信息网络与协议

实验指导书

（2023 秋季学期）

课 程 教 师

卢 汉 成　　hclu@ustc.edu.cn

助　教

李 伦 升　　**lunsheng23@mail.ustc.edu.cn**

龙 万 青　　**madoren@mail.ustc.edu.cn**

孟　　琪　　**mengqi7788@mail.ustc.edu.cn**

陈 雨 昂　　**yuangchen21@mail.ustc.edu.cn**

注意事项

1) 本课程一共包含 4 个实验，分五周完成。
2) 实验报告通过邮箱进行提交，具体提交方式见实验准备（4）。报告提交截止时间为每周三，迟交会有记录。
3) 第四次实验时间为两周，可以提前完成并提交实验报告。
4) 四次实验内容是彼此独立的，单次实验完成之后请务必点击结束实验按钮释放资源。每次实验直接启动建立好的实验，不需要重复创建。
5) 本课程实验基于未来网实验设施平台进行，如实验过程中遇到问题，请及时通过课程群与助教联系。

实验准备

本次实验基于未来网络实验设施平台 http://ceni.ustc.edu.cn 进行，请通过校园网登录该网站进行实验。关闭网页不会影响实验数据。

一、 登录

在浏览器输入地址 http://ceni.ustc.edu.cn 登录实验平台。

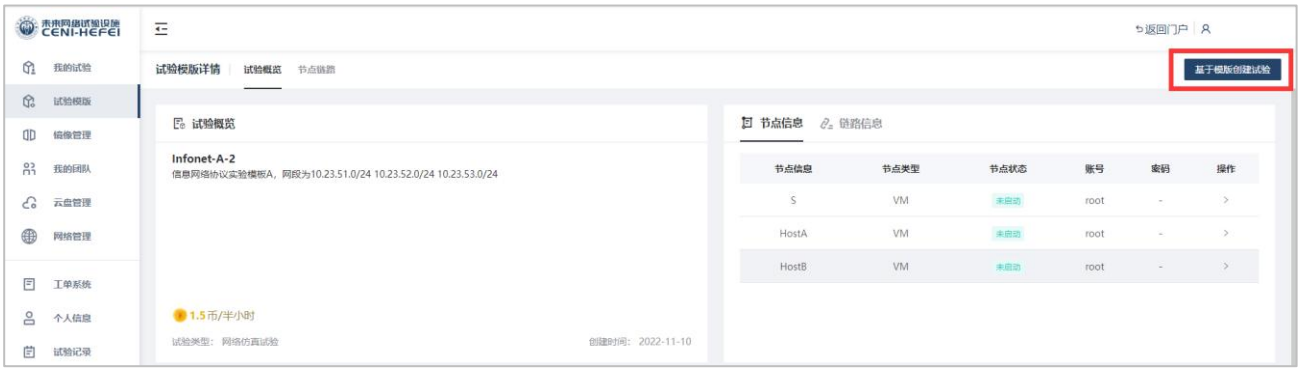
二、 实验创建

由于 ipv4 地址同一网段地址不足够支持所有同学进行实验，现在提供了两套网段，其对应关系如下

主机名	HostA/B	S	S HostA/B
网段 1	10.23.51.0/24	10.23.52.0/24	10.23.53.0/24
网段 2	10.23.54.0/24	10.23.55.0/24	10.23.56.0/24

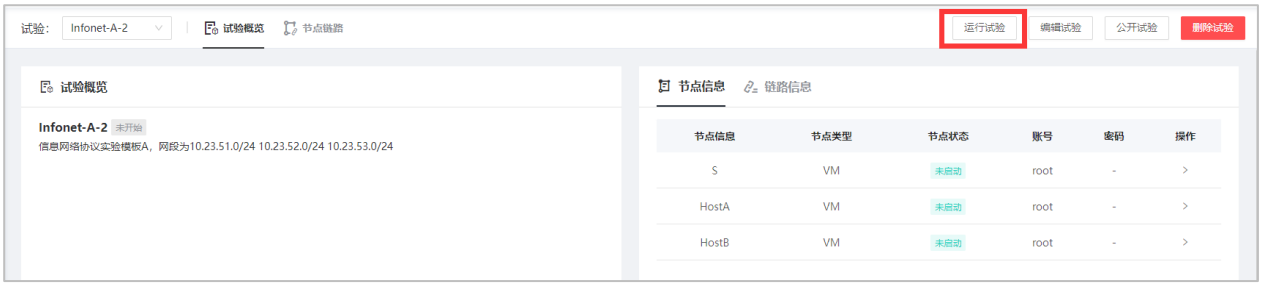
请**学号最后一位数字**为**奇数**的同学选择第一个网段，**偶数**的同学选择第二个网段进行实验。

直接使用实验模板创建实验，网段1实验模板为Infonet-A-2，网段2模板为InfonetB-2。

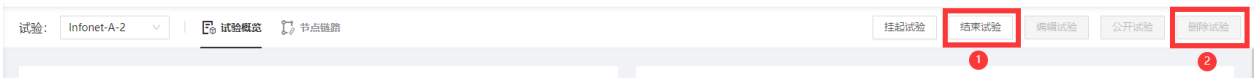


三、 实验运行

点击刚刚新创建的实验，点击运行（此过程可能需要等待一段时间），创建完成之后打开控制台，即可开始实验。请选择以**ustc账号**进行登录，其登录密码为**ustc1958**



注意：四次实验内容是彼此独立的，单次实验完成之后请务必点击**结束实验**按钮释放资源。下次实验直接启动就好，不需要重复创建实验



四、 结果提交

实验报告统一提交至邮箱: ustc_infonet@163.com ， 标题和文件命名规则为：**姓名-学号-信网第x次实验**。前三次实验请提交PDF文件，第四次将报告和代码打包为一个压缩包。

实验二：IPv6 基本操作

一、 实验目标

1. 学习使用 tcpdump 抓取 IPv6 路由器公告报文并分析报文信息。
2. 了解 TCP 三次握手的工作过程。
3. 掌握 IPv6 协议的隧道通信。

二、 实验原理

1. TCP 三次握手

所谓三次握手 (Three-way Handshake)，是指建立一个 TCP 连接时，需要客户端和服务器总共发送 3 个包。三次握手的目的是连接服务器指定端口，建立 TCP 连接，并同步连接双方的序列号和确认号，交换 TCP 窗口大小信息。在 socket 编程中，客户端执行 connect() 时，将触发三次握手。

a) 第一次握手 (SYN=1, seq=x): 客户端发送一个 TCP 的 SYN 标志位置 1 的包，指明客户端打算连接的服务器的端口，以及初始序号 X, 保存在包头的序列号 (Sequence Number) 字段里。发送完毕后，客户端进入 SYN_SEND 状态。

b) 第二次握手 (SYN=1, ACK=1, seq=y, ACKnum=x+1): 服务器发回确认包 (ACK) 应答。即 SYN 标志位和 ACK 标志位均为 1。服务器端选择自己 ISN 序列号，放到 Seq 域里，同时将确认序号(Acknowledgement Number) 设置为客户的 ISN 加 1，即 X+1。发送完毕后，服务器端进入 SYN_RCVD 状态。

c) 第三次握手 (ACK=1，ACKnum=y+1): 客户端再次发送确认包 (ACK)，SYN 标志位 为 0，ACK 标志位为 1，并且把服务器发来 ACK 的序号字段 +1，放在确定字段中发送给对方，并且在数据段放写 ISN 的 +1。发送完毕后，客户端进入 ESTABLISHED 状态，当服务器端接收到这个包时，也进入 ESTABLISHED 状态，TCP 握手结束。

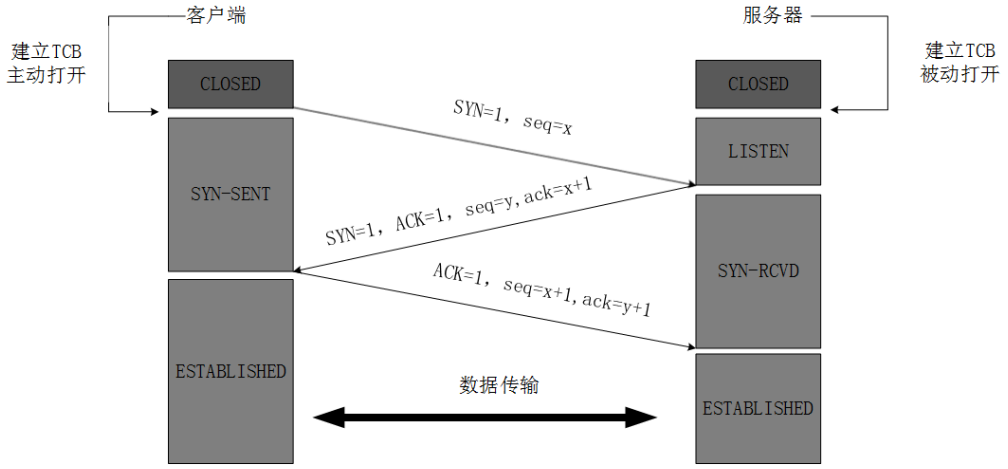


图 1: TCP 三次握手示意图

2. IPv6 隧道

隧道 (Tunnel) 技术是一种基于 IPv4 隧道来传送 IPv6 数据报文的封装技术。将 IPv6 包作为无结构意义的数据，封装在 IPv4 包中，如此穿越 IPv4 网络进行通信，并且在隧道 的两端可以分别对数据报文进行封装和解封装。隧道是一个虚拟的点对点的连接。隧道技术在定义上就是指包括数据封装、传输和解封装在内的全过程。下图展示了 IPv6 over IPv4 协议体系结构。隧道技术的实现需要有一个起点和一个终点。根据隧道终点的 IPv4 地址的获取方式不同可以将 IPv6 over IPv4 隧道分为手动隧道和自动隧道。

a) 手工配置隧道 (Confifigured Tunneling)

对每个 IPv6 分组，都事先手工配置它所对应的隧道的端点，主要是用于隧道封装所需的 IPv4 地址。

b) 自动配置隧道 (Automatic Tunneling)

分组中所包含的 IPv6 地址和/或路由的下一跳决定隧道的端点，主要是指用于隧道封装所需的 IPv4 地址。

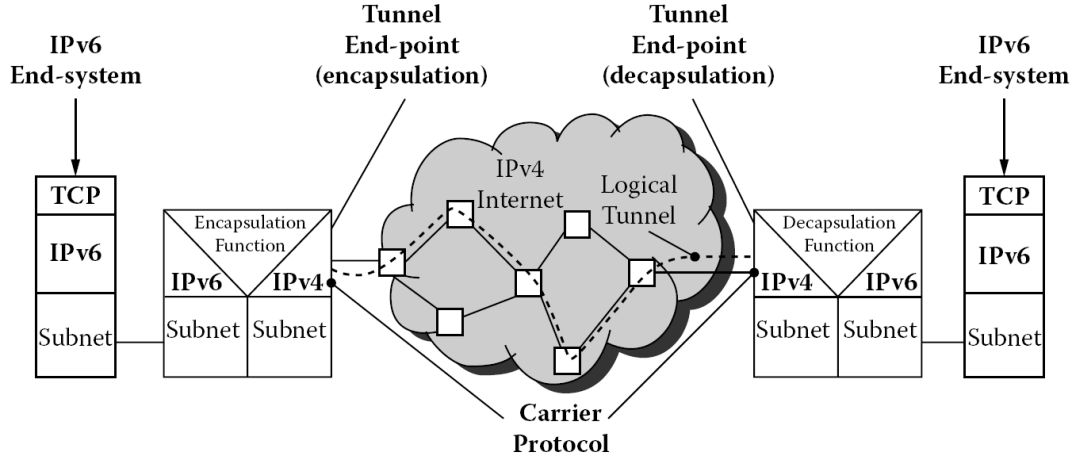


图 2: IPv6 over IPv4 or IPv6-in-IPv4 Tunneling

三、 实验内容

注意！若遇到ens5 ping不通的情况请先尝试删除实验再重新创建。

1. **基本操作**

1）查看并**记录** HostA 和 S 的 IPv6(ens5 scope:link) 地址，命令 ifconfig ens5。

2）IPv6 连接：

HostA 的终端 1 中执行 sudo tcpdump -vxn host HostA 的 IPv6(ens5 scope:link) 地址 and S 的 IPv6(ens5 scope:link）地址 -i ens5。

HostA 的终端 2 中执行 ping6 -c 1 S 的 IPv6(ens5 scope:link）地址%ens5。

【实验要求】：此步骤需要记录终端 1 中抓到的 2 个报文数据，表明哪个是请求报文，哪个是回复报文。根据 IPv6 协议报文格式分析上述 tcpdump 抓包结果，要求画出 IPv6 以及 ICMPv6 的基本报头结构并将各个字段分别填入其中 (例如 IP 协议版本、源地址和目的地址、源端口和目的端口、报文含义等)。对这个报文的含义加以解释。

3）路由器公告报文

路由器公告报文的目的地址为 IPv6 组播地址中的“全节点地址”，它的地址是 FF02::1，可用 tcpdump 侦听路由器公告报文。HostA 中另开一个终端 3 用于侦听路由器公告报文，命令为：sudo tcpdump －vxn host ff02::1 -i ens5）。

【实验要求】：记录 HostA 的终端 3 中 tcpdump 抓包得到的数据。由于路由器公告报文的发送有一定地周期，因此这里可能需要等待较长时间，可以把终端 3 最小化继续进行其他实验，等有结果后记录抓包得到的数据。如仍未顺利抓到此包，也可以参考附录中的图 4 回答下述问题。根据 tcpdump 抓取到的报文数据说明路由器通告报文通告了哪些信息并简单解释网络中的其它主机将会如何使用这些信息？

4）地址解析

地址解析的目的是通过对端的 IP 获取对端的 MAC 地址。由于地址解析过程会在数据发送前自动进行，因此需要先用 tcpdump 侦听，再 ping 对端，即可观察到 NS 和 NA 报文。

HostA 的终端 1 执行命令 sudo tcpdump -vxn host HostA 的 IPv6(ens5 scope:link) 地址 -i ens5

HostA 的终端 2 执行命令 ping6 -c 1 HostB 的 IPv6(ens5 scope:link）地址%ens5。

【实验要求】：记录 HostA 的终端 1 中观察到邻居请求 (NS) 和邻居通告 (NA) 报文。根据抓取到的报文数据说明邻居请求及邻居公告报文通告了哪些信息，这些信息有什么作用？

5）TCP 三次握手

netcat 可以在主机间建立 TCP 连接，建立连接时，可以用 tcpdump 对 报文抓包，观察到 TCP 的三次握手过程。

首先在 S 的终端 1 中执行 nc -l 1958 侦听 1958 端口。

之后在 HostA 的终端 1 执行 sudo tcpdump -vxn host HostA 的 IPv4(ens5) 地址 and S 的 IPv4(ens5) 地址 -i ens5

在 HostA 的终端 2 执行 nc S 的 IPv4(ens5)地址 1958。

【实验要求】：完整记录 HostA 的终端 1 中观察到的前三个报文，即 TCP 握手报文。标注出每个报文的类型（SYN、SYN/ACK、ACK）。简要说明 TCP 协议采用三次握手的原因。说明实验中为何无法抓到 RST 包？请问编写应用程序时我们是否需要处理这些报文，为什么？

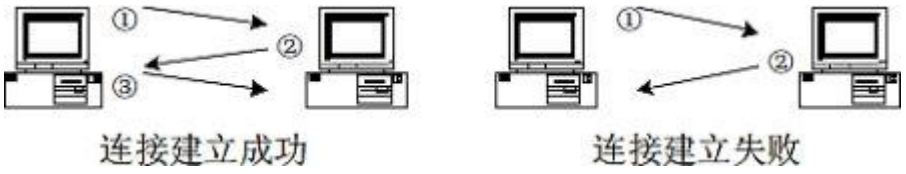


图 3: TCP 三次握手

2. 隧道

注意 隧道删除命令为 ip tunnel del 隧道名称，若添加隧道命令打错可用此命令删除后重建。

1） 打开两个 Host 虚拟机并各打开一个终端

2） 在 HostA 的终端上执行命令：

sudo ip tunnel add sit1 mode sit remote HostB 的 IPv4 地址 local HostA 的 IPv4 地址 dev ens5（IPv4 地址可以由命令 ifconfig ens5 获得）

sudo ip link set sit1 up

ip link show up【记录结果，此时可以看到名字为 sit1 的设备】

sudo ip addr add 3ffe:3216:2101:2106:1234::A/80 dev sit1

ip tunnel show【记录结果】

3）在 HostB 的终端上执行命令：

sudo ip tunnel add sit1 mode sit remote HostA 的 IPv4 地址 local HostB 的 IPv4 地址 dev ens5（IPv4 地址可以由命令 ifconfig ens5 获得）

sudo ip link set sit1 up

ip link show up【记录结果，此时可以看到名字为 sit1 的设备】

sudo ip addr add 3ffe:3216:2101:2106:1234::B/80 dev sit1

ip tunnel show【记录结果】

4）在 HostA 上打开两个终端。其中一个终端用 tcpdump 侦听报文，另一个终端用于 ping6。

(a). 首先在 HostA 的第 1 个终端中执行命令 sudo tcpdump -vxn -i sit1。

(b). 其次在 HostA 的第 2 个终端中执行命令 ping6 –c 1 3ffe:3216:2101:2106 :1234::B，检查是否可以 ping 通，若不通则需要检查之前的步骤是否正确完成。

(c). 记录 HostA 的第 1 个终端中由 tcpdump 抓取的前两个报文。

(d). 关闭 HostA 的这两个终端并重新打开两个新的终端。

(e). 在 HostA 的第 1 个终端中执行命令 sudo tcpdump -vxn –i ens5

(f). 在 HostA 的第 2 个终端中执行命令 ping6 –c 1 3ffe:3216:2101:2106:1234::B。

(g). 记录 HostA 的第 1 个终端中由 tcpdump 抓取的前两个报文（可能要等一会儿）。

【实验要求】：记录需要记录的实验数据。从报文结构上看，通过隧道通信与两个 IPv6 主机直接通信的区别是什么，即上述隧道通信的报文有什么特点？

四、 实验报告

报告要求：电子版报告，内容包括实验题目、实验原理（对实验中用到的所有命令加以解释）、实验结果（实验中所有需要记录的结果，可截图，截图中需要包含命令、结果及虚拟机控制台界面上方的“用户名、实验名和虚拟机名称”）、问题回答、实验收获。

注意 实验报告请及时提交，晚交会记录并扣分。

实验报告截止时间：11 月 19 日 23 时 59 分 59 秒

五、 附录

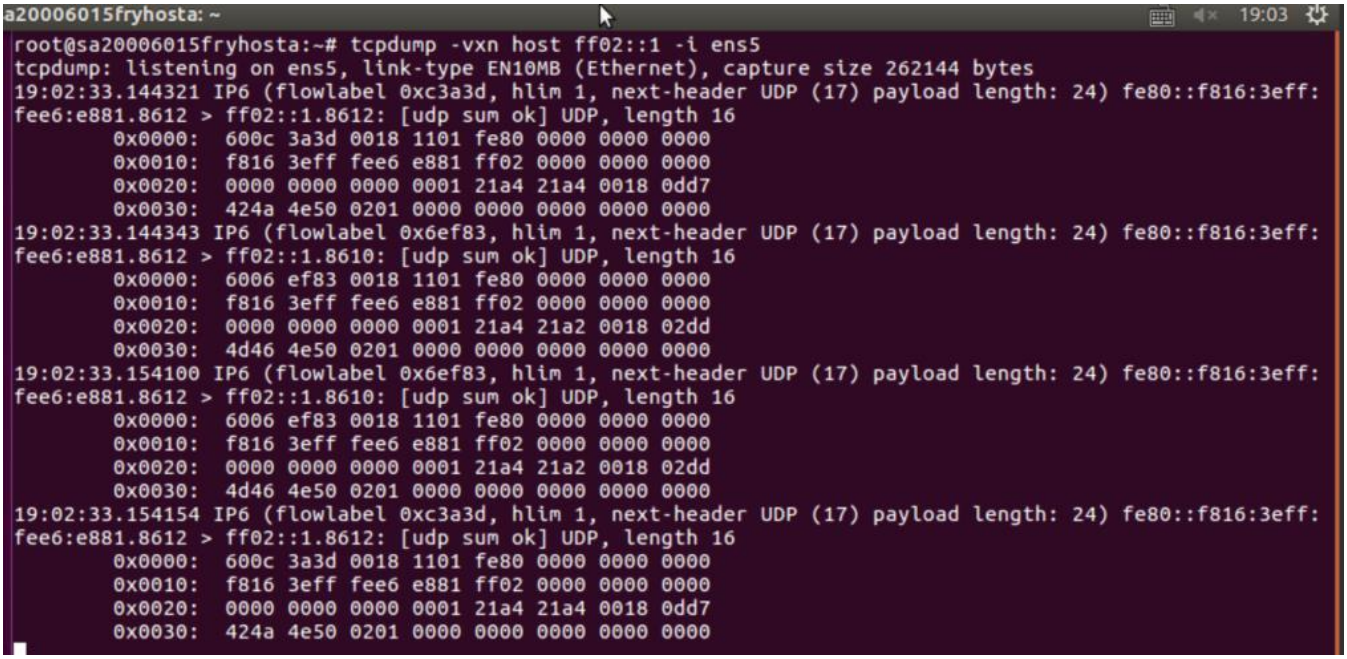


图 4: 路由器公告报文参考图