da8:0:8::/64 都会失效。Win10 访问互联网都会使用默认路由,都会被转换成电信网的 IPv6 地址。Winserv2016 服务器访问互联时,如果源 IPv6 地址是教育网的地址,将会被转换成电信网的 IPv6 地址;如果源 IPv6 地址是电信网的 IPv6 地址,将保持不变。防火墙的对应配置如下:

```
SG-6000(config)# track "edu" 创建监测对象edu
SG-6000(config-trackip)# icmp6 2001:da8:1:1::2 interface ethernet0/1 src-interface ethernet0/1 使用防火墙ethernet0/1 接口的IPv6 地址,从ethernet0/1 接口ping 教育网的互联IPv6 地址2001:da8:1:1:2
```

```
SG-6000(config-trackip)# exit
```

```
SG-6000(config)# interface ethernet0/1
```

```
SG-6000(config-if-eth0/1)# monitor track "edu" 配置对象监控,若edu 失败,该接口协议失效
```

经过上述配置后,教育网出口故障时,Win10 和 Winserv2016 仍可以正常访问教育网和电信网资源。

② 电信网故障:开启 ISP-1 路由器的 e0/0 接口,关闭 ISP-2 路由器的 e0/0 接口,模拟电信网故障。经测试可以发现,Win10 和 Winserv2016 都不能访问电信网的资源,但访问教育网的资源正常。这里配置防火墙的链路检测,从防火墙 e0/2 接口探测互联的电信网对端 IPv6 地址,若地址不可达,则认为链路故障,使防火墙 e0/2 接口的协议失效。防火墙 e0/2 接口失效后,基于该接口的目的路由::/0 和源路由 2401:da8:0:8::/64 都会失效。Win10 访问教育网有具体的路由,访问其他资源没有路由,在防火墙上添加一条默认路由,下一跳指向教育网出口,但管理距离设为 2,之前配置的电信出口的默认路由的管理距离是 1,之前配置的默认路由失效,次优的默认路由生效,这样 Win10 访问任何互联网资源都会使用真实的教育网 IPv6 地址。

在电信网出口故障时,电信网用户访问 Winserv2016 服务器的教育网 IPv6 地址时,Winserv2016 会根据会话,使用教育网 IPv6 地址作为源 IPv6 地址进行回应,而不会采用最长匹配,这是因为应用程序指定的 IPv6 地址优先于网络层的选择^[4]。

防火墙的对应配置如下:

```
SG-6000(config)# track "telcom" 创建监测对象telcom
```

```
SG-6000(config-trackip)# icmp6 2401:da8:1:1::2 interface ethernet0/2 src-interface ethernet0/2 使用防火墙ethernet0/2 接口的IPv6 地址,从ethernet0/2 接口ping 电信网的互联IPv6 地址2401:da8:1:1:2
```

```
SG-6000(config-trackip)# exit
```

```
SG-6000(config)# interface ethernet0/2
```

```
SG-6000(config-if-eth0/2)# monitor track "telcom" 配置对象监控,若telcom 失败,该接口协议失效
```

```
SG-6000(config-if-eth0/2)# exit
```

```
SG-6000(config)# ip vrouter "trust-vr"
```

```
SG-6000(config-vrouter)# ipv6 route ::/0 2001:da8:1:1::2 2 添加一条管理距离是2 的默认路由,电信出口正常时,使用不到该路由,电信出口故障时,该默认路由生效
```

```
SG-6000(config-vrouter)# snatrule id 2 from "2401:da8::/48" to "::/0" service "Any" eif ethernet0/1 trans-to 2001:da8:0:9999:1::/120 mode dynamicport 这条配置的作用是,当电信网出口故障,服务器访问电信网资源时,将被转换成教育网的IPv6 地址2001:da8:0:9999:1::/120 是随便配置的地址段,不与内网重叠即可
```

至此,本方案实现了当教育网和电信网都正常时,防火墙根据用户访问的目的地址负载分担(服务器除外,服务器根据源 IPv6 地址选择出口)。当某个运营商出口故障时,不管是服务器,还是客户机,仍能正常访问互联网的所有资源;互联网也能正常访问服务器。

3.2 IPv6 多出口解决方案二(配多运营商 IPv6 地址 + NAT66 容灾)

该方案的关键配置和测试步骤如下:

(1) 防火墙在方案一配置的基础上做如下修改:

```
SG-6000(config)# ip vrouter "trust-vr"
```

```
SG-6000(config-vrouter)#no ipv6 route 2000::/8 2001:da8:1:1::2 2 删除原来配置教育网路由
```

```
SG-6000(config-vrouter)#no ipv6 route ::/0 2001:da8:1:1::2 2 删除原来教育网的次优默认路由,原路由管理距离配置的是2
```

```
SG-6000(config-vrouter)#ipv6 route ::/0 2001:da8:1:1::2 2 添加教育网的默认路由
```

```
SG-6000(config-vrouter)#no ipv6 route source 2001:da8:0:8::/64 2001:da8:1:1::2 删除为原服务器教育网段配置的源路由
```

```
SG-6000(config-vrouter)#no ipv6 route source 2401:da8:0:8::/64 2401:da8:1:1::2 删除为原服务器电信网段配置的源路由
```

```
SG-6000(config-vrouter) # ipv6 route source 2001:da8:0::/48 2001:da8:1:1::2 添加全范围的教育网源路由
```

```
SG-6000(config-vrouter) # ipv6 route source 2401:da8:0::/48 2401:da8:1:1::2 添加全范围的电信网源路由
```

(2) 正常测试。在 Win10 上 telnet 测试路由器 2001:da8:1:3::2,然后执行 show users,可以看到源 IPv6 地址选择的是 2001 开头的教育网地址;telnet 测试路由器 2401:da8:1:3::2,然后执行 show users,可以看到源 IPv6 地址选择的是 2401 开头的电信网地址。证明了在运营商出口都正常的情况下,终端设备无论选择哪个源 IPv6 地址,访问互联网都不需要 NAT66 转换。

(3) 异常测试。

① 教育网故障:关闭 ISP-1 路由器的 e0/0 接口,模拟教育网故障。使用上述的测试方法,可以验证在教育网出口故障的情况下,终端设备访问教育网资源需要 NAT66 转换,访问电信网资源不需要 NAT66。

② 电信网故障:开启 ISP-1 路由器的 e0/0 接口,关闭 ISP-2 路由器的 e0/0 接口,模拟电信网故障,可以验证在电信网出口故障的情况下,终端设备访问电信网资源需要 NAT66 转换,访问教育网资源不需要 NAT66。

3.3 IPv6 多出口解决方案三(配多运营商 IPv6 地址,完全无 NAT66)

本方案需要借助于网关设备的两个特性互联网协议服务等级协议^[9](Internet Protocol Service-Level Agreement, IP SLA)和嵌入式事件管理器^[10](Embedded Event Manager, EEM)。IP SLA 可用于网络连通性测试。EEM 可实现进程级的自动策略控制,该功能可以利用智能网络帮助 IT 管理人员自动执行费时的任务,从而节约管理人员的时间。由于图 1 中的 Switch 交换机版本较老,不支持 IP SLA,这里使用路由器替代交换机。该方案的关键配置和测试步骤如下:

(1) 配置 SLA 和 EEM。基本配置参照方案二,这里配置异常处理,当路由器探测到教育网出口故障,就把所有分配的教育网前缀的有效时间和首选时间设置成 0;探测到教育网出口恢复时,再取消所有分配的教育网前缀的有效时间和首选时间的 0 设置。电信网出口采用类似的配置。路由器上教育网出口“正常变异常”的脚本配置如下:

```
Router(config)#ip sla 1 配置探测条目1
```

Router(config-ip-sla)# icmp-echo 2001:da8:1:1::2 使用 ping 测试,测试教育网出口的互联 IPv6 地址

```
Router(config-ip-sla-echo)# frequency 5 探测的频率是5 秒一次
```

```
Router(config-ip-sla-echo)#exit
```

Router(config)#ip sla schedule 1 life forever start-time now 探测条目1 马上开始,一直有效

Router(config)#track 100 ip sla 1 reachability 配置 track 条目 100,追踪的对像是 IP SLA 1 的可达性

```
Router(config-track)#exit
```

Router(config)#event manager applet edu-down 继续创建事件管理器 edu-down,教育网链路故障

```
Router(config-applet)# event syslog pattern "% TRACK-6-STATE: 100 ip sla 1 reachability Up→Down" 日志事件追踪,当日志中出现 "% TRACK-6-STATE :100 ip sla 1 reachability Down →Up " 这样的信息,触发该事件,执行下面的代码
```

```
Router(config-applet)# action 10 cli command "en"
```

```
Router(config-applet)# action 20 cli command "conf t"
```

```
Router(config-applet)# action 30 cli command "int e0/0" 这里配置每一个内网接口,若是核心交换机,配置的就是每一个 VLAN
```

```
Router(config-applet)# action 40 cli command " ipv6 nd prefix 2001:da8:0:0::/64 0 0"
```

```
Router(config-applet)# action 70 cli command "end"
```

教育网出口“异常变正常”的脚本以及电信网出口的配置文件这里不再列出,可以参考下载的配置文件。

(2) 异常测试。

① 教育网故障:在 Win10 上长 ping 2001:da8:1:3::2,关闭 ISP-1 路由器的 e0/0 接口,模拟教育网故障,大约丢了 2 个 ping 包后,又恢复正常。此时注意到路由器的控制台上显示下面的日志信息:

```
* Feb 20 12:23:06.527:% TRACK-6-STATE:100 ip sla 1 reachability Up→Down
```

```
* Feb 20 12:23:07.032:% SYS-5-CONFIG_I: Configured from console by on vty0 (EEM:edu-down)
```

日志信息显示“% TRACK-6-STATE:100 ip sla 1 reachability Up→Down”,这就是前面配置追踪事件中的日志显示。后面的信息显示执行了 edu-down 事件管理程序。在路由上查看此时 e0/0 接口的配置,注意接口下多出一行“ipv6 nd prefix 2001:DA8::/64 0 0”。

在 Win10 上 telnet 测试路由器 2001:da8:1:3::2,然后执行 show users,可以看到源 IPv6 地址选择的是 Win10 上电信网分配的 2401 开头的临时 IPv6 地址,并没有使用 NAT66;telnet 测试路由器 2401:da8:1:3::2,然后执行 show users,可以看到源 IPv6 地址与前面显示的一样。这证明了在教育网出口故障的情况下,终端设备不论访问的是教育网,还是电信网,使用的都是电信网的 IPv6 地址。

在 Win10 使用 netsh interface ipv6 show address,可以看到 2001 开头的教育网临时 IPv6 地址和公用 IPv6 地址的首选寿命时间都是 0 s,状态是“反对”,教育网的 IPv6 地址失效,只有电信的 IPv6 地址可用。

② 电信网故障:开启 ISP-1 路由器的 e0/0 接口,关闭 ISP-2 路由器的 e0/0 接口,模拟电信网故障。Router 上显示如下:

```
* Feb 20 14:41:40.981:% TRACK-6-STATE:100 ip sla 1 reachability Down→Up
```

```
* Feb 20 14:41:41.842:% SYS-5-CONFIG_I: Configured from console by on vty0 (EEM:edu-up)
```

```
* Feb 20 14:42:16.019:% TRACK-6-STATE:200 ip sla 2 reachability Up→Down
```

```
* Feb 20 14:42:16.866:% SYS-5-CONFIG_I: Configured from
```

console by on vty0 (EEM:telcom-down)

从上面的输出中,日志显示“100 ip sla 1 reachability Down→Up”,也就是教育网链路恢复了,执行 edu-up 程序。然后显示“200 ip sla 2 reachability Up→Down”,也就是电信网链路故障,执行 telcom-down 程序。此时,查看路由器 e0/0 接口的配置,可以看到路由器 e0/0 接口通告电信网 IPv6 前缀 2401:da8:0::/64 时,有效时间和首选时间都设置成 0。在 Win10 使用 netsh interface ipv6 show address,可以看到 2401 开头的电信网 IPv6 地址失效,只有教育网的 IPv6 地址可用。

4 三种解决方案对比

这里对三种 IPv6 多出口的解决方案做个对比,IPv6 多出口方案比较如表 1 所示。

表 1 IPv6 多出口方案比较

参数	方案一	方案二	方案三
终端设备 IPv6 前缀数量	1	2	2
链路正常时是否使用 NAT66	是	否	否
链路异常时是否使用 NAT66	是	是	否
配置的工作量	小	小	大
对硬件设备的要求	低	低	高
链路负载调节的灵活性	高	低	低
笔者推荐度	中	高	低

用户可根据表中对比,选择适合的方案。在满足负载均衡和链路冗余的情况下:若要完全避免 NAT66,只能选择方案三,但方案三的配置工作量较大,要求终端网关设备支持 SLA 和 EEM;若要考虑配置简单,可以选择方案一,但方案一大量使用 NAT66,在防火墙不支持 IPv6 前缀转换的情况下,其中一条链路不满足端到端的可达性;方案二在链路异常的情况下,才会使用 NAT66,且配置的工作量也不大,对设备的要求也不高,只是在链路负载调节的灵活性上稍差些。综合考虑各个方面,笔者推荐使用方案二。

5 结束语

随着 IPv6 的普及,数以万计多链路或多运营商

接入互联网的企事业单位将开通多 IPv6 出口,本文介绍的三种实现方案将帮助网络管理人员加深对 IPv6 多出口的理解,对具体实施起着指导作用,加快我国 IPv6 部署进程。

参考文献:

- [1] THOMSON S, NARTEN T, JINMEI T. IPv6 stateless address autoconfiguration:RFC 4862[S]. 2007.
- [2] 崔北亮,罗国富,饶德胜. 非常网管 IPv6 网络部署实战[M]. 北京:人民邮电出版社,2019:51-99.
- [3] DRAVES R, MATSUMOTO A, CHOWN T. Default address selection for Internet protocol version 6 (IPv6):RFC 3484[S]. 2012.
- [4] WASSERMAN M, BAKER F. IPv6-to-IPv6 network prefix translation:RFC 6296[S]. 2011.
- [5] 张千里,姜彩萍,王继龙,等. IPv6 地址结构标准化研究综述[J]. 计算机学报,2019,42(6):1384-1405.
ZHANG Qianli, JIANG Caiping, WANG Jilong, et al. A survey on IPv6 address structure standardization researches[J]. Chinese Journal of Computers, 2019, 42(6):1384-1405. (in Chinese)
- [6] 苍狼山庄. 各运营商 IPv6 地址段[EB/OL]. [2020-07-20]. <https://ispip.clang.cn/>.
- [7] 辜苛峻,张连成,郭毅,等. 基于多类型数据包的 IPv6 防火墙防护能力评测方法[J]. 计算机应用研究,2019,36(7):2154-2158.
GU Kejun, ZHANG Liancheng, GUO Yi, et al. IPv6 firewall defensive capability testing method based on varied packets[J]. Application Research of Computers, 2019, 36(7):2154-2158. (in Chinese)
- [8] EVE-NG Ltd. EVE-NG 站点[EB/OL]. [2020-07-20]. <https://www.eve-ng.net/>.
- [9] 孙光懿,郭建忠. VRRP 和 SLA 协议在校园网中的应用[J]. 西华大学学报(自然科学版),2019,38(2):12-18.
SUN Guangyi, GUO Jianzhong. Application of VRRP and SLA protocols in campus network[J]. Journal of Xihua University (Natural Science Edition), 2019, 38(2):12-18. (in Chinese)
- [10] CARTHERN C, WILSON W, BEDWELL R, et al. Effective network management[M] // Cisco Networks. Berkeley: Apress, 2015:623-648.