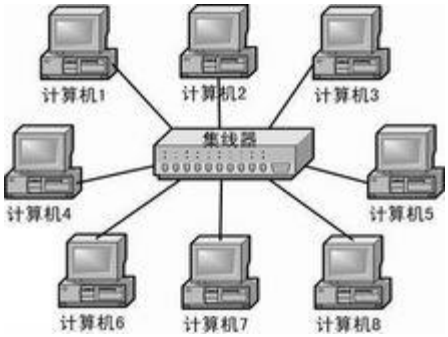
第六次作业

姓名：周玉川　　学号：2017221302006

测试点 6-1

1. **集线器能作为网络隔离设备吗？请说明理由？**

答：集线器是物理层设备，它发送数据时都是没有针对性的，而是采用广播方式发送，如图示。



集线器可以作为网络隔离设备，现实生活中，许多公司有内网和外网（我们学校也有），集线器可以实现多台终端与内外网的安全连接以及切换，进而提高了安全性保证而又实现信息共享。

2. **简述 Vlan 划分的不同方式及特点。**

答：表格如下

	基于端口划分	基于 MAC 地址划分	基于 IP 层划分	基于 IP 组播划分
优点	简单，一次定义	支持用户动态迁移	支持用户动态迁移，可按协议类型划分	可通过路由器扩展，支持广域网
缺点	灵活性差	配置工作量大，执行效率低	效率低，需要交换机支持	效率低，不适合局域网

测试点 6-2

1. **简述防火墙的典型技术分类与特点。**

答：如下表格

典型技术分类	特点
分组过滤防火墙	优点是容易实现，费用少，对性能的影响不大，对流量的管理较出色。缺点是过滤规则管理复杂，无法进行

	身份验证，不能进行应用层过滤，易受 ip 欺骗。
应用代理防火墙	优点是能提供详细日志，可以进行身份验证同时隐藏内部 ip，可以进行应用及的过滤。缺点是工作在 osi 的应用层开销大，多项服务不能共享服务器，配置不方便。
状态检测防火墙	优点是比分组过滤技术安全性高，比应用代理技术效率高。缺点不能实施代理功能，不能隐藏客户端地址
链路层代理防火墙	优点是可以支持不同的应用层协议，支持用户级的认证，可针对具体会话进行安全管理。缺点就是对客户端不透明，无法针对特定的应用协议进行安全管理。

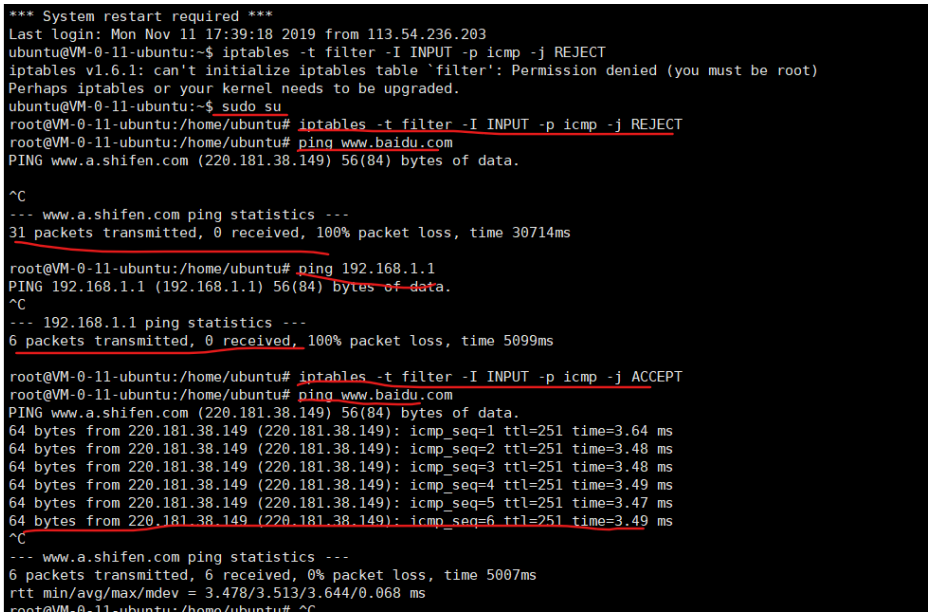
2. **简述防火墙的典型体系架构及特点。**
   1) 包过滤路由器模型， 优点：（1）处理数据包的速度较快（与代理服务器相比）；（2）实现包过滤几乎不再需要费用；（3）包过滤路由器对用户和应用来说是透明的。缺点：（1）包过滤防火墙的维护较困难；（2）只能阻止一种类型的 IP 欺骗；（3）任何直接经过路由器的数据包都有被用作数据驱动式攻击的潜在危险，一些包过滤路由器不支持有效的用户认证，仅通过 IP 地址来判断是不安全的；（4）不能提供有用的日者或者根本不能提供日志；（5）随着过滤器数目的增加，路由器的吞吐量会下降；（6）IP 包过滤器可能无法对网络上流动的信息提供全面的控制。
   2) 单宿主堡垒主机模型，优点：（1）可以将被保护的网络内部结构屏蔽起来，增强网络的安全性；（2）可用于实施较强的数据流监控、过滤、记录和报告等。缺点：（1）使访问速度变慢；（2）提供服务相对滞后或者无法提供。
   3) 双宿主堡垒主机模型，优点：（1）可以将被保护的网络内部结构屏蔽起来，增强网络的安全性；（2）可用于实施较强的数据流监控、过滤、记录和报告等。缺点：（1）使访问速度变慢；（2）提供服务相对滞后或者无法提供。
   4) 子网屏蔽防火墙模型，优点：（1）其提供的安全等级比包过滤防火墙系统要高，实现了网络层安全（包过滤）和应用层安全（代理服务）；（2）入侵者在破坏内部网络的安全性之前，必须首先渗透两种不同的安全系统；（3）安全性更高。缺点：路由器不被正常路由。

3. **如果允许 IP 地址为 192.168.1.212 的内网主机访问外部网络的 Web 服务，但禁止该主机使用邮件服务（SMTP，POP3），请给出防火墙应当配置的规则**

iptables -t filter -I INPUT -p tcp -j ACCEPT
iptables -t filter -I INPUT -p smtp -j REJECT
iptables -t filter -I INPUT -p pop3 -j REJECT

4. **在 Linux 系统中通过 Iptables 配置上述过滤规则，并验证规则的有效性。**

（选做）
命令：
iptables -t filter -I INPUT -p icmp -j REJECT
ping www.baidu.com
ping 192.168.1.1
iptables -t filter -I INPUT -p icmp -j ACCEPT
ping www.baidu.com
结果图



测试点 6-3

1. **NAT 有几种转换方式？简述其工作原理与特点。**

答：NAT 转换方式

1) 静态转换（Static NAT），是指将内部网络的私有 IP 地址与公有 IP 地址进行一一对应的转换。
2) 动态转换（Dynamic NAT），是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址是不确定的，是随机的。
3) 网络地址端口转换（NAPT），是指改变外出数据包的源端口并进行端口转换，内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。

2. **VPN 可提供哪些基本安全功能？如果一个企业需要在分支机构间提供安全通信，以及让出差的员工访问内部资源，请给出一个基于 VPN 技术的解决方案**

答：VPN 提供的安全功能，保证数据的完整性，保证通道的机密性，提供动

态密钥交换功能，提供安全防护措施和访问控制。

总部与分支机构之间使用 VPN 的隧道模式进行通信，出差员工使用传输模式进行通信。

测试点 6-4

简述物理隔离的类型与工作模式。

物理隔离的类型

a) 双网双机：两台计算机共用一套外部设备，通过开关选择两套计算机系统。
b) 双硬盘物理隔离卡：通过增加一块隔离卡、一块硬盘，将硬盘接口通过添加的隔 离卡转接到主板，网卡也通过该卡引出两个网络接口。
c) 单硬盘物理隔离：增加一块隔离卡，引出两个网口，并对原有硬盘划分安全区、非安全区。（非严格的物理隔离）
d) 隔离网关（网闸）:内、外部主机是完全网络隔离的，支持文件、数据或信息的交换。

物理隔离的工作模式

a) 单向隔离：在端上依靠由硬件访问控制信息交换分区实现信息在不同的安全域信息单向流动。
b) 协议隔离：通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。
c) 网闸隔离：位于两个不同安全域之间，通过协议转换的手段，以信息摆渡的方式实现数据交换。只有被系统明确要求传输的信息可以通过。