ENSP版IPSEC VPN的企业网仿真项目

目录

[ENSP版IPSEC VPN的企业网仿真项目 1](#_Toc163949923)

[第一章 项目简介 1](#_Toc163949924)

[1.1 项目描述 1](#_Toc163949925)

[1.2 项目背景 1](#_Toc163949926)

[1.3 项目原理 1](#_Toc163949927)

[第二章 网络拓扑的设计 3](#_Toc163949928)

[2.1 网络拓扑的设计 3](#_Toc163949929)

[2.1.1 主公司网 3](#_Toc163949930)

[2.1.2 公共网络Internet 3](#_Toc163949931)

[2.1.3 分公司1网 3](#_Toc163949932)

[2.1.4 分公司2网 3](#_Toc163949933)

[2.2 网络地址规划 4](#_Toc163949934)

[2.3 网络拓扑结构图 6](#_Toc163949935)

[第三章 网络配置过程 7](#_Toc163949936)

[3.1主公司网络配置过程 7](#_Toc163949937)

[3.2 分公司1网络配置过程和建立Ipsec VPN隧道 13](#_Toc163949938)

[3.2 分公司2网络配置过程和建立Ipsec VPN隧道 15](#_Toc163949939)

[3.2 公共网络Internet配置过程 17](#_Toc163949940)

[第四章 项目测试过程 19](#_Toc163949941)

[4.1 对分公司与分公司、分公司与总公司之间进行连通性测试 19](#_Toc163949942)

[4.2 对VPN隧道传输过程进行抓包分析 21](#_Toc163949943)

源代码链接：<https://github.com/chenaaa1/campus_network-simulation>

# 第一章 项目简介

## 1.1 项目描述

设计一个模拟企业网的网络项目，在该项目中划分出三个局域网，分别为主公司网，分公司1网，分公司2网，其中主公司的局域网下再划分出4个子网，并且这四个子网之间可以实现相互通信。然后再通过三个路由器模拟公共网络Internet，为了实现分公司与主公司之间的通信，我们采用了IPSec VPN的方式使得分公司1的局域网内设备可以与主公司中网段为192.168.4.0的子网进行通信，分公司2的局域网设备可以与主公司中网段为192.168.2.0的子网和192.168.3.0的子网进行通信。

## 1.2 项目背景

企业对网络安全性的需求日益提升，而传统的TCP/IP协议缺乏有效的安全认证和保密机制。IPSec（Internet Protocol Security）作为一种开放标准的安全框架结构，可以用来保证IP数据报文在网络上传输的机密性、完整性和防重放。

企业希望对总部子网与分部子网之间相互访问的流量进行安全保护。总部与分部通过公网建立通信，可以在总部网关与分部网关之间建立一个IPSec隧道来实施安全保护。

## 1.3 项目原理

对于IPSec VPN结构,首先建立路由器连接公共接口之间的IPSec隧道,内部网络各个子网之间传输的IP分组封装成内部网络私有IP地址为源和目的IP地址的IP分组，该IP分组经过IPSec隧道传输时，作为安全净荷(Encapsulating Security Payload,ESP)报文的净荷。根据建立IPSec 隧道两端之间的安全关联时约定的加密和鉴别算法，完成 ESP 报文的加密过程和消息鉴别码MessageAuthentication Code,MAC)的计算过程。手工方式是指通过手工配置建立IPSec 隧道两端的安全关联，并手工配置该安全关联相关的参数。

内部网络中的各个子网对于完全属于公共网络的路由器是透明的，因此,在成功建立IPSec 隧道及 IPSec 隧道两端之间的 IPSec 安全关联前,内部网络各个子网之间是无法正常通信的。

具体配置方式如下所述：

1. 手工建立IPSec 隧道两端之间的安全关联

对应路由器连接公共网络的接口，通过手工配置建立两两之间的安全关联,并手工配置安全关联相关的参数，如指定安全协议 ESP,ESP 报文加密算法,ESP报文鉴别算法和完成 ESP 报文加密及 ESP 报文 MAC 计算时使用的密钥

1. 指定通过IPSec 隧道传输的信息流

通过分类规则，指定经过IPSec隧道传输的是内部网络各个子网之间传输的IP分组,即源和目的 IP 地址为内部网络私有IP地址的 IP 分组。

1. 配置静态路由项

在路由器中配置静态路由项,静态路由项将目的网络是这些路由器非直接连接的内部网络子网的 IP 分组转发给这些路由器公共网络上的下一跳，这样做的目的是使得路由器连接公共网络的接口成为内部网络各个子网间传输的 IP 分组的输出接口。

1. 路由器连接公共网络的接口配置IPSec 策略

在路由器连接公共网络的接口配IPSec策略,IPSec策略要求将所有内部网络各个子网间传输的IP 分组封装成ESP报文隧道模式，隧道模式外层IP首部中的源和目的IP地址分别是IPSec隧道两端的全球IP地址。内部网络中各个子网间传输的IP分组作为 ESP 报文的净荷,根据手工配置的IPSec隧道两端之间安全关联的相关参数,完成 ESP 报文加密和MAC 计算过程。

# 第二章 网络拓扑的设计

## 2.1 网络拓扑的设计

### 2.1.1 主公司网

对于主公司网，首先设置成有两栋办公楼、一栋行政楼、一栋信息中心楼和一栋机房。其中信息中心楼是企业网络设备的中心，里面放置三台三层交换机和一台路由器,负责接入公共网络Internet。对于行政楼，我们放置一台PC1和Clinet1，然后连接到一台二层交换机上，最后通过三层交换机连接到信息中心楼。对于办公楼1和办公楼2，我们都放置一台PC和一台Server服务器，然后连接到各自的二层交换机上，最后通过三层交换机连接到信息中心楼。对于机房，我们放置一台PC和两台Server服务器,然后也是连接到一台二层交换机上，最后通过三层交换机连接到信息中心楼。在这个网络中，三层交换机作为汇聚层交换机，二层交换机作为接入层交换机。在本项目中采用的路由协议为OSPF，并将企业网划分为3个区域，其中核心设备即三台三层交换机运行在area 0，LSW1连接AR1的链路在area 1,LSW2连接AR1的链路在area 2，其中核心交换机采用S5700三层交换机，链路连接均使用快速以太网口。

### 2.1.2 公共网络Internet

对于公共网络Internet，主要是通过三台路由器AR2，AR3，AR4来模拟，其中这三台路由器相互连接。

### 2.1.3 分公司1网

在分公司1网内，主要放置了一台PC和一台Client，这两个设备再连接三层交换机上，三层交换机再连接到一台路由器上，再由路由器连接到公共网络Internet中。

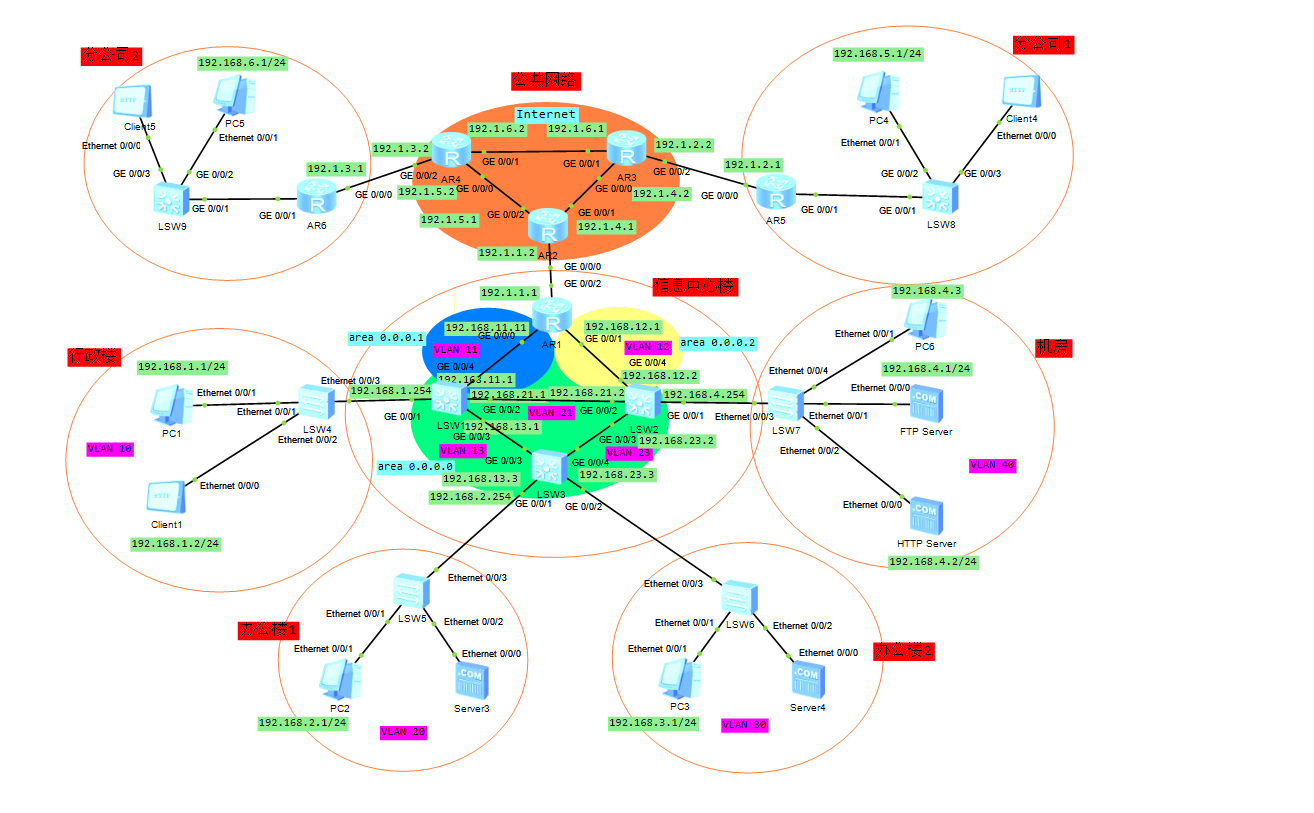
### 2.1.4 分公司2网

在分公司2网内，与分公司1网类似，也是放置了一台PC和一台Client，这两个设备再连接三层交换机上，三层交换机再连接到一台路由器上，再由路由器连接到公共网络Internet中。

## 2.2 网络地址规划

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 建筑物 | 设备名称 | 接口 | VLAN | IP地址 | 区域 |
| 信息中心楼 | AR1 | GE0/0/0 | 11 | 192.168.11.11/24 | 1 |
| GE0/0/1 | 12 | 192.168.11.11/24 | 2 |
| GE0/0/2 |  | 192.1.1.1/24 |  |
| LSW1  (三层交换机） | VLAN10 |  | 192.168.1.254/24 | 0 |
| VLAN11 |  | 192.168.11.1/24 | 1 |
| VLAN13 |  | 192.168.13.1/24 | 0 |
| VLAN21 |  | 192.168.21.1/24 | 0 |
| GE0/0/1 | 10 |  |  |
| GE0/0/2 | 21 |  |  |
| GE0/0/3 | 13 |  |  |
| GE0/0/4 | 11 |  |  |
| LSW2  （三层交换机） | VLAN 12 |  | 192.168.12.2/24 | 2 |
| VLAN 21 |  | 192.168.21.2/24 | 0 |
| VLAN 23 |  | 192.168.23.2/24 | 0 |
| VLAN 40 |  | 192.168.4.254/24 | 0 |
| GE0/0/1 | 40 |  |  |
| GE0/0/2 | 21 |  |  |
| GE0/0/3 | 23 |  |  |
| GE0/0/4 | 12 |  |  |
| LSW3  (三层交换机） | VLAN 13 |  | 192.168.13.3/24 | 0 |
| VLAN 20 |  | 192.168.2.254/24 | 0 |
| VLAN 23 |  | 192.168.23.3/24 | 0 |
| VLAN 30 |  | 192.168.3.254/24 | 0 |
| GE0/0/1 | 20 |  |  |
| GE0/0/2 | 30 |  |  |
| GE0/0/3 | 13 |  |  |
| GE0/0/4 | 23 |  |  |
| 行政楼 | LSW4 | VLAN 10 |  |  |  |
| Ethernet0/0/1 | 10 |  |  |
| Ethernet0/0/2 | 10 |  |  |
| Ethernet0/0/3 | 10 |  |  |
| PC1 |  |  | 192.168.1.1/24 |  |
| Client1 |  |  | 192.168.1.2/24 |  |
| 办公楼1 | LSW5 | VLAN20 | 20 |  |  |
| Ethernet0/0/1 | 20 |  |  |
| Ethernet0/0/2 | 20 |  |  |
| Ethernet0/0/3 | 20 |  |  |
| PC2 |  |  | 192.168.2.1/24 |  |
| Server3 |  |  | 192.168.2.2/24 |  |
| 办公楼2 | LSW6 | VLAN30 |  |  |  |
| Ethernet0/0/1 | 30 |  |  |
| Ethernet0/0/2 | 30 |  |  |
| Ethernet0/0/3 | 30 |  |  |
| PC3 |  |  | 192.168.3.1/24 |  |
| Server4 |  |  | 192.168.3.2/24 |  |
| 机房 | LSW7 | VLAN30 |  |  |  |
| Ethernet0/0/1 | 40 |  |  |
| Ethernet0/0/2 | 40 |  |  |
| Ethernet0/0/3 | 40 |  |  |
| FTP Server |  |  | 192.168.4.1/24 |  |
| HTTP Server |  |  | 192.168.4.2/24 |  |
| PC6 |  |  | 192.168.4.3/24 |  |
| 公共网络Internet | AR2 | GE0/0/0 |  | 192.1.1.2/24 |  |
| GE0/0/1 |  | 192.1.4.1/24 |  |
| GE0/0/2 |  | 192.1.5.1/24 |  |
| AR3 | GE0/0/0 |  | 192.1.4.2/24 |  |
| GE0/0/1 |  | 192.1.6.1/24 |  |
| GE0/0/2 |  | 192.1.2.2/24 |  |
| AR4 | GE0/0/0 |  | 192.1.5.2/24 |  |
| GE0/0/1 |  | 192.1.6.2/24 |  |
| GE0/0/2 |  | 192.1.3.2/24 |  |
| 分公司1 | AR5 | GE0/0/0 |  | 192.1.2.1/24 |  |
| GE0/0/1 |  | 192.168.5.254/24 |  |
| LSW8 |  |  |  |  |
| PC4 |  |  | 192.168.5.1/24 |  |
| Client4 |  |  | 192.168.5.2/24 |  |
| 分公司2 | AR6 | GE0/0/0 |  | 192.1.3.1/24 |  |
| GE0/0/1 |  | 192.168.6.254/24 |  |
| LSW9 |  |  |  |  |
| PC5 |  |  | 192.168.6.1/24 |  |
| Client5 |  |  | 192.168.6.2/24 |  |

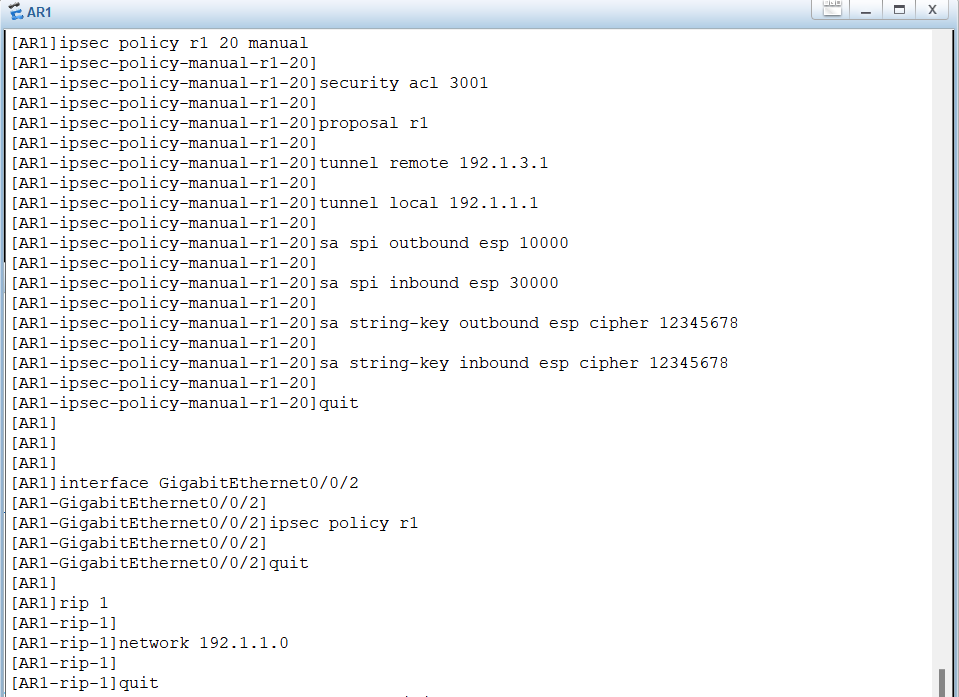
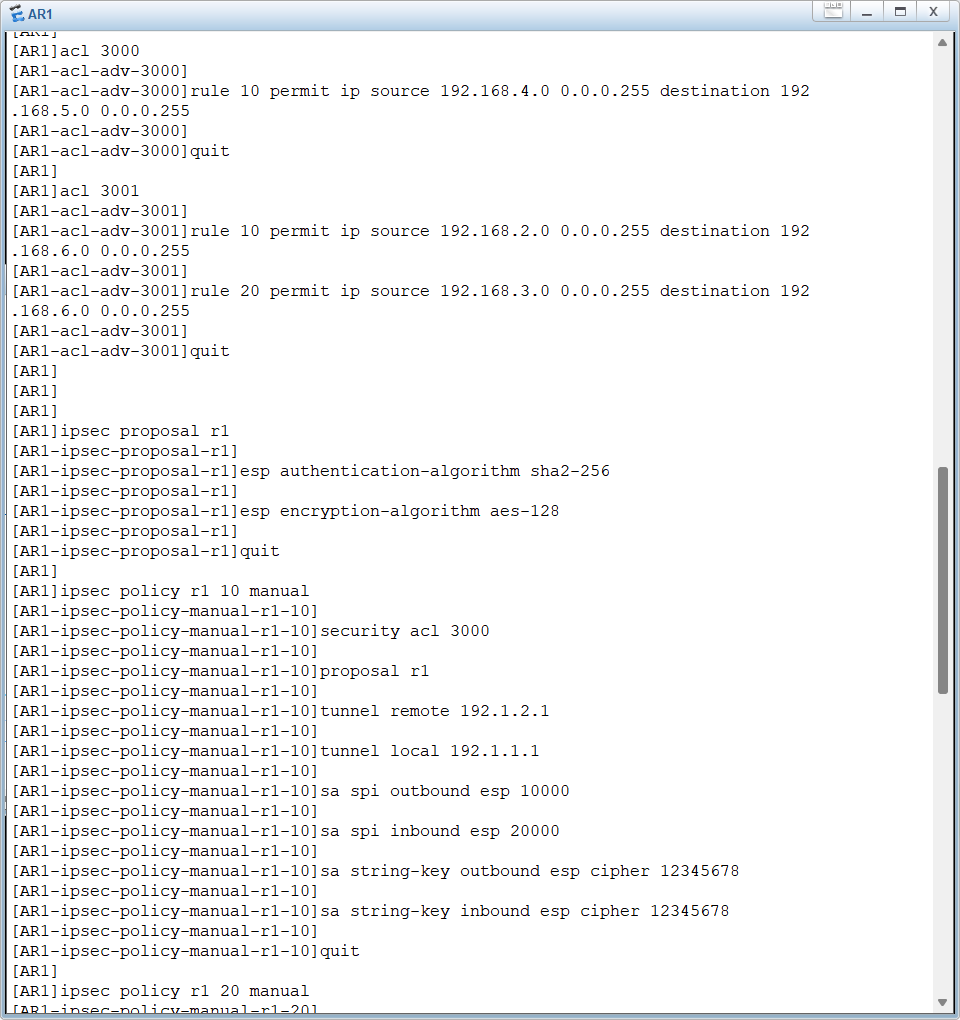
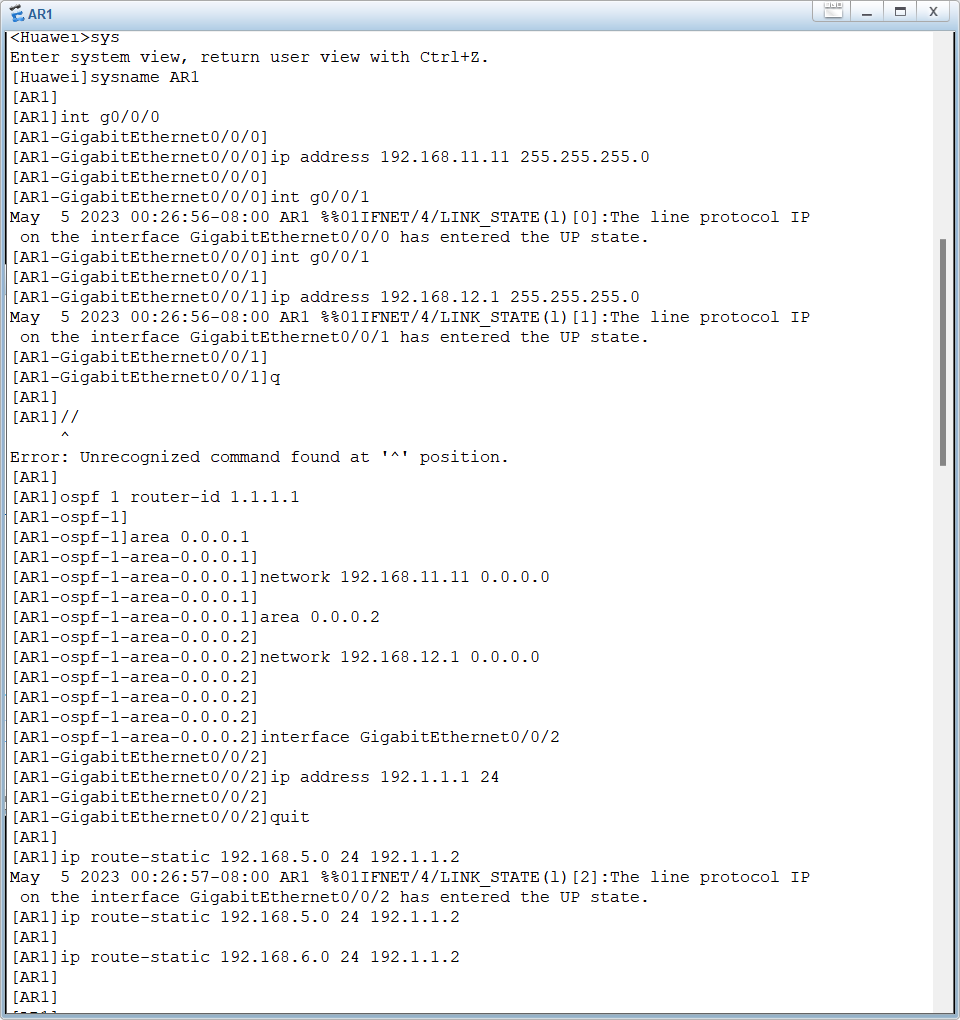
## 2.3 网络拓扑结构图



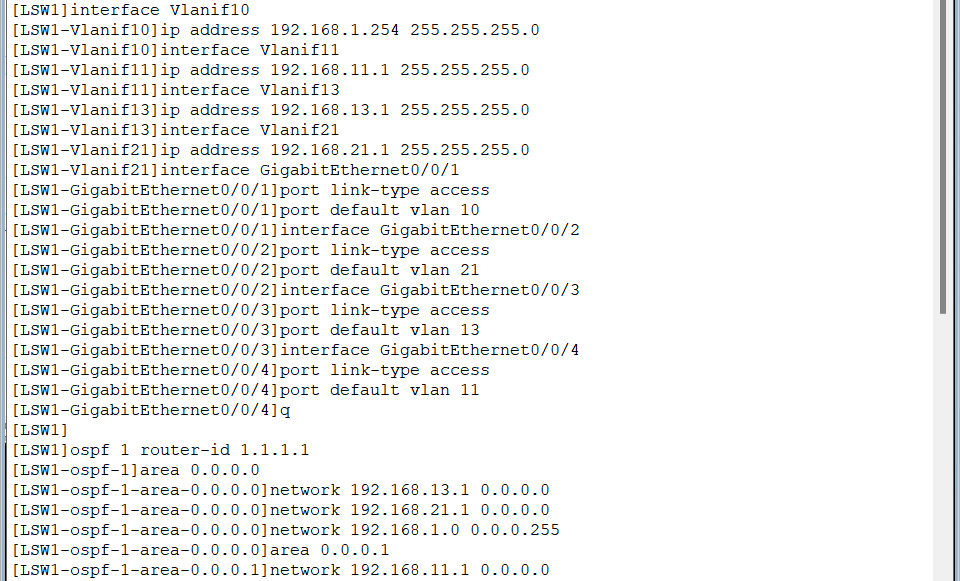
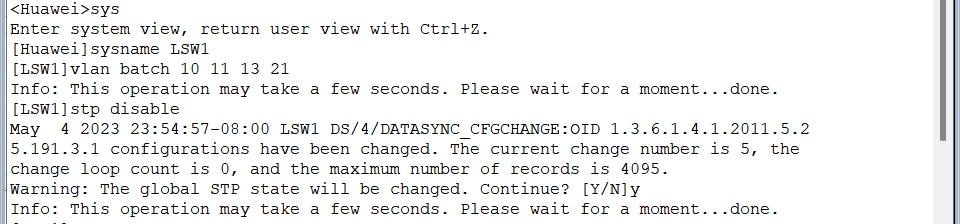
# 第三章 网络配置过程

## 3.1主公司网络配置过程

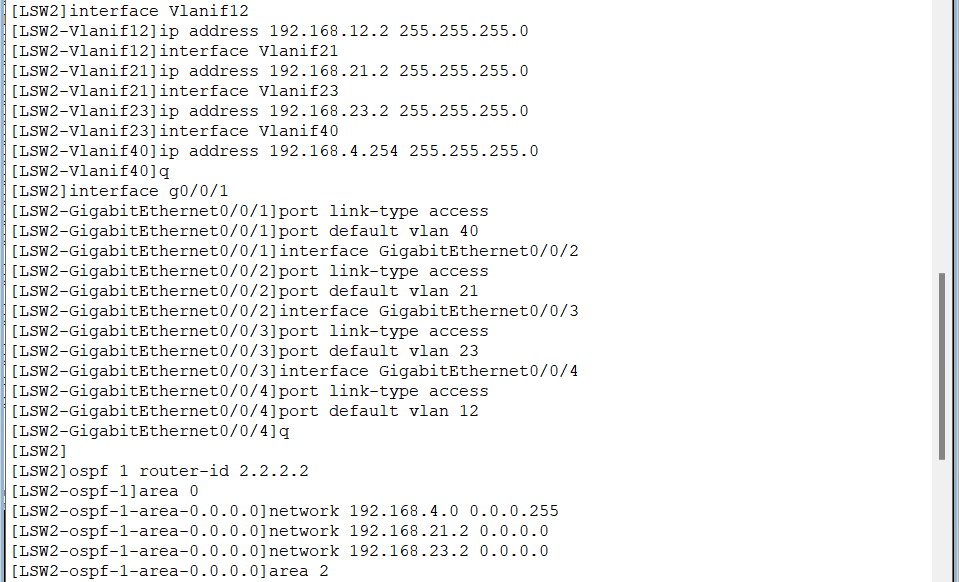
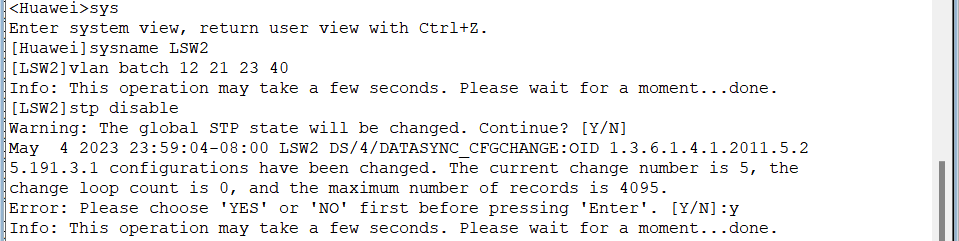
1. 对PC1进行配置，设置其IP为192.168.1.1/24，子网掩码为255.255.255.0，网关为192.168.1.254。
2. 对PC2进行配置，设置其IP为192.168.2.1/24，子网掩码为255.255.255.0，网关为192.168.2.254。
3. 对PC3进行配置，设置其IP为192.168.3.1/24，子网掩码为255.255.255.0，网关为192.168.3.254。
4. 对Client1进行配置，设置其IP为192.168.1.2/24，子网掩码为255.255.255.0，网关为192.168.1.254。
5. 对Server3进行配置，设置其IP为192.168.2.2/24，子网掩码为255.255.255.0，网关为192.168.2.254。
6. 对Server4进行配置，设置其IP为192.168.3.2/24，子网掩码为255.255.255.0，网关为192.168.3.254。
7. 对Ftp Server进行配置，设置其IP为192.168.4.1/24，子网掩码为255.255.255.0，网关为192.168.4.254。
8. 对Http Server进行配置，设置其IP为192.168.4.2/24，子网掩码为255.255.255.0，网关为192.168.4.254。
9. 对PC6进行配置，设置其IP为192.168.4.3/24，子网掩码为255.255.255.0，网关为192.168.4.254。
10. 然后对AR1进行对应的配置，在GigabitEthernet0/0/2接口上绑定IP地址192.1.1.1，在GigabitEthernet0/0/0接口上绑定IP地址192.168.11.1，在GigabitEthernet0/0/1接口上绑定IP地址192.168.12.1，然后对连接公共网络Internet的接口启用RIP协议，最后再对AR1设备进行IPSec隧道的配置。具体配置过程如下图所示。



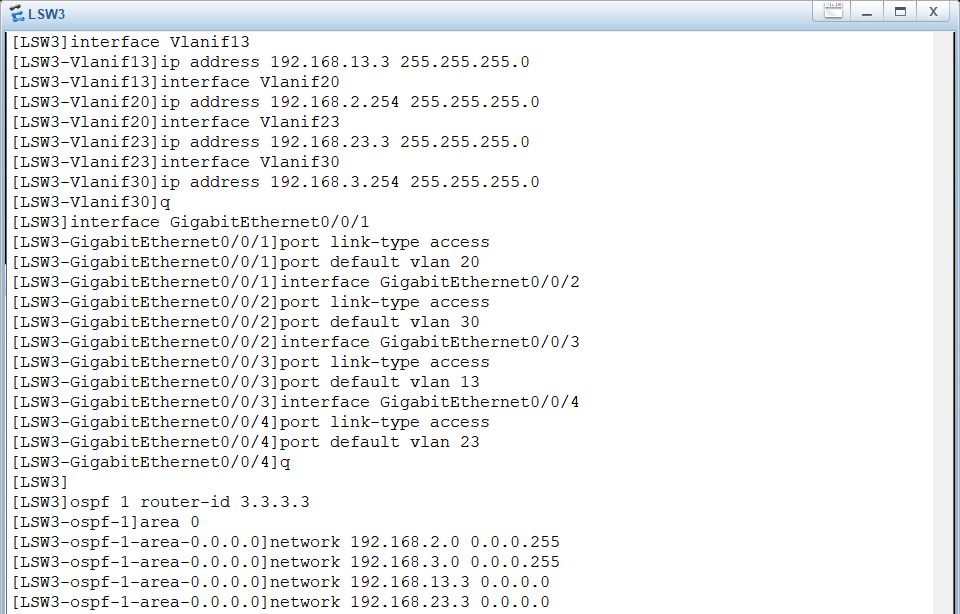
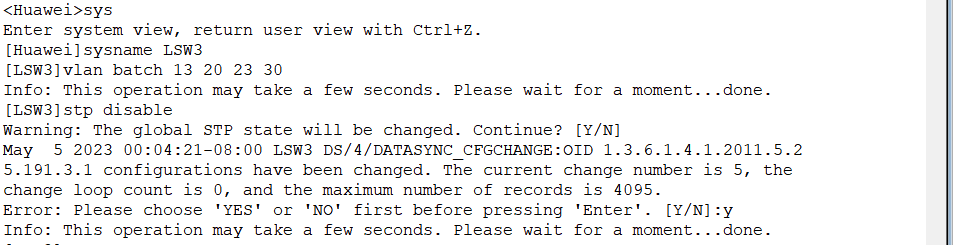
1. LSW1路由器配置



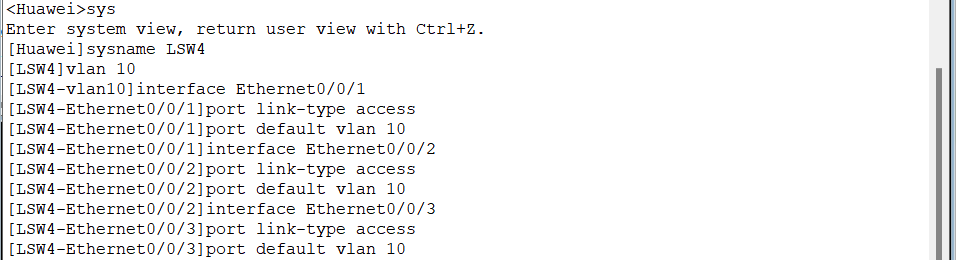
1. LSW2路由器配置



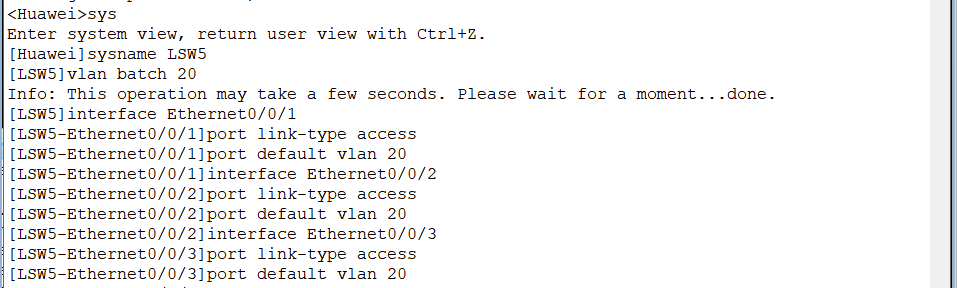
1. LSW3路由器配置



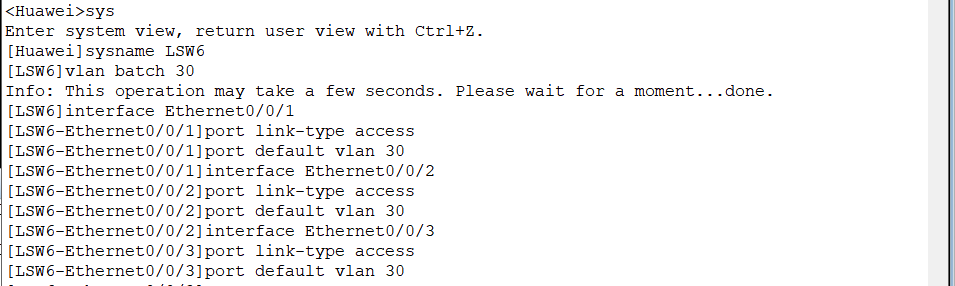
1. LSW4路由器配置



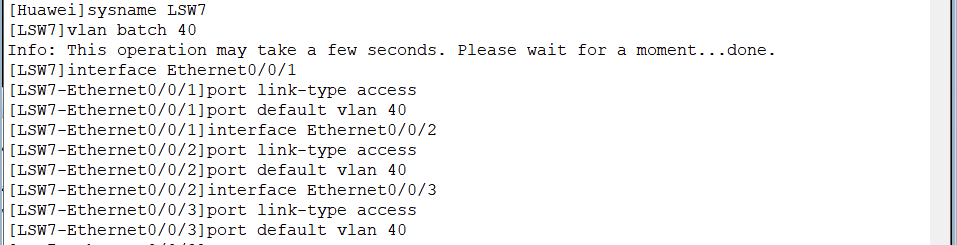
1. LSW5路由器配置



1. LSW6路由器配置

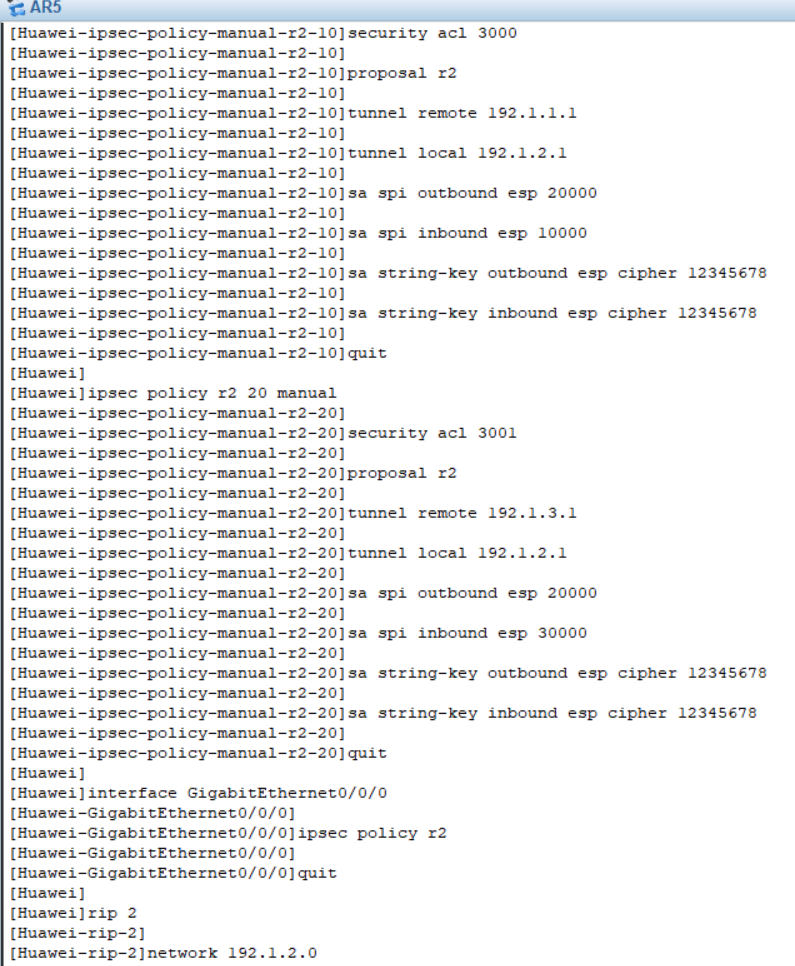
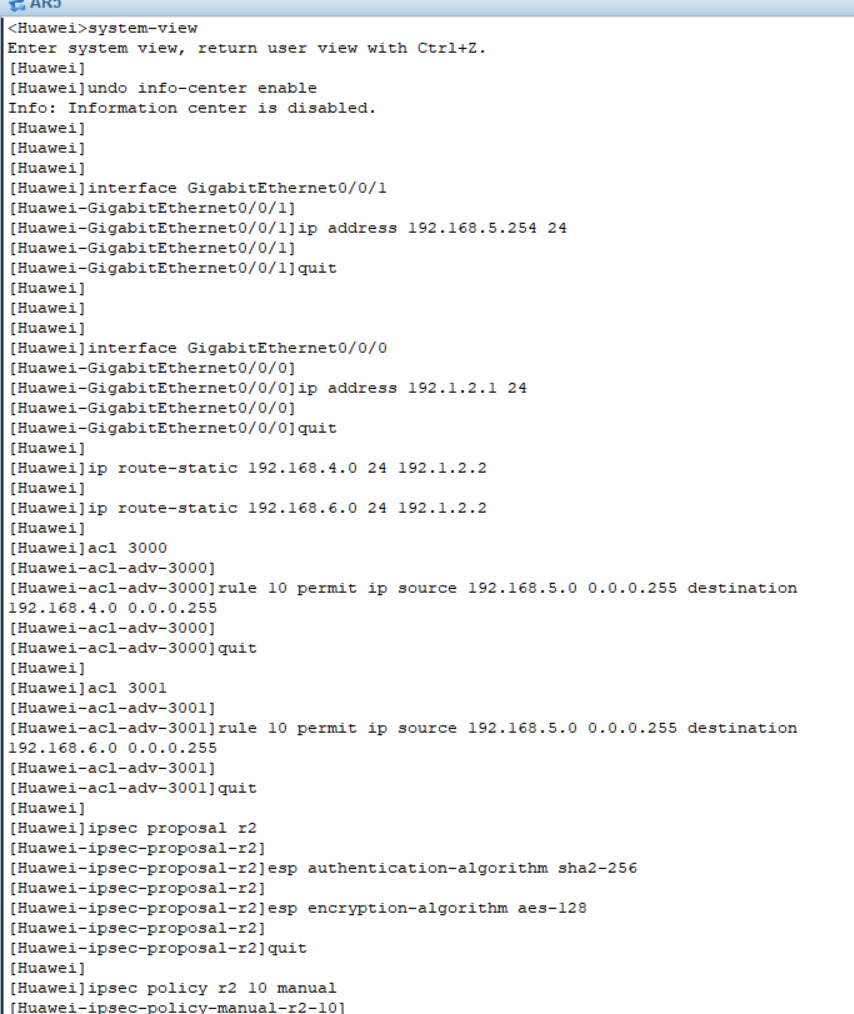


1. LSW7路由器配置



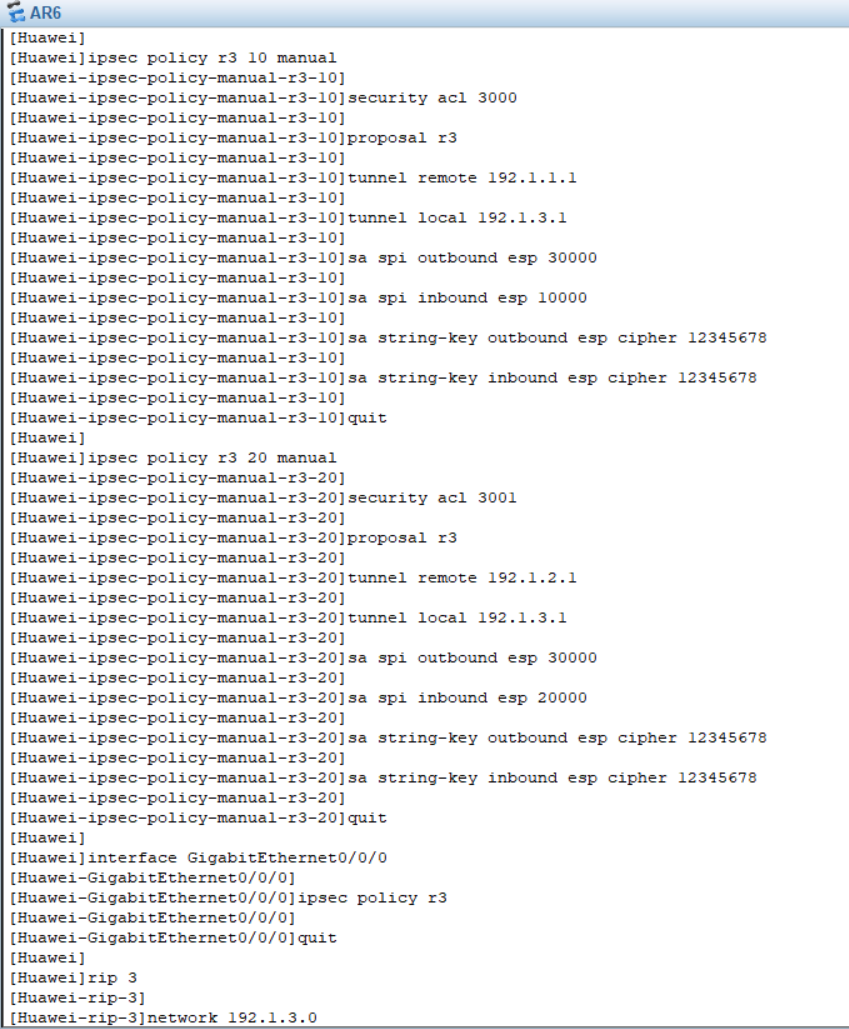
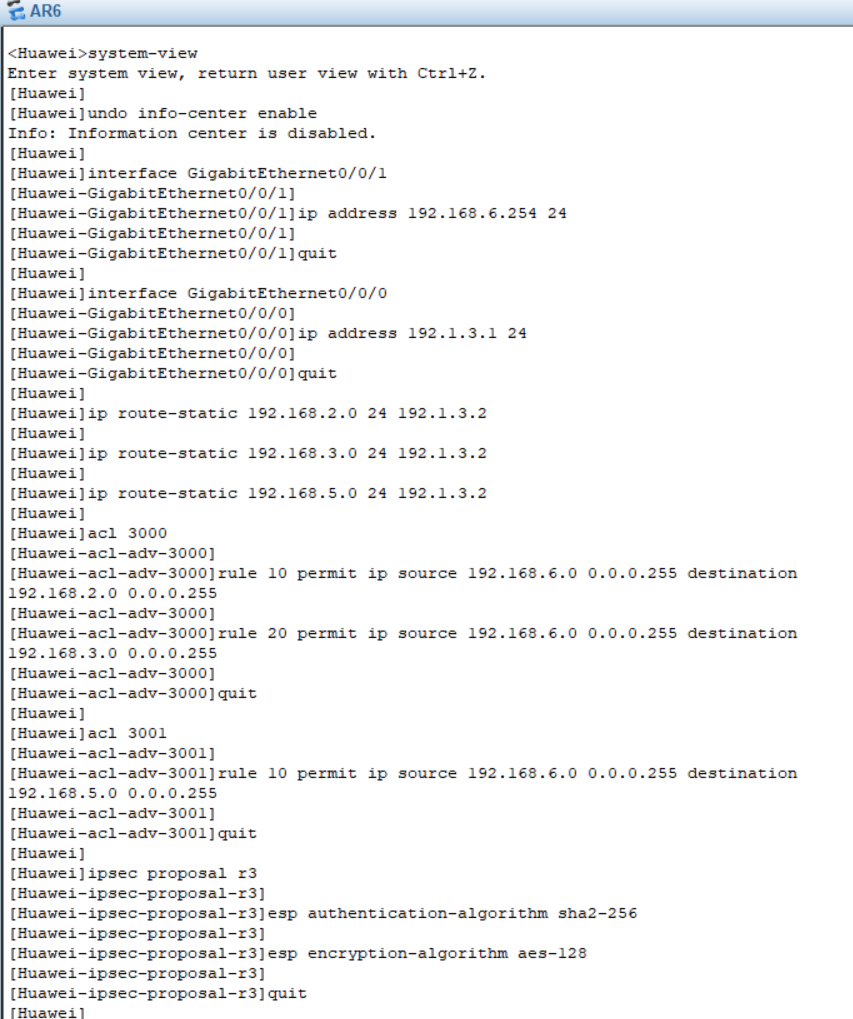
## 3.2 分公司1网络配置过程和建立Ipsec VPN隧道

1. 对PC4进行配置，设置其IP为192.168.5.1/24，子网掩码为255.255.255.0，网关为192.168.5.254。
2. 对Client4进行配置，设置其IP为192.168.5.2/24，子网掩码为255.255.255.0，网关为192.168.5.254。
3. 为了能够收到主公司内传来的数据包，还需要对主公司内的LSW2和LSW3配置对应的静态路由，其中LSW2配置命令为ip route-static 192.168.5.0 24 192.168.12.1，LSW3配置命令为ip route-static 192.168.5.0 24 192.168.23.2
4. 对路由器AR5进行配置，首先要对AR5连接公共网络Internet的接口通过手工配置安全关联相关的参数，指定安全协议ESP，ESP报文加密算法和ESP报文鉴别算法和完成ESP报文加密及ESP报文MAC计算时使用的密钥。然后通过分类规则，指定经过IPSec隧道传输的是内部网络各个子网之间传输的IP分组，即源IP地址和目的IP地址为内部网络私有IP地址的IP分组，这里设置为源IP地址为192.168.5.0/24到目的IP地址为192.168.4.0/24和192.168.6.0/24。同时为了让路由器能够正确将内部网络私有IP地址的数据包转发到公共网络中，还需要配置静态路由项，使得路由器在接收到对应的内部网络私有IP地址数据包时能正确转发到对应的接口上,这里设置为当接收到目的IP地址为192.168.4.0/24或192.168.6.0/24的数据包时转发到IP为192.1.2.2的路由器上。最后再对该路由器自身连接公共网络Internet的接口配置IPSec策略，其中IPSec策略要求将所有内部网络各个子网间传输的IP分组封装成ESP报文隧道模式，隧道模式外层为隧道两端的全球IP地址，内部子网间传输的IP分组作为ESP报文的净荷。具体配置过程如下图所示。



## 3.2 分公司2网络配置过程和建立Ipsec VPN隧道

1. 对PC5进行配置，设置其IP为192.168.6.1/24，子网掩码为255.255.255.0，网关为192.168.6.254。
2. 对Client5进行配置，设置其IP为192.168.6.2/24，子网掩码为255.255.255.0，网关为192.168.6.254。
3. 为了能够收到主公司内传来的数据包，还需要对主公司内的LSW2和LSW3配置对应的静态路由，其中LSW2配置命令为ip route-static 192.168.6.0 24 192.168.12.1，LSW3配置命令为ip route-static 192.168.6.0 24 192.168.23.2
4. 对路由器AR6进行配置，对AR6连接公共网络Internet的接口指定安全协议ESP，ESP报文加密算法和ESP报文鉴别算法和完成ESP报文加密及ESP报文MAC计算时使用的密钥。然后通过分类规则，指定经过IPSec隧道传输的是内部网络各个子网之间传输的IP分组，这里设置为源IP地址为192.168.6.0/24到目的IP地址为192.168.2.0/24和192.168.3.0/24。然后再配置静态路由项，这里设置为当接收到目的IP地址为192.168.2.0/24或192.168.3.0/24的数据包时转发到IP为192.1.3.2的路由器上。最后再对该路由器自身连接公共网络Internet的接口配置IPSec策略，其中IPSec策略要求将所有内部网络各个子网间传输的IP分组封装成ESP报文隧道模式，隧道模式外层为隧道两端的全球IP地址，内部子网间传输的IP分组作为ESP报文的净荷。具体配置过程如下图所示。

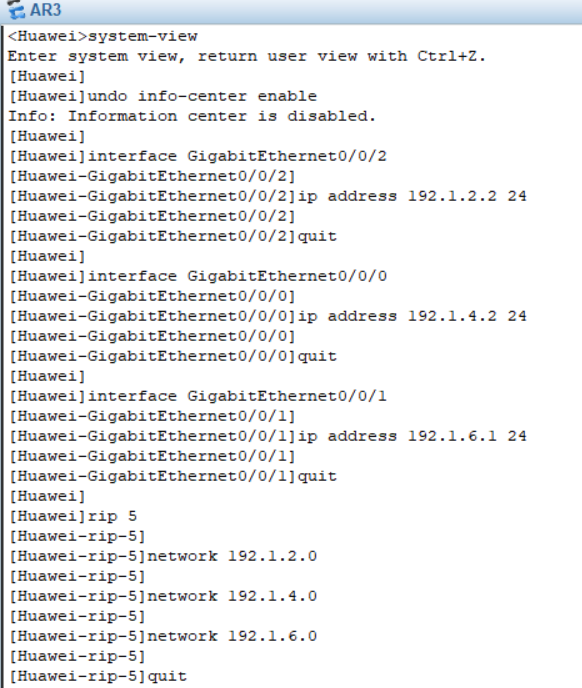


## 3.2 公共网络Internet配置过程

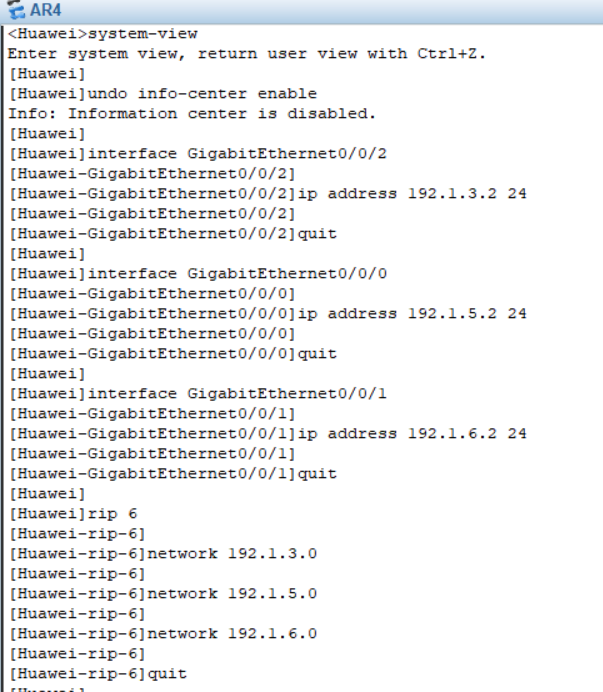
1. 首先对AR2进行对应的配置，在GigabitEthernet0/0/0接口上绑定IP地址192.1.1.2，在GigabitEthernet0/0/1接口上绑定IP地址192.1.4.1，在GigabitEthernet0/0/2接口上绑定IP地址192.1.5.1，最后再对这些接口启用RIP协议。具体配置过程如下图所示。



1. 然后对AR3进行对应的配置，在GigabitEthernet0/0/2接口上绑定IP地址192.1.2.2，在GigabitEthernet0/0/0接口上绑定IP地址192.1.4.2，在GigabitEthernet0/0/1接口上绑定IP地址192.1.6.1，最后再对这些接口启用RIP协议。具体配置过程如下图所示。



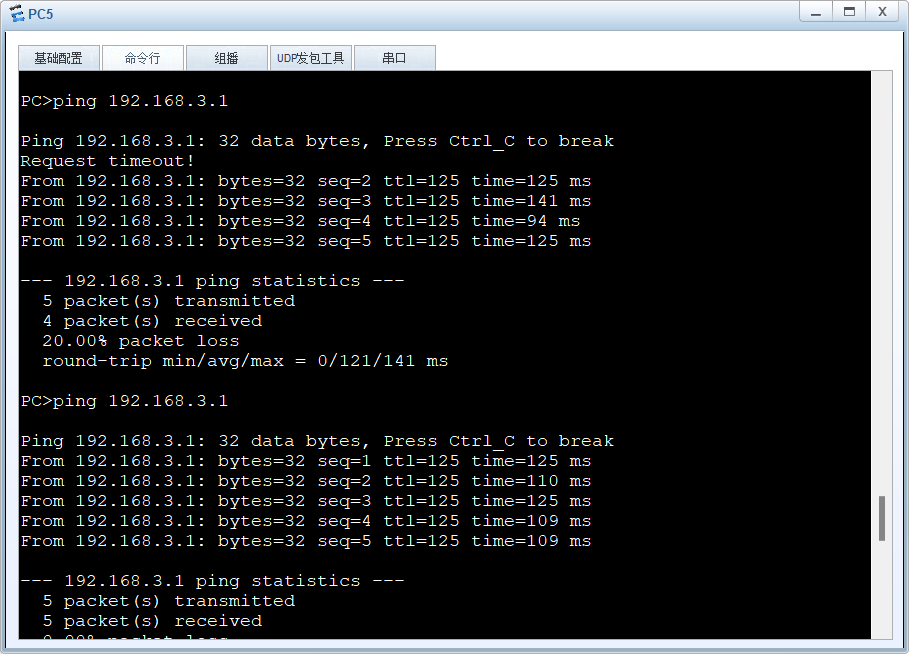
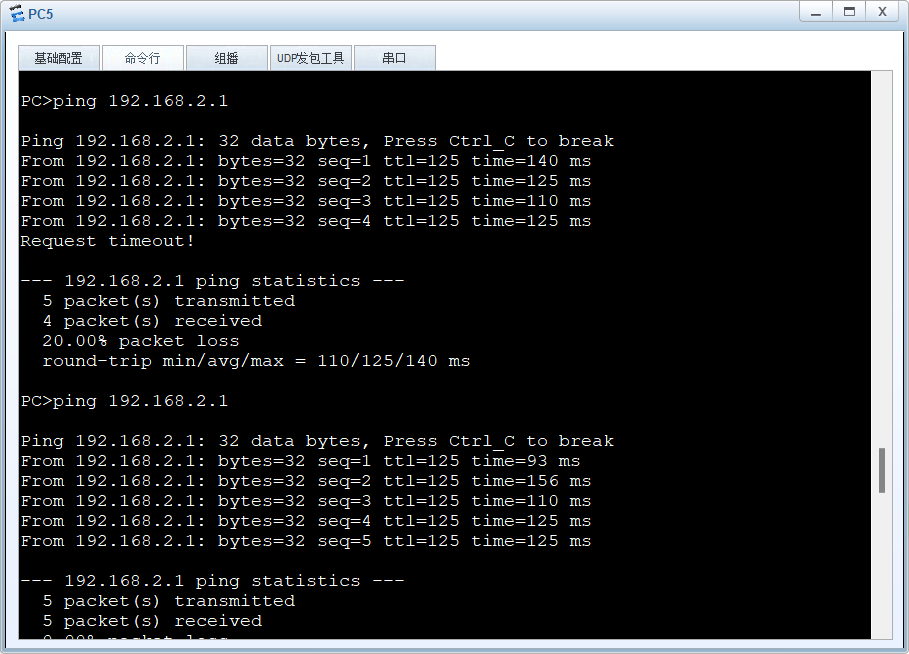
1. 最后对AR4进行对应的配置，在GigabitEthernet0/0/0接口上绑定IP地址192.1.5.2，在GigabitEthernet0/0/1接口上绑定IP地址192.1.6.2，在GigabitEthernet0/0/2接口上绑定IP地址192.1.3.2，最后再对这些接口启用RIP协议。具体配置过程如下图所示。



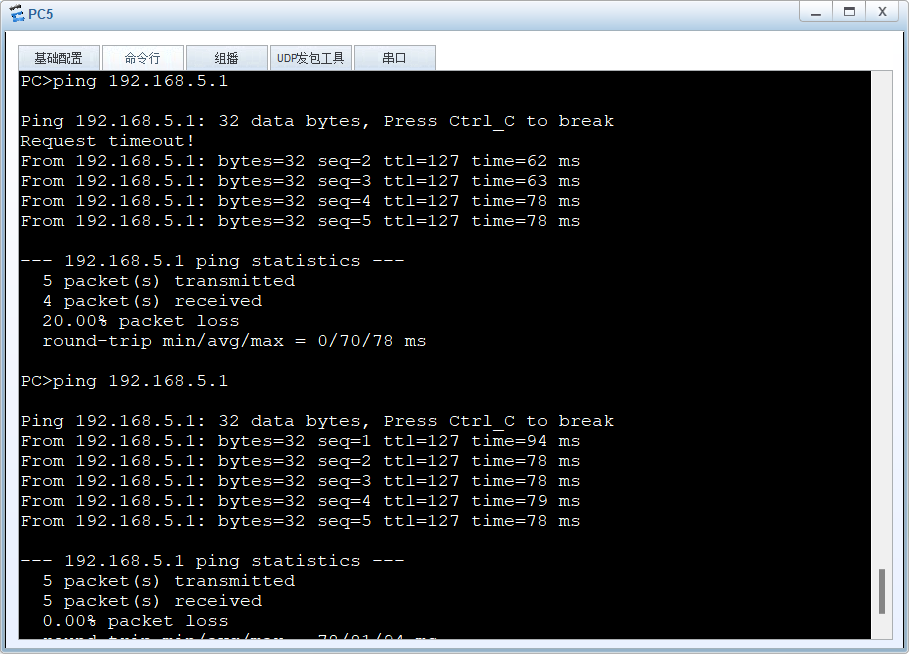
# 第四章 项目测试过程

## 4.1 对分公司与分公司、分公司与总公司之间进行连通性测试

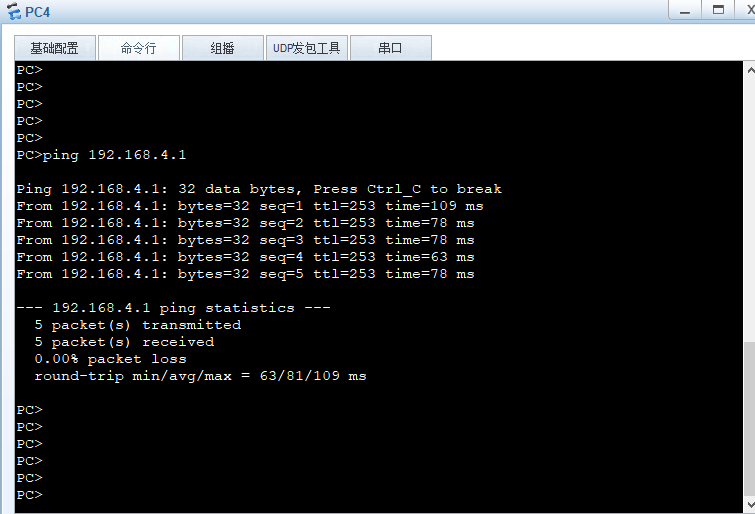
1. 令分公司2的设备Ping主公司中网段为192.168.2.0/24和192.168.3.0/24的设备。



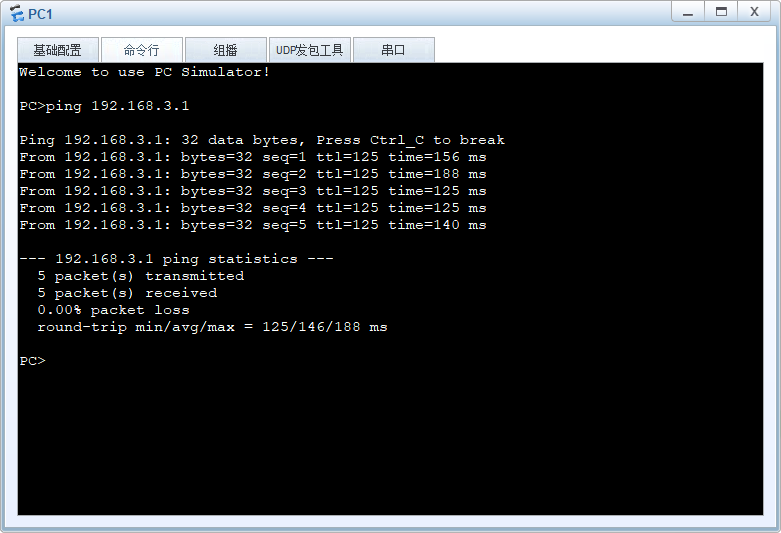
1. 令分公司2的设备Ping分公司1的设备



1. 令分公司1的设备Ping主公司网段为192.168.4.0/24的设备



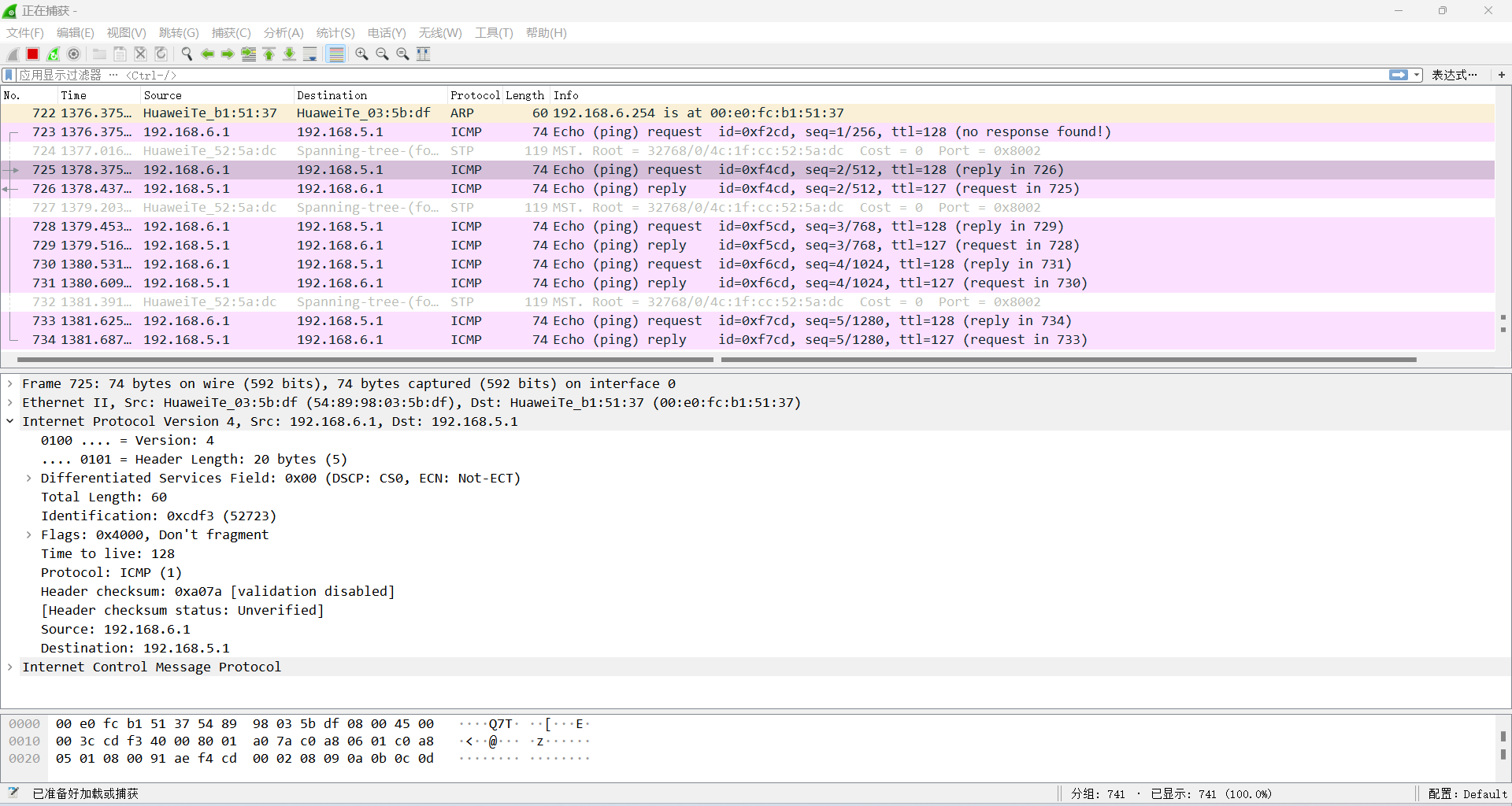
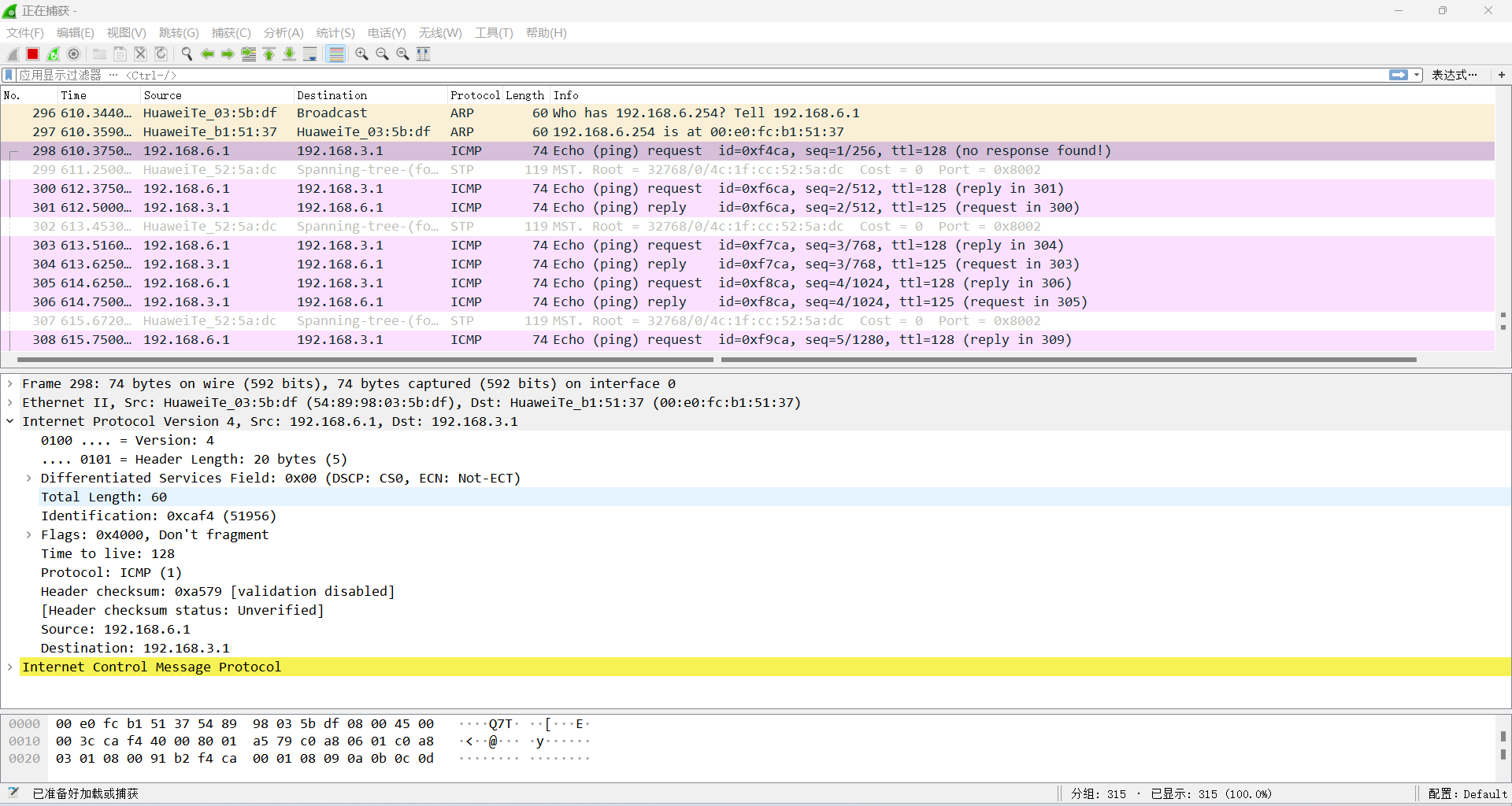
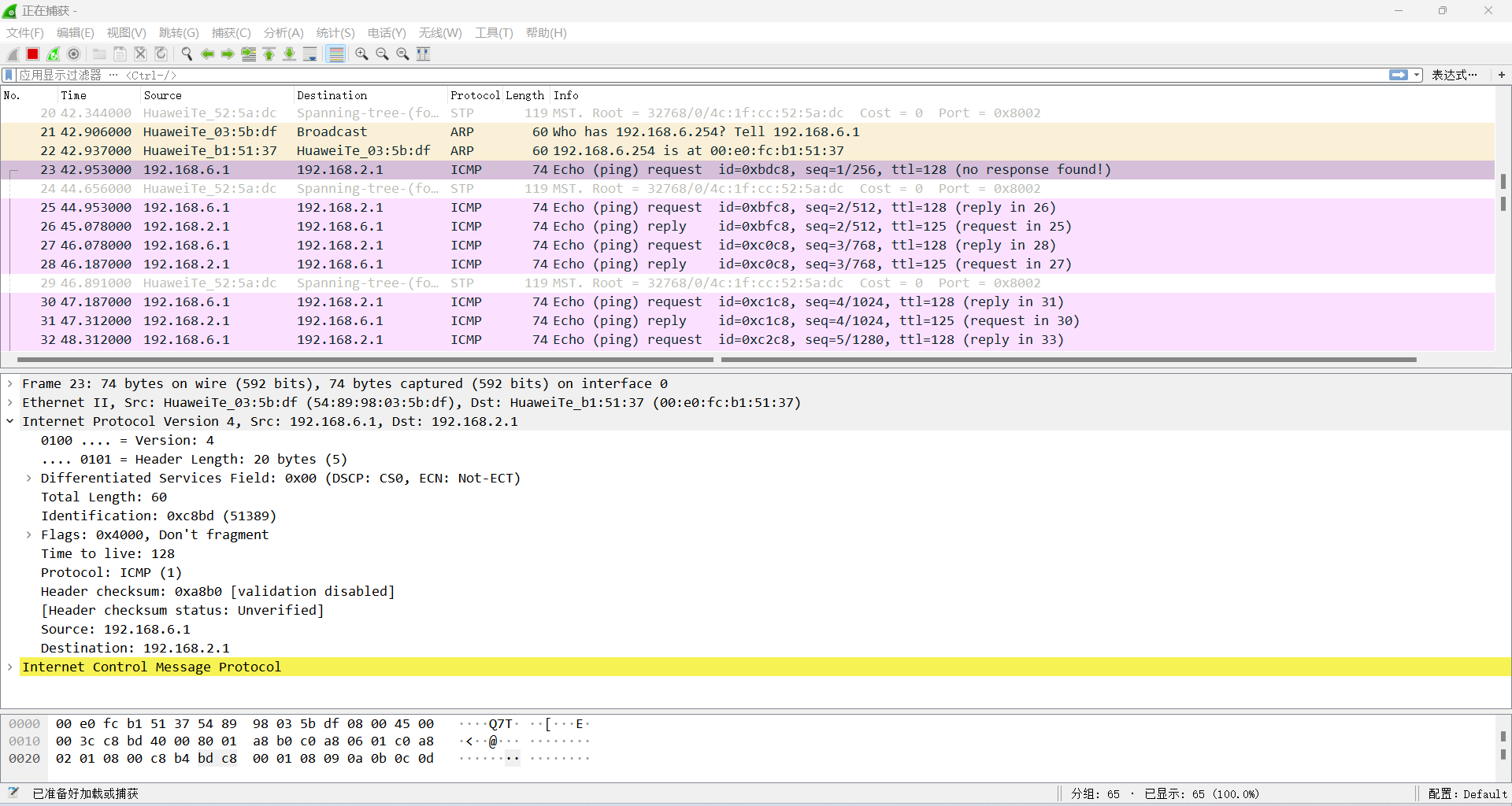
1. 主公司内设置连通性测试，令网段为192.168.1.0/24的PC1去Ping网段为192.168.3.0/24的设备PC3



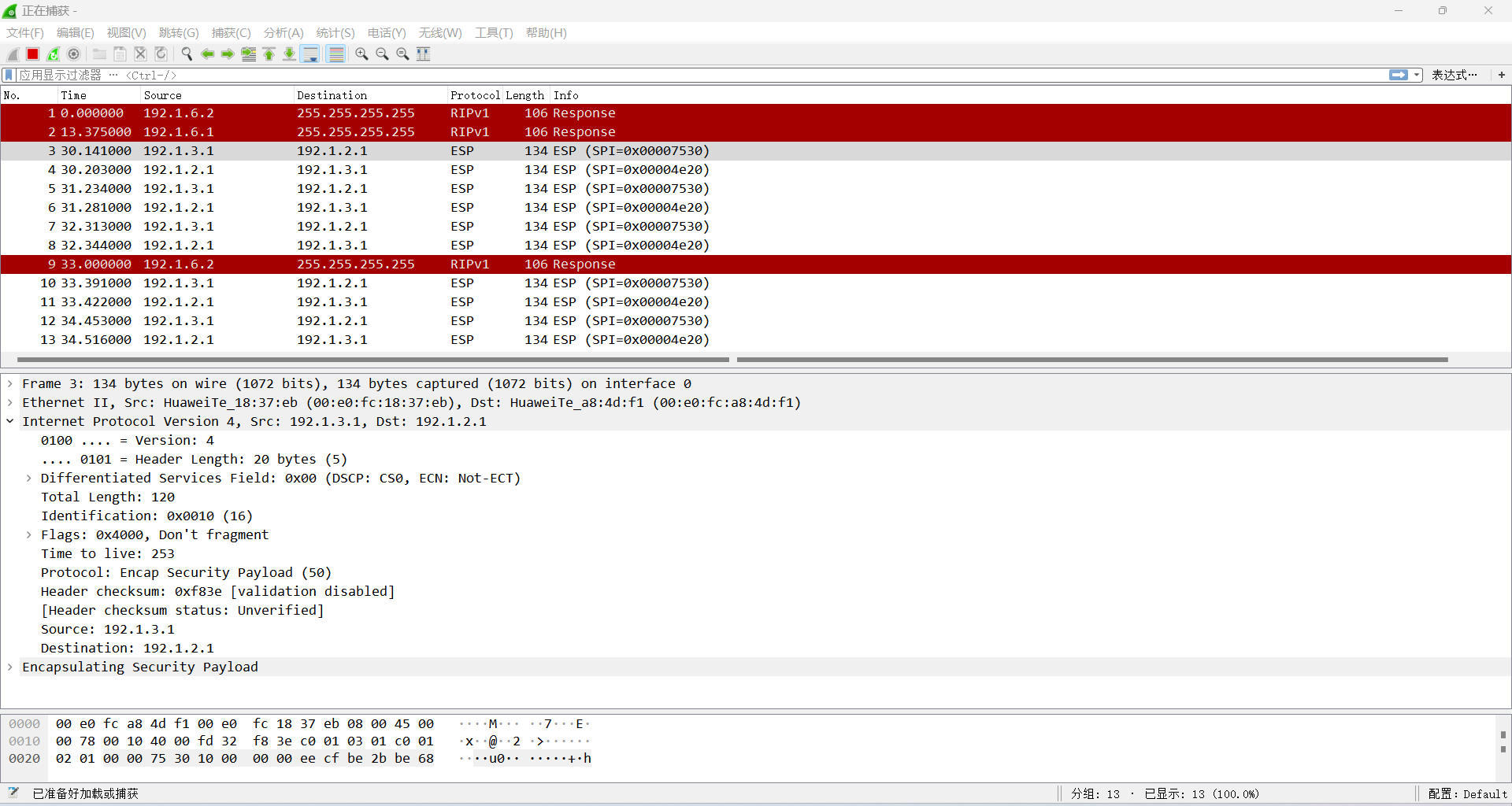
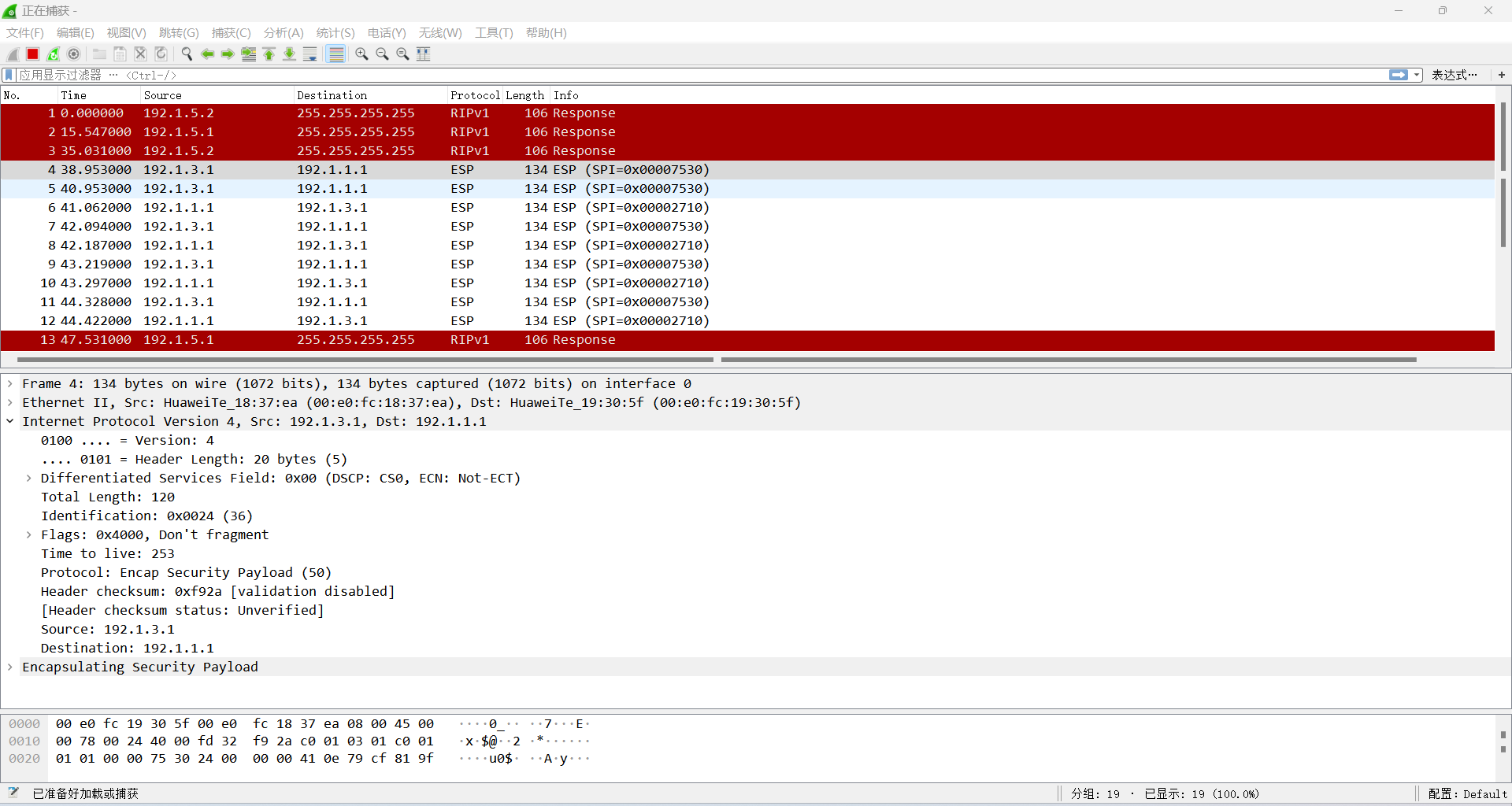
## 4.2 对VPN隧道传输过程进行抓包分析

1. 令分公司2的设备Ping主公司中网段为192.168.2.0/24和192.168.3.0/24的设备。然后再Ping分公司1中网段为192.168.5.0/24的设备。

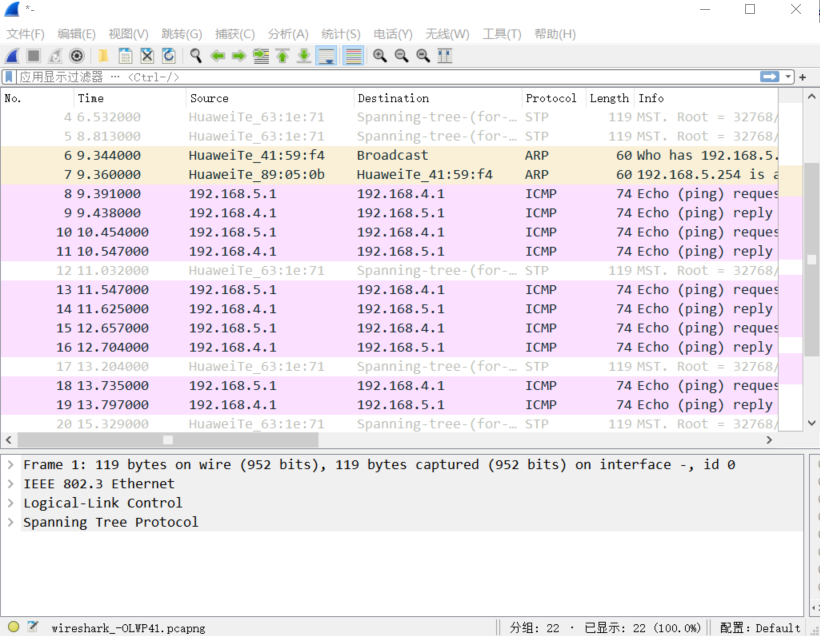
先在AR6连接内部网络的接口处进行抓包



然后在AR1连接公共网络的接口上抓包



1. 令分公司1中设备Ping主公司中网段为192.168.4.0/24的设备。然后在AR5连接内部网络的接口处进行抓包。



再对AR1连接公共网络处的接口处进行抓包

