**计算机科学与技术学院**

2021－2022学年第 2 学期

**计算机科学与技术专业**

**计算机网络大作业**

**学号：200340214**

**姓名：张启知**

**任课教师：崔鸿**

难度级： A 6个知识点

项目1、含3个以上路由器将3个以上网络连通，分别配置静态路由和RIP路由协议。

项目2、一次ARP协议的完整过程的报文捕获与分析

项目3、一个 DNS 报文的完整分析

项目4、一次 TCP 传输完整过程的报文捕获与分析

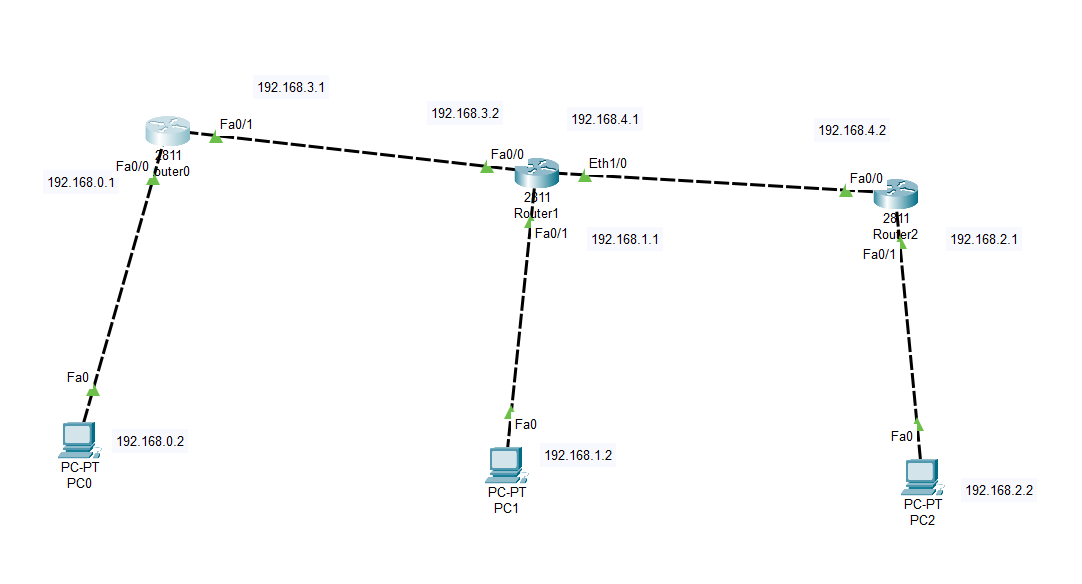
项目5、一次 HTTP 访问的完整过程的报文捕获与分析项目6、搭建 FTP 应用环境，捕获一次 FTP 文件服务的完整过程，抓包并报文

分析，或者完成 DHCP 协议完整过程的报文捕获与分析

项目1

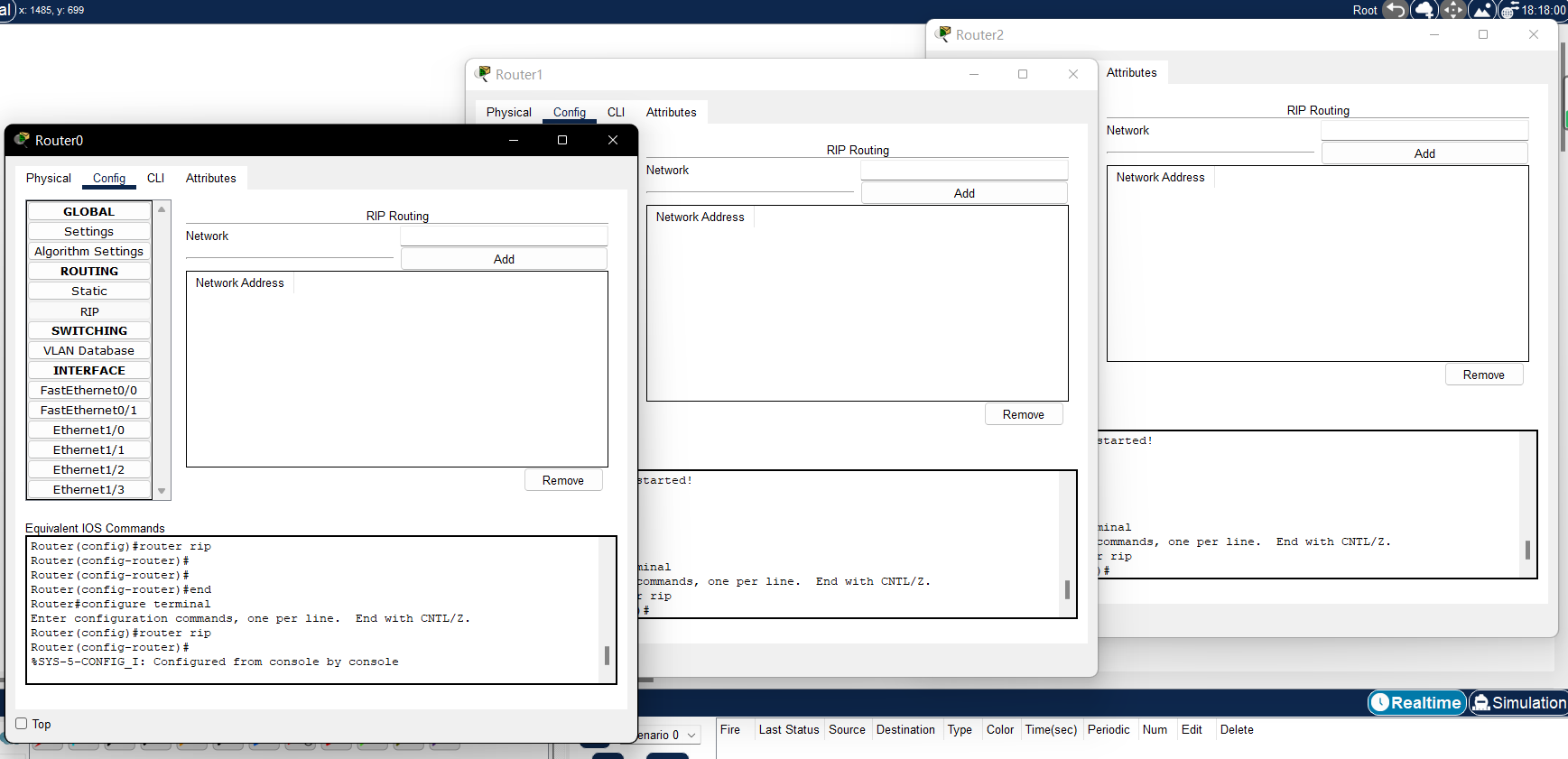
含3个以上路由器将3个以上网络连通，分别配置静态路由和RIP路由协议。

实验拓扑图如下：

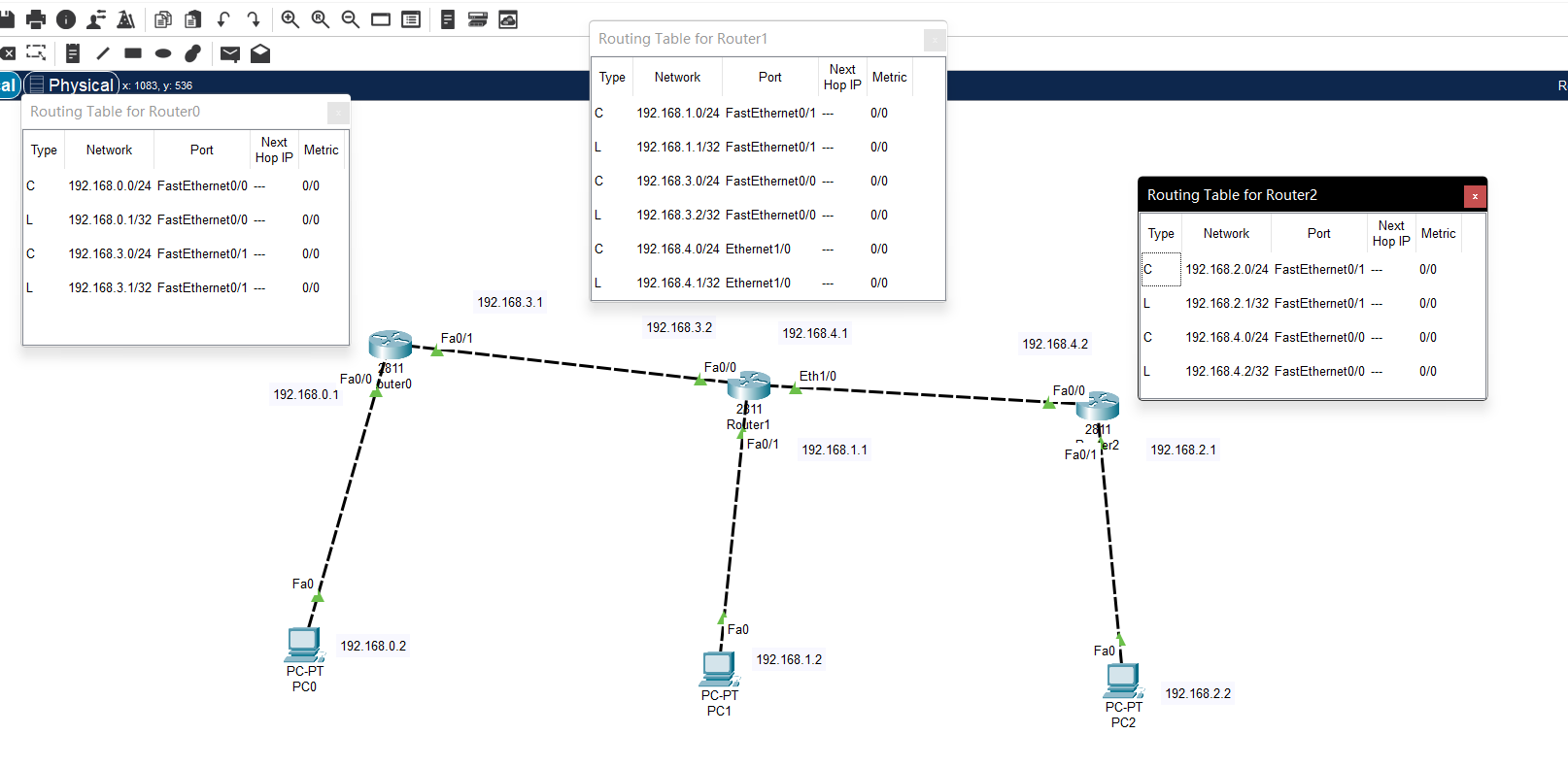


各终端及网关的IP地址如上图所示（配置过程省略）

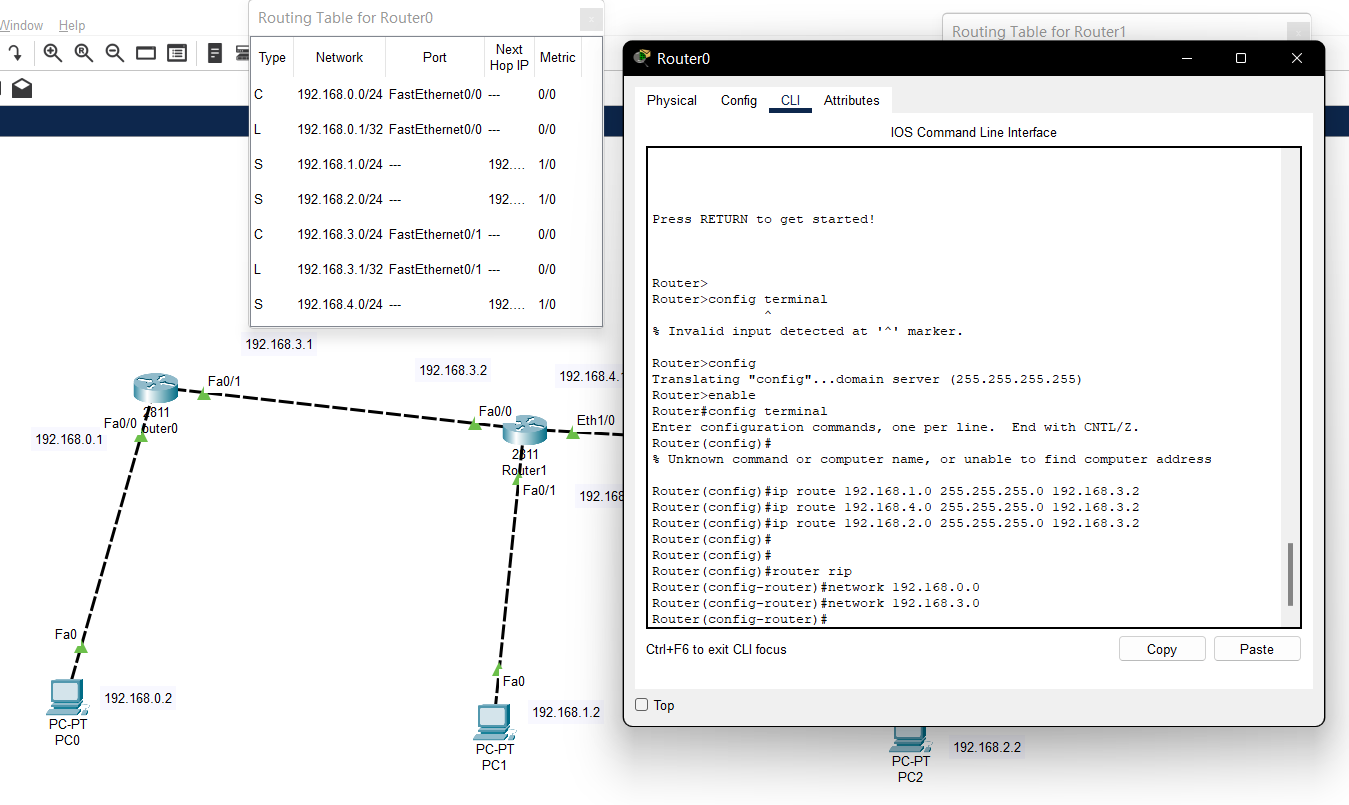
各路由器的rip在配置前的状态：



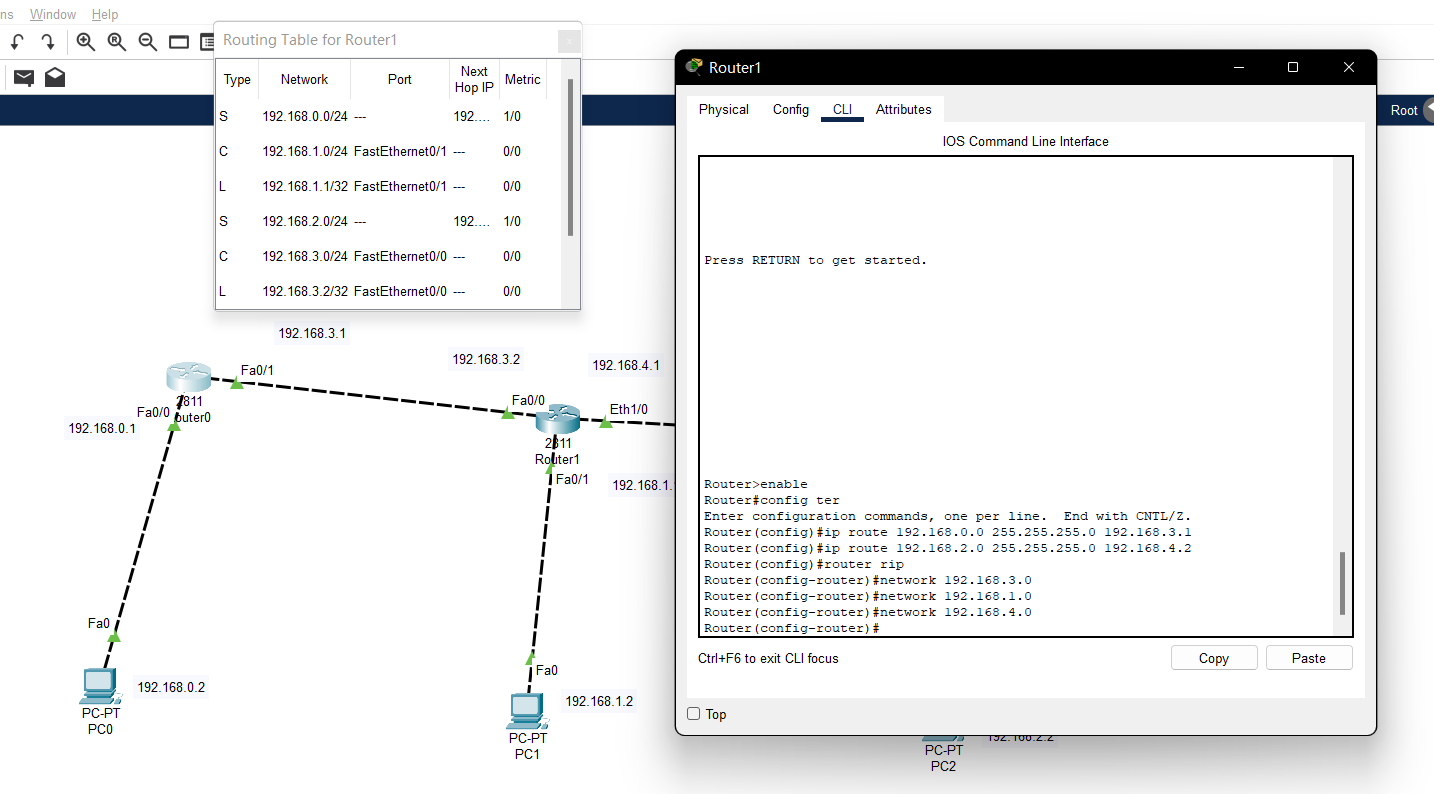
各路由器在配置下一跳前的路由表：



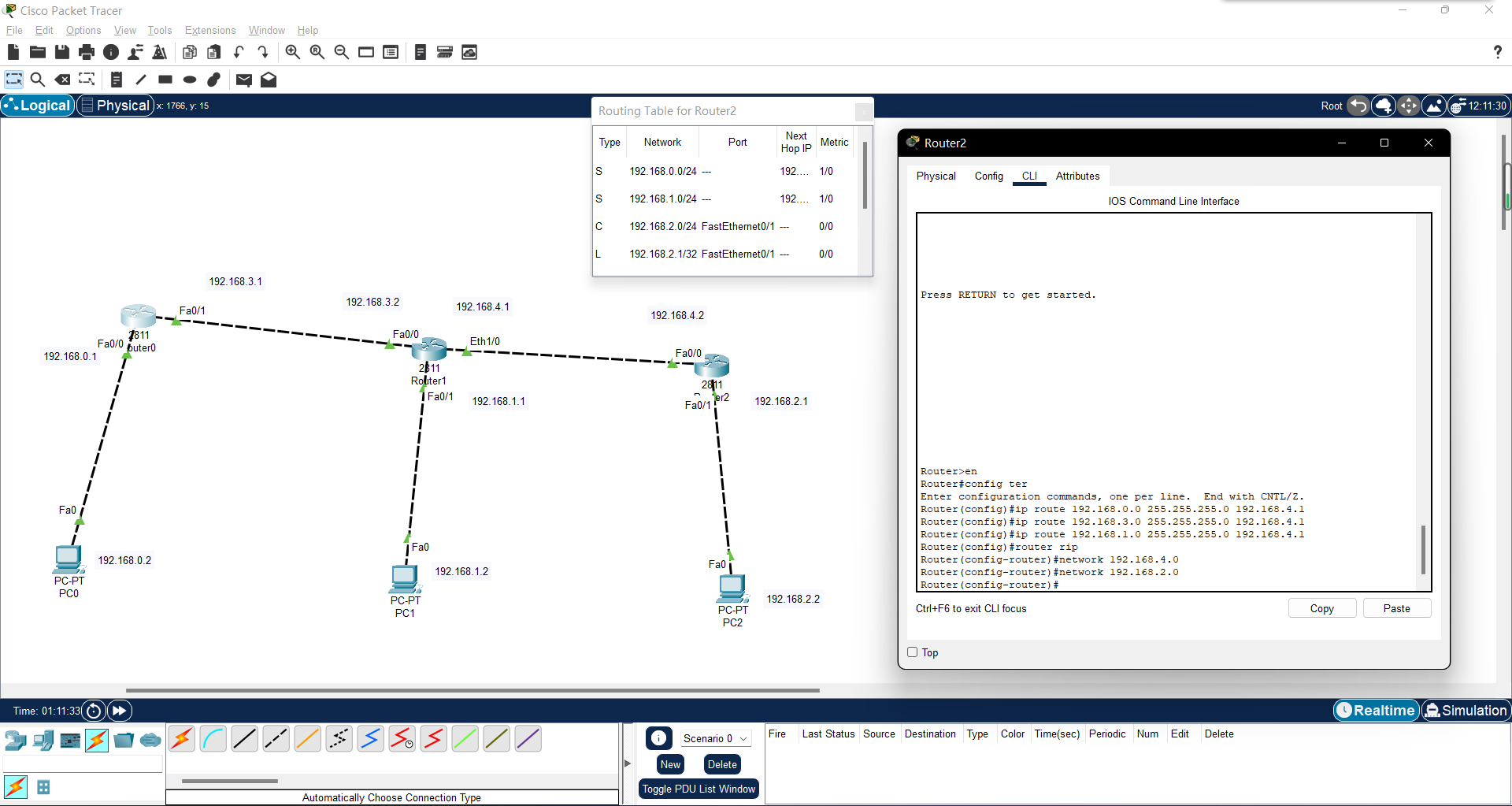
配置r0uter0的下一跳，并通告其直连网络：



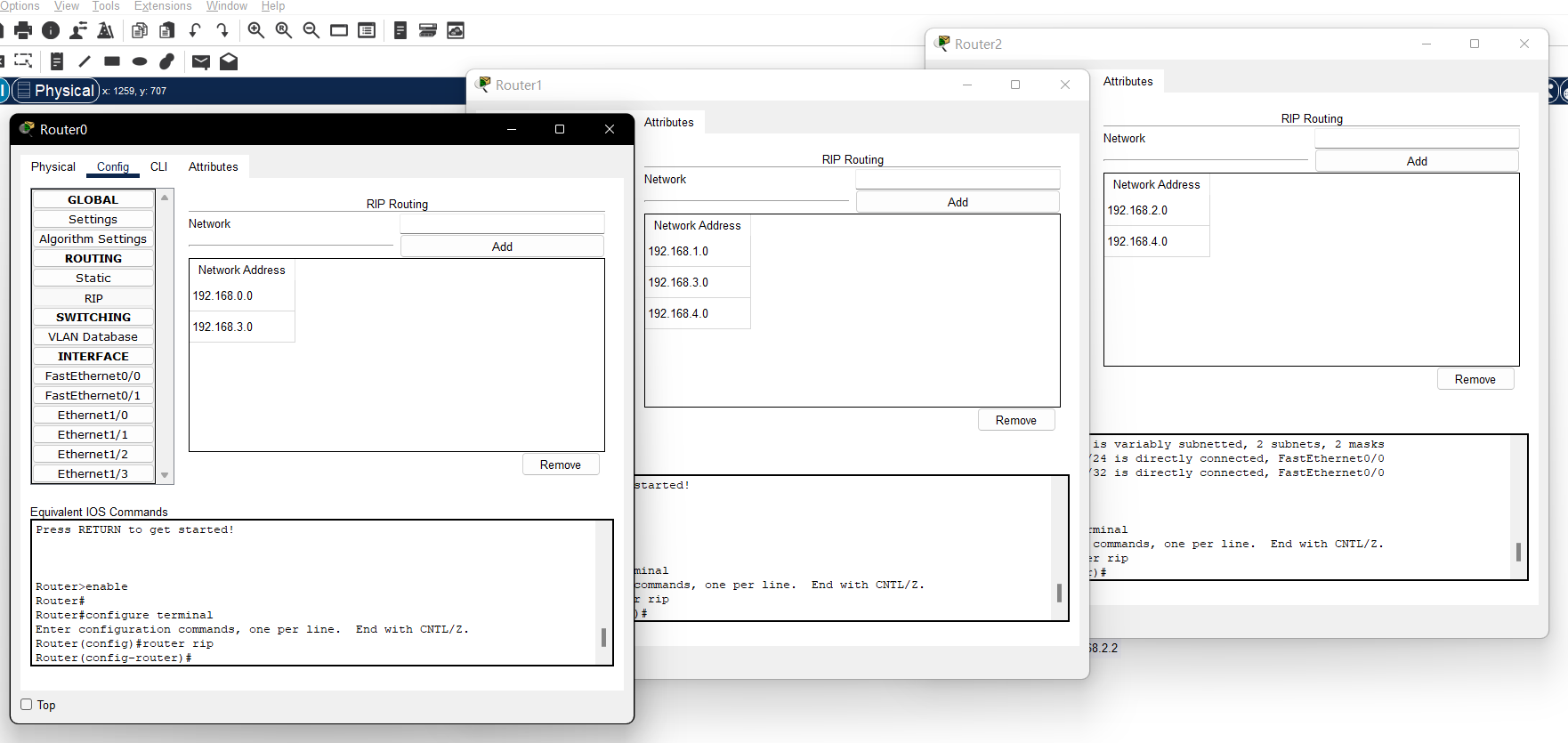
配置r0uter1的下一跳，并通告其直连网络：



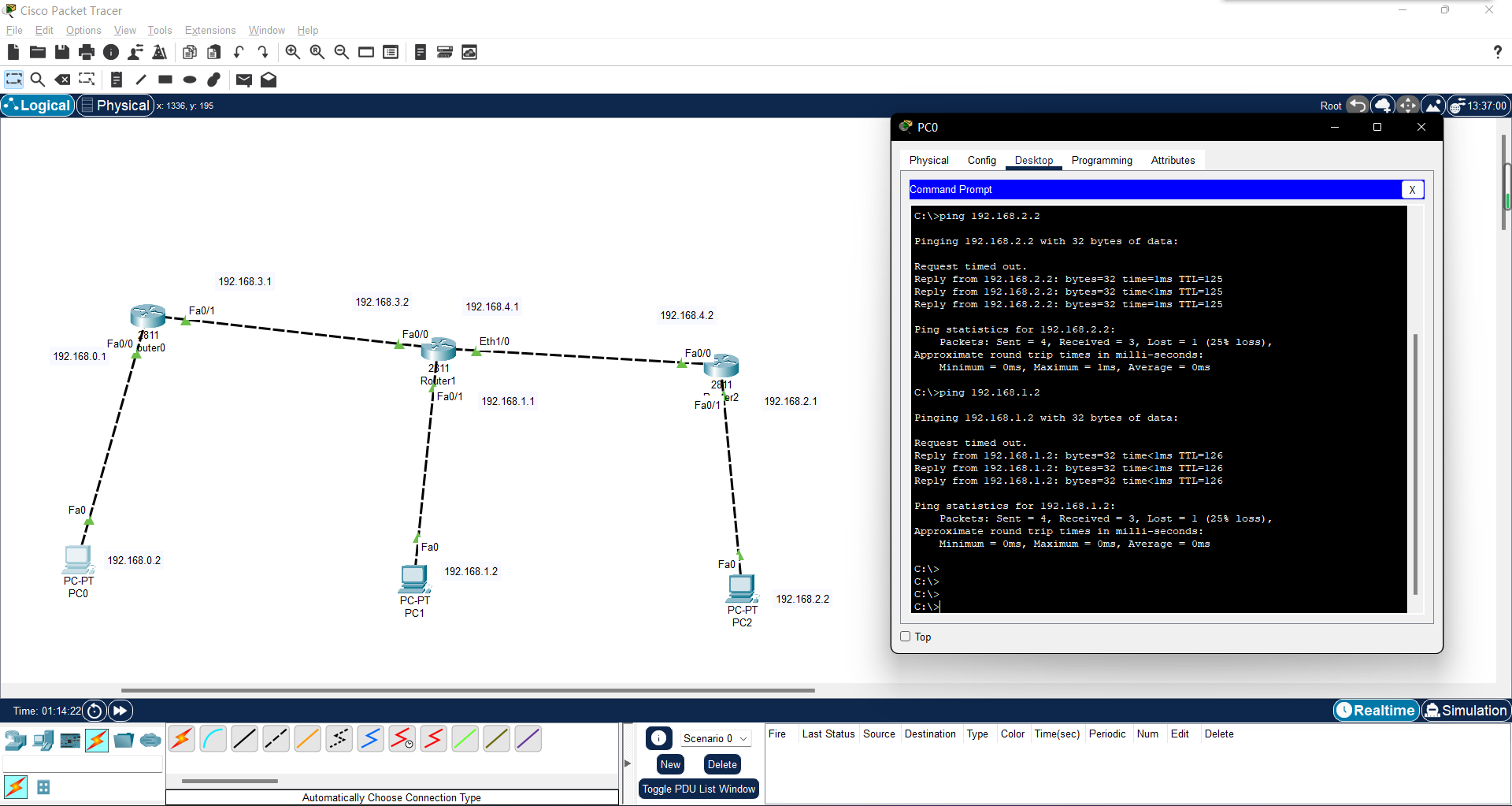
配置r0uter2的下一跳，并通告其直连网络：



各路由器的rip在配置后的状态：



测试PC0 ping PC1和PC2



第一次都超时，后三次成功ping通。

项目2

一次ARP协议的完整过程的报文捕获与分析

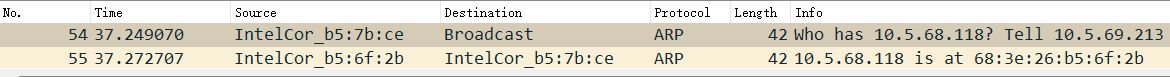
本机的IP地址为10.5.69.213

MAC地址为2c:db:07:b5:7b:ce

与另一台主机在同一网段下，另一主机的IP地址为10.5.68.118

本机的arp表无另一主机的IP地址对应的物理地址

通过ping另一主机的IP地址，用wireshark抓包，结果如下：



分析：

由于没有arp表中另一台主机的信息，所以第一个包为本机向同一网段中所有地址发送广播，询问谁是10.5.68.118？

当本网段的所有主机收到arp询问后，检查包中的想要查询的地址是否是自己的地址，若不是则直接忽略，若是，则发送arp响应包，把自己的MAC地址发送回去。

主机收到arp响应包后，将IP地址所对应的MAC地址写入arp表，若主机一直没有收到arp响应包，则表示arp查询失败。

图中第二个包则是来自10.5.68.118的arp响应包，图中的inf0信息为10.5.68.118 is at 68:3e:26:b5:6f:2b

报文分析：

（1）询问包

报文如下：

ff ff ff ff ff ff 2c db--07 b5 7b ce 08 06 00 01

08 00 06 04 00 01 2c db--07 b5 7b ce 0a 05 45 d5

00 00 00 00 00 00 0a 05--44 76

ff ff ff ff ff ff：目的地址为广播地址（全1）

2c db 07 b5 7b ce：源地址为本机的MAC地址

00 01：硬件类型，此处1表示为以太网

08 00：表示传输协议为IPv4

2c db 07 b5 7b ce：本机的MAC地址

0a 05 45 d5：本机的IP地址

00 00 00 00 00 00：目标MAC地址

0a 05 44 76：目标IP地址

（1）响应包

报文如下：

2c db 07 b5 7b ce 68 3e--26 b5 6f 2b 08 06 00 01

08 00 06 04 00 02 68 3e--26 b5 6f 2b 0a 05 44 76

2c db 07 b5 7b ce 0a 05--45 d5

2c db 07 b5 7b ce：目的地址本机地址

68 3e 26 b5 6f 2b：源地址为另一台主机的MAC地址

00 01：硬件类型，此处1表示为以太网

08 00：表示传输协议为IPv4

68 3e 26 b5 6f 2b：发送方的MAC地址

0a 05 44 76：发送方的IP地址

2c db 07 b5 7b ce：目标MAC地址

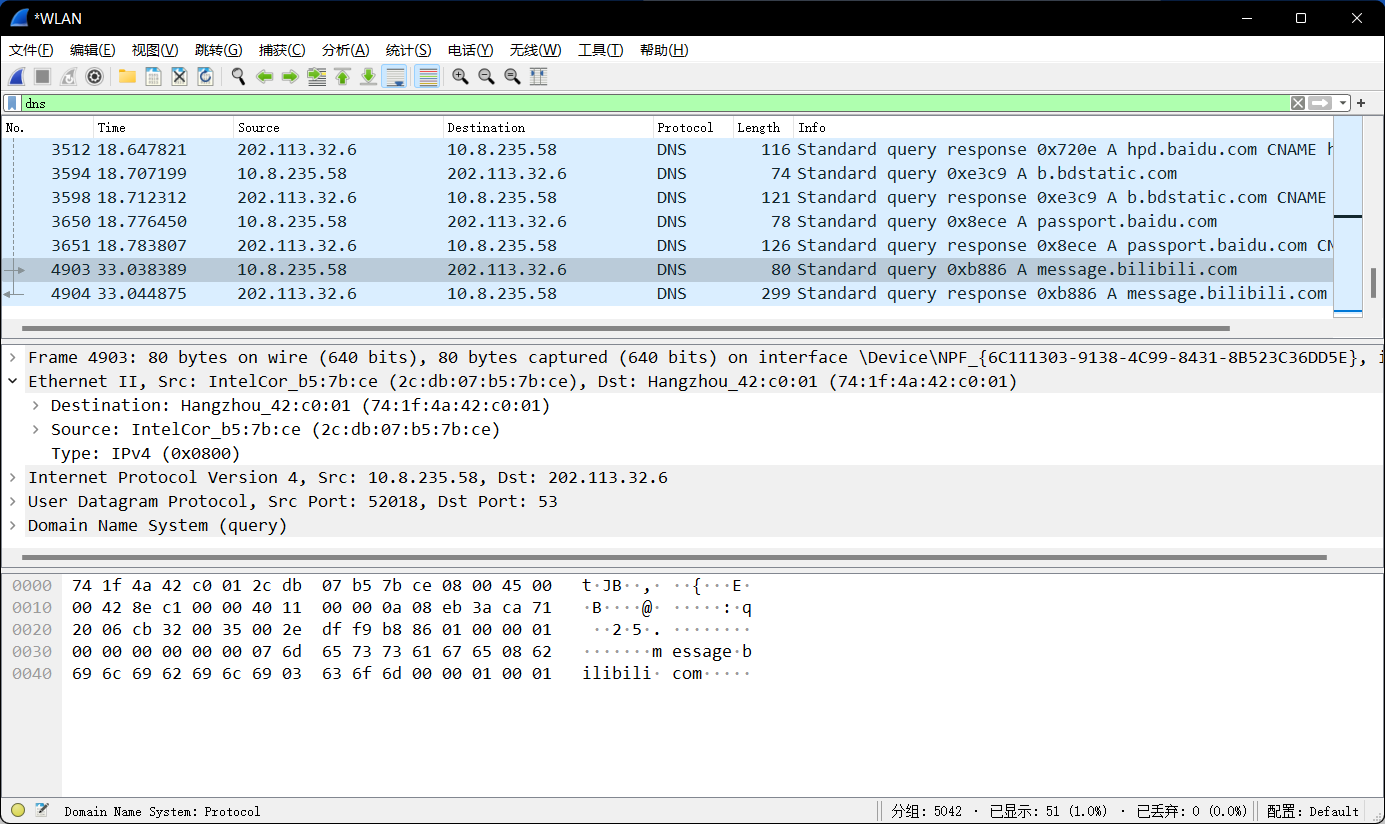
0a 05 45 d5：目标IP地址

项目3

一个 DNS 报文的完整分析

首先打开wireshark监听，在打开浏览器访问[www.bilibilib.c0m](http://www.bilibilib.com)

从wireshark中找到访问帧与应答帧（如下图）：



报文信息如下：

74 1f 4a 42 c0 01 2c db--07 b5 7b ce 08 00 45 00

00 42 8e c1 00 00 40 11--00 00 0a 08 eb 3a ca 71

20 06 cb 32 00 35 00 2e--df f9 b8 86 01 00 00 01

00 00 00 00 00 00 07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00 00 01 00 01

解析：

74 1f 4a 42 c0 01 2c db--07 b5 7b ce 08 00 45 00

00 42 8e c1 00 00 40 11--00 00 0a 08 eb 3a ca 71

20 06 cb 32 00 35 00 2e--df f9 b8 86 01 00 00 01

00 00 00 00 00 00 07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00 00 01 00 01

黄色高亮部分为MAC帧中目标地址，绿色高亮部分为MAC帧中源地址，

红色高亮0800表示类型为IPv4

74 1f 4a 42 c0 01 2c db--07 b5 7b ce 08 00 45 00

00 42 8e c1 00 00 40 11--00 00 0a 08 eb 3a ca 71

20 06 cb 32 00 35 00 2e--df f9 b8 86 01 00 00 01

00 00 00 00 00 00 07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00 00 01 00 01

红色高亮4表示Internet协议版本号为4，绿色高亮5表示首部长度为5个字节，

00表示区分服务

00 42表示总长度为66

8e c1表示标识

74 1f 4a 42 c0 01 2c db--07 b5 7b ce 08 00 45 00

00 42 8e c1 00 00 40 11--00 00 0a 08 eb 3a ca 71

20 06 cb 32 00 35 00 2e--df f9 b8 86 01 00 00 01

00 00 00 00 00 00 07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00 00 01 00 01

00 00表示标志和片偏移

40表示生存时间为64

11表示传输协议UDP

00 00表示首部检验和

0a 08 eb 3a表示源地址

ca 71 20 06表示目标地址

74 1f 4a 42 c0 01 2c db--07 b5 7b ce 08 00 45 00

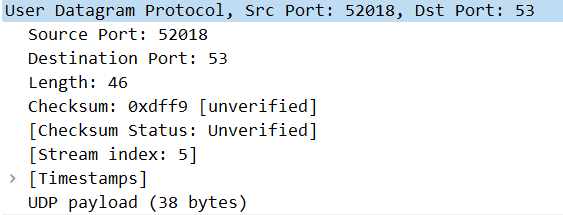
00 42 8e c1 00 00 40 11--00 00 0a 08 eb 3a ca 71

20 06 cb 32 00 35 00 2e--df f9 b8 86 01 00 00 01

00 00 00 00 00 00 07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00 00 01 00 01

绿色高亮为UDP协议：



74 1f 4a 42 c0 01 2c db--07 b5 7b ce 08 00 45 00

00 42 8e c1 00 00 40 11--00 00 0a 08 eb 3a ca 71

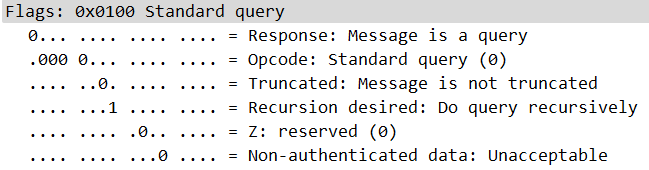
20 06 cb 32 00 35 00 2e--df f9 b8 86 01 00 00 01

00 00 00 00 00 00 07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00 00 01 00 01

b8 86表示事物ID

01 00表示报文中的标志字段具体如下：



分别为：

QR字段0，0pc0de字段0，TC字段0，RD字段1，保留字段0，保留字段0

00 01表示问题计数，这里只有一个问题

00 00 00 00 00 00这三个字节分别表示回答资源记录数，权威名称服务器计数，附加资源记录数

74 1f 4a 42 c0 01 2c db--07 b5 7b ce 08 00 45 00

00 42 8e c1 00 00 40 11--00 00 0a 08 eb 3a ca 71

20 06 cb 32 00 35 00 2e--df f9 b8 86 01 00 00 01

00 00 00 00 00 00 07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00 00 01 00 01

接下来是问题部分

07 6d--65 73 73 61 67 65 08 62

69 6c 69 62 69 6c 69 03--63 6f 6d 00表示查询的message.bilibili,c0m的ACSCII码

00 01表示查询类型字段为A类型

00 01表示查询类字段，这里是互联网地址

项目4

一次 TCP 传输完整过程的报文捕获与分析

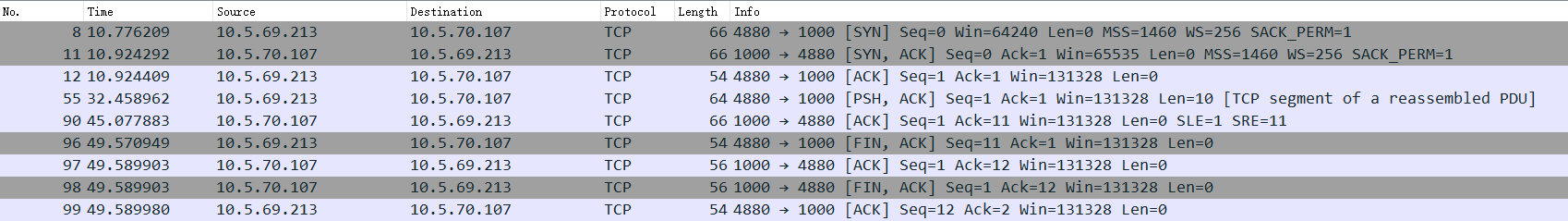
本机的IP地址为10.5.69.213

建立连接的主机的IP地址为10.5.70.107

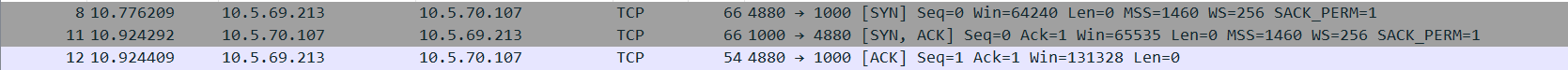
本机作为客户端，对方作为服务器端口为1000

本机成功建立连接后发送文本1928374655

用wireshark抓包如下图：



其中前三个：



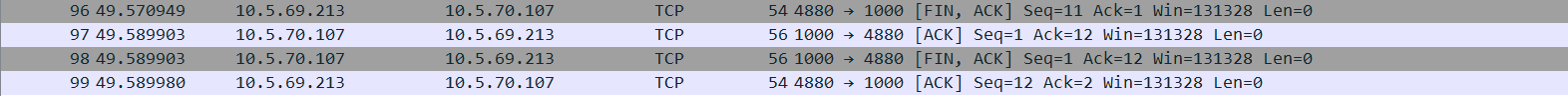
为tcp的建立过程，三次握手

中间两个：



是本机发送的数据包，以及对方的确认包ack

最后四个包：



是带有FIN标识的断开连接，释放主机资源，四次挥手

报文分析：

由于都属于TCP报文格式，所以这里选择发送数据的包作为例子分析

报文如下：

e8 6f 38 4c b9 7f 2c db--07 b5 7b ce 08 00 45 00

00 32 29 26 40 00 40 06--00 00 0a 05 45 d5 0a 05

46 6b 13 10 03 e8 fb 7b--5e fe e1 85 09 c6 50 18

02 01 a0 6e 00 00 31 39--32 38 33 37 34 36 35 35

其中绿色高亮部分为tcp报文数据，红色高亮为发送数据

Tcp报文数据分析：

13 10为发送方端口

03 e8为接收方端口

fb 7b 5e fe为序号

e1 85 09 c6为确认号

50为头部长度

18为flag标识

02 01为窗口大小

a0 6e为首部校验和

00 00为紧急指针

数据报文分析：

31 39 32 38 33 37 34 36 35 35为发送的数据1928374655文本的ASCII码

项目5

一次 HTTP 访问的完整过程的报文捕获与分析

一次HTTP完整的访问过程包括：

1.域名解析（DNS解析，在之前的项目中已经分析过了，这里不做分析）

2.TCP三次握手（同上）

3.发起HTTP请求，等待服务器响应，浏览器解析接受到的数据

4.TCP四次挥手（同上）

发起HTTP请求分析：

HTTP请求报文由三部分组成：请求行，请求头和请求正文

请求行：用于描述客户端的请求方式，请求的资源名称以及使用的HTTP协议的版本号

请求头：用于描述客户端请求哪台主机，以及客户端的一些环境信息等

请求正文：当使用POST, PUT等方法时，通常需要客户端向服务器传递数据。这些数据就储存在请求正文中

服务器响应请求过程分析：

HTTP响应也由三部分组成：状态码，响应头和实体内容

状态码：状态码用于表示服务器对请求的处理结果

列举几种常见的：200（成功）

302（临时重定向，显式重定向, Location响应首部的值为新的URL）

304（如本地缓存的资源文件和服务器上比较时，发现并没有修改，服务器返回一个304状态码， 告诉浏览器，你不用请求该资源，直接使用本地的资源即可）

403（有这个资源，但是没有访问权限）

404（服务器没有这个资源）

500（服务器内部错误）

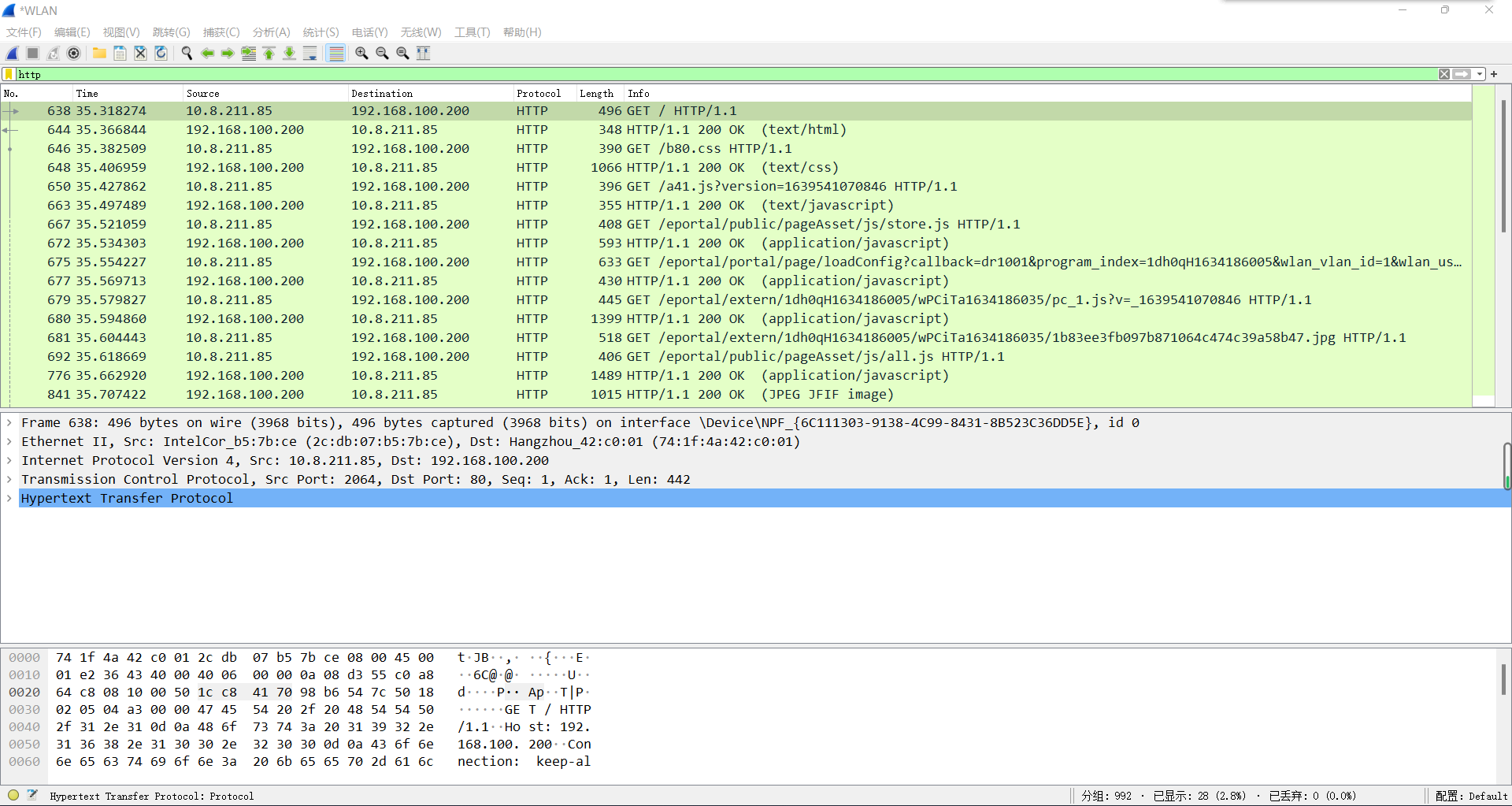
若干响应头：响应头用于描述服务器的基本信息，以及客户端如何处理数据

实体内容：服务器返回给客户端的数据

完成这些操作之后，浏览器就可以解析html代码，再对页面进行渲染。

抓包过程：

打开Wireshark并侦听， 打开chrome，访问192.168.100.200，筛选过滤条件http，捕获到的包如下：

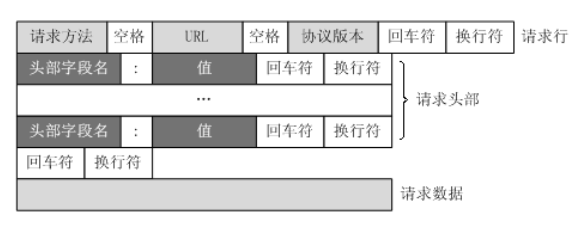


报文分析：

这里选择一个由客户端发送给服务器的请求帧，get包，进行分析



报文格式：



请求行：

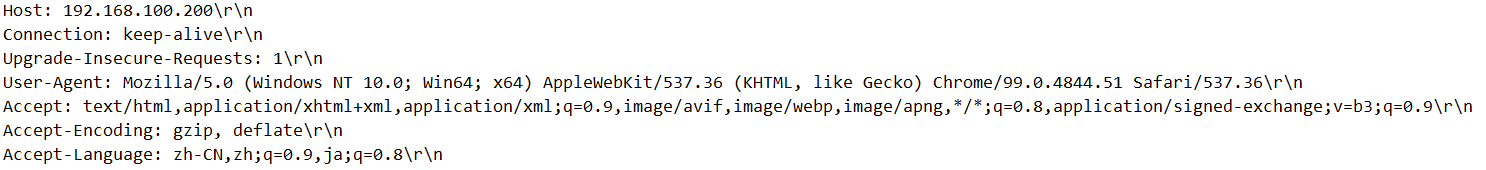
请求方法：GET

URL：空

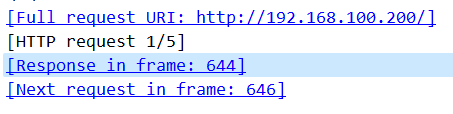
协议版本：HTTP/1.1

请求头部：

请求头部字段名：值 回车 换行（如下）



请求数据：



项目6

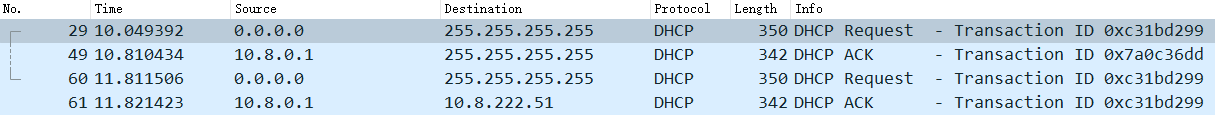
DHCP 协议完整过程的报文捕获与分析

首先打开wireshark

开始侦听，并输入筛选条件dhcp

将wifi关闭（无以太网连接），再将wifi打开，自动连接CAUC-WiFi

Wireshark捕获到的包如下：



过程分析：

1．寻找DHCP服务器

当DHCP客户端第一次登录网络的时候，计算机发现本机上没有任何IP地址设定，将以广播方式发送DHCP discover发现信息来寻找DHCP服务器，即向255.255.255.255发送特定的广播信息。网络上每一台安装了TCP/IP协议的主机都会接收这个广播信息，但只有DHCP服务器才会做出响应。

2.分配IP地址

在网络中接收到DHCP discover发现信息的DHCP服务器就会做出响应，它从尚未分配的IP地址池中挑选一个分配给DHCP客户机，向DHCP客户机发送一个包含分配的IP地址和其他设置的DHCP offer提供信息。

3.接受IP地址

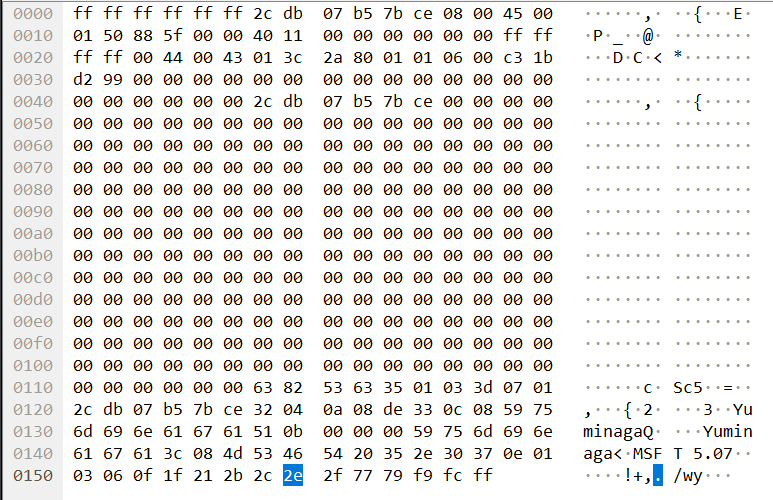
DHCP客户端接受到DHCP offer提供信息之后，选择第一个接收到的提供信息，然后以广播的方式回答一个DHCP request请求信息，该信息包含向它所选定的DHCP服务器请求IP地址的内容。

4.IP地址分配确认

当DHCP服务器收到DHCP客户端回答的DHCP request请求信息之后，便向DHCP客户端发送一个包含它所提供的IP地址和其他设置的DHCP ack确认信息，告诉DHCP客户端可以使用它提供的IP地址。然后，DHCP客户机便将其TCP/IP协议与网卡绑定，另外，除了DHCP客户机选中的DHCP服务器外，其他的DHCP服务器将收回曾经提供的IP地址。

报文分析：  
（由于都属于DHCP报文格式，所以这里选择第一个DHCP Request报文进行分析

报文如下：



DHCP Request 报文数据包是 DHCP 客户端向网络中所有 DHCP 服务器主机发出的 DHCP Request 消息。

由于此时客户端还没有真正拥有IP地址，因此源 IP 地址仍然为 0.0.0.0，该数据包是用来通知所有服务器的，以广播形式发出，因此目标 IP 地址为 255.255.255.255。

分析：

Dynamic Host Configuration Portocol (Request)

Message type: Boot Request (1) 说明：报文的操作类型, 这是一个请求包, 所以该选项的值为1

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xc31bd299 说明：事务ID

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0 说明：客户端IP地址

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: IntelCor\_b5:7b:ce (2c:db:07:b5:7b:ce)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Request)

Length: 1

DHCP: Request (3)

Option: (61) Client identifier

Length: 7

Hardware type: Ethernet (0x01)

Client MAC address: IntelCor\_b5:7b:ce (2c:db:07:b5:7b:ce)

Option: (50) Requested IP Address (10.8.222.51)

Length: 4

Requested IP Address: 10.8.222.51 说明：客户端选择租用的IP地址为10.8.222.51

…………