实验二 ARP与DNS协议分析实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 组号： | 4-2 | - |  |  |  |
| 姓名： | 林展辉 | 学号： | 2194411249 | 班级： | 计算机94 |
| 姓名： |  | 学号： |  | 班级： |  |
|  |  |  |  |  |  |

1. 实验目的

分析ARP协议报文首部格式以及在同一网段内和不同网段间的解析过程，分析DNS协议的工作过程。

1. 实验内容

（1）利用校园网及云服务器搭建内网、外网环境；

（2）用Wireshark截获ARP报文，分析报文结构及ARP协议在同一网段和不同网段间的解析过程；

（3）用Wireshark截取DNS报文，分析DNS工作过程。

1. 实验环境与分组

每2名同学一组，以现有的校园网络环境及云服务器搭建内网、外网网络。

1. 实验网络拓扑皆否

按照实际网络情况绘制拓扑图【标注出内、外地址】。



1. 实验过程及结果分析

【过程记录应当详尽，截图并加以说明。以下过程和表格仅供参考。】

* 1. ARP协议分析

（一）同一网段内IP的ARP协议分析：

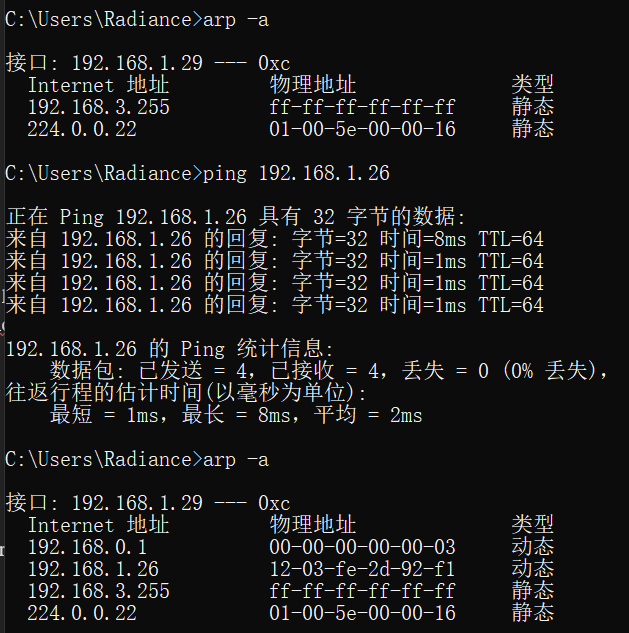
步骤1：在计算机终端的命令行窗口执行命令：

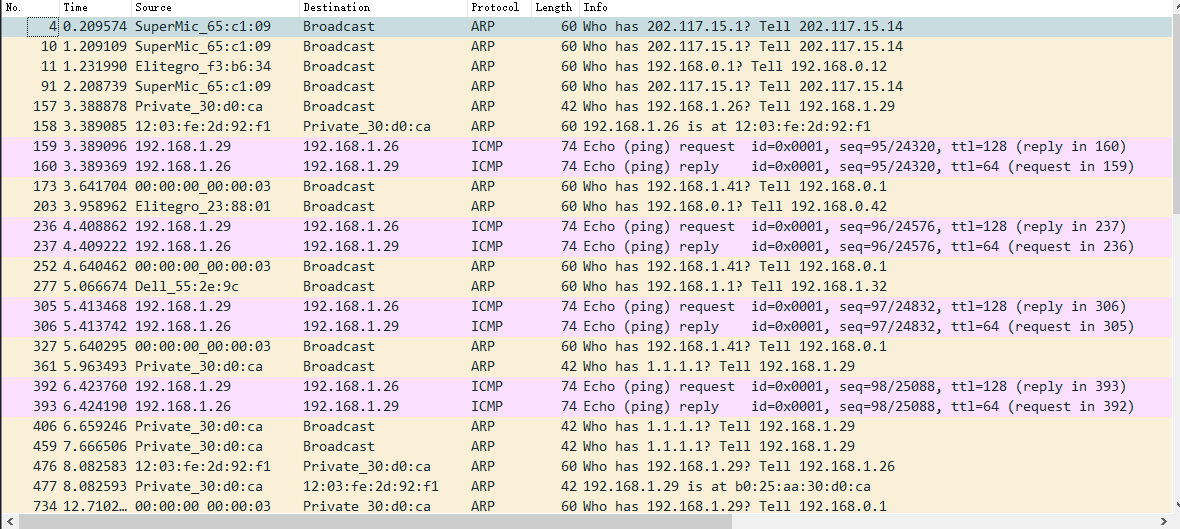
执行“arp –a”观察arp缓存；

执行“arp –d”命令清空arp缓存。

步骤2：在计算机终端上运行Wireshark截获报文，在命令行窗口ping同一网段的另一设备地址。执行完后停止报文截获，筛选出相关的arp和icmp报文进行分析（源IP地址/MAC地址、目的IP地址/MAC地址等）。

步骤3：在命令行窗口执行“arp –a”，记录结果。





（二）不同网段的ARP协议分析

步骤1：在本地计算机和云服务器执行“arp –d”清空缓存，运行Wireshark捕获报文，在本地计算机ping云服务器地址。执行完后停止报文截获，筛选出相关的arp和icmp报文进行分析（arp与icmp报文的顺序，报文源IP地址/MAC地址、目的IP地址/MAC地址及其对应的主机等）。

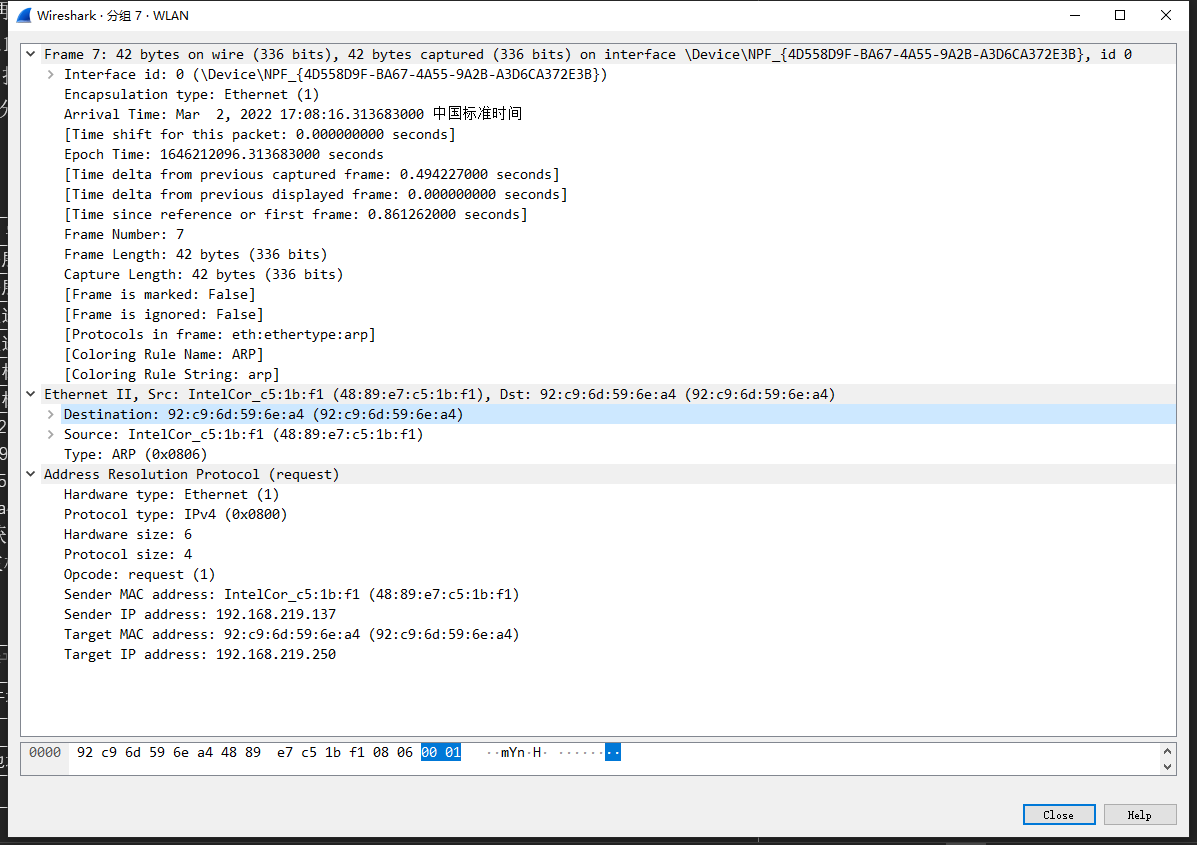
【如果网卡自动解析默认网关的MAC地址，可以删除默认网关设置，添加外网路由后再试。参考命令：route delete 0.0.0.0， route add 202.0.0.0 MASK 255.0.0.0 192.168.0.1】

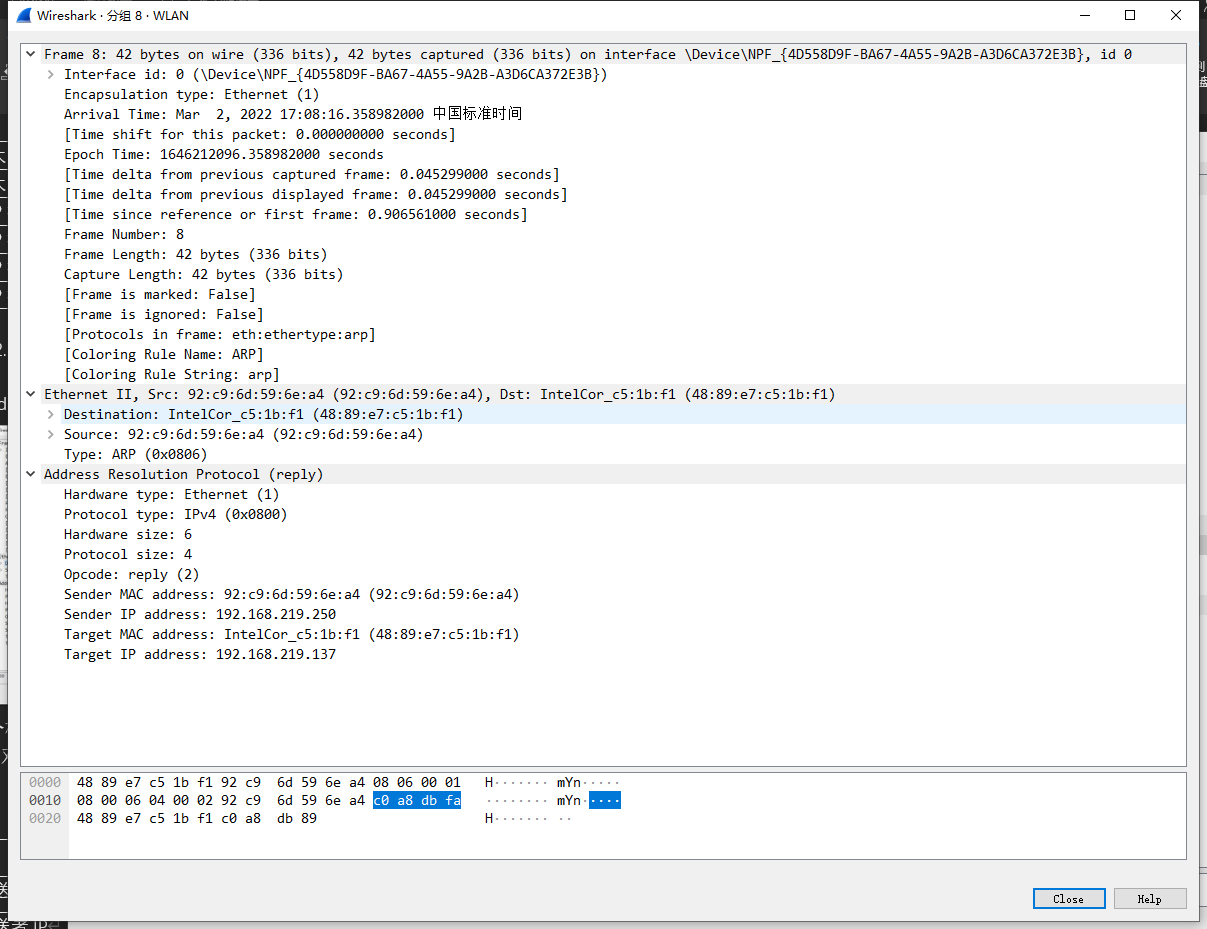
步骤2：执行“arp –a”命令，记录结果。

步骤3：分析捕获的报文，选中第一条ARP请求报文和第一条应答报文，填写2-1表。

表2-1 ARP请求报文和应答报文的字段信息

|  |  |  |
| --- | --- | --- |
| 字段 | 请求报文的值 | 应答报文的值 |
| 以太网链路层Destination项 | Destination: 92:c9:6d:59:6e:a4 (92:c9:6d:59:6e:a4) | Destination: IntelCor\_c5:1b:f1 (48:89:e7:c5:1b:f1) |
| 以太网链路层Source项 | Source: IntelCor\_c5:1b:f1 (48:89:e7:c5:1b:f1) | Source: 92:c9:6d:59:6e:a4 (92:c9:6d:59:6e:a4) |
| ARP报文发送者硬件地址 | Sender MAC address: IntelCor\_c5:1b:f1 (48:89:e7:c5:1b:f1) | Sender MAC address: 92:c9:6d:59:6e:a4 (92:c9:6d:59:6e:a4) |
| ARP报文发送者IP | Sender IP address: 192.168.219.137 | Sender IP address: 192.168.219.250 |
| ARP报文目标硬件地址 | Target MAC address: 92:c9:6d:59:6e:a4 (92:c9:6d:59:6e:a4) | Target MAC address: IntelCor\_c5:1b:f1 (48:89:e7:c5:1b:f1) |
| ARP报文目标IP | Target IP address: 192.168.219.250 | Target IP address: 192.168.219.137 |

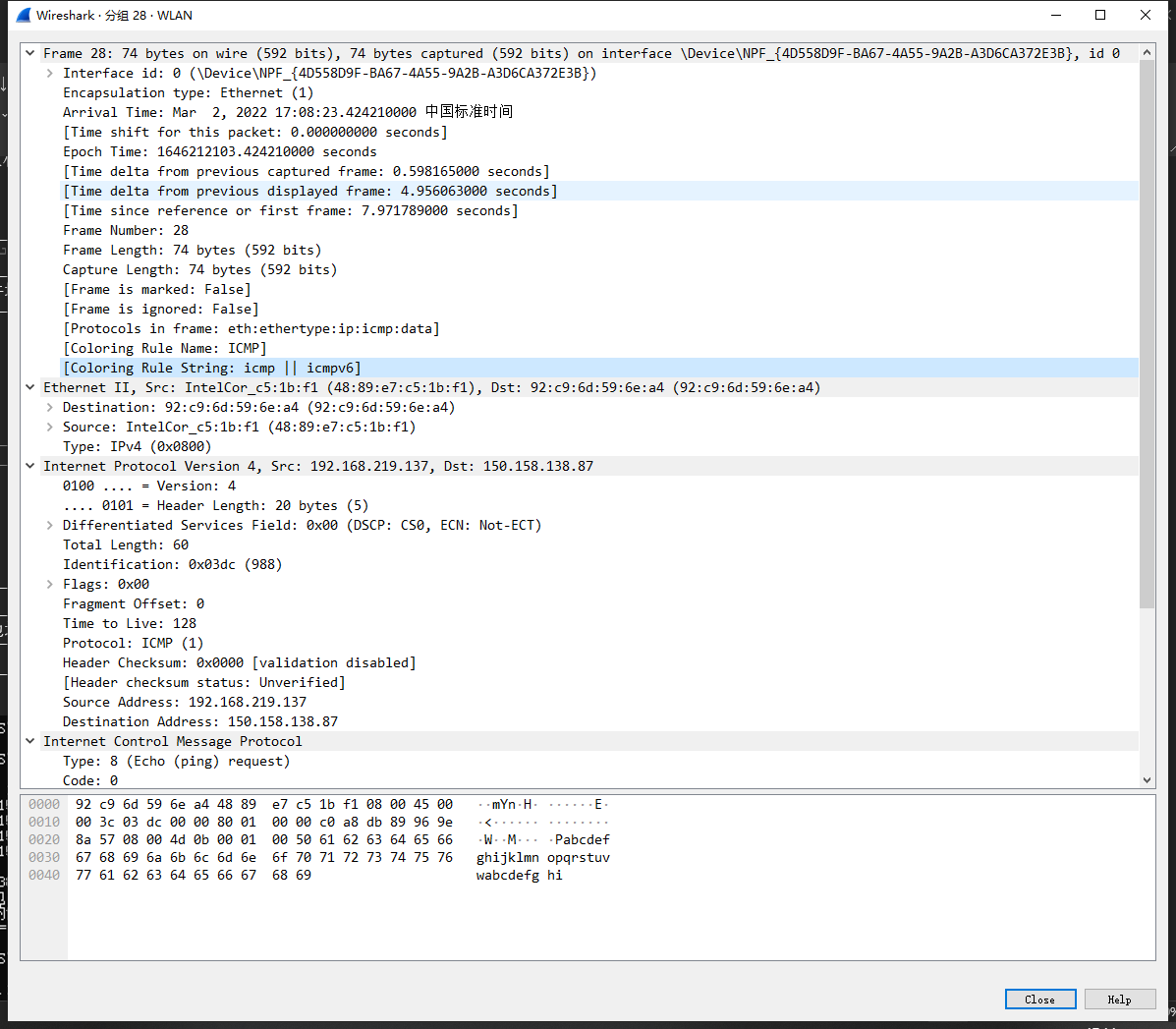


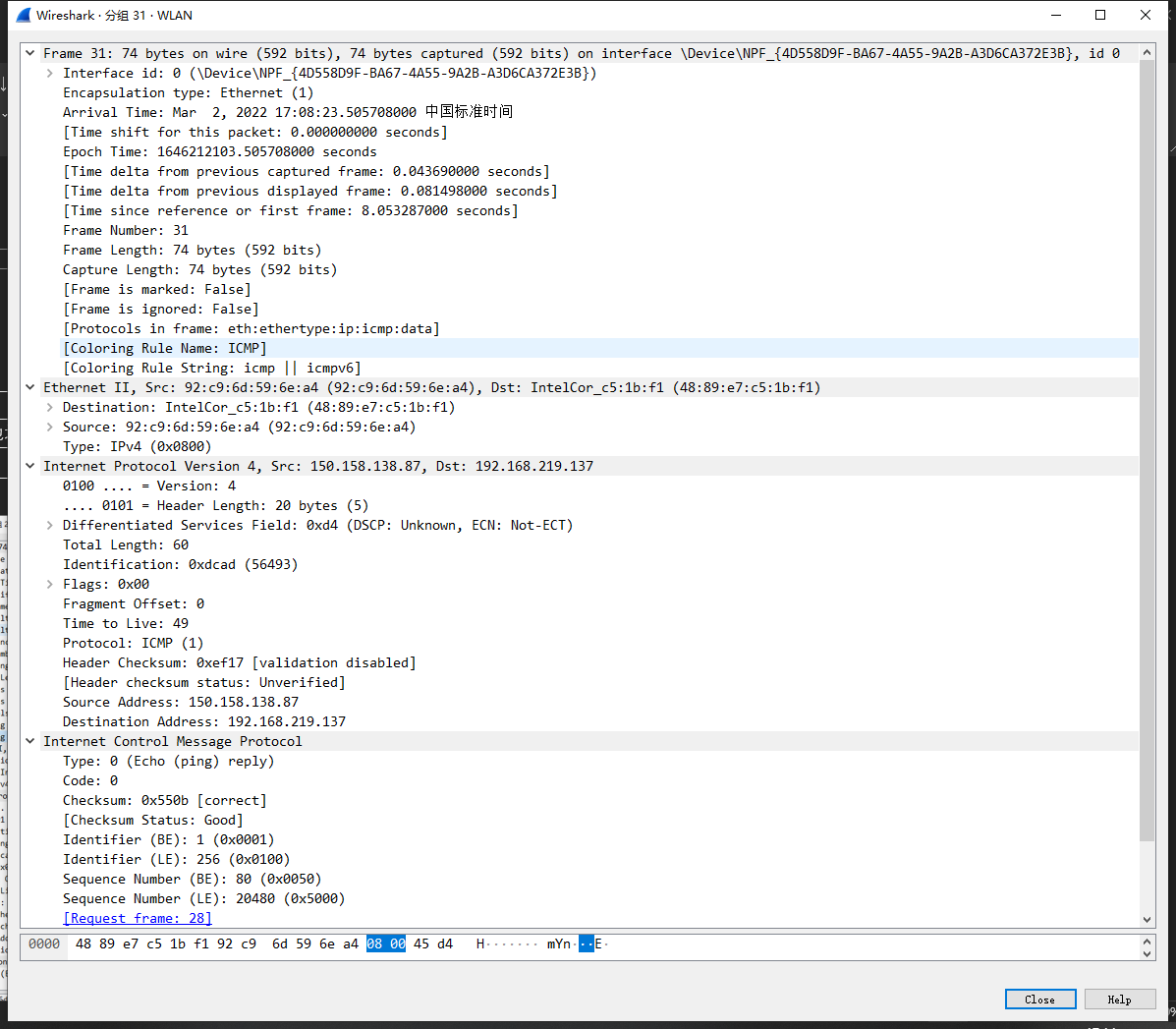


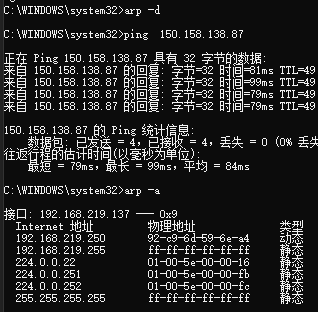
分析捕获的报文，选中第一条ICMP请求报文和第一条应答报文，填写表2-2。（对应主机填写本机、本地网关、服务器等）

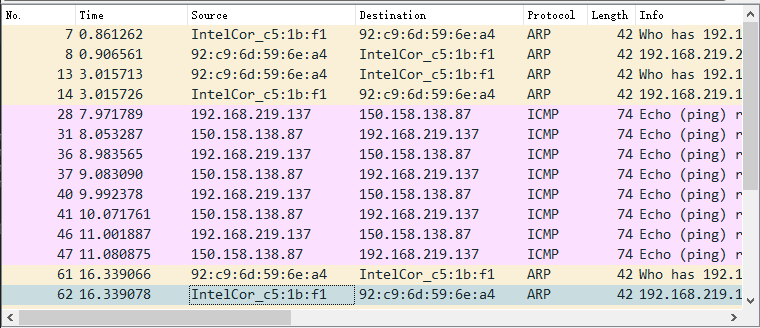
表2-2 ICMP请求报文和应答报文的字段信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 请求报文的值 | 对应主机 | 应答报文的值 | 对应主机 |
| 发送者硬件地址 | Source: IntelCor\_c5:1b:f1 (48:89:e7:c5:1b:f1) | Local | Source: 92:c9:6d:59:6e:a4 (92:c9:6d:59:6e:a4) | Server |
| 发送者IP | Source Address: 192.168.219.137 | Local | Source Address: 150.158.138.87 | Server |
| 目标硬件地址 | Destination: 92:c9:6d:59:6e:a4 (92:c9:6d:59:6e:a4) | Server | Destination: IntelCor\_c5:1b:f1 (48:89:e7:c5:1b:f1) | Local |
| 目标IP | Destination Address: 150.158.138.87 | Server | Destination Address: 192.168.219.137 | Local |









步骤4：比较ARP协议在不同网段和相同网段内解析过程的异同。

接收方和发送方在同一网段时，由于发送方无法查到相关的ARP缓存的映射，因而发送ARP报文获取接收方的IP到MAC的映射，接收方会先接收到发送方的ARP请求报文，并回复ARP响应报文。

接收方和发送方在不同网段时，发送方需要通过网关进行转发，因而将在ARP缓存中查询默认网关的IP到MAC的映射，并在未查询得到广播ARP请求报文。

* 1. DNS协议分析

（一）默认DNS域名解析

步骤1：在命令窗口执行命令：

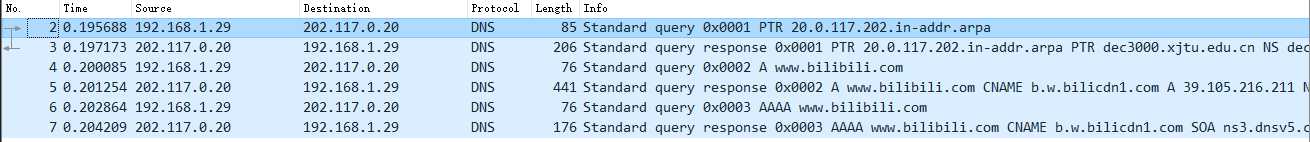
执行“ipconfig /displaydns”观察本地DNS缓存；

执行“ipconfig /flushdns”清除本地DNS缓存。



步骤2：在计算机终端上运行Wireshark截获报文，浏览器访问域名（如http://www.yahoo.com），网站打开后停止报文截获，观察分析DNS查询、回复报文分别包含哪些主要内容（UDP还是TCP、目的地址与本机默认DNS是否相同、源端口和目的端口、域名解析记录类型、解析出的IP地址等）。





（二）指定DNS域名解析

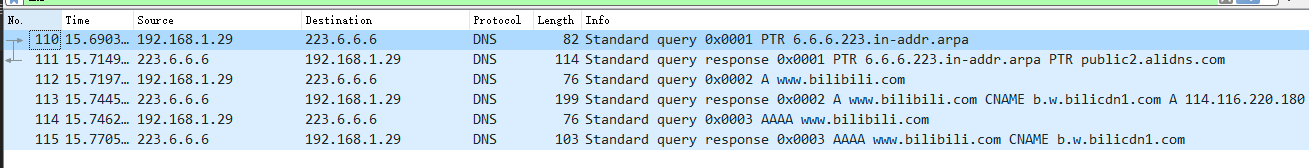
步骤1：在命令窗口执行命令：

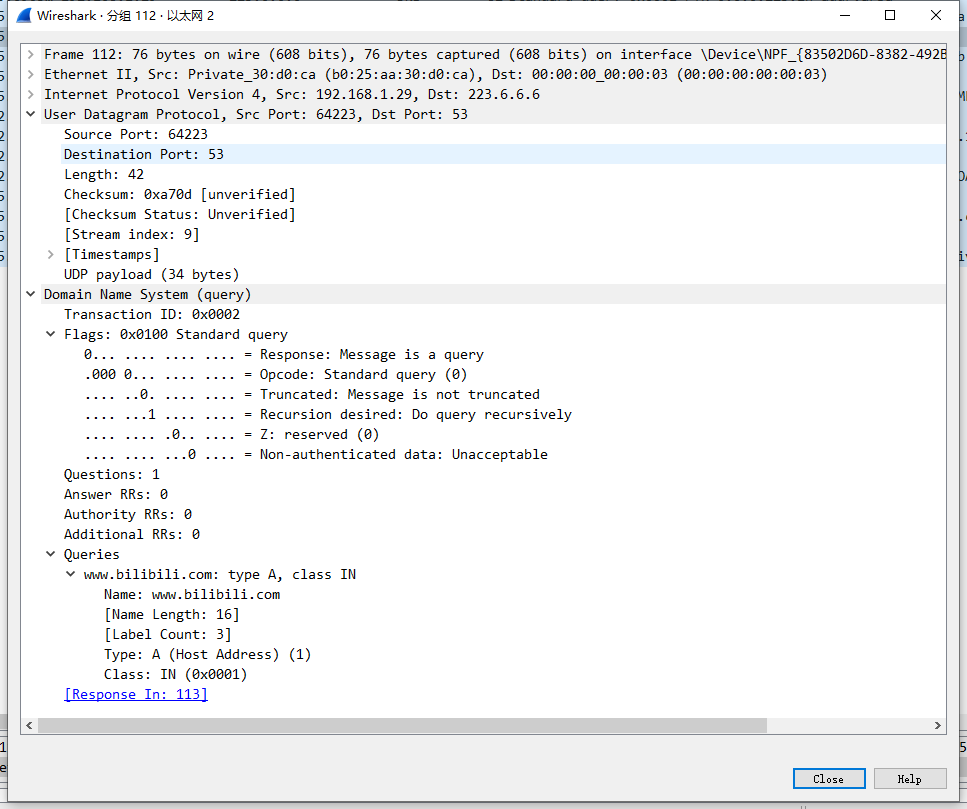
执行“ipconfig /displaydns”观察本地DNS缓存；

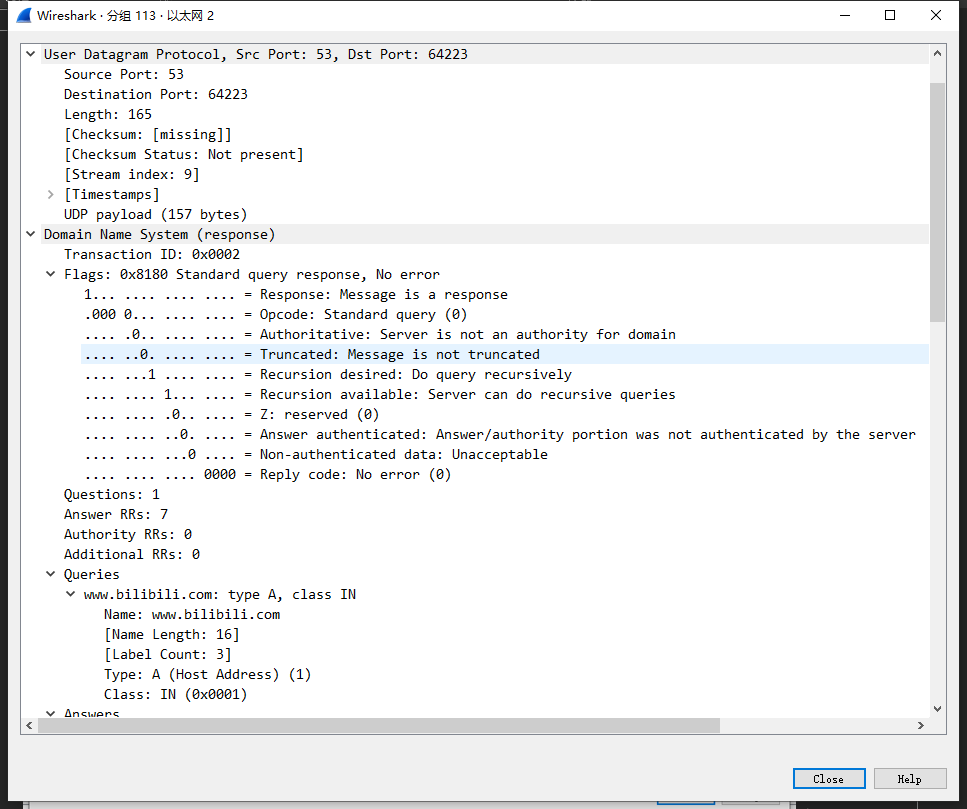
执行“ipconfig /flushdns”清除本地DNS缓存。

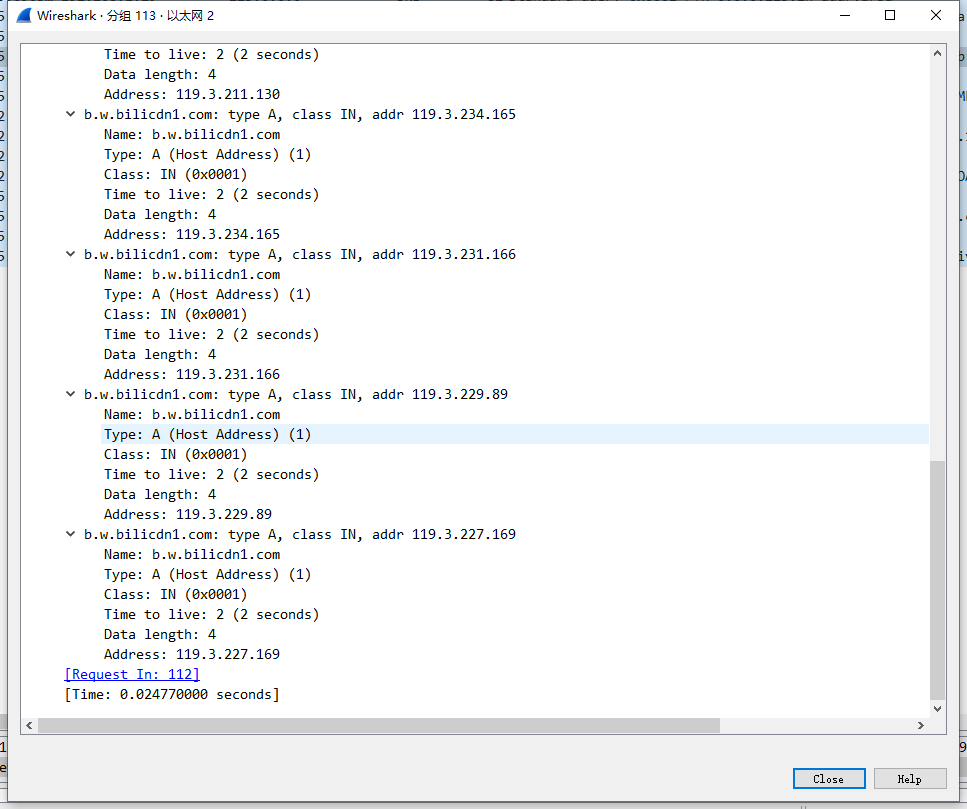
步骤2：在计算机终端上运行Wireshark截获报文，在命令窗口执行指定DNS服务器解析域名命令（如nslookup www.synlogictx.com 223.6.6.6），解析完毕后停止报文截获，观察分析DNS查询、回复报文分别包含哪些主要内容（UDP还是TCP、目的地址与本机默认DNS是否相同、源端口和目的端口、域名解析记录类型、解析出的IP地址等）。











采用的协议为UDP；查询类型为A类型，查询类字段为IN（互联网地址）互动讨论主题。

1. 发送方与接收方ARP与ICMP报文出现的次序成因；

数据链路层时，相同网段需要直到目的IP到MAC的映射，不同网段需要知道网关的IP到MAC的映射，因而需要ARP协议对这个映射进行解析。

接收方和发送方在同一网段时，由于发送方无法查到相关的ARP缓存的映射，因而发送ARP报文获取接收方的IP到MAC的映射，接收方会先接收到发送方的ARP请求报文，并回复ARP响应报文，因此ARP报文是先于ICMP报文的；

接收方和发送方在不同网段时，发送方需要通过网关进行转发，因而将在ARP缓存中查询默认网关的IP到MAC的映射，并在未查询得到时先发送ARP请求报文，再根据ARP回应报文发送ICMP报文。

1. ARP的安全性问题；

ARP协议时建立在局域网主机的相互信任之上的，因而在协议中没有包含安全验证机制。攻击者可以利用伪造的IP到MA截获其他主机之间通信的数据。ARP协议通过广播的方式进行通信。攻击者可以应答错误的MAC地址映射，也可以不断广播。

（3）DNS的欺骗带来的安全性问题；

DNS欺骗就是攻击者冒充域名服务器的一种欺骗行为。 原理：如果可以冒充域名服务器，然后把查询的IP地址设为攻击者的IP地址，这样的话，用户上网就只能看到攻击者的主页