|  |
| --- |
| 实验目的： |
| ·了解原始套接字的基本概念和使用方法；  ·掌握路由器进行IP 数据报转发的基本原理；  ·实现基于原始套接字的IP 数据报的发送和接收；  ·实现基于原始套接字的IP 数据报转发，包括AF\_INET 和AF\_PACKET 原始套接字的应用。 |
| 实验内容： |
| （1）使用虚拟机实现多主机间的UDP 数据报收发及转发  利用虚拟机搭建实验环境，掌握Linux 下的Socket 网络编程。改进程序，示例程序只实现了一个数据包（携带1 条消息）的发、转、收过程，要求实现每条消息由控制台输入，并且不限制发送消息的数目。  （2）基于单网口主机的IP 数据转发及收发  在局域网中，模拟IP 数据报的路由转发过程。通过原始套接字实现了完整的数据封装过程，实现了UDP 头部、IP 头部、MAC 帧头部的构造。扩展实验的网络规模，由原始方案中3 台主机增加到不少于5 台主机，共同完成IP 数据报转发及收发过程，要求采用转发表改进示例程序，增加程序通用性。  （3）基于双网口主机的路由转发  构造了静态路由表，并实现了不同子网间的IP 数据报查表转发过程。通过完善路由表，改进示例程序实现双向传输。 |
| 实验过程： |
| **一、使用虚拟机实现多主机间的UDP 数据报收发及转发**  采用UDP 原始套接字，将UDP 数据报由A 主机发送给B 主机，再由B 主机转发给C主机，完成了一条消息的传送。此实现方案在UDP 数据报的传输过程中，目的IP 地址发生了变化，因此属于代理转发的场景。  **1.1 配置实验环境**  使用虚拟机软件VMware 在Windows 笔记本电脑上创建Linux 虚拟机（以Debian 为例），模拟所需网络环境。为虚拟机配置网络环境，使其可以与其他主机进行通信：选择桥接模式，确保虚拟机和物理机都连接到同一个局域网，这样虚拟机就可以像独立的设备一样连接到网络。    **1.1.1 获取IP 地址**  在Windows 物理机上打开命令提示符或终端，使用命令 ipconfig 查看物理机的IP 地址。在虚拟机中打开终端，使用 ip a 命令查看虚拟机的IP 地址。虚拟机使用“桥接模式”时，一般会通过DHCP 协议获得与物理机同一子网的IP 地址。如下图所示，物理机IP 地址为192.168.164.53，虚拟机IP 地址为192.168.164.236。      **1.1.2 测试连接**  在虚拟机/物理机中，使用 ping 命令测试是否能连接到物理机/虚拟机。如下图所示，主机间可以正常通信。      **1.2 具体实现**  使用本地的VSCode 通过SSH 远程连接三台虚拟机，便于代码的编写和调试，可通过终端直接控制虚拟机的程序编译和运行。  程序运行顺序：目的主机→路由主机→源主机。  **1.2.1 发送IP 数据报**  将其中一台虚拟机作为源主机（相当于A 主机），创建 send\_ip.c 文件，编写代码以实现IP 数据报的发送功能。使用GCC 编译并运行程序：gcc -g -o send\_ip send\_ip.c、./send\_ip。  **1.2.2 转发IP 数据报**  将其中一台虚拟机作为路由主机（相当于B 主机），创建 forward\_ip.c 文件，编写代码以实现IP 数据报的转发功能。注意防火墙需要开放相应的UDP 端口（如使用了ufw）：sudo ufw allow port /udp。使用GCC 编译并运行程序：gcc -o forward\_ip forward\_ip.c、./forward\_ip。  **1.2.3 接收IP 数据报**  将其中一台虚拟机作为目的主机（相当于C 主机），创建 recv\_ip.c 文件，编写代码以实现IP 数据报的接收功能。注意防火墙需要开放相应的UDP 端口（如使用了ufw）：sudo ufw allow port /udp。使用GCC 编译并运行程序：gcc -g -o send\_ip send\_ip.c、./send\_ip。  **1.3 选做**  示例程序只实现了一个数据包（携带1 条消息）的发、转、收过程，现改进程序，实现每条消息由控制台输入，并且不限制发送消息的数目。  **1.3.1 发送IP 数据报**  在send\_ip.c 代码中，使用fgets() 函数获取控制台的输入（即要发送的消息），存在message 字符串中；并添加while 循环持续等待用户输入，实现发送任意数目的消息。  **1.3.2 转发IP 数据报**  在forward\_ip.c 代码中，在接收数据报和发送数据报部分添加while 循环，持续等待需要转发的IP 数据报，实现发送任意数目的消息。  **1.3.3 接收IP 数据报**  在recv\_ip.c 代码中，在接收数据报部分添加while 循环，持续等待需要接收的IP 数据报，实现发送任意数目的消息。  **二、基于单网口主机的IP 数据转发及收发**  路由主机只有一个网络接口，用于转发源主机和目的主机之间的数据包。由于源主机(192.168.164.236)发送的IP 数据包的目的地址为接收主机(192.168.164.137)，而二者位于一个子网中，IP 数据报将直接交付给目的主机，而不会经由路由主机(192.168.164.138)来进行转发，因此将直接处理IP 数据报的以太网帧封装，将IP 数据报交给路由主机。  **2.1 配置实验环境**  与任务一实验环境相同。  **2.2 具体实现**  在发送主机上，首先构造出IP 数据报，其头部源IP 地址为192.168.164.236，目的IP 地址为192.168.164.137，然后构造用于封装该IP 数据报的以太网帧，该帧头部的源MAC 地址不变，但其目的MAC 地址为转发主机的MAC 地址（而不是接收主机的MAC 地址），通过这种方法，将去往接收主机(192.168.164.137)的IP 数据报交给转发主机(192.168.164.138)进行转发。  程序运行顺序：目的主机→路由主机→源主机。  **2.2.1 发送IP 数据包**  数据包的IP 头部源地址为192.168.163.236，目的地址为192.168.164.137。数据包在封装到下层的以太网帧时，目的MAC 地址为路由主机192.168.164.138 的MAC 地址。  在源主机中创建send\_ip\_single.c 文件，编写代码以实现IP 数据包的发送功能，这个程序将构造并发送一个以太网帧，其中包含指定的IP 头和以太网头：  ·创建原始套接字：使用socket(AF\_PACKET, SOCK\_RAW, htons(ETH\_P\_ALL))创建一个原始套接字；  ·获取接口索引：使用ioctl 获取网络接口的索引；  ·获取接口MAC 地址：使用ioctl 获取网络接口的MAC 地址；  ·构造以太网头：设置源MAC 地址和目的MAC 地址（路由主机的MAC 地址）；  ·构造IP 头：设置源IP 地址和目的IP 地址；  ·构造UDP 头：设置源端口地址和目的端口地址；  ·设置socket 地址结构：配置发送数据包的目标地址；  ·发送数据包：使用sendto 函数发送数据包。  **2.2.2 转发IP 数据包**  在路由主机中创建forward\_ip\_single.c 文件，编写代码以实现IP 数据包的转发功能，这个程序将捕获数据包，解析IP 头部信息，修改TTL ，重新计算校验和并转发到目的主机。  **2.2.3 接收IP 数据包**  创建 recv\_ip\_single.c 文件，编写代码以实现IP 数据包的接收功能，这个程序将接收数据包并打印内容  **2.3 选做**  扩展实验的网络规模，由原始方案中3 台主机增加到5 台主机，共同完成IP 数据报转发及收发过程，采用转发表改进示例程序，增加程序通用性。  **2.3.1 具体实现**  通过克隆再创建2 台虚拟机，作为新增的路由主机，进行数据包的转发。    在其中创建forward\_ip\_single.c 文件，内容和功能与原转发主机基本一致，但需创建转发表用于存储和管理IP 地址对。程序捕获数据包，解析IP 头部信息，修改TTL ，重新计算校验和并转发给下一台主机，其中发送数据包部分需要修改下一跳的MAC 地址。    数据包的传递路径为：源主机→转发主机1→转发主机2→转发主机3→目的主机。  **三、基于双网口主机的路由转发**  构造静态路由表，并实现不同子网间的IP 数据报查表转发过程。  **3.1 配置实验环境**  **3.1.1 网络配置**  通过Vmware 在路由主机上添加第二个网口，同样选择桥接模式，由DHCP 协议自动分配IP 地址。对 /etc/network/interfaces 文件进行修改，三台主机修改如下：  （1）源主机：  将ens33 设为静态IP，address 为IP 地址（192.168.1.2，在192.168.1.0/24 网段），gateway为网关（即路由器IP 地址），也可设置默认网关为双网口虚拟机的ens33 IP 地址（sudo route add default gw 192.168.1.1）。  添加“iface ens33 inet dhcp”，DHCP 协议自动分配一个IP 地址（即192.168.164.236），便于访问外网和远程SSH 连接。    （2）路由主机：将ens33 和ens37 均设为静态IP，address为IP 地址，两者需位于不同网段（192.168.1.0/24 网段和192.168.2.0/24 网段）；添加“iface ens33 inet dhcp”和“iface ens37 inet dhcp”，DHCP 协议自动分配IP 地址（即192.168.164.138和192.168.164.148），便于访问外网和远程SSH 连接。    （3）目的主机：  将ens33 设为静态IP，address 为IP 地址（192.168.2.2，在192.168.2.0/24 网段），gateway为网关（即路由器IP 地址），也可设置默认网关为双网口虚拟机的ens33 IP 地址（sudo route add default gw 192.168.2.1）。  添加“iface ens33 inet dhcp”，DHCP 协议自动分配一个IP 地址（即192.168.164.137），便于访问外网和远程SSH 连接。    **3.1.2 路由表配置**  在源主机和目的主机上配置静态路由，以确保数据包能够正确转发。  （1）源主机：sudo ip route add 192.168.2.0/24 via 192.168.1.1。  （2）路由主机：路由器上两个接口分别连接源主机和目的主机。  （3）目的主机：sudo ip route add 192.168.1.0/24 via 192.168.2.1。  在源主机使用 ping 命令，测试目的主机是否可达：ping 192.168.2.2。如下图所示，网络成功连接，路由表配置正确。    **3.2 具体实现**  源主机发送的数据包将通过路由器转发到目的主机，目的主机将接收到并打印数据包的内容。  程序运行顺序：目的主机→路由主机→源主机。  **3.2.1 发送主机程序（源主机）**  在源主机中创建send\_ip\_single.c 文件，这个程序将发送一个简单的UDP 数据包到路由器，其中目的地址为目的主机IP。  **3.2.2 路由转发程序（中间主机）**  在路由主机中创建forward\_ip\_single.c 文件，这个程序将捕获数据包，查找路由表，修改TTL 并根据MAC 地址转发到目的主机。需要定义静态路由表route\_table，便于查找。    **3.3.3 接收主机程序（目的主机）**  创建 recv\_ip\_single.c 文件，这个程序将接收数据包并打印内容。  **3.3 选做**  通过完善路由表，改进示例程序实现双向传输。  **3.3.1 具体实现**  在源主机上添加数据包接收功能，在目的主机上添加数据包发送功能，在路由主机上添加静态路由表内容，并修改相关IP 地址和MAC 地址，使得目的主机也可以将发送的数据包通过路由器转发到源主机。 |
| 实验结果： |
| **一、使用虚拟机实现多主机间的UDP 数据报收发及转发**  源主机发送的UDP 数据报通过路由主机转发给目的主机，在目的主机控制台输出每条消息（UDP数据报）的接收时间、源端口、目的端口、消息内容等。    改进程序，每条消息由控制台输入，并且不限制发送消息的数目，在目的主机控制台输出每条消息（UDP数据报）的接收时间、源端口、目的端口、消息内容等。    **二、基于单网口主机的IP 数据转发及收发**  源主机发送的IP 数据报通过路由主机转发给目的主机，在目的主机控制台输出收到IP数据报的时间、源MAC地址、目的MAC地址、源IP地址、目的IP地址、TTL等。    主机数增至5台，共同完成IP 数据报转发及收发过程，在目的主机控制台输出收到IP数据报的时间、源MAC地址、目的MAC地址、源IP地址、目的IP地址、TTL等。。    **三、基于双网口主机的路由转发**  源主机发送的IP 数据报经路由器查阅静态路由表，在不同子网间转发，最终送至目的主机，在路由主机控制台输出收到的数据报的源MAC地址，目的MAC地址、源IP地址、目的IP地址、TTL、源端口号、目的端口号等。    改进程序，实现数据双向传输，源主机向目的主机发送“Hello, this is a test message.”消息，目的主机向源主机返回“Hello! Got your message loud and clear.”，并在路由主机控制台输出收到的数据报的源MAC地址，目的MAC地址、源IP地址、目的IP地址、TTL、源端口号、目的端口号等。 |
| 问题讨论： |
| 1. 做实验任务二时，接收主机无法输出正确的IP 地址、MAC 地址等。  原因分析：接收主机创建的套接字使用AF\_INET 协议族，类型为SOCK\_DGRAM 数据报套接字，只能提供UDP，不包含MAC 地址等封装在以太网帧中的内容。  解决方法：使用AF\_PACKET 协议族、SOCK\_RAW 类型的原始套接字，可以直接访问网络接口层的数据包（如以太网帧）。  2. 路由主机和接收主机运行程序时，会一直收到不是发给它的数据包。  解决方法：收到数据包后进行检查，可忽略IP地址、MAC地址或端口号匹配错误的数据包。  3. 做实验任务三时，在给三台主机配置静态IP、划分子网后，无法再通过SSH 远程连接。  原因分析：虚拟机IP 与物理机IP 不在相同网段。  解决方法：为三台主机的网卡添加一个由DHCP 自动分配的IP地址（如192.168.164.236），使用该地址进行远程SSH连接。 |
| 心得体会： |
| （1）实现了基于原始套接字的IP 数据报的发送和接收，掌握了路由器进行IP 数据报转发的基本原理，了解了原始套接字的基本概念和使用方法；  （2）在Vmware 虚拟机上，基于Debian 系统完成本实验，进一步学会了Linux 系统网络配置、路由表配置、编程调试等方法；学会了使用SSH 远程连接主机进行本地编程和调试，大大提高了效率；  （3）学会了Linux 系统下Tshark、TCPdump、UFW、iptables等工具的使用；  （4）学习了原始套接字的创建、分类和使用，提高了Socket 编程水平，增强了问题定位和解决能力，对以后计算机网络的学习和应用实践有很大帮助。 |