

**本科实验报告**

|  |  |
| --- | --- |
| 课程名称： | 计算机网络基础 |
| 实验名称： | 使用二层交换机组网 |
| 姓 名： | 颜晗 |
| 学 院： | 计算机学院 |
| 系： | 计算机科学与技术 |
| 专 业： | 计算机科学与技术 |
| 学 号： | 3200105515 |
| 指导教师： | 杨樾人，张泉方 |

年 月 日

**浙江大学实验报告**

实验名称： 使用二层交换机组网 实验类型： 操作实验

同组学生： 实验地点： 计算机网络实验室

# 实验目的

1. 掌握交换机的工作原理、管理配置方法；
2. 掌握VLAN的工作原理、配置方法；
3. 掌握跨交换机的VLAN Trunk配置方法；
4. 掌握多个交换机的冗余组网、负载平衡的配置方法。

# 实验内容

* 使用网线连接PC，让PC彼此能够互相Ping通；
* 配置和管理交换机：使用Console线连接交换机，运行Putty等终端软件，对交换机进行配置；
* 通过Telnet远程管理交换机；
* 配置镜像端口，用Wireshark软件抓取交换机各端口的数据；
* 配置VLAN Access端口和VLAN Trunk端口；
* 配置交换机的冗余备份；
* 配置交换机的负载均衡。

# 主要仪器设备

PC机、路由器、交换机、Console连接线、直联网络线、交叉网络线。

# 操作方法与实验步骤

IOS软件的基本操作：

1. 进入特权模式：enable；该模式下才能查看重要信息，并可进入配置模式；
2. 进入配置模式：configure terminal；在这个模式下才可以修改配置；
3. 进入到某个接口的配置模式：interface 接口名 模块号/端口号，例如interface ethernet 0/1；
4. 命令可以不输全，只要能够被唯一识别；
5. 输入？可以显示当前上下文环境下可用命令；
6. 在命令后面输入？可以显示命令的参数提示；
7. 输入命令的前一部分，再按<tab>，可以自动完成完整的命令输入；
8. 按上箭头可以重复输入上次打过的命令；
9. 鼠标左键选择需要截取的文本内容，鼠标右键粘贴复制好的文本的内容。

Part 1. 单交换机

1. 用1台二层交换机和4台PC组成一个小型局域网
2. 使用直联网络线，将每个PC机都连接到交换机的不同端口；
3. 使用Console线，连接到交换机的Console端口和控制台PC的串口，并在控制台PC上运行Putty等终端软件；
4. 观察交换机的每个端口状态指示，确认PC机都正确连接到了交换机的端口；
5. 查看当前哪些端口已连接，哪些端口未连接，连接的速率和模式，收发统计；
6. 在控制台输入命令查看当前设置了哪些VLAN，缺省所有的端口都属于同一个VLAN 1，如果有端口属于非默认VLAN，输入命令取消该VLAN；
7. 在每个PC机上互相用Ping来测试连通性，验证局域网已经建立；
8. 手工关闭某个端口，然后查看端口关闭后的效果，在对应的PC机上使用Ping测试连通性；
9. 给交换机配置一个IP地址，并在交换机上用Ping命令测试与PC间的连通性；
10. 在非控制台PC机上，通过telnet连接交换机，进行远程配置。
11. 设置交换机的镜像端口
12. 确定某个PC（假设为PC1）连接的端口为镜像端口；
13. 在该PC机上运行包捕获软件，抓取数据包；
14. 在其他2个PC机上运行Ping，互相测试彼此的连通性；
15. 查看是否能抓取到其他2个PC机之间的Ping响应包，正常情况下，由于交换机是根据MAC地址直接转发的，所以PC1是收不到其他PC之间的响应包；
16. 在交换机上将连接PC1的端口配置为镜像端口，被镜像的端口分别为另外2个PC连接的端口；
17. 在PC1上再次启动包捕获软件，抓取数据包；
18. 在其他PC机上运行Ping，测试彼此的连通性；
19. 查看是否能抓取到其他2个PC机之间的Ping响应包。镜像端口设置后，交换机将把被镜像的源端口收发数据复制一份给镜像目的端口。同时该端口的正常收发功能关闭。
20. 在交换机上设置VLAN
21. 输入命令，在交换机上增加1个新的VLAN；
22. 将PC3和PC4加入新的VLAN；
23. 通过PING验证PC之间的连通性；
24. 如果交换机上有密码，请按照下面的步骤清除密码：
25. 用控制线连接PC和交换机的Console口，PC上运行Putty软件；
26. 断开交换机电源，然后按住交换机的mode键不放，重新打开交换机电源，直到mode灯闪烁十秒左右后再放开mode键；
27. 在Putty软件上观察交换机启动过程，直到出现Switch:的提示符；
28. 输入dir flash:查看是否存在config.text文件，如果不能列出目录，输入命令flash\_init，待flash加载成功后再输入命令rename flash:config.text flash:configX.text将配置文件改名；
29. 输入命令reload 或 reset重新启动。

Part 2. 多交换机

1. 用2台交换设备和4台PC组成一个小型局域网，每个交换机都连接2台PC机；
2. 在交换机上都设置2个VLAN，将每个交换机上的PC都分成2组，各属于1个VLAN；
3. 将两个交换机连起来，设置互联端口为VLAN Trunk模式，并测试同一组VLAN跨交换机的联通性；普通模式的端口只允许一个VLAN的数据通过，VLAN Trunk模式允许多个VLAN数据同时通过一个端口。
4. 用2条网线连接2个交换机，验证Spanning-tree的作用。交换机之间自动会运行Spanning-tree协议，避免产生转发回路。如果关闭Spanning-tree,存在物理回路的网络很容易产生广播风暴，从而导致网络瘫痪。
5. Spanning-tree是按照VLAN进行管理的，不同VLAN的Spanning-tree可以有不同的设置，因此，可以利用这点实现在两个交换机上的负载平衡。测试2条网线均连接时，数据是否从2条网线分别传送，而当1条网线断开时，数据是否全部改从另外1条网线和传送。

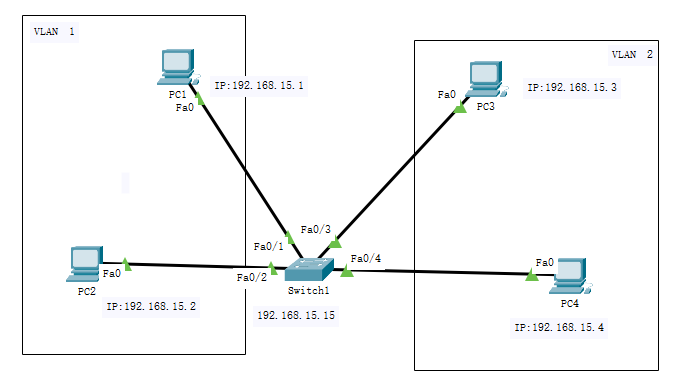
# 实验数据记录和处理

由于疫情影响，本实验在Packet tracer 模拟软件上进行，putty软件连接交换机操作部分使用交换机本身终端或者PC的telnet连接，wireshark部分使用软件模拟本身的抓包功能替代。

-------- Part 1 ---------

1. 在实验拓扑图上标记交换机的IP地址、PC的IP地址及所属VLAN、交换机的与PC的连接端口）

拓扑图参考，请替换成实际使用的：



1. 找一台有串口的PC机和一根串口控制线，将控制线的一头连接交换机的Console口，另一头连接PC机的串口。

在PC机上运行Putty软件，选择Serial方式，默认为9600, COM1。按两下回车，检查是否已经连上交换机。并输入enable命令进入到特权模式。如果有密码，请参考第四章的第4小节进行密码清除。

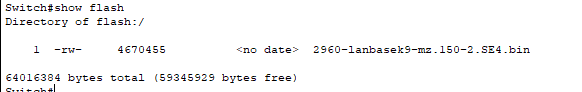
输入命令show version查看当前交换机型号信息并记录：

设备型号： C2960-LANBASEK9 ，IOS软件版本： 15.0(2)SE4 ，

软件映像文件名： flash:c2960-lanbasek9-mz.150-2.SE4.bi，端口数量： 26 。

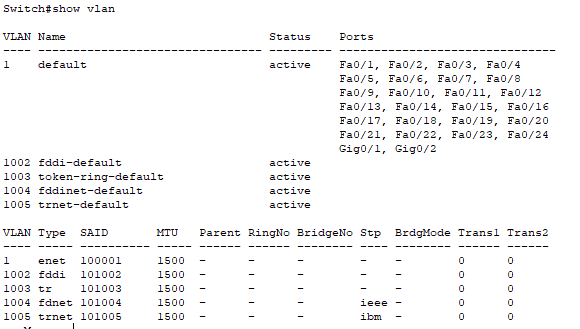
1. 输入命令show flash: 查看当前文件系统的内容：

截图参考（此处应替换成实际截获的数据）：



1. 显示交换机的VLAN数据（命令show vlan），所有的端口应该都属于VLAN 1。（如果存在其他VLAN，先通过命令no vlan id删除）

截图参考（此处应替换成实际截获的数据）：

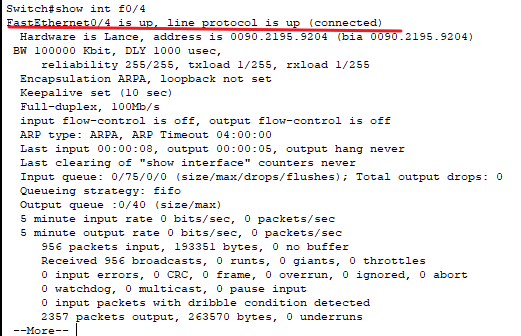


1. 用直连网线（straight through）将PC按照前述拓扑结构连接到交换机。然后给各PC配置IP地址，并用Ping检查各PC之间的联通性，确保都能Ping通，否则请检查网线连接。

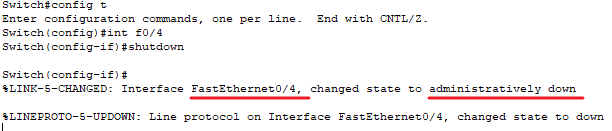
手工关闭某端口（命令：shutdown)，输入命令查看该端口状态（命令：show interface端口号，如show interface e0/1），在其他PC上使用Ping命令检测连接在该端口的PC是否能够联通。

命令输出截图：

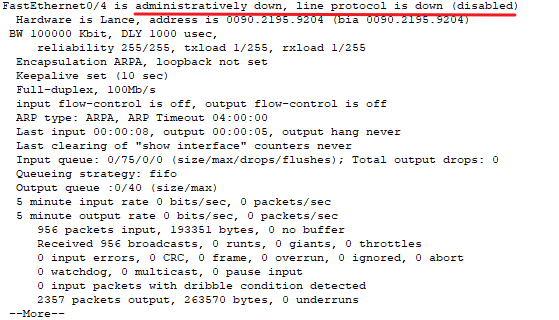
关闭端口前查看端口状态



关闭与PC4(ip = 192.168.15.4)的端口fa0/4

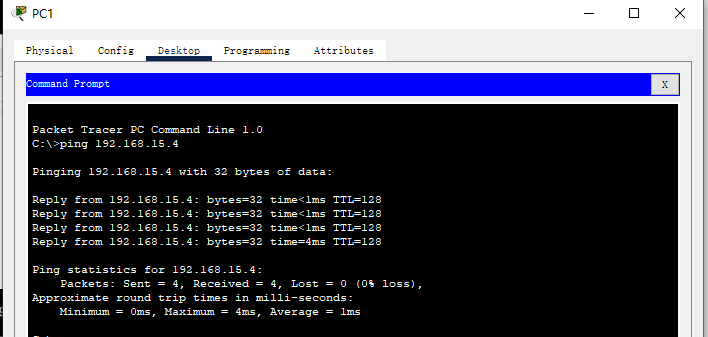


关闭端口后查看端口状态

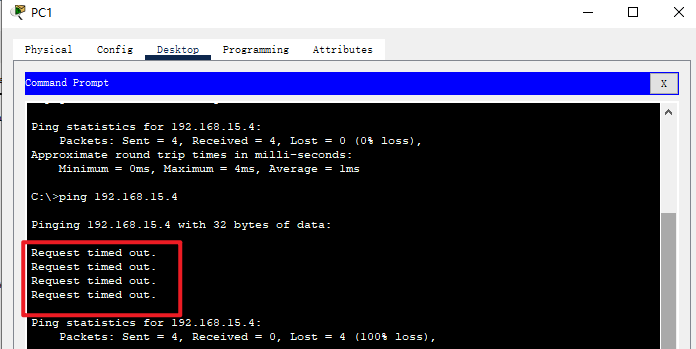


Ping结果截图：

端口关闭前PC1->PC4

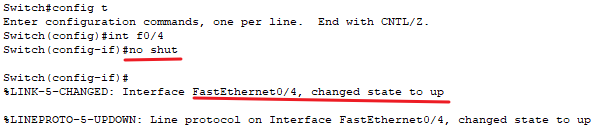


端口关闭后PC1->PC4

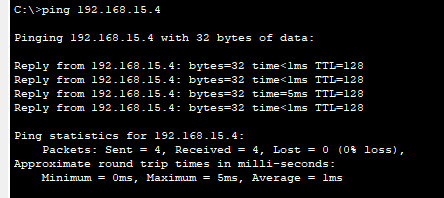


1. 重新打开该端口（命令：no shutdown），输入命令查看交换机上端口状态。使用Ping命令检测连接在该端口的PC是否能够联通。

命令输出截图：



Ping结果截图：



1. 进入VLAN1接口配置模式（命令：interface vlan 1），给VLAN 1配置IP地址即是给交换机配置管理IP地址（命令：ip address 地址 掩码）。测试PC是否能Ping通交换机的IP地址；如果不通，查看VLAN 1端口的状态是否是up，如果不是，则打开VLAN端口（no shutdown）。

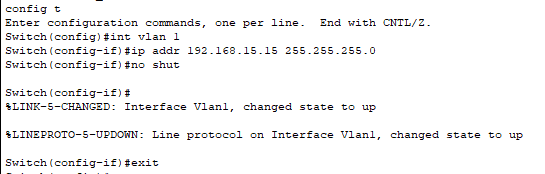
输入的命令：

config t

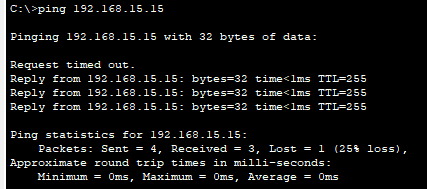
int vlan 1

ip addr 192.168.15.15 255.255.255.0

no shut

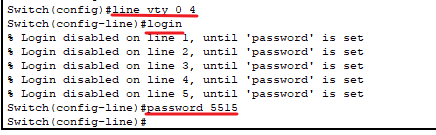


从PC4 ping 交换机



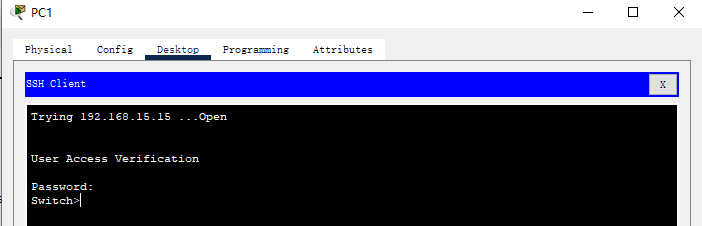
1. 输入以下命令：打开虚拟终端（命令line vty 0 4），允许远程登录（命令： login），设置登密码（命令：password 密码）

命令截图：



1. 在PC上运行Putty软件，选择telnet协议，输入交换机的IP地址，通过网络远程连接交换机，并输入密码。

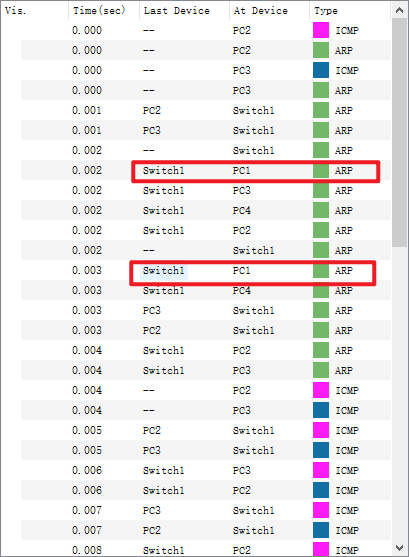
连接成功的截图：

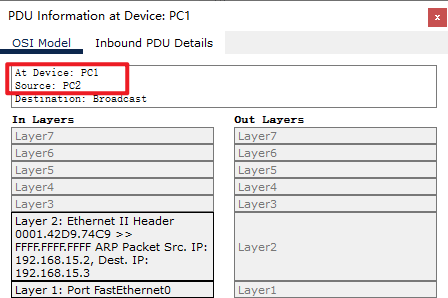


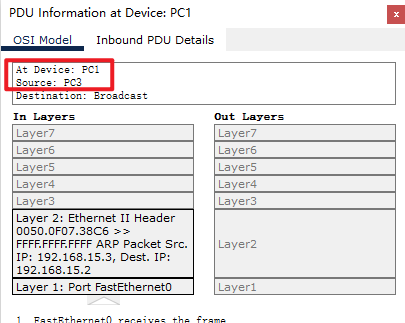
1. 在PC1上运行Wireshark，在另外2台（PC2、PC3）上互相持续的Ping（运行“ping IP地址 -t”），观察在PC1上是否能抓取到PC2和PC3发出的ARP广播包以及ICMP响应包。如果不能抓取到PC2、PC3发送的ARP广播包，在PC2、PC3上先运行“arp –d \*”删除所有主机的ARP缓存。正常情况下，ICMP响应包是不能被抓取到的。

抓包截图：

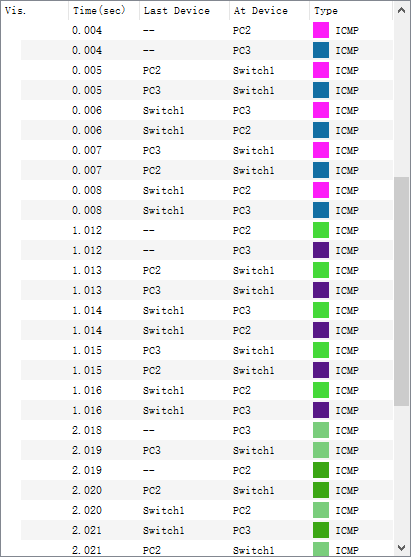
可以接收到ARP 广播包







但是接收不到ICMP响应包，可以看到只有PC2和PC3有ICMP的包



1. 选择一个交换机端口配置为镜像端口（命令：monitor session 1 destination interface 端口），将PC1的网线切换到该端口，将PC2和PC3所连端口配置为被镜像端口（命令：monitor session 1 source interface 端口）。继续运行Wireshark，观察在PC1上是否能抓取到PC2和PC3的ICMP响应包。

输入的命令：

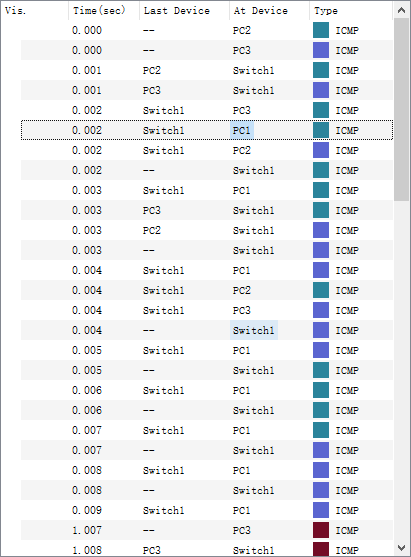
monitor session 1 destination int fa0/1

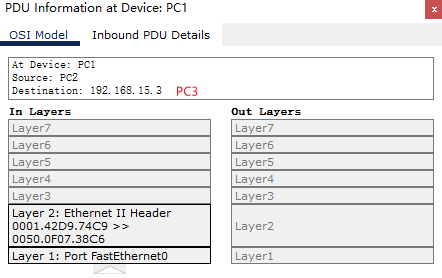
monitor session 1 source int fa0/2

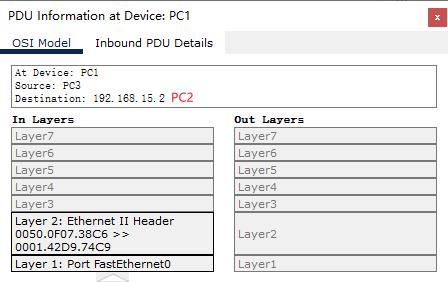
monitor session 1 source int fa0/3

抓包截图：

可以看到，虽然是PC2和PC3之间互相发包，但是交换机也会转发给PC1.







1. 关闭PC1端口的镜像功能（命令：no monitor session 1 destination interface 端口)，否则该端口不能正常收发数据。

输入的命令：

no monitor session 1 destination int fa0/1

1. 在交换机上增加VLAN 2（命令：vlan database或config terminal，vlan 2），将PC3、PC4所连端口加入到VLAN 2（命令：interface 端口，switchport access vlan 2）。用Ping检查PC之间的联通性（同一VLAN的PC之间能够通，不同VLAN的PC之间不能通）。

输入的命令：

config t

vlan 2

int fa0/3

switchport access vlan 2

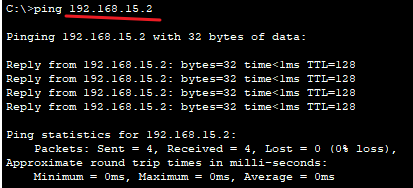
int fa0/4

switchport access vlan 2

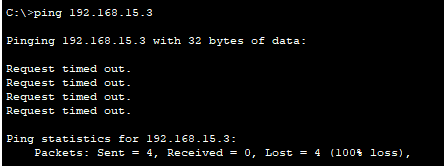
当然，对于Packet tracer实际上可以通过图形界面进行设置

联通性检测截图：

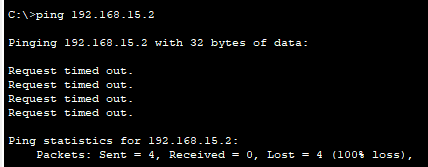
PC1🡪PC2



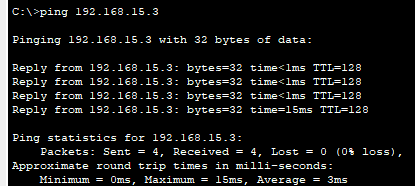
PC1🡪PC3



PC4🡪PC2



PC4🡪PC3



1. 查看交换机上的运行配置（命令show running-config），复制粘贴本节相关的文本。

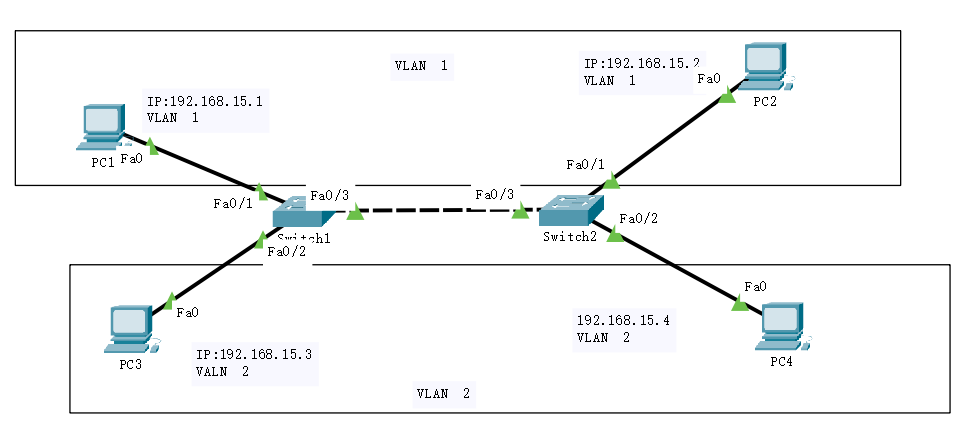
运行配置文本：

|  |
| --- |
| Current configuration : 1244 bytes  !  version 15.0  no service timestamps log datetime msec  no service timestamps debug datetime msec  no service password-encryption  !  hostname Switch  !  spanning-tree mode pvst  spanning-tree extend system-id  !  interface FastEthernet0/1  !  interface FastEthernet0/2  !  interface FastEthernet0/3  switchport access vlan 2  !  interface FastEthernet0/4  switchport access vlan 2  !  interface Vlan1  ip address 192.168.15.15 255.255.255.0  !  !  line con 0  !  line vty 0 4  password 5515  login  line vty 5 15  login  !  !  monitor session 1 source interface Fa0/2  monitor session 1 source interface Fa0/3  !  end |

-------- Part 2 ---------

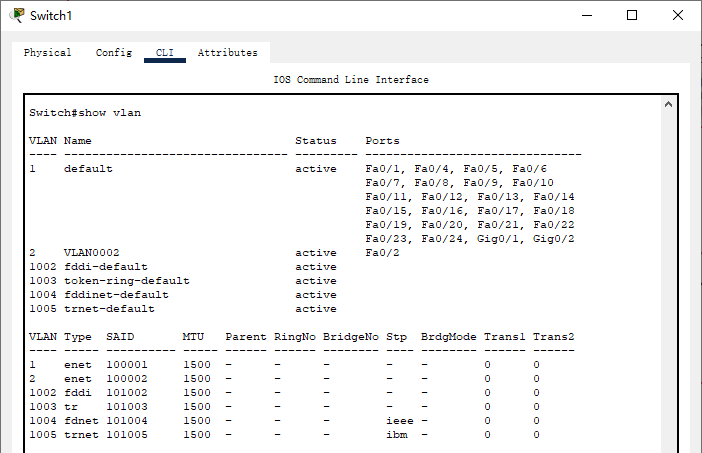
1. 增加一台交换机（Switch2），将PC2、PC4连接到该交换机，并用一根交叉网线（Cross-over）将两个交换机连接起来。在拓扑图上记录各PC的IP地址、连接端口及所在VLAN：

拓扑图参考，请替换成实际使用的：

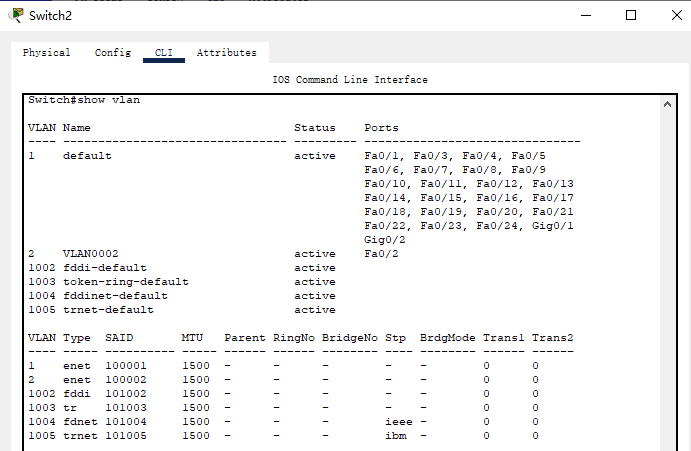


在Switch2上增加VLAN 2，将PC4所连端口加入到VLAN 2。用Ping检查不同交换机上属于同一VLAN的PC之间的联通性（即PC1与PC2应该通，PC3与PC4不能通）。然后显示2个交换机的VLAN数据（命令show vlan）

Switch1的vlan数据：

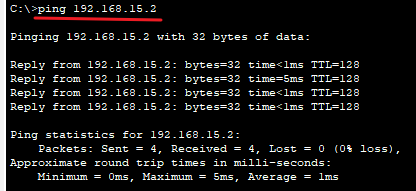


Switch2的vlan数据：

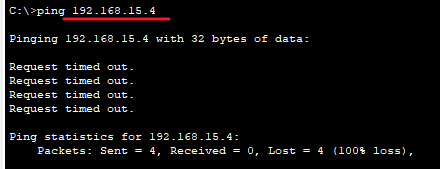


联通性检测截图：

PC1🡪PC2



PC3🡪PC4



1. 将交换机之间的互联端口配置为VLAN Trunk模式（命令：switchport mode trunk，部分型号的设备可能要先设置封装协议，命令：switchport trunk encapsulation dot1q），再次用Ping检查属于同一VLAN但在不同交换机的PC之间的联通性（即PC1与PC2应该通，PC3与PC4也应该通）。

输入的命令：

Switch 1:

config t

int fa0/3

switchport mode trunk

Switch2:

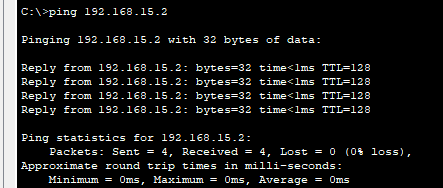
config t

int fa0/3

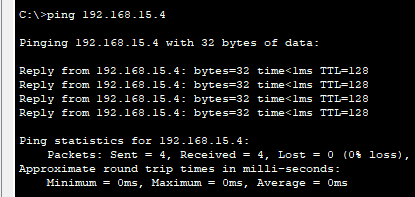
switchport mode trunk

联通性检测截图：

PC1🡪PC2



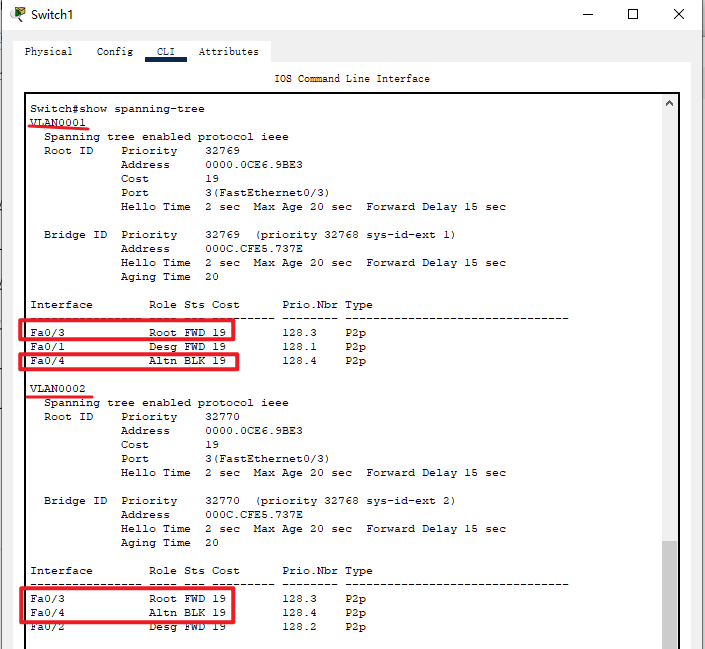
PC3🡪PC4



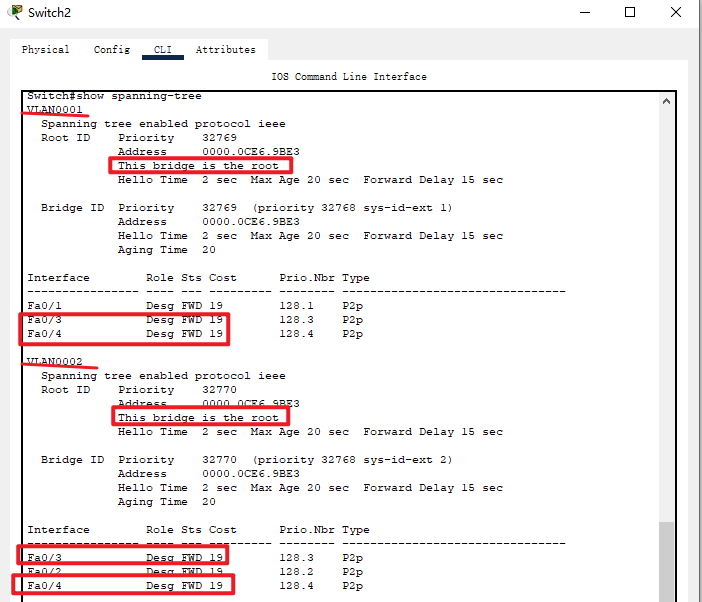
1. 再增加一根网线，把2个交换机的另外2个端口连接起来。并将这2个端口都配置成VLAN Trunk模式。稍等片刻，查看4个互联端口的状态（命令：show spanning-tree），分别在2个VLAN中标出: 哪个交换机是根网桥？哪些端口处于转发状态（FWD），哪些端口处于阻塞状态（BLK）。

Spanning-tree数据截图示例（请替换成实际显示的）：

Switch1:



Switch2:

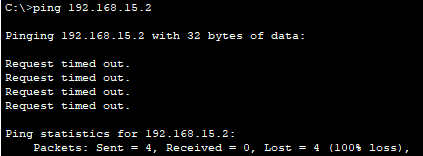


1. 关闭2个VLAN的STP（命令：no spanning-tree vlan ID），观察两个交换机的端口状态指示灯（急速闪动），并在PC上用Ping测试网络的延迟是否加大（甚至可能出现超时或丢包）。

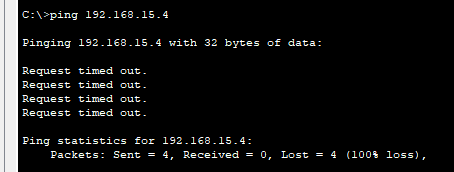
Ping结果截图：

两次ping的结果都是全部丢包。

PC1 ping PC2:



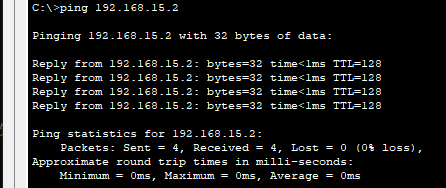
PC3 ping PC4:



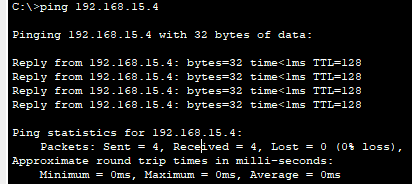
1. 重新打开2个VLAN的STP（命令：spanning-tree vlan ID）, 观察两个交换机的端口状态指示灯（缓慢闪动），并在PC上用Ping测试网络的延迟是否恢复正常。

Ping结果截图：

PC1 ping PC2:



PC3 ping PC4:

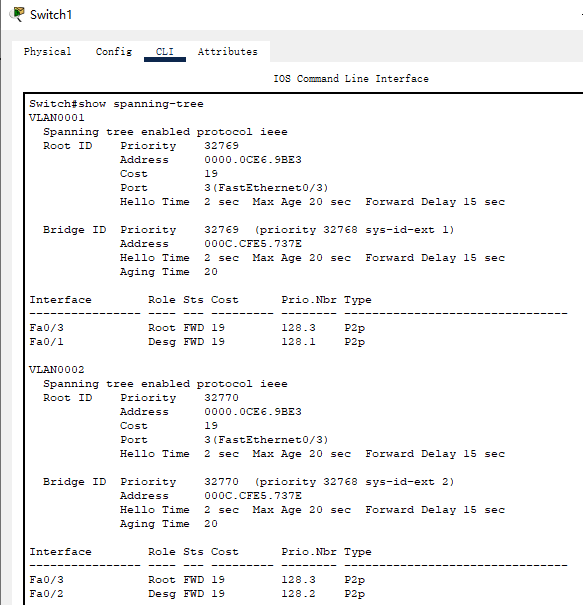


1. 掉连接在2个处于FWD状态端口之间的网线，等待一会儿，查看4个互联端口的状态（命令：show spaning-tree）（有些端口可能已经消失）。标出原BLK状态的端口是否变成了FWD状态。

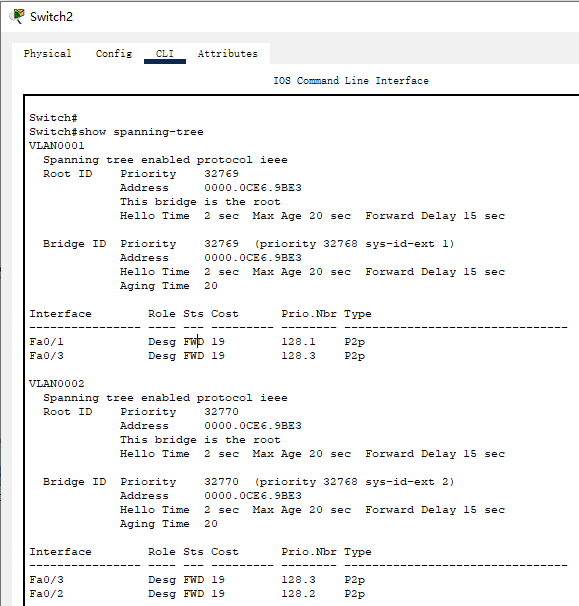
Spanning-tree数据截图（分交换机显示）：

原BLK状态的端口直接消失了。

Switch1:



Switch2:



1. 配置2个交换机的互联端口优先级(默认优先级128)，使VLAN1的数据优先通过第1对互联端口传送（命令：interface 端口, spanning-tree vlan 1 port-priority 16）。使VLAN2的数据优先通过第2对互联端口传送（命令：interface 端口, spanning-tree vlan 2 port-priority 16）。此处只记录2个交换机各自所使用的命令及参数即可。

输入的命令：

Switch1：

int fa0/3

spanning-tree vlan 1 port-priority 16

int fa0/4

spanning-tree vlan 1 port-priority 16

Switch2：

int fa0/3

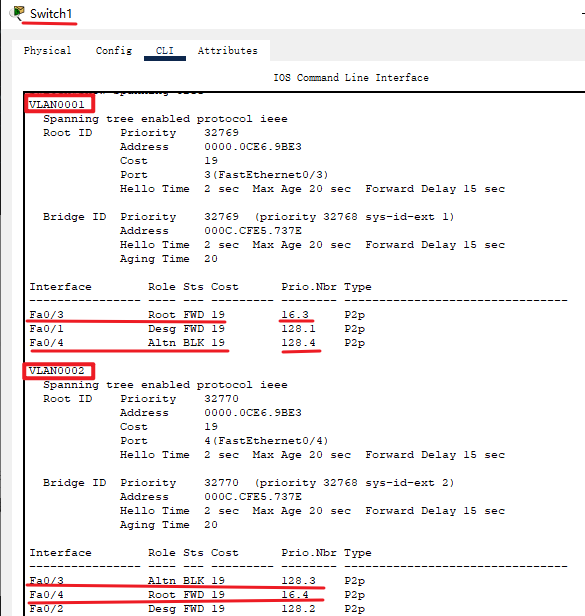
spanning-tree vlan 1 port-priority 16

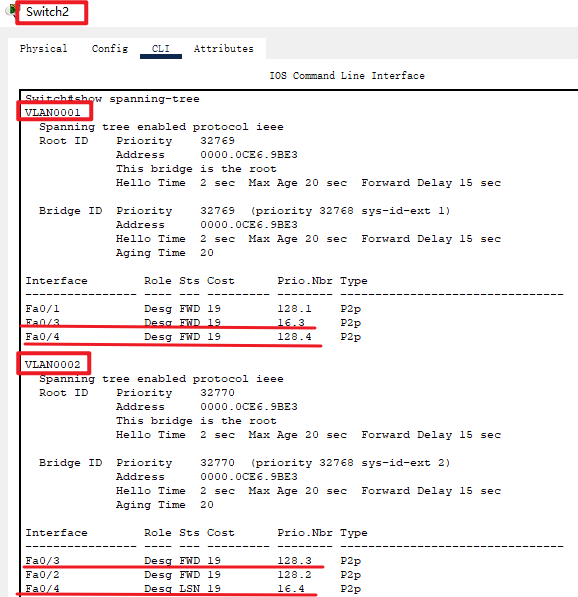
int fa0/4

spanning-tree vlan 1 port-priority 16

1. 拔掉剩下的1根连接互联端口的网线，稍后2根网线重新插上，等待一会儿，查看4个互联端口的状态，分别在2个VLAN中标出:各端口的优先级，哪些端口处于转发状态，哪些端口处于阻塞状态。

Spanning-tree数据截图（分交换机显示）：



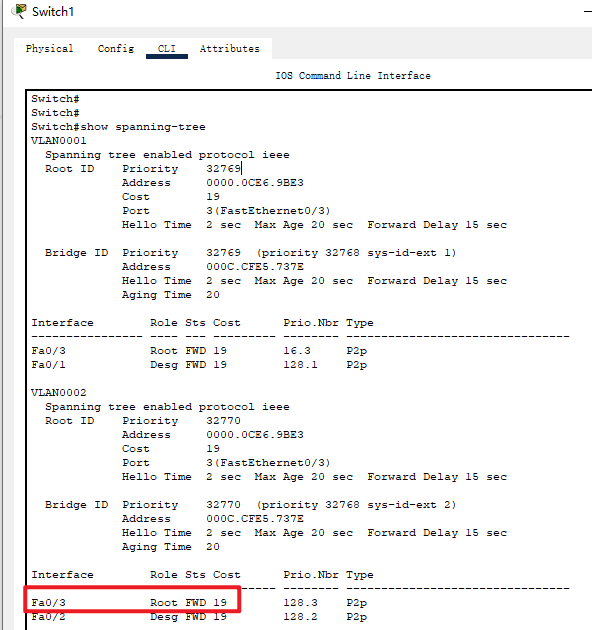


1. 拔掉其中1根连接互联端口的网线，查看4个互联端口中原先处于BLK状态的端口，是否变成了FWD状态（哪个VLAN发生了变化）

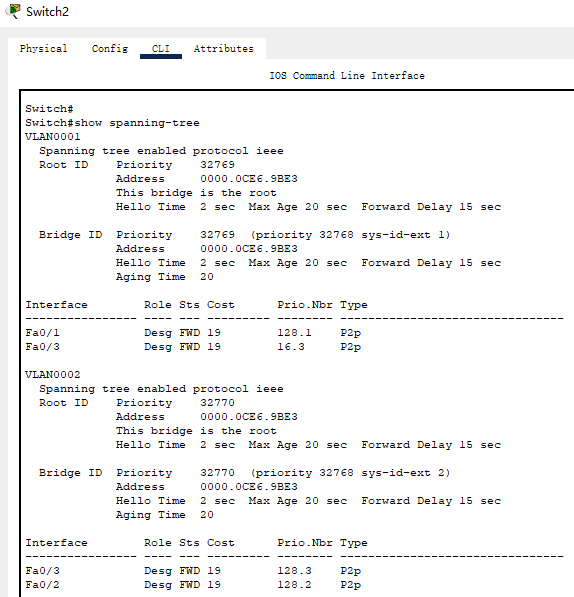
Spanning-tree数据截图（分交换机显示）：

Switch1:

VLAN 2中Fa0/3端口从原本的BLK状态变成了FWD状态（实际上中间有一段时间LSN状态）



Switch2:



1. 记录2个交换机上的运行配置（命令:show running-config），复制粘贴本节相关的文本（完整的内容请放在文件中，每个交换机一个文件，分别命名为S1.txt、S2.txt）。

运行配置文本：

Switch1：

|  |
| --- |
| interface FastEthernet0/2  switchport access vlan 2  !  interface FastEthernet0/3  switchport mode trunk  spanning-tree vlan 1 port-priority 16  !  interface FastEthernet0/4  switchport mode trunk  spanning-tree vlan 2 port-priority 16 |

Switch2：

|  |
| --- |
| interface FastEthernet0/2  switchport access vlan 2  !  interface FastEthernet0/3  switchport mode trunk  spanning-tree vlan 1 port-priority 16  !  interface FastEthernet0/4  switchport mode trunk  spanning-tree vlan 2 port-priority 16 |

# 实验结果与分析

根据你观察到的实验数据和对实验原理的理解，分别解答以下问题：

* 端口状态显示为administratively down，意味着什么意思？

答：表示该端口没有开启，即需要使用no shutdown开启该端口。

* 在交换机配置为镜像端口前，为什么可以抓取到其他PC之间的ARP请求包，而不能抓取ARP响应包？

答：ARP请求包是广播包，即会发往所有PC，所以可以抓取到其他的PC的请求包；

但是ARP响应包不是广播包，而是定向发往指定PC，因此无法抓取到其他PC的响应包。

* PC属于哪个VLAN，是由PC自己可以配置的，还是由交换机决定的？

答：由交换机决定，交换机将PC所连接的端口分配为哪个VLAN，PC就属于哪个VLAN。

* 同一个VLAN的PC，如果配置了不同长度的子网掩码，能够互相Ping通吗？

答：一般情况下不能，配置不同长度的子网掩码使得PC处于不同的网段，除非使用的交换机拥有路由功能且正确进行了相关配置的情况下这两个PC才能互相ping通。

* 为什么在划分为2个VLAN后，两组PC之间就不能进行IP通信了呢？

答：在仅使用二层交换机的情况下，交换机转发通过 MAC，而 VLAN 隔绝了广播域，请求MAC地址的ARP请求包又是广播包，因此属于不同VLAN的PC无法获得对方的MAC地址，就无法完成通信，无法ping通

* 交换机在VLAN Trunk模式下使用的封装协议是什么？

答：对于实验中使用的 Cisco 交换机，所使用的封装协议是 dot1q。

* 未启用STP（Spanning Tree Protocol）协议时，交换机之间连接了多条网线后，为什么Ping测试的响应会延迟很大甚至超时？

答：STP 协议是一个二层的链路管理协议，它在提供路径冗余的同时避免了网络中的回路。

在未启用 STP 的情况下，二层交换网络中会产生网络环路，数据包会在交换机之间形成的环路上重复发送，导致网络资源的巨大浪费，使得ping测试会延迟很大甚至超时。

* 从插上网线后开始，交换机的端口状态出现了哪些变化？大约需要多少时间才能成为FWD状态？期间，连接在该端口的计算机是否能够Ping通？

答：状态变化 LSN(listring)->LRN(learning)->FWD(forwarding),根据模拟实验中的观察结果大约需要十几秒左右的时间，在这期间连接在该端口的计算机不能够ping通。

# 讨论、心得

在完成本实验后，你可能会有很多待解答的问题，你可以把它们记在这里，接下来的学习中，你也许会逐渐得到答案的，同时也可以让老师了解到你有哪些困惑，老师在课堂可以安排针对性地解惑。等到课程结束后，你再回头看看这些问题时你或许会有不同的见解：

在实验过程中你可能会遇到的困难，并得到了宝贵的经验教训，请把它们记录下来，提供给其他人参考吧：

最初没注意part2 其实继承了part1的配置，重新开了一个工程，导致PC3 ping PC4测试结果与预期有点不一样，后面才发现。

由于packet tracer 无法连接wireshark，最初差点重回GNS3，后面发现无需具体关心包的内容，那么Packet tracer 模拟本身的抓包也足够了。

你对本实验安排有哪些更好的建议呢？欢迎献计献策：

建议实验抛弃GNS3，全面改换Packet tracer 进行教学活动。