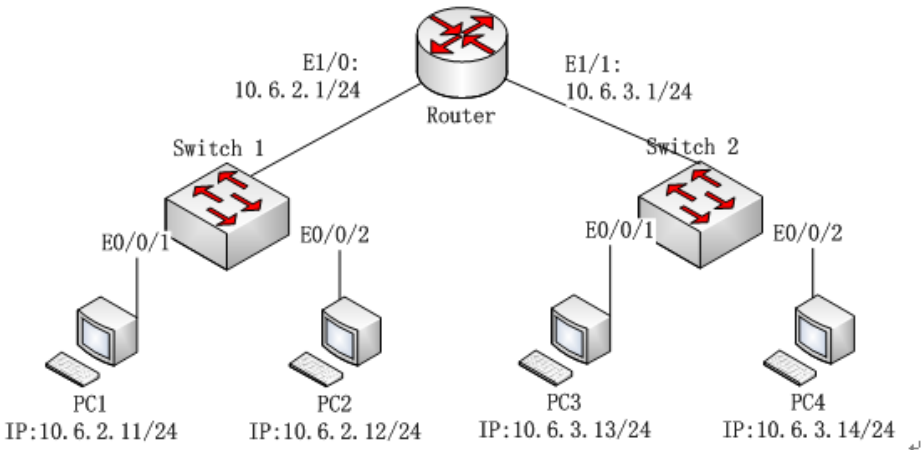


# 计算机网络专题实验现场检查单 5

实验名称：组网与 VLAN

时间： 2021 年 4 月 10 日 早 ☐ 午 ☐ 晚 ☒

组号	5-6	实验位	6	控制器地址	192.168.1.60
姓名	施炎江	高浩翔	贾星辰	薛杰锋	

实验组网图	 <p>(其余具体组网情况见下方实验过程)</p>
-------	--

实验结果

1. 组网配置完成后，网络连通测试结果：

		所用命令	能否 ping 通
同一网段中	PC1 ping PC2	Ping 10.6.2.12	Y
	PC3 ping PC4	Ping 10.6.3.14	Y
不同网段中	PC1 ping PC3	Ping 10.6.3.13	Y
	PC2 ping PC4	Ping 10.6.3.14	Y

用 show ip route 查看 R1 的路由表，分析不同网段互通原因，体会网关的作用？

```
Router#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type

VRF ID: 0

C       10.6.2.0/24[0]         is directly connected, Ethernet1/0[0]
C       10.6.3.0/24[0]         is directly connected, Ethernet1/1[0]
```

两个不同网段通过路由器进行了直接连接，因此可以相互通信。这里网关的作用是实现局域网的互联。

在 PC1 上用 `tracert -d 10.1.3.14`（PC4 的 IP 地址），查看 PC1-PC4 的路由连通路径。

```
C:\Users\Administrator>tracert -d 10.6.3.14

通过最多 30 个跃点跟踪到 10.6.3.14 的路由

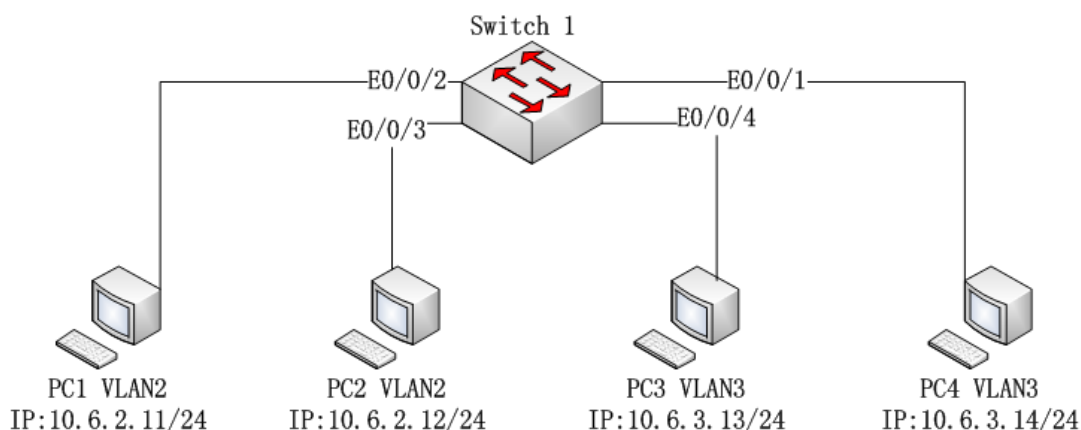
 1  <1 毫秒  <1 毫秒  <1 毫秒 10.6.2.1
 2   1 ms    1 ms    1 ms  10.6.3.14

跟踪完成。
```

第一个节点是路由器的端口，第二个节点是 PC4。

2. VLAN 配置完成后，验证同一 VLAN 的两台计算机能否通信，不同 VLAN 之间的计算机能否通信，记录结果并解释原因（步骤 3）。

网络拓扑图：



```

C:\Users\Administrator>ping 10.6.2.12

正在 Ping 10.6.2.12 具有 32 字节的数据:
来自 10.6.2.12 的回复: 字节=32 时间=1ms TTL=128
来自 10.6.2.12 的回复: 字节=32 时间=1ms TTL=128
来自 10.6.2.12 的回复: 字节=32 时间=1ms TTL=128
来自 10.6.2.12 的回复: 字节=32 时间<1ms TTL=128

10.6.2.12 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\Administrator>ping 10.6.3.14

正在 Ping 10.6.3.14 具有 32 字节的数据:
来自 10.6.2.11 的回复: 无法访问目标主机。
来自 10.6.2.11 的回复: 无法访问目标主机。
来自 10.6.2.11 的回复: 无法访问目标主机。
来自 10.6.2.11 的回复: 无法访问目标主机。

10.6.3.14 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

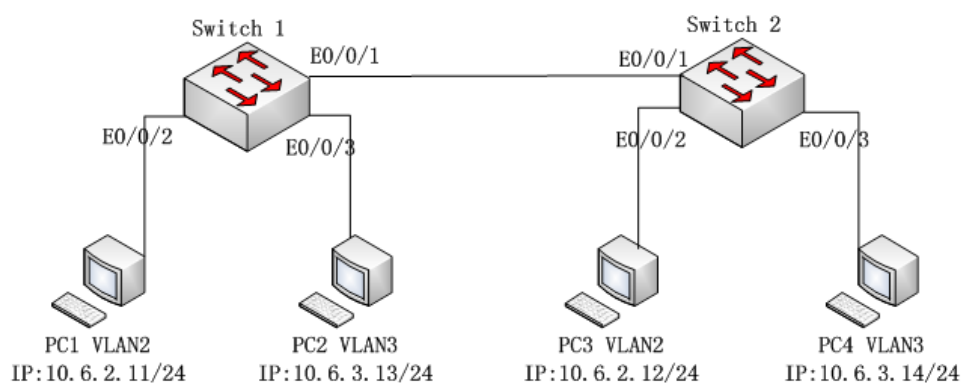
```

同一 VLAN 中的主机可以相互通信，不同 VLAN 中的主机不能相互通信。

因为交换机为每个数据包都标记上了 VLAN 号标签，当有数据包传到交换机处时，交换机只会有相同 VLAN 号的报文转发到对应的主机，从而隔离了不同 VLAN。

3. 步骤 6（完成 Trunk 端口配置）完成后，测试同一 VLAN 和不同 VLAN 中计算机的互通情况，记录测试结果并解释原因。

网络拓扑图：



同一 VLAN 中的主机可以互通，不同 VLAN 中的主机不能互通。

因为我们为两个交换机的 E0/0/1 端口都配置成了 Trunk 模式，在该模式下端口可以属于多个 VLAN，也可以接收和发送多个不同 VLAN 的报文。进入 Trunk 端口的数据帧，对于已经携带 tag 域的数据，端口直接进行转发，而对于普通数据帧，端口用自己的缺省 VLAN ID 进行封装后再转发。这样就使得两个交换机能够传输属于不同 VLAN 的数据包，使得 PC1 和 PC3 虽然不在同一交

换机下，但由于二者在同一 VLAN 中，他们依然可以相互通信。

下图是 PC1 分别 pingPC3 和 PC2 的结果：

```
C:\Users\Administrator>ping 10.6.2.12

正在 Ping 10.6.2.12 具有 32 字节的数据:
来自 10.6.2.12 的回复: 字节=32 时间<1ms TTL=128
来自 10.6.2.12 的回复: 字节=32 时间=1ms TTL=128
来自 10.6.2.12 的回复: 字节=32 时间=1ms TTL=128
来自 10.6.2.12 的回复: 字节=32 时间<1ms TTL=128

10.6.2.12 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\Administrator>ping 10.6.3.13

正在 Ping 10.6.3.13 具有 32 字节的数据:
来自 10.6.2.11 的回复: 无法访问目标主机。
来自 10.6.2.11 的回复: 无法访问目标主机。
来自 10.6.2.11 的回复: 无法访问目标主机。
请求超时。

10.6.3.13 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
```

4. 填写步骤 7 中的表格并解释原因（设置镜像端口后）。

转发过程(标明方向)	报文类型(请求/响应)	VLAN 标记(只填写观察到的)	标记出现与否的原因
PC3 — S2	请求	无	报文还未经过 S2 封装 802.1q 协议
S2 — S1	请求	2	报文经过 S2 封装后标记上了 VLAN 号为 2
S1 — PC1	请求	2	报文经过 S2 封装后标记上了 VLAN 号为 2
PC1 — S1	响应	无	监控主机新网卡过滤掉了 802.1q 协议
S1 — S2	响应	无	监控主机新网卡过滤掉了 802.1q 协议
S2 — PC3	响应	无	监控主机新网卡过滤掉了 802.1q 协议

PC2 抓包（监听 PC1）：

No.	Time	Source	Destination	Protocol	Length	Info	VLAN
3	0.000797	10.6.2.12	10.6.2.11	ICMP	78	Echo (ping) request id=0x0001, seq=45/11520, ttl=64 (reply in 6)	2
6	0.001617	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=128 (request in 3)	
7	0.991533	10.6.2.12	10.6.2.11	ICMP	78	Echo (ping) request id=0x0001, seq=46/11776, ttl=64 (reply in 8)	2
8	0.992360	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=128 (request in 7)	
9	2.005275	10.6.2.12	10.6.2.11	ICMP	78	Echo (ping) request id=0x0001, seq=47/12032, ttl=64 (reply in 10)	2
10	2.006122	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=128 (request in 9)	
11	3.019341	10.6.2.12	10.6.2.11	ICMP	78	Echo (ping) request id=0x0001, seq=48/12288, ttl=64 (reply in 12)	2
12	3.020194	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=128 (request in 11)	

Frame 7: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF\_{D8B3397C-E6C9-4273-A766-DDAFB441FCF6}, id 0  
 Ethernet II, Src: Realtek5\_68:69:00 (00:e0:4c:68:69:00), Dst: Realtek5\_68:46:00 (00:e0:4c:68:46:00)  
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2  
 000. .... = Priority: Best Effort (default) (0)  
 ...0 .... = DEI: Ineligible  
 .... 0000 0000 0010 = ID: 2  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 10.6.2.12, Dst: 10.6.2.11  
 Internet Control Message Protocol

E0/0/3 被设置成 E0/0/1 的端口镜像，因此所有经过 E0/0/1 的数据包都会被转发一份到 E0/0/3，也就是说所有传送给 PC1 的报文都会被复制一份给 PC2。PC3 和 PC4 同理。

PC4 抓包（监听 PC3）：

No.	Time	Source	Destination	Protocol	Length	Info	VLAN
10	5.111751	10.6.2.12	10.6.2.11	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=64 (reply in 11)	
11	5.112533	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=128 (request in 10)	
14	6.124486	10.6.2.12	10.6.2.11	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=64 (reply in 15)	
15	6.125268	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=128 (request in 14)	
17	7.138434	10.6.2.12	10.6.2.11	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=64 (reply in 18)	
18	7.139218	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=128 (request in 17)	
20	8.152176	10.6.2.12	10.6.2.11	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=64 (reply in 21)	
21	8.152824	10.6.2.11	10.6.2.12	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=128 (request in 20)	

Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{A2E02301-5164-49F0-8ECA-D374B3A37A63}, id 0  
 Ethernet II, Src: Realtek5\_68:69:00 (00:e0:4c:68:69:00), Dst: Realtek5\_68:46:00 (00:e0:4c:68:46:00)  
 Internet Protocol Version 4, Src: 10.6.2.12, Dst: 10.6.2.11  
 Internet Control Message Protocol

5. 完成实验步骤 10 后，解释不同 Vlan 间可以通信的原因？

No.	Time	Source	Destination	Protocol	Length	Info	VLAN
43	6.674182	10.6.2.12	10.6.3.14	ICMP	78	Echo (ping) request id=0x0001, seq=49/12544, ttl=63 (reply in 44)	3
44	6.674965	10.6.3.14	10.6.2.12	ICMP	78	Echo (ping) reply id=0x0001, seq=49/12544, ttl=127 (request in 43)	2
47	7.667758	10.6.2.12	10.6.3.14	ICMP	78	Echo (ping) request id=0x0001, seq=50/12800, ttl=63 (reply in 48)	3
48	7.668412	10.6.3.14	10.6.2.12	ICMP	78	Echo (ping) reply id=0x0001, seq=50/12800, ttl=127 (request in 47)	2
50	8.681701	10.6.2.12	10.6.3.14	ICMP	78	Echo (ping) request id=0x0001, seq=51/13056, ttl=63 (reply in 51)	3
51	8.682350	10.6.3.14	10.6.2.12	ICMP	78	Echo (ping) reply id=0x0001, seq=51/13056, ttl=127 (request in 50)	2
53	9.695623	10.6.2.12	10.6.3.14	ICMP	78	Echo (ping) request id=0x0001, seq=52/13312, ttl=63 (reply in 54)	3
54	9.696271	10.6.3.14	10.6.2.12	ICMP	78	Echo (ping) reply id=0x0001, seq=52/13312, ttl=127 (request in 53)	2

Frame 43: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF\_{D8B3397C-E6C9-4273-A766-DDAFB441FCF6}, id 0  
 Ethernet II, Src: AcctonTe\_4d:c2:40 (00:12:cf:4d:c2:40), Dst: SamsungE\_17:85:bf (e8:03:9a:17:85:bf)  
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3  
 000. .... = Priority: Best Effort (default) (0)  
 ...0 .... = DEI: Ineligible  
 .... 0000 0000 0011 = ID: 3  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 10.6.2.12, Dst: 10.6.3.14  
 Internet Control Message Protocol

trunk 类型的端口可以允许多个 VLAN 通过，比较将要发送报文的 VLAN 信息和端口的 PVID，如果不相等则直接发送。如果两者相等则剥离 VLAN 信息，再发送。实验中没有设置 PVID 缺省值为 VLAN1。

Trunk 端口收到一个报文，判断是否有 VLAN 信息：如果有，则判断该 trunk 端口是否允许该 VLAN 的数据进入：如果可以则转发，否则丢弃；在 trunk 端口出方向，比较将要发送报文的 VLAN 信息和端口的 PVID，如果不相等则直接发送。如果两者相等则剥离 VLAN 信息，再发送。

在 trunk 端口设置中，将 trunk 端口加入到了 VLAN2 和 VLAN3 中，因此 trunk 端口允许携带 VLAN2 和 VLAN3 的数据帧通过。PC3 向 PC4 发起了 ICMP 请求，携带 VLAN 信息为 VLAN3，与 VLAN1 不同所以直接转发，在 S1 处经过路由转发到 PC4；PC4 向 PC3 发起了 ICMP 应答，携带 VLAN 信息为 VLAN2，与 VLAN1 不同直接转发，经过 E0/0/1 截获的报文携带信息 VLAN2，经 S1 路由发送到 PC3。在 PC3 ping PC4 过程中发送四条报文，响应四条报文，都需要经过 E 0/0/1

端口，都被 PC2 监听到，因此总共有八条报文。

## 6. 互动讨论主题

(1) 分析不同 LAN 中 PC 互通的原因及跨越的链路；

不同 LAN 中 PC 互通是通过 trunk 端口实现的，在 trunk 端口进方向，交换机接收到数据包后，先判断是否带 VLAN tag，没有则丢弃数据包，有则按照对应 VLAN 进行转发；在 trunk 端口出方向，交换机将带 VLAN tag 的数据包原封不动转发出去，没有带 VLAN tag 数据包不会从 trunk 端口转发出去。经 trunk 端口转发的数据帧会在 S1 进行路由从而找到目标主机的地址。

不同 LAN 中的 PC 互通过程中，有源端发送数据帧，到交换机 S2，经 trunk 端口链路到交换机 S1，在 S1 路由，找到目标机的地址。

(2) 理解网关的目的及作用；

网关是用于连接两个或者两个以上网段的设备。在 TCP/IP 网络体系中，网关的基本作用是根

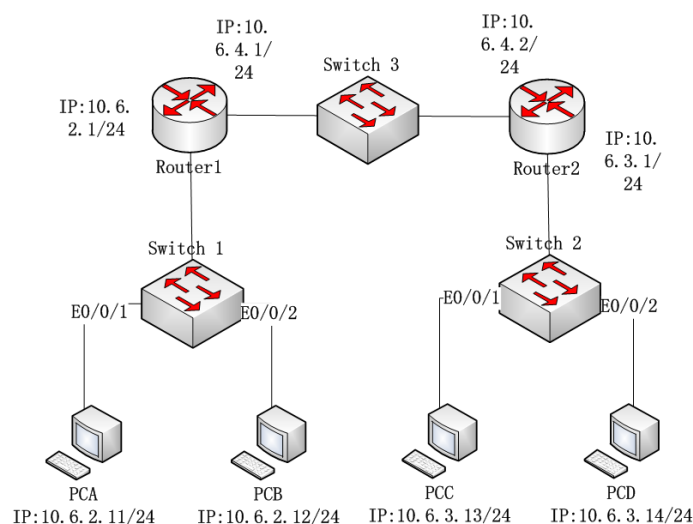
(3) 路由表的形成及使用。

静态路由：由管理员手工配置。

动态路由：如果更新的某路由表项在路由表中没有，则直接在路由表中添加该路由表项；如果路由表中已有相同目的网络的路由表项，且来源端口相同，那么无条件根据最新的路由信息更新其路由表；如果路由表中已有相同目的网络的路由表项，但来源端口不同，则要比

## 7. 进阶自设计：配置如图所示拓扑的网络，使得不同主机之间能够相互通信。

网络拓扑图：



线路连接完整之后，首先配置各设备的 IP 信息与各主机默认网关，IP 如图中信息所示，之后对路由器的路由表进行设置。本组采用配置 rip 协议的方式使路由器获取路由表如图：

```
Router_config#router rip
Router_config_rip#version 2
Router_config_rip#network 10.6.2.1
Router_config_rip#network 10.6.4.1
```

之后查看路由器的路由表如下：发现各个网络均已在路由表内。

```
Router_config#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type

VRF ID: 0

C       10.6.2.0/24[0]           is directly connected, Ethernet1/0[0]
C       10.6.4.0/24[0]           is directly connected, Ethernet1/1[0]
Router_config#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
       D - DEIGRP, DEX - external DEIGRP, O - OSPF, OIA - OSPF inter area
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       OE1 - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type

VRF ID: 0

C       10.6.2.0/24[0]           is directly connected, Ethernet1/0[0]
R       10.6.3.0/24[0]           [120,1] via 10.6.4.2(on Ethernet1/1[0])
C       10.6.4.0/24[0]           is directly connected, Ethernet1/1[0]
```

各主机之间相互 ping 命令成功，如图：

```
C:\Users\Administrator>ping 10.6.3.13

正在 Ping 10.6.3.13 具有 32 字节的数据:
来自 10.6.3.13 的回复: 字节=32 时间=3ms TTL=126
来自 10.6.3.13 的回复: 字节=32 时间=1ms TTL=126
来自 10.6.3.13 的回复: 字节=32 时间=1ms TTL=126
来自 10.6.3.13 的回复: 字节=32 时间=1ms TTL=126

10.6.3.13 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 3ms, 平均 = 1ms

C:\Users\Administrator>ping 10.6.3.14

正在 Ping 10.6.3.14 具有 32 字节的数据:
来自 10.6.3.14 的回复: 字节=32 时间=2ms TTL=126
来自 10.6.3.14 的回复: 字节=32 时间=1ms TTL=126
来自 10.6.3.14 的回复: 字节=32 时间=1ms TTL=126
来自 10.6.3.14 的回复: 字节=32 时间=1ms TTL=126

10.6.3.14 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 2ms, 平均 = 1ms

C:\Users\Administrator>ping 10.6.2.11

正在 Ping 10.6.2.11 具有 32 字节的数据:
来自 10.6.2.11 的回复: 字节=32 时间=2ms TTL=128
来自 10.6.2.11 的回复: 字节=32 时间<1ms TTL=128
来自 10.6.2.11 的回复: 字节=32 时间=1ms TTL=128
来自 10.6.2.11 的回复: 字节=32 时间<1ms TTL=128

10.6.2.11 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 2ms, 平均 = 0ms
```

## 5.8 互动讨论

### (1) 交换设备与 Vlan 配置;

交换机: 最常见的为以太网交换机, 能够为接入交换机的任意两个网络节点提供通信链路。

Vlan 配置方法: 通过修改 ACCESS 的 PVID 值, 就可以将相同 PVID 的 ACCESS 端口划分到同一个 VLAN 中, TRUNK 端口可以直接划分到一个或多个 VLAN 中。

### (2) 交换设备端口类型与镜像口;

交换机端口类型:

**ACCESS 口:** 一般用来链接用户计算机, 只能属于一个 VLAN, 端口的 PVID 与所属 VLAN 的 ID 相同, 默认为 1。

接受方法: 一般只接受“未打标签”的普通以太网 MAC 帧, 根据接受帧端口的 PVID 给帧“打标签”, 插入 4 字节的 VLAN 标记字段, 字段中的 VID 与端口的 PVID 相同。

发送方法: 若帧中的 VID 与端口的 PVID 相同, 则去标签之后转发, 否则不转发。

**TRUNK 口:** 一般用于交换机之间以及交换机与路由器之间的链接, 可与属于多个 VLAN。用户可以设置该端口的 PVID 值, 默认情况下为 1。

发送方法: 若帧中的 VID 与端口的 PVID 相同, 则去标签之后转发。

若帧中的 VID 与端口的 PVID 不同, 则不去标签直接转发。

接受方法: 接受“未打标签”的帧, 根据接受帧端口的 PVID 给帧“打标签”, 插入 4 字节的 VLAN 标记字段, 字段中的 VID 与端口的 PVID 相同。接受已经打标签的帧。

**HYBIRD 口:** 华为交换机私有的端口类型。Hybrid 端口既可用于交换机之间或交换机与路由器之间的互连(同 Trunk 端口), 也可用于交换机与用户计算机之间的互连(同 Access 端口)。Hybrid 端口可以属于多个 VLAN (同 Trunk 端口)。用户可以设置 Hybrid 端口的 PVID 值。默认情况下, Hybrid 端口的 PVID 值为 1 (同 Trunk 端口)

发送方法(与 Trunk 端口不同): 查看帧的 VID 是否在端口的“去标签”列表中:

若存在, 则“去标签”后再转发。

若不存在, 则直接转发。

接收方法(同 Trunk 端口)

接收“未打标签”的帧, 根据接收帧的端口的 PVID 给帧“打标签”, 即插入 4 字节 VLAN 标记字段, 字段中的 VID 取值与端口的 PVID 取值相等。

接收“已打标签的帧”。

### (3) 路由表生成方法;

一般有两种:

a.手动配置路由表;

b.通过对路由器配置路由协议, 路由器自动学习生成路由表。

### (4) 路由表的使用。

路由器在接受到数据报之后, 通过查找路由表来确定该数据报目的地址该如何转发, 同时, 采用路由协议的路由器之间会相互发送各自的路由表进行学习、更新自己的路由表。



本组成员主要工作：	施炎江：按实验指导进行操作，负责 PC1 的控制，连接设备，配置交换机、路由器的设置，负责实验的验收演示，负责实验报告的一部分撰写和统筹。		
	高浩翔：按实验指导进行操作，负责 PC4 的控制，连接设备，配置交换机、路由器的设置，负责实验报告的一部分撰写。		
	薛杰锋：按实验指导进行操作，负责 PC2 的控制，连接设备，配置交换机、路由器的设置，负责实验报告的一部分撰写。		
	贾星辰：按实验指导进行操作，负责 PC3 的控制，连接设备，配置交换机、路由器的设置，负责实验报告的一部分撰写。		
实验中问题及解决方法，经验总结	<p>问题一：实验 5.5（2），配置交换机上的镜像接口时，因为输入指令出错，误将本应是 destination interface 的 ethernet 0/0/3 接口配置成了 source interface，而指导书中除了重新启动交换机外，没有给出修改的指令。</p> <p>解决方法：观察设备箱上的交换机型号，在互联网上查询该型号的控制指令，找到了删除镜像端口的语句。通过该指令，删掉了配置错误的端口，并重新配置的正确镜像端口。</p> <p>经验总结：当实验过程中出现意外的情况时，除了查询参考书，还应先总结问题，通过自己的方法寻找解决问题的办法，从而锻炼自主解决问题的能力。</p> <p>问题二：实验 5.5（2），在镜像端口连接的主机上进行抓包时，和抓包主机在同一个交换机的主机发出的报文没有 vlan 号标识，而来自另一方的有 vlan 标识；实验 5.5（3）中，镜像端口抓到的报文均存在 vlan 标识。</p> <p>解决办法：通过查询资料及询问老师，得知在同一个交换机下的主机通过镜像端口抓包时，捕获的是还未经过最后处理的报文，而 vlan 标识正是在经过最后处理时添加的。所以，在同一个交换机下的主机，不会在截获报文里显示 vlan；而实验 5.5（3）中，由于抓报文的主机和收发报文的两个主机均不在同一个交换机下，故抓到的报文均存在 vlan 标识。</p> <p>经验总结：做实验的时候不仅要完成实验要求，也要善于观察实验要求中没有出现的现象，并探求机理。</p>		
师生互动交流	<p>提问：完成实验 5.5（3）步骤 10 后，解释不同 Vlan 间可以通信的原因</p> <p>回答：trunk 类型的端口可以允许多个 VLAN 通过，比较将要发送报文的 VLAN 信息和端口的 PVID，如果不相等则直接发送。如果两者相等则剥离 VLAN 信息，再发送。实验中没有设置 PVID 缺省值为 VLAN1。</p> <p>Trunk 端口收到一个报文,判断是否有 VLAN 信息：如果有，则判断该 hybrid 端口是否允许该 VLAN 的数据进入：如果可以则转发，否则丢弃；在 trunk 端口出方向，比较将要发送报文的 VLAN 信息和端口的 PVID，如果不相等则直接发送。如果两者相等则剥离 VLAN 信息，再发送。</p>		
验收教师	张利平	本实验成绩	