**实 验 报 告**

|  |  |  |  |
| --- | --- | --- | --- |
| **课程名称：** | 计算机网络实验 | | |
| **学 院：** | 计算机科学与工程学院 | | |
| **专 业：** | 计算机科学与技术 | **班级：** | 2021级 1 班 |
| **姓 名：** | 何超 | **学号：** | 202001021107 |

2020**年**12**月**16**日**

**山东科技大学教务处制**

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 路由器配置方式及基本操作 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  通过对路由器设备的几种配置手段、配置模式和基本配置命令的认识，获得路由器的基本使用能力。  **二．实验内容**  1. 认识路由器的配置方式  1.双击PacketTracer4.0进入仿真环境。  2.点击左下角的设备框中的路由器图标，在右边的框内会有多种路由器可供选择，选择2620XM路由器，然后再将2620XM的图标拖放到工作区。  3.点击设备框中的终端设备图标，选择PC-PT，再将它的图标拖放到工作区。  操作如图：    4.用Console线将PC机与路由器连起来。  操作如图：    5.点击设备框中线缆图标，选择蓝色的Console线，然后单击ＰＣ机，会弹出端口选择条，选择RS232端口  6.单击路由器，在弹出的端口选择条中选择console端口  7.单击PC机，弹出PC机的配置图。选择Desktop标签，然后再选择该标签下的Terminal 图标，弹出对话框，配置参数。点击OK，将进入路由器的用户视图并出现标识符：Router>。    2.基本命令使用  1.修改路由器的名字(Hostname)。  Router(config)# hostname Ra //（改名为Ｒa）    2.将路由器能够显示历史命令的空间扩大到100；  Router #terminal history size 100  3.配置路由器的口令  Ra#configure terminal  Ra (config)# enable secret cisco  4.配置以太网接口  Ra (config)# interface FastEthernet0/0  interfacetype slot#/port#  Ra (config-if)# ip address 192.168.1.1 255.255.255.0  Ra (config-if)# no shutdown    5.配置串行接口  Ra(config)# interface Serial0/0  Ra(config-if)# bandwidth 56  Ra(config-if)# clock rate 56000  Ra(config-if)# ip address 192.168.2.1 255.255.255.0  Ra(config-if) #no shutdown    6.配置路由协议  Ra(config)# router rip //启用RIP路由协议  Ra(config-router)#network 192.168.1.0 //加入路由通报网络  Ra(config-router)#network 192.168.2.0    7.键入show running-config查看当前运行的配置文件；  show startup-config //查看NVRAM里面的配置信息；  show flash查看flash //里面的IOS文件信息；    **三.实验思考**  1、CiscoIOS及其配置信息各存放在怎样的存储器中？  存放在路由器自带的ROM中。  2、路由器的几种配置手段分别在什么场合使用比较合适？  利用console线配置路由器适合在距离路由器比较近的情况下配置，而利用终端可以做到远程配置。  3、你认为本实验中的那几种命令的使用频率会最大？  路由器接口的开启命令，ip配置命令，用户特权切换，配置以太网接口命令的使用频率可能较大。  4、路由器为什么不需要固定的操作器和键盘？  因为路由器的工作模式比较固定，不需要频繁改变。通过console口即可利用计算机为其进行配置。  **四、心得体会**  利用思科模拟软件可以仿真各种网络设备的操作流程，软件仿真了网络设备运行的硬件环境，甚至做到了加载固件和各种配置表的功能。我们可以在网络运行中对其中的包进行抓取分析，大大方便了网络结构的分析与学习 | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 简单结构局域网组建与配置 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  了解一个局域网的基本组成，掌握一个局域网设备互通所需的基本配置，掌握报文的基本传输过程。  **二．实验内容**  1、根据所认识的设备设计一个简单的局域网并在仿真环境中画出其逻辑拓扑。  1.1设计一个局域网，按指导书连接后如图    2、配置拓扑中的各设备连通所需的参数。  **2.1.**配置各PC的IP地址与子网掩码    2.2、在模拟模式下进行包传输路径跟踪测试。  2.2.1连接好的网络结构如图所示    2.2.2实际相邻的PC机间的连通性测试，通过PC16向PC17,18,19发起ping命令 | | | | | |

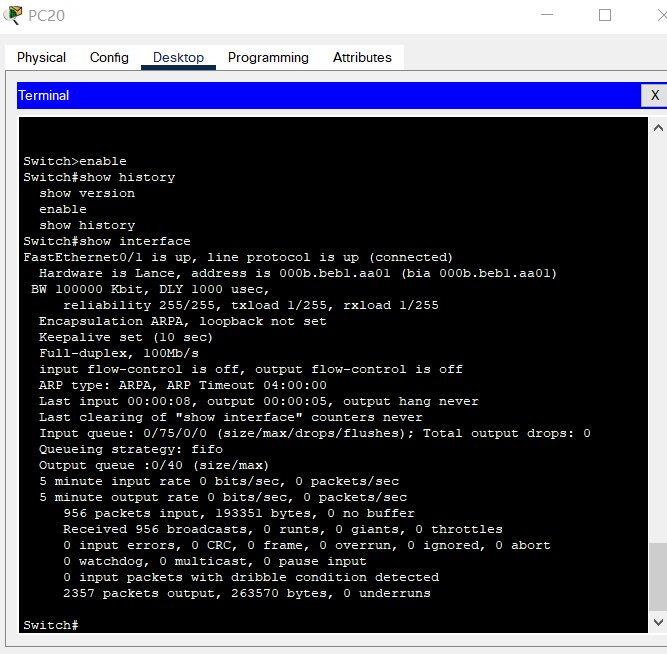
|  |
| --- |
| 2.2.3包传输路径跟踪测试  （1）交换机当pc16向pc18发出ping命令后，首先发出ARP包，送到交换机后交换机将该ARP包对其他接口进行广播，除了PC18以外的PC将丢弃这一ARP包，而PC18收到包以后向PC16发送一个反馈。这个反馈ARP包将会送回PC16.    （2）紧接着PC16开始发送PING命令使用的ICMP包，此时交换机不再对ICMP包进行广播，而是仅向PC18进行发包。PC18收到ICMP后发送反馈包，交换机同样仅对PC16发包，而不是广播。    （3）ICMP（交换机发送给PC18的一个）具体内容中，包括了原IP地址与目的IP地址，上一跳MAC与下一跳MAC。    **三、实验思考**  1、交换机的第一层功能是什么？  交换机将每个端口接收到的包按照转发表，将IP与端口一一对应，将包进行转发。交换机会进行自学习以用来完善转发表。  2、描述你在实验中的网络设备的规格和性能？  Cisco2960二层千兆交换机，共有16-48个网络接口，全半双工自适应。  3、默认网关的作用是什么？  当交换机收到某个包的IP地址查找不到有端口对应，这个包就会被发给默认网关。默认网关是网络的出口  4、参考拓扑图中PC机的默认网关是否可以不设置？为什么？  可以。因为拓扑图属于一个网络。所发送接收的包都在这个网络内，不需要通过网关进出网络。所以可以不设置。  **四、心得体会**  交换机和他的端口没有自己的IP地址，当他收到数据包的时候他只负责一项工作，就是根据自己的端口选择方向转包，他与路由器不同的是它的视野比较小，仅限于自己的端口。至于他如何对应IP与端口，那是因为交换机可以进行自学习，记录端口与IP的方向。 |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 交换机配置方式及基本命令的熟悉 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  通过对交换机设备的几种配置手段、配置模式和基本配置命令的认识，获得交换机的基本使用能力。  **二．实验设备**  Catalyst2950，运行终端仿真程序的PC、Console扁平线缆和相应的DB-9或DB-25适配器，直通线。（本实验在packet tracer 4.0环境下完成）  **三．实验内容**  3.1在CiscoPacketTracer中按拓扑图连接好    3.2.1进入PC20的终端界面，输入show version | | | | | |

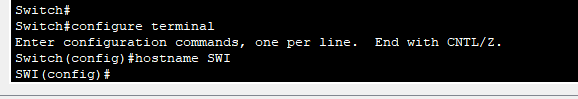
可以看出，在输入show version命令后，终端显示了交换机的某些信息

1. 交换机操作系统版本号
2. 交换机操作系统映像文件地址
3. 交换机上安装的主存大小
4. 交换机上以太网口的数量
5. 交换机ROM大小
6. 配置寄存器的值

3.2.2进入特权命令状态enable后使用show history查看前面所输入的命令（不管是错误的还是正确的）；使用show interface 端口号 来查看端口信息；最后使用disable退出特权指令状态

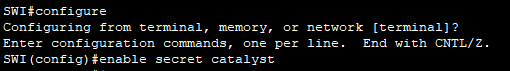
3.2.3进入全局设置状态并将交换机改名

具体命令为configure terminal， hostname SWI

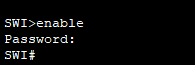


3.2.4设置进入特权状态的密码

具体命令为 enable secret “密码“



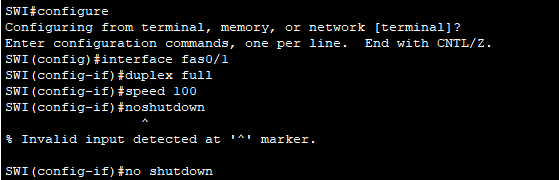
当退出特权模式后再次进入时就要求输入密码



3.2.5 使用端口配置模式，将端口设置为全双工模式，将其速率设为100bps并将端口状态设置为开。

具体命令interface fas0/1，duplex full，speed 100，no shutdown

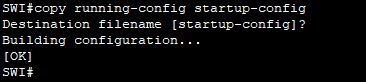
操作如图

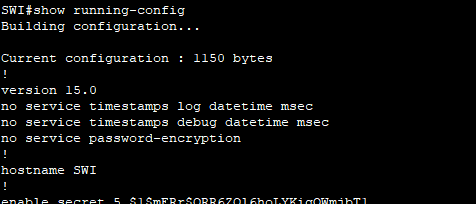


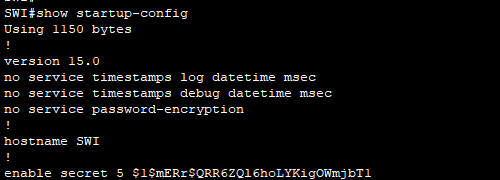
3.2.6使用copy running-config startup-config将配置从running-config保存到startup-config中，并使用show running-config，show startup-config查看其中的内容是否一致.

具体命令copy running-config startup-config，show running-config，show startup-config

操作如图

保存过程

查看running-config

查看startup\_config

可以看出，两张配置表的内容是一致的

四．思考题

1、交换机和路由器上的功能和命令集是一样的吗？

答：命令集是一样的，但是功能上是不一样的。交换机可以读取数据包信息并转发，路由器还有选路的功能

2、远程配置交换机的硬软件条件是什么？

答：需要把内网ip映射到公网，然后启动远程服务端口。之后的操作与直接配置无异。使用待操作PC的终端软件连接到交换机，向其中发送命令来配置交换机。

3、Encapsulation HAPA 是何意？ 答：采取HAPA封装

4、给出指定交换机的硬软件信息？答：可以使用show version命令查看

**四、心得体会**

交换机的命令行可以进行许多操作，比如重命名，更改配置文件等，可以在CLI界面直接操作，也可以通过console线用PC控制。

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | VLAN构建与配置 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  通过该实验理解VLAN的基本概念，掌握在二层交换机上创建VLAN的方法。  **二．实验内容**  2.1.1按照拓扑图在CiscoPacketTracer中连接线路并分配IP（192.168.10.0、192.168.20.0、192.168.30.0）    2.1.2分别为两台交换机命名与创建vlan  相关命令  Switch# configure terminal，  Switch(config) #hostname （交换机名称），  SwitchA(config)# vlan （序号），  SwitchA(config-vlan)# name （vlan命名）    配置A,B交换机更名，创建vlan，分配端口到vlan后如下图    （SwitchA的详细信息），已配置接口5为vlan10，10为vlan20，15为vlan30    （switchB的详细信息），已配置接口5为vlan10，10为vlan20，15为vlan30  具体命令：  interface FastEthernet0/XX（进入端口）  switchport access vlan XX（划分vlan） | | | | | |
| 2.1.3查看两台交换机的vlan表  具体命令：show vlan    以其中SwitchA为例  2.1.4设置SwitchA与SwitchB相连的Trunk干道  具体命令： interface FastEthernet0/24，switchport mode trunk  2.2.1 验证vlan内部通信  如图，同属于vlan10，连接在两个交换机上的PC0和PC3可以凭借vlan实现通信 | | | | | |

|  |
| --- |
| 如图，在PC0发给PC3的包中标有Dot1q帧标记是被添加上的vlan标识  2.2.2验证不同vlan之间不能直接通信  如图，虽然PC0与PC1连接在同一台交换机上，但因为处在不同vlan，所以不能通信。    PC0发给PC1的包交换机直接转发给了SwitchB，发给PC3后被PC3丢弃    PC0的命令行界面：不能成功PING通。  三、实验思考  3.1 S2950是否具有三层交换功能？若要Vlan间能够通信，交换机应具有什么层次要求？还可以加入什么设备使Vlan间能够通信？  答：不具有三层交换功能，实现vlan间通信应具三层交换机功能，可以加路由器。  3.2 端口Access和Trunk模式的含义是什么？  答：tag使用trunk连接，untag使用access连接。  3.3交换机是如何感知周围网络环境的变化的（如计算机增加，减少等）？  答：交换机根据MAC地址进行交换，所以交换机会进行自学习，自动更新地址表。  3.4三层交换技术产生的原因和技术特点？  答：三层交换技术解决了vlan间通信必须依靠路由器的问题。  **四、心得体会**  VLAN可以跨越物理结构的限制，在同一网络里划分出不同的网络，通过trunk接口又可以实现两个相同vlan但不同交换机的网络联通 |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 进阶实验 二层交换机+路由器实现VLAN间通信 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  进一步理解VLAN概念，掌握解决VLAN间通信的方法。  **二．实验内容**  2.1 按照实验参考书构建逻辑拓扑图并配置各项网络参数，如下图所示    2.2在交换机上创建vlan10与vlan20  具体命令：  进入配置模式：configure terminal  创建vlan：vlan（序号）  重命名：name（新名称）  具体如图：    将vlan分配给接口，如下图  具体命令：interface FastEthernet0/（接口号），switchport access （vlan名）    设置0/24接口为trunk    完成后如下图：    2.3在路由器子接口上配置封装模式和子接口IP地址  具体命令：interface fastethernet 0/0.（子接口）  ncapsulation dot1q （vlan序号）  ip address 192.168.10.1 255.255.255.0//配置子接口IP  操作如下图    2.4测试vlan10与vlan20的连通性  在PC21上向PC22发起PING命令  结果如下，证明连通    **三、实验思考**  1、子接口是物理接口还是逻辑接口？为什么？  答：子接口是逻辑接口，因为子接口没有独立的实体存在，多个子接口共用了一个实体出口。  2、何为三层交换机？Cisco的哪个系列交换机是三层交换机？  答：三层交换机是工作在网络层的网络设备，相较于二层交换机，三层交换机不仅仅是简单的转发，还可以进行路由交换。这样就可以实现二层交换机不能做到的vlan之间的通信。省去了外接路由器的麻烦。思科的catalyst-3700/3500/6500是三层交换机  3、路由器可以配置的带802.1Q封装的子接口数最多有多少？  答：256个  4、中继两端的封装为什么必须一致？ Isl 与Dot1.q 封装有什么不同？  答：协议不一致不能正确传输VLAN信息，ISL仅仅适用于Cisco设备，dot1q是IEEE认证的国际标准。  **四、心得体会**  二层交换机的功能比较有限，只能根据端口匹配单个IP进行转发。所以找未知目的地和路径的功能要使用三层交换机或者路由器，本实验中虽然路由器上只连接了一条线，但是它可以根据路由表告诉发来的包裹正确的目的路径和目的地。路由器在本实验中起到了沟通两个vlan的作用。 | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 多网段网络组建与静态路由配置 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  通过设计有两个路由器的网络及静态路由的配置理解静态路由原理。  **二．实验内容**  2.1 按实验指导书在Cisco模拟器中连接要求的拓扑图如下图所示    2.2 按实验指导书的要求配置各个接口IP与速率如下图所示  路由器配置接口IP命令如下图（以路由1为例）    主机配置后如下（以PC0为例）    2.3 配置静态路由并查看路由表  具体命令：ip route (原ip)（原ip子网掩码）（要转发到的IP地址）  操作如图（以路由A为例，路由B过程相同）    查看路由表  具体命令：show ip route  操作如图    保存路由表    2.4 连通性测试  2.4.1从192.168.1网段向192.168.3网段发起ping命令  如下图所示，可以PING通，证明配置有效    2.4.2 从192.168.3网段向192.168.1网段发起ping命令  如下图所示，可以PING通，证明配置有效    2.4.3对网段内其他PC互相进行PING测试  测试结果为可以PING通  2.4.4 路由器间连通性测试  使路由A和路由B互相PING，测试结果如下      结果证明可以PING通，配置有效  2.5.1 包传输路径跟踪测试  当PING命令发出的ICMP包从路由A发出后包的内容  可以看出，输出包的发送端口被直接定向为Serial0/0，是路由表的作用    2.5.2 分析Inbound PDU Details标签  1.为原始ICMP包的结构（图左）（从PC0向HUB传递）  2.为路由A向路由B发包结构（图右）    可以看出，原始ICMP包的目的地址3网段不在路由A的本地范围，但路由A的静态路由表中存有配置好的3网段包转发规则，所以该包在路由A的下一跳为路由B。因为在PC发出的包使用Ethernet，而路由间使用的是HDLC，所以两包的第一层结构是不同的。  **三．思考题**  **1、路由选择表获取信息的方式有两种：以静态路由表项的方式手工输入和通过动态路由选择协议自动获取信息。静态路由和动态路由的优先级别那个高，是绝对的吗？那么优先级是由什么来决定的呢？**  静态路由优先级高，但也不一定。路由协议不同时才会依据优先级，而路由协议相同时则要根据开销大小来确定最终选择的路由。  **2、静态路由的管理距离是多少？ 管理距离有何作用？**  是1 根据管理距离可以决定选择哪一个路由是最合适的。  **3、为何有时需要配置默认路由？ 默认路由的作用是什么？**  当路由表中没有包中所含有IP的下一跳信息时，如果没有配置默认网关，这个包就会被丢弃，而配置了默认网关后，这个包就会被发到默认网关。很多家用路由器和实际生活的网络，即末梢网络中主要用到的就是默认网关，因为家用网络需要向单一的外部运营商大量发包，这时用到的就是默认网关，他大大简化了网络结构。  **4、如何配置默认路由？（自己设计一个实验）**  在需要使用默认路由的路由器上加配一条路由表，内容是  ip route 0.0.0.0 0.0.0.0 10.0.0.2(该路由器的出口处的下一路由IP)  **四、心得体会**  路由器找路的本领来自于路由表，而路由表的获取主要有两种方式，一个是路由器之间相互交流，优化路由表，一个是人为添加路径。此外在实际生活中默认路由的用途很大，利用默认路由我们只需要简单几跳就可以到达运营商中心，然后利用运营商的专线到达各个app服务器，在服务器中我们进行各种网络活动。 | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 多网段网络组建与动态路由配置 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| 1. **实验目的**   1、理解RIP动态路由原理。  2、练习动态路由配置。  3、掌握对路由器有关状态获取和分析的方法。  **二．实验内容**  **2.1.1.按指导书链接网络拓扑结构如下图所示，并向路由器添加对应接口**    2.1.2清除两台路由器缓存配置文件，并重启路由器，以路由A为例  具体命令：erase startup-config，reload    2.1.3对两台路由器进行重命名      2.2.1对两台路由器的接口进行IP配置,DCE时钟设置与接口打开      2.2.2使用各个PC对其网关进行PING命令测试连通性  结果如图    如图，证明链接配置正确  **2.3.1进行RIP路由协议配置**  （1）分别对路由1，路由2进行RIP配置  具体命令：router rip，network（网段IP）      （2）更新配置文件（以路由A为例，路由B相同）  具体命令：copy running-config startup-config startup-config    **2.3.2**尝试从PC0所在的1网段向PC1所在的3网段发起PING命令测试连通性,然后反向测试  结果如图    由图可知RIP配置正确，网络联通。 | | | | | |
| **2.4.1检查路由器基本配置（以Router1为例）**  具体命令：show ip protocol    如图，路由协议为RIP。  **2.4.2查看路由表（以Router1为例）**    如图可得，路由直连的1，2网段显示端口，而网段3是间接链接，就是说路由器知道这个网段的下一跳的方向是Serial0/0，这条信息是由RIP自动产生的。  **2.5.1观察RIP路由的更新**  输入命令：debug ip rip  稍等片刻路由器会自动更新显示RIP接收到的信息更新  如图所示    即可说明路由器从serial0/0的收到了来自于2.2发来的更新表，表中说3.0网段距离此路由器还剩1跳。  同时，路由器也在不断向其他人发送自己的路由表，表中说2.0网段距离自己剩余1跳，3.0网段距离自己还剩2跳。  3.0网段并不是路由1的直连网段，这是路由1从RIP收到的信息，在收到其他人发来的3.0网段距离为1的信息后，路由1将距离+1并和自己的路由表比较，在最开始的时候，路由A的路由表中没有3.0网段的信息，所以将这条存储了下来，如果网络结构发生变化，那么他回从他人发来的路由表中选择距离最短的一条来更新。更新是不断进行的，以此网络中的路由器就可以知道不同网络的下一条的具体发送方向与距离。  **三．实验思考**  1、在步骤2中主机PC0到主机PC1能ping通吗？在步骤3中呢？为什么？  答：在步骤2中无法PING通，因为1.0和3.0分属于两个路由器的两个网段，路由A收到发往3.0网段的包之后，查表是不能找到下一跳的方向的，因为路由表中没有这个信息，而网关又是自己，所以这个包就会被丢弃，因此步骤2不能PING通外网段，当然，PC去PING自己的网关是正常的。然而在步骤3中，在我们配置了RIP协议后，路由器进行相互的发表，不断学习各个网段的下一跳，这个时候路由A和B都有了对方网络下的网段了，此时路由A再收到发往3.0网段的包，他查表知道下一条的位置，就会对路由B进行转发，同理，反向也一样，这样两个网络实现了正常的通信，也就可以从PC0去PING通PC1了。  2、动态路由如何与静态路由结合使用？  答：当他们结合使用的时候，静态路由可以是主静态路由，或者作为动态路由的备份表  3、练习使用本实验中提到的所有debug命令，观察其输出结果有什么异同？  答：在网络结构没有发生变化时，他们每个路由器每隔一段时间输出的内容没什么差异，当网络结构变化时，这个表就会变。  4、使用debug命令如何排错？  答：当网络出现了问题，我们可以从debug命令的反馈中提取很多的某节点错误信息，通过流量的大小等，不过这个命令比较占用资源，不能一直打开，要及时关闭  **四、心得体会**  动态路由协议可以脱离手工配置，让路由器在网络之间自行交流路由表，根据跳转次数来决定是否对自己的数据进行更新。这就省去了很多的人力去配置路由，在复杂网络中使用起来相当的方便。但是RIP也占用了一部分网络资源。尤其是如果开启了debug分析之后一定要及时的关闭，否则可能造成网络拥塞 | | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 网络访问控制与基本包过滤配置 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| 1. **实验目的**   通过本实验理解基于IP源地址的包过滤原理和应用方法。掌握标准访问控制列表的设计、配置和测试。  **二．实验内容**  2.1.1.按照实验指导给出的逻辑结构链接好拓扑图如下所示    2.1.2按给出的信息表格将拓扑图中左右的网络设备与端口分配IP，并配置各个路由器的RIP协议  （1）配置路由器接口与设备IP，成果如下，以部分设备举例，其余设备操作相同。  （2）为各个路由器配置RIP协议，使整个网络可以互联互通。  操作如下图，以insiderouter路由器为例，其余路由器操作类似    （3）检测全网联通性，以PC0为监测点向全网其余设备发送PING命令，结果如图    可以看出，整个网络是处于联通状态的，证明连接拓扑线路，配置IP地址，设置RIP协议的操作步骤是正确的。  **2.2.1建立标准访问控制列表**  在insiderouter上建立一个访问控制列表access-list1应用到其Eth1/1端口  具体命令：en，config t，access-list 1 permit 192.168.1.0 0.0.0.255，access-list 1 permit host 192.168.2.3，exit，config t，interface e1/1，ip access-group 1 out，end。  如图所示    **2.2.2 查看已经建立的访问控制列表**  具体命令：show access-lists  结果如下    **2.2.3 访问测试**  利用TogglePDUlist功能对网络进行测试，测试结果如下（图中从PC2到FTP服务器的第一次访问因未知原因失败，重复操作后成功，原因未知）    **图中可以看出，本来互联互通的网络在应用了访问控制列表后，部分设备终端因没有权限所以不能访问某部分的网络，这是访问控制列表生效的原因**  **2.3.1实验结果分析**  在这次试验的网络中，在添加了访问列表控制规则后，只有PC1才能访问行政网网段，而其他终端无权访问。比如教学网和宿舍网。图中，PC2因为访问权限控制中没有限制他访问三个服务器，所以即使他无法访问行政网段，但是对三个服务器的访问是不受限制的。  **三．实验思考**  1、解释一下在Step2.1中为什么PC1到PC4的Simple PDU的Last Status 是Failed？答：因为访问控制列表的限制，PC1无法访问PC4。  2、标准访问控制列表依据什么实现访问控制的，有什么样的优点和不足？  答：过滤规则，应用端口。优点是方便配置，缺点是不易纠错，而且不能控制传输类型与包的类型  3、标准访问控制列表的配置一般包括哪几步？答：增加过滤规则，将规则应用于端口  4、标准访问控制列表有什么样的应用原则？答：最小特权，最靠近受控对象，默认丢弃  **四、心得体会**  访问控制规则可以对网络中一些主机的访问权限做出控制，这在实际生活中又很大的应用，比如在校园网系统中普通的网络不应该有访问行政网络的权限，以及除了一卡通系统内部以外，外部设备不能访问一卡通系统，但是又要保证一卡通系统对外的充值端口可以使用，这就要求一卡通要接入网络，此时我们可以在一卡通路由上配置访问限制，实现这一功能。 | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 网络访问控制与扩展包过滤配置 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  通过本实验理解基于IP地址、协议和端口的包过滤原理和应用方法，掌握扩展访问控制列表的设计、配置和测试  **二．实验内容**  2.1使用实验8未配置访问控制列表时的拓扑结构如下图，经过测试网络正常    2.2.1 创建访问控制列表accesslist100，应用到InsideRouter的Fa0/0端口  具体命令：config t，access-list 100 deny tcp 192.168.5.0 0.0.0.255 host 192.168.1.4 eq 21，access-list 100 permit ip any any，exit，config t，interface fa0/0，ip access-group 100 out  实现如下：    2.2.2查看刚刚建立的访问控制列表    2.2.3利用ComplexPDU对网络进行测试  使用ComplexPDU进行测试如下图，主机为PC4    测试结果如下    结果说明：宿舍网段不可以访问FTP服务器，可以访问WWW和HTTP服务器  这是访问控制列表作用的结果  **2.3.1创建拓展控制列表access-list 101并应用到EageRouter的Fa0/0**  具体命令：ip access-list extend 101，access-list 101 deny tcp 218.58.100.0 0.0.0.255 host 192.168.1.4 eq21…  结果如图    可以说明规则被成功创建  **2.3.2查看创建的规则表**    这说明创建成功  **2.3.4对刚刚建立的访问控制表进行测试**  从PC5对内网1.4,1.3，1.5发包。  从PC0，4，2，1，3对218.58.100.3发包，类型分别为FTP,HTTP,FTP,SMTP  操作如图，以PC5为例，其他终端操作类似    结果如下    他们分别说明了：外网无法访问内网FTP，但是可以访问内网的WWW服务器和SMTP服务器。此外，管理，行政，教学，宿舍区域网络都可以访问WWW服务器。  **三．实验思考**  1、思考扩展访问控制列表的进行访问控制的依据有那些？  源地址，目的地址，端口号，协议类型  2、有人说在同一个Router上同一个端口的同一个方向上不能绑定多个访问控制列表，在同一个Router上同一个端口的两个不同方向（inside、outside）能分别绑定一个访问控制列表，这个说法对吗？请做实验验证。  不可以在同一端口上绑定多个访问控制列表，但是可以在两个不同方向上分别绑定一个访问控制列表。  3、扩展访问控制列表的配置一般包括哪几步？  配置过滤规则和应用端口  4、扩展访问控制列表有什么样的应用原则？  最小特权原则，最靠近受控对象原则，默认丢弃原则。  **四、心得体会**  访问控制列表继续细分成不同方向与不同端口的访问控制权限，可以实现对主机内部某些应用程序的访问控制，阻止一些关键协议被非法入侵，因为某些端口和主机的其他普通端口的重要性并不是相同的，我们这样可以做到细分控制。 | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 内外网结构下的网络地址转换 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  通过本实验理解网络地址转换的原理和技术，掌握扩展NAT/PAT设计、配置和测试。  **二．实验内容**  **2.1.0使用已经配置好的拓扑网络图和IP分配**  **2.1.1将内网地址192.168.1.3静态转换到公网IP 218.58.59.93**  具体命令：ip nat inside source static 192.168.1.3 218.58.59.93，interface fa0/0，ip nat inside，interface s0/0，ip nat outside，end    操作如上  **2.1.2查看刚配好的转换表**    **2.1.3从外网利用公网IP218.58.59.93对内网192.168.1.3进行访问**  （1）在PC5上建立一个complexPDU尝试发送到218.58.59.93  使用event list和PDUlist对其进行跟踪  PDU包内容配置如图所示    （2）对这个包的发送路径进行跟踪    **由图可知，在外网环境里发往公网IP的包因为路由eage上建立了NAT转换，所以这个IP被网络中的路由表记录，直接发给了Eage路由器。**    最终结果：成功访问。  **2.1.4分析IP地址转换详细过程**  在PC5发出的包从Eage路由器发出之后，我们推测应该有一个IP地址的转换  所以打开从eage路由器发出的PDU包，其详细内容如下    可以看出，IP的目的地址在流经eage路由器时从原来的公网地址218.58.59.93被修改为内网可以识别的内网地址192.168.1.3。  这证明转换是成功的，内网IP被成功映射到了公网上。  2.2.1**将内网IP192.168.1.5映射到公网IP218.58.59.94**  操作步骤与2.1相同，同样是在eage路由器上添加NAT转换规则    如图，规则成功添加  **2.2.2从公网主机PC5向218.58.59.94发起PDU测试**  PDU配置过程同上，测试结果和转发路径如下    转发路径说明了NAT转发表配置正确  转发细节：    最终结果：    **2.3.1配置NAT动态转换，将整个网段映射到公网上**  将管理网段192.168.2.0行政网段192.168.3.0分别映射到218.58.59.95和218.58.59.96上  配置细节：    **2.3.2对配置好的NAT进行PDU测试**  分别从PC2，PC0对218.58.100.3发起PDU测试  结果如下    证明动态NAT配置有效并转发成功  管理网段和行政网段可以访问218.58.100.3  **2.4.1验证NAT表中没有规则的包在进出路由时会被丢弃**  从PC1向218.58.100.3发包  最终结果如图所示    结果显示发送失败了，打开这个包在经过Eage路由时的详细信息    这说明，在NAT转发表中没有对应的规则，他在进出内外网时没有被转化目的IP，路由无法找到他的下一跳，所以这个包被丢弃，所以PDU测试的结果是失败的。  **2.5.1将教学网段和宿舍网段转换到公网IP**  按照刚才的过程对eage路由进行配置  如下图所示    2.5.2测试配置的正确性  从PC3，PC4向218.58.100.3发起PDU测试  结果如下图所示    证明我们刚刚配置的NAT转发表成功将宿舍和教学网段映射到了公网IP  2.5.3查看NAT转发表详细内容    可以看到刚刚向转发表中添加到信息被成功应用。  2.5.4查看转发详细包内容      可以看到Eage路由器将包根据规则成功转发。  **三．实验思考**  1、总结一下NAT和PAT的应用场景和配置步骤。  表数据的建立主要是在内外网边界路由器上进行规则添加。我们需要指定内网的某个IP或者IP网段需要映射到外网的具体地址。之后在进出这个网络时，路由器会将内外网地址进行转化。  2、思考一下图10.16中PC1到218.58.100.3 HTTP PDU为什么被丢弃  根据路由器发包的界面提示，可以知道路由器的NAT转换表中没有查到这个协议转发到具体转发方式和IP,所以路由器就将这个发出网络的包丢弃了，因为不能到达指定的目的地。  3、在Simulation模式下跟踪数据包时，数据包到达目的地时可能显示一个闪烁的X，但是PDU List Window中Last status却是successful。你能解释一下原因吗？  显示X可能的并不是目的主机需要的包，这有可能是网络中对结构变更的发包检查  **四、心得体会**  在多数局域网中都存在服务器，这些服务器有可能是主要面向于全网的其他主机的，这就需要将内网IP映射到公网IP，同时也解决了内网IP范围小的问题。再比如我们可以用NAT转换将私有网络中的设备映射到公网，这样只要我们接入了互联网，不管身处什么样的网络环境都可以访问自己建立的映射来的私有网络。当然这需要运营商的支持。但是使用NAT是主要的技术流程 | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **组 别** |  | **姓 名** | 何超 | **同组实验者** |  |
| **实验项目名称** | 综合网络设计实现 | | | **实验日期** | 月 日 |
| **教 师 评 语** |  | | | | |
| **实验成绩：** | | | **指导教师（签名）：**  2020年 月 日 | | |
| **一．实验目的**  设计一个实际生活中的仿真网络结构  **二．实验内容**  **1.确定结构的大概框架**  它可以主要分为服务器群，固定内部终端（如一卡通充值扣费终端），行政网络与其他外部网络组成构成的网络，再加上学校存储数据的服务器群，比如食堂饭卡数据库服务器，学校FTP文件共享服务器。以及学校的物联网结构，比如食堂超市收费终端，饭卡缴费入口。同时，网络中的设备除了服务器外应该都可以访问到外部网络，保证接入终端的通信。此外，现在人们的网络需求日益增强，所以我们在网络中安装了多个**WIFI终端设备**，设备只要连接上WIFI信号，配置一个当前区域的IP网段静态IP，就可以访问外部互联网（这里用一个外部网络的WWW服务器替代）  **2.按照构想设计拓扑结构**  成果如下所示。    在图中添加了WIFI设备，接入WIFI的终端需要手动配置静态IP，IP网段处在交换机上的标号，即可访问互联网（可以成功PING通outsideWWW服务器）  配置过程：   1. 实现满足需求的拓扑连接，添加路由上的各类拓展接口 2. 为所有接口配置IP地址     （如图，正在为路由器端口配置网关IP）   1. 为路由器配置RIP协议，使网络整体可以互通     （以图为例，正在配置行政区网络路由器的RIP协议）   1. 配置访问限制列表，保护关键信息。     （如图，在行政区路由上配置访问控制列表）   1. 测试所有的网络终端是否可以正常访问互联网，添加WIFI使用设备，如手机，配置静态IP，测试对外部WWW服务器的正常访问 2. 测试终端设备对学校FTP服务器，内部WWW服务器的正常访问   特点：   1. **满足各种联网设备的需求，分区严格明确。**普通终端网络分为生活，行政，教学楼设备，收付款终端，一卡通数据库服务器，除了扣费终端设备，其余设备不能访问一卡通核心服务器。   验证：一卡通服务器地址192.168.4.4，通过扣费终端可以成功访问，而其他设备则无法访问，如下图所示：  图1：扣费终端1可以访问一卡通服务器    图2：生活终端区通过WIFI连接的某智能手机无法访问一卡通服务器   1. **关键信息访问保护**，其他成员在路由器接口上配置访问控制列表，使其无法访问行政网络（10，20，30网段）。但行政楼内部的网络是互联互通的。同时，校园内的所有成员都可以访问到OutsideWWW服务器，即互联网。     如图，生活区某WIFI接入的手机（其他所有外部设备也一样）不能进入行政区网络，但是可以自由访问互联网。    如上，行政区的PC可以访问行政区设备与外网。   1. **内网WWW服务器映射到公网上，外部可以凭公网IP访问到学校内部WWW服务器**     （如图，为终端路由器在接受外网对WWW内部服务器的访问请求时，将公网IP按表转换成内网IP的过程）  **三．实验心得**  自主设计的校园网络结构参考了之前实验的部分内容，包括NAT地址转换，访问控制列表，RIP路由表的交换过程，以及在各种访问限制过程中对包的跟踪定位方法。参考当今校园网络复刻而成，对实验通透学习后深知校园网络结构的复杂性，设计之不易。校园网网络既要保证各类涉及金融安全的关键信息，服务器，比如一卡通系统的独立运行，又要接入各类与信息安全，保密相关的行政网络，以及公用FTP文件服务器，需要映射到外网访问的学校WWW服务器的同时，还要将全区域覆盖WIFI，保证所有终端都可以访问外部互联网。这将各类技术融合到了一起。本次实验增强了个人对计算机网络的进一步理解，实现了总复习的作用。 | | | | | |