**西安电子科技大学**

**组网与运维综合实验 课程实验报告**

**实验名称 TCP/IP报文分析**

网络与信息安全 学院 班

成 绩

姓名 学号

同作者

实验日期 年 月 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

# TCP/IP报文分析

## 一、实验目的

1. 掌握H3C设备Ping和Tracert命令的使用。

2. 掌握H3C设备的系统调试功能。

3. 掌握ICMP报文在Ping操作下的工作原理。

4. 掌握H3C设备TCP参数的设置。

5. 在H3C设备上进行TCP报文分析。

6. 在H3C设备上进行UDP报文分析。

7. 进一步熟悉debug命令的使用。

## 二、实验要求

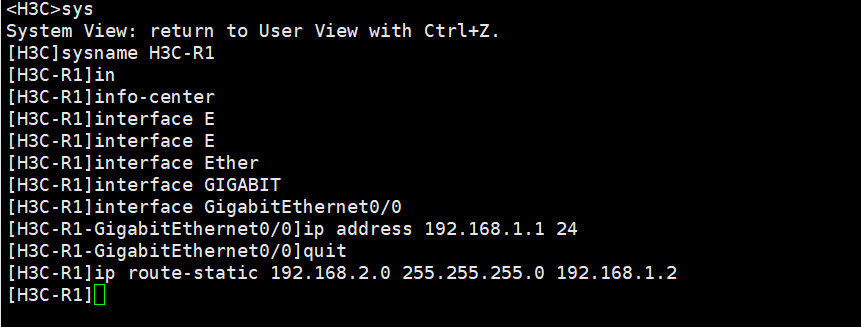
1. 3台具有24个以太网接口的交换机；

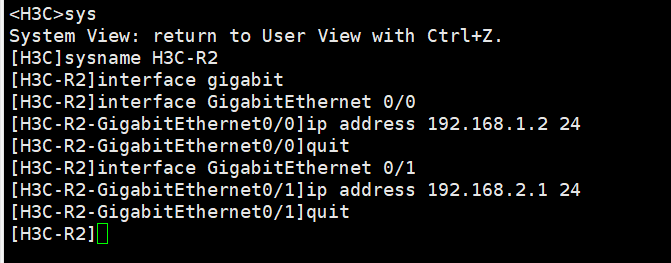
2. 2台装有Windows系列操作系统的PC（台式机或笔记本）；

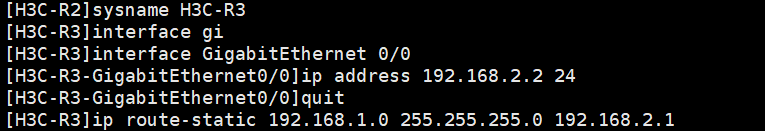
3. 2条双绞跳线（交叉线）；

## 三、实验步骤

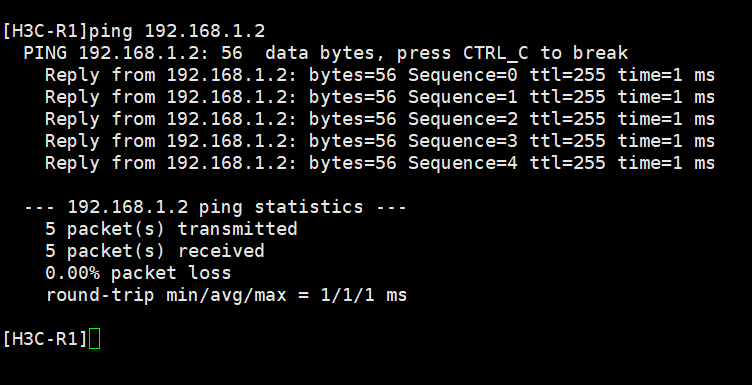
1. 按实验1要求配置H3C路由器基本参数



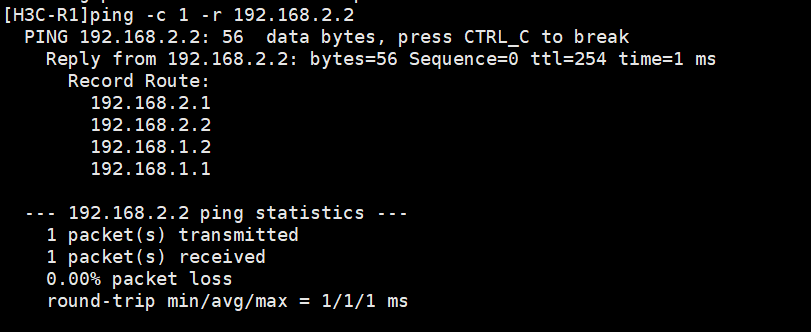




2. 掌握Ping调试工具



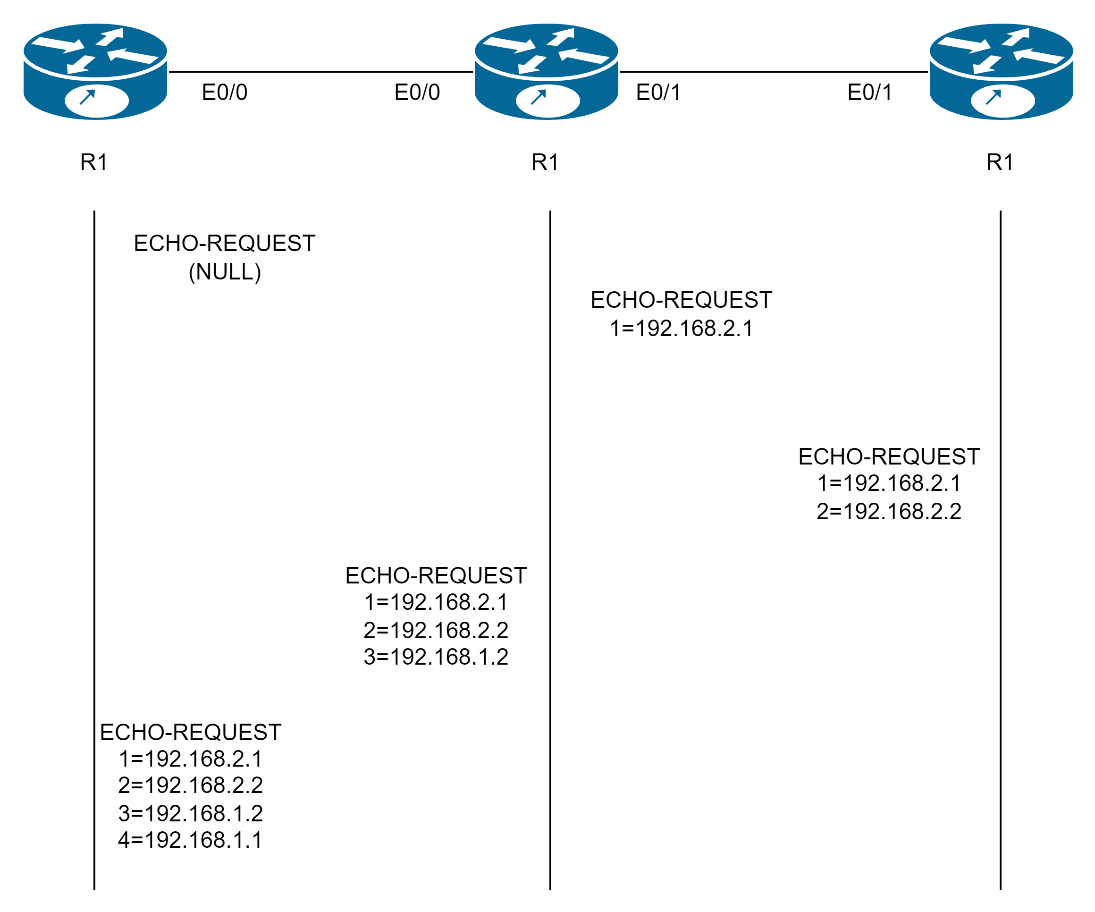
H3C-R1上ping测试H3C-R2的IP地址192.168.1.2是否可达，成功ping通，可达。



ping -r 记录计数跃点的路由，在“记录路由”字段中记录传出和返回数据包的路由， 探测经过的路由个数 ，采用倒序显示。

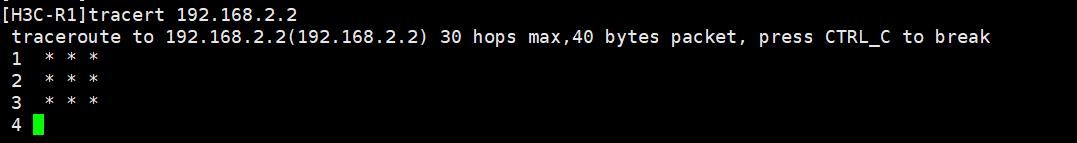
ping命令采用 ICMP 协议，它可以通过向目标设备发送 ICMP 回声请求数据包并等待回复来测试网络可达性。

R1发送的ICMP请求报文中，含有空的RR选项，当报文从某一接口转发到目的端时，该端口所在设备会将该接口的IP地址添加到RR选项中，目的端受到请求报文后，发送响应报文，拷贝请求报文的RR选项，并将自己出接口的IP添加到其中，接下来，所经过的路由器设备出接口的IP都会记录到RR中，到达源端时，将自己入接口的IP地址写入。



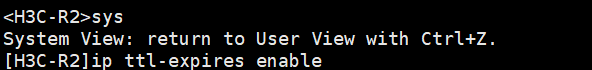
3. 掌握Tracert调试工具

Tracert超时

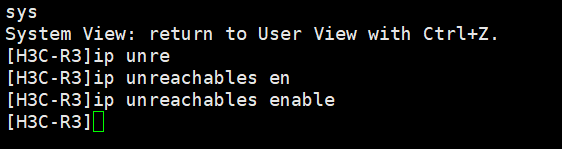


**解决方案：**

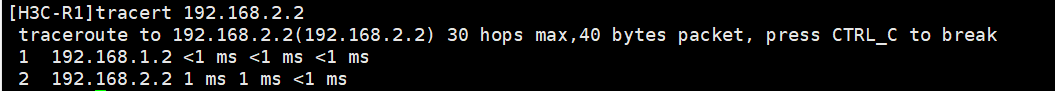
R2开启ICMP超时报文发送功能



R3开启目的端不可达报文发送功能



Tracert正常



Tracert命令可以查看报文从源端到目的端所经过的路径。

图形用户界面, 应用程序

描述已自动生成

利用超时和端口不可达的ICMP错误消息。

R1向R3发送一个IP数据报文，TTL值为1，报文的UDP端口是目的端应用程序不使用的端口号；

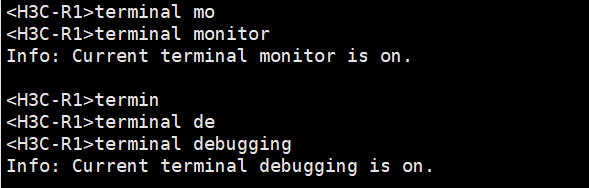
第一跳R2回应一个TTL超时的ICMP错误信息，其中含有第一跳的IP地址，源端得到第一个设备地址。

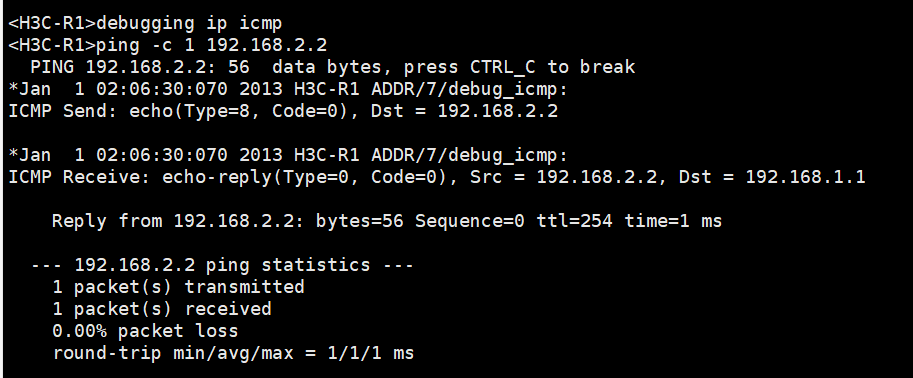
源端重新向目的端发送一个IP数据报文，TTL值为2.

直到报文到达目的端，由于目的端没有应用程序使用该UDP端口，所以返回端口不可达的ICMP错误消息，携带目的端的IP地址，当源端受到不可达的ICMP错误消息后，则知道报文到达了目的端。

4. 配置系统调试功能——Ping

H3C-R1上打开ICMP报文信息的开关来观察ICMP报文输出

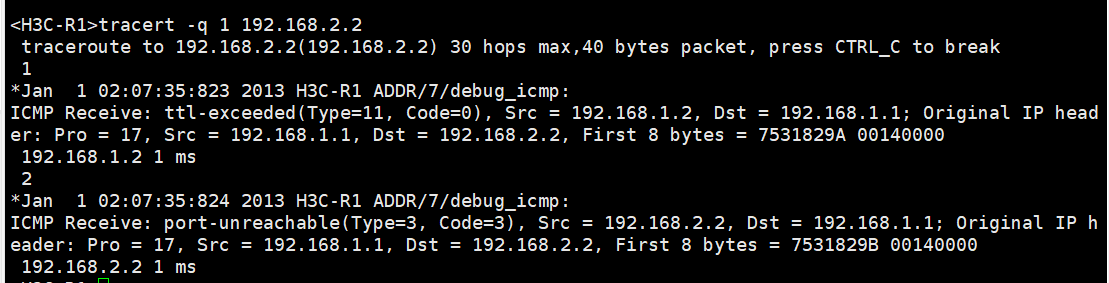
在H3C-R1上使用Ping命令向H3C-R3的IP地址192.168.2.2发送一个Ping报文



上述报文Type=8，code=0，是一个回显请求。

5. 配置系统调试功能——tracert

从tracert命令的debug调试信息可以看到H3C-R1接收的ICMP信息



从Tracert命令的debug 调试信息中可以看到H3C-R1接收的ICMP信息。H3C-R1发送一个目的地址为192.168.2.2TTL值为1的IP数据报文。当这个IP数据报文到达H3C-R2时，H3C-R2发现报文的目的地不是本地且报文的TTL字段是1，则发送“TTL超时”ICMP差错报文ttl-exceeded(Type=11，Code=0)。

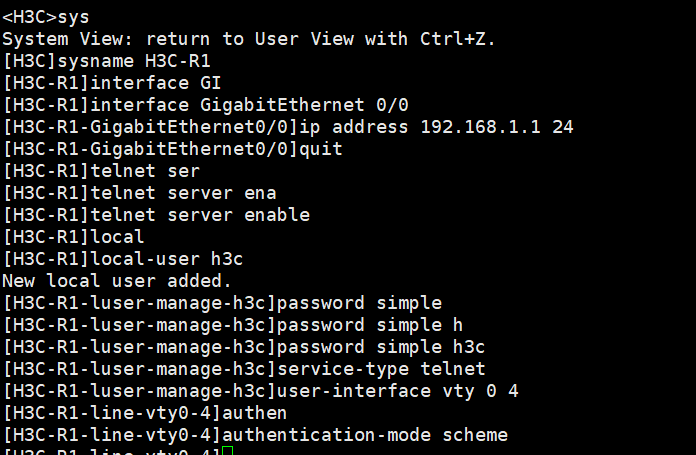
H3C-R1根据ICMP差错报文tl-exceeded(Type=11，Code-0)获得网关地址的下一跳为192.168.1.2。

H3C-R1会重新向H3C-R3发送一个IP 数据报文，其目的地址为192.168.2.2，TTL值为2，H3C-R3 收到一个UDP 的本机报文，根据报文的目的端口，无法找到对应的进程，则向报文源端发送一个ICMP不可达报文port-unreachable(Type=3，Code=3)。

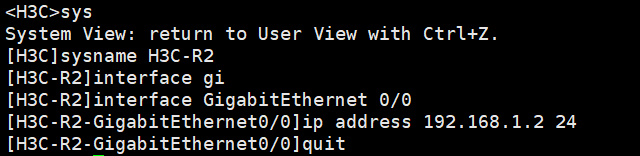
H3C-R1根据ICMP不可达报文port-unreachable(Type=3，Code-3)获知到达了目的设备H3C-R3。

6. 按实验2配置H3C路由器基本参数

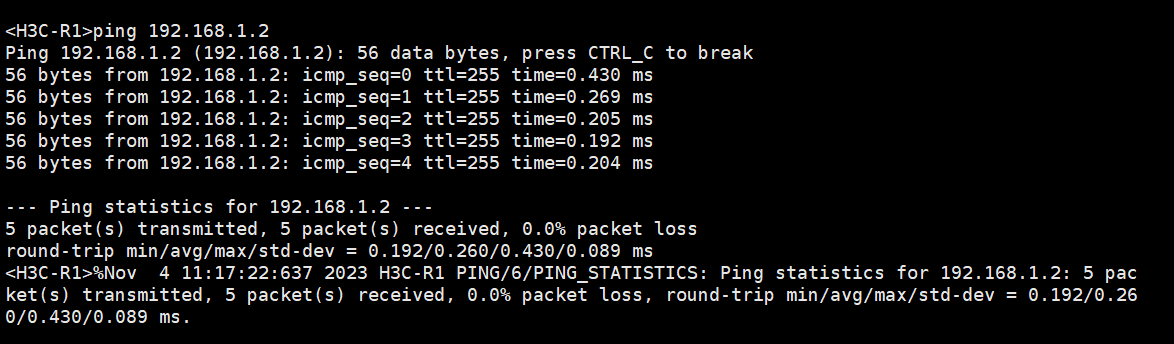
R1配置：



R2配置：

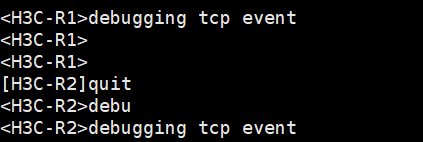


R1 ping R2，正常连通



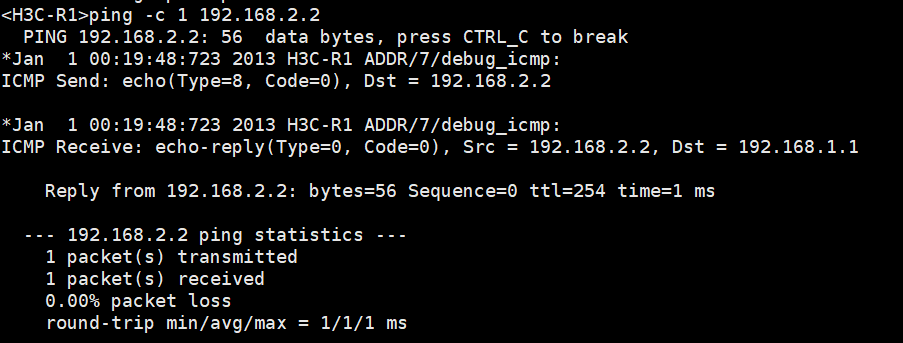
7. 测试TCP信息

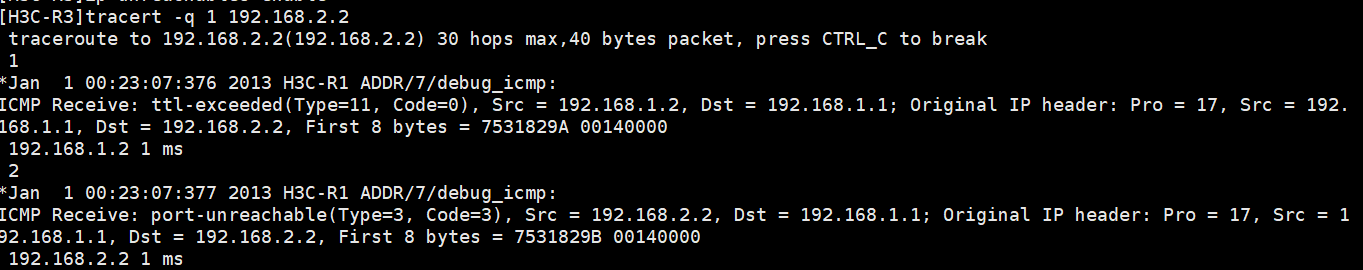
开启debugging：



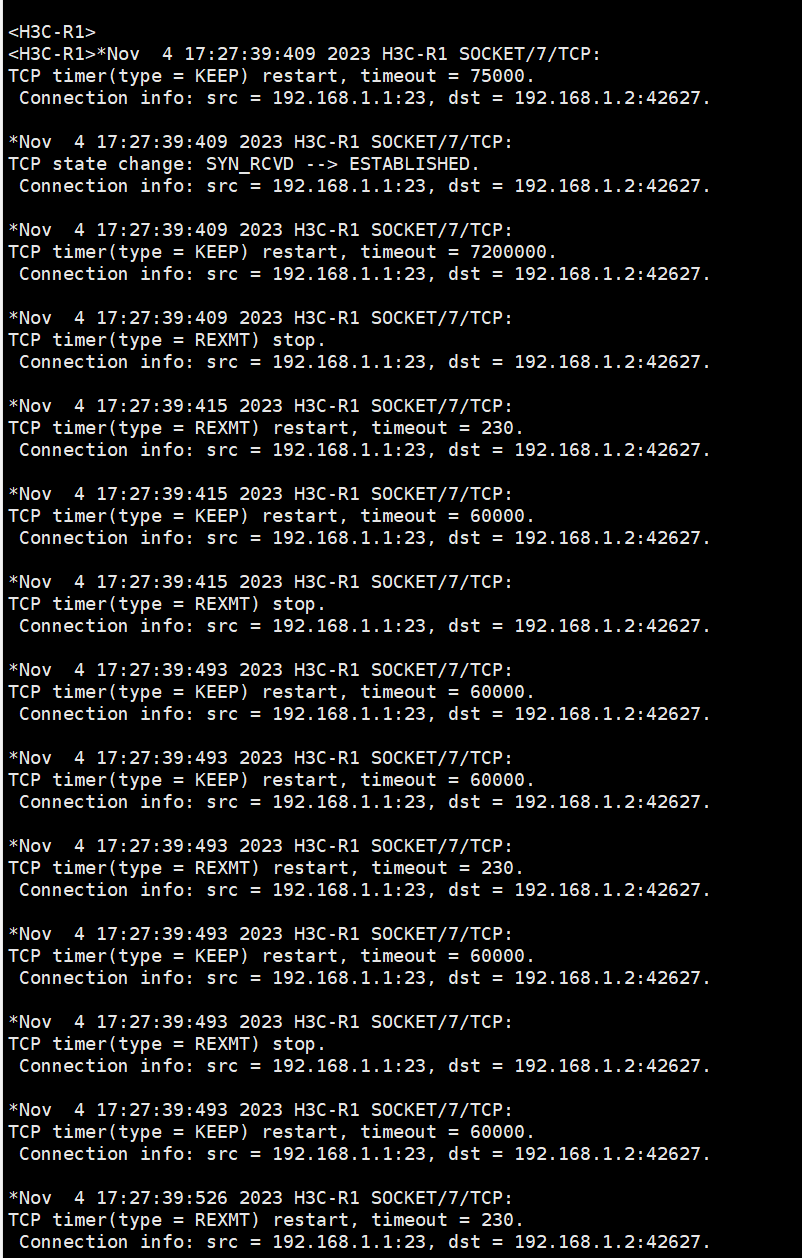
Telnet连接R1

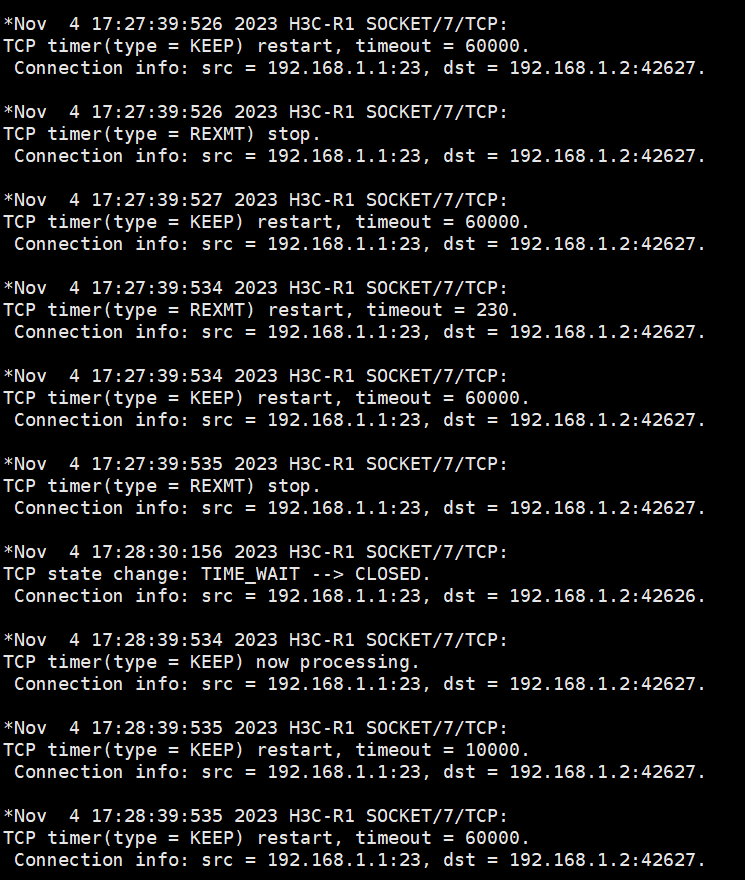




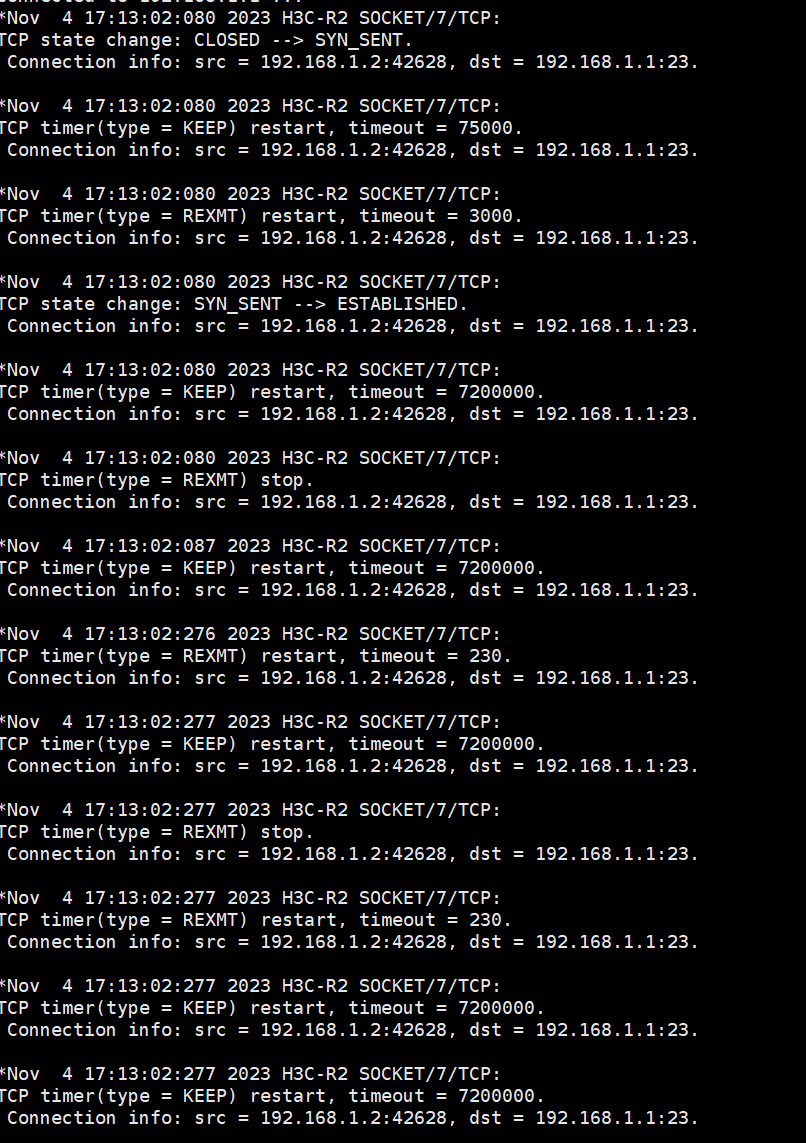


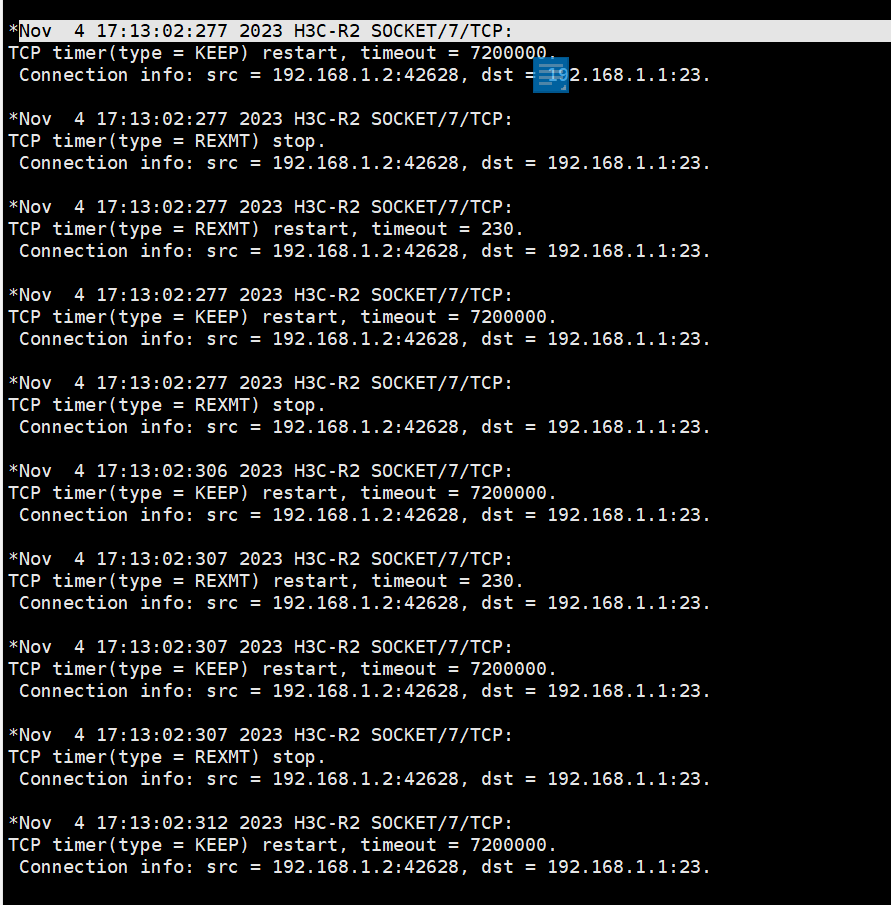
R1建立报文





R2建立报文：





三次握手的过程如下。首先，H3C-R2发送一个SYN 报文段，指明H3C-R2打算连接H3CR1的端口，以及初始顺序号(seq=a)

H3C-R1发回包含H3C-R2的初始顺序号的SYN报文段(seq=b)作为应答。同时，将确认号设置为H3C-R2的顺序号加1，以对H3C-R2的SYN报文段进行确认(ACK为a+1)

H3C-R2将确认号设置为H3C-R1的顺序号加1，以对H3CR1的SYN报文段进行确认(ACK为b+1)，该报文通知目的主机双方已完成连接建立。

state=Syn\_Sent，表示当前TCP状态处于Syn Sent。

flag=SYN，是H3C-R2向H3C-R1发出的TCPSYN报文。src=192.168.1.2:1041dst=192.168.1.1:23，显示了发送报文的源地址、目的地址、源端口和目的端口。发送到H3C-R1的目的端口是23，说明这是进行telnet访问连接seq=2523560003，seq顺序号为2523560003。这是H3C-R1的初始顺序号

在H3C-R1上收到此TCPSYN报文后，向H3C-R2发送ACKSYN报文

state=Syn\_Rcvd，表示当前TCP状态处于Syn Rcvd。

flag=ACKSYN，是H3C-R1向H3C-R2发出的TCPACKSYN报文。seq=2530540041，seq顺序号为2530540041，这是H3C-2的初始顺序号。ack=2523560004，ACK序号为为H3C-R1的seq顺序号加1，即2523560004。在H3C-R1上收到H3C-R2的此TCPACKSYN报文后，向H3C-R1发送ACK 报文

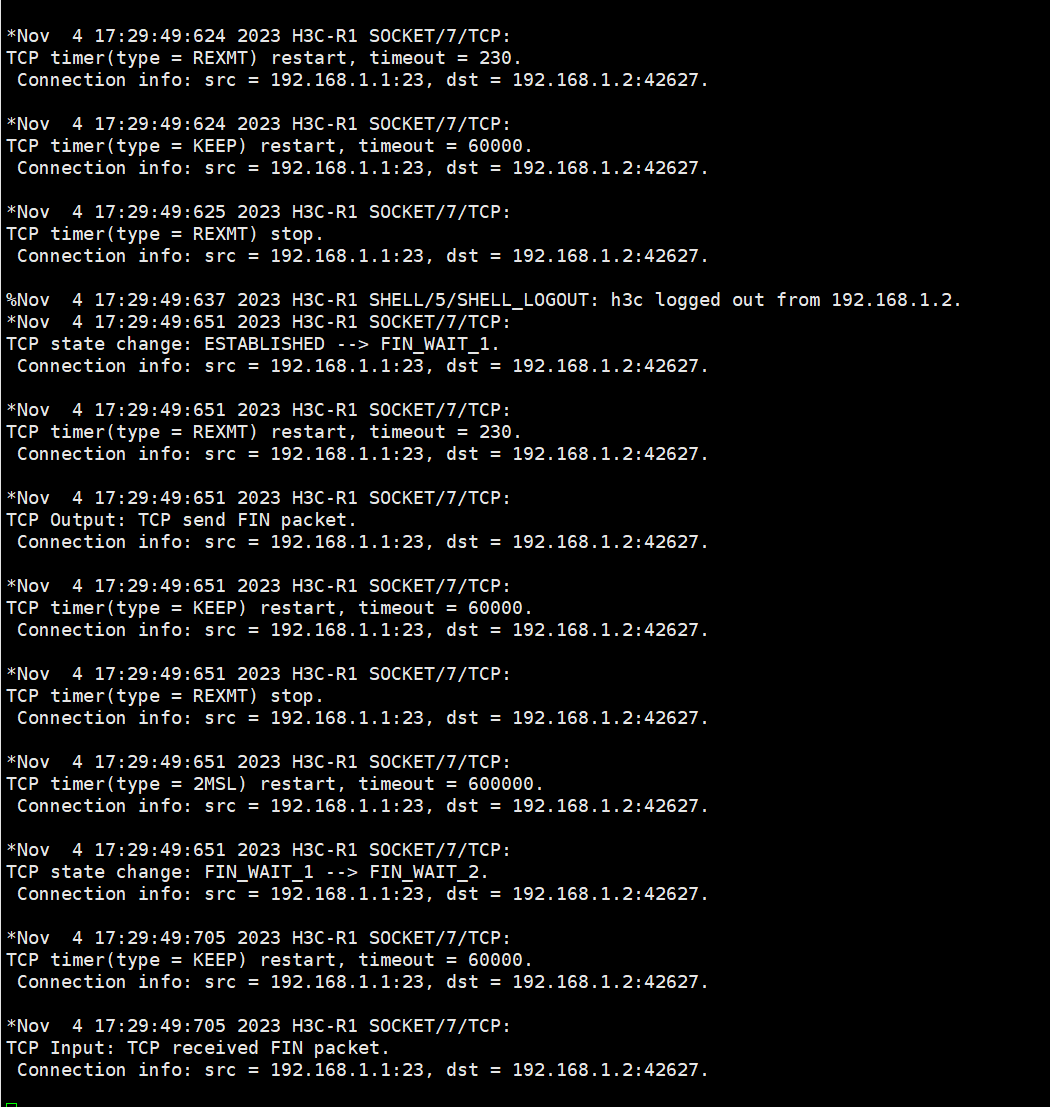
state=Established，表示当前TCP状态处于Established。

flag=ACK，是H3C-R2向H3C-R1发出的TCPACK报文。

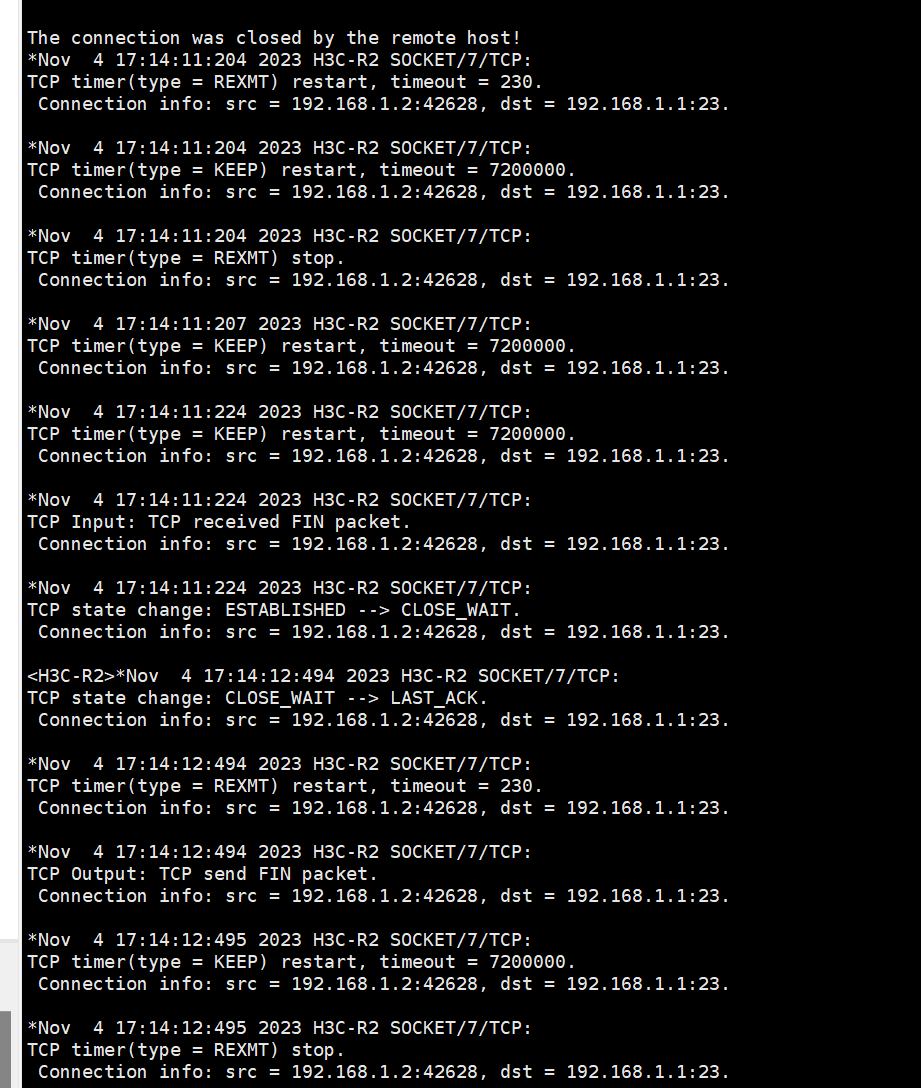
seq=2523560004，seq 顺序号为2523560004。

ack=2530540042，ACK序号为H3C-R2的seq 顺序号加1，即2530540042。

R1关闭报文：



R2关闭报文：



收到本方应用进程的关闭命令后，TCP在发送完尚未处理的报文段后，发FIN=1的报文段给对方，且TCP不再受理本方应用进程的数据发送。在FIN 以前发送的数据字节，包括FIN，都需要对方确认，否则要重传。注意FIN也占一个顺序号。一旦收到对方对FIN的确认以及对方的FIN报文段，本方TCP就对该FIN 进行确认，在等待一段时间后关闭连接。等待是为了防止本方的确认报文丢失，避免对方的重传报文干扰新的连接。

state=Fin\_Wait1，表示当前TCP 状态处于Fin\_Waitl。

flag=ACKFIN，是H3C-R1向H3C-R2发出的TCPACKFIN报文。

seq=2530540538，顺序号为2530540538在

H3C-R2上收到H3C-R1发来的TCPACKFIN报文后向H3C-R1发送TCPACK报文

state=Close\_Wait，表示当前TCP状态处于Close\_Wait。

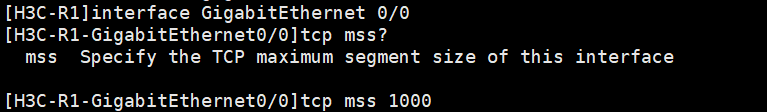
flag=ACK，是H3C-R2向H3C-R1发出的TCPACK 报文。

seq=2523560052，顺序号为2523560052。ack=2530540539，ACK号为顺序号+1，即2530540539同时，H3CR2也向H3C-R1发出关闭TCP连接报文，并等待H3C-R1的TCP ACK。

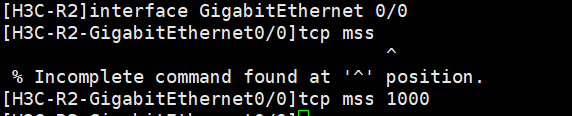
客户端收到最后一个确认ACK 报文段，其TCP实体便释放该连接，并删除连接记录返回到初始状态(CLOSED)。

8.配置TCP属性

在H3C-R1的E0/0接口配置接口的TCP最大报文段长度为1000：



在H3C-R2的E0/0接口配置接口的TCP最大报文段长度为1000：



在H3C-R1上把TCP连接的收发缓冲区大小设置为10KB



9. 查看TCP相关的状态属性

display tcp status命令显示所有TCP连接的状态。可以使用这条命令随时监控设备上的TCP连接。

TCPCB:表示TCP控制块。

Local Add:port:表示本端IP地址及端口号

Foreign Add:port:表示对端IP地址及端口号

State:表示TCP连接的状态。

从输出中，可以看到H3C-R2的1028端口向H3CR1的23端口发起TCP连接，并且TCP连接的状态是Established。

Display tcp statistics命令显示TCP连接的流量统计信息

Received packets:表示接收到TCP报文。

Sent packets:表示发送的TCP 报文。

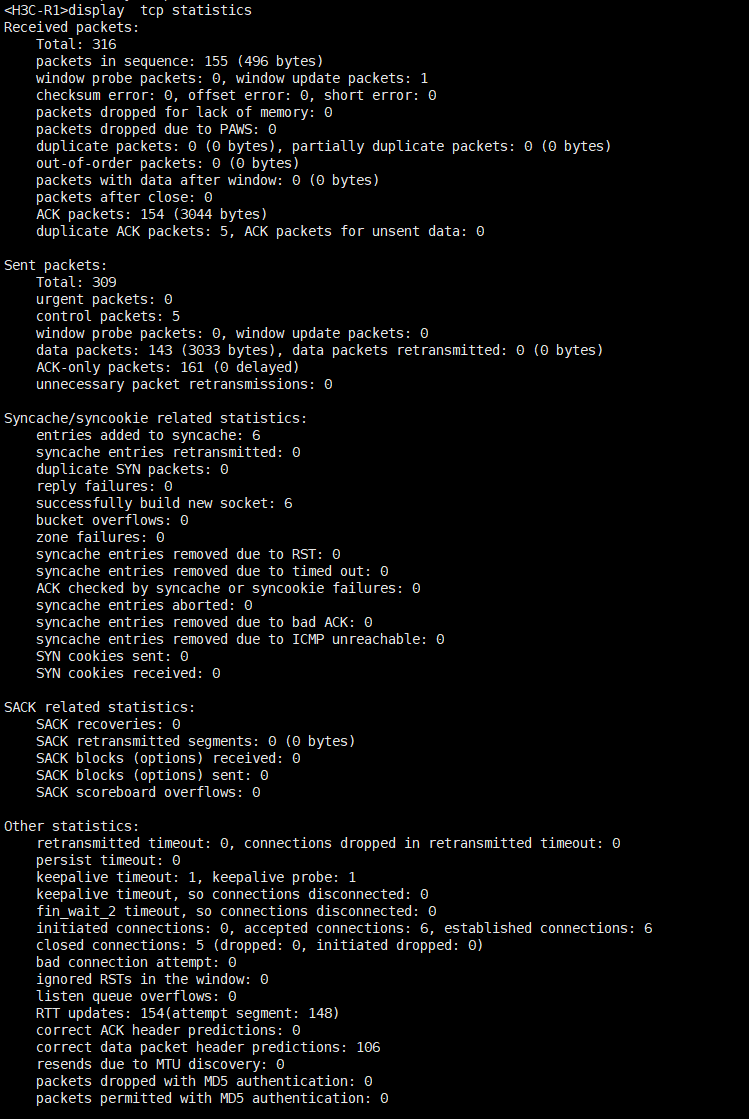
Total:表示报文总数。

Initiated connections:表示发起连接次数

Accepted connections:表示接受连接次数

Established connections:表示已建立连接数

Closed connections:表示已关闭连接数目。





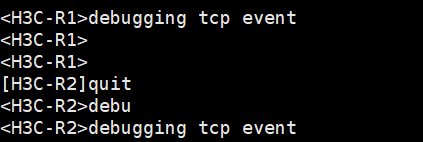
五、实验结果及分析

1. 我们第一个实验对应的图7-6所示的拓扑图和132页下面给的节本参数配置命令之间出现了什么错误？

拓扑图中，R3的E0/1与R2的E0/1口相连，应当配置R3的E0/1口，但实际下面参数配置的是E0/0口。两者不对应。

2. 整个实验过程中遇到什么问题（有截图最好），如何解决的？通过该实验有何收获？

报文debugging不显示，需要手动开启。



这次实验更系统地学习了解TCP三次握手建立连接的全过程，明白了TCP报文格式、标志位等内容含义，以及建立的三次握手菜单解析。TCP三次握手过程中，传送的包里不包含数据，三次握手完毕后，客户端与服务器才正式开始传送数据。理想状态下，TCP连接一旦建立，在通信双方中的任何一方主动关闭连接之前，TCP 连接都将被一直保持下去。另外，与建立连接的“三次握手”类似，断开一个TCP连接则需要“四次握手”四次挥手过程。