**《计算机网络实验》实验报告**

实验名称：基本网络工具集使用和协议数据单元（PDU）观测

姓名：胡育玮

学号：171860574

邮箱：[yeevee@qq.com](mailto:yeevee@qq.com)

班级：17级计算机科学与技术系 2 班

一、实验目的

1、初步了解如何使用VMWare搭建由虚拟机构成的拓扑网络，以及相关的网络设置（设置IP，路由规则等）

2、初步了解网关的作用及网关的设置

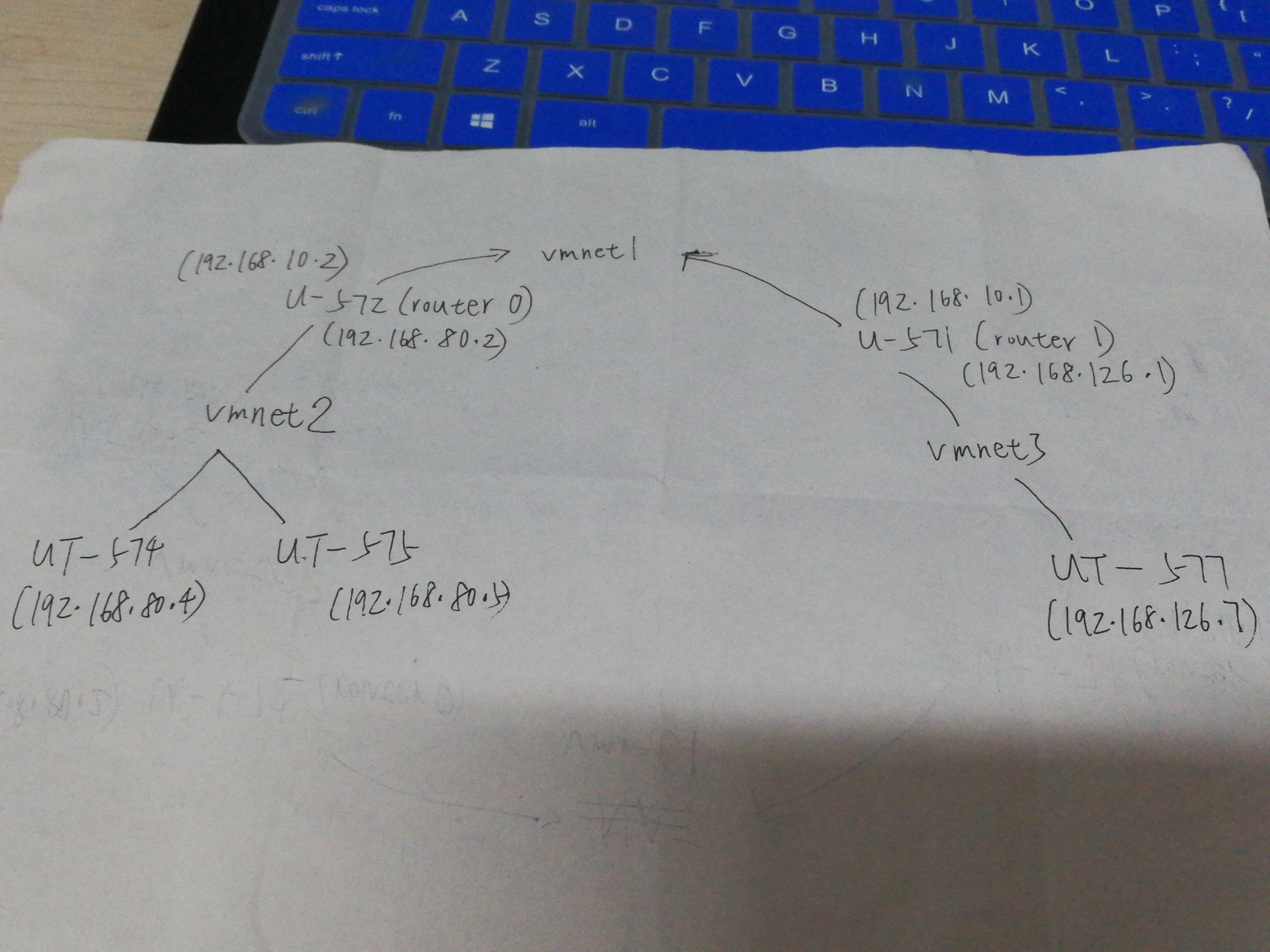
3、初步了解如何使用wireshark来观察PDU

二、网络拓扑配置

（1）表格：

|  |  |  |  |
| --- | --- | --- | --- |
| 节点名 | 虚拟设备名 | IP地址 | netmask |
| Router0 | U-572 | eth0:192.168.10.2 | 255.255.255.0 |
| eth1:192.168.80.2 | 255.255.255.0 |
| Router1 | U-571 | eth0: 192.168.10.1 | 255.255.255.0 |
| eth1: 192.168.126.1 | 255.255.255.0 |
| PC1 | UT-574 | 192.168.80.4 | 255.255.255.0 |
| PC2 | UT-575 | 192.168.80.5 | 255.255.255.0 |
| PC3 | UT-577 | 192.168.126.7 | 255.255.255.0 |

**这5个虚拟机都是从124机房的电脑上拷贝而来的。**

（2）网络拓扑结构示意图：

如上图，U-572(router0)与UT-574和UT-575通过Vmnet2连成子网2（192.168.80.xx）；U-571(router1)与UT-577通过Vmnet3连成子网3（192.168.126.xx）；U-572与U-571通过Vmnet1连成子网1（192.168.10.xx）。

（3）路由规则及网关的设置：

1. 对2个路由器router0和router1:

Router0（U-572）:

sudo service network-manager stop（关闭DHCP服务）

sudo ifconfig eth1 192.168.80.2 netmask 255.255.255.0（设置IP地址和子网掩码）

sudo ip route add 192.168.126.0/24 via 192.168.10.1（设置路由规则：从子网2到子网3的数据包的下一跳地址为192.168.10.1）

sudo su （进入root用户态）

echo 1 > /proc/sys/net/ipv4/ip\_forward （允许转发）

exit （退出root态）

执行上述语句后，Router0便设置完毕，可以工作。

Router1（U-571）：与Router0的语句形式完全一样：

sudo service network-manager stop（关闭DHCP服务）

sudo ifconfig eth1 192.168.126.1 netmask 255.255.255.0（设置IP地址和子网掩码）

sudo ip route add 192.168.80.0/24 via 192.168.10.2（设置路由规则：从子网3到子网2的数据包的下一跳地址为192.168.10.2）

sudo su （进入root用户态）

echo 1 > /proc/sys/net/ipv4/ip\_forward （允许转发）

exit （退出root态）

2. 对普通主机：PC1 – PC3

PC1（UT-574）：

sudo ifconfig eth1 192.168.80.4 netmask 255.255.255.0（设置IP地址和子网掩码）

sudo route add default gw 192.168.80.2（设置网关地址）

PC2（UT-575）：

sudo ifconfig eth1 192.168.80.5 netmask 255.255.255.0（设置IP地址和子网掩码）

sudo route add default gw 192.168.80.2（设置网关地址）

PC3（UT-577）：

sudo ifconfig eth1 192.168.126.7 netmask 255.255.255.0（设置IP地址和子网掩码）

sudo route add default gw 192.168.126.1（设置网关地址）

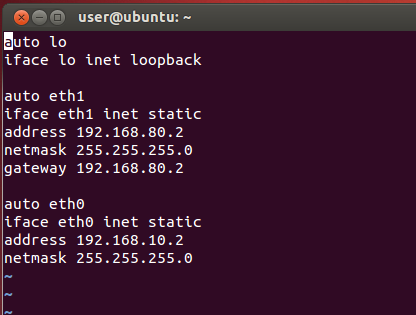
执行完上述指令，便完成了路由规则的配置。

同时，为了避免每次启动虚拟机后都要重新设置IP地址，可**将要设置的IP地址保存在特定文件中**：

对U-572（Router0）：

1 sudo vi /etc/network/interfaces （打开相应的文件）

2 将各个网卡上要设置的IP地址保存：



保存后即可。此后打开该虚拟机后，无需再次设置IP地址和网关。

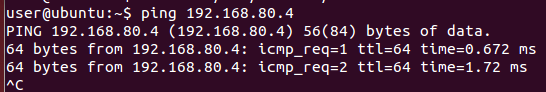
其他各台虚拟机可进行同样的设置。

（4）连接效果

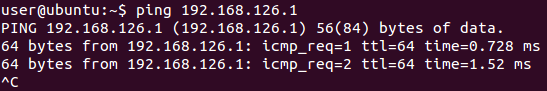
设置好路由规则，查看连接效果：

U-572（Router0）：

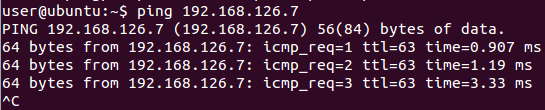
Ping UT-574（子网内连接）：



Ping U-571（Router1）：

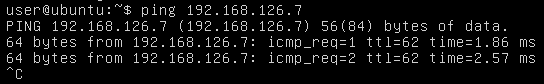


Ping UT-577（另一子网的主机）：



UT-575（子网2中的一台主机）：

Ping UT-577（子网3中的一台主机。从UT-575到UT-577是整个网络中最长的路）：

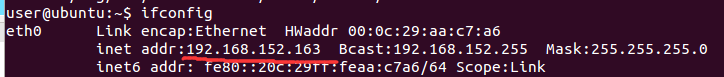


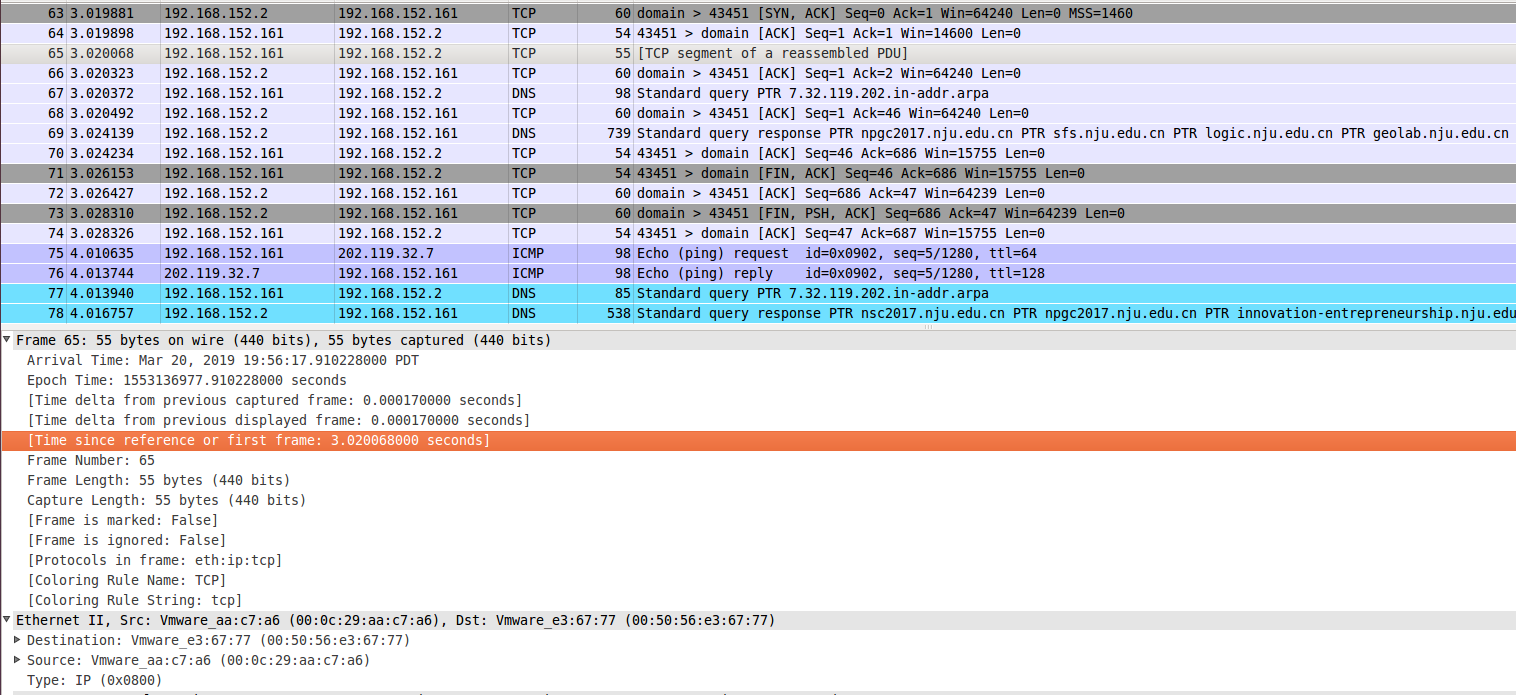
由以上连接测试知，该网络运行成功。

三、数据包截图及分析

（1）ping cs.nju.edu.cn:

Ping时的本机IP地址：192.168.152.163



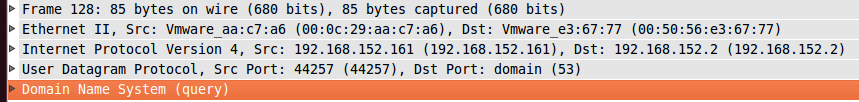
Ping后：

可见出现了多种类型的协议下的数据包。

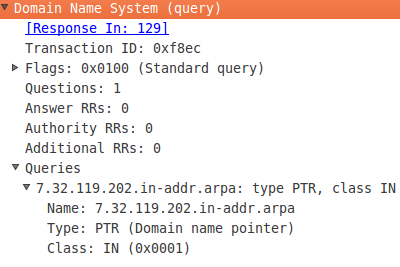
（1）DNS协议

DNS是Domain Name System的缩写，是Internet的一项服务，该服务将诸如cs.nju.edu.cn这样的域名与IP地址互相映射，提供域名与IP地址之间的转换功能。DNS协议是应用层协议。

如上图，主机（192.168.152.161）向网关（192.168.152.2）发送了一个DNS报文。

DNS报文包含了如下结构：**自底向上分析**：

Domain Name System部分：



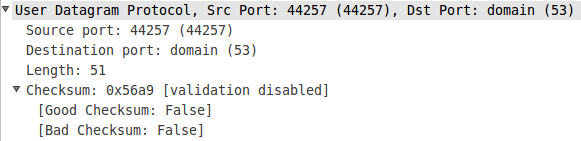
DNS是应用层协议。字段分析：

Transaction ID：交换ID，用于标记DNS的应答报文对应于哪个请求报文。Transaction ID 是随机产生的，DNS服务器返回DNS应答信息时，使用的 Transaction ID 必须和询问时使用的一致，才会被询问的主机接受。

Flags 中的 Question：表明这个报文只有一个请求

Queries：请求的具体内容。其中Type: PTR表明该请求的内容是**把IP地址转换成域名**。

UDP（User Datagram Protocol）部分



UDP是运输层的协议，是一个无连接的简单的面向数据报的运输层协议。UDP不提供可靠性，它只是把应用程序传给IP层的数据报发送出去，但是并不能保证它们能到达目的地。

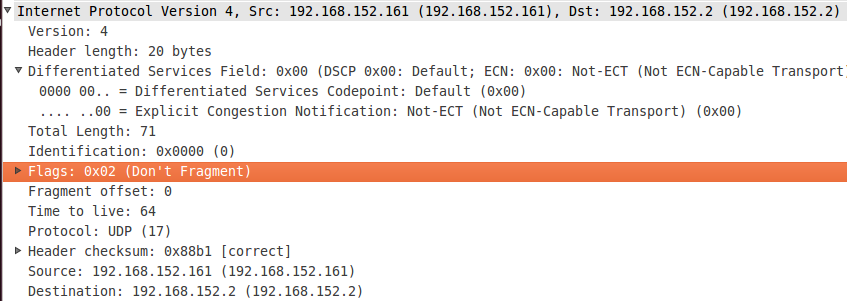
字段分析：

Source port：源端口号44257。

Destination port：目的端口号53。

Length:（报文）长度为51

Checksum：检验和：0x56a9

 IPv4协议部分

该协议为网络层协议。字段分析：

Version:版本：4

Header长度：20个字节，

IP包总长度：71字节

identification标识：0x0000

不分片（Don’t Fragment）标志：0x02

片偏移：0

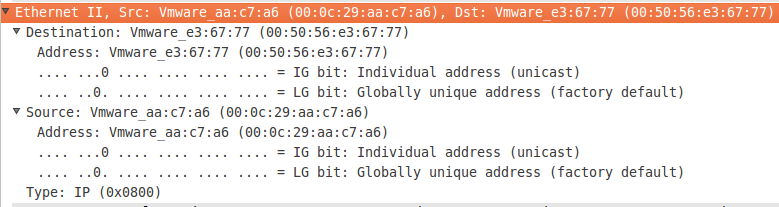
Time to live: 生存期，即数据报最多可经过的路由数

使用的协议：UDP

首部检验和：0x88b1

源地址:192.168.152.161，也即本机地址

目的地址:192.168.152.2，默认网关的IP地址。

 数据链路层以太网帧头部信息

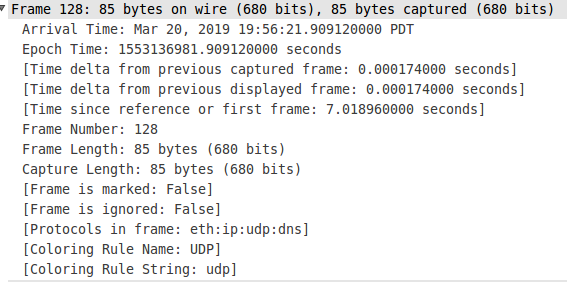
该协议为链路层协议。字段分析：

源MAC地址：00:0c:29:aa:c7:a6

目的MAC地址：00:50:56:e3:67:77

Type:IP : 0x0800，表示上一层的数据是IPv4报文的数据。

Frame部分



字段分析：

到达时间：略

Epoch time: 从标准世界时1970年1月1日0时0分0秒起到现在的总秒数

帧数：128

帧长度：85B

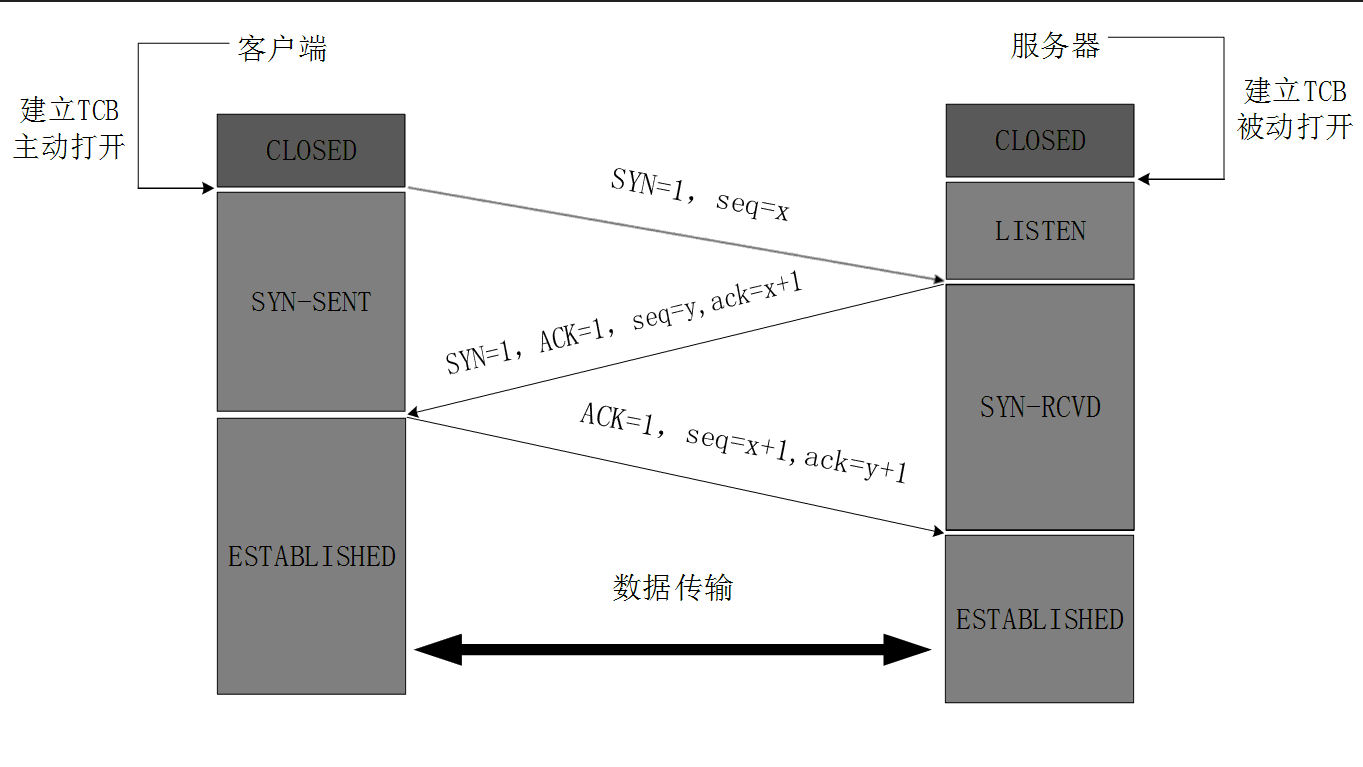
捕获长度：85B

帧已被标记：否

帧被忽略：否

染色规则名：UDP

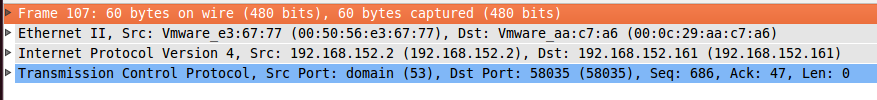
（2）TCP协议

TCP是因特网中的运输层协议，使用三次握手协议建立连接。当主动方发出SYN连接请求后，等待对方回答SYN+ACK，并最终对对方的 SYN 执行 ACK 确认。这种建立连接的方法可以防止产生错误的连接。

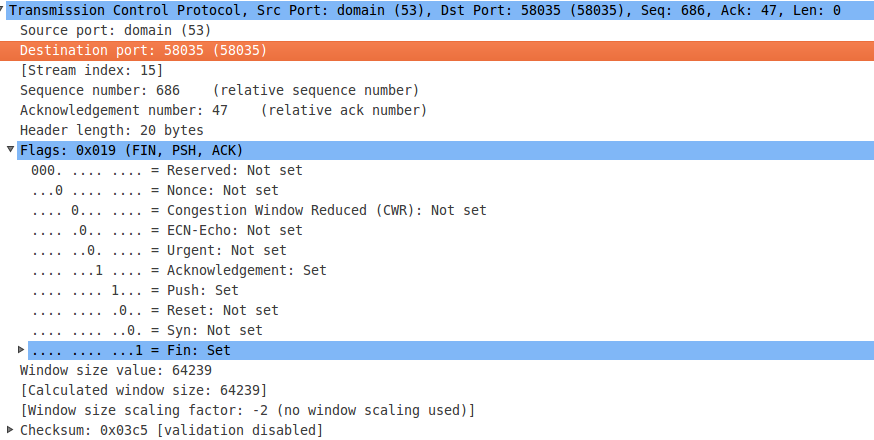
TCP的3次握手：

1. 客户端发送SYN（SEQ=x）报文给服务器端，进入SYN\_SEND状态。

2. 服务器端收到SYN报文，回应一个SYN （=y）， ACK(=x+1）报文，进入SYN\_RECV状态。

3. 客户端收到服务器端的SYN报文，回应一个ACK(=y+1）报文，进入Established状态。

上面2图为要分析的TCP报文。

其中的Frame, Ethernet II, IPv4部分与DNS报文相近，不再分析。故只分析最下面的TCP部分：

字段分析：

Source port：时源端口号53

Destination port：目的端口号58035

Sequence number：686由于为第一次握手，序号为相对序号，为0

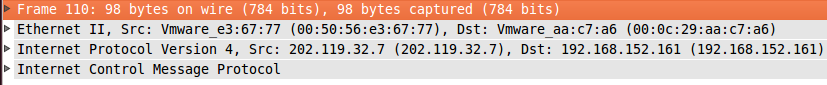
Acknowledge number: 47

Header length：头部长度: 20B

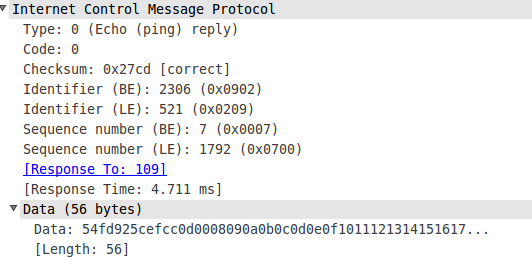
Window size: 窗口大小：64239

Checksum：检验和：0x03c5

（3）ICMP协议

ICMP（Internet Control Message Protocol）是TCP/IP协议簇的一个子协议，故属于网络层。它用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。ICMP协议是一种面向无连接的协议，

同TCP协议，此处只分析上图最下面的ICMP部分：



字段分析：

Type：值为0，表示Echo Reply，即回应请求的报文。

Checksum：检验和0x27cd

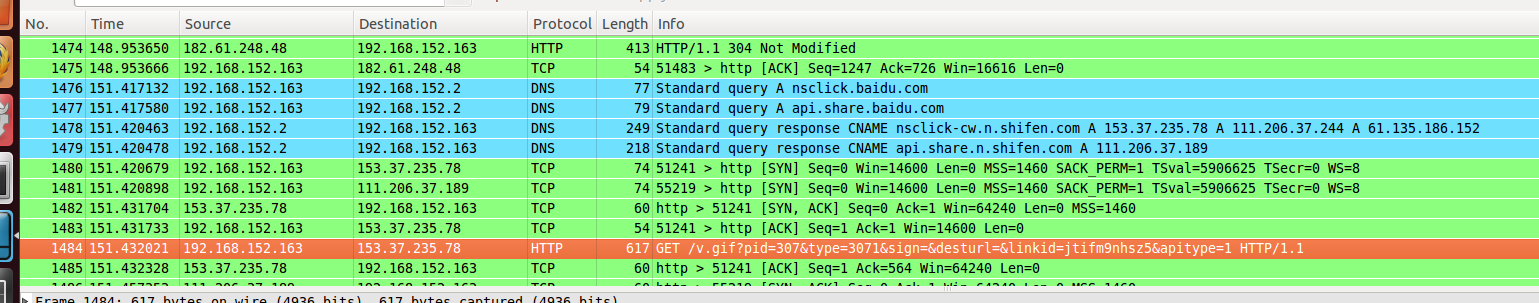
标识符（BE）：2306

标识符（LE）：521

序列号（BE）：7

序列号（LE）：1792

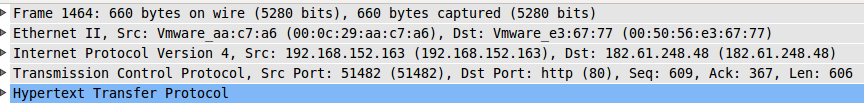
数据：回应的数据，长度56字节

（2）用浏览器打开[www.nju.edu.cn](http://www.nju.edu.cn):

出现的报文协议类型与ping系主页出现的几乎相同，多了一个HTTP协议:

HTTP协议：

HTTP协议（HyperText Transfer Protocol，超文本传输协议）是用于从WWW服务器传输超文本到本地浏览器的传输协议，是客户端浏览器或其他程序与Web服务器之间的应用层通信协议。在Internet上的Web服务器上存放的都是超文本信息，客户机需要通过HTTP协议传输所要访问的超文本信息。HTTP包含命令和传输信息，不仅可用于Web访问，也可以用于其他因特网/内联网应用系统之间的通信，从而实现各类应用资源超媒体访问的集成。

同理，只分析最下面的HTTP部分：

字段分析：

Request Method：请求方法：GET，表示向特定的网络资源发出请求

Request Version：HTTP版本：HTTP/1.1

User-Agent：指明获取资源的主机的浏览器，操作系统类型

Accept：请求的文件类型

Accept-Language：请求的语言类型

Accept-Encoding：请求的编码方式

Full request URI：请求的URI。Web上可用的每种资源：HTML文档、图像、视频片段、程序等，都由一个通用资源标识符（Uniform Resource Identifier, URI）进行定位。

Cookie: cookie值