

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 用户数据报协议 (UDP) 指导老师 某某某
实验项目编号 5 实验项目类型 综合类 实验地点 N117
学生姓名 某某 学号 XXXXXXXX
学院 网络空间安全学院 系 专业 网络空间安全
实验时间 2020 年 11 月 11 日 晚 上 ~ 2020 年 11 月 11 日 晚 上

(一) 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

(二) 实验环境

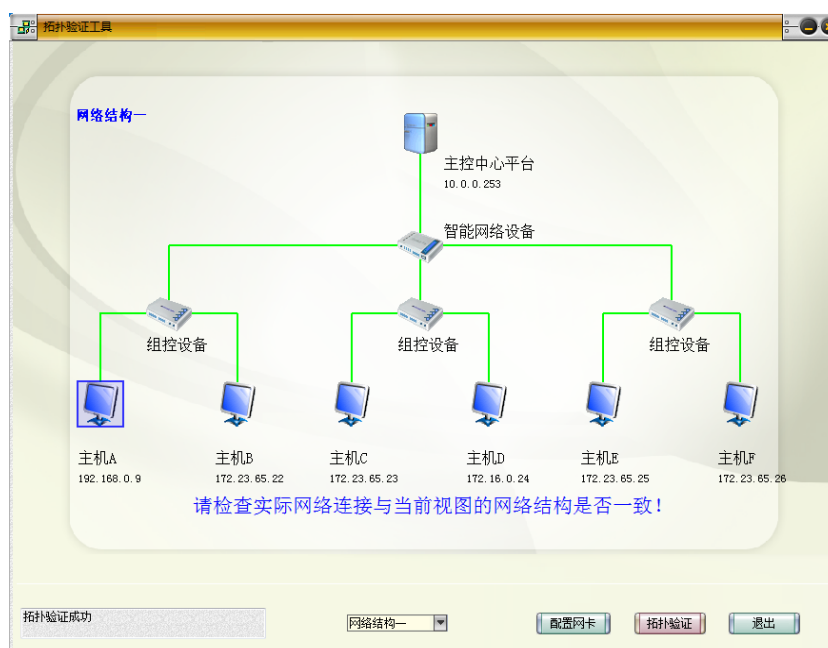


图 1：实验环境（该实验采用网络结构一，本机为主机 A）

(三) 实验原理

1. 进程到进程的通信

IP 协议负责主机到主机的通信。作为一个网络层协议，IP 协议只能把报文交付给目的主机。这是一种不完整的交付，因为这个报文还没有送交到正确的进程。像 UDP 这样的传输层协议负责进程到进程的通信。UDP 协议负责把报文交付到正确的进程。

1) 端口号

在网络中，主机是用 IP 地址来标识的。而要标识主机中的进程，就需要第二个标识符，这就是端口号。在 TCP/IP 协议族中，端口号是在 0~65535 之间的整数。

在客户/服务器模型中，客户程序使用端口号标识自己，这种端口号叫做短暂端口号，短暂的意思是生存时间比较短。一般把短暂端口取为大于 1023 的数，这样可以保证客户程序工作得比较正常。

服务器进程也必须用一个端口号标识自己。但是这个端口号不能随机选取。如果服务器随机选取端口号，那么客户端在想连接到这个服务器并使用其服务的时候就会因为不知道这个端口号而无法连接。TCP/IP 协议族采用熟知端口号的办法解决这个问题。每一个客户进程都必须知道相应的服务器进程熟知端口号。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

在一个 IP 数据包中，目的 IP 地址和端口号起着不同的寻址作用。目的 IP 地址定义了在世界范围内惟一的一台主机。当主机被选定后，端口号定义了在这台主机上运行的多个进程中的一个。

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。

2. UDP 协议简介

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 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。

3. UDP 报文格式

下图显示了 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。

（四）实验步骤

练习1 编辑并发送 UDP 数据报

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。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。

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：在其它字段填充完毕后计算并填充。

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？

协议字段（IP 层的高层协议类型）、源 IP 地址、目的 IP 地址、长度（UDP 数据总长度）、UDP 首部、UDP 数据

2. 在主机 B 上启动协议分析器捕获数据，并设置过滤条件（提取 UDP 协议）。

3. 主机 A 发送已编辑好的数据报。
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。为什么 UDP 协议的“校验和”要包含伪首部？

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，则他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报是属于 UDP 而不是属于 TCP 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 就可丢弃这个数据报，这样就不会交付给错误的协议。

比较 UDP 和 IP 的不可靠程度？

二者都是不可靠的。IP 协议负责主机到主机的通信。作为一个网络层协议，IP 协议只能把报文交付给目的主机。这是一种不完整的交付，因为这个报文还没有送交到正确的进程。像 UDP 这样的传输层协议负责进程到进程的通信。UDP 协议负责把报文交付到正确的进程。

练习2 UDP 单播通信

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

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，监听端口设置为 2483，“创建”成功。
2. 主机 C、E 上启动协议分析器开始捕获数据，并设置过滤条件（提取 UDP 协议）。
3. 主机 A 上启动实验平台工具栏中的“UDP 工具”，作为客户端，以主机 C 的 IP 为目的 IP 地址，以 2483 为端口，填写数据并发送。
4. 察看主机 B、C、D、E、F 上的“UDP 工具”接收的信息。

● 哪台主机上的“UDP 工具”能够接收到主机 A 发送的 UDP 报文？C 主机

5. 察看主机 C 协议分析器上的 UDP 报文，并回答以下问题：● UDP 是基于连接的协议吗？阐述此特性的优缺点。

UDP 不是基于连接的协议，是无连接的协议。

优点：传输效率高，无需编码。无需创建以及断开连接。当某个程序的目标是尽快地传送尽可能多的信息（其中任意给定数据的重要性相对较低）时，可使用 UDP 协议。

缺点：安全性低，它不能保证数据包以正确的顺序被接收，也不能保证数据会准确无误到达目的地。

● UDP 报文交互中含有确认报文吗？阐述此特性的优缺点。

UDP 交互中不含有确认报文。优点是提高了传输效率，缺点是传输过程中可能有丢失、重复、乱序等错误。

6. 主机 A 上使用协议编辑器向主机 E 发送 UDP 报文，其中：
目的 MAC 地址：E 的 MAC 地址

目的 IP 地址：主机 E 的 IP 地址

目的端口：2483

校验和：0

有效负载长度：UDP 层及其上层协议长度

首部校验和：其它所有字段填充完毕后填充此字段

总长度：包括 IP 层、UDP 层和数据长度

发送此报文，并回答以下问题：

● 主机 E 上的 UDP 通信程序是否接收到此数据包？UDP 是否可以使用 0 作为校验和进行通信？

能收到。可以使用 0 作为校验和通信。

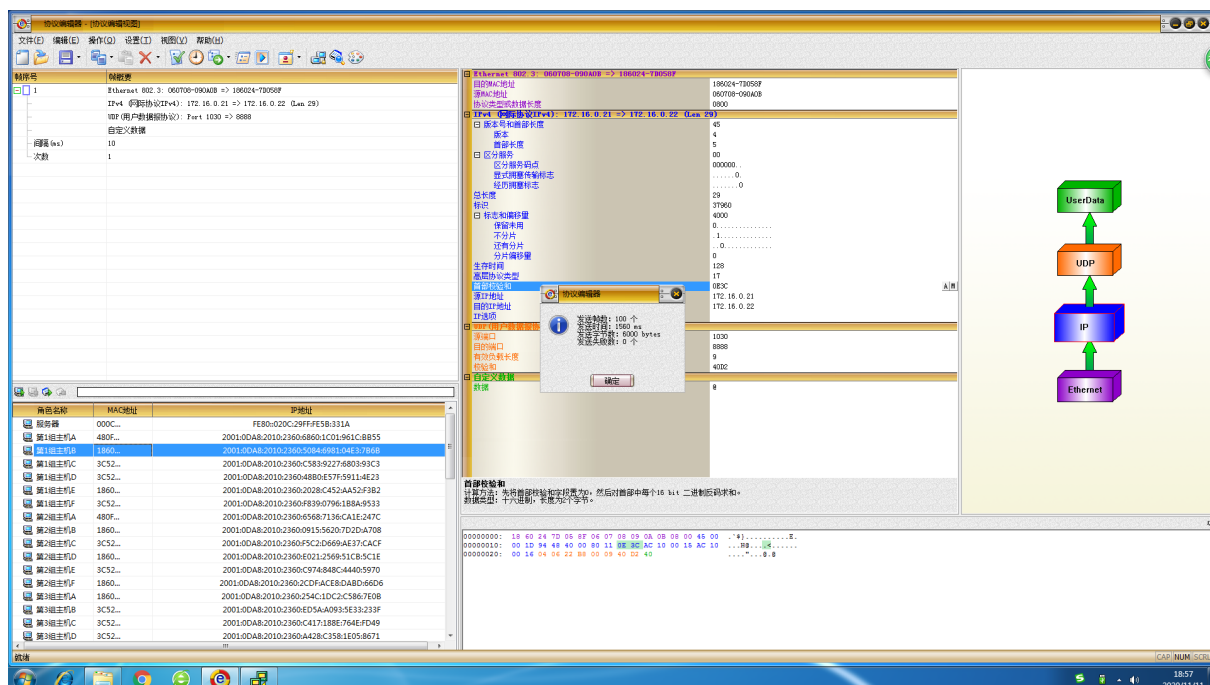
7. 主机 B、C、D、E、F 关闭服务端，主机 A 关闭客户端。

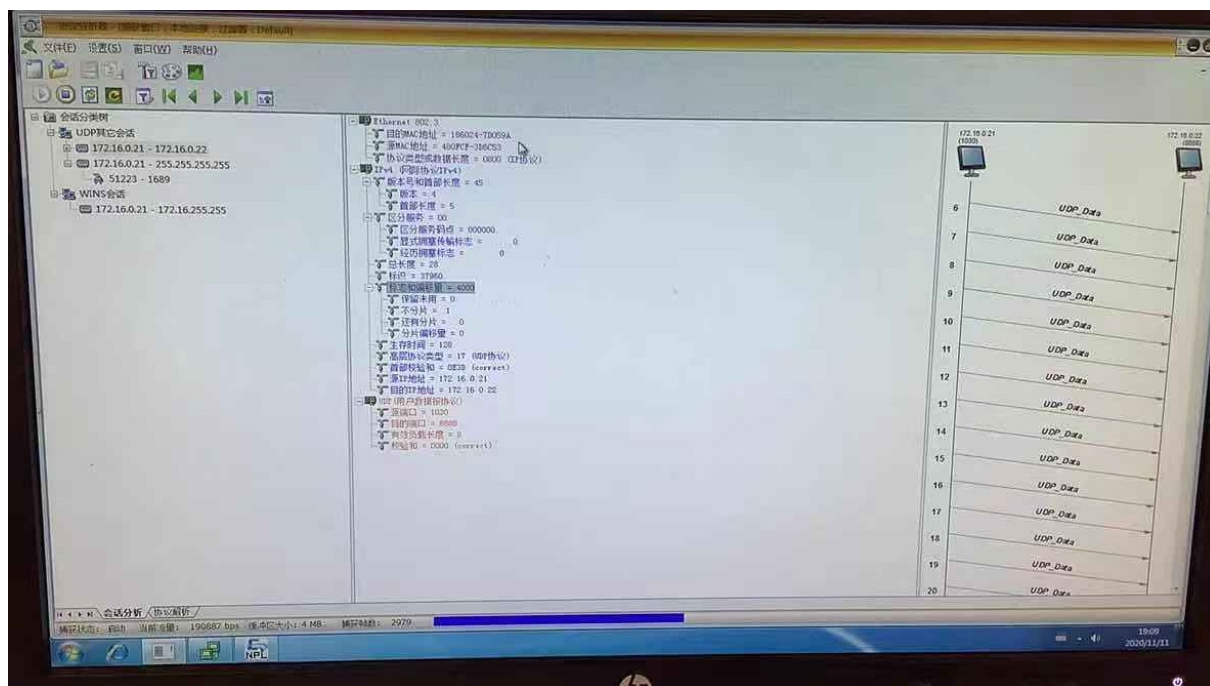
● 思考 UDP 的差错处理能力。

UDP 在一个非常低的水平上完成差错处理。UDP 没有流量控制机制，在收到分组时也没有确认。但是，UDP 提供了某种程度的差错控制。如果 UDP 检测出在收到的分组中有差错，它就偷偷地丢弃这个分组，使报文不能发送成功，而当校验和计算正确时，报文就可以成功发送。

(五) 实验结果与分析

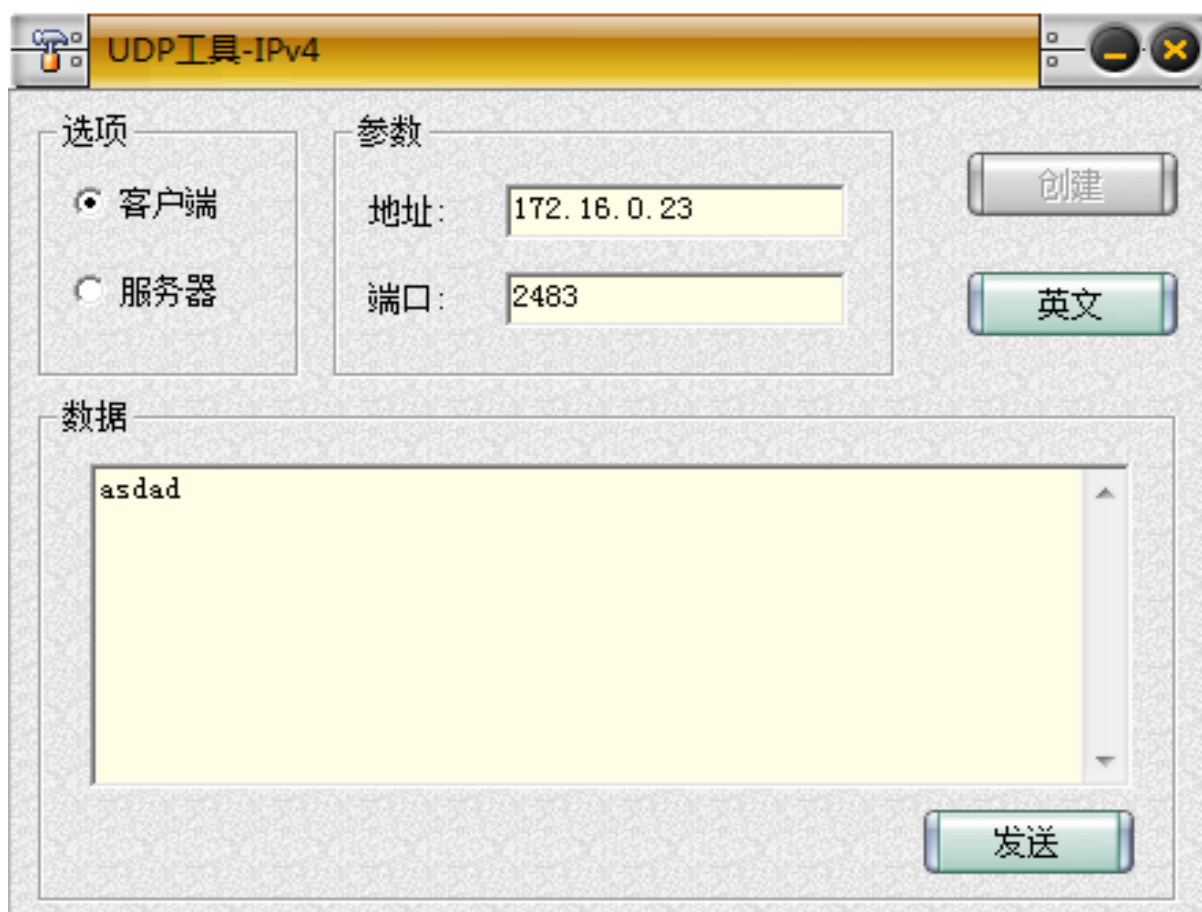
练习1 编辑并发送 UDP 数据报





分析：A 主机（本机）发送 UDP 报文至 B 主机。

练习2 UDP 单播通信



分析：A 主机（本机）向 E 主机发送一个 UDP 报文，E 主机成功收到。

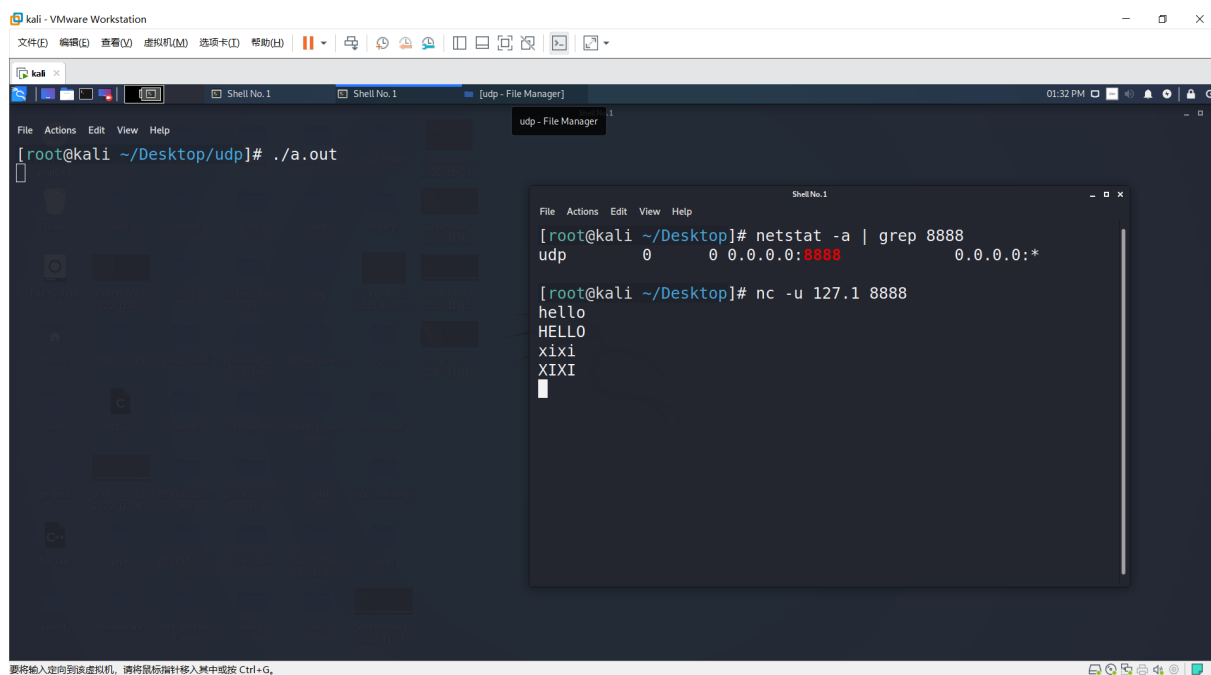
(六) 附录

因为之前对网络编程感兴趣，所以看了 APUE 和 UNP。这次是实现一个非常精简的 udp 反射服务器。

暨南大学本科实验报告专用纸(附页)

简要说明

1. 由于 udp 是无连接的，所以服务端很简单，监听端口，回射消息就行了。
2. 小程序实现把小写字母转化成大写字母。



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The main terminal window displays the command `./a.out` being executed. A secondary terminal window, titled "Shell No. 1", shows the output of `netstat -a | grep 8888`, which lists a UDP listener on port 8888. Below this, the same terminal window shows the output of `nc -u 127.1 8888`, displaying the received messages: "hello", "HELLO", "xixi", and "XIXI".

```
[root@kali ~/Desktop/udp]# ./a.out
```

```
[root@kali ~/Desktop]# netstat -a | grep 8888
udp        0          0 0.0.0.0:8888          0.0.0.0:*
```

```
[root@kali ~/Desktop]# nc -u 127.1 8888
hello
HELLO
xixi
XIXI
```