鸿鹄论坛 bbs.hh010.com

网路设备模拟器 Packet Tracer 教程

第一章　认识 Packet Tracer 软件

Packet Tracher 介绍

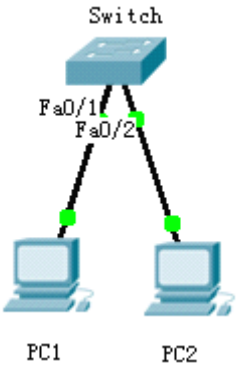
- Packet Tracer 是 Cisco 公司针对 CCNA 认证开发的一个用来设计、配置和故障排除网络的模拟软件。
- Packer Tracer 模拟器软件比 Boson 功能强大，比 Dynamips 操作简单，非常适合网络设备初学者使用。

学习任务

1、安装 Packer Tracer；
2、利用一台型号为 2960 的交换机将 2pc 机互连组建一个小型局域网；
3、分别设置 pc 机的 ip 地址；
4、验证 pc 机间可以互通。

实验设备

Switch_2960 1 台；PC 2 台；直连线



PC1

IP： 192.168.1.2

Submask： 255.255.255.0

Gateway： 192.168.1.1

PC2

IP： 192.168.1.3

Submask： 255.255.255.0

Gateway： 192.168.1.1

PC1 ping PC2 Reply

PC2 ping PC1 Reply

PC2 ping Gateway Timeout

第二章 交换机的基本配置与管理

实验目标

- 掌握交换机基本信息的配置管理。

实验背景

- 某公司新进一批交换机，在投入网络以后要进行初始配置与管理，你作为网络管理员，对交换机进行基本的配置与管理。

技术原理

- 交换机的管理方式基本分为两种：带内管理和带外管理。
  - 通过交换机的 Console 端口管理交换机属于带外管理；这种管理方式不占用交换机的网络端口，第一次配置交换机必须利用 Console 端口进行配置。
  - 通过 Telnet、拨号等方式属于带内管理。
- 交换机的命令行操作模式主要包括：
  - 用户模式 Switch>
  - 特权模式 Switch#
  - 全局配置模式 Switch(config)#
  - 端口模式 Switch(config-if)#

实验步骤：

- 新建 Packet Tracer 拓扑图
- 了解交换机命令行
  - 进入特权模式(en)

- 进入全局配置模式(conf t)
- 进入交换机端口视图模式(int f0/1)
- 返回到上级模式(exit)
- 从全局以下模式返回到特权模式(end)
- 帮助信息(如? 、co?、copy?)
- 命令简写(如 conf t)
- 命令自动补全(Tab)
- 快捷键(ctrl+c 中断测试,ctrl+z 退回到特权视图)
- Reload 重启。(在特权模式下)
- 修改交换机名称(hostname X)
- 配置交换机端口参数(speed,duplex)
- 查看交换机版本信息(show version)
- 查看当前生效的配置信息(show run)

实验设备

Switch_2960 1 台；PC 1 台；配置线；

PC console 端口

enable
conf t
interface fa 0/1
speed 100
duplex full
end
show version
show run

第三章　交换机的 Telnet 远程登陆配置

实验目标

- 掌握采用 Telnet 方式配置交换机的方法。

实验背景

- 第一次在设备机房对交换机进行了初次配置后，你希望以后在办公室或出差时也可以对设备进行远程管理。现要在交换机上做适当配置。

技术原理

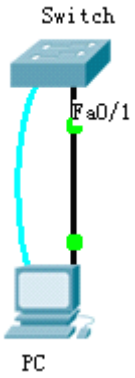
- 配置交换机的管理 IP 地址(计算机的 IP 地址与交换机管理 IP 地址在同一个网段)：
- 为 telnet 用户配置用户名和登录口令：
  - 交换机、路由器中有很多密码，设置对这些密码可以有效的提高设备的安全性。
  - switch(config)# enable password ****** 设置进入特权模式的密码
  - switch(config-line)可以设置通过 console 端口连接设备及 Telnet 远程登录时所需的密码；
    - switch(config)# line console 0
    - switch(config-line)# password 5ijsj
    - switch(config-line)# login
    - switch(config)# line vty 0 4
    - switch(config-line)# password 5ijsj
    - switch(config-line)# login

实验步骤

- 新建 Packet Tracer 拓扑图
- 配置交换机管理 ip 地址
  - Switch(config)# int vlan 1
  - Switch(config-if)# ip address **IP** **submask***
- 配置用户登录密码
  - Switch(config)# enable password ******* 设置进入特权模式的密码
  - Switch(config)# line vty 0 4
  - Switch(config-line)# password 5ijsj
  - Switch(config-line)# login

实验设备

Switch_2960 1 台；PC 1 台；直连线；配置线



PC

192.168.1.2

255.255.255.0

192.168.1.1

PC 终端

en

conf t

inter vlan 1(默认交换机的所有端口都在 VLAN1 中)

ip address 192.168.1.1 255.255.255.0

no shutdown
exit

enable password 123456
line vty 0 4
password 5ijsj
login
end
show run

PC CMD
ping 192.168.1.1
telnet 192.168.1.1
password:5ijsj
enable
password:123456
show runing

第四章　交换机划分 Vlan 配置

实验目标

- 理解虚拟 LAN(VLAN)基本配置；
- 掌握一般交换机按端口划分 VLAN 的配置方法；
- 掌握 Tag VLAN 配置方法。

实验背景

- 某一公司内财务部、销售部的 PC 通过 2 台交换机实现通信；要求财务部和销售部的 PC 可以互通，但为了数据安全起见，销售部和财务部需要进行互相隔离，现要在交换机上做适当配置来实现这一目标。

技术原理

- VLAN 是指在一个物理网段内。进行逻辑的划分，划分成若干个虚拟局域网，VLAN 做大的特性是不受物理位置的限制，可以进行灵活的划分。VLAN 具备了一个物理网段所具备的特性。相同 VLAN 内的主机可以相互直接通信，不同 VLAN 间的主机之间互相访问必须经路由设备进行转发，广播数据包只可以在本 VLAN 内进行广播，不能传输到其他 VLAN 中。
- Port VLAN 是实现 VLAN 的方式之一，它利用交换机的端口进行 VALN 的划分，一个端口只能属于一个 VLAN。
- Tag VLAN 是基于交换机端口的另一种类型，主要用于是交换机的相同 Vlan 内的主机之间可以直接访问，同时对不同 Vlan 的主机进行隔离。Tag VLAN 遵循 IEEE802.1Q 协议的标准，在使用配置了 Tag VLAN 的端口进行数据传输时，需要在数据帧内添加 4 个字节的 8021.Q 标签信息，用于标示该数据帧属于哪个 VLAN, 便于对端交换机接收到数据帧后进行准确的过滤。

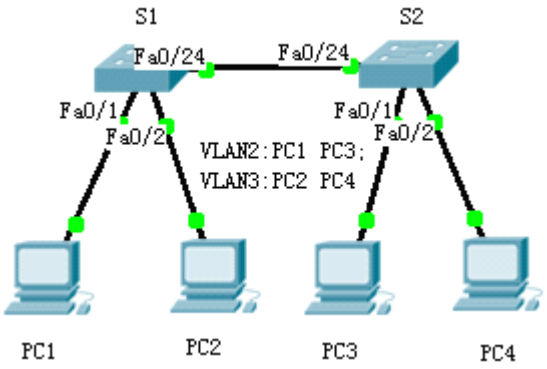
实验步骤

- 新建 Packet Tracer 拓扑图；
- 划分 VLAN；

- 将端口划分到相应 VLAN 中；
- 设置 Tag VLAN Trunk 属性；
- 测试

实验设备

Switch_2960 2 台；PC 4 台；直连线



PC1

IP: 192.168.1.2
Submark: 255.255.255.0
Gateway: 192.168.1.1

PC2

IP: 192.168.1.3
Submark: 255.255.255.0
Gateway: 192.168.1.1

PC3

IP: 192.168.1.4
Submark: 255.255.255.0
Gateway: 192.168.1.1

PC4

IP: 192.168.1.5
Submark: 255.255.255.0
Gateway: 192.168.1.1

Switch1

```
en
conf t
vlan 2
exit
vlan 3
exit
inter fa 0/1
switch access vlan 2
exit
inter fa 0/2
switch access vlan 3
```

exit
inter fa 0/24
switch mode trunk
end
show vlan

Switch2

en
conf t
vlan 2
exit
vlan 3
exit
int fa 0/1
switch access vlan 2
exit
int fa 0/2
switch access vlan 3
exit
int fa 0/24
switch mode trunk
end
show vlan

PC1 ping PC2 timeout
PC1 ping PC3 Reply

第五章　利用三层交换机实现 VLAN 间路由

实验目标

- 掌握交换机 Tag VLAN 的配置
- 掌握三层交换机基本配置方法；
- 掌握三层交换机 VLAN 路由的配置方法；
- 通过三层交换机实现 VLAN 间相互通信；

实验背景

- 某企业有两个主要部门，技术部和销售部，分处于不同的办公室，为了安全和便于管理对两个部门的主机进行了 VLAN 的划分，技术部和销售部分处于不同的 VLAN，先由于业务的需求需要销售部和技术部的主机能够相互访问，获得相应的资源，两个部门的交换机通过一台三层交换机进行了连接。

技术原理

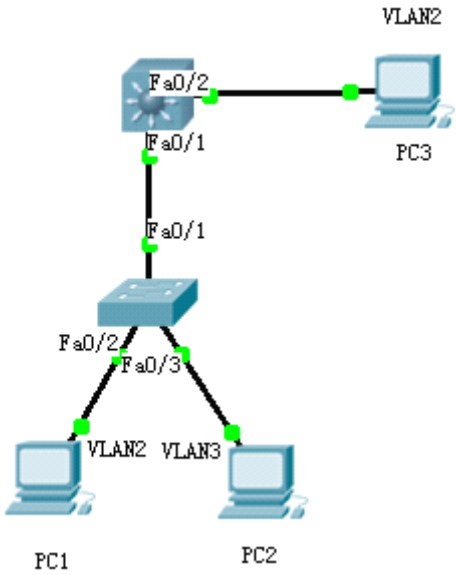
- 三层交换机具备网络层的功能，实现 VLAN 相互访问的原理是：利用三层交换机的路由功能，通过识别数据包的 IP 地址，查找路由表进行选路转发，三层交换机利用直连路由可以实现不同 VLAN 之间的相互访问。三层交换机给接口配置 IP 地址。采用 SVI（交换虚拟接口）的方式实现 VLAN 间互连。SVI 是指为交换机中的 VLAN 创建虚拟接口，并且配置 IP 地址。

实验步骤

- 新建 packet tracer 拓扑图
- （1）在二层交换机上配置 VLAN2、VLAN3，分别将端口 2、端口 3 划分给 VLAN2、VLAN3。
- （2）将二层交换机与三层交换机相连的端口 fa 0/1 都定义为 tag Vlan 模式。
- （3）在三层交换机上配置 VLAN2、VLAN3，此时验证二层交换机 VLAN2、VLAN3 下的主机之间不能相互通信。
- （4）设置三层交换机 VLAN 间的通信，创建 VLAN2,VLAN3 的虚接口，并配置虚接口 VLAN2、VLAN3 的 IP 地址。
- （5）查看三层交换机路由表。
- （6）将二层交换机 VLAN2、VLAN3 下的主机默认网关分别设置为相应虚拟接口的 IP 地址。
- （7）验证二层交换机 VLAN2,VALN3 下的主机之间可以相互通信。

实验设备

Switch_2960 1 台；Swithc_3560 1 台；PC 3 台；直连线



PC1

IP: 192.168.1.2

Submark: 255.255.255.0

Gateway: 192.168.1.1

PC2

IP: 192.168.2.2

Submark: 255.255.255.0

Gateway: 192.168.2.1

PC3

IP: 192.168.1.3

Submark: 255.255.255.0

Gateway: 192.168.1.1

S2960

en
conf t
vlan 2
exit
vlan 3
exit

int fa 0/2
switchport access vlan 2
int fa 0/3
switchport access vlan 3
int fa 0/1
switchport mode trunk
exit
show vlan

S3560

en
conf t
vlan 2
exit
vlan 3
exit
int fa 0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
int fa 0/2
switchport access vlan 2
exit

interface vlan 2
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface vlan 3
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
show ip route
show vlan

PC3 Ping PC1

Ping 192.168.1.2

PC3 Ping PC2

Ping 192.168.1.3

第六章　快速生成树配置

实验目标

- 理解生成树协议工作原理；
- 掌握快速生成树协议 RSTP 基本配置方法；

实验背景

- 学校为了开展计算机教学和网络办公，建立的一个计算机教室和一个校办公区，这两处的计算机网络通过两台交换机互联组成内部校园网，为了提高网络的可靠性，作为网络管理员，你要用 2 条链路将交换机互连，现要求在交换机上做适当配置，是网络避免环路。

技术原理

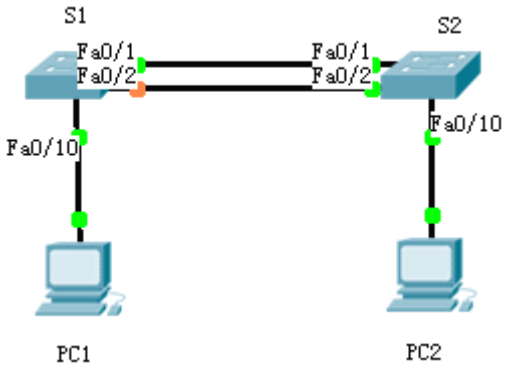
- 生成树协议（spanning-tree）,作用是在交换网络中提供冗余备份链路，并且解决交换网络中的环路问题；
- 生成树协议是利用 SPA 算法，在存在交换机环路的网络中生成一个没有环路的属性网络，运用该算法将交换网络的冗余备份链路从逻辑上断开，当主链路出现故障时，能够自动的切换到备份链路，保证数据的正常转发。
- 生成树协议版本：STP、RSTP（快速生成树协议）、MSTP（多生成树协议）。
- 生成树协议的特点收敛时间长。从主要链路出现故障到切换至备份链路需要 50 秒时间。
- 快速生成树在生成树协议的基础上增加了两种端口角色，替换端口或备份端口，分别作为根端口和指定端口。当根端口或指定端口出现故障时，冗余端口不需要经过 50 秒的收敛时间，可以直接切换到替换端口或备份端口，从而实现 RSTP 协议小于 1 秒的快速收敛。

实验步骤

- 新建 packet tracer 拓扑图
- 默认情况下 STP 协议是启用的。通过两台交换机之间传送 BPDU 协议数据单元。选出跟交换机、根端口等，以便确定端口的转发状态。图中标记为黄色的端口处于 block 堵塞状态。
- 设置 RSTP。
- 查看交换机 show spanning-tree 状态，了解跟交换机和根端口情况。
- 通过更改交换机生成树的优先级 spanning-tree vlan 10 priority 4096 可以变化跟交换机的角色。
- 测试。当主链路处于 down 状态时候，能够自动的切换到备份链路，保证数据的正常转发。

实验设备

Switch_2960 2 台；PC 2 台；直连线（各设备互联）



PC1

IP: 192.168.1.2

Submask: 255.255.255.0

Gateway: 192.168.1.1

PC2

IP: 192.168.1.3

Submask: 255.255.255.0

Gateway: 192.168.1.1

S1

```
en
show spanning-tree
conf t
hostname S1
int fa 0/10
switchport access vlan 10
exit
int rang fa 0/1 - 2
switchport mode trunk
exit
spanning-tree mode rapid-pvst
end
```

S2

```
en
conf t
hostname S2
int fa 0/10
switchport access vlan 10
exit
int range fa 0/1 - 2
switchport mode turnk
exit
spanning-tree mode rapid-pvst
```

end
show spanning-tree

PC1
ipconfig
ping -t 192.168.1.3

S2
en
conf t
int fa 0/1
shut
（查看 PC1 的 ping 情况是否正常）

第七章　路由器的基本配置

实验目标

- 掌握路由器几种常用配置方法；
- 掌握采用 Console 线缆配置路由器的方法；
- 掌握采用 Telnet 方式配置路由器的方法；
- 熟悉路由器不同的命令行操作模式以及各种模式之间的切换；
- 掌握路由器的基本配置命令；

实验背景

- 你是某公司新进的网管，公司要求你熟悉网络产品，首先要求你登录路由器，了解、掌握路由器的命令行操作；
- 作为网络管理员，你第一次在设备机房对路由器进行了初次配置后，希望以后在办公室或出差时也可以对设备进行远程管理，现要在路由器上做适当配置。

技术原理

- 路由器的管理方式基本分为两种：带内管理和带外管理。通过路由器的 Console 口管理路由器属于带外管理，不占用路由器的网络接口，其特点是需要使用配置线缆，近距离配置。第一次配置时必须利用 Console 端口进行配置。

实验步骤

- 新建 packet tracer 拓扑图
- （1）用标准 console 线缆用于连接计算机的串口和路由器的 console 上。在计算机上启用超级终端，并配置超级终端的参数，是计算机与路由器通过 console 接口建立连接；
- （2）配置路由器的管理的 IP 地址，并为 Telnet 用户配置用户名和登录口令。配置计算机的 IP 地址（与路由器管理 IP 地址在同一个网段），通过网线将计算机和路由器相连，通过计算机 Telnet 到路由器上对交换机进行查看；
- （3）更改路由器的主机名；
- （4）擦除配置信息。保存配置信息，显示配置信息；
- （5）显示当前配置信息；
- （6）显示历史命令。

实验设备

Router_2811 1 台；PC 1 台；交叉线；配置线

说明：　交叉线：路由器与计算机相连 路由器与交换机相连

　　直连线：计算机与交换机相连

PC

IP: 192.168.1.2

Submask: 255.255.255.0

Gageway:192.168.1.1

Router

图形化：界面开启 FastEthernet0/0 端口

命令行：rip 视图：router rip; ospf 视图:router ospf 1

PC 终端

```
en
conf t
hostname R1
enable secret 123456 //设置特权密码
exit
exit

en
password:此时输入密码，输入的密码不显示
conf t
line vty 0 4     //设置 telnet 密码
password 5ijsj
login
exit
interface fa 0/0
ip address 192.168.1.1 255.255.255.0
no shut
end
```

PC CMD

ipconfig

ping 192.168.1.1

telnet 192.168.1.1

password:5ijsi

en

password:123456

show runing

第八章　路由器单臂路由配置

实验目标

掌握单臂路由器配置方法；

通过单臂路由器实现不同 VLAN 之间互相通信；

实验背景

某企业有两个主要部门，技术部和销售部，分处于不同的办公室，为了安全和便于管理对两个部门的主机进行了 VLAN 的划分，技术部和销售部分处于不同的 VLAN。现由于业务的需求需要销售部和技术部的主机能够相互访问，获得相应的资源，两个部门的交换机通过一台路由器进行了连接。

技术原理

单臂路由：是为实现 VLAN 间通信的三层网络设备路由器，它只需要一个以太网，通过创建子接口可以承担所有 VLAN 的网关，而在不同的 VLAN 间转发数据。

实验步骤

新建 packer tracer 拓扑图

当交换机设置两个 Vlan 时，逻辑上已经成为两个网络，广播被隔离了。两个 Vlan 的网络要通信，必须通过路由器，如果接入路由器的一个物理端口，则必须有两个子接口分别与两个 Vlan 对应，同时还要求与路由器相连得交换机的端口 fa 0/1 要设置为 trunk，因为这个接口要通过两个 Vlan 的数据包。

检查设置情况，应该能够正确的看到 Vlan 和 Trunk 信息。

计算机的网关分别指向路由器的子接口。

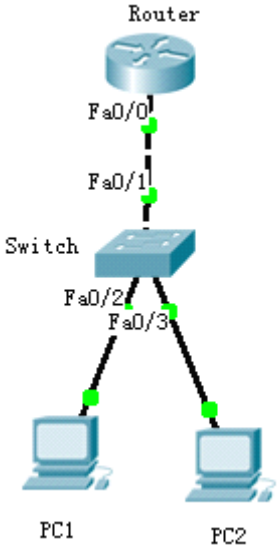
配置子接口，开启路由器物理接口。

默认封装 dot1q 协议。

配置路由器子接口 IP 地址。

实验设备

PC 2 台；Router_2811 1 台；Switch_2960 1 台



Switch

en
conf t
vlan 2
exit
vlan 3
exit

interface fastEthernet 0/2
switchport access vlan 2
exit
int fa 0/3
switchport access vlan 3
exit

int fa 0/1
switchport mode trunk

Router

en
conf t
int fa 0/0
no shutdown
exit

interface fast 0/0.1
encapsulation dot1Q 2
ip address 192.168.1.1 255.255.255.0
exit

int fa 0/0.2
encapsulation dot1q 3
ip address 192.168.2.1 255.255.255.0
end

show ip route

第九章　路由器静态路由配置

实验目标

- 掌握静态路由的配置方法和技巧；
- 掌握通过静态路由方式实现网络的连通性；
- 熟悉广域网线缆的链接方式；

实验背景

学校有新旧两个校区，每个校区是一个独立的局域网，为了使新旧校区能够正常相互通讯，共享资源。每个校区出口利用一台路由器进行连接，两台路由器间学校申请了一条 2M 的 DDN 专线进行相连，要求做适当配置实现两个校区的正常相互访问。

技术原理

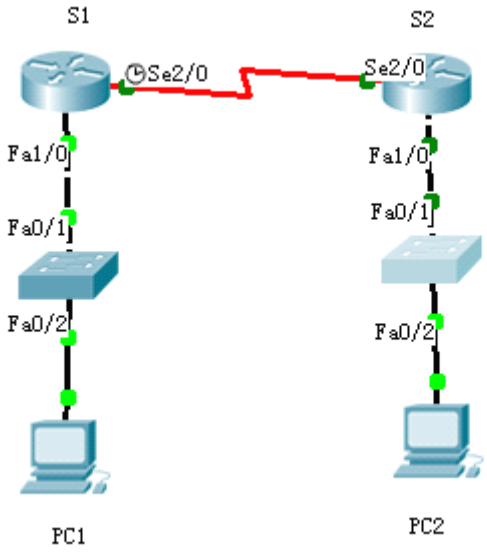
- 路由器属于网络层设备，能够根据 IP 包头的信息，选择一条最佳路径，将数据包转发出去。实现不同网段的主机之间的互相访问。路由器是根据路由表进行选路和转发的。而路由表里就是由一条条路由信息组成。
- 生成路由表主要有两种方法：手工配置和动态配置，即静态路由协议配置和动态路由协议配置。
- 静态路由是指有网络管理员手工配置的路由信息。
- 静态路由除了具有简单、高效、可靠的优点外，它的另一个好处是网络安全保密性高。
- 缺省路由可以看做是静态路由的一种特殊情况。当数据在查找路由表时，没有找到和目标相匹配的路由表项时，为数据指定路由。

实验步骤

- 新建 packet tracer 拓扑图
- （1）在路由器 R1、R2 上配置接口的 IP 地址和 R1 串口上的时钟频率；
- （2）查看路由器生成的直连路由；
- （3）在路由器 R1、R2 上配置静态路由；
- （4）验证 R1、R2 上的静态路由配置；
- （5）将 PC1、PC2 主机默认网关分别设置为路由器接口 fa 1/0 的 IP 地址；
- （6）PC1、PC2 主机之间可以相互通信；

实验设备

pc 2 台；Router-PT 可扩展路由 2 台（Switch_2811 无 V.35 线接口）；Switch_2960 2 台；DCE 串口线；直连线；交叉线



PC1

IP: 192.168.1.2

Submask: 255.255.255.0

Gateway: 192.168.1.1

PC2

IP: 192.168.2.2

Submask: 255.255.255.0

Gateway: 192.168.2.1

R1

```
en
conf t
hostname R1
int fa 1/0
no shut
ip address 192.168.1.1 255.255.255.0
exit
int serial 2/0
no shut
ip address 192.168.3.1 255.255.255.0
clock rate 64000（必须配置时钟才可通信）
end
```

R2

```
en
conf t
hostname R2
int fa 1/0
no shut
```

ip address 192.168.2.1 255.255.255.0
exit
int serial 2/0
ip address 192.168.3.2 255.255.255.0
no shut
end

R1

en
conf t
ip route 192.168.2.0 255.255.255.0 192.168.3.2
end
show ip route

R2

en
conf t
ip route 192.168.1.0 255.255.255.0 192.168.3.1
end
show ip route

第十章　路由器 RIP 动态路由配置

实验目的

- 掌握 RIP 协议的配置方法；
- 掌握查看通过动态路由协议 RIP 学习产生的路由；
- 熟悉广域网线缆的链接方式；

实验背景

假设校园网通过一台三层交换机连到校园网出口路由器上，路由器再和校园外的另一台路由器连接。现要做适当配置，实现校园网内部主机与校园网外部主机之间的相互通信。为了简化网管的管理维护工作，学校决定采用 RIPV2 协议实现互通。

技术原理

- **RIP(Routing Information Protocols,路由信息协议)**是应用较早、使用较普遍的 IGP 内部网管协议，使用于小型同类网络，是距离矢量协议；
- **RIP** 协议跳数作为衡量路径开销的，**RIP** 协议里规定最大跳数为 15；
- **RIP** 协议有两个版本：**RIPv1** 和 **RIPv2**，**RIPv1** 属于有类路由协议，不支持 **VLSM**，以广播形式进行路由信息的更新，更新周期为 30 秒；**RIPv2** 属于无类路由协议，支持 **VLSM**，以组播形式进行路由更细。

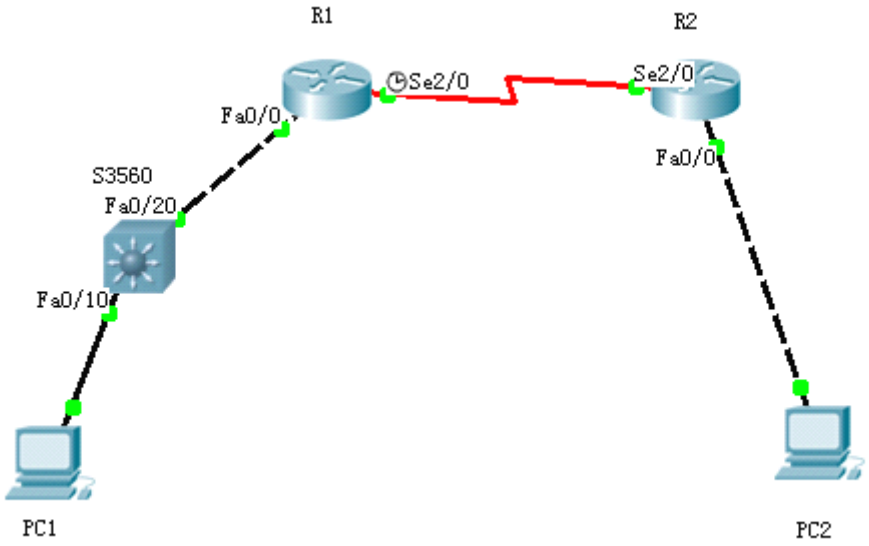
实验步骤

- 建立建立 packet tracer 拓扑图
- （1）在本实验中的三层交换机上划分 VLAN10 和 VLAN20，其中 VLAN10 用于连接校园网主机，VLAN20 用于连接 R1。
- （2）路由器之间通过 V.35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000。

- （3）主机和交换机通过直连线，主机与路由器通过交叉线连接。
- （4）在 S3560 上配置 RIPV2 路由协议。
- （5）在路由器 R1、R2 上配置 RIPV2 路由协议。
- （6）将 PC1、PC2 主机默认网关设置为与直连网路设备接口 IP 地址。
- （7）验证 PC1、PC2 主机之间可以互相同信；

实验设备

PC 2 台；Switch_3560 1 台；Router-PT 2 台；直连线；交叉线；DCE 串口线



PC1

IP: 192.168.1.2

Submask: 255.255.255.0

Gateway: 192.168.1.1

PC2

IP: 192.168.2.2

Submask: 255.255.255.0

Gateway: 192.168.2.1

S3560

```
en
conf t
hostname S3560
vlan 10
exit
vlan 20
exit
interface fa 0/10
switchport access vlan 10
exit
interface fa 0/20
```

switchport access valn 20
exit
end
show vlan

conf t
interface vlan 10
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface vlan 20
ip address 192.168.3.1 255.255.255.0
no shutdown
end
show ip route
show runing

conf t
router rip
network 192.168.1.0
network 192.168.3.0
version 2
end
show ip route

R1

en
conf t
hostname R1
interface fa 0/0
no shutdown
ip address 192.168.3.2 255.255.255.0

interface serial 2/0
no shutdown
ip address 192.168.4.1 255.255.255.0
clock rate 64000
end
show ip route

conf t
router rip
network 192.168.3.0
network 192.168.4.0

version 2
exit

R2

en
conf t
hostname R2
interface fa 0/0
no shutdown
ip address 192.168.2.1 255.255.255.0
interface serial 2/0
no shutdown
ip address 192.168.4.2 255.255.255.0
end
show ip route
conf t
router rip
network 192.168.2.0
netword 192.168.4.0
version 2
end

第十一章　路由器 OSPF 动态路由配置

实验目的

- 掌握 OSPF 协议的配置方法；
- 掌握查看通过动态路由协议 OSPF 学习产生的路由；
- 熟悉广域网线缆的链接方式；

实验背景

假设校园网通过一台三层交换机连到校园网出口路由器上，路由器再和校园外的另一台路由器连接。现要做适当配置，实现校园网内部主机与校园网外部主机之间的相互通信。为了简化网管的管理维护工作，学校决定采用 OSPF 协议实现互通。

技术原理

- OSPF 开放式最短路径优先协议，是目前网路中应用最广泛的路由协议之一。属于内部网管路由协议，能够适应各种规模的网络环境，是典型的链路状态协议。OSPF 路由协议通过向全网扩散本设备的链路状态信息，使网络中每台设备最终同步一个具有全网链路状态的数据库，然后路由器采用 SPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。

实验步骤

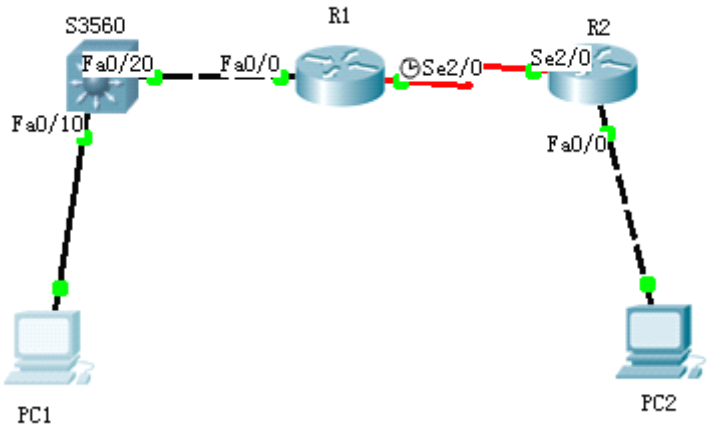
- 新建 packet tracer 拓扑图
- （1）在本实验中的三层交换机上划分 VLAN10 和 VLAN20，其中 VLAN10 用于连接校园网主机，VLAN20 用于连接 R1。
- （2）路由器之间通过 V35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟

频率 64000。

- （3）主机和交换机通过直连线，主机与路由器通过交叉线连接。
- （4）在 S3560 上配置 OSPF 路由协议。
- （5）在路由器 R1、R2 上配置 OSPF 路由协议。
- （6）将 PC1、PC2 主机默认网关设置为与直连网路设备接口 IP 地址。
- （7）验证 PC1、PC2 主机之间可以互相同信；

实验设备

PC 2 台；Switch_3560 1 台；Router-PT 2 台；直连线；交叉线；DCE 串口线



PC1

IP: 192.168.1.2

Submask: 255.255.255.0

Gateway: 192.168.1.1

PC2

IP: 192.168.2.2

Submask: 255.255.255.0

Gateway: 192.168.2.1

S3560

```
en
conf t
hostname S3569
vlan 10
exit
vlan 20
interface fa 0/10
switchport access vlan 10
exit
int fa 0/20
switchport access valn 20
exit
interface valn 10
ip address 192.168.1.1 255.255.255.0
```

```
no shutdown
exit
interface vlan 20
ip address 192.168.3.1 255.255.255.0
no shutdown
end
show ip route

conf t
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
end
show ip route
```

R1

```
en
conf t
hostname R1
interface fa 0/0
no shutdown
ip address 192.168.3.2 255.255.255.0
exit
interface serial 2/0
no shutdown
clock rate 64000
ip address 192.168.4.1 255.255.255.0
end
show ip route

conf t
router ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
end
show ip route
```

R2

```
en
conf t
hostname R2
interface fa 0/0
no shutdown
ip address 192.168.2.1 255.255.255.0
```

```
exit

interface serial 2/0
no shutdown
ip address 192.168.4.2 255.255.255.0
end
show ip route

conf t
router ospf 1
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
end
show ip route
```

第十二章　路由器综合路由配置

实验目标

掌握综合路由器的配置方法；

掌握查看通过路由重分布学习产生的路由；

熟悉广域网线缆的链接方式；

实验背景

假设某公司通过一台三层交换机连到公司出口路由器 R1 上，路由器 R1 再和公司外的另一台路由器 R2 连接。三层交换机与 R1 间运行 RIPV2 路由协议，R1 与 R2 间运行 OSPF 路由协议。现要做适当配置，实现公司内部主机与公司外部主机之间的相互通信。

技术原理

为了支持本设备能够运行多个路由协议进程，系统软件提供了路由信息从一个路由进程重分布到另一个路由进程的功能。比如你可以将 OSPF 路由域的路由重新分布后通高 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。

要把路由从一个路由域分布到另一个路由域，并且进行控制路由重分布，在路由进程配置模式中执行以下命令：

redistribute protocol [metric metric][metric-type metric-type][match internal|external type|nssa-external type][tag tag][route-map route-map-name][subnets]

实验步骤

新建 Packet Tracer 拓扑图

（1）PC 与交换机间用直连线连接；PC 与路由、路由与路由之间用交叉线连接。

（2）在三层上划分 2 个 Vlan，运行 RIPV2 协议；R2 运行 OSPF 协议。

（5）在路由器 R1 上左侧配置 RIPV2 路由协议；右侧配置 OSPF 协议。

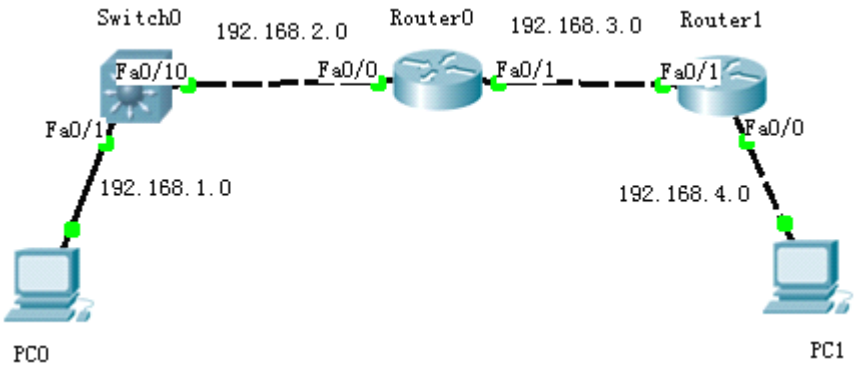
（6）在 R1 路由进程中引入外部路由，进行路由重分布。

（7）将 PC1、PC2 主机默认网关分别设置为与直接网络设备接口 IP 地址。

（8）验证 PC1、PC2 主机之间可以互相通信；

实验设备

Router_1841 2 台；Switch_3560 1 台；直通线；交叉线



PC0

IP: 192.168.1.2

Submask: 255.255.255.0

Gageway: 192.168.1.1

PC1

IP: 192.168.4.2

Submask: 255.255.255.0

Gageway: 192.168.4.1

Switch0

en

conf t

vlan 2

exit

int fa 0/10

switchport access vlan 2

exit

int vlan 1

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

int vlan 2

ip address 192.168.2.1 225.255.255.0

no shutdown

end

show int vlan 1

conf t

router rip

network 192.168.1.0

network 192.168.2.0

version 2

Router0

en

conf t
host R1
inf fa 0/0
ip address 192.168.2.2 255.255.255.0
no shutdown
int fa 0/1
ip address 192.168.3.1 255.255.255.0
no shutdown
exit

router rip
network 192.168.2.0
version 2
router ospf 1
network 192.168.3.0 0.0.0.255 area 0

Route1

en
conf t
host R2
int fa 0/1
ip address 192.168.3.2 255.255.255.0
no shutdown
int fa 0/0
ip address 192.168.4.1 255.255.255.0
no shutdown
exit
router ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
end
show ip route

Router0

end
show ip route
show run
show ip route
ping 192.168.1.2 (success)
ping 192.168.4.2 (success)

PC0

ping 192.168.4.2 (Replay form 192.168.1.1: Destination host unreachable)

Switch_3560

show ip rout (只有两条直连路由)

Router0

conf t

router rip
redistribute ospf 1
exit
router ospf 1
redistribute rip subnets
end

Router1

show ip route

PC0

ping 192.168.4.2 (Replay form 192.168.4.2: byes=32 time=125ms TTL=125)

说明：本例在 Packet Tracer 5.2 上能正常运行，在 Packet Tracer 5.3 上 Switch0 不能学习到 192.168.3.0、192.168.4.0 的路由信息，需要给 Switch0 指定静态路由：ip route 0.0.0.0 0.0.0.0 192.168.2.2

第十三章　标准 IP 访问控制列表配置

实验目标

理解标准 IP 访问控制列表的原理及功能；

掌握编号的标准 IP 访问控制列表的配置方法；

实验背景

你是公司的网络管理员，公司的经理部、财务部们和销售部门分属于不同的 3 个网段，三部门之间用路由器进行信息传递，为了安全起见，公司领导要求销售部门不能对财务部进行访问，但经理部可以对财务部进行访问。

PC1 代表经理部的主机、PC2 代表销售部的主机、PC3 代表财务部的主机。

技术原理

ACLs 的全称为接入控制列表（Access Control Lists），也称访问控制列表（Access Lists），俗称防火墙，在有的文档中还称包过滤。ACLs 通过定义一些规则对网络设备接口上的数据包文进行控制；允许通过或丢弃，从而提高网络可管理型和安全性；

IP ACL 分为两种：标准 IP 访问列表和扩展 IP 访问列表，编号范围为 1～99、1300～1999、100～199、2000～2699；

标准 IP 访问控制列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤；

扩展 IP 访问列表可以根据数据包的原 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤；

IP ACL 基于接口进行规则的应用，分为：入栈应用和出栈应用；

实验步骤

新建 Packet Tracer 拓扑图

（1）路由器之间通过 V.35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000；主机与路由器通过交叉线连接。

（2）配置路由器接口 IP 地址。

（3）在路由器上配置静态路由协议，让三台 PC 能够相互 Ping 通，因为只有在互通的前提下才涉及到方控制列表。

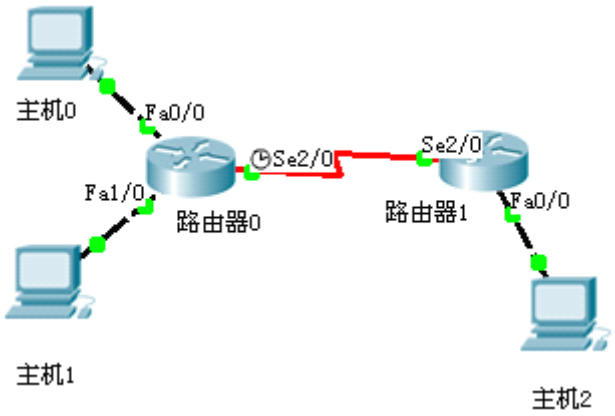
（4）在 R1 上编号的 IP 标准访问控制

（5）将标准 IP 访问控制应用到接口上。

（6）验证主机之间的互通性。

实验设备

PC 3 台；Router-PT 2 台；交叉线；DCE 串口线；



PC0

IP: 172.16.1.2

Submask: 255.255.255.0

Gageway: 172.16.1.1

PC1

IP: 172.16.2.2

Submask: 255.255.255.0

Gageway: 172.16.2.1

PC2

IP: 172.16.4.2

Submask: 255.255.255.0

Gageway: 172.16.4.1

Router0

```
en
conf t
host R0
int fa 0/0
ip address 172.16.1.1 255.255.255.0
no shutdown
int fa 1/0
ip address 172.16.2.1 255.255.255.0
no shutdown
int s 2/0
ip address 172.16.3.1 255.255.255.0
no shutdown
clock rate 64000
```

Router1

```
en
conf t
host R1
```

int s 2/0
ip address 172.16.3.2 255.255.255.0
no shutdown
int fa 0/0
ip address 172.16.4.1 255.255.255.0
no shutdown

Router0
exit
ip route 172.16.4.0 255.255.255.0 172.16.3.2

Router1
exit
ip route 0.0.0.0 0.0.0.0 172.16.3.1
end
show ip route

PC0
ping 172.16.4.2 (success)

PC1
ping 172.16.4.2 (success)

Router0
ip access-list standard 5ijsj
permit 172.16.1.0 0.0.0.255
deny 172.16.2.0 0.0.0.255 (如果有上面的 permit 默认跟一个 deny，所以此命令可不写)
conf t
int s 2/0
ip access-group 5ijsj out
end

PC0
ping 172.16.4.2 (success)

PC1
ping 172.16.4.2 (Replay from 172.16.2.1: Destination host unreachable)

第十四章　扩展 IP 访问控制列表配置

实验目标

理解标准 IP 访问控制列表的原理及功能；

掌握编号的标准 IP 访问控制列表的配置方法；

实验背景

你是公司的网络管理员，公司的经理部、财务部们和销售部门分属于不同的 3 个网段，三部门之间用路由器进行信息传递，为了安全起见，公司领导要求销售部门不能对财务部进行访问，但经理部可以对财务部进行访问。

PC1 代表经理部的主机、PC2 代表销售部的主机、PC3 代表财务部的主机。

技术原理

访问列表中定义的典型规则主要有以下：源地址、目标地址、上层协议、时间区域；

扩展 IP 访问列表（编号 100-199、2000、2699）使用以上四种组合来进行转发或阻断分

组；可以根据数据包的源 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。

扩展 IP 访问列表的配置包括以下两部：

定义扩展 IP 访问列表

将扩展 IP 访问列表应用于特定接口上

实验步骤

新建 Packet Tracer 拓扑图

（1）分公司出口路由器与外路由器之间通过 V.35 电缆串口连接，DCE 端连接在 R2 上，配置其时钟频率 64000；主机与路由器通过交叉线连接。

（2）配置 PC 机、服务器及路由器接口 IP 地址。

（3）在各路由器上配置静态路由协议，让 PC 间能相互 ping 通，因为只有在互通的前提下才涉及到访问控制列表。

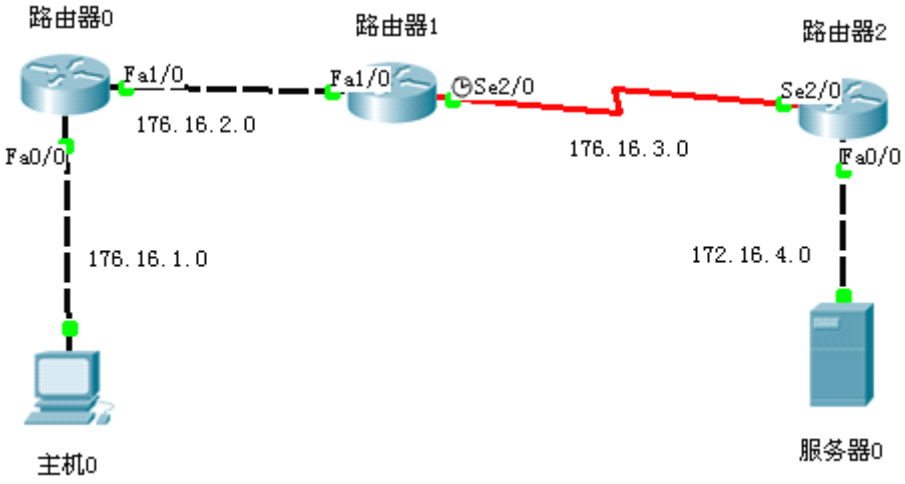
（4）在 R2 上配置编号的 IP 扩展访问控制列表。

（5）将扩展 IP 访问列表应用到接口上、。

（6）验证主机之间的互通性。

实验设备

PC 1 台；Server-PT 1 台； Router-PT 3 台；交叉线；DCE 串口线



PC0

IP: 172.16.1.2

Submask: 255.255.255.0

Gateway: 172.16.1.1

Server0

IP: 172.16.4.2

Submask: 255.255.255.0

Gateway: 172.16.4.1

Router0

en

conf t

host R0

int fa 0/0

ip address 172.16.1.1 255.255.255.0

no shutdown
int fa 1/0
ip address 172.16.2.1 255.255.255.0
no shutdown
exit

Router1

en
conf t
host R1
int fa 1/0
ip address 172.16.2.2 255.255.255.0
no shutdown
int s 2/0
ip address 172.16.3.1 255.255.255.0
no shutdown
clock rate 64000

Router2

en
conf t
host R2
int s 2/0
ip address 172.16.3.2 255.255.255.0
no shutdown
int fa 0/0
ip address 172.16.4.1 255.255.255.0
no shutdown

Router0

ip route 0.0.0.0 0.0.0.0 172.16.2.2

Router2

exit
ip route 0.0.0.0 0.0.0.0 172.16.3.1

Router1

eixt
ip route 172.16.1.0 255.255.255.0 172.16.2.1
ip route 172.16.4.0 255.255.255.0 172.16.3.2
end
show ip route

PC0

ping 172.16.4.2(success)

Web 浏览器：http://172.16.4.2(success)

Router1

conf t

access-list 100 permit tcp host 172.16.1.2 host 172.16.4.2 eq www
access-lint 100 deny icmp host 172.16.1.2 host 172.16.4.2 echo
int s 2/0
ip access-group 100 out
end

PC0

Web 浏览器：http://172.16.4.2(success)
ping 172.16.4.2(Reply from 172.16.2.2: Destination host unreachable)

第十五章　网络地址转换 NAT 配置

实验目标

理解 NAT 网络地址转换的原理及功能；
掌握静态 NAT 的配置，实现局域网访问互联网；

实验背景

你是某公司的网络管理员，欲发布公司的 WWW 服务。现要求将内网 Web 服务器 IP 地址映射为全局 IP 地址，实现外部网络可以访问公司内部 Web 服务器。

技术原理

网络地址转换 NAT（Network Address Translation），被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

默认情况下，内部 IP 地址是无法被路由到外网的，内部主机 10.1.1.1 要与外部 Internet 通信，IP 包到达 NAT 路由器时，IP 包头的源地址 10.1.1.1 被替换成一个合法的外网 IP，并在 NAT 转发表中保存这条记录。当外部主机发送一个应答到内网时，NAT 路由器受到后，查看当前 NAT 转换表，用 10.1.1.1 替换掉这个外网地址。

NAT 将网络划分为内部网络和外部网络两部分，局域网主机利用 NAT 访问网络时，是将局域网内部的本地地址转换为全局地址（互联网合法的 IP 地址）后转发数据包；

NAT 分为两种类型：NAT（网络地址转换）和 NAPT（网络端口地址转换 IP 地址对应一个全局地址）。

静态 NAT：实现内部地址与外部地址一对一的映射。现实中，一般都用于服务器；
动态 NAT：定义一个地址池，自动映射，也是一对一的。现实中，用得比较少；
NAPT：使用不同的端口来映射多个内网 IP 地址到一个指定的外网 IP 地址，多对一。

实验步骤

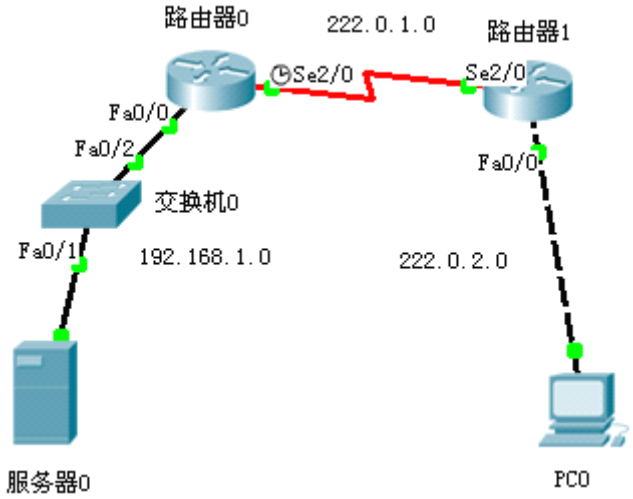
新建 Packet Tracer 拓扑图

（1）R1 为公司出口路由器，其与外部路由器之间通过 V.35 电缆串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000；
（2）配置 PC 机、服务器及路由器接口 IP 地址；
（3）在各路由器上配置静态路由协议，让 PC 间能相互 Ping 通；
（4）在 R1 上配置静态 NAT。
（5）在 R1 上定义内外网络接口。
（6）验证主机之间的互通性。

实验设备

PC 1 台；Server-PT 1 台；Switch_2950-24 1 台；Router-PT 2 台；直连线；交叉线；DCE

串口线



Server-PT

192.168.1.2

255.255.255.0

192.168.1.1

PC0

222.0.2.2

255.255.255.0

222.0.2.1

Router0

en

conf t

host R0

int fa 0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

int s 2/0

ip address 222.0.1.1 255.255.255.0

no shutdown

clock rate 64000

Router1

en

conf t

host R1

int s 2/0

ip address 222.0.1.2 255.255.255.0

no shut

int fa 0/0

ip address 222.0.2.1 255.255.255.0

no shutdown

Router0

exit;
ip route 222.0.2.0 255.255.255.0 222.0.1.2
Router1
exit
ip route 192.168.1.0 255.255.255.0 222.0.1.1
end
show ip route
PC0
CMD
ping 192.168.1.2 (success)
Web 浏览器
http://192.168.1.2 (success)
Router0
int fa 0/0
ip nat inside
int s 2/0
ip nat outside
exit
ip nat inside source static 192.168.1.2 222.0.1.3
end
show ip nat translations
PC0
Web 浏览器
http://222.0.1.3 (success)
Router0
show ip nat translations

第十六章　网络端口地址转换 NAPT 配置

实验背景

理解 NAT 网络地址转换的原理及功能；

掌握 NAPT 的配置，实现局域网访问互联网；

实验背景

你是某公司的网络管理员，公司办公网需要接入互联网，公司只向 ISP 申请了一条专线，该专线分配了一个公司 IP 地址，配置实现全公司的主机都能访问外网。

技术原理

NAT 将网络划分为内部网络和外部网络两部分，局域网主机利用 NAT 访问网络时，是将局域网内部的本地地址转换为全局地址（互联网合法的 IP 地址）后转发数据包；

NAT 分为两种类型：NAT（网络地址转换）和 NAPT（网络端口地址转换 IP 地址对应一个全局地址）。

NAPT：使用不同的端口来映射多个内网 IP 地址到一个指定的外网 IP 地址，多对一。

NAPT 采用端口多路复用方式。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。同时，又可隐藏网络内部的所

有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

实验步骤

新建 Packet Tracer 拓扑图

（1）R1 为公司出口路由器，其与 ISP 路由器之间通过 V.35 电缆串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000；

（2）配置 PC 机、服务器及路由器接口 IP 地址；

（3）在各路由器上配置静态路由协议，让 PC 间能相互 Ping 通；

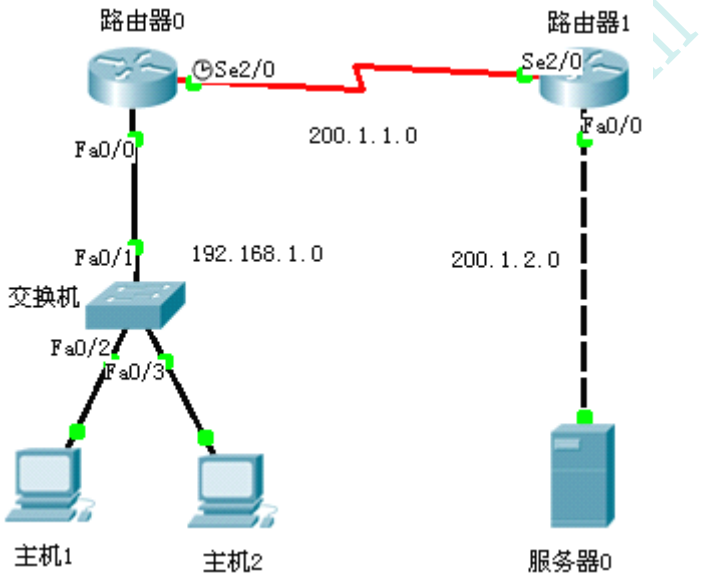
（4）在 R1 上配置 NAPT。

（5）在 R1 上定义内外网络接口。

（6）验证主机之间的互通性。

实验设备

PC 2 台；Server-PT 1 台；Switch_2950-24 1 台 Router-PT 2 台；直通线；交叉线；DCE 串口线



PC1

192.168.1.2

255.255.255.0

192.168.1.1

PC2

192.168.1.3

255.255.255.0

192.168.1.1

Server

200.1.2.2

255.255.255.0

200.1.2.1

Router0

en

conf t
host R0
int fa 0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
int s 2/0
ip address 200.1.1.1 255.255.255.0
no shutdown
clock rate 64000

Router1

en
conf t
host R1
int s 2/0
ip address 200.1.1.2 255.255.255.0
no shutdown
int fa 0/0
ip address 200.1.2.1 255.255.255.0
no shutdown

Router0

exit
ip route 200.1.2.0 255.255.255.0 200.1.1.2

Router1

exit
ip route 192.168.1.0 255.255.255.0 200.1.1.1
end
show ip route

PC1

CMD

ping 200.1.2.2 (success)

Web 浏览器

http://200.1.2.2 (success)

Router0

int fa 0/0
ip nat inside
int s 2/0
ip nat outside
exit
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat pool 5ijsj 200.1.1.3 200.1.1.3 netmask 255.255.255.0
ip nat inside source list 1 pool 5ijsj overload (无 overload 表示多对多，有 overload 表示多对一)
end
show ip nat translations(无结果)

PC1

Web 浏览器

http://200.1.2.2 (success)

Router0

show ip nat translations(有 1 个结果)

PC2

Web 浏览器

http://200.1.2.2 (success)

Router0

show ip nat translations(有 2 个结果)