**【实验名称】：**UDP用户数据报分析实验

**学生姓名：2151133**孙韩雅

**实验地点：**济事楼330 **实验时间：**2023-12-4

**【实验目的】**

了解UDP数据包的概念和应用特点，熟悉其报文格式，通过使用Cisco Packet Tracer仿真模拟软件以及Wireshark软件进行UDP数据报分析实验。

**【实验原理】**

1.UDP的概述

UDP是传输层的协议，功能即为在IP的数据报服务之上增加了最基本的服务：复用和分用以及差错检测。UDP提供不可靠服务，具有TCP所没有的优势。UDP无连接，时间上不存在建立连接需要的时延。空间上，TCP需要在端系统中维护连接状态，需要一定的销。此连接装入包括接收和发送缓存，拥塞控制参数和序号与确认号的参数。UCP不维护连接状态，也不跟踪这些参数，开销小。空间和时间上都具有优势。

2.UDP的应用特点

DNS如果运行在TCP之上而不是UDP，那么DNS的速度将会慢很多。HTTP使用TCP而不是UDP，是因为对于基于文本数据的Web网页来说，可靠性很重要。同一种专用应用服务器在支持UDP时，一定能支持更多的活动客户机。分组首部开销小，TCP首部20字节，UDP首部8字节。

UDP没有拥塞控制，应用层能够更好的控制要发送的数据和发送时间，网络中的拥塞控制也不会影响主机的发送速率。某些实时应用要求以稳定的速度发送，能容忍一些数据的丢失，但是不能允许有较大的时延（比如实时视频，直播等）。

UDP提供尽最大努力的交付，不保证可靠交付。所有维护传输可靠性的工作需要用户在应用层来完成。没有TCP的确认机制、重传机制。如果因为网络原因没有传送到对端，UDP也不会给应用层返回错误信息。

UDP没有拥塞控制，应用层能够更好的控制要发送的数据和发送时间，网络中的拥塞控制也不会影响主机的发送速率。某些实时应用要求以稳定的速度发送，能容忍一些数据的丢失，但是不能允许有较大的时延（比如实时视频，直播等）

UDP提供尽最大努力的交付，不保证可靠交付。所有维护传输可靠性的工作需要用户在应用层来完成。没有TCP的确认机制、重传机制。如果因为网络原因没有传送到对端，UDP也不会给应用层返回错误信息。

UDP是面向报文的，对应用层交下来的报文，添加首部后直接乡下交付为IP层，既不合并，也不拆分，保留这些报文的边界。对IP层交上来UDP用户数据报，在去除首部后就原封不动地交付给上层应用进程，报文不可分割，是UDP数据报处理的最小单位。正是如此UDP显得不够灵活，不能控制读写数据的次数和数量。比如我们要发送100个字节的报文，调用一次sendto函数就会发送100字节，对端也需要用recvfrom函数一次性接收100字节，不能使用循环每次获取10个字节，获取十次这样的做法。

UDP常用一次性传输比较少量数据的网络应用，如DNS,SNMP等，因为对于这些应用，若是采用TCP，为连接的创建，维护和拆除带来不小的开销。UDP也常用于多媒体应用（如IP电话，实时视频会议，流媒体等）数据的可靠传输对他们而言并不重要，TCP的拥塞控制会使它们有较大的延迟，也是不可容忍的。总之，UDP协议提供不可靠无连接的数据报传输服务。

3.UDP报文格式

UDP的首部格式：UDP数据报分为首部和用户数据部分，整个UDP数据报作为IP数据报的数据部分封装在IP数据报中，UDP数据报文结构如图1所示：

****

UDP首部有8个字节，由4个字段构成，每个字段都是两个字节：

1）源端口： 源端口号，需要对方回信时选用，不需要时全部置0。

2）目的端口：目的端口号，在终点交付报文的时候需要用到。

3）长度：UDP的数据报的长度（包括首部和数据）其最小值为8（只有首部）。

4）校验和：检测UDP数据报在传输中是否有错，有错则丢弃。该字段是可选的，当源主机不想计算校验和，则直接令该字段全为0。

当传输层从IP层收到UDP数据报时，就根据首部中的目的端口，把UDP数据报通过相应的端口，上交给应用进程。

如果接收方UDP发现收到的报文中的目的端口号不正确（不存在对应端口号的应用进程0），就丢弃该报文，并由ICMP发送“端口不可达”差错报文给对方。

UDP校验：在计算校验和的时候，需要在UDP数据报之前增加12字节的伪首部，伪首部并不是UDP真正的首部。只是在计算校验和，临时添加在UDP数据报的前面，得到一个临时的UDP数据报。校验和就是按照这个临时的UDP数据报计算的。伪首部既不向下传送也不向上递交，而仅仅是为了计算校验和。这样的校验和，既检查了UDP数据报，又对IP数据报的源IP地址和目的IP地址进行了检验。

UDP校验和的计算方法和IP数据报首部校验和的计算方法相似，都使用二进制反码运算求和再取反，但不同的是：IP数据报的校验和只检 验IP数据报的首部，但UDP的校验和是把首部和数据部分一起校验。

发送方，首先是把全零放入校验和字段并且添加伪首部，然后把UDP数据报看成是由许多16位的子串连接起来，若UDP数据报的数据部分不是偶数个字节，则要在数据部分末尾增加一个全零字节（此字节不发送），接下来就按照二制反码计算出这些16位字的和。将此和的二进制反码写入校验和字段。在接收方，把收到得UDP数据报加上伪首部（如果不为偶数个字节，还需要补上全零字节）后，按二进制反码计算出这些16位字的和。

当无差错时其结果全为1，否则就表明有差错出现，接收方应该丢弃这个UDP数据报。注意：

1）校验时，若UDP数据报部分的长度不是偶数个字节，则需要填入一个全0字节，但是此字节和伪首部一样，是不发送的。

2）如果UDP校验和校验出UDP数据报是错误的，可以丢弃，也可以交付上层，但是要附上错误报告，告诉上层这是错误的数据报。

3）通过伪首部，不仅可以检查源端口号，目的端口号和UDP用户数据报的数据部分，还可以检查IP数据报的源IP地址和目的地址。这种差错检验的检错能力不强，但是简单，速度快。

**【实验设备】**

HUAWEI MateBook X Pro（安装有Cisco Packet Tracer与Wireshark抓包分析工具）

【**实验步骤**】

1.设置WEB服务器和简单的DNS服务器。

2.使用PC2访问WEB服务器，产生UDP数据报文。

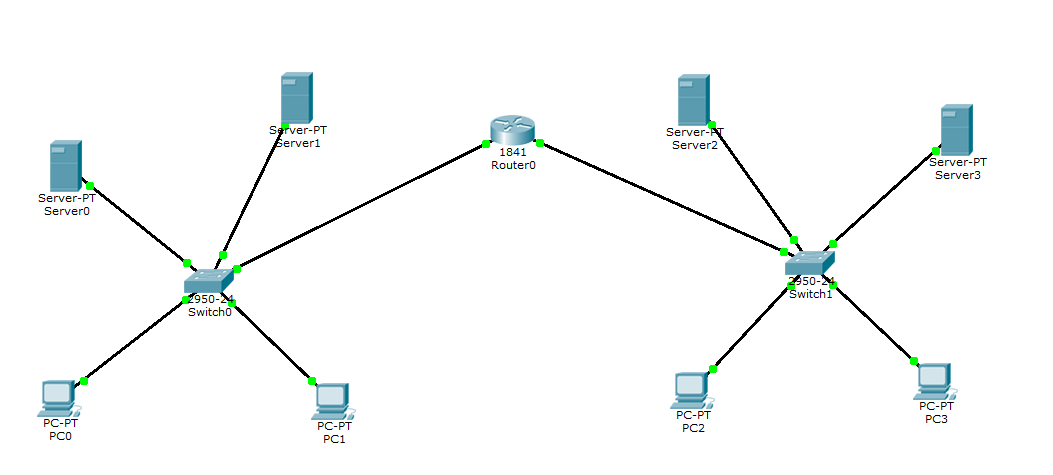
3.查看UDP报文详细内容。

4.使用WireShark软件抓取报文，并使用“udp”过滤器；

5.分析报文内容。

**【实验现象】**

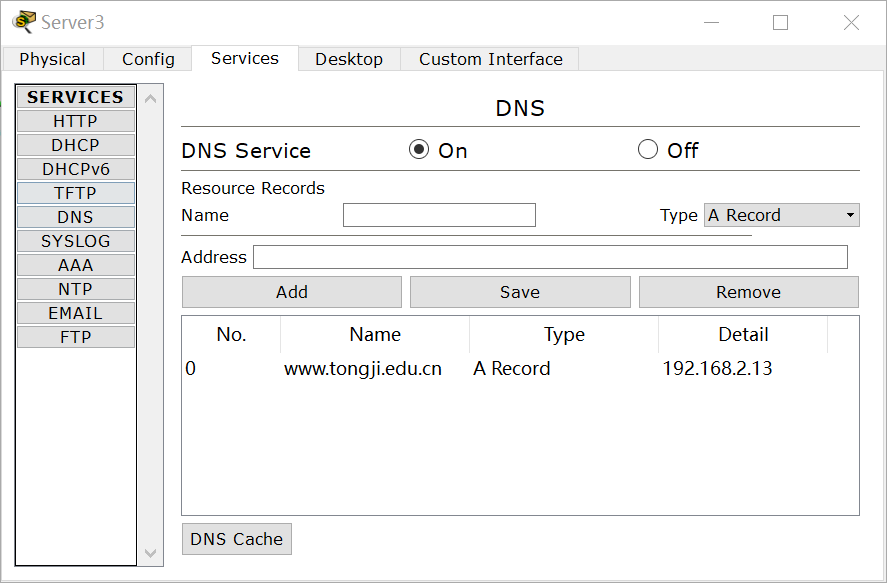
1.设置WEB服务器和简单的DNS服务器。



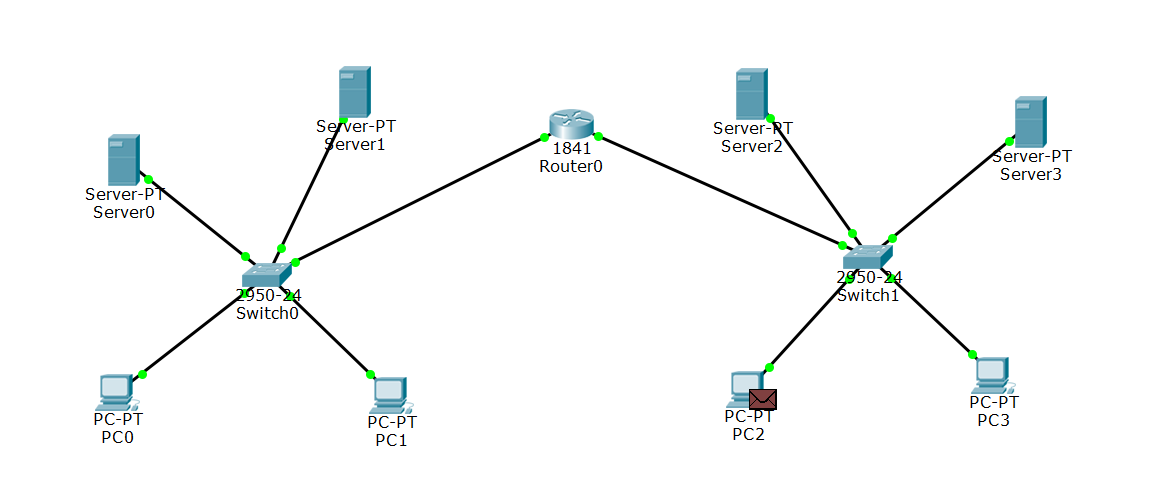
在Server2、3上配置gateway、ip、子网掩码。

在Server3上配置detail为server2的ip的DNS。

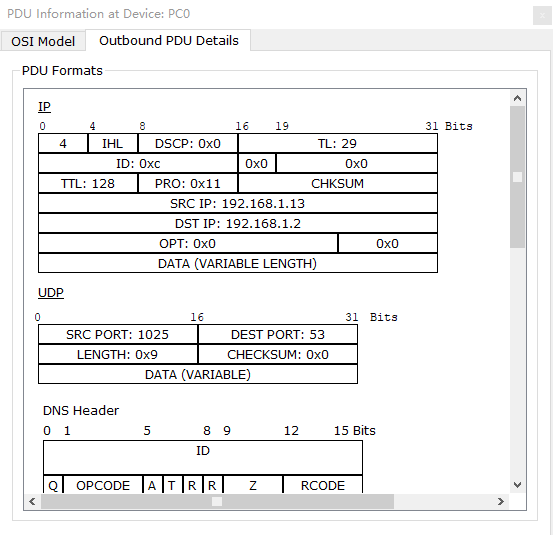
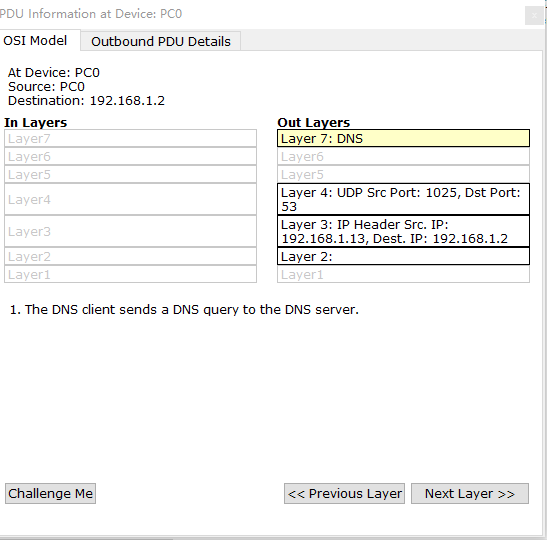
在WEB服务器上配置DNS。

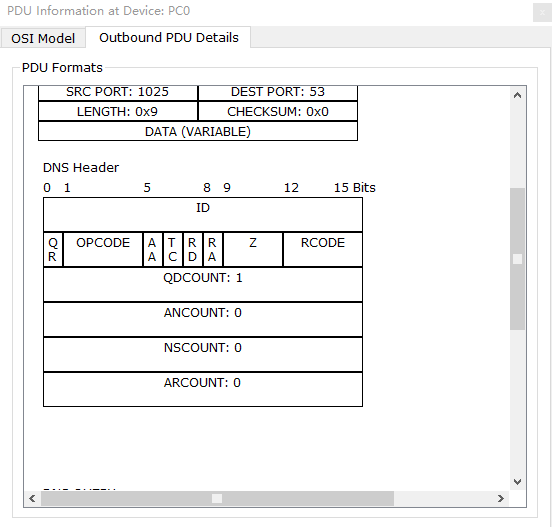


2.使用PC2访问WEB服务器，产生UDP数据报文。

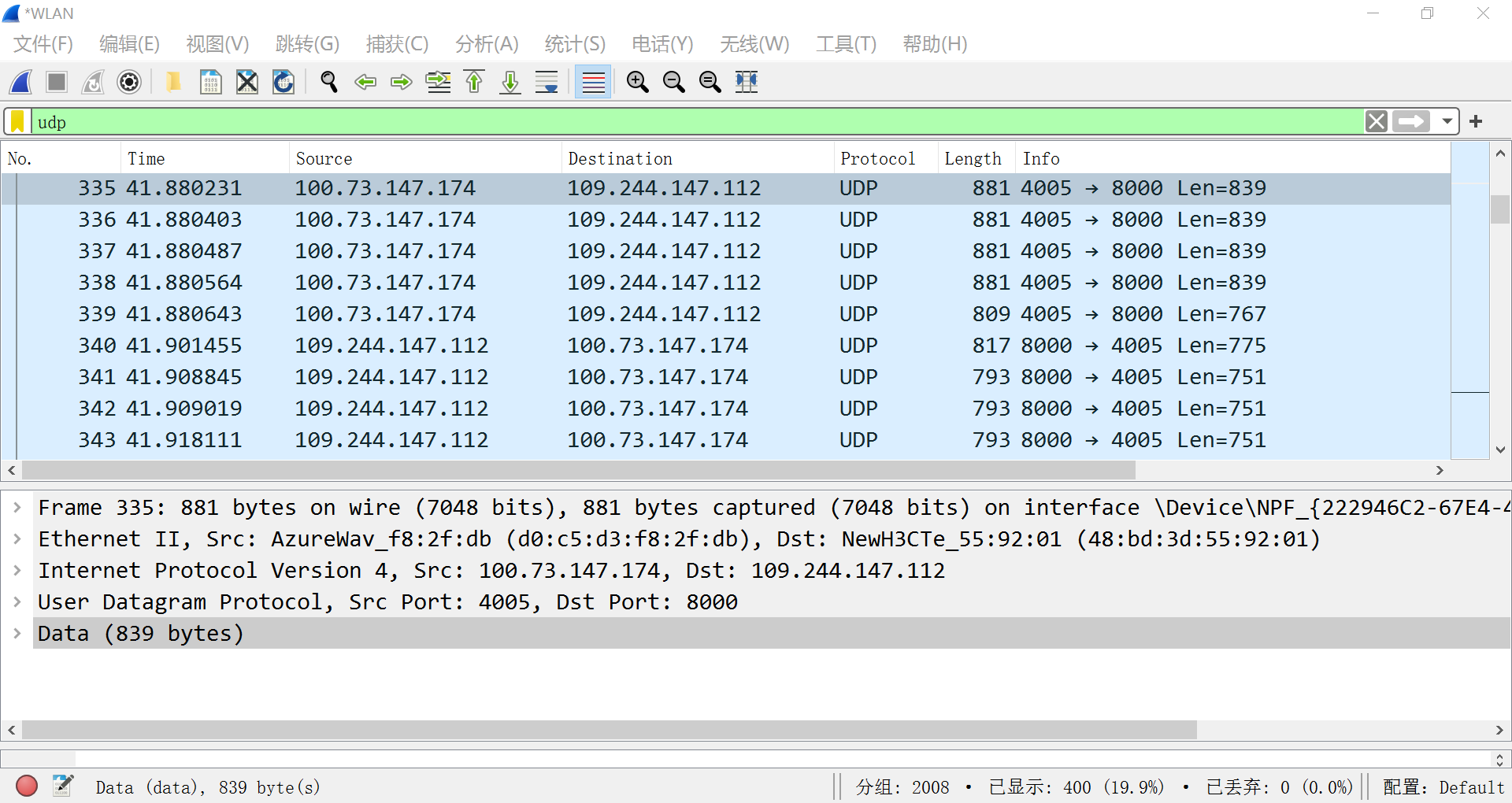


数据包内容如下图所示：

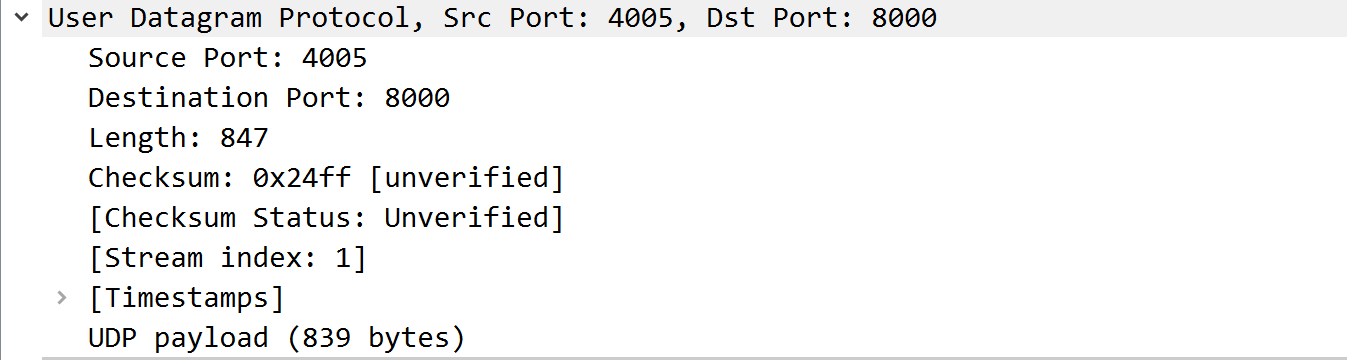




3.使用WireShark软件抓取报文，并使用“udp”过滤器：



4.分析报文内容。第四行为UDP协议部分，有源端口号、目的端口号、UDP首部和数据长度、校验和等内容。第五行Data为数据部分。前三行中，Frame部分有到达时间、新纪元时间、帧序号、帧长度、协议名称等内容；Ethernet部分有目的MAC地址、源MAC地址、协议版本等内容；Internet Protocal部分有目的IP地址、源IP地址等内容。



**【分析讨论】**

通过本次实验，我认识到UDP是一种无连接的、不可靠的协议。与TCP（传输控制协议）相比，UDP在数据传输上没有确认机制，也没有重传丢失的数据包。因此，在使用UDP时，我们需要注意数据的可靠性可能会受到影响。

UDP数据报的格式相对简单，它包含源端口、目的端口、长度和校验和等字段。在分析数据报时，我注意到可以通过这些字段来判断数据报的来源和目标，以及确定数据报的完整性。