**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 2118021 班

成 绩

姓名 夏雨轩 学号 21009201006

同作者 无

实验日期 2023 年 11 月 23 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；

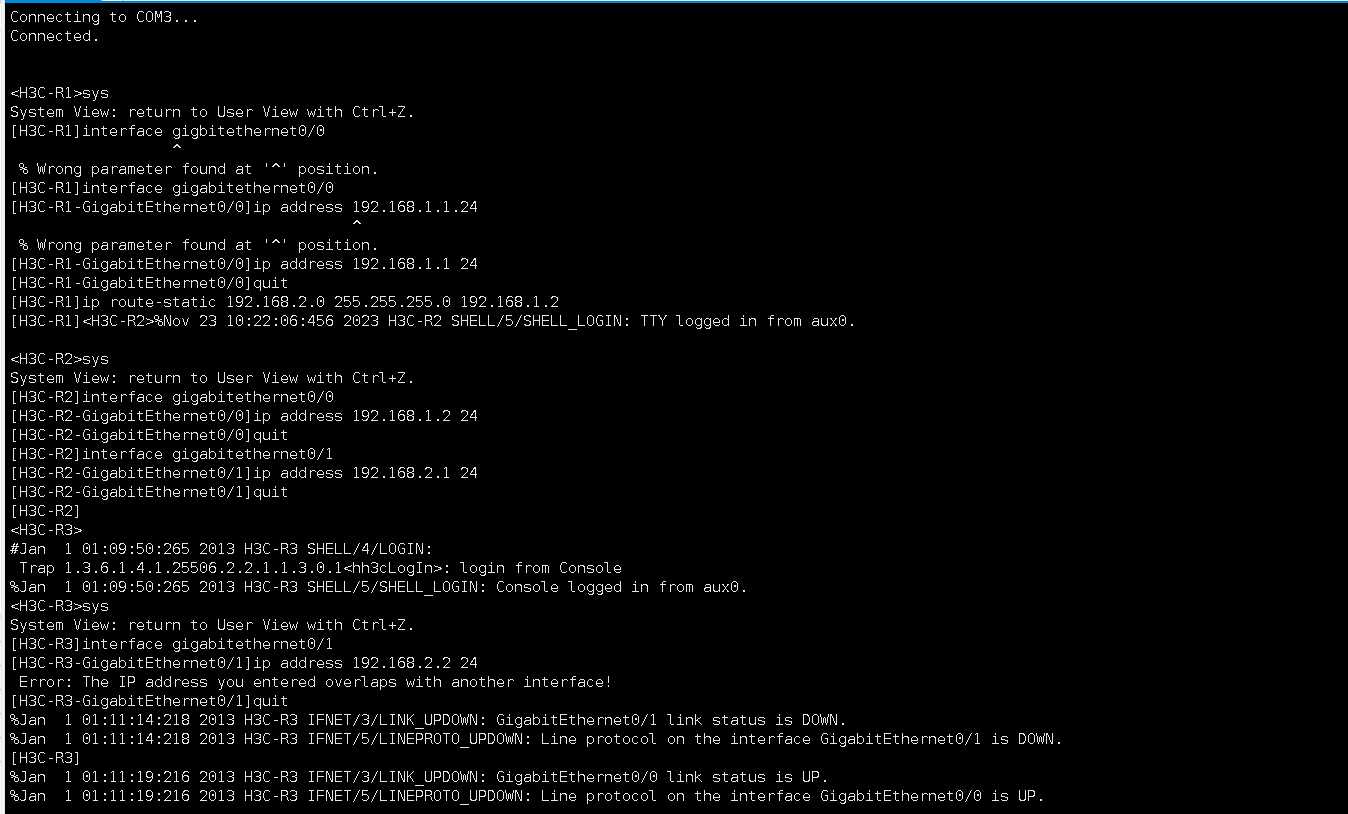
2. 2台装有Windows系列操作系统的PC（台式机或笔记本）；

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

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）



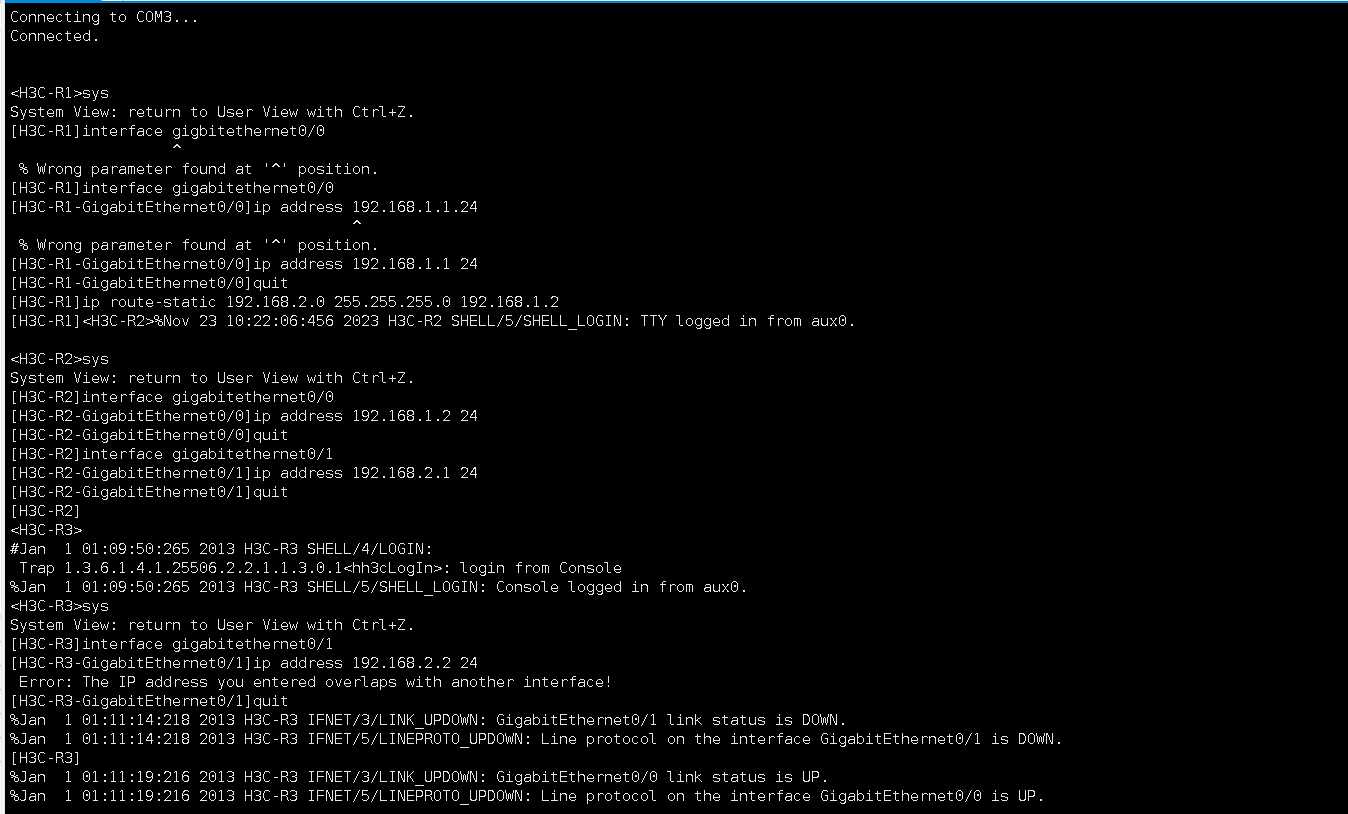
H3C-R1配置:

interface gigabitEthernet0/0--这行命令指定了配置的接口为GigabitEthernet0/0。在路由器或交换机上，这通常是指定某个物理接口或虚拟接口，以便对其进行配置。

ip address 192.168.1.1 24--这行命令设置了接口的IP地址为192.168.1.1，子网掩码为255.255.255.0（/24）。这是为了将IP地址分配给该接口，使其属于192.168.1.0/24网络。

quit

ip route-static 192.168.2.0 255.255.255.0 192.168.1.2--这行命令配置了一个静态路由。要访问目标网络192.168.2.0/24，下一跳（即路由的下一跳）是192.168.1.2。这表示所有发送到192.168.2.0/24的流量都将被发送到192.168.1.2这个地址。



H3C-R2配置:

interface gigabitEthernet0/0

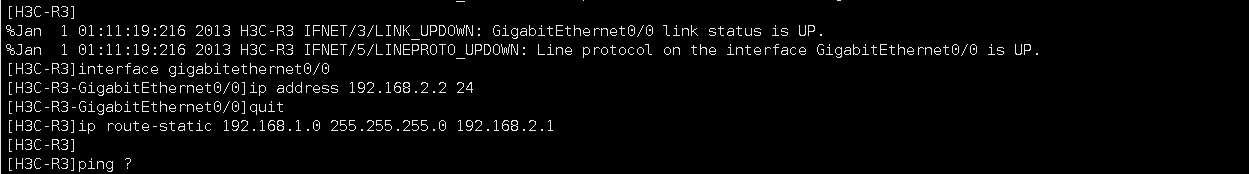
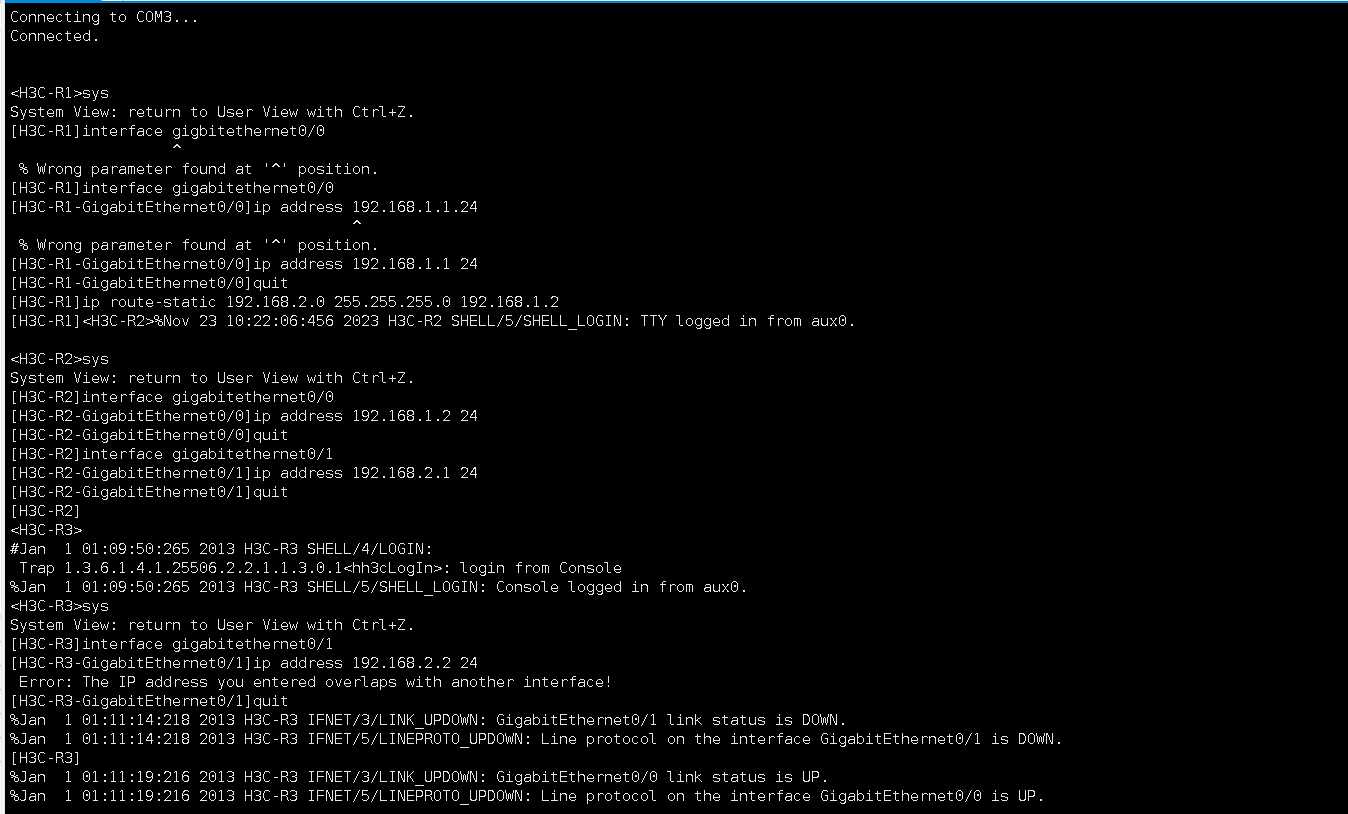
ip address 192.168.1.2 24--配置了 GigabitEthernet0/0 接口，设置了IP地址为192.168.1.2，子网掩码为255.255.255.0（/24）

Quit--退出了接口配置模式，回到全局配置模式

interface gigabitEthernet0/1

ip address 192.168.2.124--配置了 GigabitEthernet0/1 接口，设置了IP地址为192.168.2.124，未指定子网掩码。可能会默认使用 /24 的子网掩码

quit



H3C-R3配置:

interface gigabitEthernet0/0

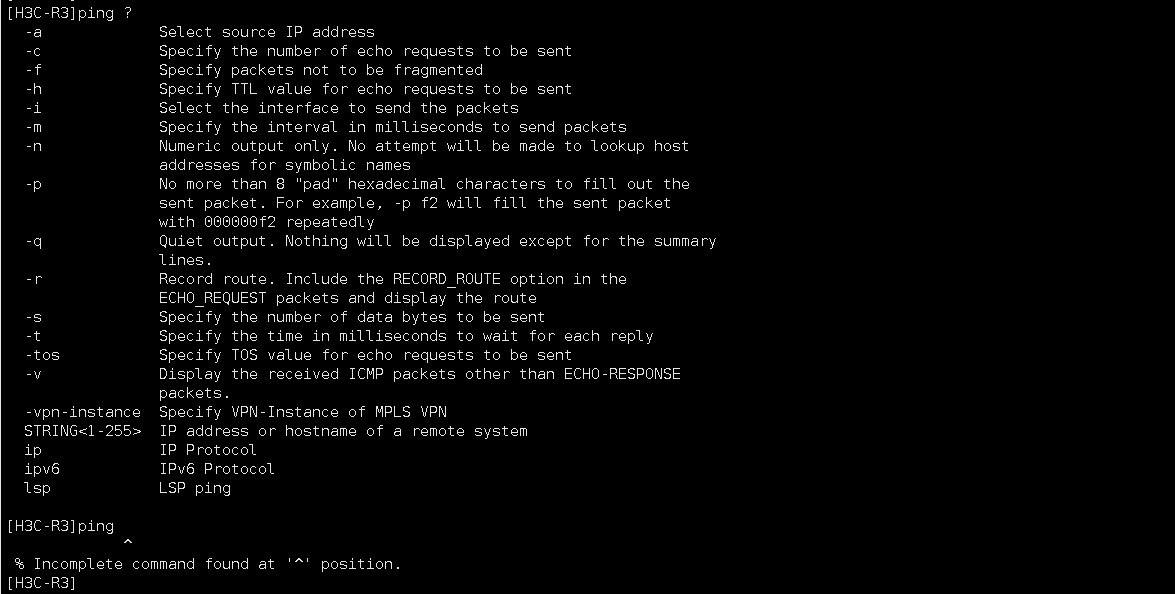
ip address 192.168.2.2 24--设置了接口 GigabitEthernet0/0 的IP地址为192.168.2.2，子网掩码为255.255.255.0（/24）。这将把该接口分配到192.168.2.0/24网络中

Quit--退出了接口配置模式，回到全局配置模式

ip route-static 192.168.1.0 255.255.255.0 192.168.2.1--配置了一个静态路由。它告诉路由器，要访问目标网络192.168.1.0/24，下一跳是192.168.2.1。这表示所有发送到192.168.1.0/24的流量都将被发送到192.168.2.1这个地址。

2. 掌握Ping调试工具

（请截取你从H3C-R1上ping测试H3C-R2的IP地址192.168.1.2是否可达的图片，并参考图7-7自己绘图并配简单文字分析ping -r的原理。）



Ping ？--获取帮助信息

- ip: 支持IPv4协议。如果不指定该参数，也表示支持IPv4协议。

-a source-ip: 指定ICMP回显请求(ECHO-REQUEST)报文的源IP地址。该地址必须是设备上已配置的IP地址。如果不指定该参数，ICMP回显请求报文的源IP地址将是该报文出接口的主IP地址。

-c count: 指定ICMP回显请求报文的发送次数，取值范围为1~4294967295，默认值为5。

-f: 将长度大于接口MTU的报文直接丢弃，即不允许对发送的ICMP回显请求报文进行分片。

-h ttl: 指定ICMP回显请求报文中的TTL值，取值范围为1~255，默认值为255。

-i interface-type inferface-number: 指定发送ICMP回显请求报文的接口的类型和编号。如果不指定该参数，将根据目的IP查找路由表或者转发表来确定发送ICMP回显请求报文的接口。

-n: 对host参数不进行域名解析。如果不指定该参数，系统将对host参数表示的是目的端的主机名进行域名解析。

-q: 只显示统计信息。如果不指定该参数，系统将显示包括统计信息在内的全部信息。

-J: 记录路由信息。如果不指定该参数，系统不记录路由。

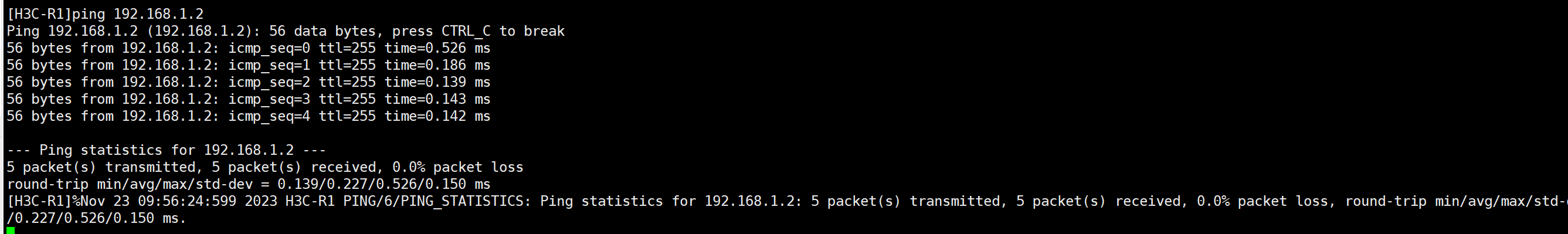
-s packet-size: 指定发送的ICMP回显请求报文的长度(不包括IP和ICMP报文头)，取值范围为20~8100，单位为字节，默认值为56字节。

-t timeout: 指定ICMP回显应答(ECHO-REPLY)报文的超时时间，发送ICMP回显求报文timeout后还没有收到ICMP回显应答报文，源端则认为ICMP回显应答报文超时。值范围为0~65535，单位为毫秒，默认值为2000毫秒。

-tos tos: 指定ICMP回显请求报文中的服务类型 (Type of Service，ToS)域的值，取值范围为0~255，默认值为0。

-v: 显示接收到的非回显应答的ICMP报文。如果不指定该参数，系统不显示非回显应答的ICMP报文。

Host: 目的端的IP地址或主机名，主机名为1-255个字符的字符串。

执行ping命令后，源端向目的端发送ICMP回显请求报文。如果目的端的名称不可识别，则输出提示信息“Error: Ping: Unknown host host-name"。如果在超时时间内收到目的端的ICMP回显响应报文，则输出响应报文的相关信息。如果在超时时间内没有收到目的端的ICMP回显响应报文，则输出“Request time out“提示用户。在使用-i参数指定发送报文的接口时，只能ping直连网段地址。

Ping 192.168.1.2--这将发送 ICMP Echo 请求到192.169.1.2并等待响应。如果目标主机可达，将看到一系列回应，其中包括每个请求的延迟（Round-Trip Time）。

以上输出信息表明，H3C-R1 访问 192.168.1.2，目的端可达，源端发出的ICMP 回显请求报文均能得到回应，报文往返的最短时间、平均时间和最长时间分别为1ms，1ms和1ms。

下面介绍 Ping 命令输出的字段信息。

“56 data bytes”表示每个ICMP 回显请求报文中的数据字节数。默认情况下，使用56字节的报文发送。

“press CTRL C to break”表示在执行命令过程中，按快捷键[Ctrl+C]可终止ping 操作

“Reply from 192.168.1.2 : bytes=56 Sequence=1 ttl=255 time=1 ms”表示收到P 地址为1.1.2.2 的设备回复的ICMP 响应报文，若超时仍没有收到ICMP 应报文，则直接输出“Request time out”

“bytes”表示ICMP响应报文中的数据字节数。

“Sequence”表示报文序号，用来判断报文是否有分组丢失、失序或重复。

“ttl”表示ICMP 响应报文中的TTL值。

time”表示响应时间。

“--- 1.1.2.2 ping statistics ---”以下字段表示Ping操作中收发数据的统计结果。

5 packet(s) transmitted”表示发送的ICMP 回显请求报文数。

“5 packet(s) received”表示收到的ICMP 响应报文数。

“0.00% packet loss”表示未响应请求报文占发送的总请求报文的百分比。“round-trip min/avg/max =1/1/1ms”表示响应时间的最小值、平均值和最大值，单位为ms。

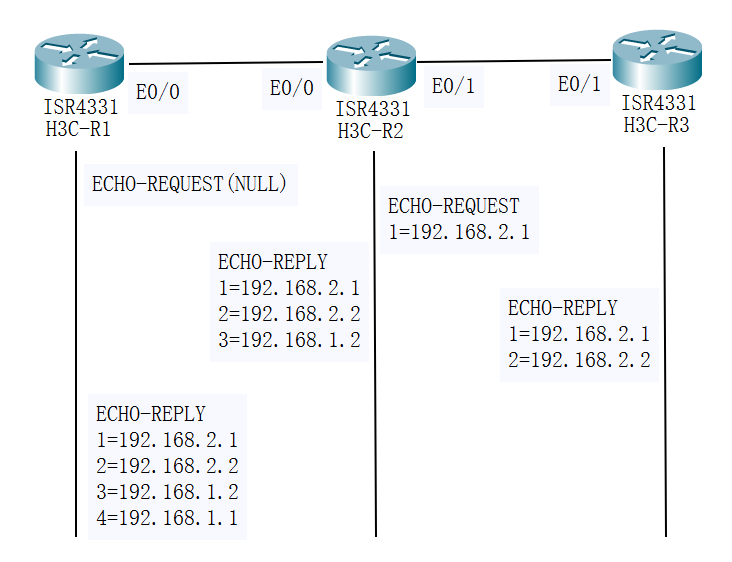


Ping -c 1 -r 192.168.2.2

在H3C-R1上ping 测试H3C-R3的IP地址192168.22，并显示路由信息。

“Record Route”表示ICMP 回显请求报文经过的路由器，采用倒序显示，距离目的端越

近的路由器越先显示。



Ping r原理：

h3c-r1 rr选项(icmp消息的字段)将空icmp请求传递给目标设备h3c-r3。

中间装置h3c-r2在icmp生态请求消息的rr选项中添加输出接口的ip地址(192.168.2.1)并传递消息。

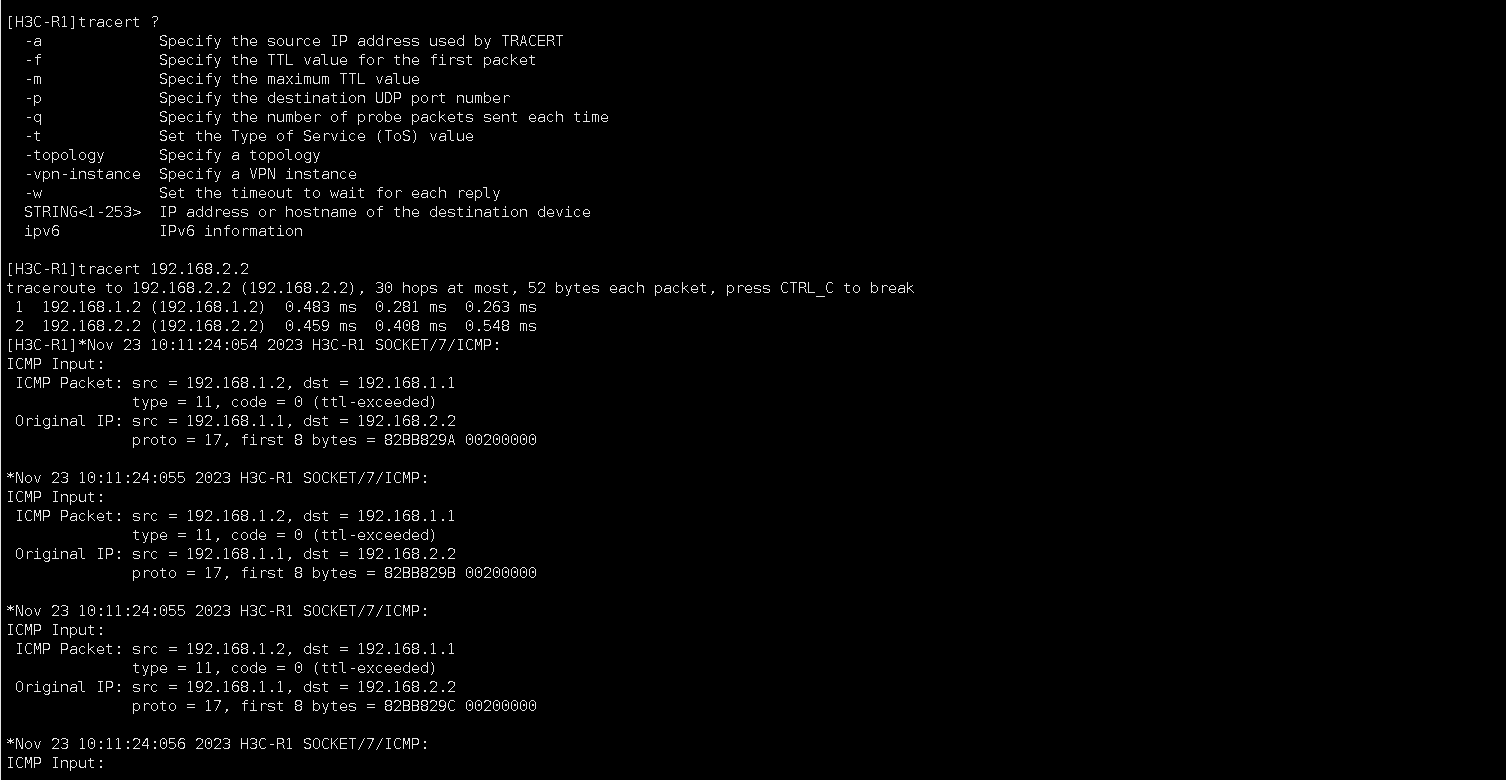
h3c-r3在收到请求消息时发送icmp响应消息。响应消息复制请求消息的rr选项，并将自己输出接口的ip地址(192.168.2.2)添加到rr选项中。

中间装置h3c-r2将输出接口的ip地址(192.168.1.2)添加到rr选项中，并发送报文。

h3c-r1接收icmp响应后，原始接口的ip地址(192.168.1.1)将被添加到rr选项中。因此，h3c-r1到h3c-r2的路由具体为192.168.1.1 <-> {192.168.1.2;192.168.2.1} <-> 192.168.2.2。

1. 掌握tracert调试工具

(使用tracert命令从h3c-r1源到目标(ip地址192.168.2.2)的消息路径。并说明了解决路由器超时现象的方法，并拍摄了截图。使用简单的文本直接绘制tracert原理。)



完成Ping命令测试网络连通性后，利用Tracert调试工具能够观察IP报文从源端到达目的端所经过的三层设备，从而验证网络连接的可用性。

-a source-ip：指定Tracert报文的源IP地址，该地址必须是设备上已配置的合法IP地址。如果不指定该参数，Tracert报文的源IP地址将是报文出接口的主IP地址。

-first-l initial-ttl：指定初始TTL，即第一个报文允许的跳数。取值范围为1到255，且小于最大TTL，默认值为1。

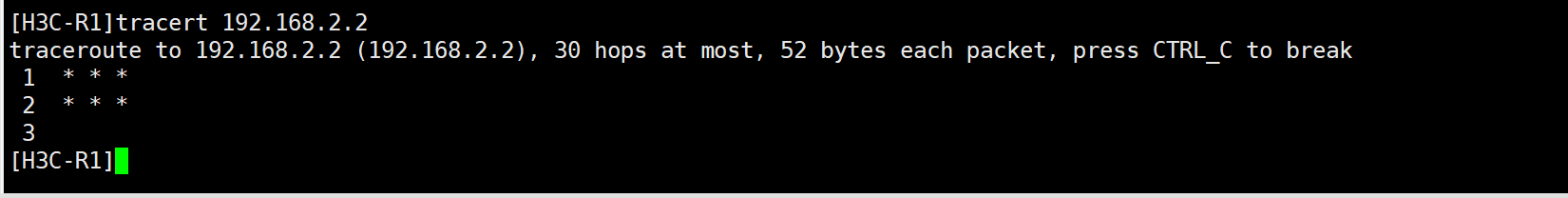
-m max-ttl：指定最大TTL，即一个报文允许的最大跳数。取值范围为1到255，且大于初始TTL，默认值为30。

-p port：指定目的端的UDP端口号，取值范围为1到65,535，默认值为33,434。

-q packet-number：指定每次发送的探测报文个数，取值范围为1到65,535，默认值为3。

-w timeout：指定探测报文的响应报文的超时时间，取值范围为1到65,535毫秒，默认值为5,000毫秒。

Host：目的端的IP地址或主机名，主机名为1到255个字符的字符串。



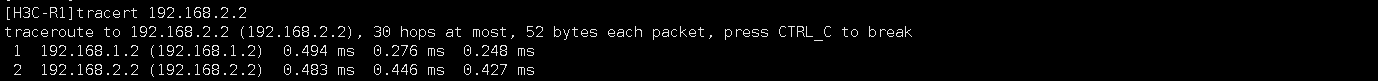
这时，我们会发现路由器超时“\*\*\*”。这是因为默认情况下，H3C 设备的ICMP 超时报文发送功能是处于关闭状态的。

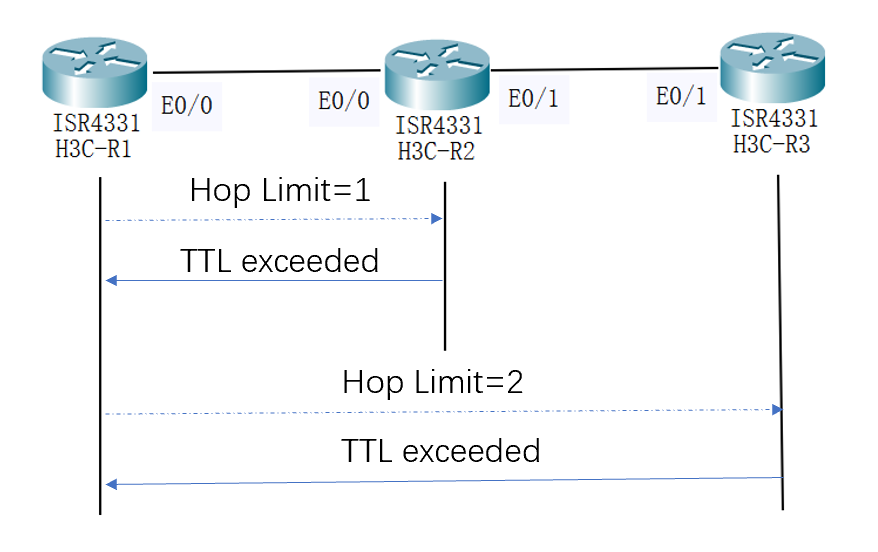
在进行 tracert命令操作前需要做一些配置准备工作。

(1)在中间设备(源端与目的编之间的设备》上开启ICMP 超时报文发送功能

(2)在目的端开启ICMP目的不可达报文发送功能。

在H3C-R1上使用tracert命令查看报文从源端到目的端（IP地址为192.168.2.2）所经过的路径：





Tracert命令的运作原理是这样的：源端H3C-R1向目的端H3C-R3发送一份IP数据报文，其TTL值被设定为1，同时该报文的UDP端口号选择了一个目的端任何应用程序都不可能使用的端口号。

在第一跳，即报文到达的第一个三层设备H3C-R2，该设备回应一个TTL超时的ICMP错误信息，携带了第一跳设备的IP地址192.168.1.2。通过这个响应，源端获得了第一个三层设备的地址（192.168.1.2）。

源端再次向目的端发送一份IP数据报文，但这次将TTL值设为2。这个过程不断重复，每次TTL值递增，直到报文最终到达目的端。由于目的端没有应用程序使用所选的UDP端口，因此目的端会回复一个端口不可达的ICMP错误消息，携带了目的端的IP地址192.168.2.2。

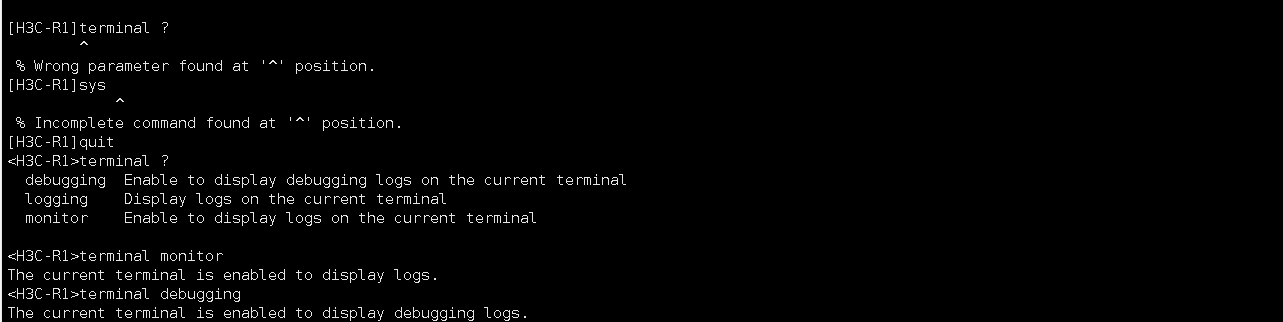
当源端H3C-R1接收到这个端口不可达的ICMP错误消息时，便知晓报文已经成功到达目的端H3C-R3。通过这一系列的交互，源端得知了数据报文从H3C-R1到H3C-R3所经过的路径，包括中间经过的设备IP地址（192.168.1.2、192.168.2.2）。

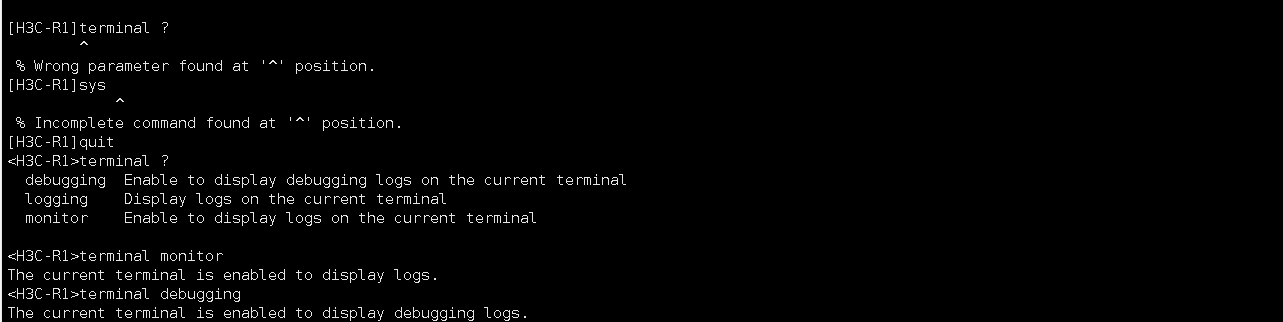
4. 配置系统调试功能——Ping

（对“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，并在H3C-R1上打开ICMP报文信息的开关来观察ICMP

报文输出”进行截图并加以文字简单说明。）

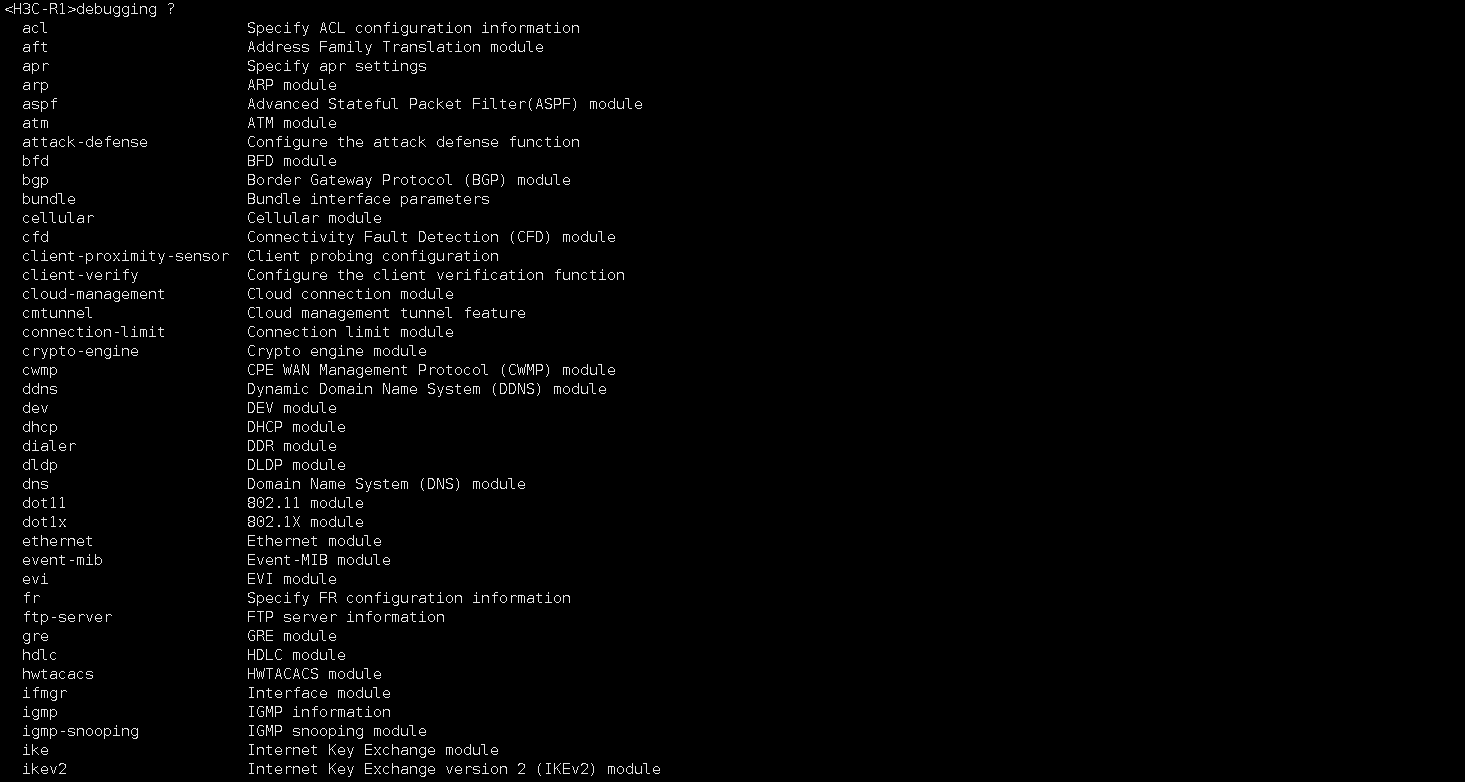




terminal monitor命令用于在用户视图下启用终端对系统信息的监视功能。尽管默认情况下，控制台的监视功能是启用的，但监视终端的监视功能是禁用的。

terminal debugging命令用于在用户视图下启用终端对调试信息的显示功能。虽然默认情况下，控制台对调试信息的显示功能是禁用的。

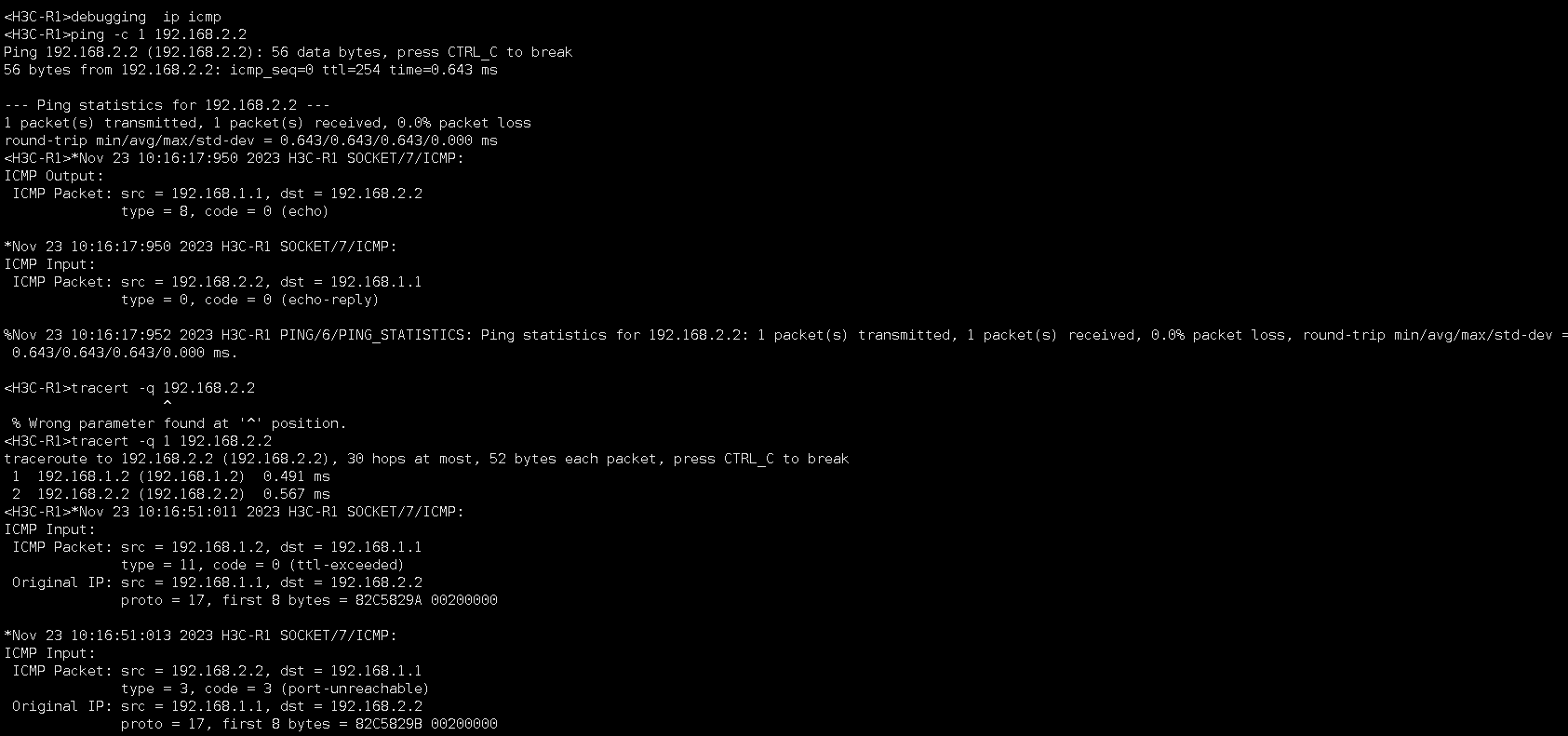
需要注意的是，只有同时启用终端对系统信息的监视功能和终端对调试信息的显示功能，调试信息才会在终端上显示出来。这两个开关默认状态分别是开启和关闭，因此需要手动执行相应命令以确保系统信息和调试信息都能及时在终端上展示。

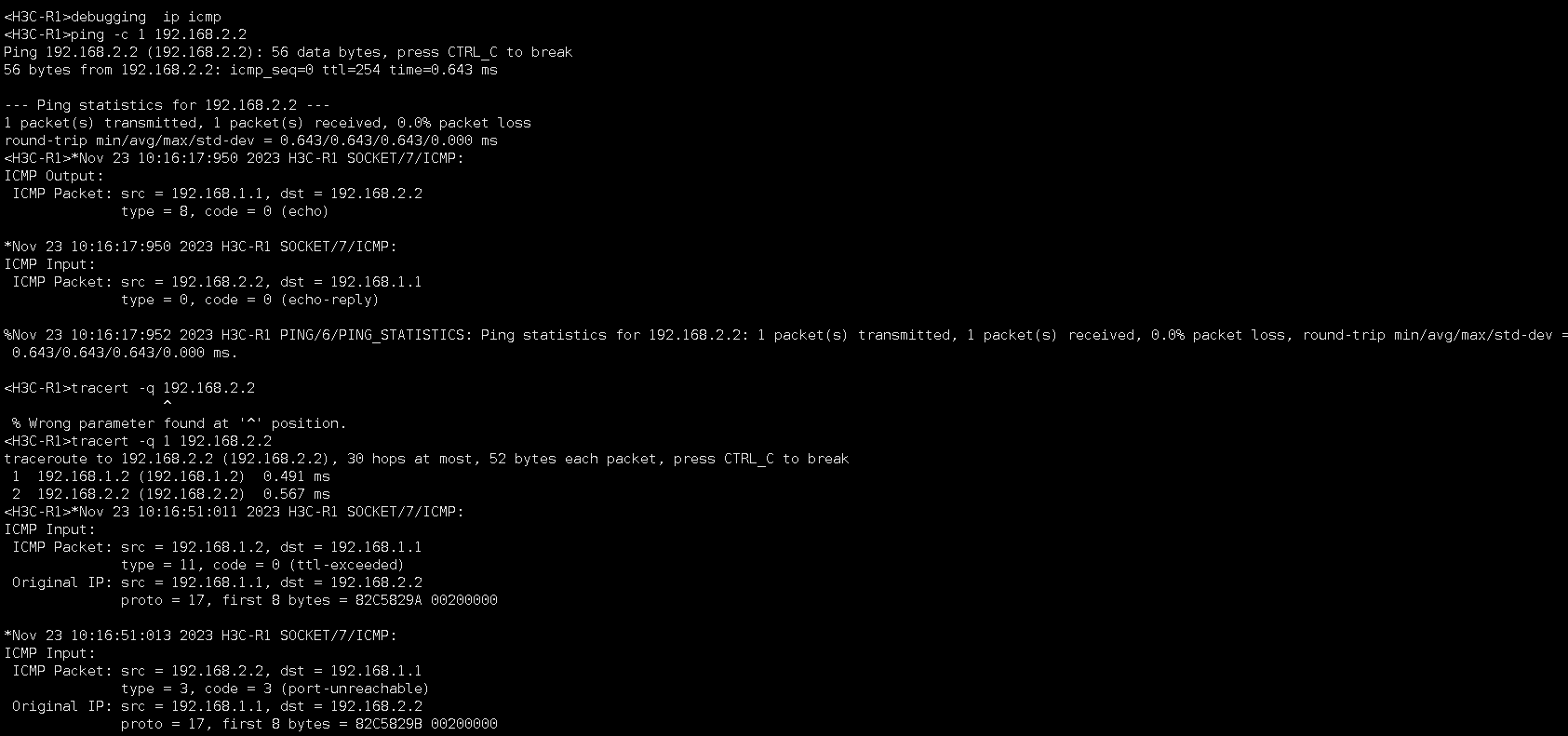
IMG_256

调试信息的生成、输出会响系绕的运行效率，因此，调试结束后，请及时关闭调试开关，或者使用undo debugging all命令，关闭所有模块的调试开关。

5. 配置系统调试功能——tracert

（截取“从tracert命令的debug调试信息可以看到H3C-R1接收的ICMP信息”，并配以简单文字解释。）





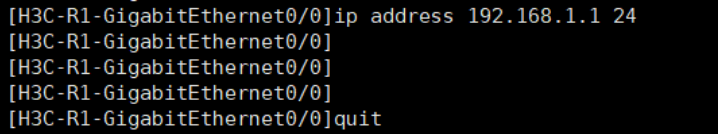
从Tracert命令的debug调试信息中可以观察到H3C-R1接收到的ICMP信息。H3C-R1发送了一份IP数据报文，目标地址为192.168.2.2，TTL值为1。当该IP数据报文抵达H3C-R2时，H3C-R2发现报文的目的地不是本地，并且TTL字段为1，于是发送了“TTL超时”ICMP差错报文ttl-exceeded（Type=11, Code=0）。

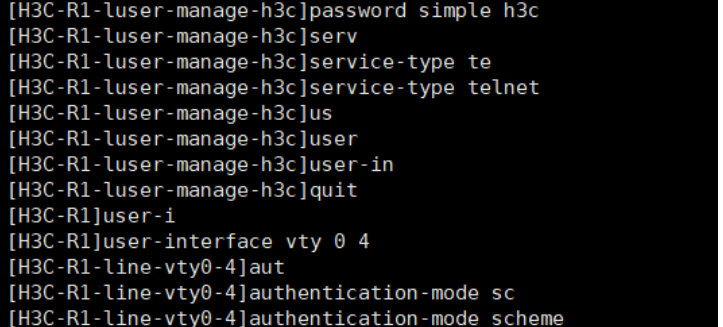
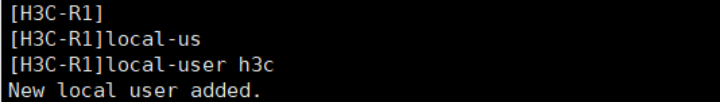
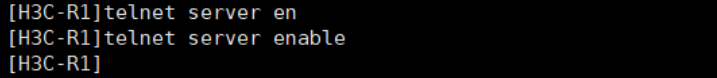
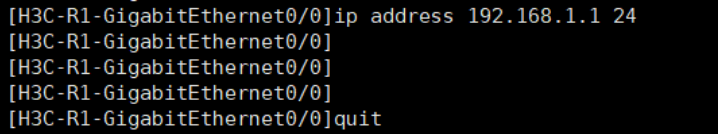
H3C-R1根据收到的ICMP差错报文ttl-exceeded（Type=11, Code=0）获取到网关地址的下一跳为192.168.1.2。随后，H3C-R1重新向H3C-R3发送了一份IP数据报文，目的地址为192.168.2.2，TTL值为2。在这一步，H3C-R3接收到了一个UDP的本地报文，但由于找不到对应进程的目的端口，于是向报文的源端发送了一个ICMP不可达报文port-unreachable（Type=3, Code=3）。

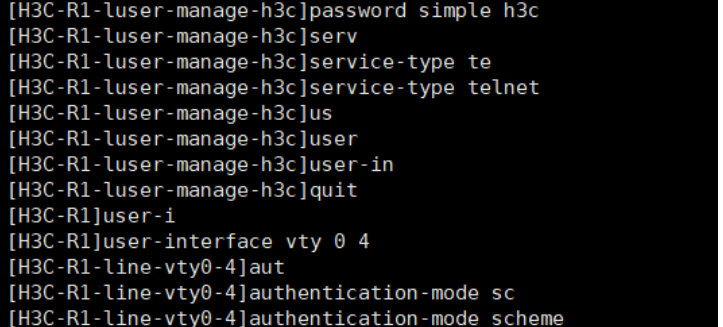
H3C-R1根据收到的ICMP不可达报文port-unreachable（Type=3, Code=3）得知已经到达了目的设备H3C-R3。这一系列的ICMP报文交互提供了Tracert命令所需的路径信息。

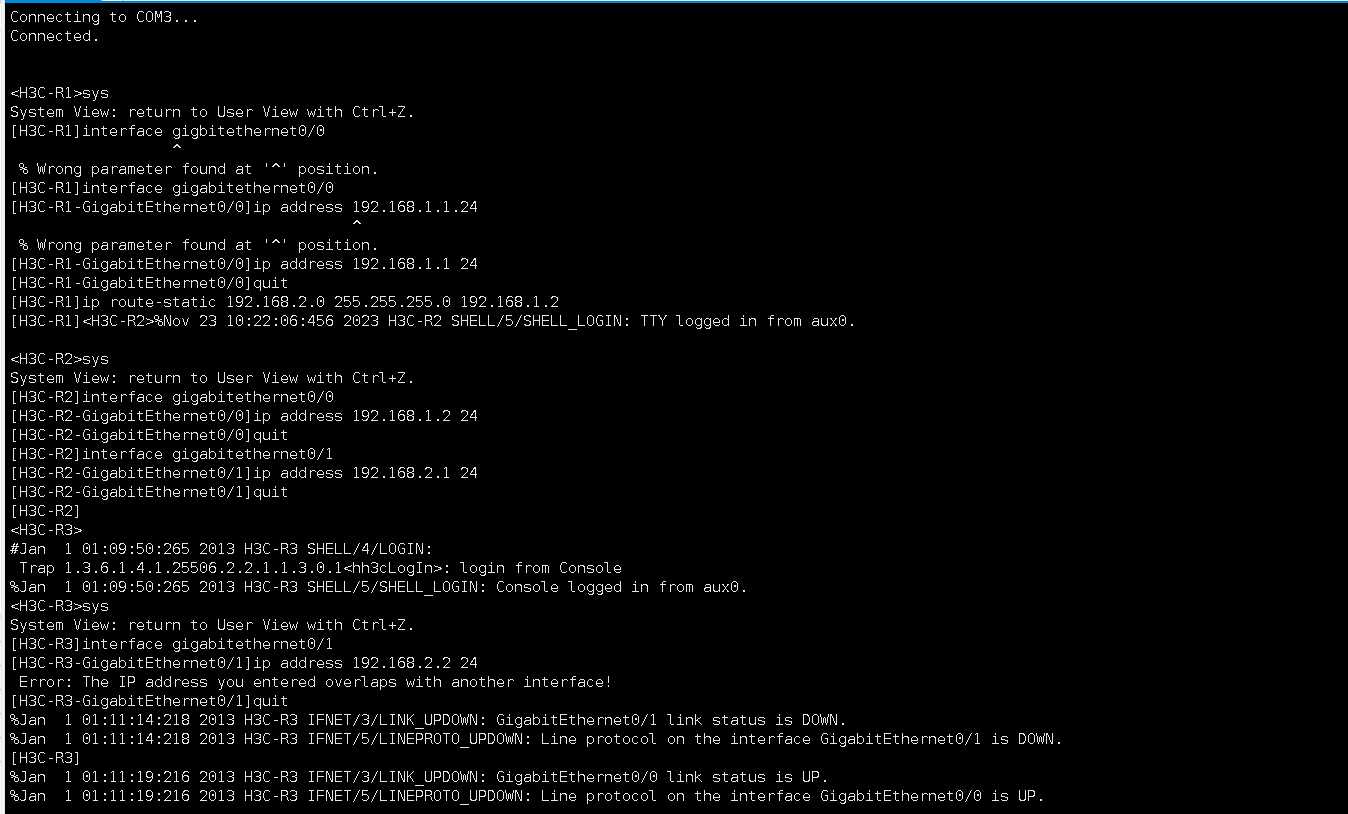
6. 按实验2配置H3C路由器基本参数

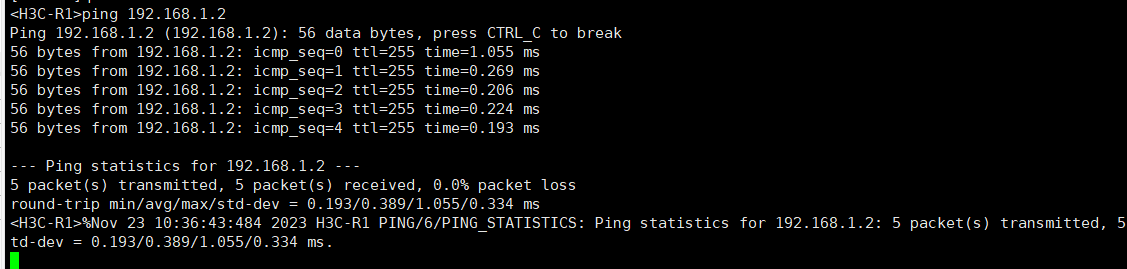
（截取你配置H3C路由器基本参数的界面，以及配置完后，测试H3C-R1和H3C-R2连通性的界面）





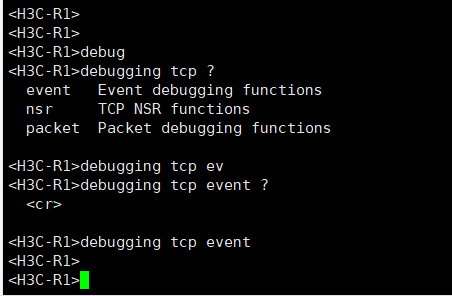


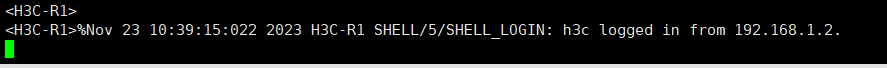


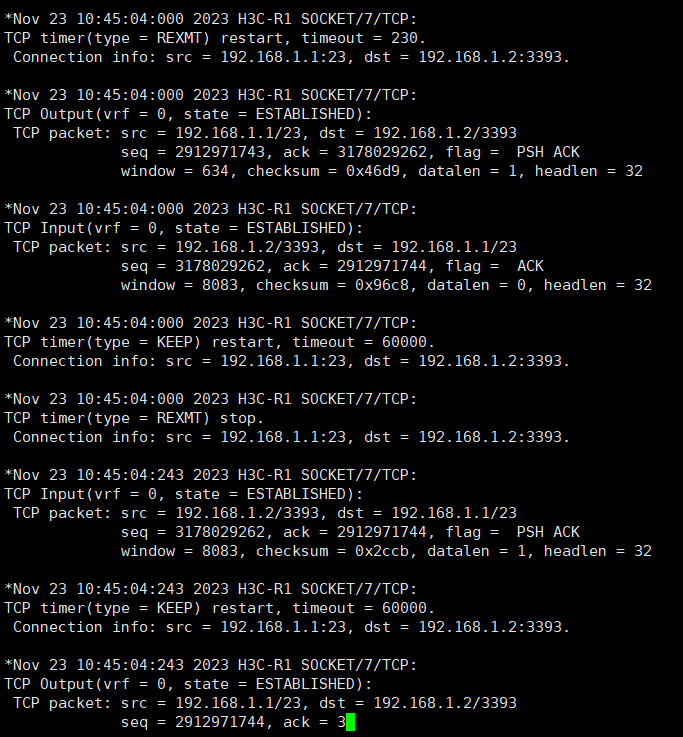


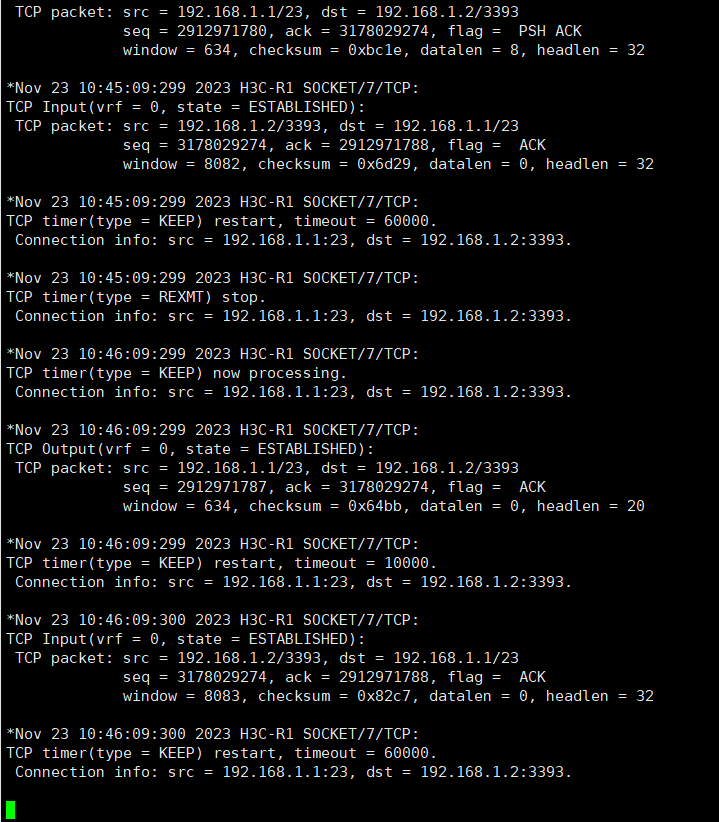
7. 测试TCP信息

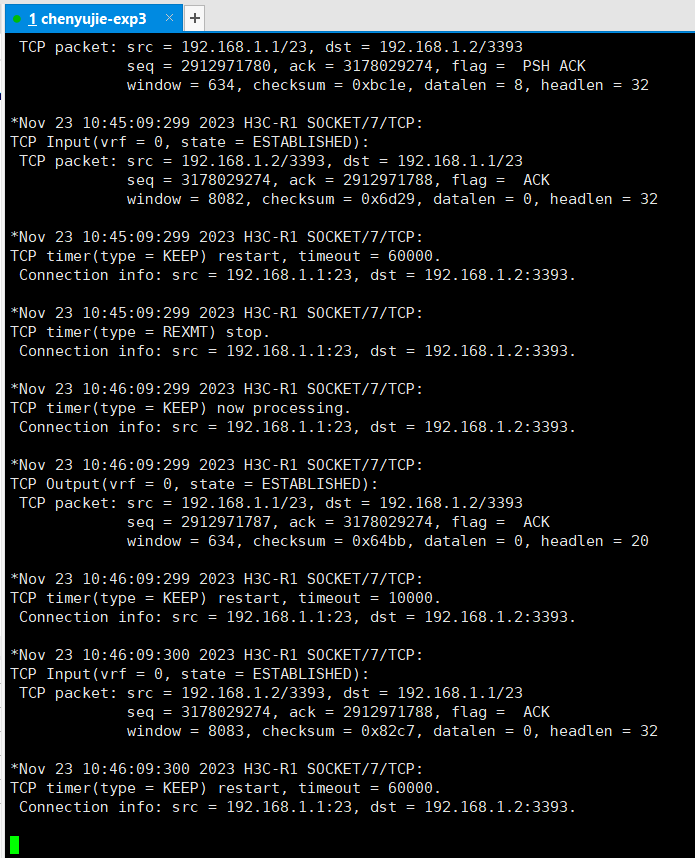
（截取你在H3C-R2上使用telnet命令访问H3C-R1的过程中出现的调试信息输出报文，并根据调试信息输出的报文具体分析TCP建立连接三次握手的具体过程，根据调试信息输出的报文具体分析关闭TCP连接四次握手的具体过程。）









、

**TCP建立连接三次握手的具体过程：**

tcp创建第三个握手的过程是：state=syn\_sent，这意味着目前tcp的状态是syn\_sent。flag=syn是h3c-r2向h3c-r1发送的tcpsny消息。

str=192.168.1.2:1041,dst=192.168.1.1:23显示发信地的原始地址、目标地址、源端口和目标端口。h3c-r1通过23号端口传送，这意味着访问telnet的连接。seq=2523560003, seq号为2523560003。这是h3c-r1的第一个序列。当tcpsyn消息从h3c-r1接收时，acksyn消息将被发送到h3c-r2。syn\_rcvd表示目前tcp的状态是syn\_rcvd。

flag=acksyn是由h3c-r1发送到h3c-r2的tcpacksyn消息。seq=2530540041, seq号码为2530540041，是h3c-r2的初始号码。ack=2523560004, ack序列号码是h3c-r1的seq序列号码加上1的2523560004。从h3c-r2接收tcpacksyn的消息，并将ack消息发送到h3c-r1。

state=established表示目前tcp处于established状态。falg=ack是h3c-r2向h3c-r1发送的tcpack信息。seq=2523560004, seq号是2523560004。ack=2530540042是h3c-r2的seq序列号码加上1的2530540042。

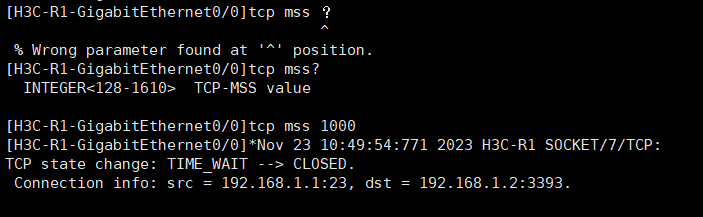
**关闭TCP连接四次握手的具体过程：**

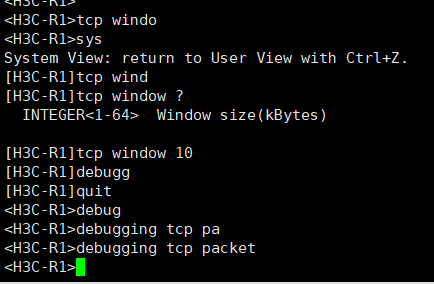
state=fin\_wait1,表示当前TCP状态在fin\_wait1。Flag=ACKFIN,是TCPACKFIN报文,由H3C-R1发送给H3C-R2。QQ=2530540538,顺序号。在H3C-R2上收到H3C-R1发送的TCPACKFIN报文TCPACK报文被发送到。

state=close\_wait,表示当前TCP状态在close\_wait。Flag=ACK,是一份TCPACK报文,由H3C-R2发送给H3C-R1。QQ=2523560052,顺序号。ACK=2530540539,ACK编号为顺序号+1,即2530540539。同时,H3C-R2也将关闭TCP连接的报文发送给H3C-R1,并等待H3C-R1的TCPACK。

8.配置TCP属性

（截取你自己的界面，并配以简单文字解释重要命令的含义。）





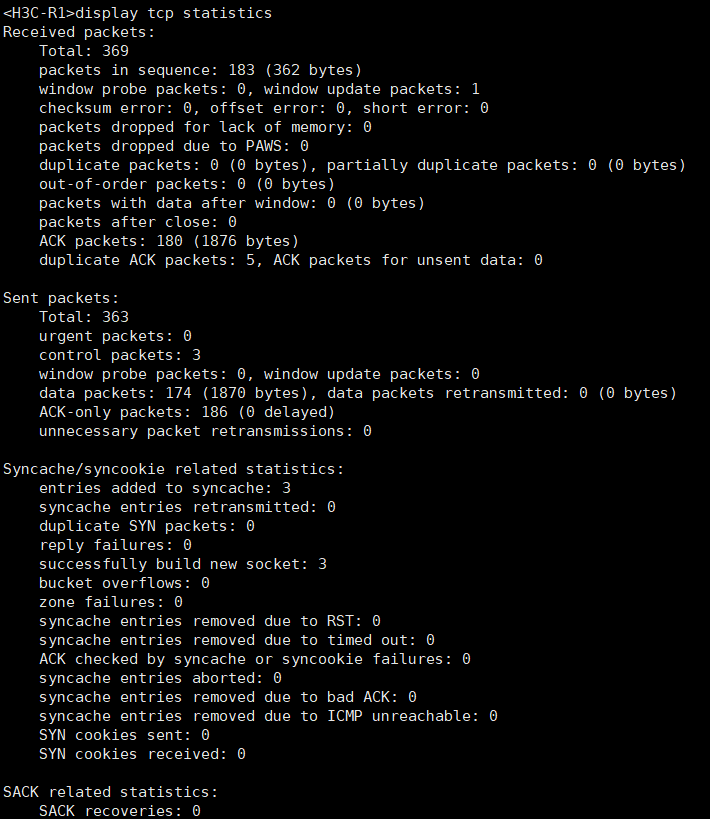
tcp mss 1000--设置TCP最大段大小为1000字节。MSS是TCP报文中的有效载荷部分的最大尺寸

tcp window 10--设置TCP窗口大小为10。TCP窗口大小是指在未收到确认之前可以发送的数据量

debugging tcp packet--启用TCP数据包调试，允许系统记录和显示TCP数据包的详细信息，用于诊断和调试TCP连接问题

9. 查看TCP相关的状态属性

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）



Dis play TCP status:命令显示所有TCP连接的状态。可利用该指令在设备上随时监控TCP连接。

\*:TCPMD5连接某个连接前有星号标志,说明TCP连接是经过MD5加密算法认证的连接。

TCPCB:表示TCP控制块、

Local Add port:表示IP地址和端口号在本端。

Foreign Add:port：表示对端IP 地址及端口号。

State：表示TCP连接的状态。从输出可以看到,H3C-R2的1028端口向H3C-R1的23端口发起TCP连接连接状态为ESTABLISHED。

Display TCP Statistic：显示了TCP连接的流量统计信息。

Received packets：表示收到TCP报文。

Sent packet：表示发送的TCP报文。

Initiated Connections:代表启动连接的次数。

Accepted Connections:表示接受连接的次数。

Established Connections:表示已经建立了连接。

Closed Connections;:表示已停机号码

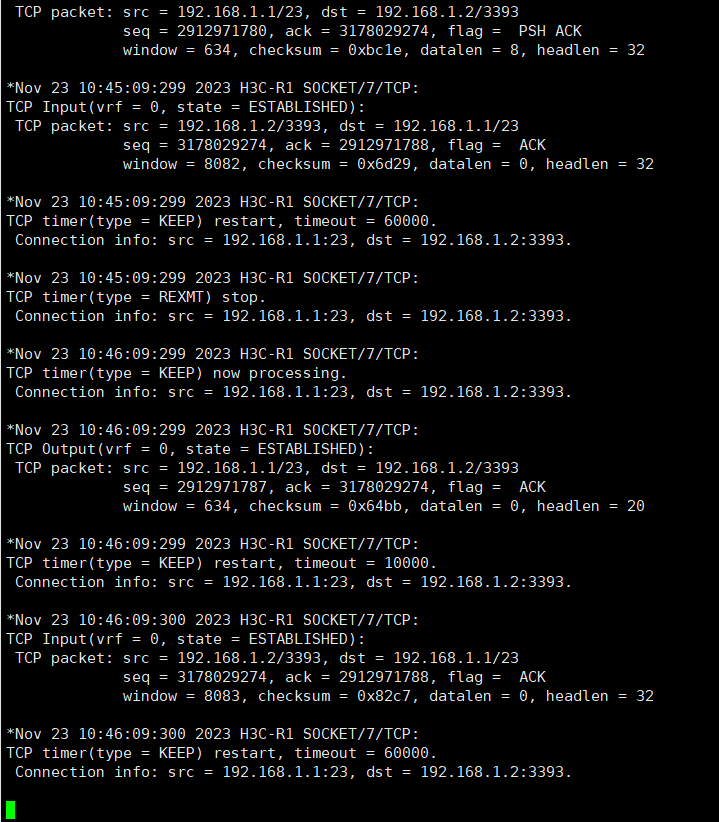
五、实验结果及分析

1. 我们第一个实验对应的图6-7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？

图7-6所示的拓扑图中，H3C-R2和H3C-R3连接的端口均为E0/1，但132页下面给的H3C-R3配置命令中却写成了“interface Ethernet0/0”，应该为“interface Ethernet0/1”才对。

其次，应将Ethernet 变为GigabitEthernet，因为实验室实际是千兆网口。

1. 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？



开始没有收到数据包的信息，后来听老师讲解，此部分应在实验一debugging 的基础上去做便会有结果。在输入实验一的debugging相关操作后问题解决。

收获：TCP/IP报文分析实验是网络学习中的关键实践，通过深入研究TCP/IP协议栈中的数据包，我深刻领悟了网络通信的运作和协议机制。在实验中，我透彻了解了TCP/IP协议栈的层次结构，从物理层到应用层各个层次的协同工作，数据的封装和解封装过程清晰呈现。

通过深入分析TCP/IP报文的格式和字段，我掌握了TCP和IP报文中各个字段的涵义和相互关系。这使我能够更精准地诊断网络故障，理解连接建立失败或数据传输问题的本质原因。此外，我培养了对网络流量特征的敏感性，能够识别网络中占用带宽的协议、应用程序或主机，以便进行网络优化和性能调整。

这个实验不仅提高了我的网络故障排除能力，还加强了我对网络安全的认识。实验过程中，我通过网络数据包的捕获和分析，提升了在实际网络环境中的操作经验。

综合而言，TCP/IP报文分析实验为我提供了将理论知识应用于实际网络场景的机会，推动我深入理解网络通信和协议相互作用的过程。这种实践经验不仅提升了我的网络管理和优化技能，还为我未来在网络领域的发展奠定了坚实的基础。