**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 交换机基本配置和网络层协议分析

指导教师 潘冰

实验项目编号 实验项目类型 验证型

实验地点 计算机网络实验室

学生姓名 许铭燊 学号 2019051106

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 10 月 12 日 下 午～ 10 月 12 日 下 午

**实验目的】**

1. 理解链路层、网络层主要协议格式，以及协议的工作原理
2. 理解网关和子网掩码概念
3. 学会利用网络嗅探器（如**Wireshark**）分析协议格式和协议的工作过程
4. 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。

**【实验内容】**

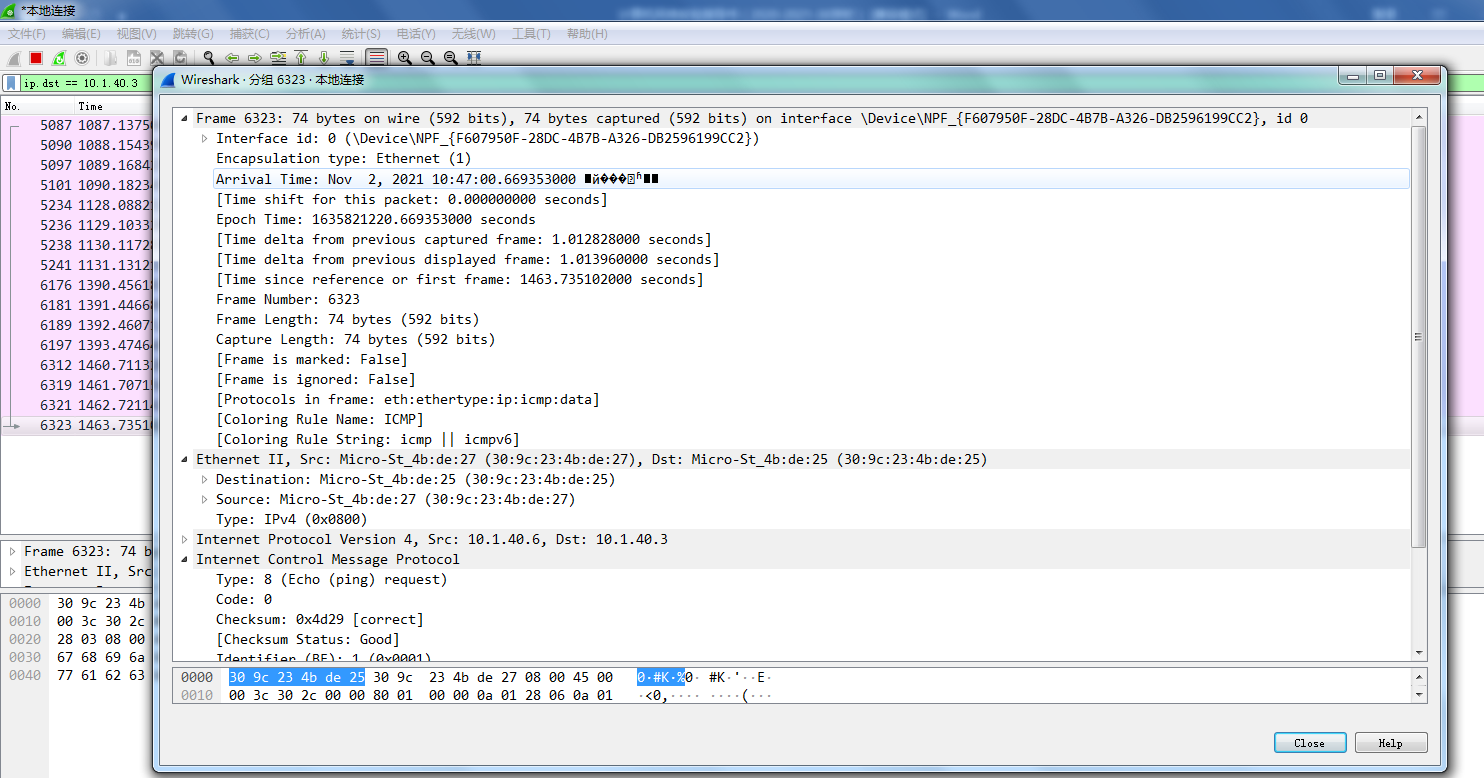
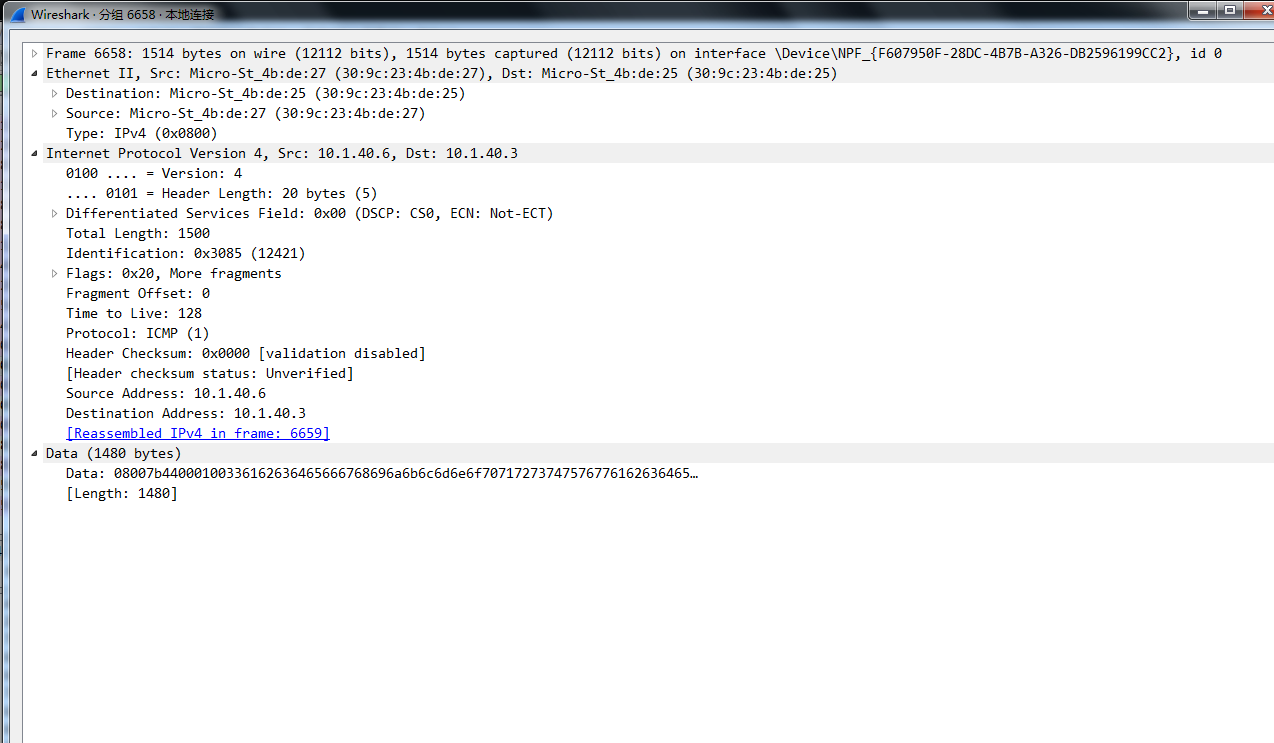
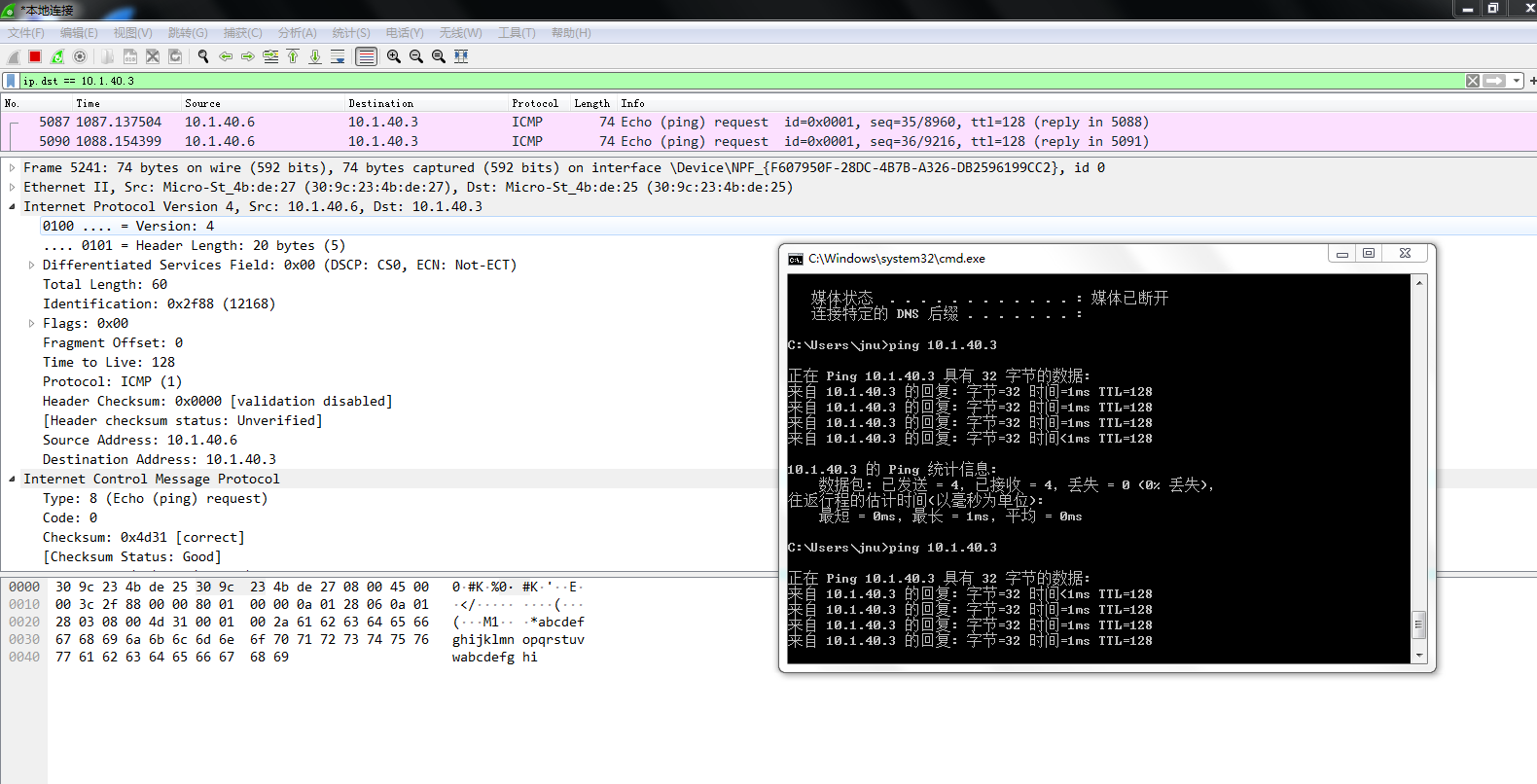
1. 用嗅探器捕获数据包。
2. 分析以太网帧、ARP协议、IP协议、ICMP协议格式
3. 分析PING、TRACERT、ARP命令的工作过程
4. 通过修改主机的网关为指定默认网关、本机IP地址或不设置网关，观察ping的结果，用嗅探器捕获数据包并分析。

**【实验步骤】**

1. 安装Wireshark
2. 以太网协议分析

从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。

1. ARP协议分析

* 进入DOS窗口，用arp – a 查看本机上的ARP表的情况，然后用 arp –d B 删除B的记录（如果有的话）；
* 运行Wireshark程序；
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；
* 从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；
* 通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址；
* 再次从主机A上向主机B发PING检测报文，或者再次从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文；
* 
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。

4、IP协议分析

* 从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;
* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。

1. ICMP协议分析

通过ping和tracet命令，了解ICMP协议的使用。

* 从主机A上向主机B发PING检测报文，捕获ICMP请求数据包和应答数据包，记录并分析各字段的含义，并与ICMP数据包格式进行比较；如果返回的差错信息，请分析是由于什么差错引起的。
* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。

**【思考题】（分析原因并通过实验验证）**

1. 在ARP包分析实验过程中，为什么A有时能捕获ARP报文，有时却不能捕获ARP报文？

答：请求报文是广播，目的mac地址是FF-FF-FF-FF-FF-FF。应答报文是单播，目的mac地址是本机的MAC地址。

1. 为什么运行ping 127.0.0.1时，不能捕获到ICMP报文？如果运行ping 本机IP地址能收到报文吗？ 为什么？

答：127.0.0.1直接定向本机,无ICMP，收IP地址经过路由，有ICMP，但ping本机可以。

1. 在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

答：前者是IP不正确，后者为局域网中DHCP分配IP，而DHCP失效

4、请通过实验**验证**：

主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。

主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

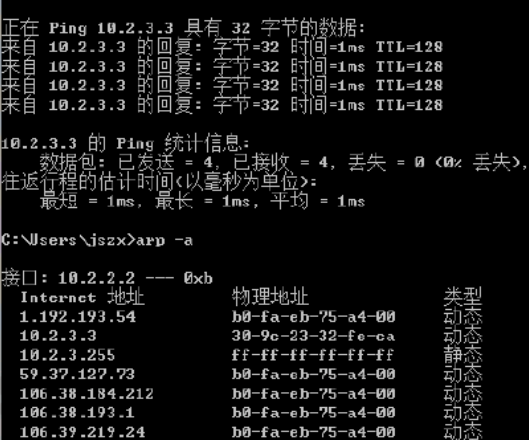
答：不设置网关同一网段，不设置网关不同网段，设置网关同一网段

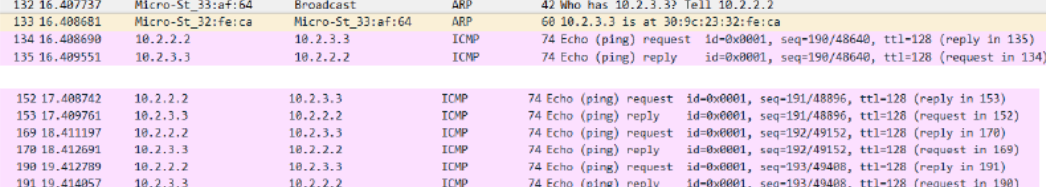
5、通过下面实验**理解网关**

假设主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。

假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/23，两主机不设置网关，分别在主机A和主机B上用ping测试与对方的连通性，用ARP查看物理地址。对测试结果进行分析。

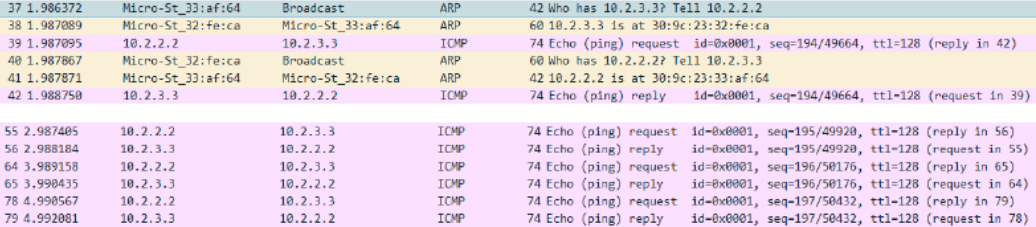
1. 不设网关



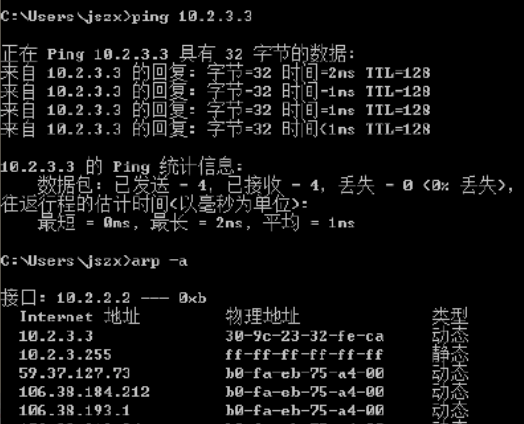


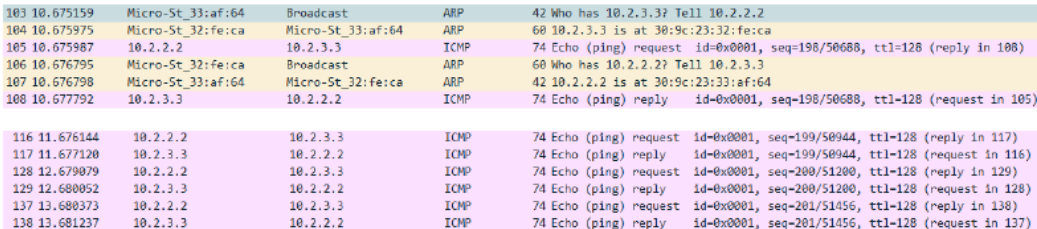
，不设网关后：





设本机地址为网关





设本机为网关

