**实验7 IPv6技术实验**

1. 3.5节步骤2中，请思考下面问题：

主机加入到组播组中的过程是什么？

**答：1．主机通过地址自动配置，获得多播组地址。**

**2．主机发出MLD组播侦听者报文给本地链路上的路由器，宣告自己加入的组播组。**

**3．路由器收到后，根据报文中的信息向多播转发表添加中相关表项，记录多播组的成员身份，对于链路本地的组播则不添加。**

1. 3.5节步骤3中，仔细观察PC1与RT1之间的交互报文，回答下述问题：
   1. 为什么报文中的“next header”采用hop-by-hop的选项？

**答：因为hop-by-hop选项是每一个中间路由器必须处理的唯一扩展报头，在组播侦听报告报文中，使用该项提醒路由器对MLD报文进行深入检查扩展报头字段值，该字段主要用于为在传送路径上的每次跳转指定发送参数，传送路径上的每个中间节点都要读取并处理该字段。此外，当使用超大IP数据包的时候长度信息会发生变化，在该选项中会用一个新的字段值来表示。**

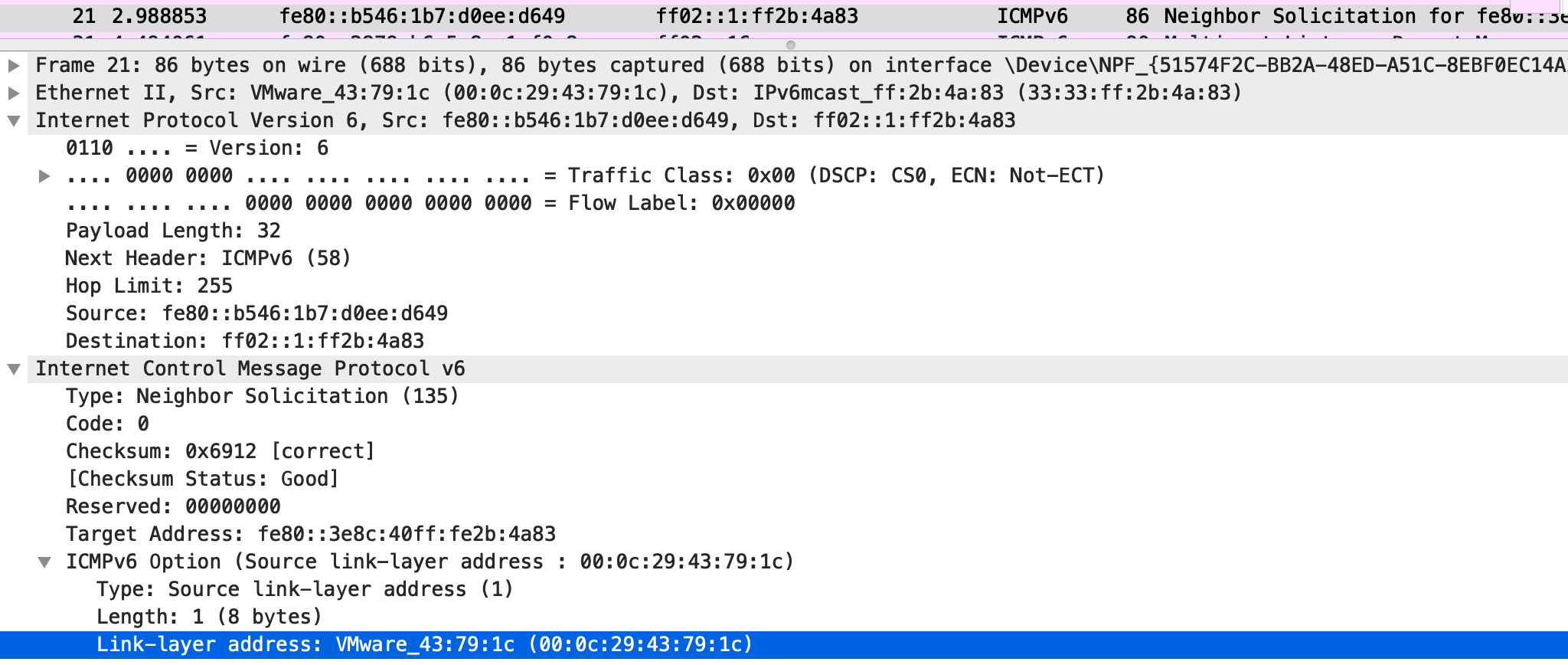
* 1. 为什么跳数被限制为1？

**答：可以让所有的MLD报文都被限制在链路本地上。**

* 1. 在“Hop-by-Hop”选项中，有一个“Padn”，它的作用是什么？

**答：Padn是用于插入两个或者多个填充字节，目的在于使选项符合对齐要求，保证选项中特定字段位于期望的边界之内。**

1. 3.5节步骤4中，仔细观察Router Solicitation的报文，回答下述问题：



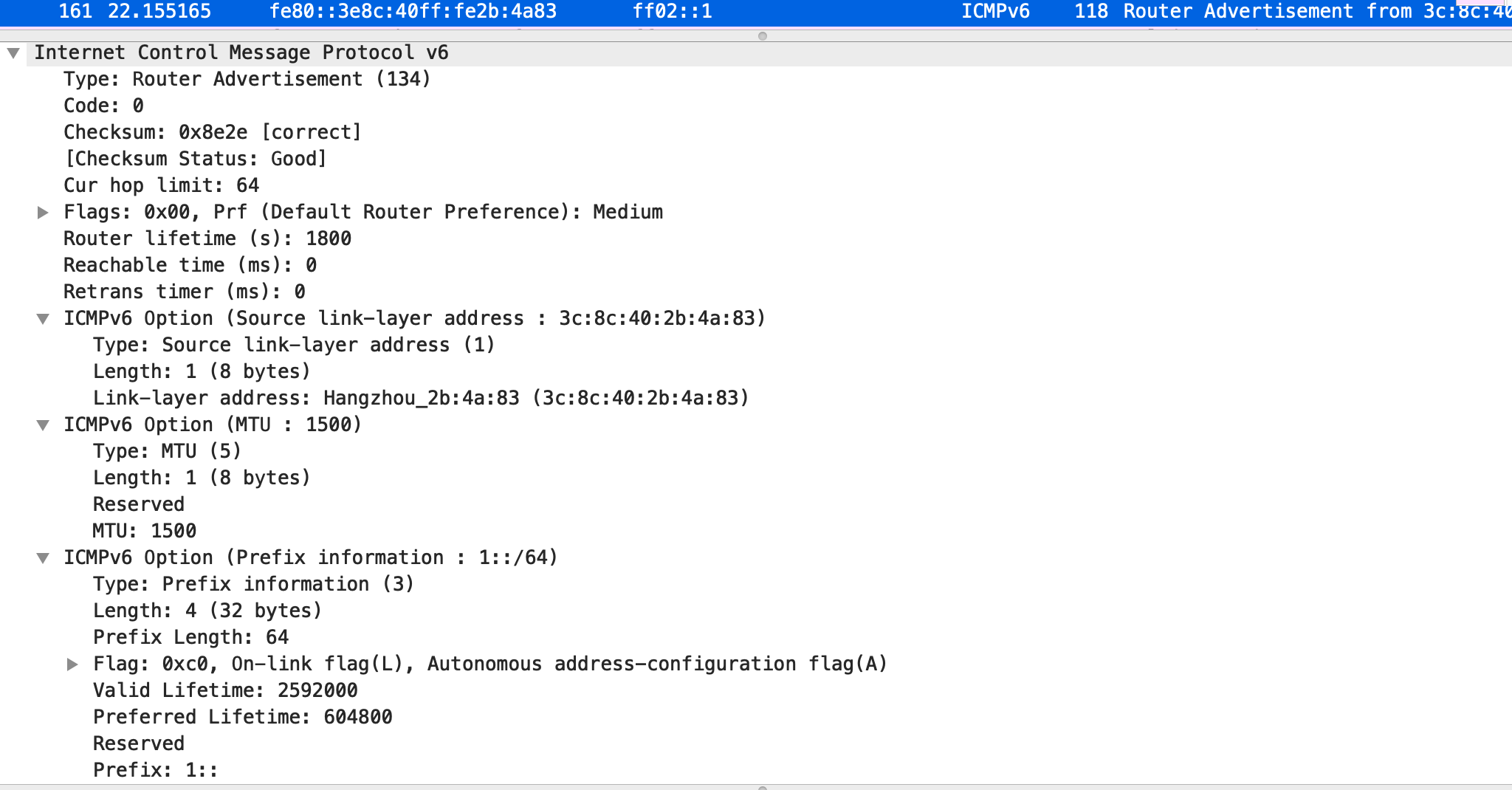
* 1. 在前面的multicast listener report报文中，报文的跳数限制为1，而在这里，同样是主机发给路由器的报文，为什么跳数却采用255？

**答：因为封装ICMP RA报文的IPv6报文头中的Hop Limit必须设置成255，确保非本链路的设备不能通过发送路由器宣告来试图干扰通信流，确保安全。如果非本链路设备向本链路发送RA，经过路由器以后跳水限制减1，使该报文成为非法。接受节点只认为条数限制是255的RA是有效的。**

* 1. 报文中的ICMP选项中的“source link-layer address”的作用是什么？

**答：source link-layer address是发送者的MAC地址，表示发送该RS报文的接口所处的链路层地址，这样可以让路由器在收到RS报文后无需进行地址解析，就可以返回用于应答RS的RA报文。**

1. 3.5节步骤6中，仔细观察Router Advertisement的报文，回答下述问题：



* 1. “Cur hop limit”的含义是什么？

**答：主机发送报文使用的默认跳数限制。**

* 1. 报文中“lifetime”的含义是什么？

**答：发送该RA报文的路由器作为缺省路由器的生命周期，缺省为30分。这里表示已经正常运行1800s。**

* 1. “reachable time”的含义是什么？

**答：路由器在接口上通过发送RA报文，让同一链路上的所有节点都使用相同的可达时间，此处为0说明未配置。**

* 1. “retransmit time”的含义是什么？

**答：重传NS报文的时间间隔，用于邻居不可达检测和地址解析，此处为0说明未配置**

* 1. 这里为什么会有“source link-layer”地址呢？

**答：为了表示路由器发送RA报文的接口的链路层地址。**

1. 4.4节步骤2中，路由 ::1和2001::各代表什么意思？并通过IPv4中的相关路由举例说明。

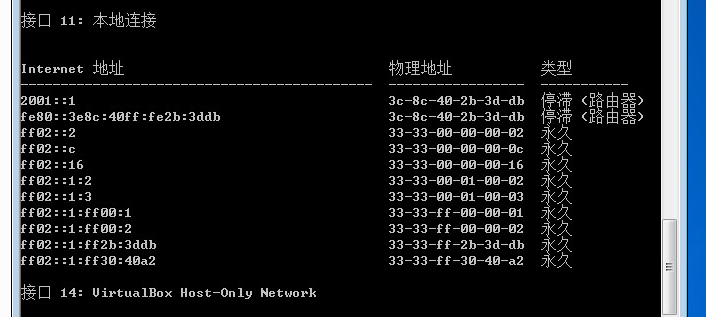
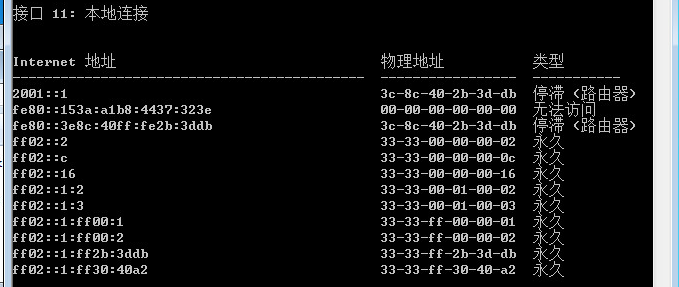
**答：路由::1表示的是路由器的本地回路地址，类似于IPv4中的本地回路地址127.0.0.1，指的是路由器的loopback口，相当于路由黑洞，路由下一跳指向这里可以达到禁止访问的作用。2001::表示的是2001::/64这个网段号，类似于IPv4中的网络号192.168.0.0/16。**

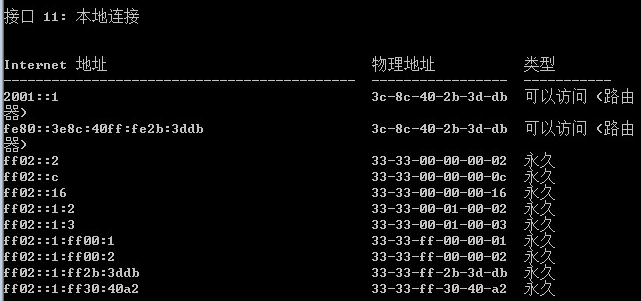
1. 4.4节步骤2中，为什么会有2007::2这条主机路由？

**答：因为路由器的接口E0/0的接口地址为2007::2，与这个接口直连的网段是2007::，可以看到2007::2的下一跳为::1表示下一跳还是指向路由本身。**

1. 5.4节步骤1中，记录邻居状态的变化过程。

**答：邻居状态由一开始断开连接时候的不完整，到停滞最后到可以访问。**

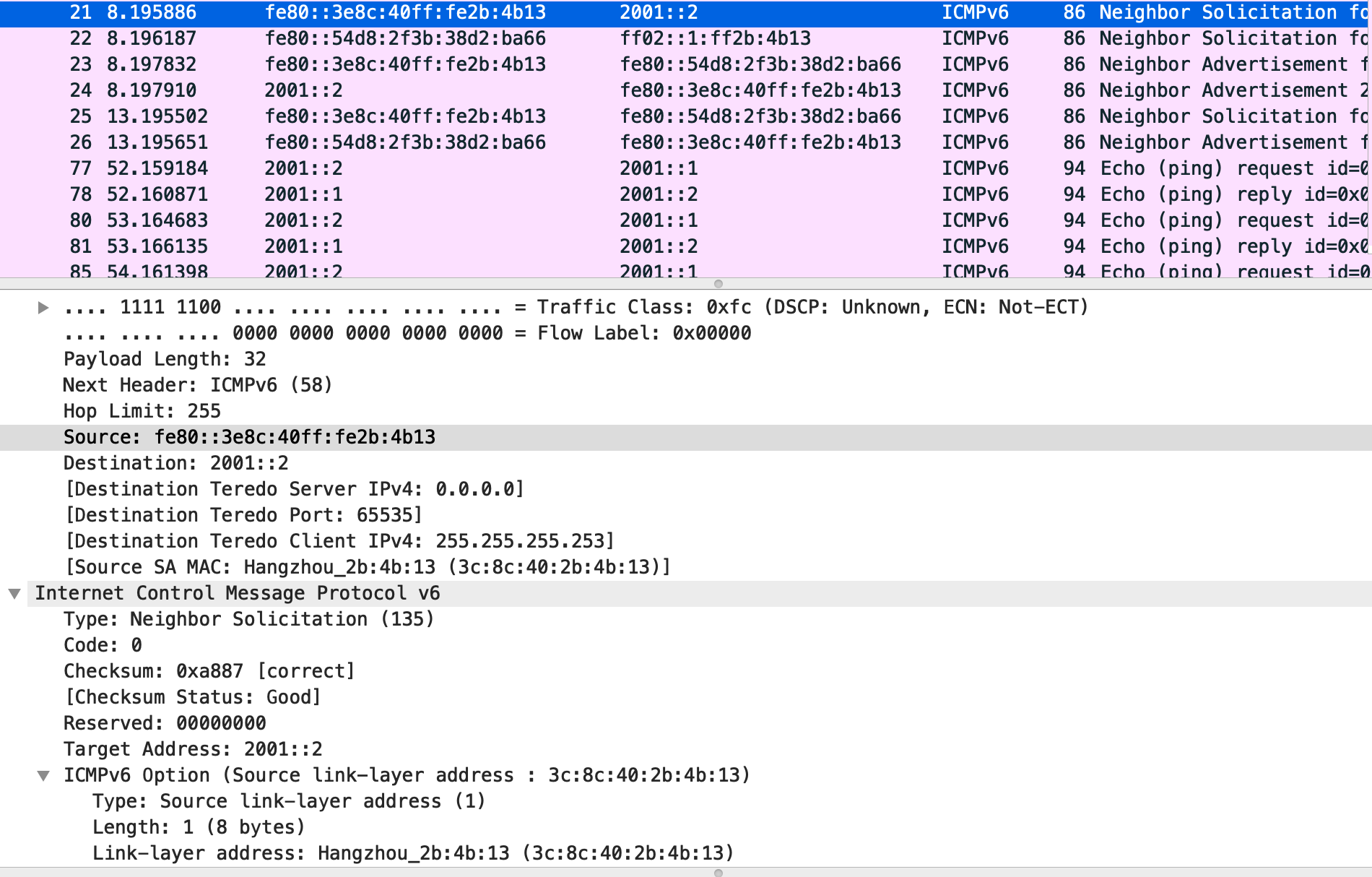


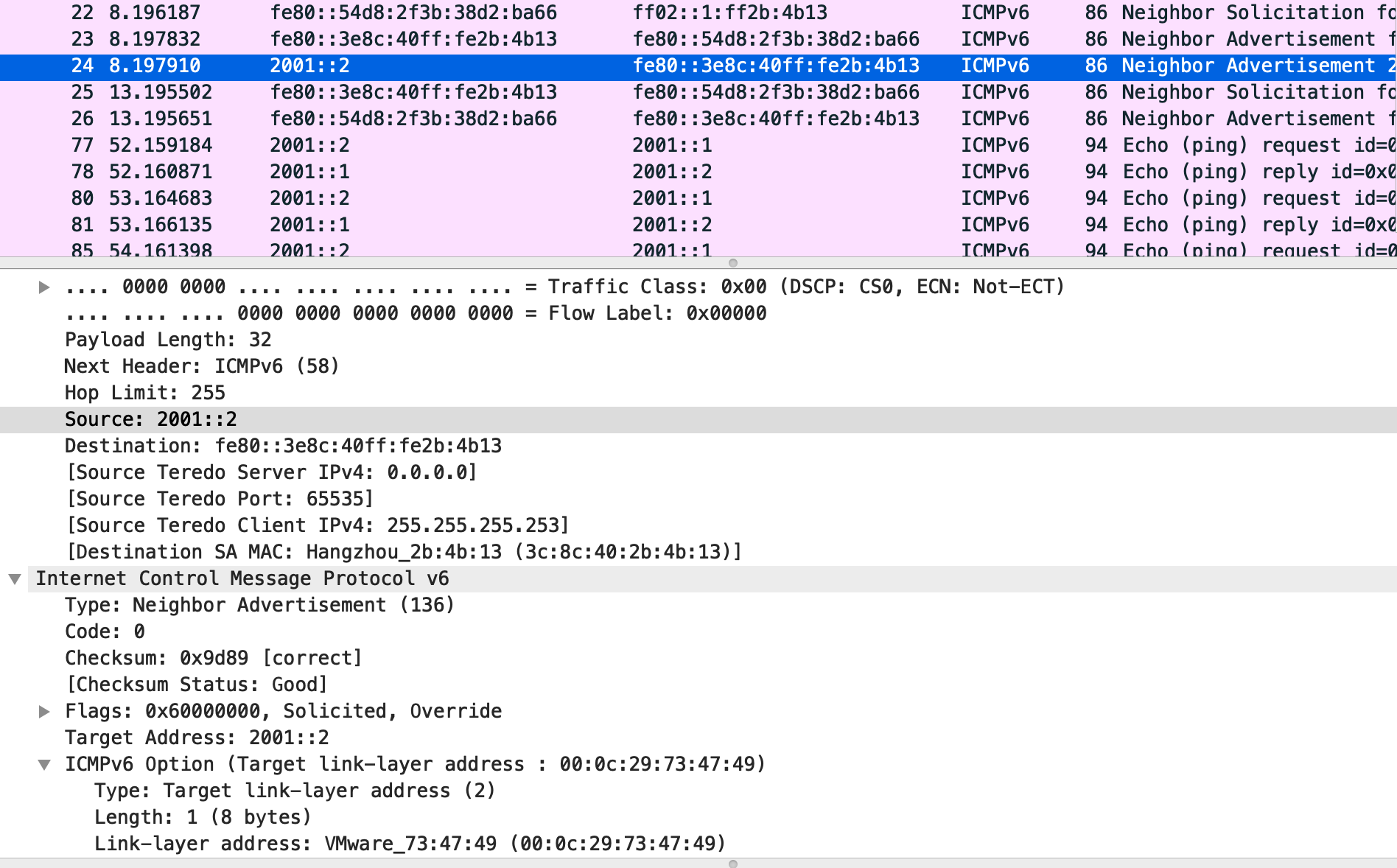


1. 5.4节步骤1中，结合截获报文和邻居状态变化，简述On-link地址解析的全过程。

**答：邻居状态在整体过程从不完整到可以访问的状态转变。**

1. **首先PCA查找邻居缓存，若有，封装并发送数据包；若无，创建2001::2为索引的表项，并标识状态为Incomplete（不完整）。**
2. **PCA发送NS报文，IPv6目的地址为2001::2对应的被请求节点（Solicited-node）组播地址ff02::1:ff2b:4b13，并在其中的Target域包含待解析地址2001::2。（PS:被请求节点组播地址为ff02::1:ff+24位地址,24位地址取决于地址配置）**
3. **PCB收到后发送NA报文，包含Target2001::2及其链路层地址，同时将对端2001::1与其链路层地址映射加入到本地邻居缓存表，设置其状态为Stale（停滞，因为只知道PCA到PCB是通的，不确定PCB到PCA是否通）。**
4. **PCA收到PCB的NA报文，并将2001::2及其链路层地址加入邻居缓存表，设置其状态为Reachable（可到达的）。**





1. 5.4节步骤1中，请结合Neighbor Solicitation和Neighbor Advertisement报文分析IPv4与IPv6地址解析的同异之处。

**答：相同：地址解析技术基本类似，采用一问一答的方式。在IPv4中当主机与目标主机需要通信时，必须先通过ARP协议获得目标主机的链路层地址。而在IPv6中通过邻居发现协议(ND)获得IP地址解析到链路层地址。**

**不同：IPv4通过APR解析，IPv6通过NS和NA解析；APR用广播，NS用被请求节点的组播，由于被请求节点组播地址的接受者通常只有一个，组播的优点是显而易见的；IP头部中的跳数限制不同。**

1. 5.4节步骤2中，分析截获的报文，请分析IPv4中的ARP报文被何种报文所替代？新的报文与ARP报文相比有何差异？

**答：Neighbor Solicitation和Neighbor Advertisement报文所替代。**

**Neighbor Solicitation报文用来当做多播使用，替代ARP请求报文的广播，能够节省网络带宽。**

**Neighbor Advertisement报文本身是基于ICMPv6实现的，以太网协议类型为0x86DD,可以被看做第三层的协议，使用第三层的安全机制避免地址解析攻击。**

**NS和NA报文会在option段中包含所请求的MAC地址，报文通信是用组播和单播。**

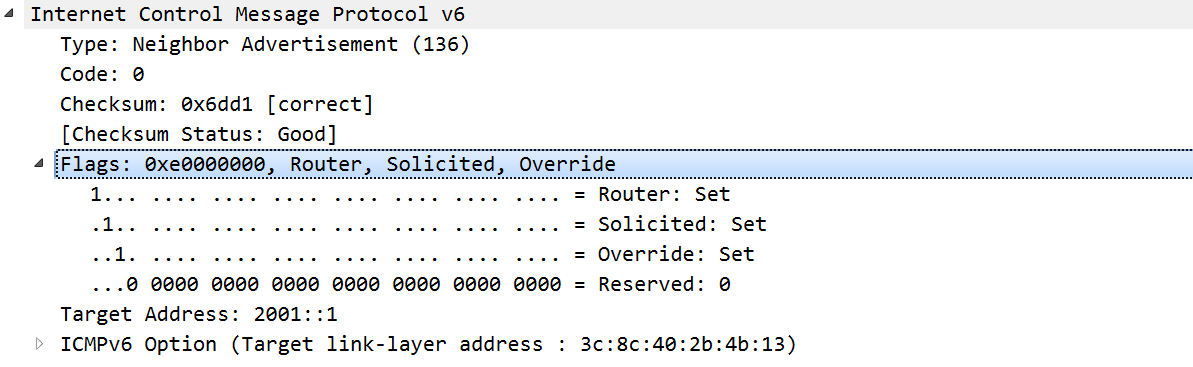
**ARP报文是直接封装在以太网报文中，以太网协议类型为0x0806，被认为是2.5层的协议。ARP报文会直接包含源和目的的MAC地址。**

1. 5.4节步骤2中，查看截获的neighbor advertisement报文，请解释其中flags域中的router、solicited、overfide字段的作用是什么？

**答：1.** **R：路由器标记（Router Flag）,表示报文发送者的角色。值为1表示发送者是路由器，值为0表示主机。**

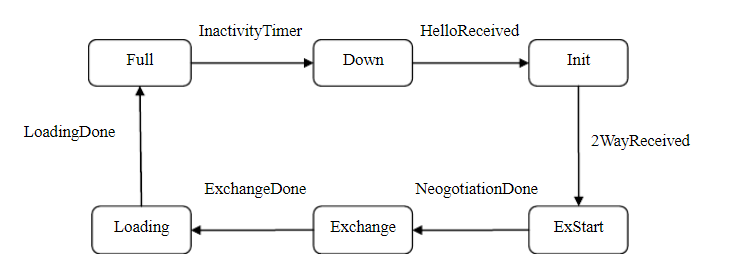
**2. S:请求标记（Solicited Flag）。值为1表示该报文是对NS报文的响应。**

**3. O:覆盖标记（Override Flag）。值为1表示节点可用NA中的目标链路层地址来覆盖原有的邻居缓存表；值为0表示只有在链路层地址未知时，才能更新邻居缓存表项。**

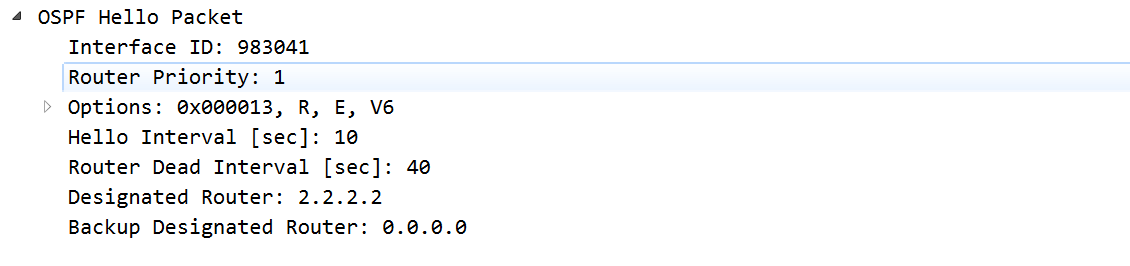


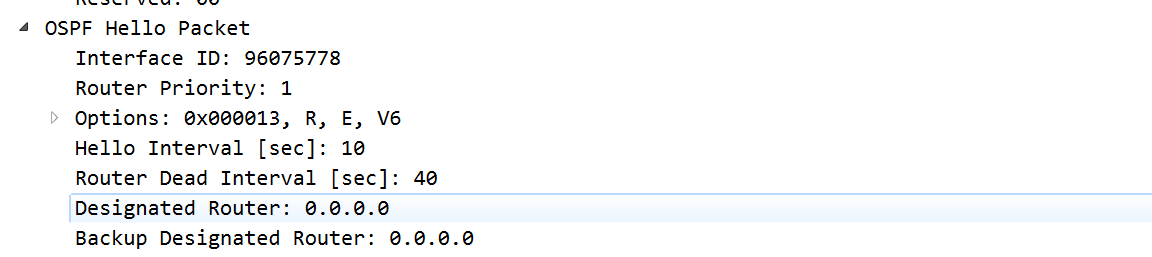
1. 6.6节步骤4中，根据所捕获的报文，简述路由器在启动OSPFv3后建立邻接关系及同步LSDB的过程。

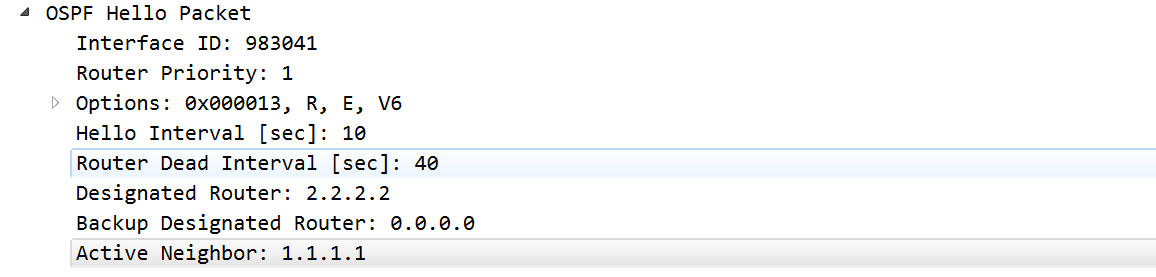
**答：路由器和交换机之间周期性发送Hello报文，在收到Hello报文后，把邻居对象放入邻居列表中，双方发送DD报文来描述自己的LSDB，进行数据库的同步，收到后检查自己LSDB库中缺乏哪些信息，将缺少的LSA信息通过LSR请求报文获取，对方收到后用LSU报文发送，收到后用LSAck报文应答。**



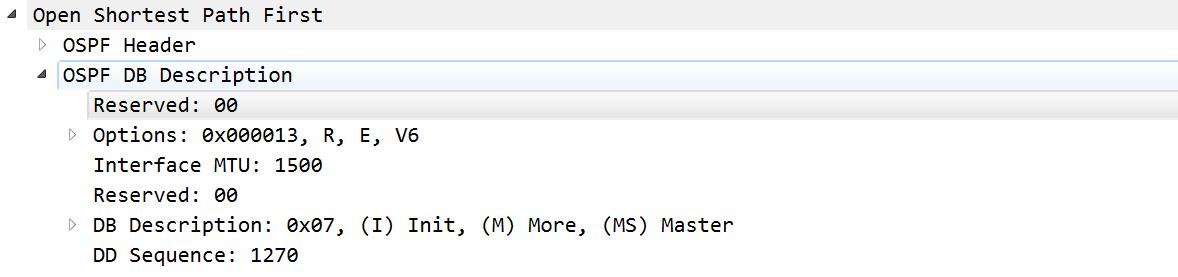
1. **R1启动OSPFv3之后不断向S1发送Hello报文，但是没收到S1的Hello报文。**



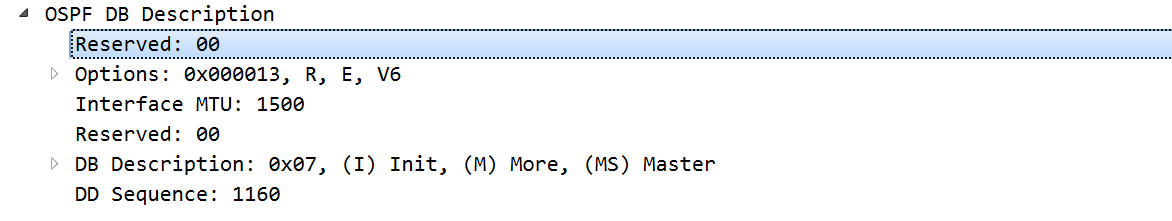
1. **S1启动OSPFv3后，在收到R1的Hello报文后将R1的状态设置为Init,并向R1发送Hello报文。**
2. **R1收到S1发送的Hello报文后，将S1的状态设置为ExStart,再次发送Hello报文并且把Active Neighbor字段设置为S1的router-id**



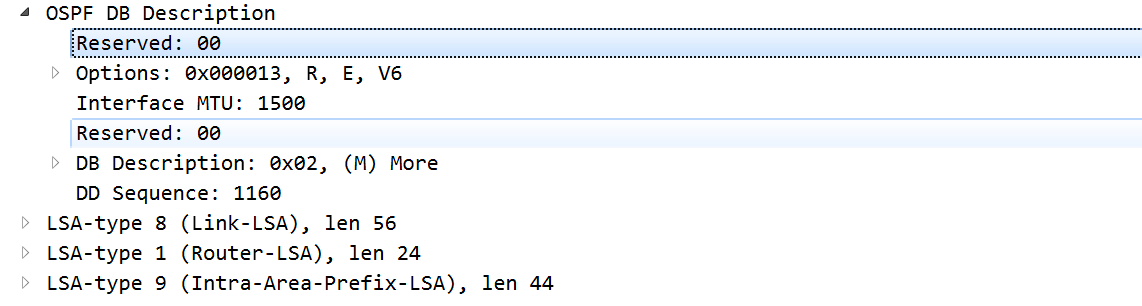
1. **S1收到R1的Hello报文后，将R1的状态设置为ExStart，开始发送DD报文协商主从关系。**



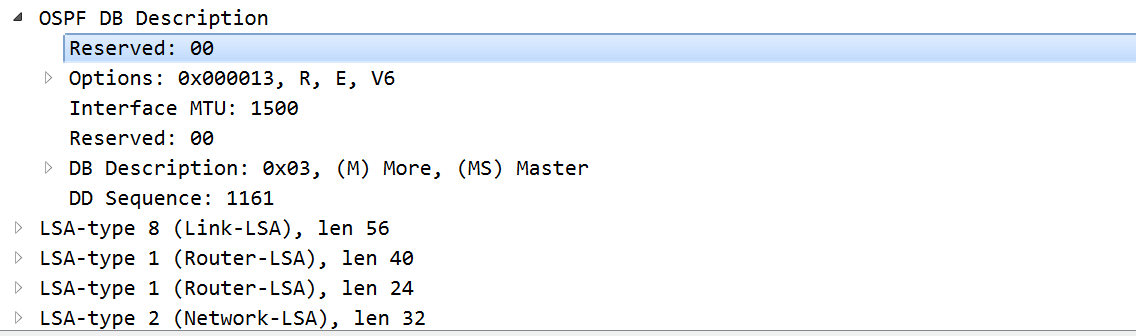
1. **R1收到DD报文后对比自己router-id设置自己为DR并且发送DD报文协商主从关系。**



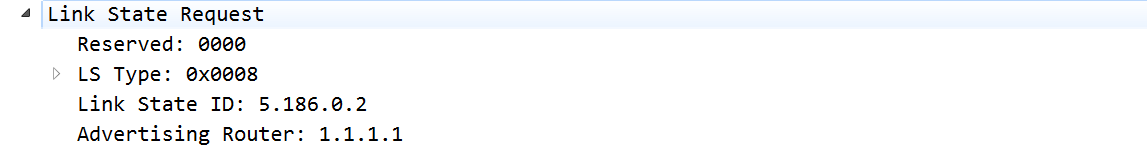
1. **S1收到后承认R1为主路由器，发送DD描述报文并且附带LSA信息，进入Exchange状态。**



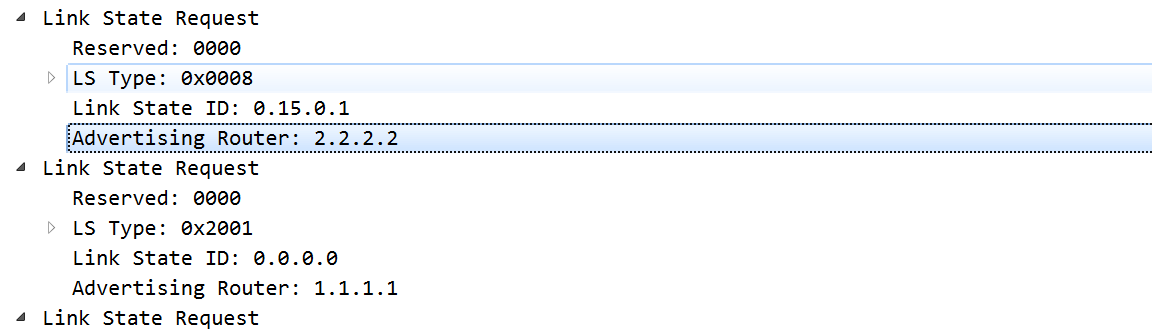
1. **R1回复DD报文并携带LSA信息。**



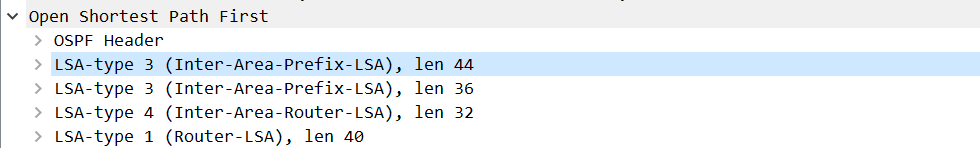
1. **R1将S1的状态设置为Loading状态，发送LSR报文请求LSA知道LSDB完全同步进入Full状态。**



1. **S1将R1的状态设置为Loading状态，发送LSR报文请求LSA知道LSDB完全同步进入Full状态。**



1. **最后R1和S1收到LSU报文后，回复LSAck报文**



1. 6.6节步骤4中，查看OSPFv3的Hello报文内容，其中报文的源地址类型为 **链路本地地址** ，目的地址类型为 **组播地址** ，报文中是否携带有IPv6地址信息？

**答：**

**没有携带ipv6地址信息，只有路由器的routerID信息。**

1. 6.6节步骤5中，查看RT1的LSDB，回答其中的Router-LSA和Network-LSA中是否包含地址前缀信息，OSPFv3为什么要增加Link-LSA和Intra-Area-Prefix-LSA这两类LSA？分别解释它们的作用。

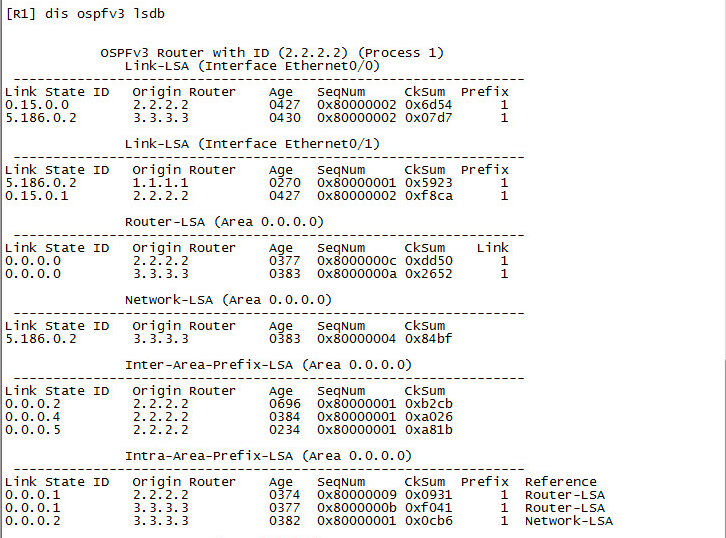
**答：**

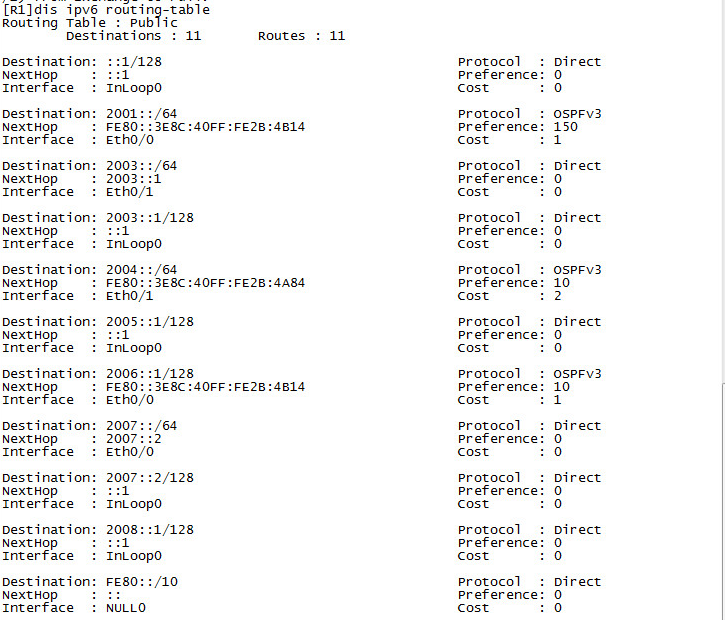
**Router-LSA和Network-LSA中不包含地址前缀信息；**

**首先OSPFv3因为在所有的协议报文字段中不再包含网络地址相关内容，网络地址相关内容包含在链路状态通告报文（Link-LSAs）的载荷中。由于Router-LSA和Network-LSA不再包含地址信息，导致了Intra-Area-Prefix-LSAs的引入。**

**Link-LSAs：路由器为每一条链路生成一个Link-LSA，在本地链路范围内传播。每一个Link-LSA描述了该链路上所连接的IPv6地址前缀及路由器的Link-local地址。**

**Intra-Area-Prefix-LSAs：每个Intra-Area-Prefix-LSA 包含路由器上的IPv6 前缀信息，Stub 区域信息或穿越区域（Transit Area）的网段信息，该LSA在区域内传播。由于Router-LSA和Network-LSA不再包含地址信息，导致了Intra-Area-Prefix-LSAs的引入。**





# 7 BGP4+协议分析实验

## 7.1 实验内容

BGP4+协议分析

## 7.2 实验目的

了解BGP4+协议与BGP4协议的不同，理解BGP4+的扩展。

## 实验原理

### 7.3.1 BGP4+概述

传统的BGP-4只能传递IPv4单播的路由信息，不能传递其它网络层协议（如IPv6 等）的路由信息。为了提供对多种网络层协议的支持，IETF对BGP-4 进行了扩展，形成BGP4+（Multiprotocol Border Gateway Protocol，MP-BGP多协议边界网关协议）。BGP4+可以为多种网络层协议传递路由信息，如IPv6 单播、IPv4 组播、IPv6 组播、VPNv4、VPNv6、L2VPN、IPv4 MDT 等。本实验重点介绍BGP4+针对IPv6的扩展。

BGP对等体在建立BGP连接、发布BGP路由之前，需要发送OPEN消息进行BGP能力协商。BGP能力协商由RFC3392中定义的一种新的Optional Parameter（可选参数）-Capabilities Advertisement（能力通告）实现的。

Capabilities Advertisement使用CLV（Code，Length，Value）格式，用于通告本路由器支持的多种能力，其格式如图1所示：

|  |
| --- |
| Capability Code（1 octet） |
| Capability Length（1 octet） |
| Capability Value（Variable） |

图1 Capabilities Advertisement格式

### 7.3.2 BGP4+（MP-BGP）的扩展属性

通常，路由信息中与网络层协议相关的关键信息包括路由前缀和下一跳地址。BGP-4 通过Update 消息中的NLRI（Network Layer Reachability Information，网络层可达性信息）字段携带可达路由的前缀信息，Withdrawn Routes 字段携带不可达路由的前缀信息，NEXT\_HOP 属性携带下一跳地址信息。

由于NLRI 字段、Withdrawn Routes 字段和NEXT\_HOP 属性不易于扩展，无法携带多种网络层协议的信息。因此，为实现对多种网络层协议的支持，MP-BGP 定义了两个新的路径属性：

• MP\_REACH\_NLRI（Multiprotocol Reachable NLRI，多协议可达NLRI）：用于携带多种网络层协议的可达路由前缀及下一跳地址信息，以便向邻居发布该路由。

• MP\_UNREACH\_NLRI（Multiprotocol Unreachable NLRI，多协议不可达NLRI）：用于携带多种网络层协议的不可达路由前缀信息，以便撤销该路由。

MP-BGP 通过上述两个路径属性传递不同网络层协议的可达路由和不可达路由信息。不支持MP-BGP 的BGP 发言者接收到带有这两个属性的Update 消息后，忽略这两个属性，不把它们传递给其它邻居。

|  |
| --- |
| Address Family Identifier (2 octets) |
| Subsequent Address Family Identifier (1 octet) |
| Length of Next Hop Network Address (1 octet) |
| Network Address of Next Hop (variable) |
| Number of SNPAs (1 octet) |
| Length of first SNPA(1 octet) |
| First SNPA (variable) |
| Length of second SNPA (1 octet) |
| Second SNPA (variable) |
| …… |
| Length of Last SNPA (1 octet) |
| Last SNPA (variable) |
| Network Layer Reachability Information (variable) |

图2 MP\_REACH\_NLRI属性的格式

|  |
| --- |
| Address Family Identifier (2 octets) |
| Subsequent Address Family Identifier (1 octet) |
| Withdrawn Routes (variable) |

图3 MP\_UNREACH\_NLRI 属性的格式

MP-BGP 采用地址族（Address Family）和子地址族（Subsequent Address Family）来区分MP\_REACH\_NLRI 属性、MP\_UNREACH\_NLRI 属性中携带路由信息所属的网络层协议。例如，如果MP\_REACH\_NLRI 属性中AFI（Address Family Identifier，地址族标识符）为2、SAFI（Subsequent Address Family Identifier，子地址族标识符）为1，则表示该属性中携带的是IPv6单播路由信息。关于地址族的一些取值可以参考RFC 1700。

## 7.4 实验环境

支持IPv6的路由器和交换机各两台，网线若干。

## 7.5 实验组网

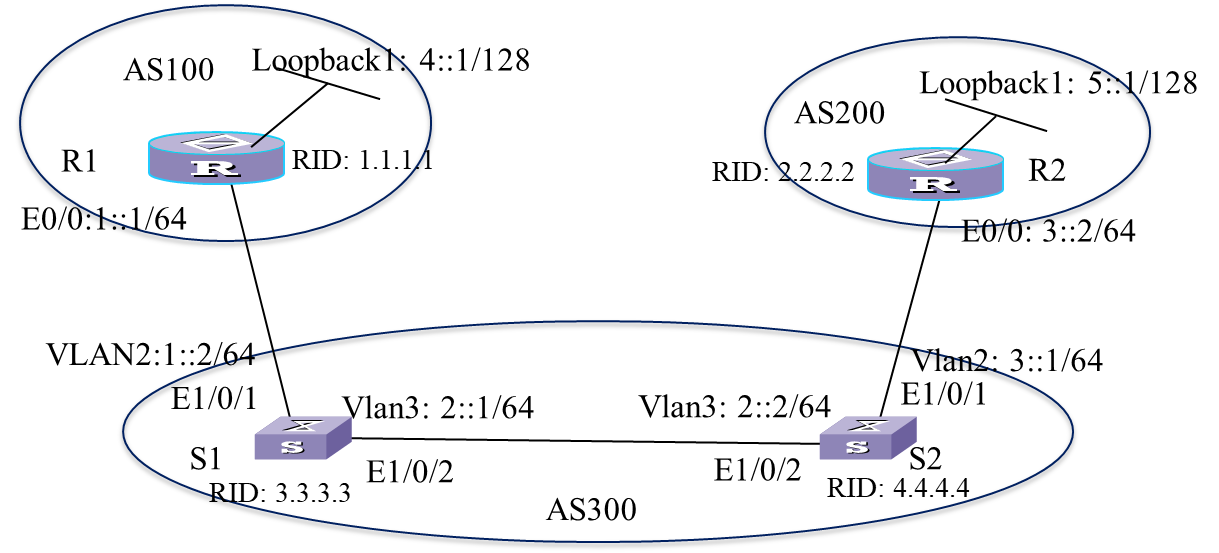


图4 实验组网图

## 7.6 实验步骤

步骤1 按照图4进行连线组网。

步骤2 按照图4配置相关设备的IP地址和Vlan。

步骤3 按照图4配置BGP4+协议，参考配置如下：

~~<R1> system-view~~

~~[R1] bgp 100~~

~~[R1-bgp] router-id 1.1.1.1~~

~~[R1-bgp] peer 1::2 as-number 300~~

~~[R1-bgp] address-family ipv6~~

~~[R1-bgp-ipv6] peer 1::2 enable~~

~~[R1-bgp-ipv6] network 4::1 128~~

**V5版本的设备，请参考以下命令。**

[H3C] ipv6

[H3C] bgp 100

[H3C-bgp] router-id 2.2.2.2

[H3C-bgp] ipv6-family

[H3C-bgp-af-ipv6] peer 1::2 as-number 100

[H3C-bgp-af-ipv6] peer 3::2 as-number 200

[H3C-bgp-af-ipv6] network 4::1 128

**V7版本的设备，请参考以下命令：**

[R1] bgp 100

[R1-bgp] router-id 1.1.1.1

[R1-bgp] peer 1::2 as-number 200

[R1-bgp] address-family ipv6

[R1-bgp-ipv6] peer 1::2 enable

[R1-bgp-ipv6] network 4::1 128

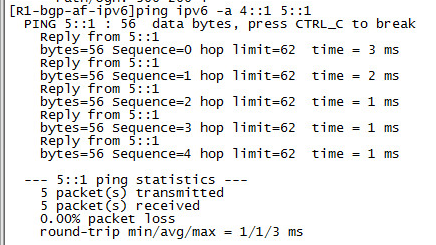
还要强制下一跳！！！！！！！！！！(真的是沙比实验！)

其它设备配置类似。

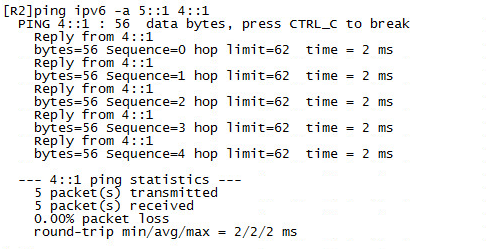
步骤4 实验验证与BGP4+协议报文分析。

（1）验证R1和R2的Loopback1接口网段的路由可以通过BGP4+传播，并能够相互ping通。

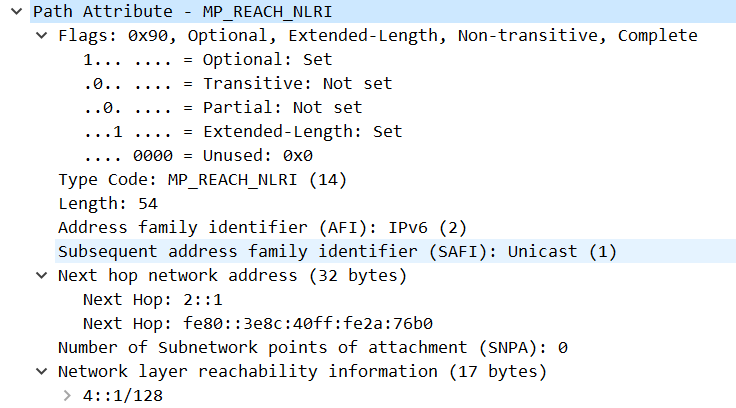
**R1 Loopback ping R2 Loopback**

****

**反向ping检查**



（2）截获BGP4+协议报文，在实验报告上写出报文中MP\_REACH\_NLRI属性和MP\_UNREACH\_NLRI属性的内容。



MP\_REACH\_NLRI属性

|  |  |
| --- | --- |
| Address Family Identifier (2 octets) | 2（IPv6） |
| Subsequent Address Family Identifier (1 octet) | 1（Unicast） |
| Length of Next Hop Network Address (1 octet) | 32 |
| Network Address of Next Hop (variable) | 2::1 |
| Network Address of Next Hop (variable) | fe80::3e8c:40ff:fe2a:76b0 |
| Number of SNPAs (1 octet) | 0 |
| Network Layer Reachability Information (variable) | 4::1/128 |

**注意：这里想要获得unreach报文是得手动断开连接时才会传递的，而reach报文是正常连通情况下传递的。**

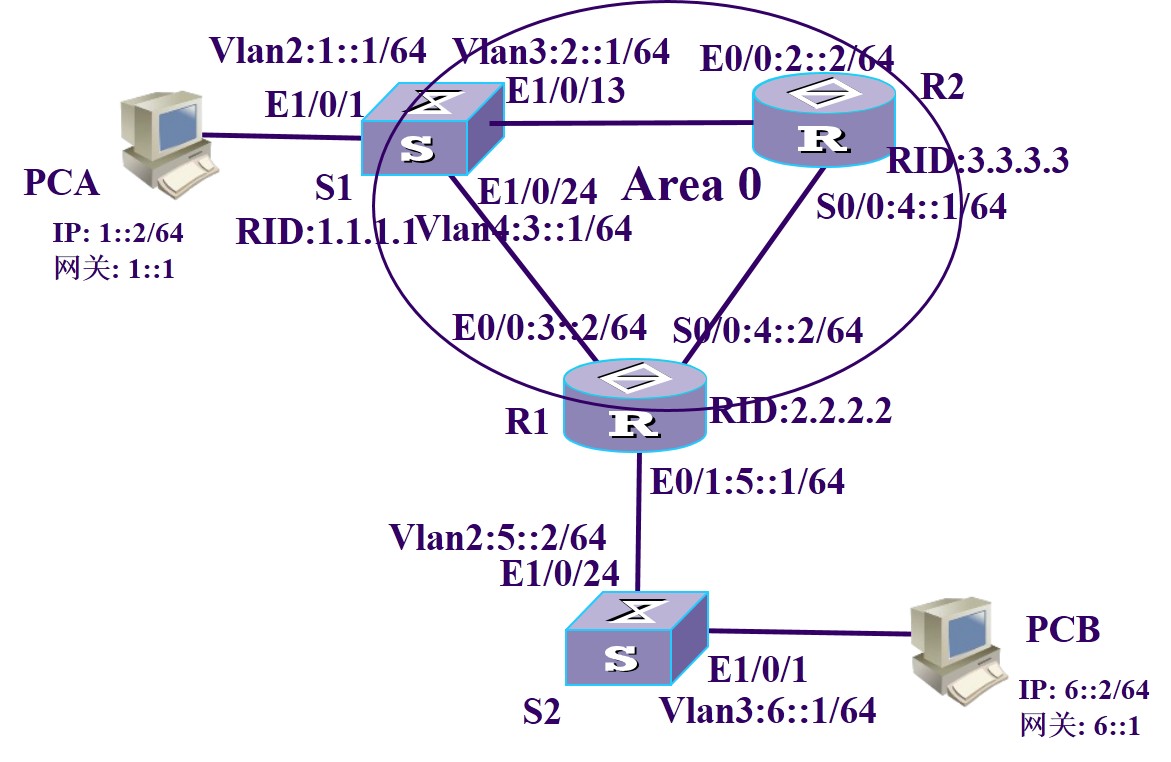
MP\_UNREACH\_NLRI属性

|  |  |
| --- | --- |
| Address Family Identifier (2 octets) | 2（IPv6） |
| Subsequent Address Family Identifier (1 octet) | 1（Unicast） |
| Withdrawn Routes (variable) | 3::/64 |
| Withdrawn Routes (variable) | 5::1/128 |

# 8 设计型实验

设计由两台路由器、两台交换机组成的IPv6网络。满足如下要求：

1. 正确组网；
2. 在S1和S2上合理划分VLAN；
3. 配置各台设备接口的IP地址；
4. 在S1，R1，R2上启动OSPFv3协议，完成相关配置；
5. 在相关设备上配置静态路由（不允许使用路由引入和扩大ospf区域范围），保证全网互通，并确保两台计算机之间通信优先选择PCA—S1—R2—R1—S2—PCB路径，另外的路径作为备份。
6. 请将OSPFv3和静态路由的主要配置写在实验报告上
7. 请用ipconfig和tracert命令验证，并将截图粘贴在实验报告。



PCA、PCB配置好IP和网关

S1:

ospfv3 1

router-id 1.1.1.1

interface vlan 3

ospfv3 1 area 0

interface vlan 4

ospfv3 1 area 0

ipv6 route-static 5:: 64 3::2

ipv6 route-static 5:: 64 4::2 preference 10

ipv6 route-static 6:: 64 3::2

ipv6 route-static 6:: 64 4::2 preference 10

R1:

ospfv3 1

router-id 2.2.2.2

interface e0/0

ospfv3 1 area 0

interface s1/0

ospfv3 1 area 0

ipv6 route-static 1:: 64 3::1

ipv6 route-static 1:: 64 2::1 preference 10

ipv6 route-static 6:: 64 5::2

S2:

ipv6 route-static 1:: 64 5::1

ipv6 route-static 2:: 64 5::1

ipv6 route-static 3:: 64 5::1

ipv6 route-static 4:: 64 5::1

R2:

ospfv3 1

router-id 3.3.3.3

interface e0/0

ospfv3 1 area 0

interface s1/0

ospfv3 1 area 0

ipv6 route-static 1:: 64 2::1

ipv6 route-static 5:: 64 4::2

ipv6 route-static 6:: 64 4::2





ipv6 route-static 1:: 64 2::1 preference 10

配置上面命令的原因就是当S1-R2断开时候，假如是ipv6 route-static 1:: 64 3::1 preference 10

PCB ping PCA的报文还会从R1-R2走，并不知道路由已经断开了，这是报文就会在R2丢失产生丢包，所以这里静态路由下一跳填写2::1，断开后R1路由表会发现没有到2::1的路由表项，并且因为配置了OSPF所以路由器会自己查找路由表去往2::1的出口下一跳，从而选择走R1-S1这条路径。

断开S1-R2：



断开R1-R2：

