实验二 ARP与DNS协议分析实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 组号： |  |  |  |  |  |
| 姓名： | 曾水靖 | 学号： | 22146611804 | 班级： | 计算机2102 |
| 姓名： | 向胤兴 | 学号： | 2215012469 | 班级： | 计算机2102 |
|  |  |  |  |  |  |

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；

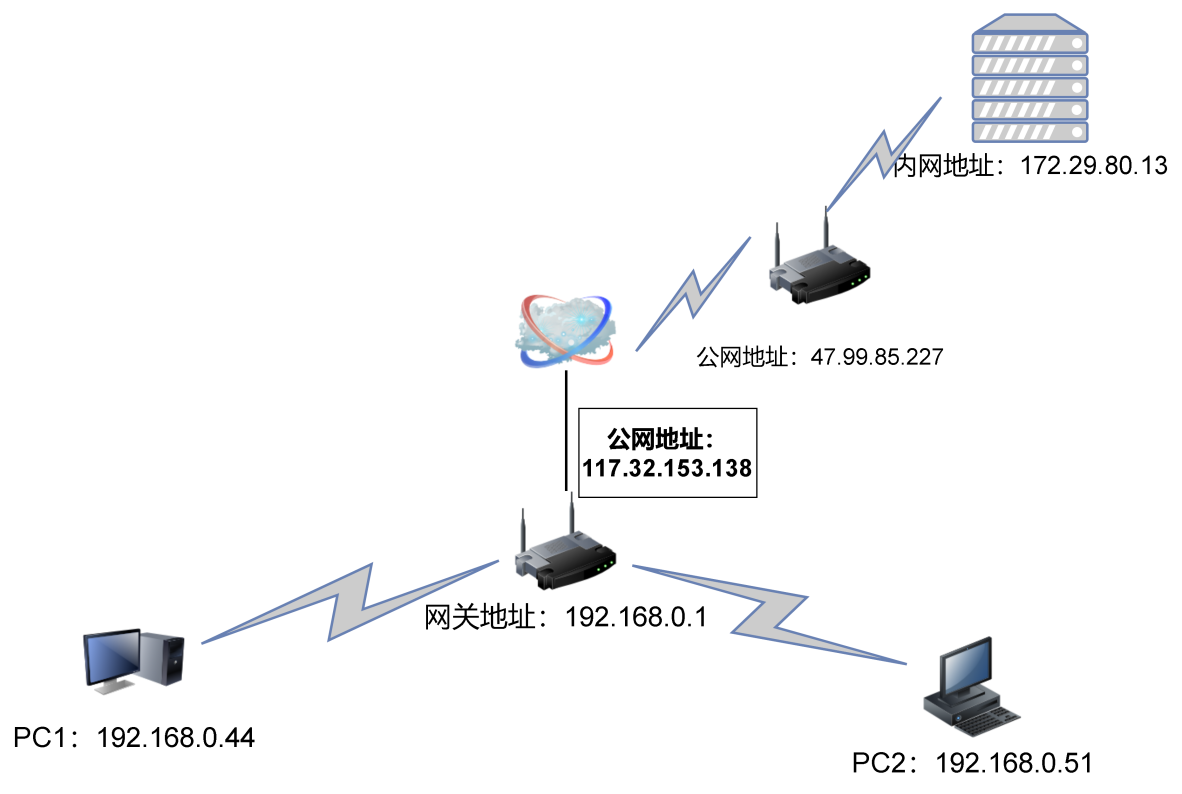
（3）用Wireshark截取DNS报文，分析DNS工作过程。

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

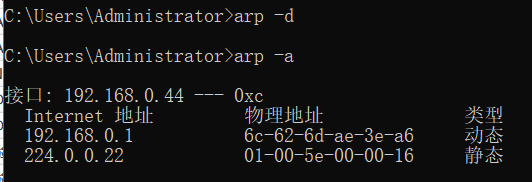
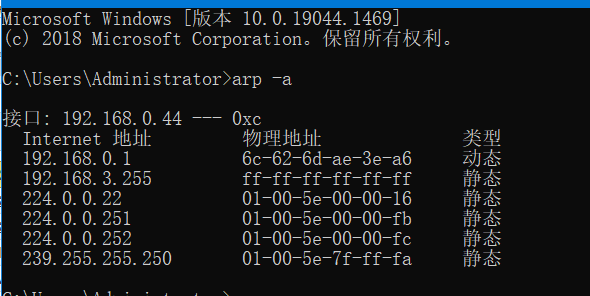
（一）同一网段内IP的ARP协议分析：

步骤1：在计算机终端的命令行窗口执行命令：

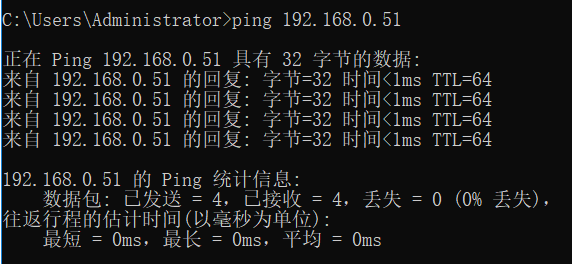
执行“arp –a”观察arp缓存；

执行“arp –d”命令清空arp缓存。

清空arp缓存表，目的是保证可以截获到arp报文而不是直接使用已有的arp表项。

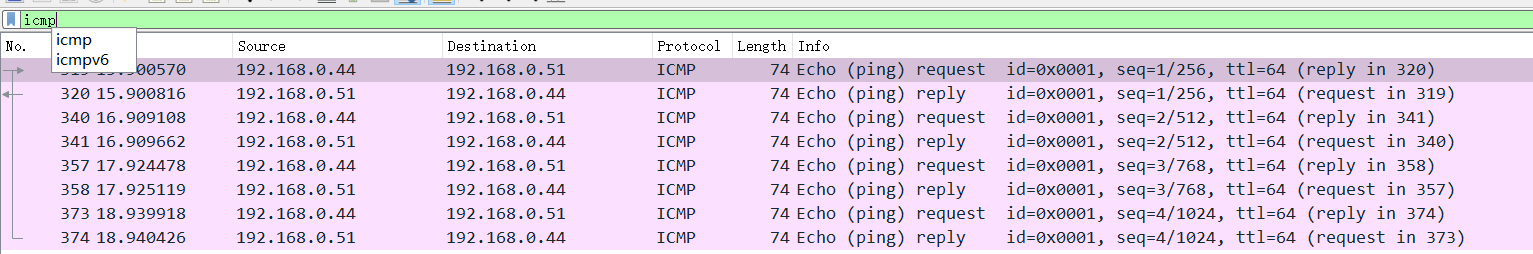


步骤2：在计算机终端上运行Wireshark截获报文，在命令行窗口ping同一网段的另一设备地址。执行完后停止报文截获，筛选出相关的arp和icmp报文进行分析（源IP地址/MAC地址、目的IP地址/MAC地址等）。









Arp报文：

本机（192.168.0.44）在以太网中广播询问“who has 192.168.0.51”并附带自己的ip地址”192.168.0.44”，当局域网其他主机有ip地址为192.168.0.50的arp项时，会向本机回复要查询主机的MAC地址。

同理，通讯目的主机（192.168.0.51）也会在以太网中广播查询本机的MAC地址，以保障双方通信的正常进行。

此过程的源IP地址：本机：192.168.0.50

目的IP地址：广播

ICMP报文：以第一个报文为例，通过arp报文，本机已经知道了目的主机的MAC地址，源主机、目的主机的IP、MAC地址如下：

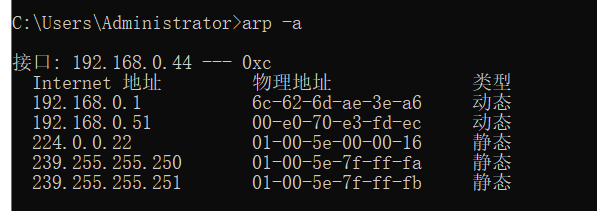
源IP地址：192.168.0.44

源MAC地址：00:e0:70:e3:fe:cc

目的IP地址：192.168.0.51

目的MAC地址：00:e0:70:e3:fd:ec

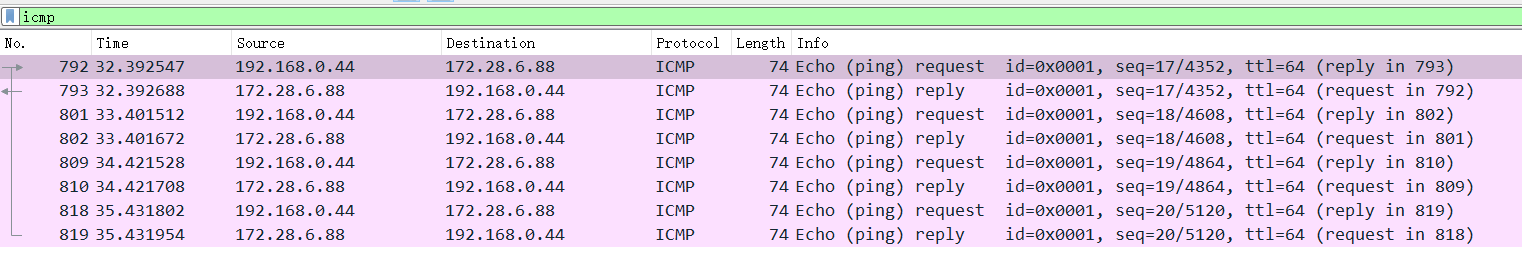
步骤3：在命令行窗口执行“arp –a”，记录结果。

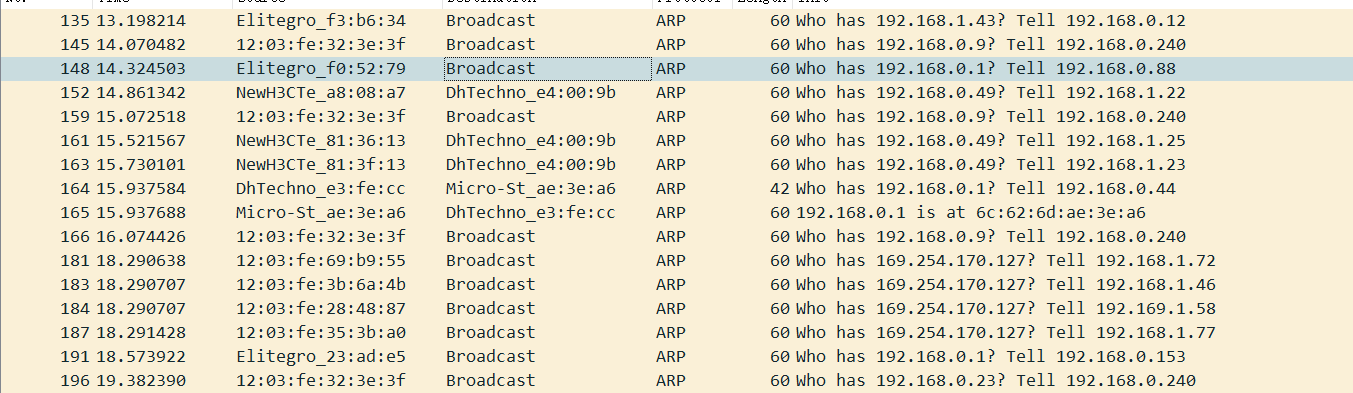


可以看到新增了目的主机（192.168.0.51）的arp表项。

（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）。





arp与icmp报文的顺序：通过报文抓获时间可以看出，先进行了arp报文的发送，后进行icmp报文。

源IP地址：192.168.0.44（源主机）

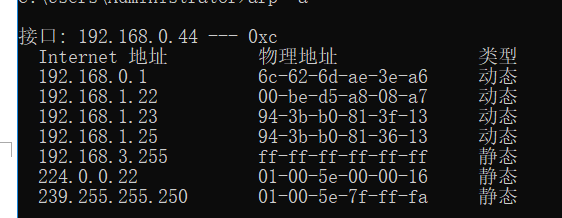
源MAC地址：00:e0:70:e3:fe:cc（目的主机）

目的IP地址：172.168.0.44 （目的主机）

目的MAC地址：6c:62:6d:ae:3e:a6 （网关）

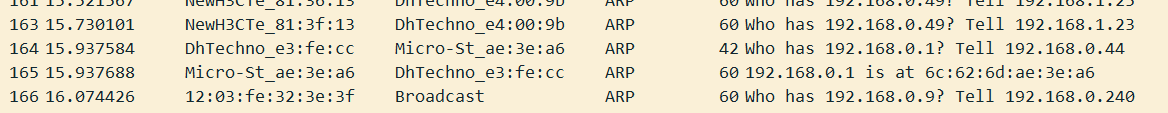
由于源主机与目的注意不在同一个以太网，源主机与目的主机进行通信需要经过网关。发出的ICMP报文目的IP地址为172.168.0.44，目的主机的地址，但是ICMP报文的MAC地址是网关，保证能正确的送到网关进行转发。

步骤2：执行“arp –a”命令，记录结果。

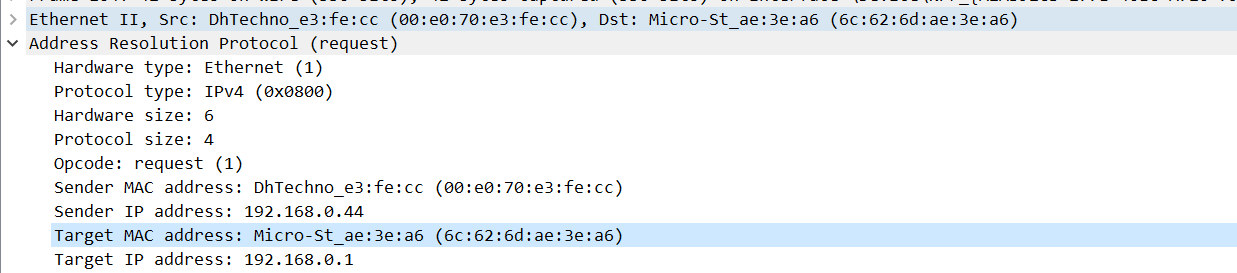


可以看到本机并没有新增直接与目的主机相关的IP地址为172.168.0.44的arp项，对此主机的通信是通过第一条网关的arp项进行的。

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。



请求报文



应答报文

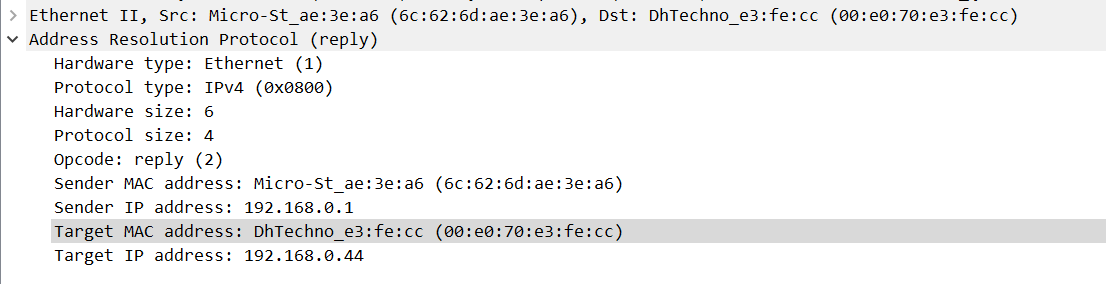


表2-1 ARP请求报文和应答报文的字段信息

|  |  |  |
| --- | --- | --- |
| 字段 | 请求报文 | 应答报文 |
| Ethernet II Dst: | Micro-St\_ae:3e:a6 (6c:62:6d:ae:3e:a6) | DhTechno\_e3:fe:cc (00:e0:70:e3:fe:cc) |
| Ethernet II Src: | DhTechno\_e3:fe:cc (00:e0:70:e3:fe:cc) | Micro-St\_ae:3e:a6 (6c:62:6d:ae:3e:a6) |
| ARP Sender MAC address: | DhTechno\_e3:fe:cc (00:e0:70:e3:fe:cc) | Micro-St\_ae:3e:a6 (6c:62:6d:ae:3e:a6) |
| ARP Sender IP address: | 192.168.0.44 | 192.168.0.1 |
| ARP Target MAC address: | Micro-St\_ae:3e:a6 (6c:62:6d:ae:3e:a6) | DhTechno\_e3:fe:cc (00:e0:70:e3:fe:cc) |
| ARP Target IP address: | 192.168.0.1 | 192.168.0.44 |

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）

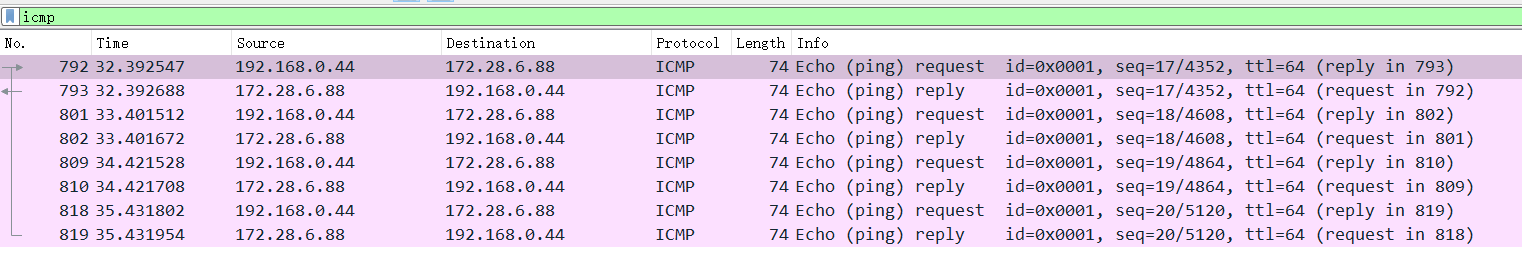


表2-2 ICMP请求报文和应答报文的字段信息

请求报文



应答报文



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 请求报文 | 对应主机 | 应答报文 | 对应主机 |
| Ethernet II Src: | DhTechno\_e3:fe:cc (00:e0:70:e3:fe:cc), | 本机 | Micro-St\_ae:3e:a6 (6c:62:6d:ae:3e:a6) | 本地网关 |
| IP Src: | 192.168.0.44 | 本机 | 118.31.245.1 | 服务器（目的主机） |
| Ethernet II Dst: | Micro-St\_ae:3e:a6 (6c:62:6d:ae:3e:a6) | 本地网关 | DhTechno\_e3:fe:cc (00:e0:70:e3:fe:cc), | 本机 |
| IP Dst: | 118.31.245.1 | 服务器 | 192.168.0.44 | 本机 |

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。

相同网段：在相同网段内进行arp解析时，源主机在统一网关管理的网络中进行广播查询目的IP地址，其他存有目的主机的arp解析的主机会应答源主机的请求，整个过程不需要网关的参与。

不同网段：源主机与不同网段的主机通信需要借助网关，在同网段进行广播查询无法查询到目的主机的IP地址时，需要通过网关在其他网段查询，此后网关替源主机在其他网段中查询。网关查询到后，会给源主机hi发送应答报文，但不会直接提供目的主机的arp解析，应答的报文中的硬件地址设为自己（网关硬件地址），此后源主机与本地网段外部的主机进行通信，IP地址始终为目的主机，MAC地址首先设置为网关的MAC地址，正常发送到网关后网关对报文进行处理后再发送给目的主机。

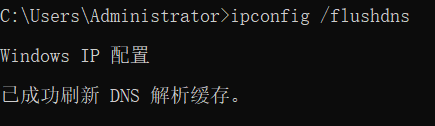
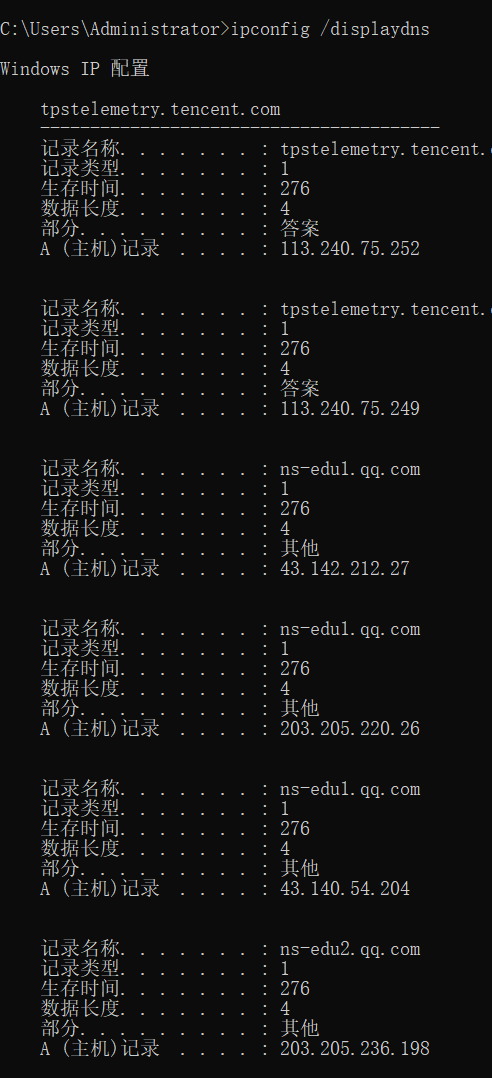
* 1. DNS协议分析

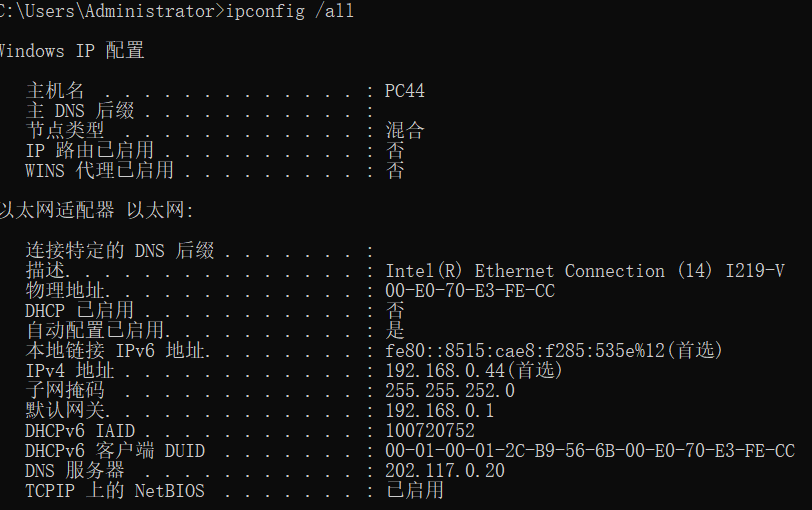
（一）默认DNS域名解析

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。





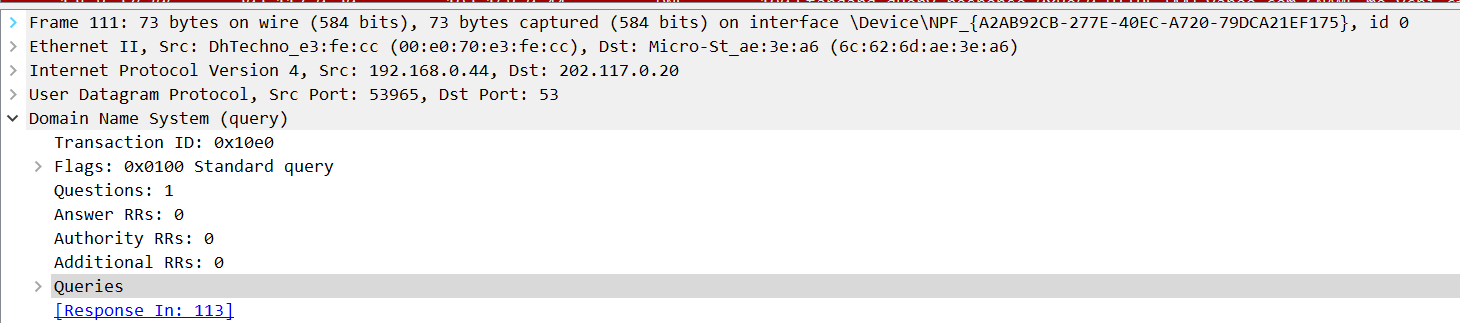
步骤2：在计算机终端上运行Wireshark截获报文，浏览器访问域名（如http://www.yahoo.com），网站打开后停止报文截获，观察分析DNS查询、回复报文分别包含哪些主要内容（UDP还是TCP、目的地址与本机默认DNS是否相同、源端口和目的端口、域名解析记录类型、解析出的IP地址等）。

本机访问外网，首先要向本地网关发出请求，本地dns解析外网，得到IP地址，然后才向外网发出访问请求，外网应答也要通过外网网关然后，再通过本地网关，将应答传回本机，所以在这里截到的DNS报文只是本机与本地网关之间的报文。





请求报文：



传输层协议：UDP

源地址：192.168.0.44

目的地址：202.117.0.20 本机默认DNS：202.113.0.20

源端口：53965 目的端口：53



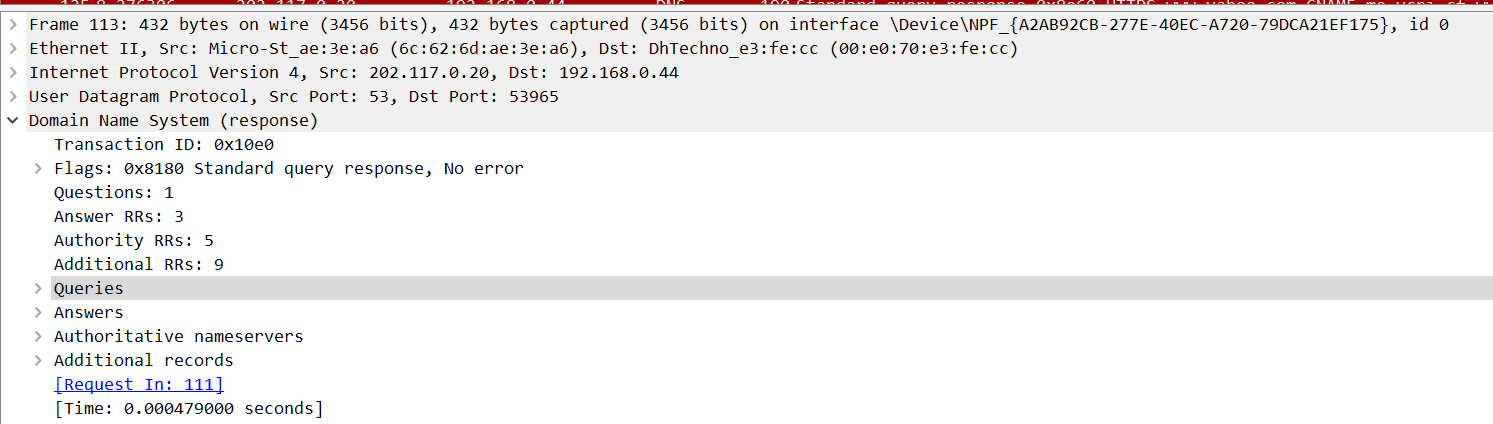
（域名解析应答报文）由此可得

域名解析记录类型：A记录（将域名指向一个IPv4地址）指向的地址为69.147.88.8

CNAME记录（将域名指向一个域名，实现与被指向域名相同的访 问效果，这个域名一般是主机服务商提供的一个域名） 指向的 域名为me-ycpi-cf-www.yahoodns.net

解析出的IP地址：69.147.88.8

应答报文



传输层协议：UDP

源地址：202.113.0.20

目的地址：192.168.0.44 本机默认DNS：202.113.0.20

源端口：53 目的端口：53965



（域名解析应答报文）由此可得

域名解析记录类型：A记录（将域名指向一个IPv4地址）指向的地址为69.147.88.8

CNAME记录（将域名指向一个域名，实现与被指向域名相同的访 问效果，这个域名一般是主机服务商提供的一个域名） 指向的 域名为me-ycpi-cf-www.yahoodns.net

解析出的IP地址：69.147.88.8

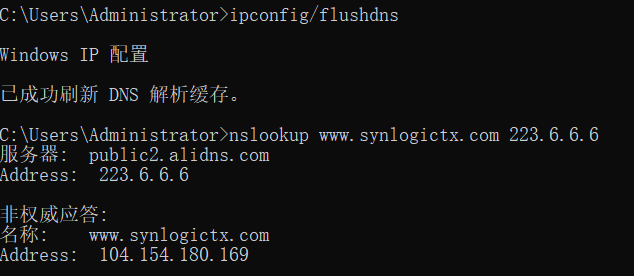
（二）指定DNS域名解析

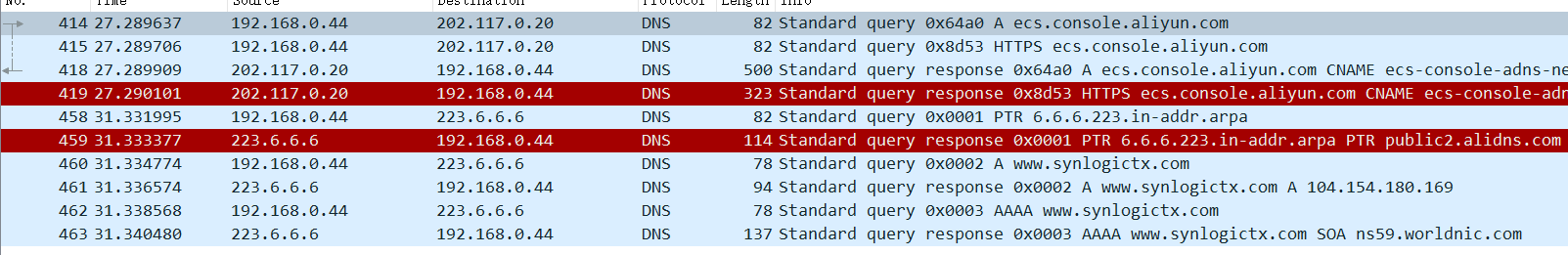
步骤1：在命令窗口执行命令：

执行“ipconfig /displaydns”观察本地DNS缓存；

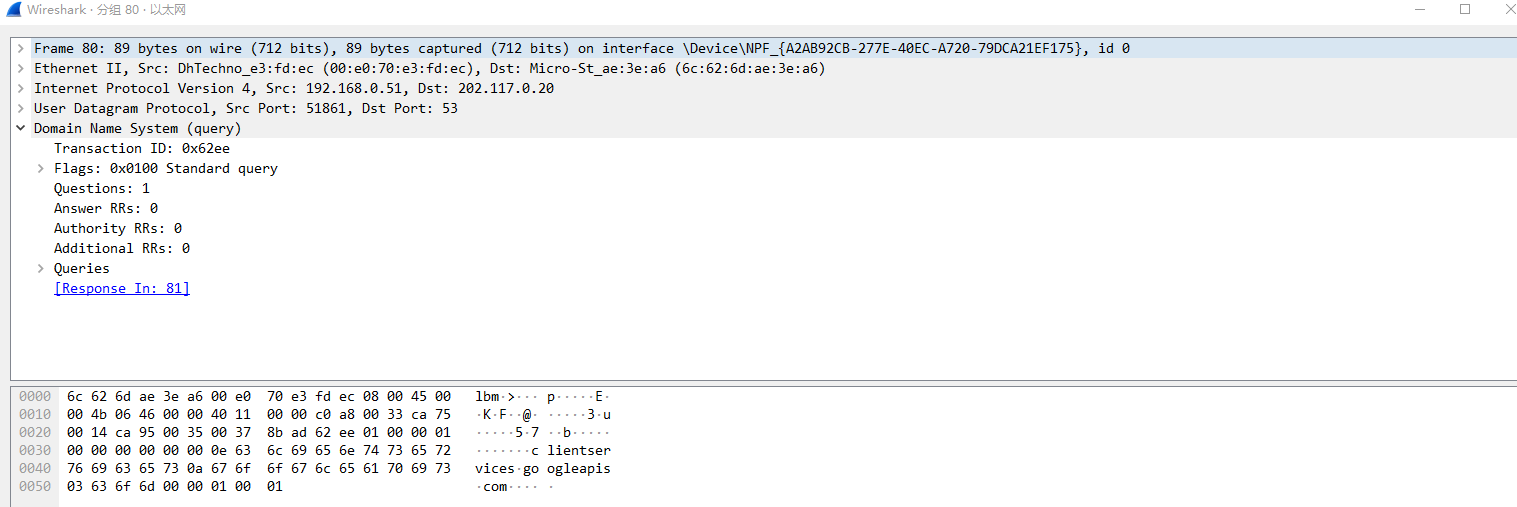
执行“ipconfig /flushdns”清除本地DNS缓存。

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）。





请求报文



传输层协议：UDP

源地址：192.168.0.44

目的地址：202.117.0.20 本机默认DNS：202.113.0.20

源端口：53 目的端口：49896





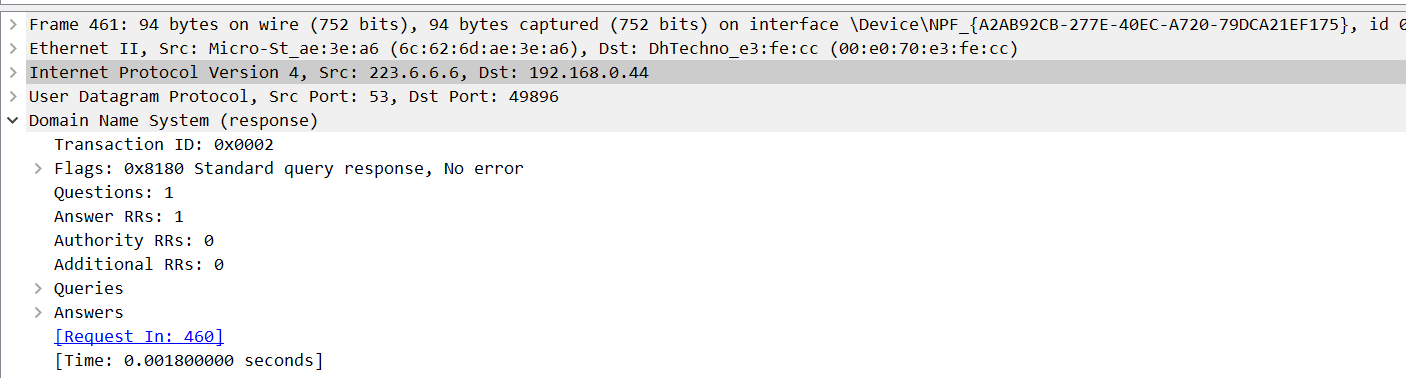
域名解析记录类型：A记录（将域名指向一个IPv4地址） 指向地址为104.154.180.169

AAAA记录：将主机名（或域名）指向一个IPv6地址；

解析出的IP地址：104.154.180.169

应答报文





传输层协议：UDP

源地址：223.6.6.6

目的地址：192.168.0.44 本机默认DNS：202.113.0.20





域名解析记录类型：A记录（将域名指向一个IPv4地址） 指向地址为104.154.180.169

AAAA记录：将主机名（或域名）指向一个IPv6地址；

解析出的IP地址：104.154.180.169

* 1. 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；

（2）ARP的安全性问题；

（3）DNS的欺骗带来的安全性问题；

1. ：ARP报文先出现，而ICMP报文后出现，原因是ICMP报文中带有目的主机的MAC地址，而目的主机的MAC地址首先需要通过arp报文获得。

（2）： ARP协议的安全性问题主要体现在ARP欺骗和ARP病毒两个方面。

ARP欺骗是指攻击者发送伪造的ARP响应报文，将受害主机的ARP缓存中的MAC地址替换为攻击者的MAC地址，从而截获发送给受害主机的数据包。这种攻击方式可能导致数据泄露、网络中断等严重后果。

ARP病毒则是通过大量发送虚假的ARP请求报文，导致网络中出现广播风暴，使正常的网络通信受到干扰。这种攻击不仅会影响网络性能，还可能导致网络拥塞和崩溃。

（3）：DNS欺骗是一种攻击手段，攻击者通过伪造DNS响应来欺骗客户端，使其解析到错误的IP地址。这样，当客户端直接通过域名访问时，以为把信息正确的发送给了服务器，实际上发送给了错误的IP地址的主机，造成了信息的泄露。

* 1. \*进阶自设计

Scapy是一个 Python程序，它允许用户发送、嗅探、分析和伪造网络包。这种能力允许构建能够探测、扫描或攻击网络的工具。换句话说，Scapy是一个强大的交互式包操作程序。它能够伪造或解码大量协议的数据包，在网络上发送它们，捕获它们，匹配请求和响应，等等。Scapy可以轻松地处理大多数经典任务，如扫描、跟踪、探测、单元测试、攻击或网络发现。它可以代替hping、arpsoof、arp-sk、arping、p0f甚至Nmap、tcpdump和tshark的某些部分。

（1）使用scapy在Linux下写程序来模拟完成一个简单的ARP欺骗。

（2）使用scapy在Linux下写程序来模拟完成一个简单的DNS欺骗。完整的攻击实现工作量和难度都很大。为了降低难度，可以不实现中间人攻击，而是直接让受害者把DNS服务器修改为欺骗者的地址。