

「计算机网络及应用」实验指导书

参考阅读：教材附录实验 9 - 实验 12

地点：华中科技大学东校区工程实训中心

开机启动：进入 WIN7_x64_2 或者 WIN10_x64_2(不同教室操作系统版本有差异)

Cisco Packet Tracer 版本：5.3.0.0088(不需要登录)

1 Cisco Packet Tracer 使用基础

Packet Tracer 是思科(Cisco)公司针对其网络设备产品开发的一款用于网络设计、配置和故障排除的模拟软件。使用者可以自己选择设备，包括路由器、交换机、集线器、无线 AP、无线宽带路由器、各种线缆、计算机和服务器等，然后完成设备的配置，并进行测试，感觉和真实场景几乎没有差别。

1.1 基本界面

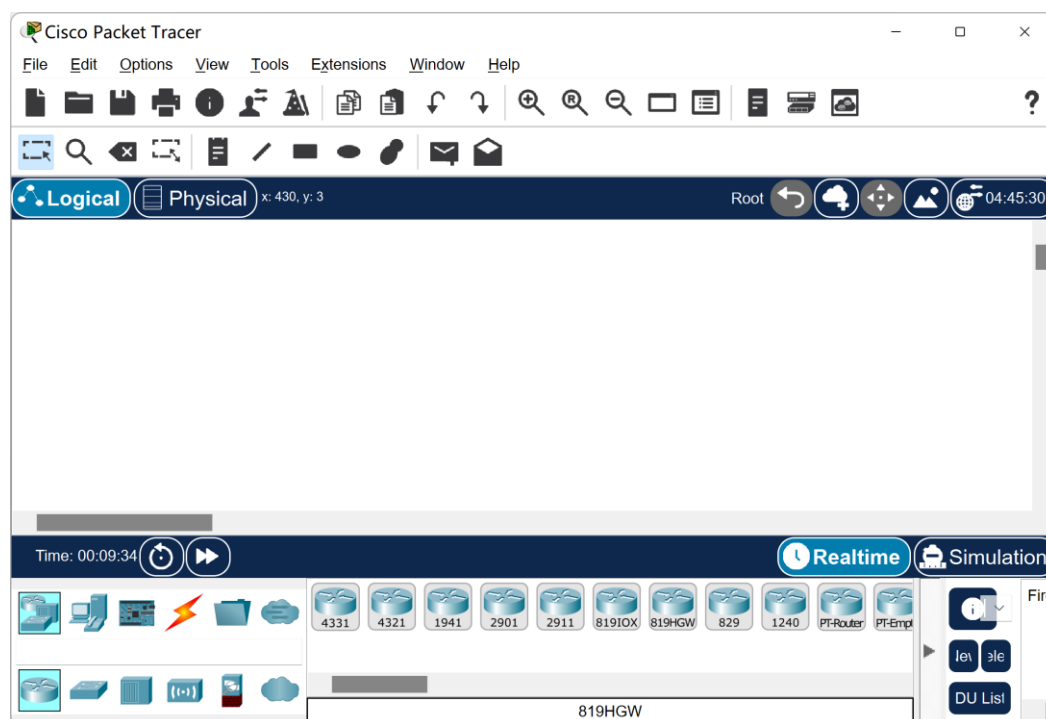


图 1-1 Packet Tracer 8.1.0 主界面

1.2 选择并添加设备

先选择设备类型，再选择网络设备，用鼠标拖到工作区即可。

1.3 连接设备

选取合适的线型将设备链接起来。最简单的方式可以自动选择连接线型。

如果选择双绞线，要注意交换机与路由器之间、交换机与 PC 之间使用直连线（Straight-Through）连接，而两个交换机之间、两个路由器之间以及路由器和 PC 之间要使用交叉线（Cross-Over）连接。

连接完成后，可以看到各线缆两端有不同颜色的三角形，他们表示的含义如表 1-1 所示。

表 1-1 线缆两端状态及含义

链路状态	含义
绿色	物理连接准备就绪
闪烁的绿色	连接激活
红色	物理连接不通，没有信号
黄色	交换机端口处于“阻塞”状态

1.4 实时/模拟导航

默认为**实时模式**，不显示包轨迹。当需要观察包的运动轨迹时，需要切换到**模拟模式**下。此时会出现 Event List 对话框，显示当前捕获到数据包的具体情况。要进一步了解协议的详细情况，可单击协议类型信息，也可以单击具体设备上显示的包，得到 OSI 模型信息和各层 PDU。




可编辑过滤特定协议包，并通过单击上一步、下一步及播放按钮等反复观看，从而更清晰地观察特定协议包的封装及其走向。

图 1-2 中选择**只观察 ICMP 包**。另外，Show All/None 按钮可以帮助更有效地选择协议。

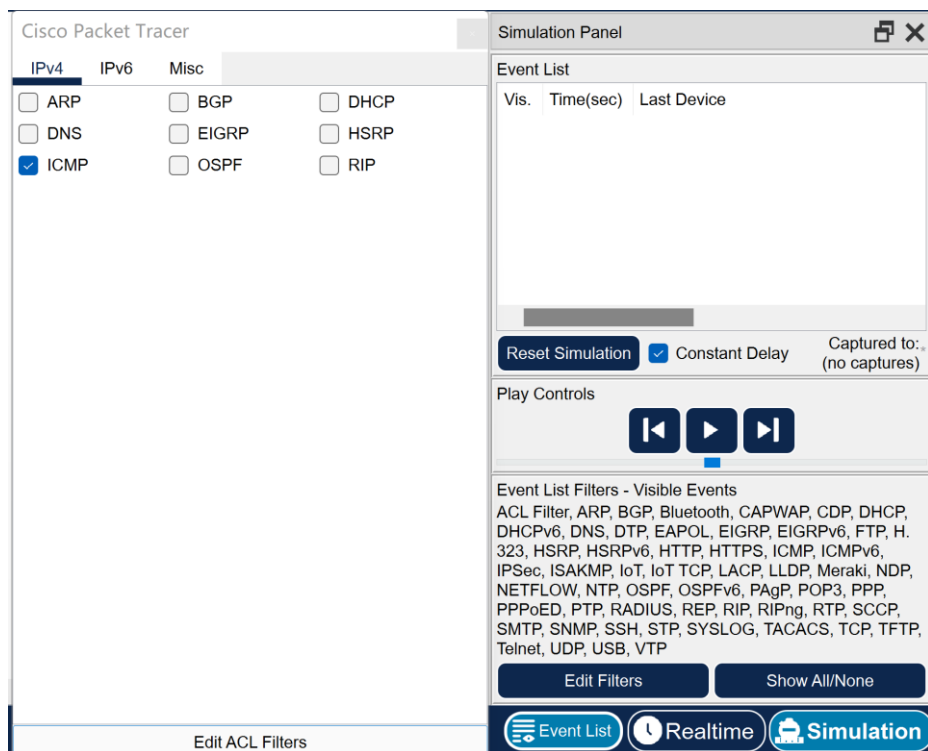


图 1-2 模拟面板

1.5 配置模式

配置交换机或路由器时，首先进入的是用户模式，此时只能查看设备的某些信息。需要进行其他操作时，必须先进入到特权模式，然后再根据需要进入其他模式。以交换机为例，模式之间的切换如图 1-3 所示。

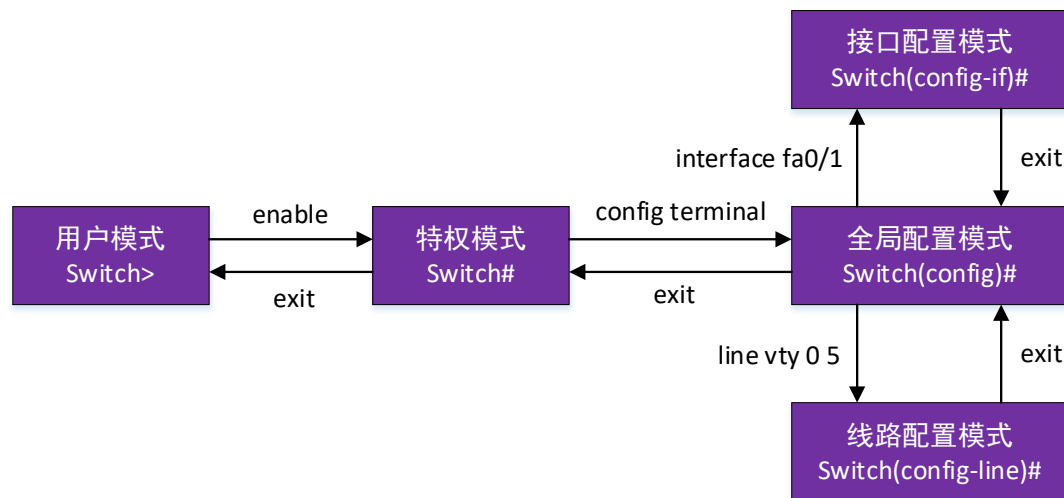


图 1-3 设备配置模式

1. 用户模式

设备启动后按 Enter，首先进入的就是用户模式。在此模式下用户功能受到限制，只能查看一些统计信息。

2. 特权模式

在用户模式下输入 enable（可简写为 en），进入特权模式，用户在此模式下可查看并修改设备配置。

3. 全局配置模式

在特权模式下输入 config terminal（可简写为 conf t），进入全局配置模式，用户在此模式下可修改设备的全局配置，如主机名等。

3a. 接口配置模式

在全局配置模式下输入 interface fastethernet 0/1（可简写为 int f0/1），进入接口配置模式。在此模式下所做的配置都是针对 f0/1 接口进行的，如设定 IP 等。

3b. 线路配置模式

在全局配置模式下输入 line vty 0 5，进入线路配置模式，进行虚通道的配置，如远程登录。

2 交换机 VLAN 实验

2.1 实验目的

- (1) 熟悉 Cisco Packet Tracer 的基本使用。
- (2) 理解交换机的 VLAN，掌握其应用场合。
- (3) 掌握二层交换机 VLAN 的基本配置方法。

2.2 VLAN 基础知识

一个二层交换网络属于一个广播域，广播域也可以理解为一个广播帧所能达到的范围。在网络中存在大量的广播，许多协议及应用通过广播来完成某种功能，如 MAC 地址的查询、ARP 协议等。但过多的广播包在网络中会发生碰撞，使得网络性能下降，甚至造成网络瘫痪。

VLAN 可将一个较大的二层交换网络划分为若干个较小的逻辑网络，每个逻辑网络为一个广播域，且与具体的物理位置没有关系，这使得 VLAN 在局域网中被普遍使用。

VLAN 有如下优点：

- (1) 控制广播域。每个 VLAN 属于一个广播域，通过划分不同的 VLAN，广播被限制在一个 VLAN 内部，有效控制了广播范围。
- (2) 增强网络安全性。对于有敏感数据的用户组可与其他用户通过 VLAN 隔离，减少被广播监听而造成泄密的可能性。
- (3) 组网灵活，便于管理。可以按职能部门、项目组或其他管理逻辑来划分 VLAN，便于部门内部的资源共享。由于 VLAN 只是逻辑上的分组网络，因此可以将不同地理位置上的用户划分到同一 VLAN。

交换机中的每个 VLAN 都被赋予一个 VLAN 号，以区别于其他 VLAN，也可以对每个 VLAN 起个有意义的名字，方便理解。

VLAN 划分的方式有：

- (1) 基于端口的划分。如将交换机端口划分到某个 VLAN，则连接到该端口上的用户即属于该 VLAN。优点是简单、方便，缺点是当该用户离开端口时，需要根据情况重新定义该端口的 VLAN。
- (2) 基于 MAC 地址、网络层协议类型等划分 VLAN。

基于端口的划分方式应用最多，所有支持 VLAN 的交换机都支持这种方式。

交换机及其 VLAN 常用配置命令如表 2-1 所示。

表 2-1 交换机及其 VLAN 常用配置命令

命令格式	含义
vlan vlan-id	创建 VLAN，如 vlan 10
name vlan-name	给 VLAN 命名
int switchport	指定交换机端口，例如：int f0/1
int range switchport	指定交换机一组端口，例如：int range f0/2-5
switchport mode access	将端口定义为 access 模式，应用于端口模式下
switchport access vlan vlan-id	将端口划分到特定 VLAN，应用于端口模式下
show vlan	特权模式下显示 VLAN 及端口信息
do show vlan	配置模式下显示 VLAN 及端口信息
no vlan vlan-id	删除特定 VLAN
show mac ad	查看交换机转发表
clear mac ad	清除交换机转发表

2.3 实验流程

用一台主机去 ping 另一台主机，并在不同情况下观察帧的轨迹，理解碰撞域。实验流程如图 2-1 所示。

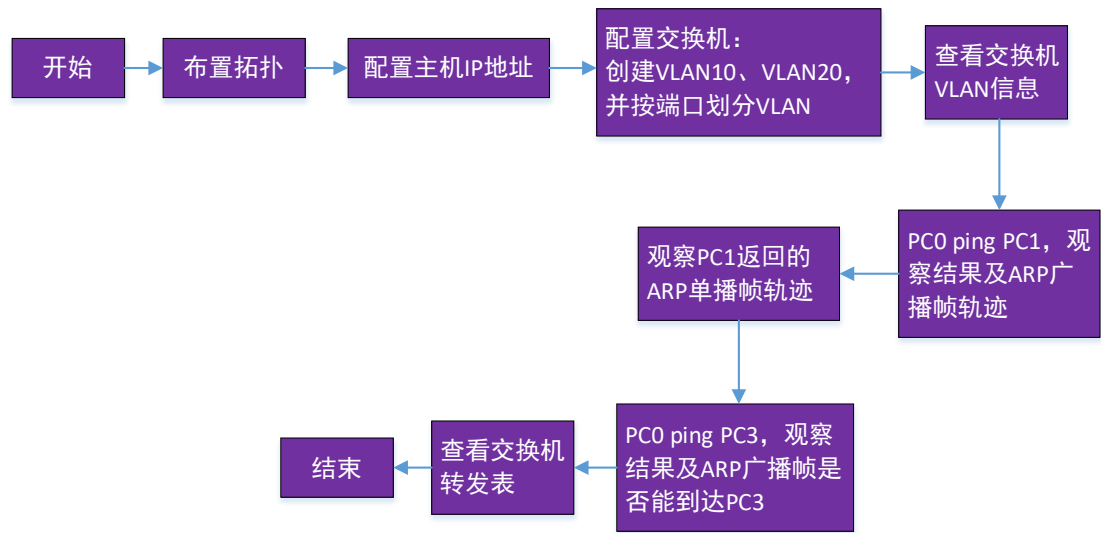


图 2-1 实验流程图

2.4 实验步骤

2.4.1 布置拓扑

实验拓扑如图 2-2 所示，包括 1 台 24 端口二层交换机 2960 和 6 台主机，通过快速网络接口相连，其中 6 台主机的 IP 地址均属于 192.168.1.0/24 网段。

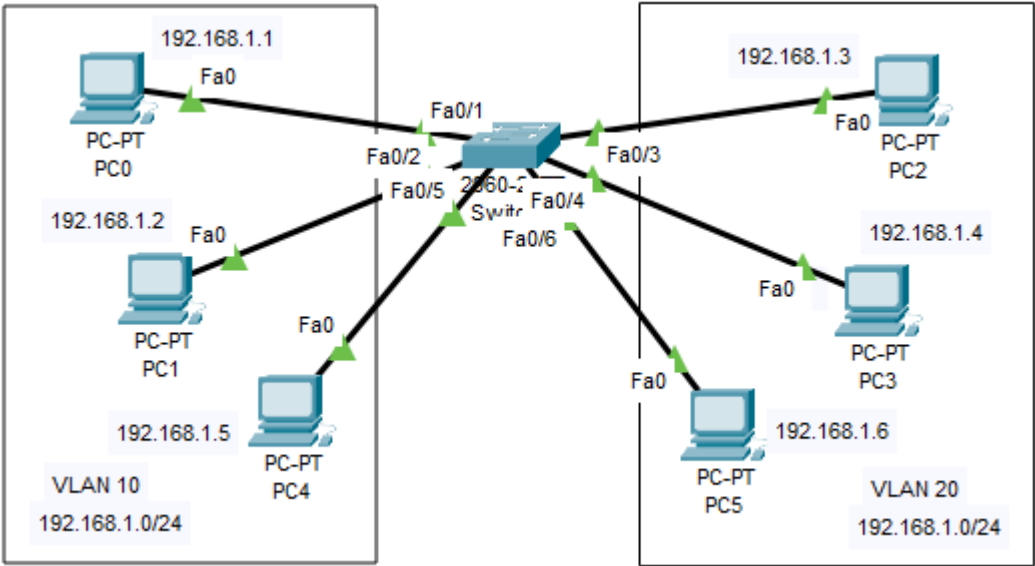


图 2-2 创建 VLAN 10 和 VLAN 20

交换机 VLAN 号、端口分配和各 PC 的 IP 地址如表 2-2 所示。

表 2-2 交换机 VLAN 配置参数

VLAN	交换机端口	PC	PC 端口	IP 地址	掩码
VLAN 10	Fa0/1	PC0	Fa0	192.168.1.1	255.255.255.0
	Fa0/2	PC1	Fa0	192.168.1.2	255.255.255.0
	Fa0/5	PC2	Fa0	192.168.1.5	255.255.255.0
VLAN 20	Fa0/3	PC2	Fa0	192.168.1.3	255.255.255.0
	Fa0/4	PC3	Fa0	192.168.1.4	255.255.255.0
	Fa0/6	PC5	Fa0	192.168.1.6	255.255.255.0

可以通过 Config 或者 Desktop 面板下的 IP Configuration 为每台 PC 的 FastEthernet0 端口按表 2-2 配置好 IP 地址和掩码。

2.4.2 配置交换机

按如下命令在 CLI 中配置交换机 VLAN：

```
Switch>en
Switch#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#vlan 10           // 创建 VLAN 10
```

```
Switch(config)#int range f0/1-2, f0/5    // 将端口 f0/1、f0/2 和 f0/5 划入 VLAN 10
```

```
Switch(config-if-range)#switchport access vlan 10
```

```
Switch(config)#int range f0/3-4, f0/6    // 将端口 f0/3、f0/4 和 f0/6 划入 VLAN 20
```

```
Switch(config-if-range)#switchport access vlan 20    // VLAN 20 不存在，自动创建
```

注：以上所有 VLAN 配置也可以通过图形界面 Config 进行操作。

查看交换机 VLAN 信息：

```
Switch(config)#do show vlan
```

VLAN Name		Status	Ports

1	default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	VLAN0010	active	Fa0/1, Fa0/2, Fa0/5
20	VLAN0020	active	Fa0/3, Fa0/4, Fa0/6
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

可以发现，默认情况下所有端口均属于 VLAN 1。

2.4.3 同一 VLAN 广播帧

在模拟模式下，从 PC0 ping PC1，选择只观察 ARP 和 ICMP 分组。其中第一个 ARP 分组是广播帧，这里我们暂时只关注其广播属性。由于该包从 Fa0/1 端口进入，属于 VLAN 10，因此它将在 VLAN 10 中广播。观察 VLAN 10 的广播域，显然，只有 PC1、PC4 可以收到这个帧，其中 PC4 丢弃该帧。不属于 VLAN 10 的主机将收不到该广播帧。

注意观察 PC0 处封装的 ARP 广播帧，其目的地址为广播地址（全 1），如图 2-3 所示。

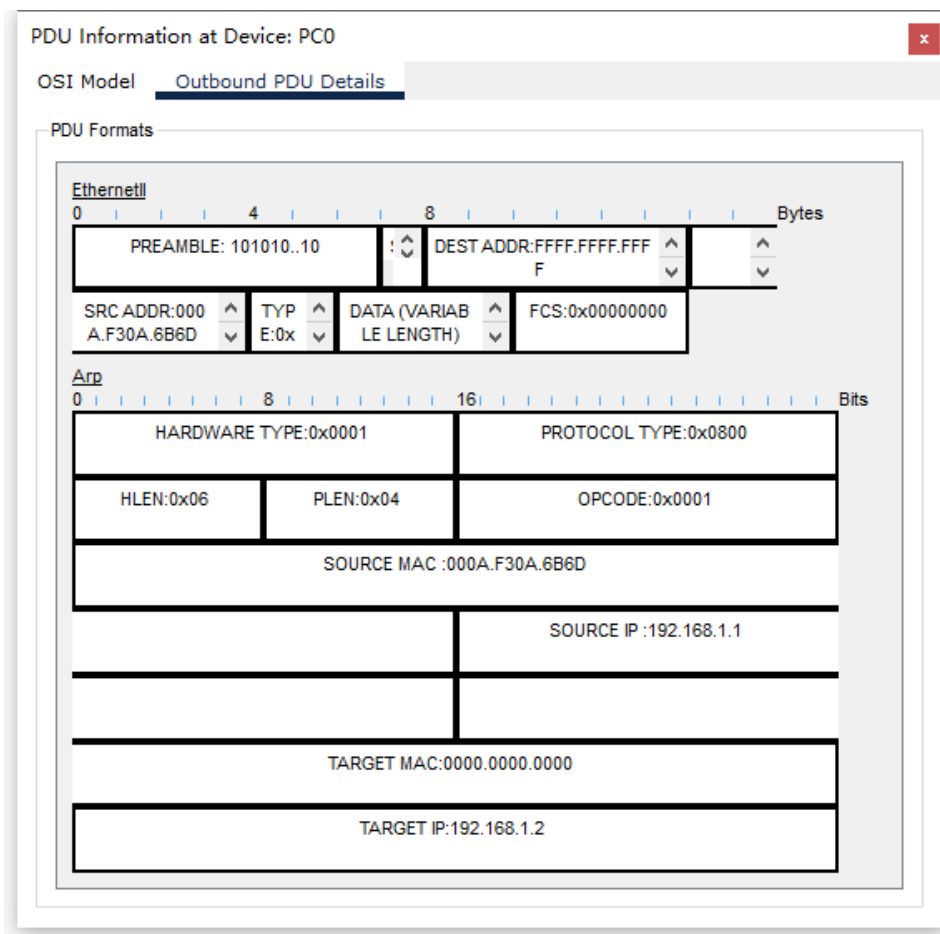


图 2-3 PC0 封装的广播帧

注：除了第一次模拟，如果要观察 ARP 帧，需要清除 PC 上的 ARP 缓存（可以思考下为什么？）：

`arp -d`

可通过 `arp -a` 命令查看 PC 上的 ARP 缓存。

ping 命令结束后，查看交换机 MAC 地址表，注意地址表中 MAC 地址前都有 VLAN 标识，目前转发表中没有 VLAN 20 的记录。

```
Switch#show mac-address-table
```

```
Mac Address Table
```

```
-----
```

```
Vlan Mac Address Type Ports
```

```
-----
```

```
10 000a.f30a.6b6d DYNAMIC Fa0/1
10 00e0.8f29.c530 DYNAMIC Fa0/2
```

可使用 `clear mac-address-table dynamic` 清除动态 MAC 地址列表。

2.4.4 同一 VLAN 单播帧

ARP 广播帧到达 PC1 后，PC1 会向 PC0 回复一个单播帧，根据交换机的交换表自学习算法，PC0 的 MAC 地址会被交换机学习到，所以单播帧将被直接转发到 PC0，而不会向其他端口转发。当然，若转发表中没有该地址，则会在 VLAN 10 中广播该帧。

需要注意的是，前面自学习算法没有提到 VLAN，而转发表是基于 VLAN 的，因为转发表的建立需要用到广播功能，而广播只能在同一 VLAN 内部进行。当交换机的 Fa0/2（该端口属于 VLAN 10）收到该 ARP 回复帧后，接下来只会查询 VLAN 10 的交换表，而不会查询 VLAN 20 的交换表。

实际上，属于哪个 VLAN 是交换机的事情，对于主机来说，对此毫不知情。主机端封装的帧在进入交换机端口时才被打上 VLAN 标识，而在离开端口时会删掉 VLAN 标识，再交给主机。

2.4.5 不同 VLAN 单播帧

从 PC0 ping PC3，此时 2 台 PC 属于不同的 VLAN，交换机从 Fa0/1 端口收到 ARP 广播帧后，会在 VLAN 10 中广播，PC1 和 PC4 收到广播帧后均被丢弃，而 PC3 则收不到该广播帧，说明该单播帧局限于 VLAN 10 之内。

查看交换机转发表，注意转发表中 MAC 地址前都有 VLAN 标识，目前转发表中没有 VLAN 20 的记录。

```
Switch#show mac ad
Mac Address Table
-----

VLAN Mac Address Type Ports
-----
10 000a.f30a.6b6d DYNAMIC Fa0/1
10 00e0.8f29.c530 DYNAMIC Fa0/2
```

2.5 实验报告要求

实验报告应包括如下内容：

[实验名称]

交换机 VLAN 实验。

[实验过程]

按照 2.4 进行实验，记录实验结果，并描述实验过程中遇到的问题以及解决问题的过程。

1、实验结果：

要求使用 ping 命令观察主机之间的连通情况：

- a. 未划分 VLAN 时 6 台主机的连通情况；
- b. 划分 VLAN 后，同一 VLAN 内部主机的连通情况；
- c. 划分 VLAN 后，不同 VLAN 之间主机的连通情况。

2、问题及解决过程：

[回答问题]

- 1、PC0 能否 ping 通 PC2、PC3、PC4、PC5？为什么？
- 2、使用二层交换机连接的网络需要配置网关吗？为什么？

[实验小结]

通过实验，可以得出关于 VLAN 的哪些结论？

[实验心得]

解决问题过程中自己的收获。

3 静态路由与默认路由配置

3.1 实验目的

掌握基本的路由器配置命令，并配置静态路由和默认路由。

3.2 基础知识

静态路由是指路由信息由管理员手工配置，而不是路由器通过路由算法和其他路由器学习得到。所以，静态路由主要适合网络规模不大、拓扑结构相对固定的网络使用。当网络环境比较复杂时，由于其拓扑或链路状态相对容易变化，就需要管理员再手工改变路由，工作既繁琐又频受人工干预，此时使用静态路由就不合适了。

默认路由也是一种静态路由，它位于路由表的最后，当数据报与路由表中前面的表项都不匹配时，数据报将根据默认路由转发。默认路由可以大大简化路由器的项目数量及配置，减轻路由器和网络管理员的工作负担。

静态路由常用配置命令如表 3-1 所示。

表 3-1 静态路由常用配置命令

命令格式	含义
ip route 目的网络号 目的网络子网掩码 下一跳 IP 地址	配置静态路由
no ip route 目的网络号 目的网络子网掩码 下一跳 IP 地址	删除静态路由
ip route 0.0.0.0 0.0.0.0 下一跳 IP 地址	配置默认路由
int f0/0	选择路由器端口
ip add IP 地址 掩码	为路由器端口配置 IP 地址
no sh / sh	激活(no shut down)/关闭(shut down)路由器端口
show ip route	特权模式下查看路由表
do show ip route	配置模式下查看路由表

3.3 实验流程

配置静态路由和默认路由，要求各 IP 全部可达。实验流程如图 3-1 所示。

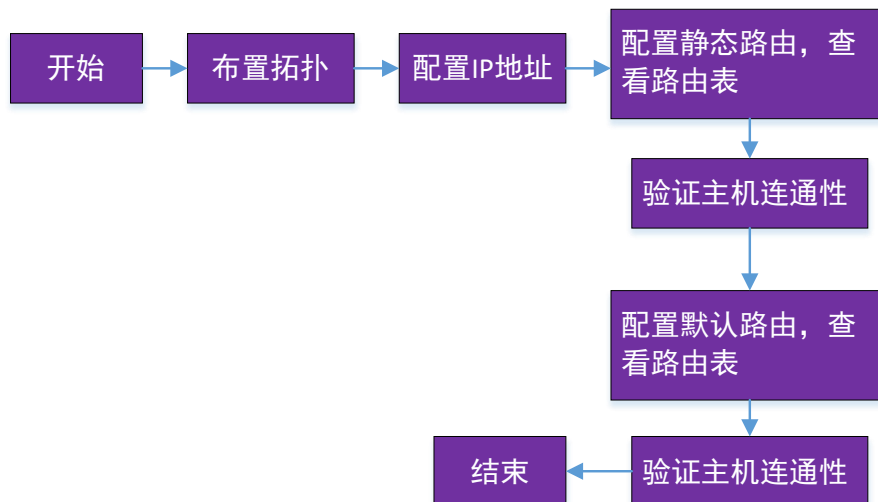


图 3-1 实验流程图

3.4 实验步骤

3.4.1 布置拓扑

实验拓扑如图 3-2 所示，包括 3 台路由器、2 台交换机和 2 台 PC。其中 3 台路由器之间用交叉线相连。

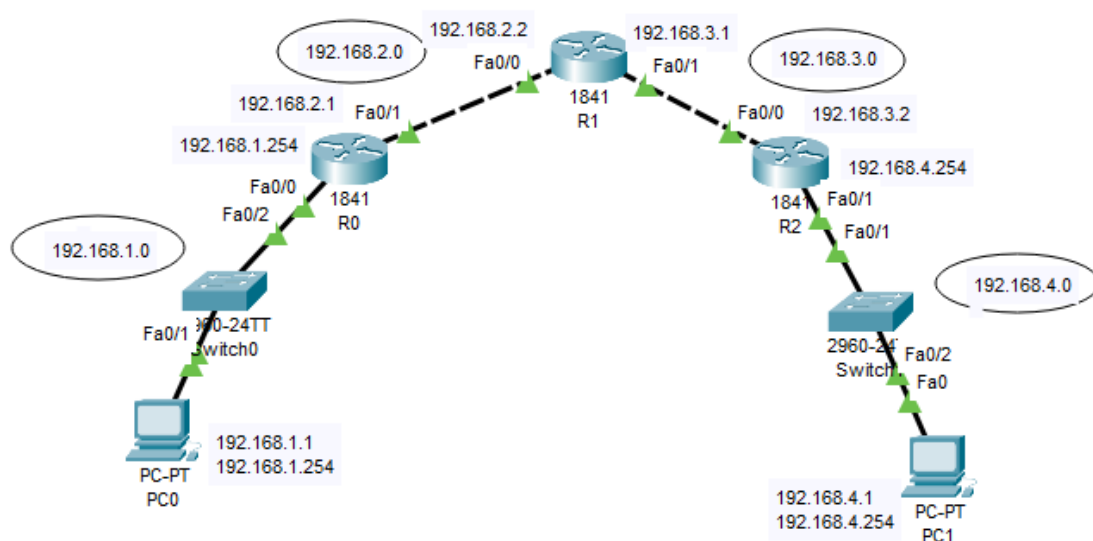


图 3-2 拓扑图

路由器和 PC 的 IP 地址配置见表 3-2。

表 3-2 IP 地址配置

设备名称	端口	IP 地址	默认网关
路由器 R0	Fa0/0	192.168.1.254	
	Fa0/1	192.168.2.1	
路由器 R1	Fa0/0	192.168.2.2	
	Fa0/1	192.168.3.1	
路由器 R2	Fa0/0	192.168.3.2	
	Fa0/1	192.168.4.254	
PC0	Fa0	192.168.1.1	192.168.1.254
PC1	Fa0	192.168.4.1	192.168.4.254

PC 的 IP 地址可通过 Config 或者 Desktop 面板下的 IP Configuration 进行配置，路由器的 IP 地址既可以通过 Config 面板配置，也可以通过命令行接口 CLI 进行配置。

IP 地址配置好以后，如果拓扑图中某段线缆两端为红色，说明该段物理连接不通，请检查线缆两端的路由器或者 PC 机上使用的相应端口是否激活。

可通过命令行接口 CLI 激活路由器端口：

```
Router(config)#int f0/0           // 选择路由器端口
Router(config-if)#no sh           // 激活该端口
Router(config-if)#int f0/1
Router(config-if)#no sh
```

也可以通过图形界面 Config 进行操作。

物理连接准备就绪后，所有链路状态显示为绿色。此时，从 PC0 可以 ping 通路由器 R0 两个端口的 IP(从 PC1 也可以 ping 通路由器 R2 的两个端口的 IP)，但除此之外的其他 IP 地址均不能 ping 通。需要配置所有路由器的路由表之后，不同网络之间才能连通。

3.4.2 配置静态路由

路由器 R0：

R0 有两个直连网络，分别是 192.168.1.0 和 192.168.2.0，这两个网络不需要配置静态路由。R0 不知道的是到 192.168.3.0 和 192.168.4.0 的路由。所以需要在 R0 上配置到这两个网络的路由：

```
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.2.2
```

注：以上静态路由配置也可以通过图形界面 *Config* 进行操作，如图 3-3 所示。可以看到，等效的 *IOS* 命令与上述配置命令是一致的。

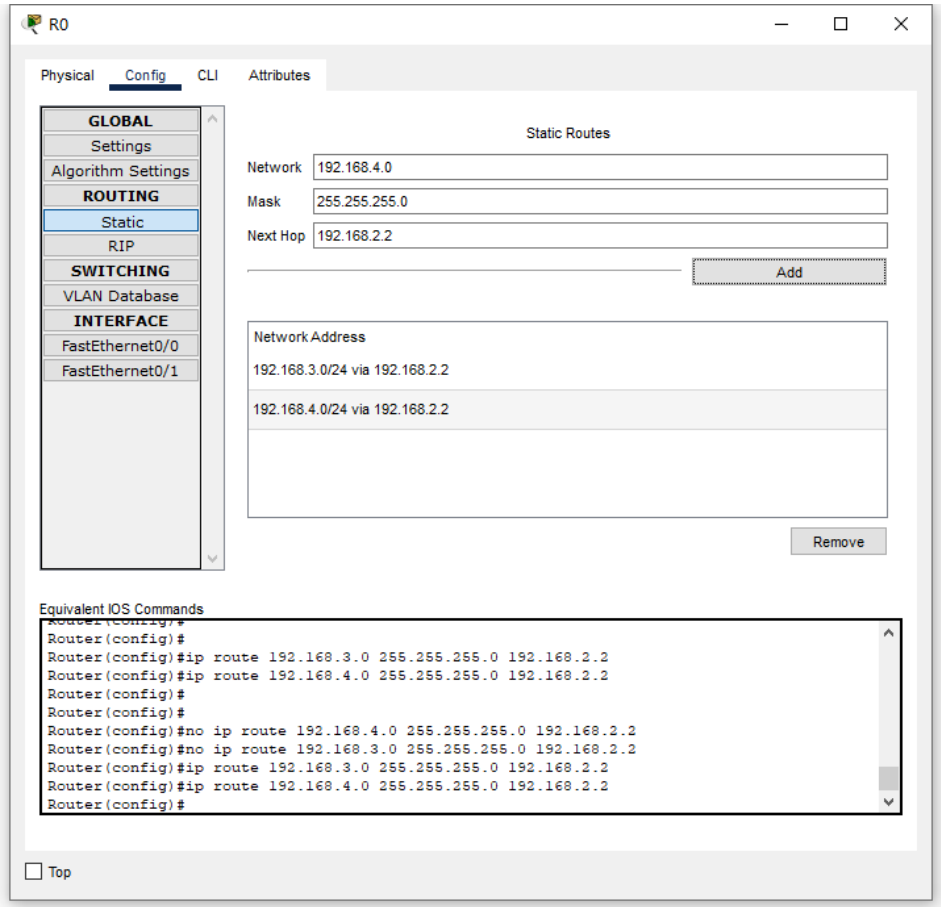


图 3-3 图形界面配置 R0 静态路由

路由器 R1:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1  
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2
```

路由器 R2:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1  
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.1
```

查看路由器的路由表，以 R1 为例，其中 S 开头的为静态路由，C 开头的为直连路由。

```
S 192.168.1.0/24 [1/0] via 192.168.2.1  
C 192.168.2.0/24 is directly connected, FastEthernet0/0  
C 192.168.3.0/24 is directly connected, FastEthernet0/1
```

```
S 192.168.4.0/24 [1/0] via 192.168.3.2
```

验证网络的连通情况：

静态路由配置好后，可以从 PC1 ping PC0 检查网络的连通情况：如果能够 ping 通，说明 IP 地址、网关以及静态路由配置正确；否则，检查出错误，直到 ping 通为止。

3.4.3 配置默认路由

对于路由器 R0 来说，两个直连网络 192.168.1.0 和 192.168.2.0 不需要配置静态路由，到 192.168.3.0 和 192.168.4.0 两个网络的下一跳都是 192.168.2.2，所以，这两条静态路由可由一条指向 192.168.2.2 的默认路由替代。在前面配置的基础上，删除静态路由，再增加一条默认路由即可。

```
Router(config)#no ip route 192.168.3.0 255.255.255.0 192.168.2.2
Router(config)#no ip route 192.168.4.0 255.255.255.0 192.168.2.2
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

路由器 R2 的默认路由配置与 R0 类似。

```
Router(config)#no ip route 192.168.1.0 255.255.255.0 192.168.3.1
Router(config)#no ip route 192.168.2.0 255.255.255.0 192.168.3.1
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

查看 R0 的路由表，其中，以 S*开头的为默认路由。

```
Gateway of last resort is 192.168.2.2 to network 0.0.0.0

C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.2.2
```

验证网络的连通情况：

与静态路由类似，默认路由配置好后，同样可以从 PC1 ping PC0 检查网络的连通情况，直到 ping 通为止。

3.5 实验报告要求

实验报告应包括如下内容：

[实验名称]

静态路由与默认路由配置。

[实验过程]

按照 3.4 进行实验，记录实验结果，并描述实验过程中遇到的问题以及解决问题的过程。

1、实验结果：

要求使用 ping 命令观察主机 PC1 和 PC0 之间的连通情况：

- a. 配置静态路由时主机的连通情况；
- b. 配置默认路由时主机的连通情况。

2、问题及解决过程：

[回答问题]

- 1、简单讨论 192.168.1.0 和 192.168.1.255 这两个 IP 地址所代表的含义。
- 2、在配置 R0 静态路由时，命令“ip route 192.168.3.0 255.255.255.0 192.168.2.2”中，192.168.3.0 和 192.168.2.2 分别代表什么？能不能用 192.168.3.1 代替 192.168.3.0，用 192.168.2.1 代替 192.168.2.2？请测试并说明原因。
- 3、若 PC 不配置默认网关，PC0 和 PC1 是否能够相互 ping 通？进行测试并解释原因。

[实验小结]

通过实验，可以得出关于静态路由和默认路由的哪些结论？

[实验心得]

解决问题过程中自己的收获。