

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 UDP 协议分析实验 指导教师雷小林、魏林锋

实验项目编号 实验项目类型 综合 实验地点 N117

学生姓名 陈宇 学号 2020101642

学院 信息科学技术学院 系 计算机系 专业 软件工程

实验时间2022年9月20日下午~9月20日 下 午 温度℃湿度

实验目的

1. 掌握 UDP 协议的报文格式
2. 掌握 UDP 协议校验和的计算方法
3. 理解 UDP 协议的优缺点
4. 理解协议栈对 UDP 协议的处理方法
5. 理解 UDP 上层接口应满足的条件

实验原理

1. UDP 协议介绍

UDP（用户数据报协议），主要用来支持那些需要在计算机之间传输数据的网络应用。包括网络视频会议系统在内的众多的客户/服务器模式的网络应用都需要使用 UDP 协议。

UDP 协议从问世至今已经被使用了很多年，虽然其最初的光彩已经被一些类似的协议所掩盖，但是即使是在今天，UDP 仍然不失为一项非常实用和可行的网络传输层协议。UDP 协议直接位于 IP 协议的上层。根据 OSI 参考模型，UDP 和 TCP 都属于传输层协议。UDP 协议不提供端到端的确认和重传功能，它不保证数据包一定能到达目的地，因此是不可靠协议。UDP 的熟知端口号如下表所示：

端口	协议	说明
7	Echo	把收到的数据报回送到发送端
9	Discard	丢弃收到的任何数据报
11	Users	活跃的用户
13	Daytime	返回日期和时间
17	Quote	返回日期和引用（译者注：可参阅 RFC856）
19	Chargen	返回字符串
53	Nameserver	域名服务
67	Bootps	下载引导程序信息的服务器端口
68	Bootpc	下载引导程序信息的客户端端口
69	TFTP	简单文件传送协议
111	RPC	远程过程调用
123	NTP	网络时间协议
161	SNMP	简单网络管理协议

162	SNMP	简单网络管理协议（陷阱）
520	RIP	路由信息协议

UDP 协议有以下特点：

- UDP 是面向事务的协议，它用最少的传输量为应用程序向其它程序发送报文提供了一个途径。
- UDP 是无连接的、不可靠的传输机制。在发送数据报前，UDP 在发送和接收两者之间不建立连接。
- UDP 让应用程序能直接访问网络层的数据报服务，例如分段和重组等网络层所提供的数据报服务。
- UDP 使用IP 协议作为数据传输机制的底层协议。
- UDP 报头和数据都以与最初传输时相同的形式被传送到最终目的地。
- UDP 不提供确认，也不对数据的到达顺序加以控制。因此 UDP 报文可能会丢失。不实现数据包的传送和重复检测。
- 当数据包在传送过程中发生错误时，UDP 不能报告错误。
- 吞吐量不受拥塞控制算法的调节，只受应用程序生成数据的速率、传输带宽、发送端和接收端主机性能的限制。

UDP 报文格式

每个UDP报文称为一个用户数据报（User Datagram），用户数据报分为两个部分：UDP首部和UDP数据。首部被分为四个 16 位的字段，分别代表源端口号、目的端口号、报文的长度以及 UDP 校验和。

源端口（16 位）	目的端口（16 位）
有效负载长度（16 位）	校验和（16 位）
数 据	
.....	

- 源端口：该字段表示发送端的端口号。如果源端口没有使用，那么此字段的值就被指定为 0。这是一个可选的字段。不同的应用程序使用不同的端口号，UDP 协议使用端口号为不同的应用程序保留其各自的数据传输通道，从而实现了同一时间段内多个应用程序可以一起使用网络进行数据的发送和接收。

- 目的端口：该字段表示数据包被发往的目的端的端口号。

- 有效负载长度：该字段表示包括 UDP 首部和 UDP 数据在内的整个用户数据报的长度。该字段的最小值是 8。数据报的最大尺寸随操作系统的不同而不同。在两字节字段中，理论上数据报最多可达 65535 字节。然而，一些 UDP 实现将数据报的大小限制到了 8192 字节。

- 校验和：UDP 的校验的校验范围包括伪首部（IP 首部一部分字段）、UDP 首部和UDP 数据，该字段是可选的。如果该字段值为零就说明不进行校验。

UDP 封装

当进程有报文要通过 UDP 发送时，它就把这个报文连同一对套接字地址以及数据的长度传递给 UDP。UDP 收到数据后就加上 UDP 首部。然后 UDP 就把这用户数据报连同套接字地址一起传递给 IP。IP 加上自己的首部，在高层协议类型字段使用值 17，指出该数据是从 UDP协议来的。这个 IP 数据报再传递给数据链路层。数据链路层接收到 IP 数据报后，加上自己的首部（可能还有尾部），再传给物理层。物理层把这些位编码为电信号或光信号，把它发送到远程的主机。如下图所示：



暨南大学本科实验报告专用纸(附页)

UDP 校验和

UDP 校验和的计算与IP 和ICMP 校验和的计算不同。UDP 校验和校验的范围包括三部分：伪首部、UDP 首部以及从应用层来的数据。伪首部是 IP 首部的一部分，其中有些字段要填入0。用户数据报封装在 IP 数据包中。如下图所示：



若校验和不包括伪首部，用户数据报也可能是安全的和正确的。但是，若 IP 首部受到损伤，则它可能被交付到错误的主机。

伪首部中包含高层协议类型字段是为了确保这个数据包是属于 UDP 而不是属于 TCP（参见实验 5.1）的。使用 UDP 的进程和使用 TCP 的进程可以使用同一个端口号。UDP 的高层协议类型字段是 17。若在传输过程中这个值改变了，在接收端计算校验和时就可检测出来，UDP 就可丢弃这个数据包。这样就不会交付给错误的协议。

2. 套接字地址

一个 IP 地址与一个端口号结合起来就叫做一个套接字地址。客户套接字地址惟一地定义了客户进程，而服务器套接字地址惟一地定义了服务器进程。

要使用 UDP 的服务，就需要一对套接字地址：客户套接字地址和服务器套接字地址。客户套接字地址指定了客户端的 IP 地址和客户进程，服务器套接字地址指定了服务器的 IP 地址和服务器进程。

3 . 实验环境与说明

实验设备和连接图如图 35 所示，一台锐捷 S2126G 交换机连接了 2 台 PC 机，分别命名为主机 A、主机 B，交换机命名为 Switch。

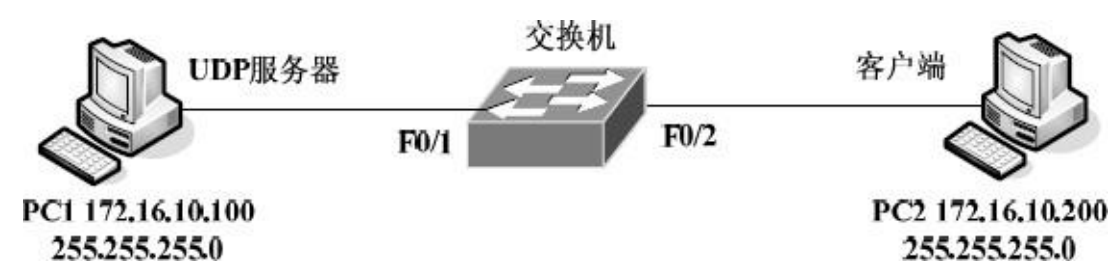


图35 UDP 协议分析实验连接图

暨南大学本科实验报告专用纸(附页)

每六名同学为一组，其中每两人一小组，每小组各自独立完成实验。将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

Ip地址： a: 172.23.65.91 b: 172.23.65.92
Mac_a: 18 60 24 7d 05 9c mac_b: 3c 52 82 7a d1 58

实验步骤

练习一、编辑并发送 UDP 数据报

本练习将主机 A和B 作为一组，主机 C和D 作为一组，主机 E 和F 作为一组。现仅以主机A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

步骤1： 主机 A 打开协议编辑器，编辑发送给主机 B 的 UDP 数据报。

MAC 层：

- 目的 MAC 地址：接收方 MAC 地址
- 源 MAC 地址：发送方 MAC 地址
- 协议类型或数据长度：0800，即 IP 协议

IP 层：

- 总长度：包括 IP 层、UDP 层和数据长度
- 高层协议类型：17，即 UDP 协议
- 首部校验和：其它所有字段填充完毕后填充此字段
- 源 IP 地址：发送方 IP 地址
- 目的 IP 地址：接收方 IP 地址

UDP 层：

- 源端口：1030
- 目的端口：大于 1024 的端口号
- 有效负载长度：UDP 层及其上层协议长度

其它字段默认，计算校验和。

- UDP 在计算校验和时包括哪些内容？
答：用到了：udp伪首部，udp首部，应用层数据
- UDP 是否可以使用 0 作为校验和进行通信？
答：可以：如果为0，则代表不进行校验

步骤2： 在主机B 上运行Wireshark 捕获数据，并设置过滤条件（提取 UDP 协议） 步骤
3： 主机 A 发送已编辑好的数据报。
步骤4： 主机 B 停止捕获数据，在捕获到的数据中查找主机 A 所发送的数据报。将截获的结果命名为 UDP-学号并保存，分析 UDP 报文结构，
回答如下问题。

1) UDP 报文头部有几个字段，绘制 UDP 报文的结构图。

答：首部：源端口，目的端口，有效负载长度，校验和

源端口（16 位）	目的端口（16 位）
有效负载长度（16 位）	校验和（16 位）
数 据	



2) 选择第一个 UDP 报文，分析其结构，填写表 14。

表14 UDP 报文分析

IP 报文	源IP 地址	172. 23. 65. 91		协议	Udp 17
	目的 IP 地址	172. 23. 65. 92		总长度	60
UDP 报文	字段名	字段长度	字段值	字段表达信息	
	源端口	16位	1030	表示发送端的端口号	
	目的端口	16位	1688	该字段表示数据包被发往的目的端的端口号	
	长度	16位	40	该字段表示包括 UDP 首部和 UDP 数据在内的整个用户数据报的长度	
	校验和	16位	6f76	UDP 的校验的校验范围包括伪首部（IP 首部一部分字段）UDP 首部和UDP 数据，该字段是可选的。	

3) UDP 报文与 TCP 报文有何不同？体会 UDP 协议和 TCP 协议的区别。

答：

UDP 是一种无连接协议，而 TCP 是一种面向连接的协议。TCP 比 UDP 要慢，这是两种协议的主要区别之一。

总的来说，UDP 是一种更快、更简单、更高效的协议。但是只有 TCP 允许对丢失的数据包进行重新传输。

TCP 和 UDP 的另一个区别是 TCP 可以确保数据从用户到服务器的有序传输（反之亦然）。UDP 不是为端到端通信而设计的，并不会检查接收方的准备情况，因此它需要相对更少的开销并占用更少的空间。

4) 为什么 UDP 协议的“校验和”要包含伪首部？

答：收到这个udp的对端也做同样的校验和计算，如果接收端IP层传递了错误的数据报到UDP层的话（目的ip不是本机ip或者协议类型不对），校验和就会不一致，丢弃包。

5) 比较 UDP 和 IP 的不可靠程度？

答：UDP和IP都是无连接的协议 和不可靠传输的协议。UDP用户数据报和IP数据报的首部都有校验和字段。当校验出有差错时，就把收到的UDP用户数据报或IP数据包丢弃。这是它们的相同之处。

但UDP和IP的可靠性是有区别的。UDP用户数据报的校验是既检验首部，又要检验数据部分，而IP数据报的校验仅仅检验首部。UDP用户数据报的校验还增加了伪首部，即 还检验了下面IP数据报的源IP地址和目的IP地址。

练习二、UDP 广播通信

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

步骤1：主机B、C、D、E、F上启动实验平台工具栏中的“UDP工具”，作为服务器端，监听端口设为 2483。

步骤 2：主机 B、C、D、E、F 运行Wireshark 捕获数据，并设置过滤条件（提取 UDP 协议）

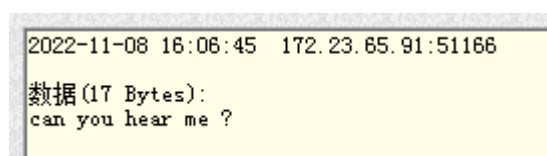
步骤3：主机 A 上启动UDP 工具，作为客户端，以 255. 255. 255. 255 为目的地址，以 2483 为端口，填写数据并发送。

暨南大学本科实验报告专用纸(附页)



步骤4: 察看主机 B、C、D、E、F 上的“UDP 工具”接收的信息。

- 哪台主机能够接收到主机 A 发送的 UDP 报文?



答: 都能收到。

步骤5: 察看 Wireshark 捕获的 UDP 报文, 并回答以下问题:

- 主机 A 发送的报文的目的 MAC 地址和目的 IP 地址的含义是什么?

答: 含义: mac: ff. ff. ff. ff. ff. ff 广播地址

IP: 255. 255. 255. 255 同一个局域网的广播

思考问题:

- 1) 如果将目的 MAC 地址换成某一个主机的 MAC 地址, 是否所有主机还会收到这种报文?

答: 不会。

- 2) 如果将目的 MAC 地址设成广播地址, 目的 IP 设成某一主机的 IP 地址, 结果怎样?

答: 同样是只有该主机能收到, 其他主机将数据抛弃。

- 3) 在可靠性不是最重要的情况下, UDP 可能是一个好的传输协议。试给出这种特定情况的一些示例。

答: UDP是一种不可靠的网络协议, 但在有些情况下UDP协议可能会变得非常有用。因为UDP具有TCP所望尘莫及的速度优势。虽然TCP协议中植入了各种安全保障功能, 但是在实际执行的过程中会占用大量的系统开销, 无疑使速度受到严重的影响。反观UDP由于排除了信息可靠传递机制, 将安全和排序等功能移交给上层应用来完成, 极大降低了执行时间, 使速度得到了保证。

- 4) UDP 协议本身是否能确保数据报的发送和接收顺序?

答: UDP是一种不可靠无连接的网络协议, 与可靠连接协议TCP相比, 它**不能保证发送的数据一定能被对方按顺序收到**, 如果数据在传送的过程中丢失, 它也不会自动重发。

暨南大学本科实验报告专用纸(附页)

实验总结

通过实验掌握了 UDP 协议的报文格式
通过实践掌握了 UDP 协议校验和的计算方法
通过学习和查询理解了 UDP 协议的优缺点
理解了协议栈对 UDP 协议的处理方法
理解了 UDP 上层接口应满足的条件

