互联网应用 IPv6 交换机 RA 抑制以及服务器网卡优化分享

（国联证券供稿 江苏局指导）

一、引言

IPv6 规模部署是加快网络强国和加强国家信息安全的重要事项，党中央、国务院高度重视 IPv6 的发展应用，2017 年 11 月中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》；2019 年中国人民银行、银保监会、证监会发布《关于金融行业贯彻<推进互联网协议第六版（IPv6）规模部署行动>的实施意见要求》。国联证券高度重视 IPv6 规模部署工作，公司信息技术治理委员会确定由信息技术总部负责牵头成立 IPv6 改造小组，公司首席信息官担任组长，多部门共同参与，制定了 IPv6 从测试到生产环境改造部署的详细方案和计划，保障 IPv6 改造按照文件要求顺利落地。

二、IPv6 改造技术路线说明

（一）NAT66 模式

NPTv6（IPv6-to-IPv6 Network Prefix Translation，IPv6-to-IPv6 网络前缀转换）是基于 IPv6 网络的地址转换技术，用于将 IPv6 报文中的 IPv6 地址前缀转换为另一个

IPv6 地址前缀，这种地址转换方式称为 NAT66。使用 NAT66 设备连接单个内部网络和公网，内部网络中的主机使用仅支持在本地范围内路由的 IPv6 地址前缀。当内部网络中的主机访问外部网络时，报文中的源 IPv6 地址前缀将被 NAT66 设备转换为全球单播 IPv6 地址前缀，NAT66 的好处是可以对外隐藏内部 IPv6 的真实地址。

（二）IPv4/IPv6 双栈模式

双栈技术是 IPv4 与 IPv6 共存技术，在终端设备和网络节点上同时安装 IPv4 和 IPv6 的协议栈，从而实现分别与 IPv4 或 IPv6 节点间的信息互通[1]。

国联证券首先从网络、交换机、防火墙、安全设备等通过 IPv4/IPv6 双栈模式改造，支持 IPv6 协议，并根据一行两会的改造指引要求，确保 IPv6 具有和 IPv4 同等的性能和安全防护能力。面向公众服务应用接入服务器优先考虑通过 IPv4/IPv6 双栈模式改造，进而支持 IPv6 协议，确保能够对访问应用的 IPv6 地址进行溯源。应用系统后台数据库服务器、业务中间件暂保留为 IPv4 协议，确保后台服务器的稳定性。

三、国联证券互联网应用 IPv6 网络改造经验分享

现阶段我国 IPv6 普及率仍比较低，IPv6 改造建设实际经验和具体范例还比较欠缺，而 IPv6 改造涉及的外部单位也比较多[2]。国联证券结合 IPv6 改造测试实施工作，不断积

累 IPv6 网络改造建设及运维的理论和经验。

国联证券的网络架构是主灾双中心双活模式，在前期 IPv6 改造中，发现灾备中心互联网应用进出 IPv6 流量出现在主中心设备上的问题。技术人员立即深入追查，初步定位问题后，模拟 IPv6 改造环境进行测试，成功复现该情况。接着通过不断的测试和抓包，成功解决该问题。现将在 IPv6 改造工作中关于 IPv6 交换机 RA 抑制和服务器网卡优化的经验总结如下:

（一）IPv6 交换机 RA 抑制基本概念

RA(Router Advertisement)就是路由器通告：路由器周期性地通告它的存在以及配置的链路和网络参数，或者对路由器请求消息做出响应。

SLAAC（Stateless Address AutoConfiguration）无状态自动配置：根据路由通告报文 RA（Router Advertisement）客户端收到 RA 包含的 prefix 前缀信息广播后，自动配置 IPv6 地址，组成方式是 Prefix + (EUI64 or 随机)。无状态自动配置不需要消耗很多硬件资源，也不像传统 DHCP 一样需要维护一个本地数据库来维护地址分配状态。

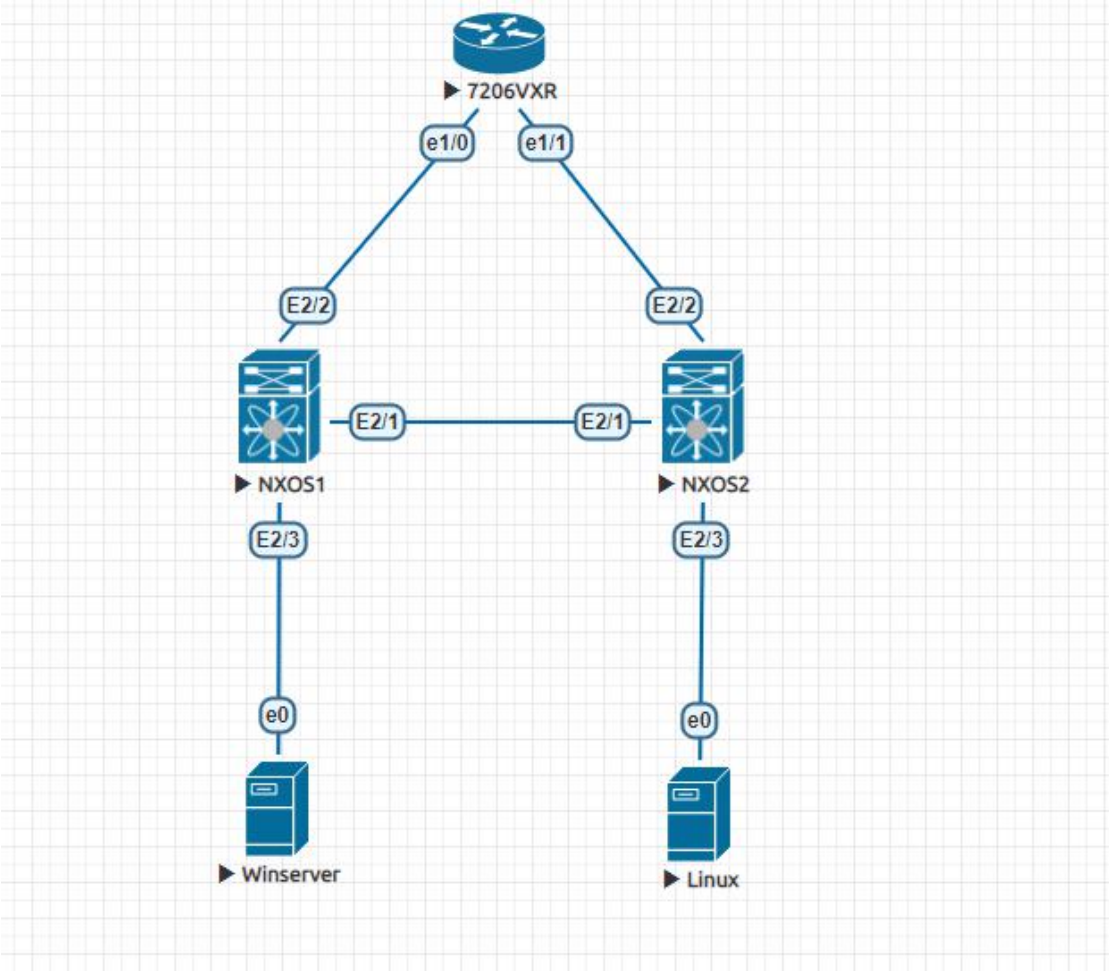
（二）模拟测试拓扑图

1、路由器模拟出口设备;

2、两台交换机模拟现有 IPv6 互联网应用区域汇聚交换

机；

3、一台 Windows server 和一台 Linux server。

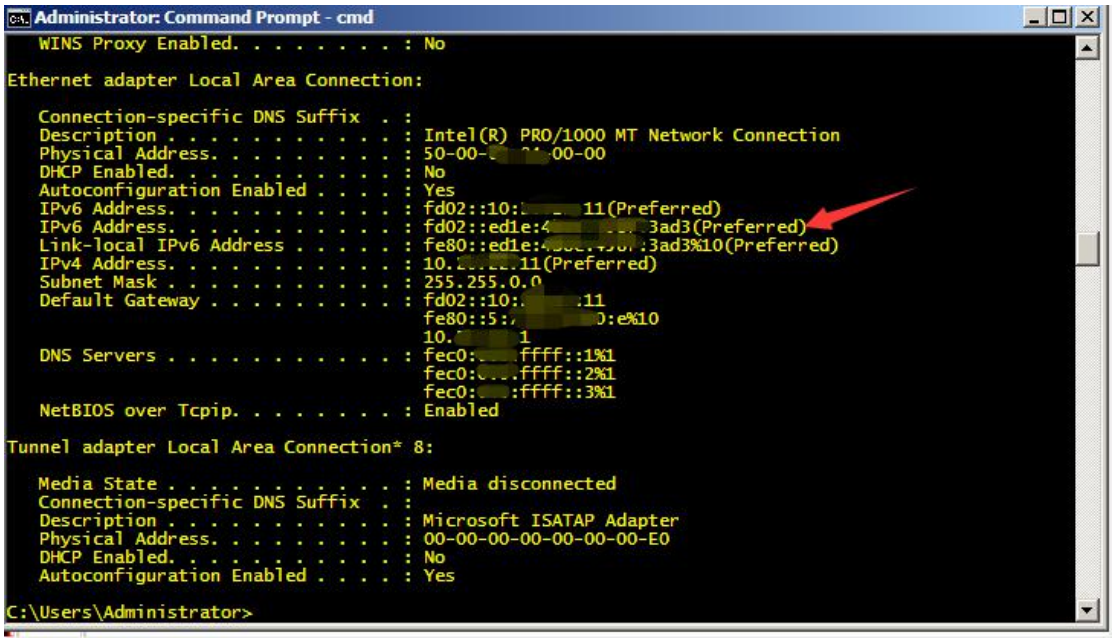


两台交换机完全模拟灾备中心互联网应用，IPv4 和 IPv6 网关全部在交换机上。

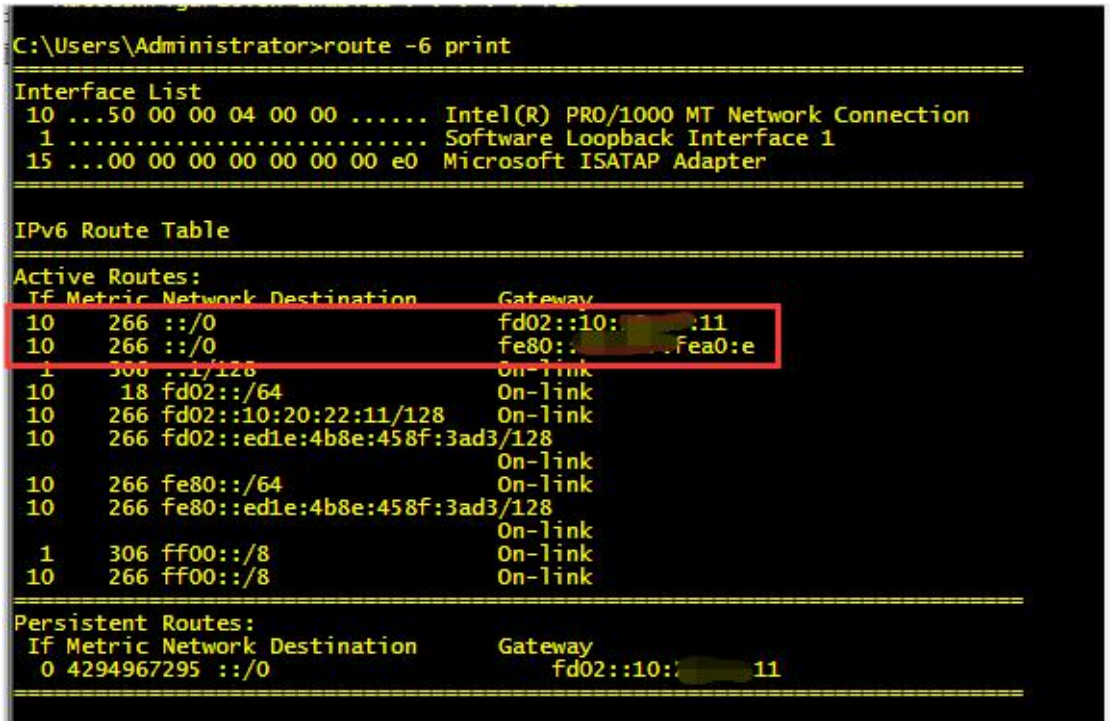
（三）问题出现

在 Windows Server 上，手工配置 IPv4 /IPv6 双栈地址以后，由于交换机使用默认配置，所以广播域内会定期发送 ICMPv6 信息，其中携带有 RA 和前缀消息。服务器网卡会根据 RA 消息，自动生成另外一个 IPv6 地址，主机对该单播地址进行 DAD，DAD 通过后该 IPv6 地址即启用，出

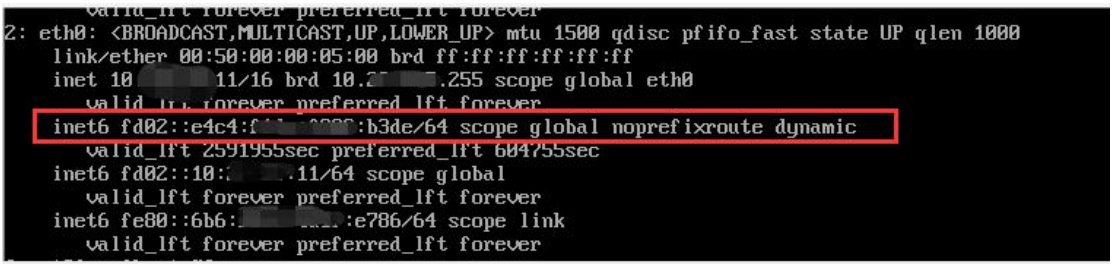
现了两个被指定 Preferred 的 IPv6 地址。



同时检查 IPv6 路由时，会存在两条默认路由，这样就会引起异常的网络问题。

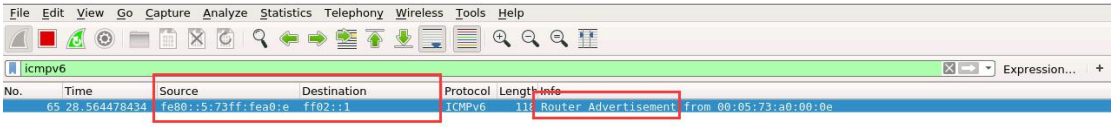


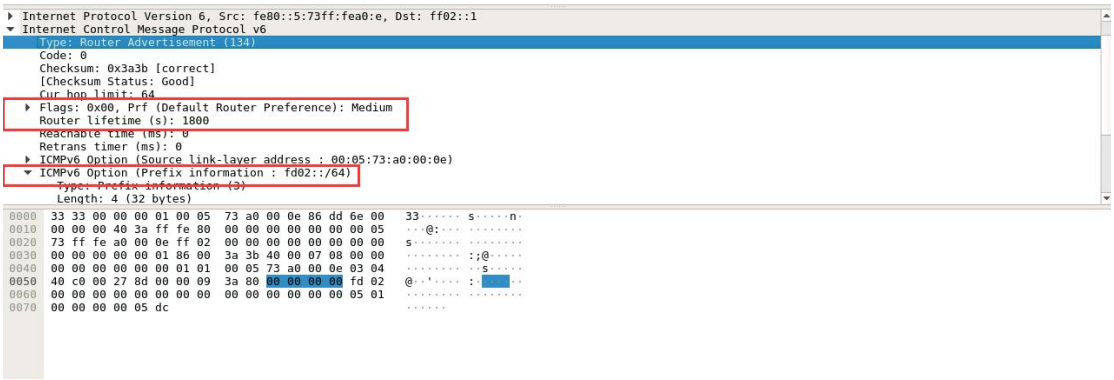
同样的默认配置，Linux Server 也存在相同的问题



（四）抓包分析

通过在交换机上 debug 抓包分析，在交换机默认配置下，接口会默认发送 IPv6 的 RA 信息。

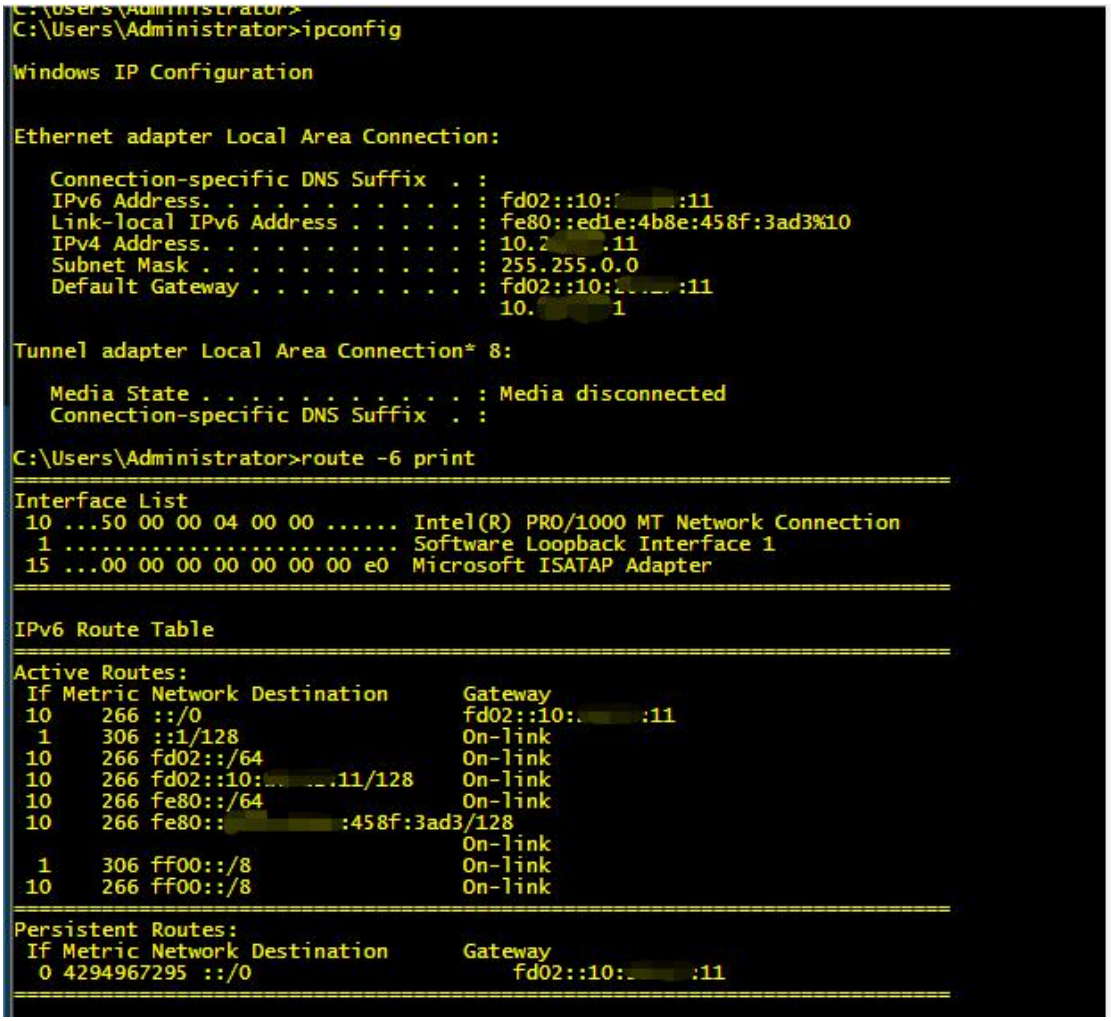




（五）交换机配置优化

将 Windows Server 和 Linux Server 的 Autoconfig 功能都开启，网卡上 IPv6 地址除手工绑定之外，仍有自动生成的地址，同时服务器上存在多条 IPv6 路由。根据交换机厂商 TAC 建议，在接口下开启 ipv6 nd suppress -ra 功能，将 RA 消息抑制，观察效果后发现，Window Server 和 Linux Server 网卡均只存在手动设置的 IPv6 地址，无状

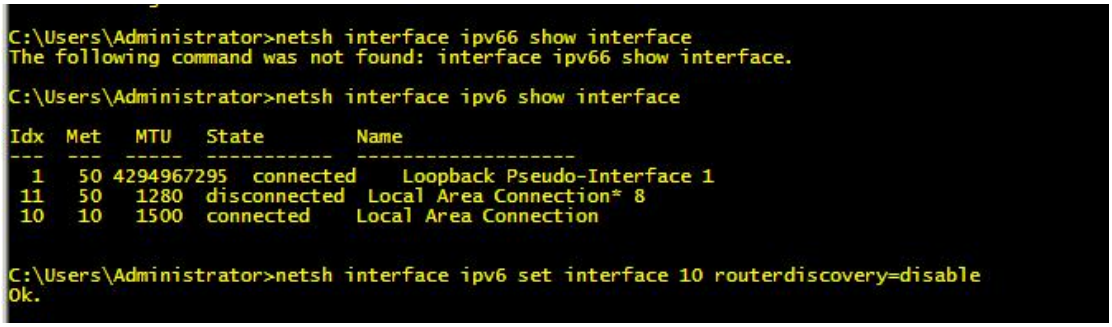
态自动获取到的地址消失了，路由也恢复正常。随后在生产改造中，对 IPv6 交换机均进行了 RA 抑制的设置，保障网络不出现两条路由信息的问题。



（六）服务器网卡优化

在对交换机进行 RA 抑制后，为了提高网络安全，又对服务器的网卡进行优化，谨慎设置 ICMPv6 报文的访问策略，根据实际情况选择合适的安全措施。例如配置 ACL 白名单，

仅允许必须的 ICMPv6 等报文通过,接口关闭 ICMPv6 重定向、端口停止发送 RA 消息，关闭发送 ICMP 不可达信息，关闭源路由，防止 Type 0 Routing Header 攻击等，以免影响正常的服务和应用 Windows Server IPv6 网卡配置。



1、查找网卡 index 和网卡名对应关系

>netsh interface ipv6 show interface 检查 IPv6 网卡 index 和网卡名对应关系

2、禁用网卡无状态功能，有两种办法，使用 index 或者名字，二选一

>netsh interface ipv6 set interface 10 routerdiscovery=disable

针对 index 为 10 的名为 Local Area Connection 的网卡禁用 IPv6 无状态地址获取

>netsh interface ipv6 set interface "Local Area Connection" routerdiscovery=disable

重新检查网卡，只有手工配置的网卡信息了，默认路由也只有手工配置的一个。

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 50-00-00-04-00-00
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fd02::10:[redacted]:11(Preferred)
   Link-local IPv6 Address . . . . . : fe80::ed1e:[redacted]:3ad3%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.[redacted].11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fd02::10:[redacted]:11
                                       10.[redacted].1
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
C:\Users\Administrator>route -6 print
===========================================================================
Interface List
 10 ...50 00 00 04 00 00 ...... Intel(R) PRO/1000 MT Network Connection
  1 ........................... Software Loopback Interface 1
 11 ...00 00 00 00 00 00 00 e0  isatap.{F512A551-C949-48CE-AD44-E9EB8CE51322}
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 10    266 ::/0                     fd02:[redacted]:17:11
  1    306 ::1/128                  On-link
 10    266 fd02::10:[redacted]11/128    On-link
 10    266 fe80::/64                On-link
 10    266 fe80::ed1e:[redacted]:3ad3/128
                                    On-link
  1    306 ff00::/8                 On-link
 10    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
 If Metric Network Destination      Gateway
  0 4294967295 ::/0                     fd02::10:[redacted]:11
===========================================================================
```

Linux 网卡 IPv6 配置

```
valid_lft forever preferred_lft forever
[root@localhost network-scripts]# more ifcfg-eth0
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0
UUID=fa15ff9e-b81c-47ec-a6a9-49741487791c
DEVICE=eth0
ONBOOT=yes
IPADDR=10.[redacted].11
PREFIX=16
GATEWAY=10.[redacted].1
IPV6ADDR=fd02::10:[redacted]:11/64
IPV6_DEFAULTGW=fd02::10:[redacted]:1
```

其中 IPV6_AUTOCONF=no；

检查 Linux 网卡信息，Linux 的网卡上 IPv6 也只有一个 IPv6 地址可用，恢复正常。

通过前期改造过程中碰到此类问题的总结和实验经验的转化，国联证券在后期的互联网应用区 IPv6 改造中，均同时对 IPv6 交换机进行 RA 抑制和双栈服务器网卡进行优化，提高了改造的效率和网络层的安全性。

四、结语

2022 年国联证券继续贯彻一行两会文件要求，持续稳步推进 IPv6 改造。针对新上线且面向互联网的系统，做好 IPv4/IPv6 双栈支持，借鉴同行业 IPv6 相关技术分享，以保障和优化客户服务为宗旨，构建安全稳定的 IPv6 网络环境。

IPv6 改造是一项复杂的系统性工程，改造后的稳定性还有待后续较长时间的验证，相关系统运维经验还需要较长时间的积累。当前金融行业 IPv6 规模部署已经进入第三阶段“持续建设阶段”，国联证券将继续遵照一行两会实施意见的要求，坚持“一个前提，两个结合”基本原则，稳中求进，不断总结 IPv6 改造经验。

参考文献：

[1]杨玲,宋烜,陈林等. 大型商业银行数据中心 IPV6 研究与实践[J]. 中国金融电脑,2020(03):60-64.

[2]龙剑飞,方涌,潘光远等.广发证券 IPv6 改造实践[J]. 金融电子化,2020(03):68-69.