# 实验八：交换机

# 一、实验内容：

**实验8.1：交换机基本配置**

**实验8.2：交换机端口安全**

**实验8.3：STP生成树协议**

# 二、实验原理

# 1.交换机基本配置

交换机是局域网中最重要的设备，交换机是基于MAC来进行工作的。和路由器类似，交换机也有IOS，IOS的基本使用方法是一样的。本章将简单介绍交换的一些基本配置。关于VLAN和Trunk等将在后面章节介绍。

## 交换机简介

交换机是第2层的设备，可以隔离冲突域。交换机是基于收到的数据帧中的源MAC地址和目的MAC地址来进行工作的。交换机的作用主要有两个：一个是维护CAM（Context Address Memory）表，该表是计算机的MAC地址和交换端口的映射表；另一个是根据CAM来进行数据帧的转发。交换对帧的处理有3种：交换机收到帧后，查询CAM表，如果能查询到目的计算机所在的端口，并且目的计算机所在的端口不是交换接收帧的源端口，交换机将把帧从这一端口转发出去（Forward）；如果该计算机所在的端口和交换机接收帧的源端口是同一端口，交换机将过滤掉该帧（Filter）；如果交换机不能查询到目的计算机所在的端口，交换机将把帧从源端口以外的其他所有端口上发送出去，这称为泛洪（Flood），当交换机接收到的帧是广播帧或多播帧，交换机也会泛洪帧。

# 2.STP生成树协议

为了增加局域网的冗余性，我们常常会在网络中引入冗余链路，然而这样却会引起交换环路。交换环路会带来3个问题：广播风暴、同一帧的多个拷贝以及交换机CAM表不稳定。STP（STP，Spanning Tree Protocol）可以解决这些问题，STP基本思路是阻断一些交换机接口，构建一棵没有环路的转发树。STP利用BPDU（Bridge Protocol Data Unit）和其他交换机进行通信，从而确定哪个交换机该阻断哪个接口。在BPDU中有几个关键的字段，例如：根桥ID、路径代价和端口ID等。

为了在网络中形成一个没有环路的拓扑，网络中的交换机要进行以下几个步骤：①选举根桥，②选取根端口，③选取指定端口，④确定阻塞端口。

每个交换机都具有一个唯一的桥ID，这个ID由两部分组成：网桥优先级+MAC地址。网桥优先级是一个2字节的数，交换机的默认优先级为32768 ；MAC地址就是交换机的MAC地址。具有最低桥ID的交换机就是根桥。根桥上的接口都是指定端口，会转发数据包。

选举了根桥后，其他的交换就成为了非根桥。每台非根桥要选择一个根端口。STP使用路径Cost来决定到达根桥的最佳路径（Cost是累加的，带宽大的链路Cost低），最低Cost值的路径就是根路径，该接口就是根端口；如果Cost一样，就根据端口ID选举根端口。端口ID由优先级和端口号共同组成。如果端口优先级相同，则默认端口号小的作为根端口。根端口转发数据包。交换机然后选择各个网段的指定接口，它到达根桥的代价最小。如果代价相同，根据网桥ID选择小的作为指定端口。指定口是转发数据帧的。剩下的其他的接口将被阻断，不转发数据包。这样网络就构建出一棵没有环路的转发树。

当网络的拓扑发生变化时，网络会从一个状态向另一个状态过渡，重新打开或阻断某些接口。交换机的端口要经过几种状态：禁用（Disable）、阻塞（Blocking）、监听状态（Listening）和学习状态（Learning），最后是转发状态（Forwarding）。

## 实验8.1：交换机基本配置

**1.实验目的:**

通过本实验，可以掌握交换机的基本配置这项技能。

**2.实验拓扑**

实验拓扑图如下图所示。从设备列表中选取一台2960交换机。



实验1拓扑图

**3.实验步骤**

**（1）步骤1：接口基本配置**

默认时，交换机的以太网接口是开启的，对于交换机的以太网口可以配置其双工模式和速率等。

Switch>enable

Switch#configure terminal

Switch(config)# interface f0/1

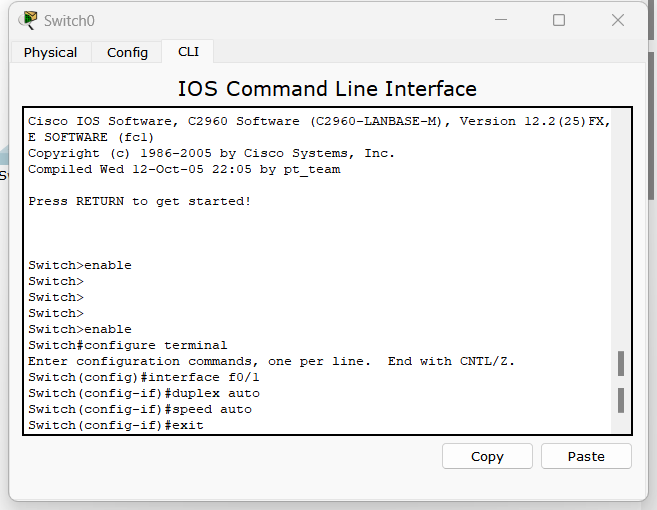
Switch(config-if)#duplex auto

//duplex来用配置接口的双工模式,参数包括：full——全双工；half——半双工；auto——自动检测双工的模式

Switch (config-if)#speed auto

//speed命令用来配置交换机的接口速度，,参数包括:10——10Mbps；100——100 Mbps；1000——1000 Mbps；auto——自动检测接口速度

Switch(config-if)#exit



**（2）步骤2：配置管理地址**

交换机也允许在网络中被通过Telnet、SSH等形式远程访问，这时需要在交换机上配置一个IP地址和默认网关，这个地址是在Vlan接口上配置的,如下：

Switch (config)#interface vlan 1

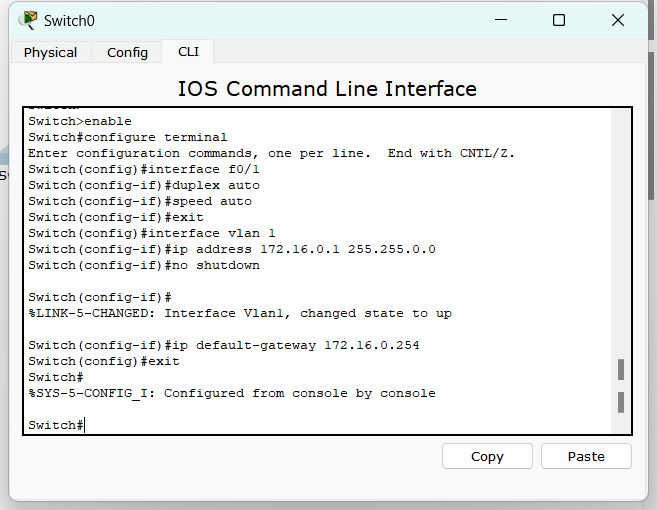
Switch (config-if)#ip address 172.16.0.1 255.255.0.0

Switch (config-if)#no shutdown

Switch (config)#ip default-gateway 172.16.0.254

Switch (config)#exit

//以上在VLAN1接口上配置了管理地址，为了其他网段的用户通过Telnet、SSH等形式访问交换机，在交换机上配置了默认网关。



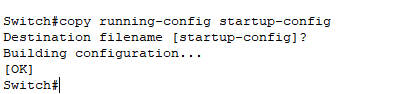
**（3）步骤3: 保存配置**

Switch #copy running-config startup-config

Destination filename[startup-config]? 回车

Building configuration...

［OK］



## 实验8.2：交换机端口安全

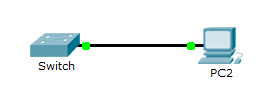
**1.实验目的**

通过本实验，可以掌握如下技能：

1. 理解交换机表的作用；
2. 理解交换机的端口安全；
3. 配置交换的端口安全特性。

**2.实验拓扑**

实验拓扑图如下图所示。从设备列表中自行选择一台主机、一台交换机，使用直通线将二者连接。假设交换机的连接端口为f0/1接口。



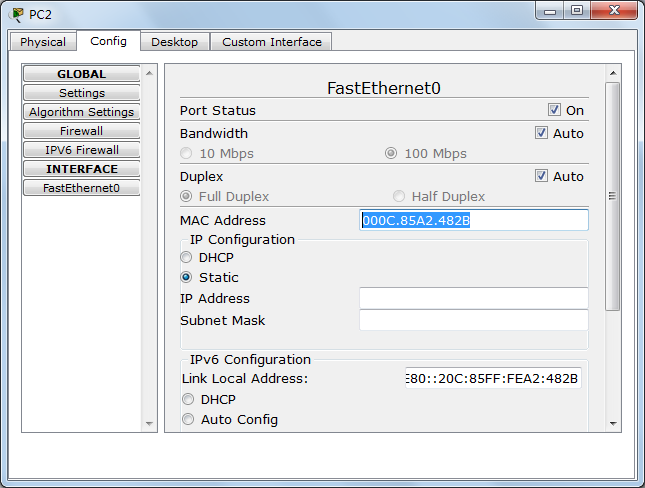
实验8.2拓扑图

**3.实验步骤**

交换机端口安全特性可以让我们配置交换机端口，使得当具有非法MAC地址的设备接入时，交换机会自动关闭接口或者拒绝非法设备接入，也可以限制某个端口上最大的MAC地址数。在这里限制f0/1接口只允许主机PC2接入。

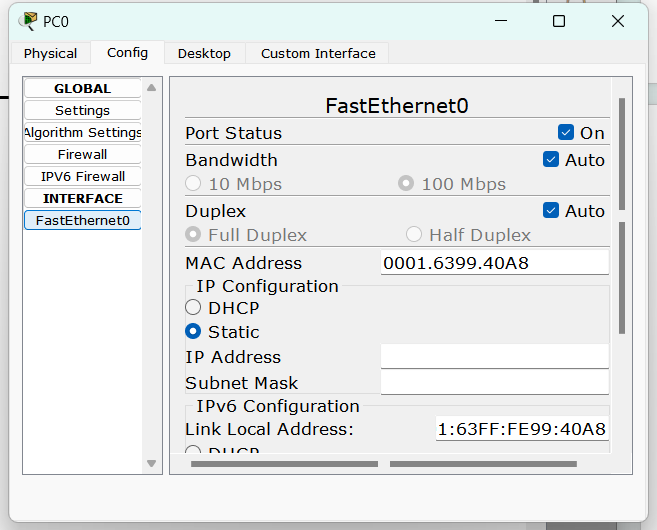
**（1）步骤1：检查主机PC2的MAC地址**

在如下界面中，读出你选中的主机**的MAC地址**



**//问题一、记下你选中的主机的MAC地址，写到实验报告**

**我的主机MAC地址是 0001.6399.40A8**



**（2）步骤2：配置交换端口安全**

Switch>enable

Switch#configure terminal

Switch (config)#interface f0/1

Switch (config-if)#shutdown

Switch (config-if)#switchport mode access

//以上命令把端口改为访问模式，即用来接入计算机

Switch (config-if)#switchport port-security

//以上命令是打开交换机的端口安全功能

Switch (confg-if)#switchport port-security maximum 1

//以上命令只允许该端口下的MAC条目最大数量为1，即只允许一个设备接入

Switch (config-if)#switchport port-security mac-address 000C.85A2.482B **(此处填步骤1中你看到主机的Mac地址) 0001.6399.40A8**

//允许主机接入

Switch (config-if)#switchport port-security violation shutdown

//“switch port-security violation{protect|shutdown|restrict}”命令含义如下：

* protect:当新的计算机接入时，如果该接口的MAC条目超过最大数量，则这个新的计算机将无法接入，而原有的计算机不受影响；
* shutdown:当新的计算机接入时，如果该接口的MAC条目超过最大数量，则该接口将会被关闭，则这个新的计算机和原有的计算机都无法接入，需要管理员使用”no shutdown”命令重新打开；
* restrict:当新的计算机接入时，如果该接口的MAC条目超过最大数量，则这个新的计算机可以接入，然而交换机将向发送警告信息。

Switch (config-if)#no shutdown

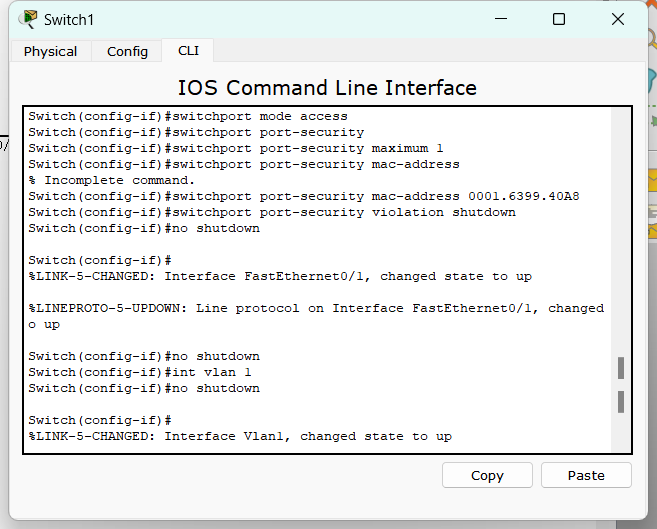
Switch (config)#int vlan 1

Switch (config-if)#no shutdown

Switch (config-if)#ip address 172.16.0.1 255.255.0.0

Switch(config-if)#end

//以上配置交换机的管理地址为172.16.0.1



**（3）步骤3：检查MAC地址表**

Switch #show mac-address-table

Mac Address Table

Switch#sh mac-address-table

Mac Address Table

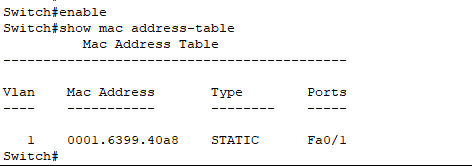
-------------------------------------------

Vlan Mac Address Type Ports

---- ----------- -------- -----

1 000C.85A2.482B STATIC Fa0/1

//主机的MAC已经被登记在f0/1接口，并且表明是静态加入的

****

**（4）步骤4：模拟非法接入**

**在**PC2上配置IP地址：172.16.0.2，子网掩码：255.255.0.0。

这时从PC2 ping 交换机的管理地址172.16.0.1，可以ping 通，

PC>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:

Request timed out.

Reply from 172.16.0.1: bytes=32 time=0ms TTL=255

Reply from 172.16.0.1: bytes=32 time=1ms TTL=255

Reply from 172.16.0.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.16.0.1:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

表明当前二者可以通信。

在PC2上将MAC地址修改为另一个地址，模拟是另外一台设备接入。

几秒钟后，则在S1上出现：

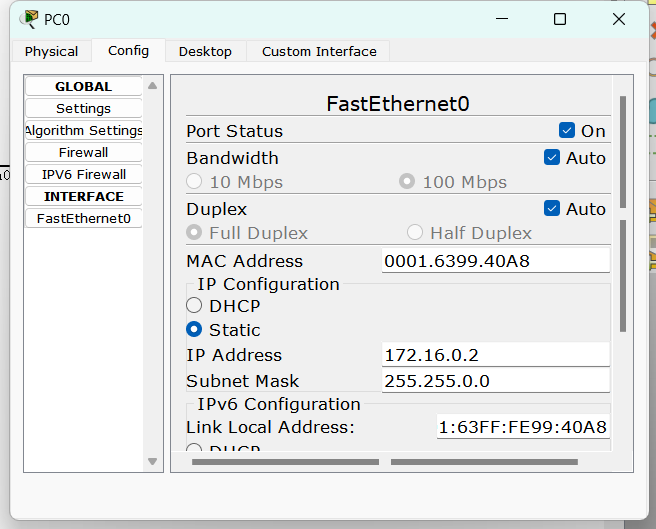
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

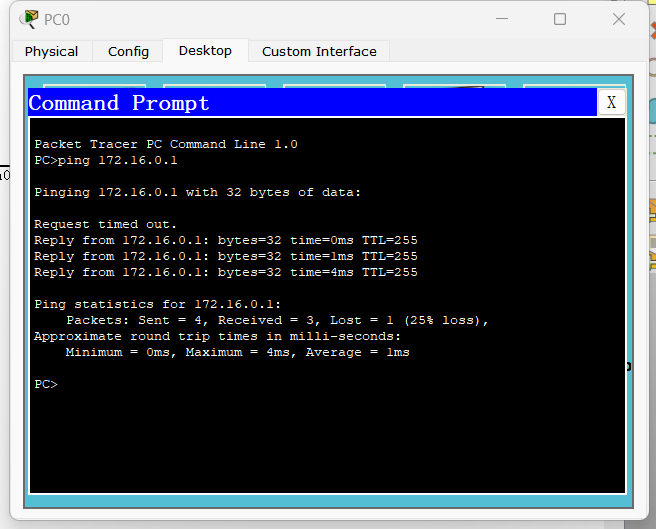
//以上提示f0/1接口被关闭

当非法设备移除后(把主机PC2的MAC地址修改为原来的地址，**模拟这一场景**)，在交换机f0/1接口下，执行”shutdown”和”no shutdown”命令可以重新打开该接口。

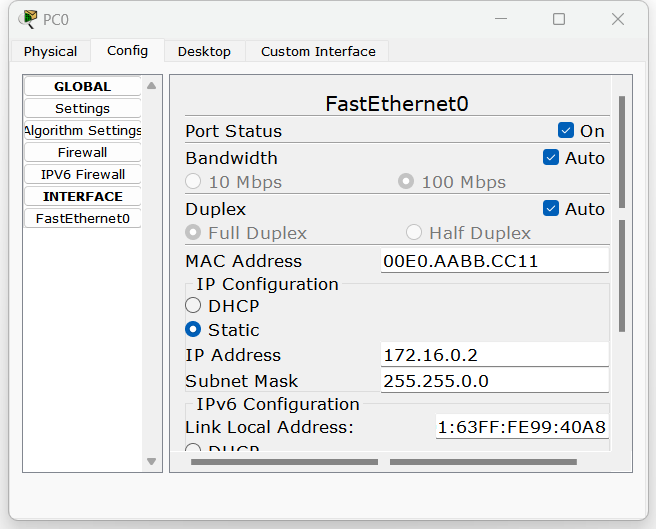
PC2 #ping 172.16.0.1

看看主机和交换机的通信是否恢复正常。





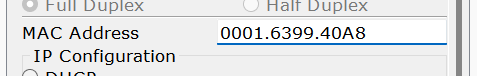
**修改MAC地址**



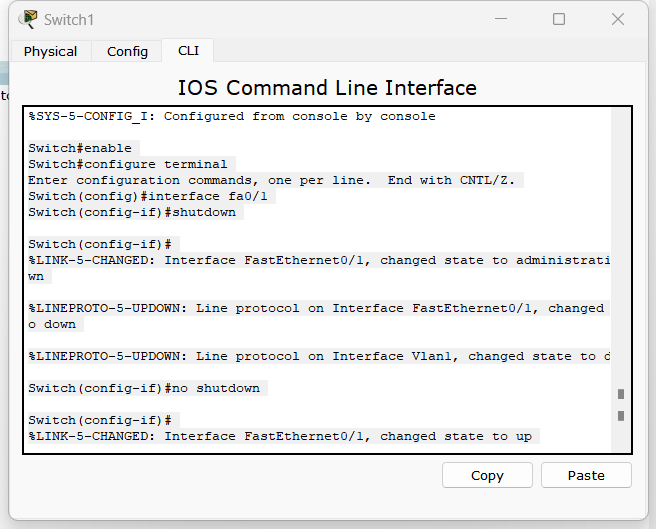
发现 Switch 提示报错



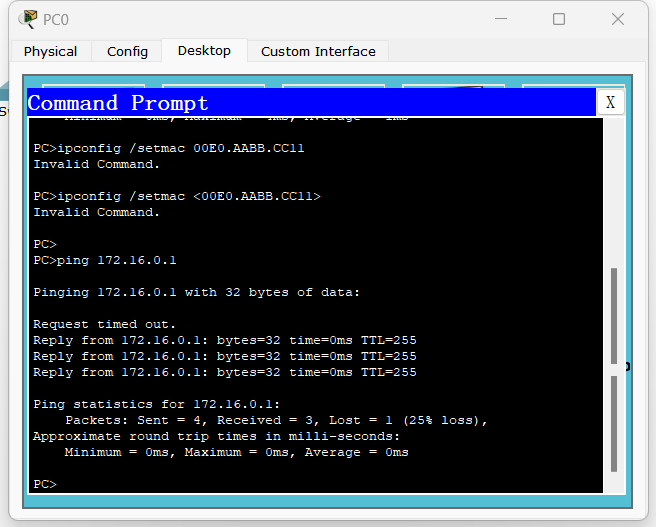
恢复MAC地址



恢复接口状态



通信结果



**(二、将该命令的执行结果写到实验报告)**

## 实验8-3：STP（使用“生成树协议分析.pka”文件）

**一、拓扑图：**

在“生成树协议STP分析.pka”文件中包含两个拓扑图，其中拓扑图1中关闭了4台交换机的生成树协议（使用Switch(config)#no spanning-tree vlan 1），拓扑图2 中开启了4台交换机的生成树协议，拓扑图1和拓扑图2 的其他配置完全相同。实验过程中，任务一在拓扑图1中完成，任务二和任务三在拓扑图2 中完成。

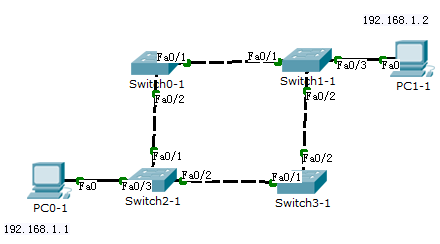


图 STP实验一拓扑图

**二、实验目的**

1.理解交换式以太网中的环路问题；

2.理解生成树协议的工作原理。

**三、实验步骤：**

**1. 任务一：观察无生成树协议的以太网环路中广播帧的传播**

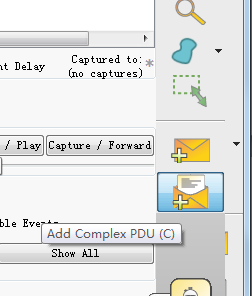
**步骤1：准备工作**

打开文件生成树协议STP分析.pka。若此时拓扑图1中交换机端口指示灯呈橙色，则单击主窗口右下角Realtime和Simulation模式切换按钮数次，直至交换机指示灯呈绿色。否则，略过此步骤。

**步骤2：在拓扑图1中添加广播包**

进入Simulation模式，点击Edit Filters按钮设置事件列表过滤器，使其只显示与ICMP协议相关事件。

单击Add Complex PDU按钮（位置如下图所示），单击拓扑图1中的PC0，在弹出的对话框中设置参数：Destination IP Address设置为255.255.255.255（广播地址），Source IP Address设置为192.168.1.1（PC0 的IP地址），Sequence Number设置为1，Size设置为0，Simulation Settings中One shot time设定为1，然后单击对话框中下方的Create PDU按钮，创建数据包。



**步骤3：捕获数据包，观察广播包的传播**

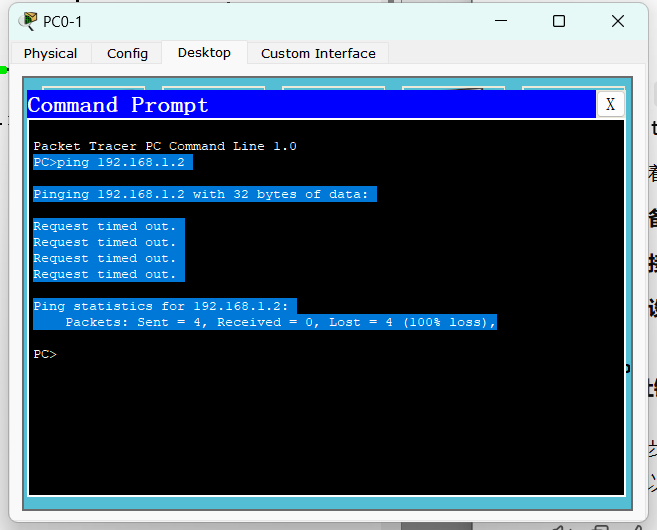
单击Auto Capture/Play按钮，捕获数据包。观察拓扑图1中广播包的传播动画。

此时，每台交换机在接收到数据包后都会通过其他所有端口转发出去。交换机不停接收来自其他交换机转发的数据包，再向其他交换机转发数据包，导致该广播包无休止的在四台交换机形成的环路中传播。

**注意：**此过程不会停止，完成步骤3后单击Realtime模式按钮切换的实时模式，进行步骤4的操作。

**步骤4：在实时模式下，测试网络是否正常**

进入Realtime模式，单击PC0，选择Desktop选项，选择其中的Command Prompt工具，在界面中输入ping 192.168.1.2并回车**，测试PC0和PC1是否能够连通。**



1. **任务一中，为什么PC0 无法保证ping通PC1？**

**存在网络环路，导致了广播风暴**

单击Packet Tracer窗口下方的Delete按钮，删除所有场景，为下一个任务做好准备。

**2. 任务二：观察启用生成树协议的以太网环路中广播帧的传播**

**步骤1：观察分析拓扑图2中启用生成树协议后的逻辑拓扑图**

观察拓扑图2中各端口的指示灯颜色。端口指示灯为绿色表示该端口可以接收和转发数据帧，端口指示灯为橙色表示该端口不能接收和转发数据帧。

**注意：**生成树协议的计算需要消耗一定的时间。需要等待拓扑图中只有一个端口指示灯为橙色时方可进行实验。这一过程可以通过交替单击主窗口右下角的Realtime和Simulation模式切换按钮数次进行加速。

在网络正常运行情况下，生成树协议会将环路中的一些端口屏蔽，禁止其接收和转发数据帧，形成无环的树型逻辑拓扑，避免广播帧无休止的传播。拓扑图中指示灯为橙色的端口即为生成树协议屏蔽的端口。

**步骤2：在拓扑图2中添加广播包**

进入Simulation模式，在拓扑图2中添加广播包。具体操作参照任务一中的步骤2。

**步骤3：捕获数据包，观察广播包的传播**

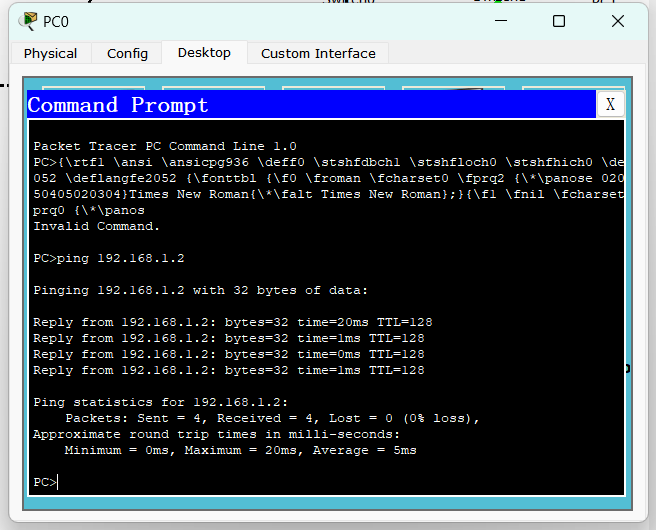
逐步单击Capture/Forward按钮捕获数据包，直至该过程结束不再产生新的数据包。在此过程中仔细观察广播包的转发情况，每台交换机的哪些端口丢弃该广播包，哪些端口转发该广播包。并与步骤1记录的树型拓扑图进行对比。

**步骤4：在实时模式下，测试网络是否正常**

进入Realtime模式，单击PC0，选择Desktop选项，选择其中的Command Prompt工具，在界面中输入ping 192.168.1.2并回车，测试PC0和PC1是否能够连通。

1. **PC0和PC1是否能够连通？**

**可以连通了**



**如果能够连通，说明STP协议避免了网络环路导致的广播风暴。通过对比任务一和任务二的连通性测试结果，可以深入理解生成树协议的作用。**

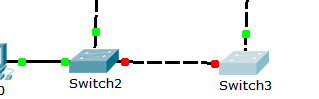
单击Packet Tracer窗口下方的Delete按钮，删除所有场景，为下一个任务做好准备。

**3. 任务三：观察链路故障时生成树协议启用冗余链路的情况**

**步骤1：制造链路故障**

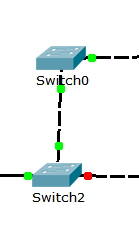
单击拓扑图2中的Switch3，在其配置窗口中选择Config选项卡，在INTERFACE列表下单击FastEthernet0/1端口，在其右端配置界面中单击Port Status项对应的复选框，取消勾选，即关闭该端口。

此时可以观察到拓扑图2中的Switch2和Switch3连接的链路上两个端口指示灯为红色，表示该链路已经中断。



**步骤2：观察生成树协议启用冗余链路**

当树形逻辑拓扑图中出现故障时，生成树协议将自动启用屏蔽端口形成新的树形拓扑，保证网络的连通性。为了加快这一过程，可以通过交替单击主窗口右下角的Realtime和Simulation模式切换按钮数次进行加速，直至原来橙色指示灯变绿色。



**注意：生成树协议重新计算生成树时在Packet Tracer中耗时较长，可能持续数十秒甚至1—2分钟左右的时间。**

1. **任务三中，当网络发生链路故障后，等待原来橙色指示灯变绿色后，PC0和PC1 能否进行通信？**

**可以了。**

