

# 计算机网络实验报告

## 计算机网络实验四： 跨路由器实现 VLAN

院(系)名称：数据科学与计算机学院

专业名称：计算机科学与技术

学生姓名：王永锋, 颜彬, 杨陈泽

学生学号：16337237, 16337269, 16337271

指导教师：陈立文

二〇一八年五月十七日

# 目 录

<b>1 小组成员及分工 .....</b>	<b>1</b>
1.1 小组成员 .....	1
1.2 小组分工表及自评 .....	1
<b>2 实验一：跨交换实现 VLAN .....</b>	<b>2</b>
2.1 实验拓扑 .....	2
2.2 实验步骤 .....	2
2.2.1 步骤 1 .....	2
2.2.2 步骤 2: 路由器 1 设置 vlan10 .....	3
2.3 步骤 3: 设置路由器 1 设置 VLAN 20 .....	3
2.4 步骤 4: 设置路由器 1 端口的 trunk 模式 .....	4
2.5 步骤 5: 设置路由器 2 .....	6
2.6 步骤 6: 设置路由器 2 端口的 trunk 模式 .....	6
2.7 步骤 7: 验证 .....	6
2.8 实验思考 .....	9
<b>3 实验二：通过三层交换机实现 VLAN 间路由 .....</b>	<b>11</b>
3.1 实验拓扑 .....	11
3.2 实验步骤 .....	11
3.2.1 步骤 1: 连接线路并测试连通性 .....	11
3.2.2 步骤 2: 交换机 A 创建 VLAN10 .....	13
3.2.3 步骤 3: 交换机 A 创建 VLAN20 .....	13
3.2.4 步骤 4: 设置 A 与 B 连接的端口模式 .....	13
3.2.5 步骤 5: 交换机 B 创建 VLAN20 .....	14
3.2.6 步骤 6: 设置 B 与 A 连接的端口模式 .....	14
3.2.7 步骤 7: 测试 .....	14
3.2.8 步骤 8: 设置三层交换机 VLAN 间的通信 .....	14
3.2.9 步骤 9: 设置网关 .....	17
3.2.10 步骤 10: 测试是否 ping 通 .....	17

3.3	实验结果 .....	18
3.3.1	实验观察 .....	18
3.4	实验思考 .....	21
3.4.1	思考题一 .....	21
3.4.2	思考题二 .....	21
3.4.3	思考题三 .....	22
<b>4</b>	<b>问题三 .....</b>	<b>23</b>
	<b>附录 A 有附录吗？ .....</b>	<b>25</b>

# 1 小组成员及分工

## 1.1 小组成员

表 1.1 小组成员信息

组员姓名	学号
王永锋（组长）	16337237
颜彬	16337269
杨陈泽	16337271

## 1.2 小组分工表及自评

表 1.2 小组分工表

小组成员姓名	自评	分工
王永锋	100	实验 6-2 6-3 操作实践及报告编写及最终实验报告排版
颜彬	100	实验 6-2 6-3 操作实践实验 6-2 报告编写，
杨陈泽	100	实验 6-2 6-3 操作实践实验补充问题三实验及报告编写

## 2 实验一：跨交换实现 VLAN

### 2.1 实验拓扑

TODO: 画一个拓扑图，这个图和书本的图一样。

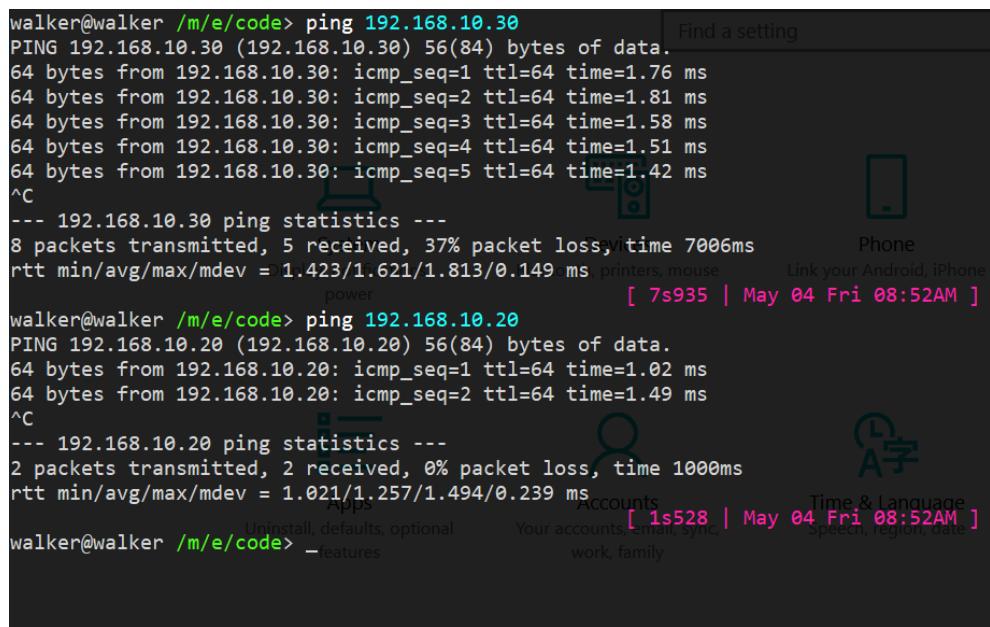
PC1, 我 PC2, 颜彬 PC3, 陈泽

### 2.2 实验步骤

#### 2.2.1 步骤 1

将我们的三台电脑按照拓扑图配置好 IP 地址，用网线将各电脑与交换机对应的端口相连。

然后检测三台电脑间能否互相 ping 通，下图 2.1展示了 PC1 ping PC2 与 PC3 的结果，都能够 ping 通，表明网络线路没有问题。



The screenshot shows a Mac OS X desktop with two terminal windows. The top window displays the command `walker@walker /m/e/code> ping 192.168.10.30` and its output, which shows successful ping results to IP 192.168.10.30. The bottom window displays the command `walker@walker /m/e/code> ping 192.168.10.20` and its output, which shows successful ping results to IP 192.168.10.20. The desktop background features icons for Phone, power, and Time & Language.

```
walker@walker /m/e/code> ping 192.168.10.30
PING 192.168.10.30 (192.168.10.30) 56(84) bytes of data.
64 bytes from 192.168.10.30: icmp_seq=1 ttl=64 time=1.76 ms
64 bytes from 192.168.10.30: icmp_seq=2 ttl=64 time=1.81 ms
64 bytes from 192.168.10.30: icmp_seq=3 ttl=64 time=1.58 ms
64 bytes from 192.168.10.30: icmp_seq=4 ttl=64 time=1.51 ms
64 bytes from 192.168.10.30: icmp_seq=5 ttl=64 time=1.42 ms
^C
--- 192.168.10.30 ping statistics ---
8 packets transmitted, 5 received, 37% packet loss, time 7006ms
rtt min/avg/max/mdev = 1.423/1.621/1.813/0.149 ms
power [ 7s935 | May 04 Fri 08:52AM ] Link your Android, iPhone
Phone
walker@walker /m/e/code> ping 192.168.10.20
PING 192.168.10.20 (192.168.10.20) 56(84) bytes of data.
64 bytes from 192.168.10.20: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.10.20: icmp_seq=2 ttl=64 time=1.49 ms
^C
--- 192.168.10.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 1.021/1.257/1.494/0.239 ms
Apps Accounts [ 1s528 | May 04 Fri 08:52AM ]
Time & Language
Uninstall, defaults, optional Your accounts, iCloud, sync, speech, region, date
work, family
walker@walker /m/e/code> -features
```

图 2.1 PC1 ping PC2 PC3

### 2.2.2 步骤 2: 路由器 1 设置 vlan10

该步骤需要路由器 1 将 PC1 对应的端口 (gig 0/5) 设置为 vlan 10。

相关设置的步骤可见图 2.2。

```
Interface IP-Address(Pri) OK? Status
19-S5750-1(config)#vlan 10
19-S5750-1(config-vlan)#name sales
19-S5750-1(config-vlan)#exit
19-S5750-1(config)#interface gig 0/5
19-S5750-1(config-if-GigabitEthernet 0/5)#switchport access vlan 10
19-S5750-1(config-if-GigabitEthernet 0/5)#_
```

图 2.2 路由器 1 设置 PC1 端口为 vlan 10

完成设置后, 由于 PC1 在 VLAN 10 中, 而 PC2, PC3 在默认的 VLAN1 中, 如果设置成功的话是 PC2 是无法 ping 通 PC1 的, 下面进行验证。

1. 使用指令 `show vlan id 10` 查看 vlan10 对应的端口, 可见图 2.3

```
Interface IP-Address(Pri) OK? Status
19-S5750-1(config)#vlan 10
19-S5750-1(config-vlan)#name sales
19-S5750-1(config-vlan)#exit
19-S5750-1(config)#interface gig 0/5
19-S5750-1(config-if-GigabitEthernet 0/5)#switchport access vlan 10
19-S5750-1(config-if-GigabitEthernet 0/5)#_
```

图 2.3 查看 VLAN 10 对应的端口

2. PC2 无法 ping 通 PC1, 可见图 2.4.

```
yb@yb-thinkpad-e450:~% ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
From 192.168.199.101 icmp_seq=1 Destination Host Unreachable
From 192.168.199.101 icmp_seq=2 Destination Host Unreachable
From 192.168.199.101 icmp_seq=3 Destination Host Unreachable
From 192.168.199.101 icmp_seq=4 Destination Host Unreachable
From 192.168.199.101 icmp_seq=5 Destination Host Unreachable
From 192.168.199.101 icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.10.10 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6110ms
pipe 4
yb@yb-thinkpad-e450:~%
```

图 2.4 PC2 无法 ping 通 PC1

### 2.3 步骤 3: 设置路由器 1 设置 VLAN 20

该步骤要求将 PC2 对应的交换机的端口设置为 VLAN 20。这时候, 原本能够相互 ping 通的 PC2 与 PC3 也开始不能相互 ping 通。

相关设置的步骤可见图 2.5.

```
19-S5750-1(config-if-GigabitEthernet 0/15)#vlan 20
19-S5750-1(config-vlan)#name technical
19-S5750-1(config-vlan)#exit
19-S5750-1(config)#inter gig 0/15
19-S5750-1(config-if-GigabitEthernet 0/15)#switchport access vlan 20
```

图 2.5 设置 VLAN 20

设置后，我们进行验证，查看路由器的配置与检查 PC2 与 PC3 是否能够 ping 通。

1. 使用指令 `show vlan id 20` 查看 vlan20 对应的端口，可见图 2.6

```
19-S5750-1(config-if-GigabitEthernet 0/15)#show vlan id 20
VLAN Name          Status    Ports
-----  -----
  20  technical      STATIC   Gi0/15
```

图 2.6 查看 VLAN 20 对应的端口

2. PC2 无法 ping 通 PC3，可见图 2.7.

```
yb@yb-thinkpad-e450:~% ping 192.168.10.30
PING 192.168.10.30 (192.168.10.30) 56(84) bytes of data.
From 192.168.199.101 icmp_seq=1 Destination Host Unreachable
From 192.168.199.101 icmp_seq=2 Destination Host Unreachable
From 192.168.199.101 icmp_seq=3 Destination Host Unreachable
From 192.168.199.101 icmp_seq=4 Destination Host Unreachable
From 192.168.199.101 icmp_seq=5 Destination Host Unreachable
From 192.168.199.101 icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.10.30 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6130ms
pipe 4
yb@yb-thinkpad-e450:~%
```

图 2.7 PC2 无法 ping 通 PC3

## 2.4 步骤 4::: 设置路由器 1 端口的 trunk 模式

该步骤要求设置两路由器相连的端口 (0/24) 设置为 `trunk` 模式。设置步骤可见图 2.8。

```
19-S5750-1(config-if-GigabitEthernet 0/15)#interface gig 0/24
19-S5750-1(config-if-GigabitEthernet 0/24)#switchport mode trunk
```

图 2.8 将路由器 1 的 0/24 端口设置为 trunk 模式

设置完成后，使用 `show interface gig 0/24 switchport` 该指令验证，可见图 2.9。

Interface	Switchport Mode	Access Native VLAN	Protected VLAN lists
GigabitEthernet 0/24	enabled	TRUNK	1 1 Disabled ALL

图 2.9 验证路由器 1 的 trunk 设置

这个时候由于路由器 2 上的端口尚未设置，因此仍然不能够 ping 通。

## 2.5 步骤 5: 设置路由器 2

由于设置路由器 2 的指令与设置路由器 1 的指令类似，这里并不放设置的截图，仅放验证的截图。

由图 2.10 可知，该次设置成功。

19-S5750-2#show vlan id 20		Status	Ports
20 technical	STATIC	Gi0/5	
19-S5750-2#show interfaces Gi0/5 switchport	Switchport Mode	Access Native Protected VLAN lists	
<hr/>			
GigabitEthernet 0/5	enabled	ACCESS	20 1 Disabled ALL

图 2.10 验证路由器 2 的 vlan20 设置

此时 PC2, PC3 之间仍不能够 ping 通。

## 2.6 步骤 6: 设置路由器 2 端口的 trunk 模式

路由器 2 的 gigabitethernet 0/24 端口与路由器 1 之间相连，需要设置为 trunk 模式用以转发链路帧，设置后，验证设置如图 2.11，可知设置成功。

19-S5750-2#show vlan id 20		Status	Ports
20 technical	STATIC	Gi0/5, Gi0/24	
19-S5750-2#show interfaces Gi0/24 switchport	Switchport Mode	Access Native Protected VLAN lists	
<hr/>			
GigabitEthernet 0/24	enabled	TRUNK	1 1 Disabled ALL

图 2.11 验证 PC2 的 trunk 模式设置

## 2.7 步骤 7: 验证

这一个步骤我们需要验证 PC2 与 PC3 之间能相互通信，但 PC1 与 PC3 不能相互通信。

因此我们完成了以下几个问题

观察一

主机之间能否互相通信？

TODO: 需要互 ping 的图 wyf

## 观察二

能否检测到 PC1, PC2, PC3 的 ICMP 包?

当一台主机能 ping 到另一台主机时, wireshark 可以捕捉到另一台主机的 ICMP response 包。

在本拓扑中, PC3 可以捕捉到 PC2 的 ICMP 包, 但无法捕捉到 PC1 的 ICMP 包。PC2 可以捕捉到 PC3 可以捕捉到 PC2 的 ICMP 包, 但无法捕捉到 PC1 的 ICMP 包。PC2 可以捕捉到 PC3 的 ICMP 包, 但无法捕捉到 PC1 的 ICMP 包。PC1 由于不与 PC2 和 PC3 在同一个 VLAN 中, 故其无法捕捉到 PC2 和 PC3 的 ICMP 包。

## 观察三

能否捕获到 Trunk 链路上的 VLAN ID? 请讨论原因。

交换机的 vlan 模式分为 access, trunk 和 hybrid 三种。

在 trunk 模式的接收端口中, 所有进入的链路层帧, 有 tag 时, 不改变原来的 tag, 直接转发该帧; 若帧无 tag, 则加上 PVID (端口默认 VLAN 的 ID, 默认为 1) 和加上默认优先级, 并转发。

在 trunk 模式的发送端口中, 若帧带有 tag (且 VID 与 PVID 不同), 则不修改 tag 直接转发该包。若帧不带有 tag, 则直接进行转发。

在 access 模式的发送端口中, 若 VID 等于 PVID, 则去掉 tag 再转发。若 VID 不等于 PVID, 则不转发。

综上讨论, 所有主机不可能捕获到 Trunk 链路上的 VID。这是因为所有主机通过 access 模式连接到路由器。所有链路层帧要么被 access 模式的端口丢弃, 要么被去除 tag。所有无法捕获到 VID。

## 观察四

- 查看交换机的地址表。清楚地址表, 适当更改、增加网线接口, 然后观察, 分析地址表的形成与变化过程 (配合 wireshark 分析泛洪现象)。
- show mac-address-table 命令显示的 MAC 地址与在命令提示符下通过 ifconfig /all 命令显示的 mac 地址是否相同。

以下讨论基于下列假设: A 主机 192.168.10.200 B 主机 192.168.10.20 两个主机共同处于 10 号 VLAN 中。展示的 wireshark 截图中, wireshark 均运行在 B 主机。

在交换机刚启动时, 其 mac 地址表为空。当一个帧经过交换机时, 交换机会提取源 mac 地址。若源 mac 地址已经在地址表中, 则该表项的失效时间被刷新 (重新

模式	方向	条件	应该处理方式	是否支持	备注
Access	(接收)	Tagged = PVID	不接收	不支持	转发
Access	(接收)	Tagged /= PVID	不接收	支持	设置过滤模式
Access	(接收)	从 PC 接收 Untagged	增加 tag=PVID	支持	
Access	发送	Tagged = PVID	转发删除 tag	支持	
Access	发送	Tagged /= PVID	不转发不处理	不支持	依然转发删除 tag, 可设置路由表过滤
Access	发送	Untagged	无此情况		
Tag	(接收)	Tagged = PVID	接收 不修改 tag	支持	
Tag	(接收)	Tagged /= PVID	接收 不修改 tag	支持	
Tag	(接收)	从 PC 接收 Untagged	增加 tag=PVID	支持	
Tag	发送	Tagged = PVID	路由表允许转发则删除 tag	不支持	依然透传, 不会出 Untag 包
Tag	发送	Tagged /= PVID	路由表允许转发则不修改 tag	支持	
Tag	发送	Untagged	无此情况		
Hybrid	(接收)	Tagged = PVID	不修改 tag	支持	
Hybrid	(接收)	Tagged /= PVID	不修改 tag	支持	
Hybrid	(接收)	从 PC 接收 Untagged	增加 tag=PVID	支持	
Hybrid	发送	Tagged = PVID	路由表允许转发则删除 tag	不支持	
Hybrid	发送	Tagged /= PVID	路由表允许转发则不修改 tag	支持	
Hybrid	发送	Untagged	进入端口为 Untag, 路由表允许转发则发送 Untag	支持	支持 Untag 包

图 2.12 补充说明

回到 300s)。否则，交换机将源 mac 地址和输入端口这一对信息存入 MAC 地址表中，并设置失效时间到 300s。每当一个帧进入交换机时，交换机会检查其目的 MAC 地址。若地址在 MAC 地址表中，则交换机根据地址表的信息将帧送到输出端口。若该地址不在表中，则交换机将帧送出到每一个端口。特别地，由于没有一个源 MAC 地址是广播地址 ('FF:FF:FF:FF:FF:FF')，故广播地址不可能出现在 MAC 地址表中(不可能被交换机学习到)。故所有以广播地址为目的地址的帧，都会被广播。下图显示了 A 主机 ping 向 B 主机时，ARP 请求、ARP 应答和 ICMP 协议的抓包情况。

246 203.776658747 00:88:99:00:13:ab	ARP	62 Who has 192.168.10.20? Tell 192.168.10.200
247 203.776697778 LcfHeFe_99:89:41	ARP	44 192.168.10.20 is at 68:f7:28:99:89:41
248 203.776917514 192.168.10.200	192.168.10.20	ICMP
249 203.776961334 192.168.10.20	192.168.10.200	ICMP
250 204.778919543 192.168.10.200	192.168.10.20	ICMP
251 204.778957837 192.168.10.20	192.168.10.200	ICMP
252 205.779767468 192.168.10.200	192.168.10.20	ICMP
253 205.779905642 192.168.10.20	192.168.10.200	ICMP
254 206.783920580 192.168.10.200	192.168.10.20	ICMP
255 206.783950280 192.168.10.20	192.168.10.200	ICMP
256 206.783950280 192.168.10.20	192.168.10.200	ICMP
257 206.783950280 192.168.10.20	192.168.10.200	ICMP
258 206.783950280 192.168.10.20	192.168.10.200	ICMP
259 206.783950280 192.168.10.20	192.168.10.200	ICMP
260 206.783950280 192.168.10.20	192.168.10.200	ICMP
261 206.783950280 192.168.10.20	192.168.10.200	ICMP
262 206.783950280 192.168.10.20	192.168.10.200	ICMP
263 206.783950280 192.168.10.20	192.168.10.200	ICMP
264 206.783950280 192.168.10.20	192.168.10.200	ICMP
265 206.783950280 192.168.10.20	192.168.10.200	ICMP
266 206.783950280 192.168.10.20	192.168.10.200	ICMP
267 206.783950280 192.168.10.20	192.168.10.200	ICMP
268 206.783950280 192.168.10.20	192.168.10.200	ICMP
269 206.783950280 192.168.10.20	192.168.10.200	ICMP
270 206.783950280 192.168.10.20	192.168.10.200	ICMP
271 206.783950280 192.168.10.20	192.168.10.200	ICMP
272 206.783950280 192.168.10.20	192.168.10.200	ICMP
273 206.783950280 192.168.10.20	192.168.10.200	ICMP
274 206.783950280 192.168.10.20	192.168.10.200	ICMP
275 206.783950280 192.168.10.20	192.168.10.200	ICMP
276 206.783950280 192.168.10.20	192.168.10.200	ICMP
277 206.783950280 192.168.10.20	192.168.10.200	ICMP
278 206.783950280 192.168.10.20	192.168.10.200	ICMP
279 206.783950280 192.168.10.20	192.168.10.200	ICMP
280 206.783950280 192.168.10.20	192.168.10.200	ICMP
281 206.783950280 192.168.10.20	192.168.10.200	ICMP
282 206.783950280 192.168.10.20	192.168.10.200	ICMP
283 206.783950280 192.168.10.20	192.168.10.200	ICMP
284 206.783950280 192.168.10.20	192.168.10.200	ICMP
285 206.783950280 192.168.10.20	192.168.10.200	ICMP
286 206.783950280 192.168.10.20	192.168.10.200	ICMP
287 206.783950280 192.168.10.20	192.168.10.200	ICMP

图 2.13

每当主机更换 IP 地址时，它都会告知其所有邻居。如图 2.13 所示。

假设主机 A 将其 IP 地址更换成 192.168.10.111。主机 A 会首先使用 ARP 协议请求自己的 IP 地址对应的 mac 地址。这一步的目的是确保自己的 IP 不与子网内的其他 IP 地址冲突。当 IP 地址不冲突时，该 ARP 请求应该得不到任何回应。主

机 A 在等待一段时间且没有接收到 ARP 应答时，可以确信自己的 IP 地址不重复，于是主机 A 发送 Gratuitous ARP 帧。Gratuitous ARP 是一种主动 ARP 请求，它的作用是告知其他主机，本主机的 IP 地址和 MAC 地址，省去其他主机发送 ARP 请求的麻烦。Gratuitous ARP 是一种 ARP 请求，但该请求不会收到任何应答。

179 124.237852270 00:88:99:00:13:ab	ARP	62 Who has 192.168.10.111? Tell 0.0.0.0
180 125.238996665 00:88:99:00:13:ab	ARP	62 Who has 192.168.10.111? Tell 0.0.0.0
181 126.238815661 00:88:99:00:13:ab	ARP	62 Who has 192.168.10.111? Tell 0.0.0.0
182 127.238822374 00:88:99:00:13:ab	ARP	62 Gratuitous ARP for 192.168.10.111 (Request)

图 2.14 补充说明

麻烦唉，第二题没法做。没有 show mac-address-table 命令截图啊。也不知道是不是相同。。。怎么办好呢

#### 观察五

判断实验是否达到预期目标。

在本次实验中，我们所有的实验现象都符合我们的预期。

同一个交换机中，同一个 VLAN 内的主机可以 ping 通，不同 VLAN 内的主机无法 ping 通。在不同交换机中，用 trunk 模式相连两个交换机时，同一个 VLAN 内的主机可以连通。若不设置 trunk 模式，则跨交换机时主机无法 ping 通。

同时，我们还根据实验现象给出了思考和解释。VLAN 的三种访问模式是 access, trunk 和 hybrid. 在本实验中我们涉及到的是 access (交换机与主机相连) 和 trunk (交换机之间互联)。这三种模式都对链路层帧的 tag 情况有不同的行为。所有的实验现象都符合访问模式的特点。前面的题目中，我们给出了相关的解释。

## 2.8 实验思考

思考题来自于老师的 pdf 材料.

#### 思考题一

说明 vlan 技术中的 trunk 模式端口的意义。

如图图 2.12所示。

配置为 trunk 模式的接收端口中，若其接收到不带 tag 的帧，则自动为其加上 PVID (Port VLAN ID) 和默认优先级。否则，该帧的 tag 不被修改，直接进行转发。

配置为 trunk 模式的发送端口中，若帧带有 tag 的 VLAN ID 恰好为 PVID，则去掉 VLAN ID tag 再转发。否则，不改变 tag 直接转发。

其中 PVID (Port VLAN ID) 是端口的默认 VLAN ID。若没有被配置，trunk 端口的 PVID 为 VLAN 1。

### 思考题二

如何查看 trunk 接口允许哪些 VLAN 通过？

可以使用 `show interface gig 0/24 switchport` 命令来查看，效果如下图所示。其中红箭头表示允许的 vlan 为所有 (all)。

```
0-S5750-1#show interface gig 0/24 switchport
Interface          Switchport Mode     Access Native Protected VLAN lists
-----
igabitEthernet 0/24      enabled      TRUNK      1      1      Disabled ALL
0-S5750-1#
```

图 2.15 查看允许 VLAN

### 思考题三

实验开始前请先确定三台 PC 机处于一个网段里面。为什么做这样的限定？

我们这一次实验并没有设计默认网关，也没有设置路由转发，因此当发往处于不同网段的主机时，不可能发送过去。

### 3 实验二：通过三层交换机实现 VLAN 间路由

#### 3.1 实验拓扑

TODO: 书本图片 P177

#### 3.2 实验步骤

分析: 本实验的预期是将??中的三台计算机, 划分进不同的 VLAN, 并让处于不同 VLAN 的计算机互相隔离. 然后启用三层交换机的路由功能, 让已经隔离的计算机能互相通信. (如: 隔离后 PC1 能 ping 通 PC2,PC3).

##### 3.2.1 步骤 1: 连接线路并测试连通性

1. 设置每一台主机的 IP 地址

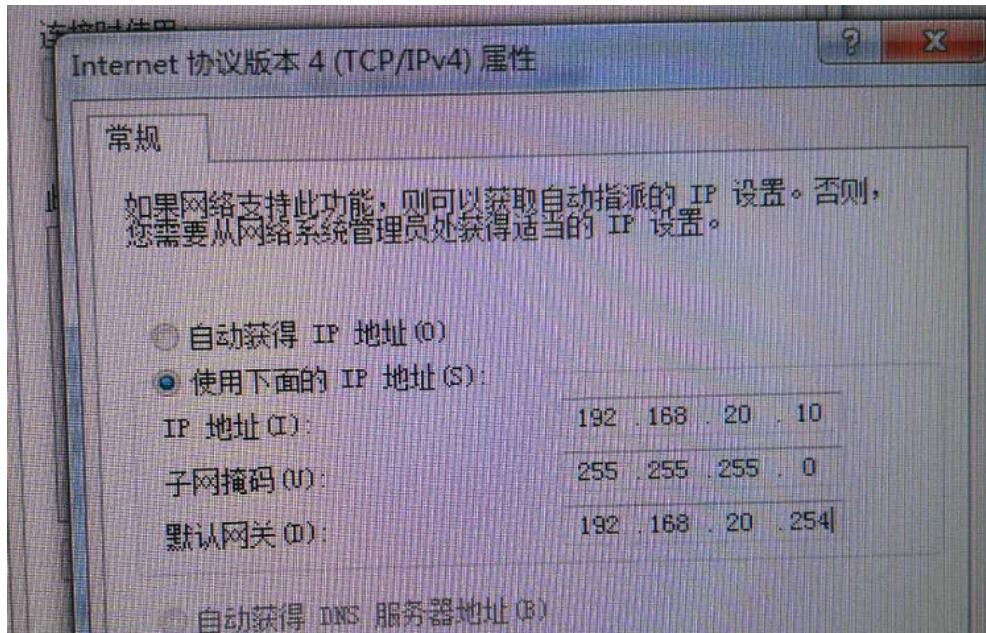


图 3.1 PC1 设置 IP 地址的截图

2. 测试 PC1, PC2, PC3 的连通性, 发现 PC1 无法 ping 通 PC2, PC3, 其他的 PC2 和 PC3 可以相互 ping 通。

```
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.10.20

正在 Ping 192.168.10.20 具有 32 字节的数据:
来自 172.16.4.2 的回复: 无法访问目标主机。

192.168.10.20 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 <0% 丢失>,
Control-C
^C
C:\Users\Administrator>ping 192.168.10.30

正在 Ping 192.168.10.30 具有 32 字节的数据:
来自 172.16.4.2 的回复: 无法访问目标主机。

192.168.10.30 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 <0% 丢失>,
Control-C
^C
C:\Users\Administrator>
```

图 3.2 PC1 无法 ping 通 PC2,PC3

### 思考

PC1 的网段不同于 PC2,PC3, 请讨论原因

这里做的是不同 vlan 间通过路由转发消息的实验。如果 PC1 与 PC2, PC3 所在网段相同, 那么 PC1 在发送 IP 包的时候就会认为在同一个子网中, 永远也不会发往默认网关。

3. 使用 `show ip route` 命令查看三层交换机的路由表, 并记录

```
Password: usage
20-S5750-1#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default

Gateway of last resort is not set
20-S5750-1#
```

图 3.3 查看三层交换机的路由表

### 3.2.2 步骤 2: 交换机 A 创建 VLAN10

该步骤需要在交换机 A 上创建 VLAN10, 并将端口 0/5(即 PC1 对应的接口)划分到 VLAN10 中.

```
20-S5750-1(config)#vlan 10
20-S5750-1(config-vlan)#name technical
20-S5750-1(config-vlan)#exit
20-S5750-1(config)#interface gig 0/5
20-S5750-1(config-if-GigabitEthernet 0/5)#switchport access vlan 10
20-S5750-1(config-if-GigabitEthernet 0/5)#exit
20-S5750-1(config)#exit
20-S5750-1#*Apr  8 03:07:54: %SYS-5-CONFIG_I: Configured from console by console
```

图 3.4 交换机 A 创建 VLAN 10

操作完成后, 使用 `show vlan id 10` 验证实验操作.

```
20-S5750-1#show vlan id 10
VLAN Name                               Status    Ports
---- -----
  10 technical                           STATIC   Gi0/5
20-S5750-1#
```

图 3.5 查看 vlan 10 信息

### 3.2.3 步骤 3: 交换机 A 创建 VLAN20

该步骤需要在交换机 A 上创建 VLAN20, 并将端口 0/15(即 PC2 对应端口)划分到 VLAN20 中.

```
20-S5750-1(config)#vlan 20
20-S5750-1(config-vlan)#name sales
20-S5750-1(config-vlan)#exit
20-S5750-1(config)#interface gig 0/15
20-S5750-1(config-if-GigabitEthernet 0/15)#switchport access vlan 20
20-S5750-1(config-if-GigabitEthernet 0/15)#exit
20-S5750-1(config)#exit
20-S5750-1#*Apr  8 03:09:27: %SYS-5-CONFIG_I: Configured from console by console
```

图 3.6 创建 VLAN20

操作完成后, 使用 `show vlan id 20` 验证实验操作.

### 3.2.4 步骤 4: 设置 A 与 B 连接的端口模式

将交换机 A 上与交换机 B 相连的端口 (假设为端口 0/24) 定义为 tag VLAN 模式。设置步骤可见

操作完成后, 使用 `show interface gig 0/24 switchport` 验证设置.

VLAN Name	Status	Ports
20 sales	STATIC	Gi0/15

图 3.7 查看 VLAN20

```

20-S5750-1#config term
Enter configuration commands, one per line. End with CNTL/Z.
20-S5750-1(config)#interface gig 0/24
20-S5750-1(config-if-GigabitEthernet 0/24)#switchport mode trunk
% Unknown command.

20-S5750-1(config-if-GigabitEthernet 0/24)#switchport mode trunk
20-S5750-1(config-if-GigabitEthernet 0/24)#exit
20-S5750-1(config)#exit
20-S5750-1#*Apr 8 03:11:10: %SYS-5-CONFIG_I: Configured from console by console
...

```

图 3.8 设置端口模式

### 3.2.5 步骤 5: 交换机 B 创建 VLAN20

在交换机 B 上创建 VLAN20, 并将端口 0/5 划分到 VLAN20 中. 如图 3.10 操作完成后, 使用 `show vlan id 20` 验证实验操作. 如图 3.11

### 3.2.6 步骤 6: 设置 B 与 A 连接的端口模式

将交换机 B 上与交换机 A 相连的端口 (假设为端口 0/24) 定义为 tag VLAN 模式。设置步骤可见图 3.12

操作完成后, 使用 `show interface gig 0/24 switchport` 验证设置. 见图 3.13

### 3.2.7 步骤 7: 测试

1. 测试 PC2 与 PC3 的连通性, 发现 PC2 与 PC3 能够 ping 通。
2. 测试 PC1 与 PC2 的连通性从图中可以看出,ifconfig 指令指示出 PC2 的 IP 地址。其后的 ping 中, 与 PC3 可以连通, 与 PC1 无法连通。
3. 使用 `show ip route` 命令查看三层交换机的路由表, 并与步骤 1 比较. 如图 3.16, 步骤一中路由表可见图 3.3。他们目前都是空的。

### 3.2.8 步骤 8: 设置三层交换机 VLAN 间的通信

将交换机 A 配置成具有路由器的功能, 配置不同 VLAN 接口的地址.

Interface	Switchport Mode	Access	Native	Protected	VLAN lists
GigabitEthernet 0/24	enabled	TRUNK	1	1	Disabled ALL

图 3.9 验证设置

```

20-S5750-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
20-S5750-2(config)#vlan 20
20-S5750-2(config-vlan)#name sales
20-S5750-2(config-vlan)#interface Giga 0/5
20-S5750-2(config-if-GigabitEthernet 0/5)#switchport access vlan 20
20-S5750-2(config-if-GigabitEthernet 0/5)#exit
20-S5750-2(config)#interface Giga 0/24
20-S5750-2(config-if-GigabitEthernet 0/24)#switchport mode trunk
20-S5750-2(config-if-GigabitEthernet 0/24)#exit

```

图 3.10 交换机 B 创建 VLAN20

VLAN Name	Status	Ports
20 sales	STATIC	Gi0/5, Gi0/24

Interface	Switchport Mode	Access	Native	Protected	VLAN lists
GigabitEthernet 0/5	enabled	ACCESS	20	1	Disabled ALL

Interface	Switchport Mode	Access	Native	Protected	VLAN lists
GigabitEthernet 0/24	enabled	TRUNK	1	1	Disabled ALL

图 3.11 在交换机 B 上查看 vlan20

```

20-S5750-2(config)#interface Giga 0/24
20-S5750-2(config-if-GigabitEthernet 0/24)#switchport mode trunk
20-S5750-2(config-if-GigabitEthernet 0/24)#exit

```

图 3.12 设置端口模式

Interface	Switchport Mode	Access	Native	Protected	VLAN lists
GigabitEthernet 0/5	enabled	ACCESS	20	1	Disabled ALL

图 3.13 设置端口模式

```

yb@yb-thinkpad-e450:~% ifconfig
enp0s25 Link encap:Ethernet HWaddr 68:f7:28:99:89:41
          inet addr:192.168.10.20 Bcast:192.168.10.255 Mask:255.255.255.0
          inet6 addr: fe80::6af7:28ff:fe99:8941/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:66 errors:0 dropped:0 overruns:0 frame:0
            TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:16624 (16.6 KB) TX bytes:29531 (29.5 KB)
            Interrupt:20 Memory:d0700000-d0720000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:65536 Metric:1
            RX packets:814 errors:0 dropped:0 overruns:0 frame:0
            TX packets:814 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:64668 (64.6 KB) TX bytes:64668 (64.6 KB)

yb@yb-thinkpad-e450:~% ping 192.168.20.10
connect: Network is unreachable
yb@yb-thinkpad-e450:~% ping 192.168.10.30
PING 192.168.10.30 (192.168.10.30) 56(84) bytes of data.
64 bytes from 192.168.10.30: icmp_seq=1 ttl=64 time=0.362 ms
64 bytes from 192.168.10.30: icmp_seq=2 ttl=64 time=0.809 ms
64 bytes from 192.168.10.30: icmp_seq=3 ttl=64 time=0.848 ms
64 bytes from 192.168.10.30: icmp_seq=4 ttl=64 time=0.876 ms
^C
--- 192.168.10.30 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.362/0.723/0.876/0.212 ms
yb@yb-thinkpad-e450:~% █

```

图 3.14

```

C:\Users\Administrator>ping 192.168.10.20
正在 Ping 192.168.10.20 具有 32 字节的数据:
来自 172.16.4.2 的回复: 无法访问目标主机。

192.168.10.20 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
Control-C
^C
C:\Users\Administrator>ping 192.168.10.30

正在 Ping 192.168.10.30 具有 32 字节的数据:
来自 172.16.4.2 的回复: 无法访问目标主机。

192.168.10.30 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
Control-C
^C
C:\Users\Administrator>

```

图 3.15 PC1 与 PC2 无法 ping 通

```

PASSWORD.
20-S5750-1#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
20-S5750-1#

```

图 3.16 查看路由表

```

Enter configuration commands, one per line. End with Ctrl/Z.
20-S5750-1(config)#interface vlan 10
20-S5750-1(config-if-VLAN 10)*Apr 8 03:22:40: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 10, changed state to up.
20-S5750-1(config-if-VLAN 10)#ip address 192.168.20.254 255.255.255.0
20-S5750-1(config-if-VLAN 10)#exit
20-S5750-1(config)#interface vlan 20
20-S5750-1(config-if-VLAN 20)*Apr 8 03:23:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface VLAN 20, changed state to up.
ip
% Incomplete command.
  ip
  ^VPN
20-S5750-1(config-if-VLAN 20)#ip address 192.168.10.254 255.255.255.0
% Invalid input detected at '' marker.

20-S5750-1(config-if-VLAN 20)#ip address 192.168.10.254 255.255.255.0
20-S5750-1(config-if-VLAN 20)#exit
20-S5750-1(config)#exit
20-S5750-1#"Apr 8 03:24:08: %SYS-5-CONFIG_I: Configured from console by console

```

图 3.17 设置 vlan 间通信

## 讨论

虚拟接口 VLAN10 与虚拟接口 VLAN20 的 IP 地址能不能在同一个网段? 回答步骤 1 提出的问题.

不能. 如果在同一个子网中, 主机不会尝试将这个数据包发往默认网关, 这也就意味着交换机的路由模块无法收到这个数据包.

### 3.2.9 步骤 9: 设置网关

该步骤设置网关可见步骤一, 已经将 VLAN 10 和 VLAN 20 内的主机分别将默认网关设为 192.168.10.254, 192.168.20.254。

### 3.2.10 步骤 10: 测试是否 ping 通

实验测试, 使用 ping 命令查看不同 VLAN 内的主机能够互相 ping 通. 启动监控软件 Wireshark, 互相 ping 两台计算机并观察.

关于此步骤结果, 可见下一节“实验结果”。

### 3.3 实验结果

#### 3.3.1 实验观察

观察一

计算机之间是否连通?

能够 ping 通。

```
yb@yb-thinkpad-e450:~>
<function f at 0x7f38053e6598>
>>> def f():
...     return g
...
>>> def g():
...     return f
...
>>> f()
<function g at 0x7f3804c8ad08>
>>> g()
<function f at 0x7f3806b40f28>
>>> f()
<function g at 0x7f3804c8ad08>
>>> f()()
<function f at 0x7f3806b40f28>
>>> f()()
<function f at 0x7f3806b40f28>
>>> de
KeyboardInterrupt
>>>
KeyboardInterrupt
>>>
ubgub@thinkpad-e450:~% sudo route add default gw 192.168.10.254
ubgub@thinkpad-e450:~% ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
^C
--- 192.168.20.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3079ms
ubgub@thinkpad-e450:~% ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=127 time=0.265 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=127 time=0.447 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=127 time=0.479 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=127 time=0.454 ms
64 bytes from 192.168.20.10: icmp_seq=5 ttl=127 time=0.444 ms
64 bytes from 192.168.20.10: icmp_seq=6 ttl=127 time=0.152 ms
64 bytes from 192.168.20.10: icmp_seq=7 ttl=127 time=0.193 ms
^C
--- 192.168.20.10 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6136ms
rtt min/avg/max/mdev = 0.152/0.347/0.479/0.131 ms
yb@yb-thinkpad-e450:~%
```

图 3.18 PC1 与 PC2, PC3 能够 ping 通

观察二

能否监控到 PC1, PC2, PC3 的 ICMP 包?

TODO: 插入图片 id005.png 从图中可以看出, 主机 PC2 成功抓到了 PC1 和 PC3 的 ICMP 包。

观察三

使用 `show ip route` 查看三层交换机的路由表, 并与步骤 1 比较.

与拓扑图比较, 该路由表中的表项的意思为:

1. 表示与该交换机直连着的 VLAN 相应的子网范围。
2. 表示该交换机的端口 IP。

观察四

在命令提示符窗口下, 使用 `route print` 是否能够查看实验设置的路由?

```
20-S5750-1(config-if-VLAN 20)#ip address 192.168.10.254 255.255.255.0
20-S5750-1(config-if-VLAN 20)#exit
20-S5750-1(config)#exit
20-S5750-1#*Apr 8 03:24:08: %SYS-5-CONFIG_I: Configured from console by console

20-S5750-1#show ip route
    Proxy
Codes: C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C     192.168.10.0/24 is directly connected, VLAN 20
C     192.168.10.254/32 is local host.
C     192.168.20.0/24 is directly connected, VLAN 10
C     192.168.20.254/32 is local host.
20-S5750-1#
```

图 3.19 三层交换机路由表

如图 3.20所示，可以在默认网关处看到设置的路由。

路由表					
网络目标	网络掩码	网关	接口	跃点数	
0.0.0.0	0.0.0.0	192.168.20.254	192.168.20.10	266	
127.0.0.0	255.0.0.0		在链路上	127.0.0.1	306
127.0.0.1	255.255.255.255		在链路上	127.0.0.1	306
127.255.255.255	255.255.255.255		在链路上	127.0.0.1	306
169.254.0.0	255.255.0.0		在链路上	169.254.205.159	286
169.254.0.0	255.255.0.0		在链路上	169.254.241.129	266
169.254.205.159	255.255.255.255		在链路上	169.254.205.159	286
169.254.241.129	255.255.255.255		在链路上	169.254.241.129	266
169.254.255.255	255.255.255.255		在链路上	169.254.205.159	286
169.254.255.255	255.255.255.255		在链路上	169.254.241.129	266
192.168.20.9	255.255.255.0		在链路上	192.168.20.10	266
192.168.20.10	255.255.255.255		在链路上	192.168.20.10	266
192.168.20.255	255.255.255.255		在链路上	192.168.20.10	266
192.168.74.0	255.255.255.0		在链路上	192.168.74.1	276
192.168.74.1	255.255.255.255		在链路上	192.168.74.1	276
192.168.74.255	255.255.255.255		在链路上	192.168.74.1	276
192.168.164.0	255.255.255.0		在链路上	192.168.164.1	276
192.168.164.1	255.255.255.255		在链路上	192.168.164.1	276
192.168.164.255	255.255.255.255		在链路上	192.168.164.1	276
224.0.0.0	240.0.0.0		在链路上	127.0.0.1	306
224.0.0.0	240.0.0.0		在链路上	192.168.74.1	276
224.0.0.0	240.0.0.0		在链路上	192.168.164.1	276
224.0.0.0	240.0.0.0		在链路上	192.168.20.10	266
224.0.0.0	240.0.0.0		在链路上	169.254.241.129	266
224.0.0.0	240.0.0.0		在链路上	169.254.205.159	286
255.255.255.255	255.255.255.255		在链路上	127.0.0.1	306
255.255.255.255	255.255.255.255		在链路上	192.168.74.1	276
255.255.255.255	255.255.255.255		在链路上	192.168.164.1	276
255.255.255.255	255.255.255.255		在链路上	192.168.20.10	266
255.255.255.255	255.255.255.255		在链路上	169.254.241.129	266
255.255.255.255	255.255.255.255		在链路上	169.254.205.159	286

图 3.20 打印主机路由表

## 3.4 实验思考

思考题来自书本与老师提供的 PDF 材料.

### 3.4.1 思考题一

思考题一

实验用到了三层交换机的路由功能, 为什么在 VLAN 配置好 IP 地址之后, 不同的 VLAN 间 (PC1,PC2) 就可以相互通信了?

这里的问题是, 为什么不需要设置转发表, 只需要设置 IP 地址, 不同的 VLAN 就可以相互通信呢?

这里我们需要理解 IP 包的转发原理。由前面的图我们可以看到路由器的转发表会自动加上直连的子网和端口 IP

### 3.4.2 思考题二

思考题二

请使用 `show ip route` 命令查看三层交换机的路由表, 并说明每个条目表示什么?

```
20-S5750-1(config-if-VLAN 20)#ip address 192.168.10.254 255.255.255.0
20-S5750-1(config-if-VLAN 20)#exit
20-S5750-1(config)#exit
20-S5750-1#*Apr  8 03:24:08: %SYS-5-CONFIG_I: Configured from console by console

20-S5750-1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
      O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default
      Gateway of last resort is no set

C    192.168.10.0/24 is directly connected, VLAN 20
C    192.168.10.254/32 is local host.
3 C    192.168.20.0/24 is directly connected, VLAN 10
C    192.168.20.254/32 is local host.

20-S5750-1#
```

图 3.21

### 3.4.3 思考题三

#### 思考题三

(跨交换机的不同 vlan 间通信) 若要 PC1 和 PC3 相互通信, 需要怎么进行配置.

在这里, 经过测试, 在前面的配置的基础上, 已经可以直接 ping 通。

在另一种情况中, 如果两台交换机各自具有两个不同的 VLAN, 可以在交换机中各自增加一个与对面 VLAN 一致的网关, 作为一个虚接口, 就可以连通了。

## 4 问题三

该部分主要解决这样的问题：跨交换机不借助 trunk 模式实现 VLAN 通信，如何做到？

我们使用了以下的方式来实现：

跨交换机实现 VLAN 通信，而不借助 trunk 模式，我们可以将两个交换机用两条跳线连接起来，交换机 A 的 24 号端口连交换机 B 的 24 号端口，A 的 23 号端口连 B 的 23 号端口，然后按照下面的拓扑图，PC1 属于交换机 A 的 VLAN10，PC2 属于交换机 A 的 VLAN20，PC3 属于交换机 B 的 VLAN20，PC4 属于交换机 B 的 VLAN10，然后再将交换机 A 和 B 的 24 号端口划分为 VLAN10，交换机 A 和 B 的 23 号端口划分为 VLAN20。

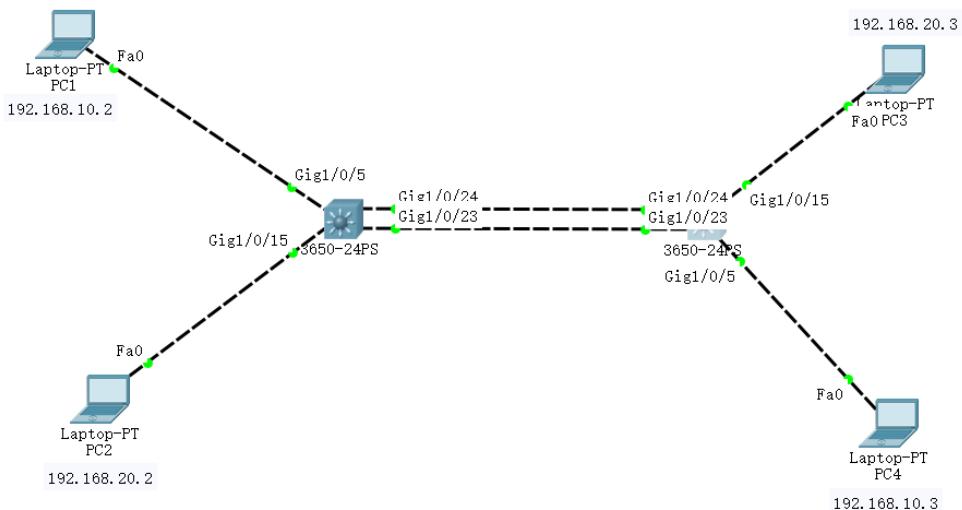


图 4.1 拓扑图

下面测试 PC3 与 PC2 的互联（它们是属于同一 VLAN 下，但是在不同交换机，并且没有借助 trunk 模式）：

结果是，PC3 与 PC2 是可以互联的，因为 PC3 发出的报文是先在交换机 B 里面广播给所有属于 VLAN20 的端口，即就是 23 号端口，然后交换机 B 的 23 号端口会将数据转给交换机 A 的 23 号端口，交换机 A 又会将该报文在自己里面广播给所有属于 VLAN20 的端口，即就是 15 号端口，所以 PC4 会收到来自于 PC3 的报文，而 PC4 发送给 PC3 的报文也是按照这个流程转发给 PC3。

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

图 4.2 ping 通图

## 附录 A 有附录吗？

TODO: 可能有附录，先留着？