**Lab24\_UDP数据包分析实验项目**

学生姓名：苏家铭 合作学生：无

实验地点：宿舍 实验时间：2023年12月20日

**【实验目的】**

通过使用UDP协议进行数据传输的实验，了解UDP协议的特点和应用场景。通过实验，可以掌握UDP协议的无连接、不可靠传输特性，理解UDP在少量数据传输和实时应用方面的优势。同时，实验还旨在熟悉UDP的报文格式和校验方法，理解UDP在网络通信中的作用和限制，为后续网络编程和应用开发提供基础和参考。

**【实验原理】**

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，需要一定的开销。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。 UDP数据报(用户数据报协议)

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。

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数据报文结构如图所示：



UDP数据报文结构

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）

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。

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 二进制反码计算出这些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】**

PC机一台，并安装有Cisco Packet Tracer软件

**【实验步骤】**

按照PPT提示放置网络设备，并连线

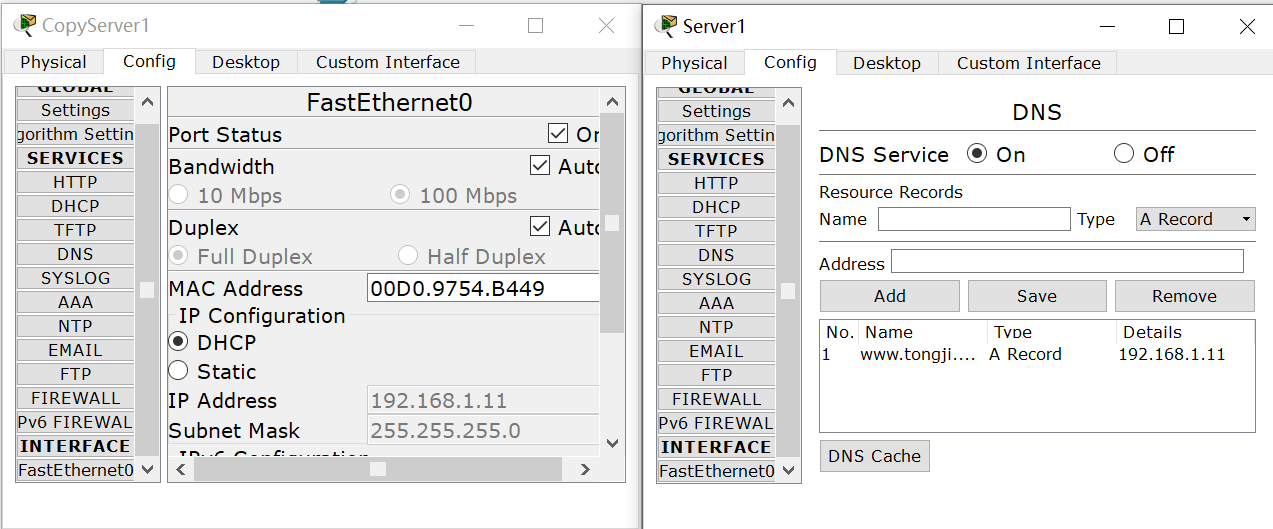
配置DNS服务器

设置仿真模式，设置网络请求

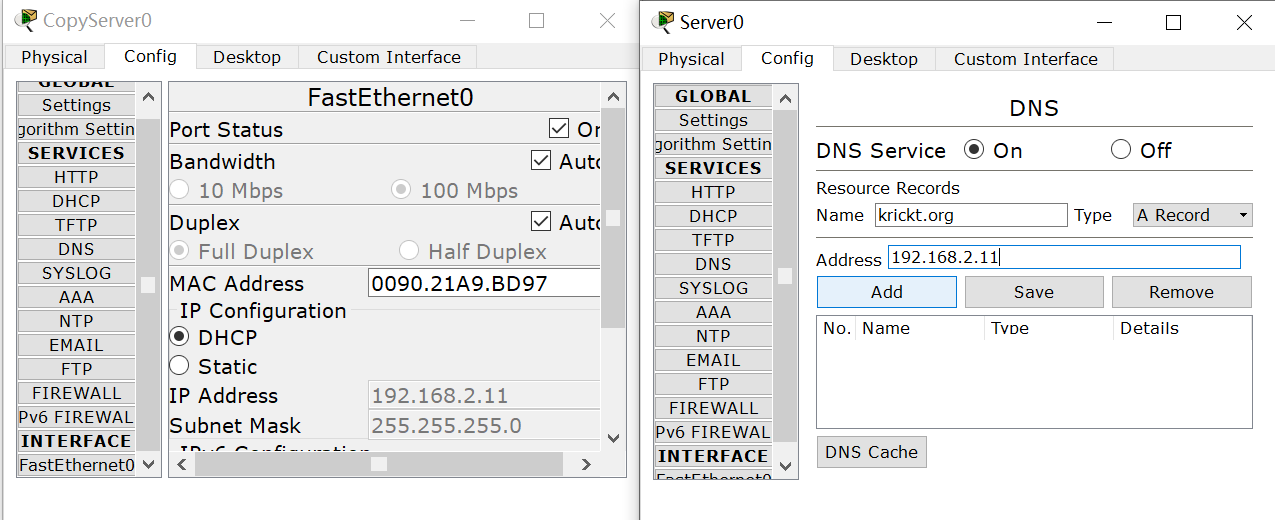
单步调试抓取UDP报文并分析

利用Wireshark抓取UDP报文并分析

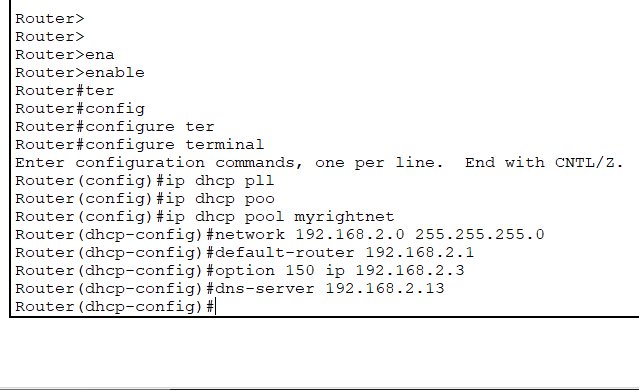
**【实验现象】**



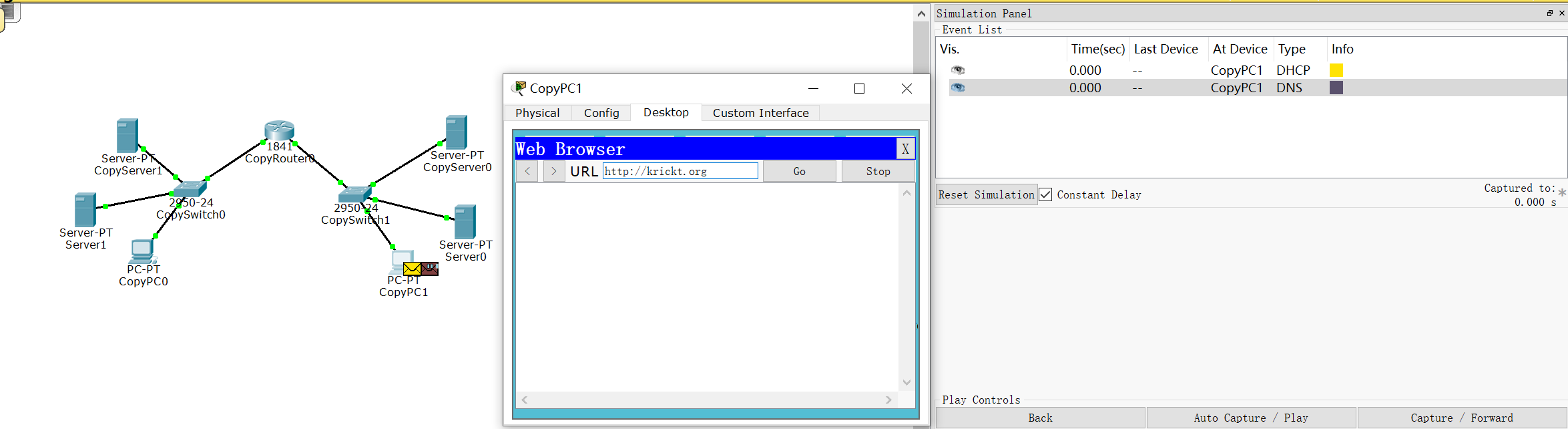
配置DNS



配置DNS



配置路由器DNS



网络拓扑图与CopyPC1发出去

|  |  |
| --- | --- |
|  |  |

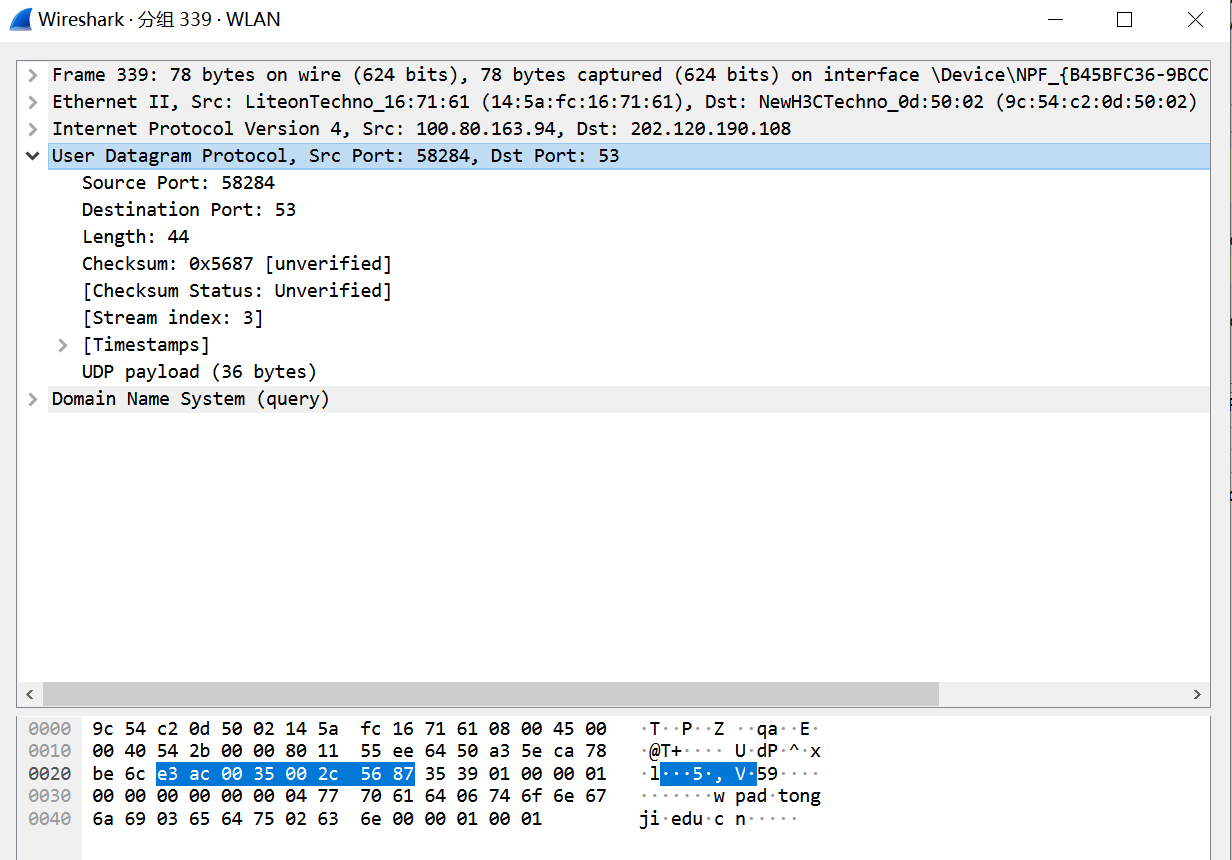
UPD报文结构

|  |  |
| --- | --- |
|  |  |

server0发出去

|  |  |
| --- | --- |
|  |  |

CopyPC1收到



wireshark捕捉UDP数据报文

**【分析讨论】**

这里分析wireshark捕捉的数据报文

e3 ac 00 35 00 2c 56 87

e3 ac表示src port为58284

00 35表示destination port为53

00 2c表示长度为44

56 87表示检验和

通过比较发现，UDP的头部比TCP少很多东西。者决定了UDP牺牲了可靠性，节省了额外的开销，提供了更高的性能和效率。

* 无连接性：UDP是一种无连接协议，不需要在数据传输之前进行建立连接的握手过程，从而减少了延迟和开销。相比之下，TCP需要建立连接、维护状态和执行可靠的数据传输，但提供了可靠的、有序的数据传输。
* 无可靠性：UDP报文不提供可靠性保证，它不保证数据传输的完整性、顺序性和可靠性。UDP报文没有确认机制，一旦发送出去就无法得知是否被正确接收。而TCP通过确认机制、重传机制和流量控制来确保数据的可靠传输。
* 简单轻量：UDP报文相对简单，它只包含了必要的头部信息，没有复杂的控制字段和拥塞控制机制。这使得UDP报文的开销小，传输效率高，适合在性能敏感的实时应用中使用。
* 适用场景：UDP由于其低延迟和高效性，适合用于实时通信、音频/视频传输、游戏、DNS查询等应用。在这些场景下，速度和实时性更加重要，而数据可靠性可以通过应用层的机制来处理。