**Lab22\_UDP 用户数据报分析实验项目**

学生姓名：苏家铭 合作学生：无

实验地点：济世楼 330 实验时间：2023 年 12 月 20 日

**【实验目的】**

UDP 协议是非常重要的传输层协议﹐人们常用的即时工具软件就是使用 UDP 作为传输层协议，UDP 用户数据包格式非常简单，了解 UDP 用户数据包有利于帮助理解传输层作用。本实验将借助 Tcpdump，捕获和分析 UDP 用户数据包。

1. 理解传输层作用。
2. 了解 UDP 用户数据包结构。

**【实验原理】**

UDP 是一种无连接的传输协议，全称为用户数据报协议（User DatagramProtocol）。UDP 为应用程序提供了一种无需建立连接就可以发送封装的 IP 数据包的方法。

相对于 TCP，UDP 有以下优势：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。同时 UDP 的分组首部开销小，TCP 首部 20 字节，UDP 首部 8 字节

作用方面，UDP 与 TCP 为传输层的两个主要协议，互为补充。UDP 为无连接，除了给应用程序发送数据包功能并允许它们在所需的层次上架构自己的协议之外，几乎没有做什么特别的事情。面向连接的是 TCP，该协议几乎做了所有关于连接的事情。

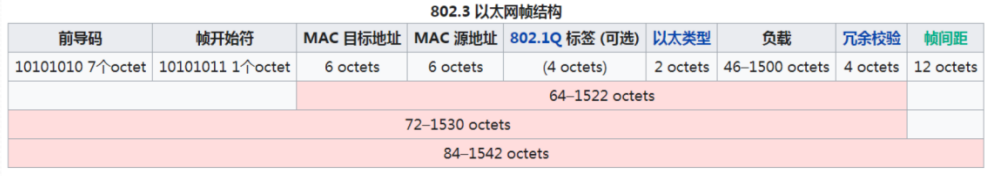
UDP 没有拥塞控制，应用层能够更好的控制要发送的数据和发送时间，网络中的拥塞控制也不会影响主机的发送速率。某些实时应用要求以稳定的速度发送，能容忍一些数据的丢失，但是不能允许有较大的时延（比如实时视频，直播等），UDP 就非常合适。

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。

DNS 是互联网的一项服务。它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。DNS 服务器保存了一张域名和与之相对应的 IP 地址表，以解析消息的域名。其它设备需要解析域名时向它们发送 DNS 请求获取结果。

DNS 服务使用 UDP 而不是 TCP。DNS 如果运行在 TCP 之上，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，能支持更多的活动客户机。

典型的以太网帧结构



典型的 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）。
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 伪首部



UDP 的校验和需要计算 UDP 首部加数据荷载部分，但也需要加上 UDP 伪首部。这个伪首部指，源地址、目的地址、UDP 数据长度、协议类型（0x11），协议类型就一个字节，但需要补一个字节的 0x0，构成 12 个字节。伪首部+UDP 首部+数据一起计算校验和。数据字节数不为偶数则补一个字节。

UDP 检验和的计算方法是：

按每 16 位求和得出一个 32 位的数；

如果这个 32 位的数，高 16 位不为 0，则高 16 位加低 16 位再得到一个 32 位的数；重复第 2 步直到高 16 位为 0，将低 16 位取反，得到校验和。

**【实验内容】**

1. 一个终端，启用 Tcpdump 工具软件，并设置相应过滤条件，从指定网卡捕获 UDP 用户数据包，对 UDP 用户数据包进行分析。
2. 另一个终端，使用 echo 命令，发送一串字符串重定向 Windows 节点一个 UDP 端口。

**【实验设备】**

实验环境主要由一台计算机组成，配有 ubuntu 环境。

**【实验步骤】**

1. 创建终端 1,启动抓包监听,以便在网络上捕获 UDP 用户数据包，“应用程序”-“附件”→“终端”。

监听 UDP 端口 5555; sudo tcpdump-xp-i enp0s3 udp and port 5555 口令:123456789,处于监听状态。

1. 产生 UDP 用户数据包。创建终端，使用 Linux 命令方式向 Windows 节点UDP5555 端口发送字符串,以触发 UDP 用户数据包。
2. 输入“echo 'networklab'>/dev/udp/192.168.1.254/5555”,将字符串重定向到 Windows 主机的 UDP5555 端口。
3. 分析捕获 UDP 数据包。终端 1,捕获了封装 UDP 用户数据包的 IP 数据包。
4. UDP 用户数据包前面是 IP 数据包头部,共 20 个字节,其中,IP 数据包头部中的第三组数标识IP包被封装的上层协议,对应IP数据包头部格式第三行前半行，TTL=Ox40,表示生存时间,折算成十进制是 64;type=0x1l,标识封装类型,折算成十进制 17,表示上层协议是 UDP 协议。
5. UDP 用户数据包头部分成两行,其余是 UDP 用户数据包数据体,即应用程序数据。1 个数字代表半个字节,每组 8 个数字刚好对应 UDP 用户数据包格式中一行,特意用矩形框分隔，下面按照格式中行顺序来分析数据含义。
6. 第一行 ,UDP SOURCE PORT=0xa109, 表 示 源 端 口 号 ;UDP DESTINATION PORT=OX15b3,表示目标端口号,折算成十进制为 5555。
7. 第二行,UDP MESSAGE LENGTH=0xl3,表示 UDP 用户数据包长度,19.个字节长,8 个字节头部,11 个字节数据;UDP CHECKSUM=0x8486,表示 UDP 用户数据包校验和。
8. 第三行+第四行+第五行,代表 UDP 数据体,0x6e65 7477 6f726b6c 6162,按照 ASCII 编码就是发送的字符串“networklab”; 0x0a，则代表 ASCII 编码换行,刚好是 11 个字节。

**【实验现象】**

1. 第一行：
2. **UDP SOURCE PORT（源端口号）:** 0xa109，表示16进制数，转换为十进制是41289。这是发送方使用的端口号。
3. **UDP DESTINATION PORT（目标端口号）:** 0x15b3，表示16进制数，转换为十进制是5555。这是接收方期望接收数据的端口号。
4. 第二行：
5. **UDP MESSAGE LENGTH（UDP用户数据包长度）:** 0x13，表示16进制数，转换为十进制是19。整个UDP用户数据包的长度为19个字节，包括头部和数据。
6. **UDP CHECKSUM（UDP用户数据包校验和）:** 0x8486，表示16进制数，转换为十进制是33926。这个字段用于校验数据包的完整性，以确保数据在传输过程中没有被篡改。
7. 第三行 + 第四行 + 第五行：

这部分代表UDP的数据体，即应用程序数据。

1. **0x6e65:** ASCII编码表示为 "ne"。
2. **0x7477:** ASCII编码表示为 "tw"。
3. **0x6f726b6c6162:** ASCII编码表示为 "orklab"。
4. **0x0a:** ASCII编码表示为换行符。

将这些ASCII编码组合在一起，得到的字符串是 "networklab"，符合实际的应用程序数据。

通过这个解析，我们可以更清晰地了解UDP用户数据包的各个字段的含义和作用。

UDP作为一种无连接、不可靠的传输协议，它的简单头部结构使其在某些场景下非常适用，尤其是对实时性要求高、可以容忍一定数据丢失的应用。

**【分析讨论】**

这次实验后我不仅学到了如何使用工具进行抓包，还深入了解了UDP（用户数据报协议）的数据包格式。这使我能够更深刻地分析获取到的包，特别是对UDP数据包头部格式有了更全面的认识。

UDP作为一种无连接、不可靠的传输协议，在一些特定的网络应用中发挥着关键作用，如DNS（域名系统）、SNMP（简单网络管理协议）等。相对于TCP，这些应用选择UDP主要是因为TCP在连接的创建、维护和拆除方面带来了较大的开销。UDP的轻量级特性使其成为一次性传输较少量数据的理想选择。

此外，我了解到UDP还广泛应用于多媒体应用，如IP电话、实时视频会议和流媒体等。在这些应用中，实时性是首要考虑因素，而对数据可靠性的要求相对较低。与TCP相比，UDP避免了拥塞控制可能带来的较大延迟，使得这些对实时性要求较高的应用能够更加流畅地运行。

总体而言，UDP协议提供了频繁的、不可靠的无连接的数据报传输服务，适用于那些对实时性要求较高，而对数据可靠性要求相对较低的场景。通过这次学习，我对UDP的应用场景有了更清晰的认识，这对我未来在网络领域的工作和学习中将会有着积极的影响，我爱计网实验给我的丰富知识。