第一次实验

认识 Packet Tracer 软件

Packet Tracher 介绍

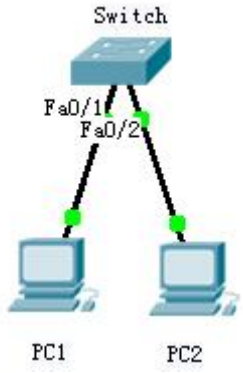
- Packet Tracer 是 Cisco 公司针对 CCNA 认证开发的一个用来设计、配置和故障排除网络的模拟软件。
- Packer Tracer 模拟器软件比 Boson 功能强大，比 Dynamips 操作简单，非常适合网络设备初学者使用。 No ip domain-lookup

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

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)#
  - Vlan 模式 Switch(config-vlan)#
  - Vlan 接口模式 Switch(config-if-vlan)#
  - 线路模式 Switch(config-line)#

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)

实验设备

Switch_2960 1 台；PC 1 台；配置线；

PC console 端口

Switch>enable

Switch#conf t

Switch(config)#hostname X

X(config)#interface fa 0/1

X(config-if)#end

使用 tab 键，命令简写，帮助命令？

交换机的端口配置与管理

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，对交换机进行端口的配置与管理。

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。

- 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：

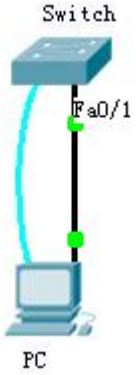
- 新建 Packet Tracer 拓扑图
- 了解交换机端口配置命令行
  - 修改交换机名称(hostname X)
  - 配置交换机端口参数(speed,duplex)
  - 查看交换机版本信息(show version)
  - 查看当前生效的配置信息(show running-config)
  - 查看保存在 NVRAM 中的启动配置信息(show startup-config)
  - 查看端口信息 Switch#show interface
  - 查看交换机的 MAC 地址表 Switch#show mac-address-table
  - 选择某个端口 Switch(config)# interface　type mod/port　(type 表示端口类型，通常有 ethernet、Fastethernet、Gigabitethernet)（mod 表示端口所在的模块，port 表示在该模块中的编号）例如 interface fastethernet0/1
  - 选择多个端口 Switch(config)#interface　type mod/startport-endport
  - 设置端口通信速度 Switch(config-if)#speed [10/100/auto]
  - 设置端口单双工模式 Switch(config-if)#duplex [half/full/auto]
  - 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 表示配置控制台线路，0 是控制台的线路编号。
  - switch(config-line)# login　用于打开登录认证功能。
  - switch(config-line)# password 5ijsj　//设置进入控制台访问的密码
  -

若交换机设置为 auto 以外的具体速度，此时应注意保证通信双方也要有相同的设置值。

注意事项：在配置交换机时，要注意交换机端口的单双工模式的匹配，如果链路一端设置的是全双工，另一端是自动协商，则会造成响应差和高出错率，丢包现象会很严重。通常两端设置为相同的模式。

实验设备

Switch_2960 1 台；PC 1 台；配置线；直通线



PC console 端口

Switch>enable

Switch#conf　t

Switch(config)#hostname　S2960

S2960(config)#interface fa 0/1

S2960(config-if)#speed 100

S2960(config-if)#duplex full

S2960(config-if)#exit

同时将 PC 的网卡改成全双工模式，100M 速率，否则链路不通

S2960(config)#hostname switch

Switch(config)#exit

Switch#show version

Switch#show run

Switch#show interface

Switch#show mac-address-table

Switch#config t

Switch(config)#enable　password　123//激活特权模式密码为 123

//Switch(config)#no enable password //取消特权模式密码

Switch(config)#line console 0

Switch(config-line)#password 456

Switch(config-line)#login

//Switch(config-line)#no password//取消密码

//请注意验证特权模式密码 123 与 console 口密码 456 使用范围

交换机的端口聚合配置

实验目标

理解端口聚合基本原理；

掌握一般交换机端口聚合的配置方法；

实验背景

端口聚合（又称为链路聚合），将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起，形成一个拥有较大宽带的端口，可以实现负载分担，并提供冗余链路。

技术原理

端口聚合使用的是 EtherChannel 特性，在交换机到交换机之间提供冗余的高速的连接方式。将两个设备之间多条 FastEthernet 或 GigabitEthernet 物理链路捆在一起组成一条设备间逻辑链路，从而增强带宽，提供冗余。

两台交换机到计算机的速率都是 100M，SW1 和 SW2 之间虽有两条 100M 的物理通道相连，可由于生成树的原因，只有 100M 可用，交换机之间的链路很容易形成瓶颈，使用端口聚合技术，把两个 100M 链路聚合成一个 200M 的逻辑链路，当一条链路出现故障，另一条链路会继续工作。

一台 S2000 系列以太网交换机只能有 1 个汇聚组，1 个汇聚组最多可以有 4 个端口。组内的端口号必须连续，但对起始端口无特殊要求。

在一个端口汇聚组中，端口号最小的作为主端口，其他的作为成员端口。同一个汇聚组中成员端口的链路类型与主端口的链路类型保持一致，即如果主端口为 Trunk 端口，则成员端口也为 Trunk 端口；如主端口的链路类型改为 Access 端口，则成员端口的链路类型也变为 Access 端口。

所有参加聚合的端口都必须工作在全双工模式下，且工作速率相同才能进行聚合。并且聚合功能需要在链路两端同时配置方能生效。

端口聚合主要应用的场合：

交换机与交换机之间的连接：汇聚层交换机到核心层交换机或核心层交换机之间。

交换机与服务器之间的连接：集群服务器采用多网卡与交换机连接提供集中访问。

交换机与路由器之间的连接：交换机和路由器采用端口聚合解决广域网和局域网连接瓶颈。

服务器和路由器之间的连接：集群服务器采用多网卡与路由器连接提供集中访问

视图：全局配置模式下

命令：

interface range interface_name1 to interface_name2

Switchport mode trunk

channel-group 1 mode on 加入链路组 1 并开启

参数：

interface_name1：聚合起始端口

interface_name2：聚合结束端口。

trunk 表示端口可以转发所有 Vlan 包

将 2 个或多个物理端口组合在一起成为一条逻辑的路径 ，即链路 channel-group，同时也形成了一个逻辑端口 port-channel（一个整体）

switchport mode access 是直接接主机的，所属 VLAN 中的接口，都是 access

switchport mode trunk　trunk mode 的接口可以同时传输多个 VLAN 信息的。

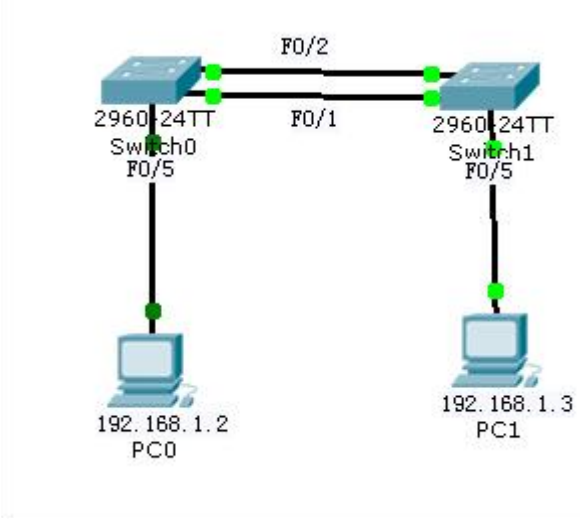
trunk mode 常用在两个 SWITCH　and　ROUTER，switch and switch

特权模式下

Switch#show etherchannel summary：显示相关汇聚端口组的信息；

实验设备

Switch_2960 2 台；PC 4 台；直连线



Switch0:具体操作

Switch>

Switch#config　t

Switch(config)#interface range f0/1-2

Switch(config-if-range)#Switchport mode trunk　　//设置端口模式为 trunk

Switch(config-if-range)#channel-group 1 mode on　　//加入链路组 1 并开启

Switch(config-if-range)#exit

Switch(config)#port-channel load-balance dst-ip　//按照目标主机 IP 地址数据分发来实现负载平衡

Switch(config)#exit

Switch#show etherchannel summary

Switch1:具体操作

Switch>

Switch#config　t

Switch(config)#interface range f0/1-2

Switch(config-if-range)#Switchport mode trunk　　//设置端口模式为 trunk

Switch(config-if-range)#channel-group 1 mode on　　//加入链路组 1 并开启

Switch(config-if-range)#exit

Switch(config)#port-channel load-balance dst-ip　//按照目标主机 IP 地址数据分发来实现以太网通道组负载平衡

Switch(config)#exit

Switch#show etherchannel summary　//显示以太网通道组的情况

PC0 设置

192.168.1.2

255.255.255.0

PC1 设置

192.168.1.3

255.255.255.0

PC0 ping PC1　　Reply

PC1 ping PC0　　Reply

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

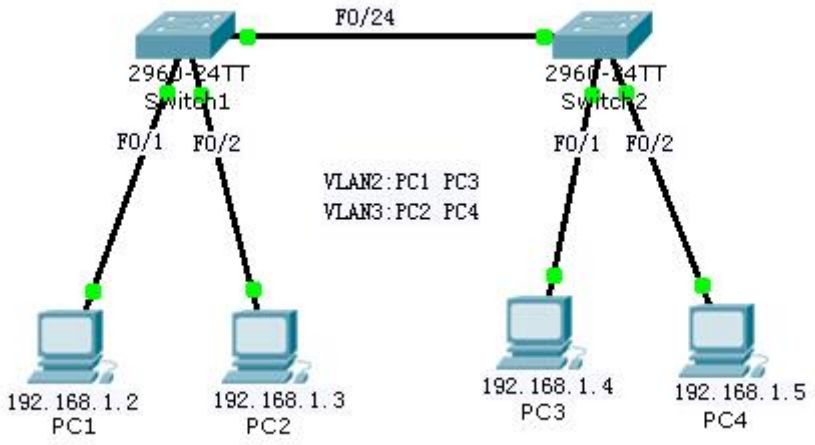
- VLAN 是指在一个物理网段内。进行逻辑的划分，划分成若干个虚拟局域网，VLAN 做大的特性是不受物理位置的限制，可以进行灵活的划分。VLAN 具备了一个物理网段所具备的特性。相同 VLAN 内的主机可以相互直接通信，不同 VLAN 间的主机之间互相访问必须经路由设备进行转发，广播数据包只可以在本 VLAN 内进行广播，不能传输到其他 VLAN 中。

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 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

```
Switch>en
Switch#conf  t
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#inter fa 0/1
Switch(config-if)#switch access vlan 2
Switch(config-if)#exit
Switch(config)#inter fa 0/2
Switch(config-if)#switch access vlan 3
Switch(config-if)#exit
Switch(config)#inter fa 0/24
Switch(config-if)#switch mode trunk
```

Switch(config-if)#end
Switch#show vlan

Switch2
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#int fa 0/1
Switch(config-if)#switch access vlan 2
Switch(config-if)#exit
Switch(config)#int fa 0/2
Switch(config-if)#switch access vlan 3
Switch(config-if)#exit
Switch(config)#int fa 0/24
Switch(config-if)#switch mode trunk
Switch(config-if)#end
Switch#show vlan

PC1 ping PC2 timeout
PC1 ping PC3 Reply

第二次实验

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 口上。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；如果端口没有接线，IP 地址也不会被激活。
- （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。
- 

-  配置线

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（不需做）

图形化：界面开启 FastEthernet0/0 端口

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

PC 终端

Router>en

Router #conf t

Router (config)#hostname R1

R1(config)#enable secret 123456 //设置特权模式密码

R1(config)#exit

R1#exit

R1>en

password:此时输入密码，输入的密码不显示

R1#conf t

R1(config)#line vty 0 4 //设置 telnet 远程登录密码

R1(config-line)#password 123

R1(config-line)#login

R1(config-line)#exit

R1(config)#interface fa 0/0 //进入路由器 0 模块第 0 端口

R1(config-if)#ip address 192.168.1.1 255.255.255.0 //该端口配置相应的 IP 地址和子网掩码

R1(config-if)#no shut //开启端口

R1(config-if)#end

PC CMD

Ipconfig /all　//查看本机 TCP/IP 配置情况（IP 地址、子网掩码、网关、MAC 地址）

ping 192.168.1.1

telnet 192.168.1.1　//远程登录到路由器上

password: 123　//输入 telnet 密码

en

password:123456　//输入特权模式密码

show running　//显示路由器当前配置情况

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的交换机的端口 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。

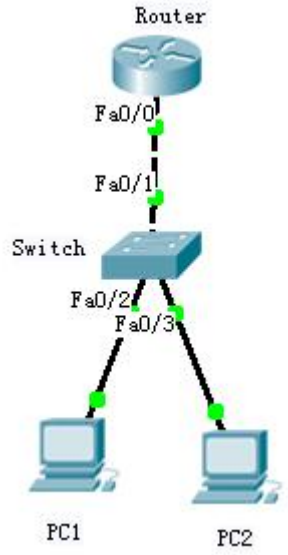
配置子接口，开启路由器物理接口。

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



PC1

IP: 192.168.1.2

Submask: 255.255.255.0

Gageway:192.168.1.1

PC2

IP: 192.168.2.2

Submask: 255.255.255.0

Gageway:192.168.2.1

PC1 Ping PC2

Ping 192.168.2.2 timeout

Switch

```
en
conf t
vlan 2
exit
vlan 3
exit
interface fastEthernet 0/2  //进入交换机 0 模块第 2 端口
switchport access vlan 2  //加入 vlan 2
exit
int fa 0/3  //进入交换机 0 模块第 3 端口
switchport access vlan 3  //加入 vlan 3
exit
int fa 0/1  //进入交换机 0 模块第 1 端口
switchport mode trunk  //设置端口的工作模式为 trunk
```

Router

```
Router>en
```

Router#conf t
int fa 0/0　//进入路由器 0 模块第 0 端口
no shutdown　//开启该端口
exit
interface fast 0/0.1　//进入路由器 0 模块第 0 端口第 1 子接口
encapsulation dot1Q 2　//封装协议设置为 dot1q 允许通过的 vlan 为 2
ip address 192.168.1.1 255.255.255.0　//该子接口配置 IP 地址为 192.168.1.1
exit
int fa 0/0.2　　//进入路由器 0 模块第 0 端口第 2 子接口
encapsulation dot1q 3 //封装协议设置为 dot1q 允许通过的 vlan 为 3
ip address 192.168.2.1 255.255.255.0 //该子接口配置 IP 地址为 192.168.2.1
end

show ip route

PC1 Ping PC2
Ping 192.168.2.2　　reply

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。静态路由的一个缺点就是不能自动适应网络拓扑的变化
- 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。
- 配置静态路由的一般步骤
- 为路由器每个接口配置 IP 地址，确定本路由器有哪些直连网段
- 确定网络中有哪些网段属于本路由器的非直连网段
- 添加本路由器的非直连网段的相关路由信息

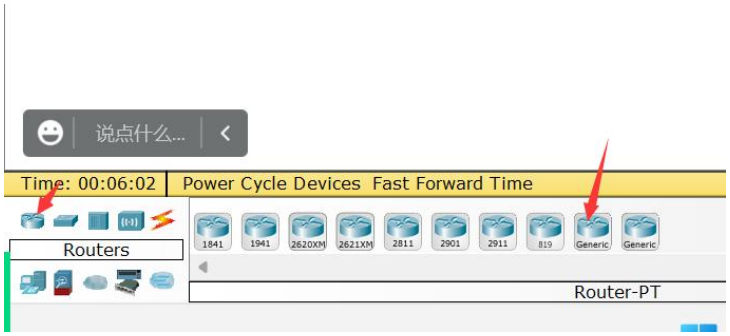
实验步骤

- 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

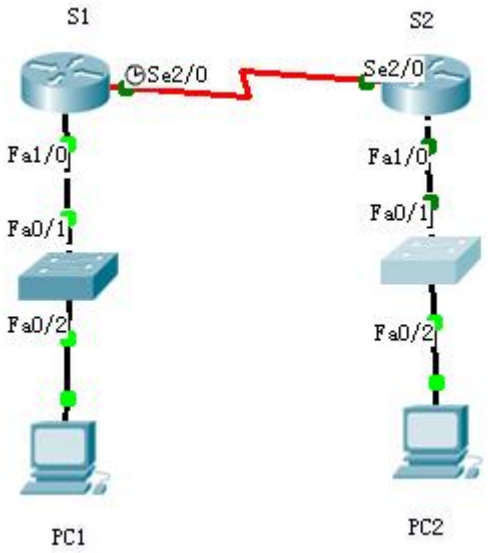
pc 2 台；Router-PT 可扩展路由 2 台；Switch_2960 2 台；DCE 串口线；直连线；交叉线

其中 Route-PT 可扩展路由在这里：



//电脑和交换机，路由器，集线器这些设备连的时候用直连

//电脑之间，路由器之间用交叉连



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

PC1 ping PC2

Ping 192.168.2.2 timeout

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

ip address 192.168.3.1 255.255.255.0

clock rate 64000（必须配置时钟才可通信）//使用串行线必须设置时钟，而且只要链路的一端设置，另一端不必设置。

no shut

end

R2

en

conf t

hostname R2

int fa 1/0

ip address 192.168.2.1 255.255.255.0

no shut

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 // 192.168.2.0 是要到达的目标网络，255.255.255.0 为目标网络对应的子网掩码，192.168.3.2 为与本路由器直接相连的下一跳路由器的接口地址。在静态路由中，只需要指出下一跳的地址，至于以后如何指向，那是下一跳路由器考虑的事情。

end

show ip route

R2

en

conf t
ip route 192.168.1.0 255.255.255.0 192.168.3.1//增加一条静态路由
end
show ip route　　//显示路由表

PC1 Ping PC2
Ping 192.168.2.2　　reply

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；跳计数 16 则表示目标不可达。
- **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。
- RIP 是一个距离矢量的路由协议，它是定期的更新，默认时间是 30S，也就是说如果刚刚发送过更新，即使网络拓扑发生了变化，路由器也不进行更新，要等待下一个更新周期才发送更新。
- 配置动态路由的一般步骤
- 为路由器每个接口配置 IP 地址，确定本路由器有哪些直连网段
- 添加本路由器的直连网段，根据使用的不同动态路由协议，配置相关信息
- (config-router)#default-information originate 在 RIP 域内发布缺省路由
  (config)#ip route 0.0.0.0 0.0.0.0 172.31.16.4 创建一条静态路由
  (config-router)#no auto-summary 在类路由边界关闭自动汇总功能

实验步骤

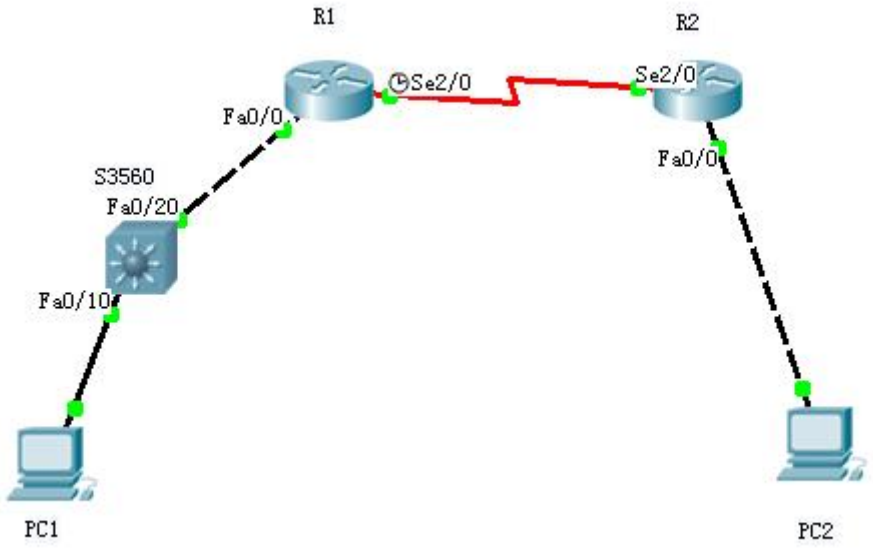
- 建立建立 packet tracer 拓扑图
- （1）在本实验中的三层交换机上划分 VLAN10 和 VLAN20，其中 VLAN10 用于连接校园网主机，VLAN20 用于连接 R1。
- （2）路由器之间通过 V.35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000。
- （3）主机和交换机通过直连线，主机与路由器通过交叉线连接。
- （4）在 S3560 上配置 RIPV2 路由协议。
- （5）在路由器 R1、R2 上配置 RIPV2 路由协议。

- （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 主机之间可以互相通信；

-

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 vlan 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 running

conf t
ip routing     //启动路由功能
router rip     //启动 RIP 路由
network 192.168.1.0     //加入主类网络，能通过 vlan10 的
network 192.168.3.0     //加入主类网络，能通过 vlan20 的
version 2   //配置 RIP 版本是 2，RIP 协议默认运行的是版本 1
end
show ip route   //显示路由
```

C 即直连路由
R 通过 RIP 学来的路由
S 静态路由

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
ip address 192.168.4.1 255.255.255.0
clock rate 64000
end
show ip route

conf t
router rip      //进入 RIP 路由协议配置模式
network 192.168.3.0 //加入端口 f0/0 的主类网络
network 192.168.4.0    //加入串口 S2/0 的主类网络
version 2    //配置 RIP 版本 2，RIP 协议默认运行的是版本 1
exit
```

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 rip
network 192.168.2.0
netword 192.168.4.0
version 2
end
show ip route
```

PC1 Ping PC2

Ping 192.168.2.2　　reply

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。
- 配置动态路由的一般步骤
- 为路由器每个接口配置 IP 地址，确定本路由器有哪些直连网段
- 添加本路由器的直连网段，根据使用的不同动态路由协议，配置相关信息
- 路由算法使用了许多不同的度量标准去决定最佳路径。
- 直连路由是由链路层协议发现的，一般指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，只要该接口处于激活状态，路由器就会把通向该网段的路由信息填写到路由表中去
- 静态路由是手工配置的路由。在静态路由中，只需要指出下一跳的地址，至于以后如何指向，那是下一跳路由器考虑的事情
- 默认路由规定了所有未知数据包发往何处，一个路由器不知道数据包所需要的路由，就发送到它自己的默认路由，并且这个过程一直持续直至到达目的网络，ip route 0.0.0.0 0.0.0.0 12.1.1.2
- 动态路由是指路由器自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。动态路由的运作机制依赖路由器的两个基本功能：对路由表的维护和路由器之间适时的路由信息交换
- 所有的路由，无论是动态的或是静态的，都赋予一个管辖距离，按照管辖距离来排序，管辖距离最小的那个路由被采用。静态路由的管辖距离也可以手工修改。
- 路由器如何进行路由的选择呢？：子网掩码最长匹配，管辖距离最小优先，度量值最小优先，参考带宽除以实际的链路带宽得出链路花费，把整个路径上的所有花费加起来就得到度量值。

方法	管辖距离
直接连接	0
静态	1
OSPF	110
RIP	120

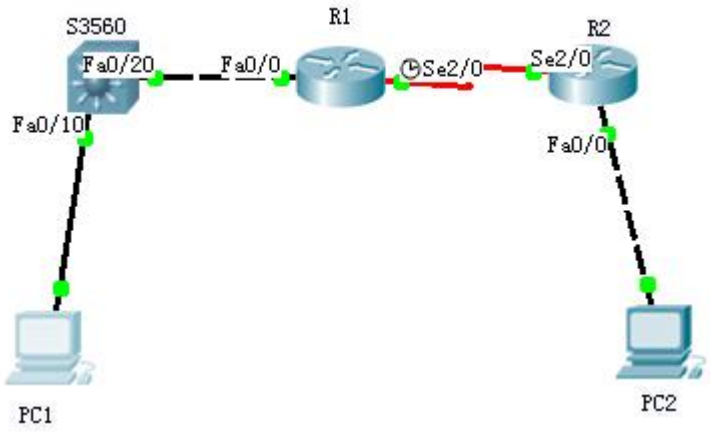
-

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 主机之间可以互相通信；

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
int fa 0/20
switchport access vlan 20
exit
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
将显示结果记录在本子上

conf t
ip routing　//启动路由功能
router ospf 1　//进入 OSPF 协议配置模式，这里 1 是进程号
network 192.168.1.0 0.0.0.255 area 0　//192.168.1.0 表示要加入的直连网络，0.0.0.255 表示的是反向掩码，area 0 表示把该网段放入区域 0，表示单区域的配置，所以路由器的所有网段都加入区域 0
network 192.168.3.0 0.0.0.255 area 0　////192.168.3.0 表示要加入的直连网络，0.0.0.255 表示的是反向掩码，area 0 表示把该网段放入区域 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
no shutdown
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
将显示结果记录在本子上

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

将显示结果记录在本子上

PC1 CMD

PC1 Ping PC2 reply （等一段时间才会出来 reply）

第三次实验

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；

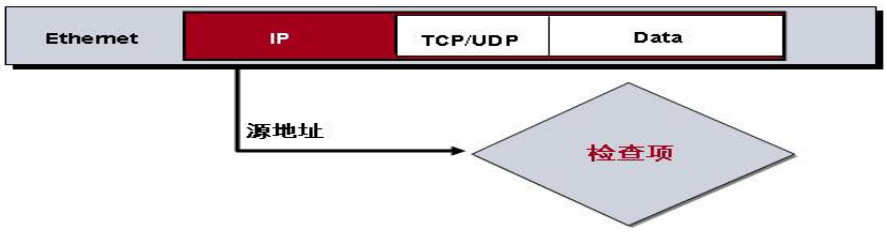
扩展 IP 访问列表可以根据数据包的原 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤；

IP ACL 基于接口进行规则的应用，分为：入栈应用和出栈应用；

- 什么是 ACL
  - ACL 就是访问控制列表，是应用于 IP 地址的允许或禁止规则的集合，对于每一个数据包，路由器顺序执行某个访问控制列表中的语句，如果没有找到与该数据包匹配的语句，则丢弃该数据包。
  - 访问控制列表用号码来表示
- ACL 的作用：拒绝、允许特定的数据流通过网络设备，可以防止攻击，实现访问控制，节省带宽。
- 通配符掩码与源或目标地址一起来分辨匹配的地址范围，告知路由器为了判断是否匹配，需要检查 IP 地址中的多少位。
- 通配符掩码位设成 0 则表示 IP 地址中相对应的位必须精确匹配，通配符掩码中 1 表示忽略位，相对应的位既可以是 1 也可以是 0。
- 192.168.1.0 0.0.0.255，实现的就是匹配从 192.168.1.0-192.168.1.255 的所有 IP 地址。
- Any 匹配任何的 IP 地址
- 用访问控制列表中的通配符掩码和地址执行逻辑或，得出操作结果
- 用访问控制列表中的通配符掩码和数据包中的 IP 地址执行逻辑或，得出结果
- 将两个结果相减，如果相减的结果为 0，则匹配，否则不匹配。
- ACL 的工作机制
  - 由一组访问控制规则组成（ACL 规则）
  - 网络设备根据 ACL 规则检查收到或发送的报文，并采取相应操作
  - ACL 规则匹配顺序：从上至下，当报文匹配某条规则后，将执行操作，跳出匹配过程
  - 任何 ACL 的默认操作是“拒绝所有”

标准访问控制列表

- 编号规则
  - 1~99 和 1300~1399
- 过滤元素
  - 仅源 IP 地址信息



用于简单的访问控制、路由过滤等

创建标准访问控制列表：

access-list *access-list-numbe*r { **permit** | **deny** } { **any** | *source source-wildcard* } [**time-range** *time-range-name*]

把访问控制列表应用于路由器的某个接口入站方向或者出站方向

ip access-group *access-list-number* { **in** | **out** }

- **in** 表示应用到接口的入方向（从端口到路由器），对收到的报文进行检查
- **out** 表示应用到接口的外出方向（从路由器由端口流出），对发送的报文进行检查

配置标准访问控制列表注意事项

- 标准访问控制列表要应用在靠近目标端
- 扩展访问控制列表要应用在靠近源端
- 访问控制列表只对穿越流量起作用
- 放置的顺序
- 隐含的拒绝所有
- 列表的编辑
- 列表的调用

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。

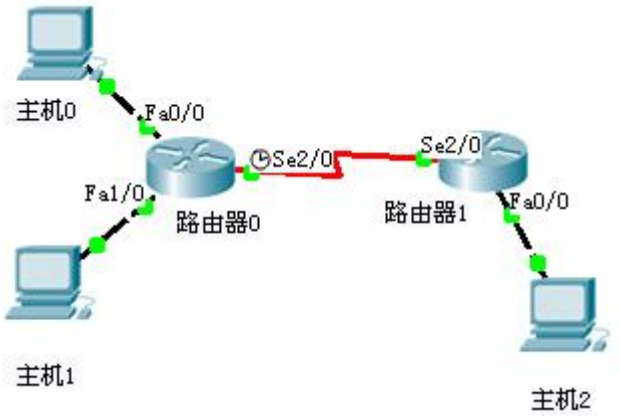
（4）在 R1 上编号的 IP 标准访问控制

（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

clock rate 64000

no shutdown

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 //加入静态路由

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

conf t　　//所有的路由器与交换器 默认的情况下，所有条件都是被否定 deny

Router(config)#access-list 1 permit 172.16.1.0 0.0.0.255　//建立标准访问控制列表编号为1，允许 172.16.1.0 网络通过。因为访问控制列表最后隐含了一条 deny any 的规则，匹配的顺序是从上至下，当条件匹配即执行操作。

Router(config)#access-list 1 deny 172.16.2.0 0.0.0.255　　//拒绝 172.16.2.0 网络通过

Router(config)#int s2/0

Router(config-if)#ip access-group 1 out

Router(config-if)#exit

PC0

ping 172.16.4.2 (success)

PC1

ping 172.16.4.2 (Replay from 172.16.2.1: Destination host unreachable)

CHAP 验证

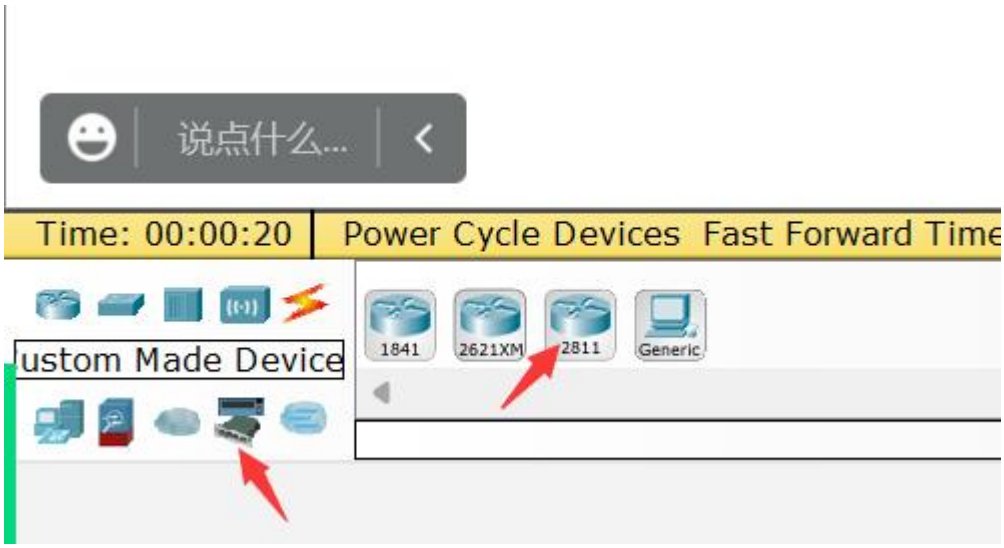
一、实验目的

（一）CHAP 验证配置

（二）CHAP 验证调试

二、实验拓扑

注意：图中的 2811 这台路由器比较特殊，要在下图的这个文件夹中找到



三、实验步骤

（一）配置路由器 R1

```
Router(config)#host R1
R1(config)#username R2 password cisco
R1(config)#int s0/0/0
R1(config-if)#ip addr 172.16.12.1 255.255.255.0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)#no shut
```

（二）配置路由器 R2

```
Router(config)#host R2
R2(config)#username R1 password cisco
R2(config)#int s0/0/0
R2(config-if)#ip addr 172.16.12.2 255.255.255.0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#clock rate 128000
R2(config-if)#no shut
```

四、实验调试

```
R1#debug ppp authentication
R1#debug ppp authentication
PPP authentication debugging is on
```

路由器上配置 DHCP

实验目的

配置 DHCP

背景描述

减轻网管 IP 地址手工配置的负担，实现全公司的计算机 IP 地址的自动分配。

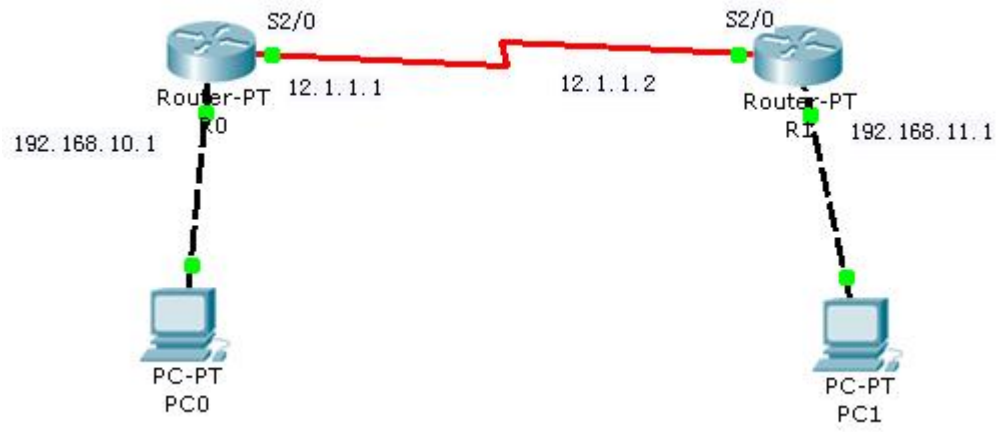
实现功能

自动获取 IP 地址

实验设备

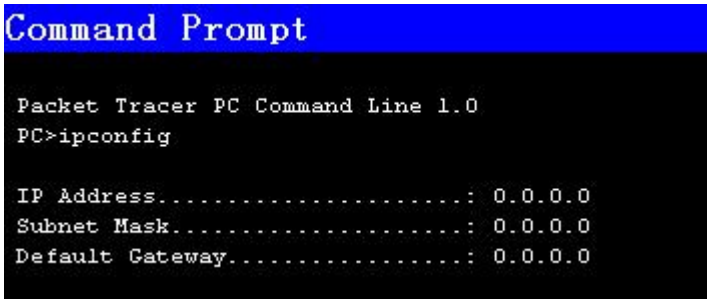
Router-PT 路由器（2 台），PC（2 台）、交叉网线（2 条），串行线 1 条

实验拓扑



PC0、PC1

PC0 与 PC1 的“Gateway/DNS”设置为 DHCP “Gateway/DNS IPv6”设置 DHCP 测试 IP 值：



R1 配置命令如下：

En

config t

host R1

int f0/0

ip address 192.168.10.1 255.255.255.0

no shut

int s2/0

ip address 12.1.1.1 255.255.255.0

clock rate 64000

no shut

exit

ip route 192.168.11.0 255.255.255.0 12.1.1.2

R2 的配置

en

config t
int f0/0
ip address 192.168.11.1 255.255.255.0
no shut
int s2/0
ip address 12.1.1.2 255.255.255.0
no shut
exit
ip route 192.168.10.0 255.255.255.0 12.1.1.1

R1 配置
ip dhcp pool zhulou　//配置主楼 DHCP 地址池
network 192.168.10.0 255.255.255.0　//动态分配 192.168.10.0/24 这个网段内的 IP 地址
dns-server 218.2.135.1　//为主楼计算机配置 DNS 服务器
default-router 192.168.10.1　//为主楼的客户机配置网关
ip dhcp pool fulou　//配置辅楼 DHCP 地址池
network 192.168.11.0 255.255.255.0　//动态分配 192.168.11.0/24 这个网段内的 IP 地址
dns-server 218.2.135.1　//为辅楼计算机配置 DNS 服务器
default-router 192.168.11.1　//为辅楼的客户机配置网关
exit
ip dhcp excluded-address 192.168.10.1　//排除主楼客户机的网关
ip dhcp excluded-address 192.168.11.1　//排除辅楼客户机的网关

R2 配置（配置 DHCP 中继）

int f0/0
ip helper-address 12.1.1.1　//配置辅助寻址，指向 DHCP 服务器的地址，即路由器 R1 的 IP 地址

最后
PC0、PC1
查看 IP 地址，如果有，则成功。

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；

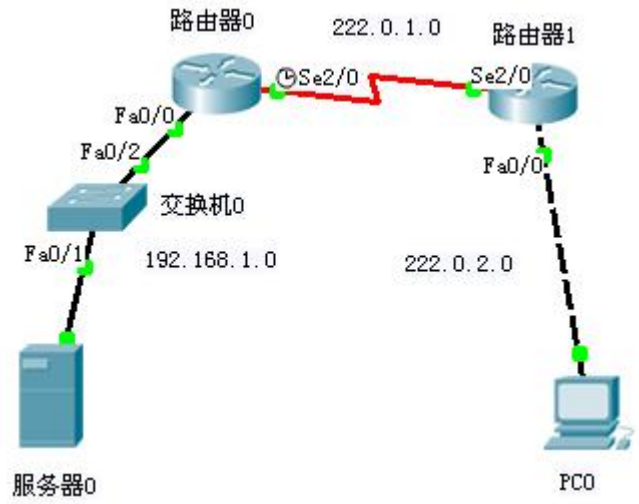
（4）在 R1 上配置静态 NAT。

（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
clock rate 64000
no shutdown

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 //指明这个端口是对内的端口
int s 2/0
ip nat outside //指明这个端口是对外的端口
exit
ip nat inside source static 192.168.1.2 222.0.1.1 //配置端口映射，指明外界对 220.0.1.1 的

访问被静态的转换到内网 192.168.1.2 上。

end

show ip nat translations

将上面显示结果记录在本子上

PC0

Web 浏览器

http://222.0.1.1 (success)

Router0

show ip nat translations

将上面显示结果记录在本子上

无线路由实验

实验目标

理解 WLAN 技术；

掌握无线路由基本配置；

实验背景

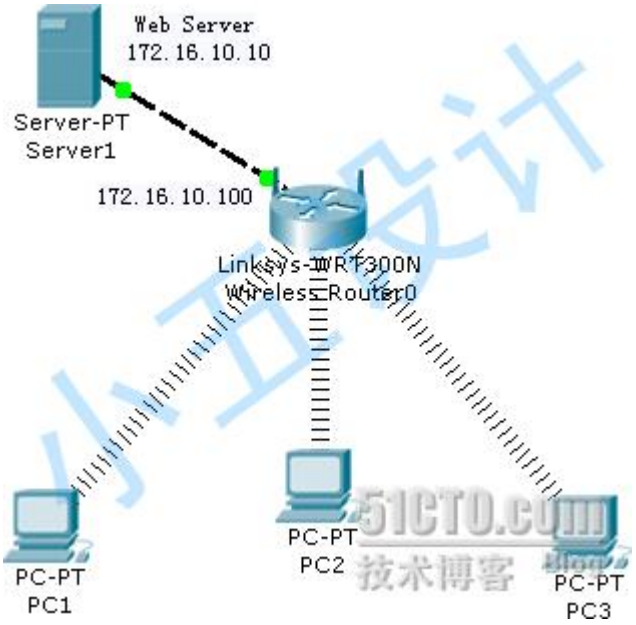
你是某公司的网络管理员，欲以无线网络的方式对公司组网。

实验设备

略

实验步骤

实验拓扑图如下



简要说明：

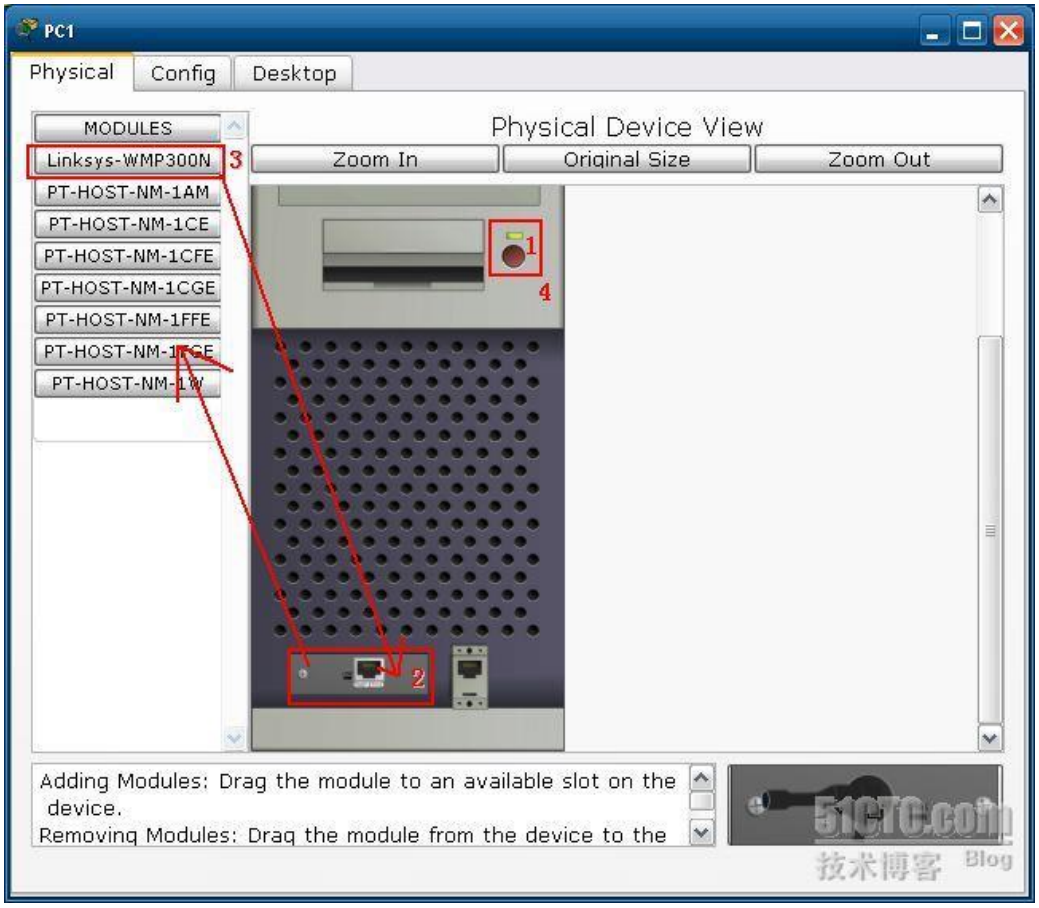
Server 1 是一台服务器，上面运行着 Web 服务

三台 PC 无线连接 Wireless Router0 ，Router0 开启了 DHCP 服务，所以，三台 PC 为动态获取 IP

具体操作步骤：

1、添加一台无线路由

2、添加三台 PC，并去掉其有线网卡，更换为无线网卡



1）关闭电源，点击那个红色按钮

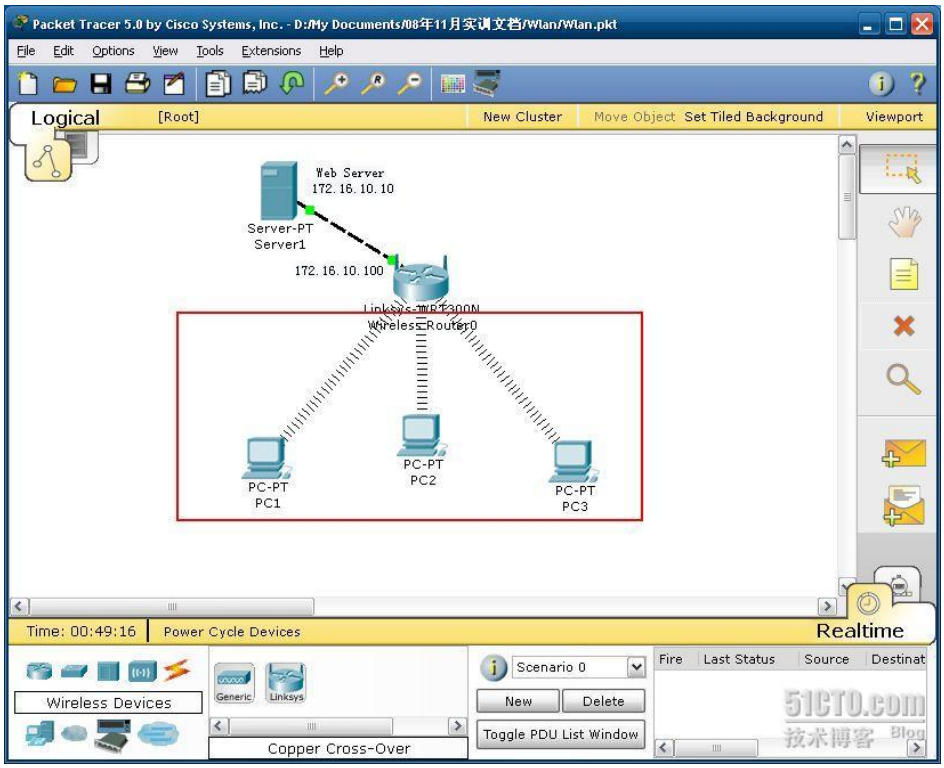
2）将有线网卡拖拽到配件区域

3）将 Linksys-WMP300N 拖拽到有线网卡区

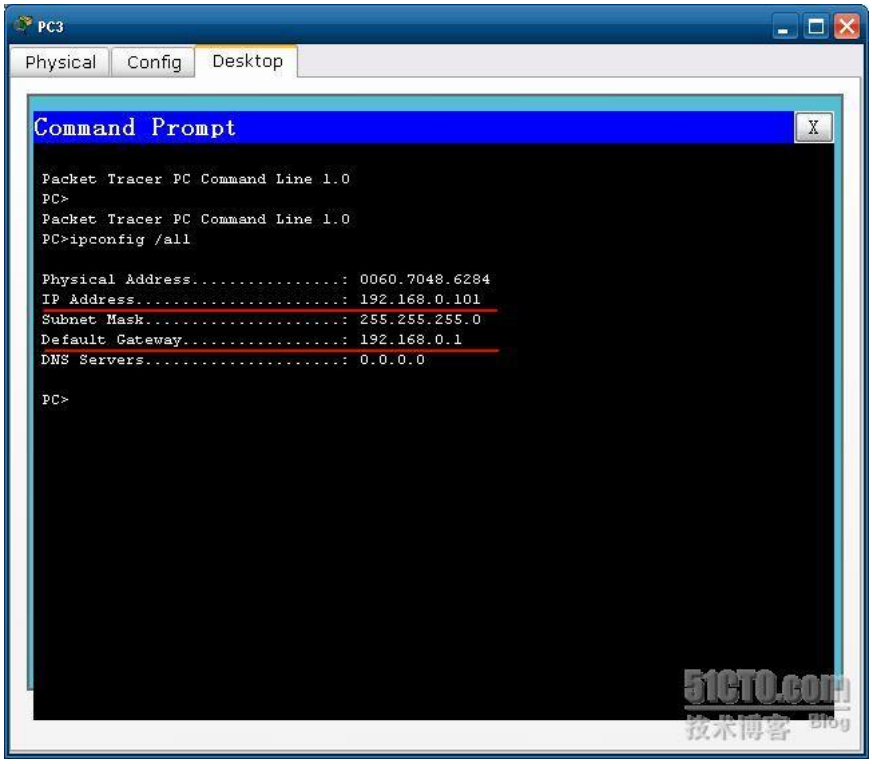
4）重新开启电源

配置好了如下图

三台 PC 都配置好，我们会看到多了很多波线，表示已经连接到了无线路由



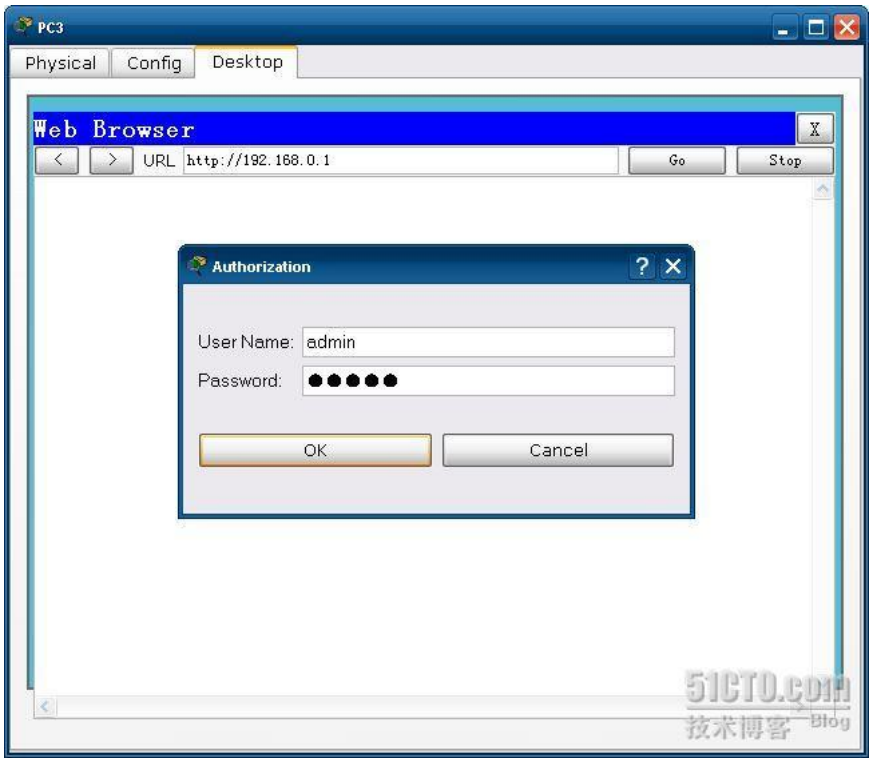
此时我们在任意一台 PC 上执行 IPCONFIG 命令



发现已经自动获取了 IP 地址，证明与无线路由通信正常。

在任意一台 PC 上，打开浏览器 Web Browser

在地址栏中输入 192.168.0.1，弹出的登录窗口中用户名和密码都是 admin



登录后就看到亲切的 Web 管理界面了，现在就可以进行相关配置了