

网络技术与信息安全



第1讲：构建局域网

河南中医药大学信息技术学院
许成刚

一、认识以太网

认识以太网

□ 计算机网络的分类

类别	作用范围或距离
广域网 WAN (Wide Area Network)	通常为几十到几千公里。有时也称为 远程网 (long haul network)。是互联网的核心部分。
城域网 MAN (Metropolitan Area Network)	作用范围一般是一个城市，作用距离约为 5~50 公里。
局域网 LAN (Local Area Network)	局限在较小的范围（如 1 公里左右）。通常采用高速通信线路。
个人区域网 PAN (Personal Area Network)	范围很小，大约在 10 米左右。有时也称为 无线个人区域网 WPAN (Wireless PAN)。

认识以太网

□ 局域网的特点

- 网络所覆盖的地理范围比较小；
- 数据的传输速率比较高；
- 具有较低的延迟和误码率；
- 局域网的经营权和管理权属于某个单位；
- 协议简单、结构灵活、建网成本低、周期短、便于管理和扩充。

认识以太网

□ 什么是以太网

- 以太网是目前全球应用最广泛的有线局域网技术，它基于IEEE 802.3标准，通过网线、光纤等介质实现设备之间的高速、稳定数据传输，早已取代令牌环、FDDI等早期局域网技术，成为家庭、企业、工业场景的主流网络连接方案

认识以太网

□ 以太网的应用

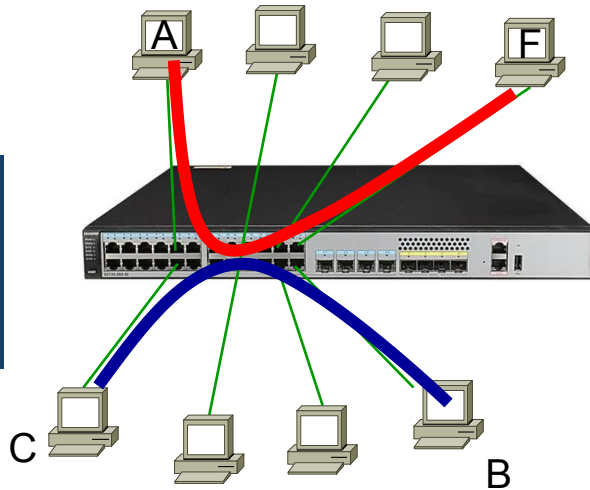
- 以太网的两个标准DIX Ethernet V2与IEEE的802.3标准只有很小的差别，因此很多人也常把IEEE802.3局域网简称为“以太网”。
- IEEE802.3以太网标准被ISO接收为国际标准，这意味着以太网技术已成为一种世界性的标准，全球的销售商都可以生产适用于以太网系统的设备。
- 到了20世纪90年代，快速的发展，较好的兼容性，使得以太网在激烈竞争的局域网市场占有了统治地位，激烈竞争的局域网市场逐渐明朗。以太网在局域网市场中已经取得了垄断地位，并且几乎成了局域网的代名词。

认识以太网

□ 使用交换机的星型拓扑以太网

- 交换机是以太网组网的主要设备，采用星形拓扑结构
- 交换机内部可同时提供多个传输通道，允许不同用户间（即不同接口对之间）同时进行传送，大大提高通信效率。

在交换式以太网中，交换机的不同端口对之间，可同时传送数据



认识以太网

□ 使用交换机的星型拓扑

- 交换机是二层设备（具有物理层、**数据链路层功能**）。因此，交换机可以识别所收到的数据帧首部中的**MAC地址**，并根据目的**MAC地址**，决定数据帧应发向交换机的哪个端口，而不用再采用广播方式。

二、以太网是如何与TCP/IP协议结合的？



TCP/IP模型协议族

应用层	HTTP FTP TELNET SMTP	DNS RIP DHCP
运输层	TCP	UDP
网络层	IGMP ICMP IP ARP	
网络接口层	以太网 令牌环网 帧中继	

以太网是如何与TCP/IP协议结合的？

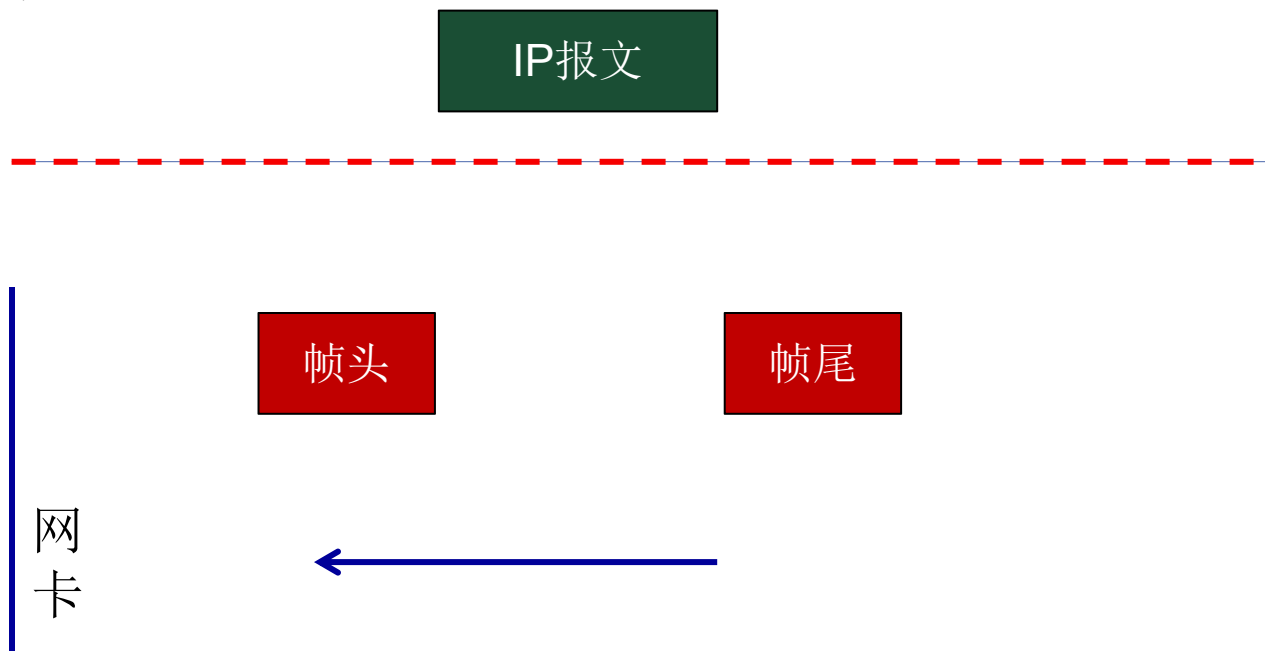
□ TCP/IP协议和以太网的结合的两个关键点

- 以太网属于局域网技术，其主要目的是实现数据通信，即尽最大努力完成数据帧的传送，它是一个通信网，也就是说，以太网技术主要体现在物理层和数据链路层，更高层功能可借助其他的通信网络协议，如TCP/IP协议。
- 这里的结合有两个关键点：**协议封装、两种地址共用**。

以太网是如何与TCP/IP协议结合的？

□ TCP/IP协议和以太网的结合的两个关键点

1、协议封装



以太网是如何与TCP/IP协议结合的？

□ TCP/IP协议和以太网的结合的两个关键点

2、两种地址共用

➤ TCP/IP体系实现网络互连的方法

- TCP/IP体系并没有改变已有网络的“异构性”，而是在异构网络“之上”，设计了一套相互通信的统一标准，使得异构的网络通过这个位于上层的统一标准，实现相互通信。具体的讲，就是保持了物理层、数据链路层的异构性，在网络层采用了标准化协议——IP (Internet Protocol)。

➤ IP主要包含三方面内容：

- IP编址方案：在数据链路层之上，统一了地址的格式。即IP地址
- 分组封装格式：明确了分组的格式。
- 分组转发规则：明确了分组在互联网中如何被转

以太网是如何与TCP/IP协议结合的？

□ TCP/IP协议和以太网的结合的两个关键点

1、协议封装

- 通过封装，以太网帧携带了高层协议包，它把整个分组看成是填入以太网帧的数据字段的未知数据。
- 当以太网帧送达目的主机时，就由目的主机中数据链路层的网络协议进行处理，即从以太网帧数据字段中提取高层协议包。这样，以太网系统就能传递各种各样的高层网络协议（例如TCP/IP、Novell协议等）报文，而不必担心他们是如何工作的。



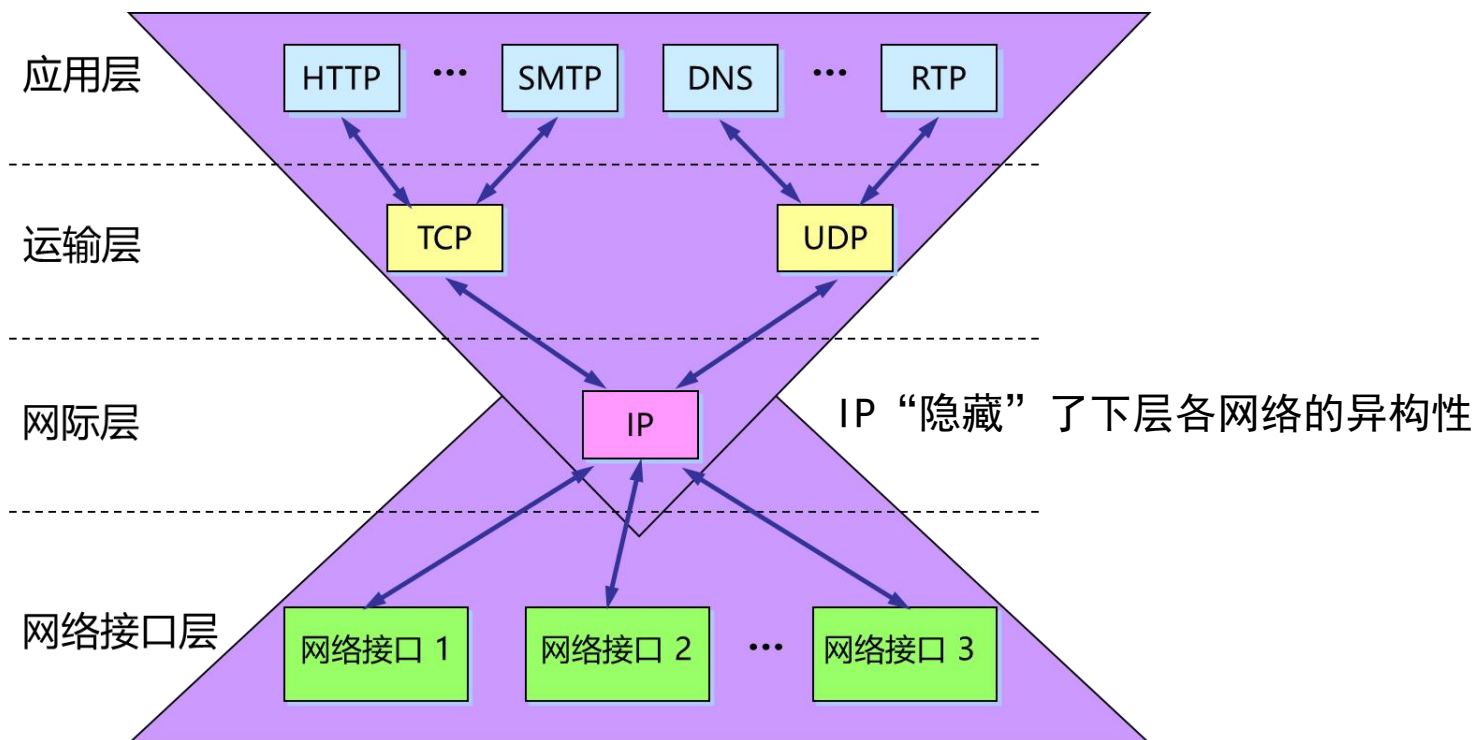
以太网是如何与TCP/IP协议结合的？

□ TCP/IP协议和以太网的结合的两个关键点

2、两种地址共用

- **IP地址**：在网络层，用于实现不同网络之间的通信。每个数据包首部都包含一个源IP地址和一个目的IP地址，当该数据包在互联网中（不同网络间）传输时，这两个地址指明了源网络和目的网络，通常保持不变。
- **MAC地址**：在数据链路层，用以实现同一网络内部的目标定位。封装成帧后，每个帧的首部包含源MAC地址和目的MAC地址，用于在以太网内部，定位目的主机。
- 在TCP/IP系统中，为了使高层协议报文能到达目的地，高层协议软件和以太网系统必须相互作用，也就是说，主机的IP地址和网卡的MAC地址都是必需的，它们在不同的层面上发挥着自己的作用。
- 动画演示

沙漏计时器形状的TCP/IP协议族示意

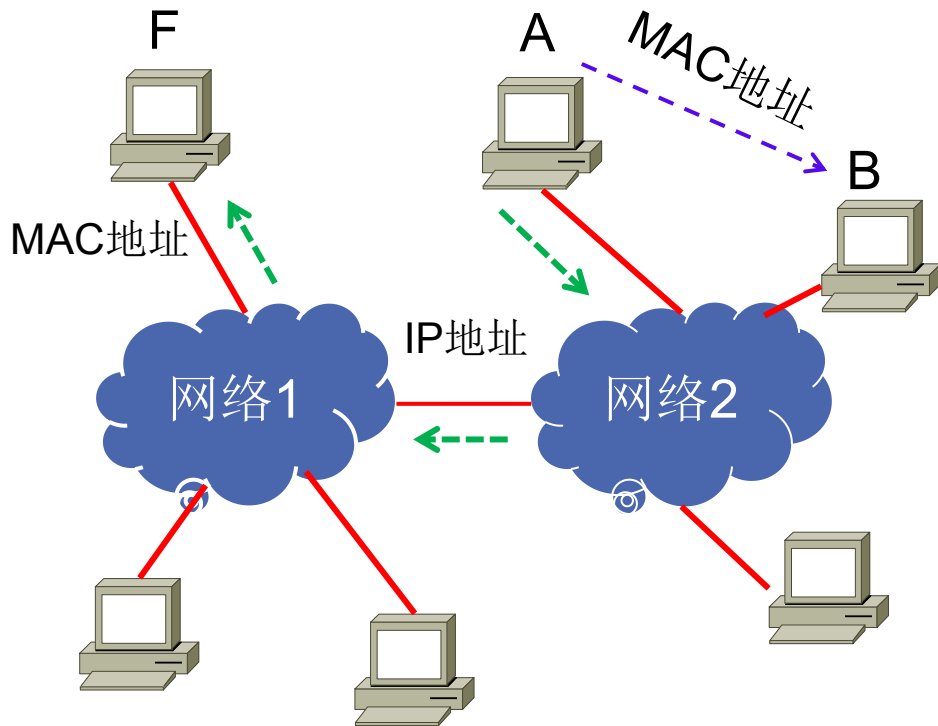


以太网是如何与TCP/IP协议结合的？

□ TCP/IP协议和以太网的结合的两个关键点

2、两种地址共用（动画演示）

- 通过MAC地址实现同一网络内部通信时的目标定位。例如A访问B；
- 但是，若要访问不同网络内的主机，就需要用到IP地址了。例如A和F通信。通过IP地址到达目的网络，然后通过MAC地址定位具体的目的主机。



以太网是如何与TCP/IP协议结合的？

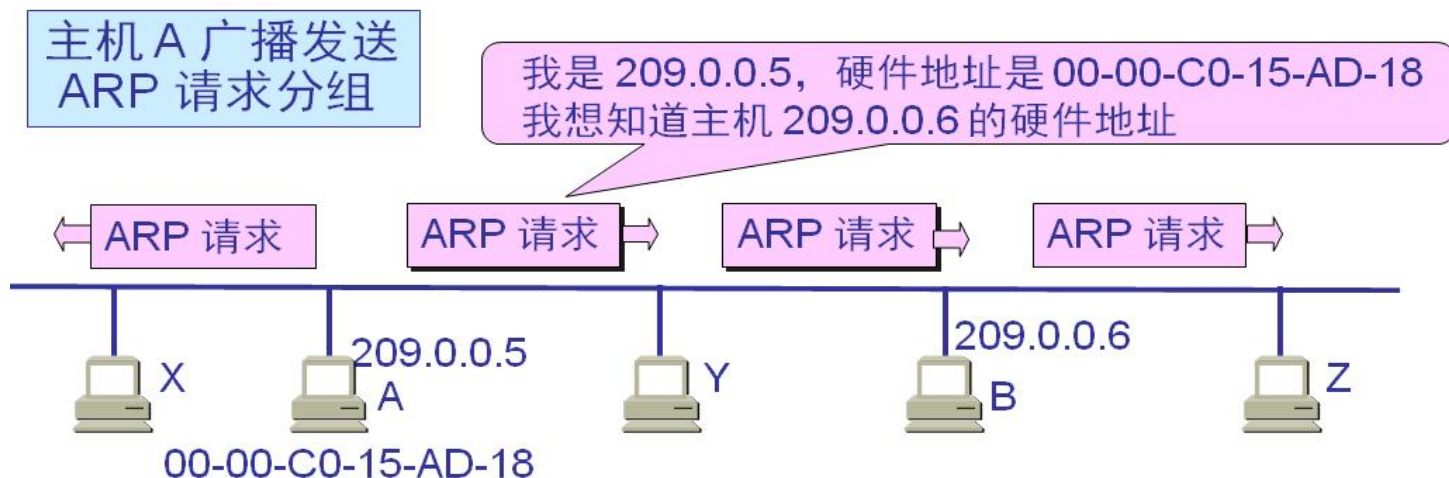
□ 如何实现从IP地址到物理地址的映射？

- 在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的MAC地址的。一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是如何获得的呢？

■ ARP协议

- 地址解析协议（Address Resolution Protocol, ARP）是在仅知道主机的IP地址时确定其物理地址的一种协议，即实现从IP地址到物理地址的映射
- ARP协议的基本功能，就是只要知道同一物理网络上目标设备的IP地址，就可以查询目标设备的MAC地址，以保证通信的顺利进行。
- 所谓“地址解析”就是主机在发送帧前通过目标IP地址获得目标MAC地址的过程。

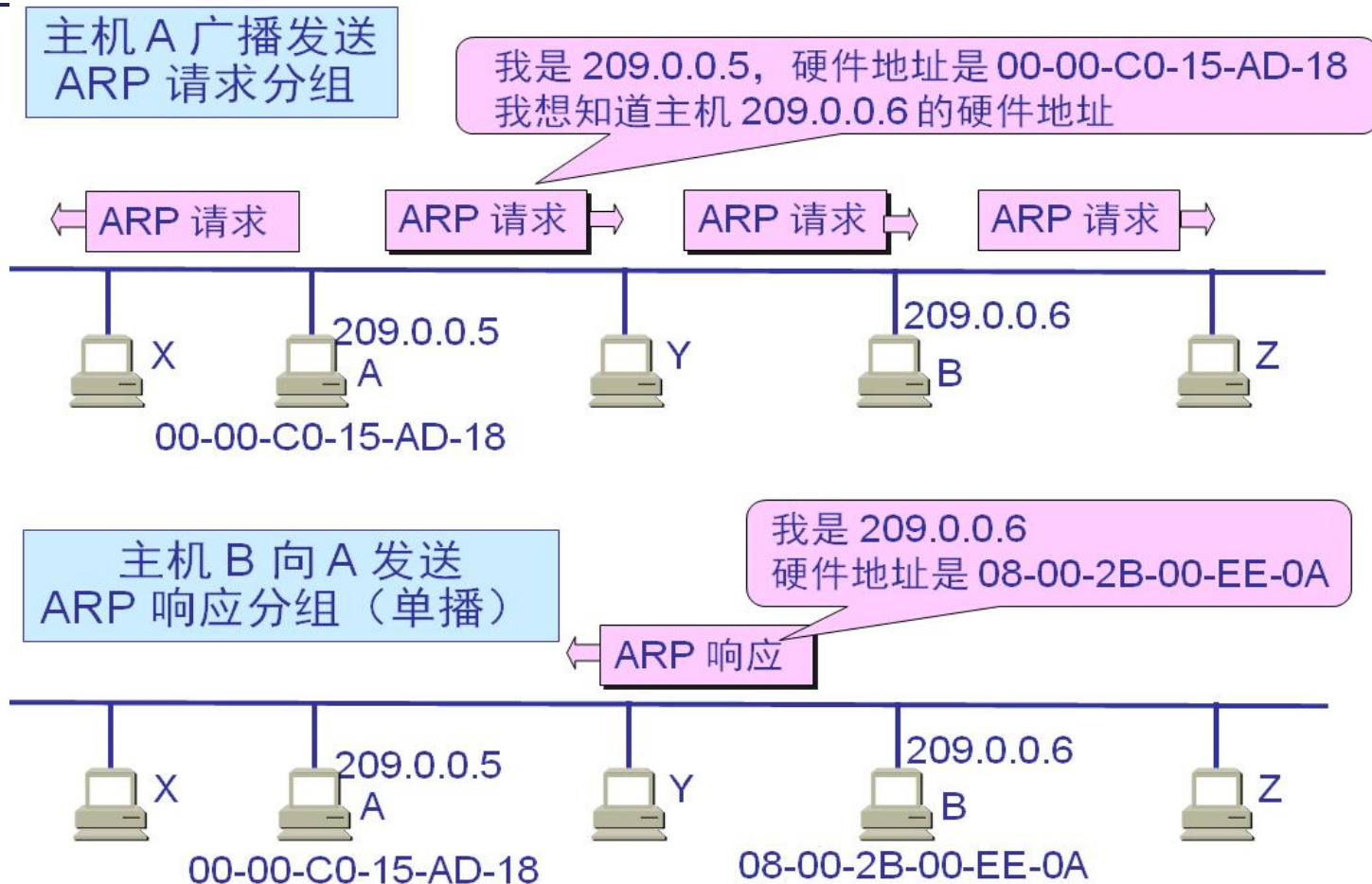
□ ARP协议的工作过程



TX1-77

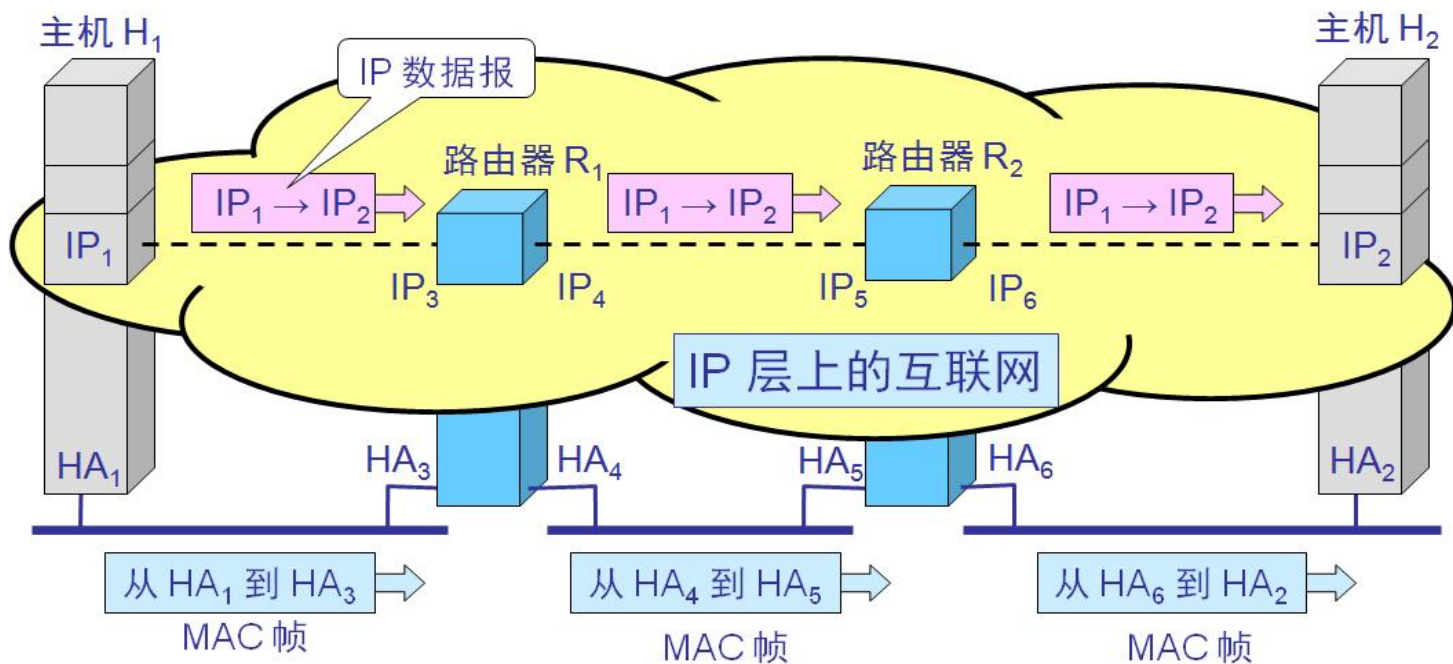
Source	Destination	Protocol	Info
Mettler-_1e:1a:38	Broadcast	ARP	Who has 211.69.32.1? Tell 211.69.32.100
Shanghai_7a:9e:b8	Mettler-_1e:1...	ARP	211.69.32.1 is at 00:e0:0f:7a:9e:b8
211.69.32.100	10.1.1.1	ICMP	Echo (ping) request id=0x0001, seq=29/74
10.1.1.1	211.69.32.100	ICMP	Echo (ping) reply id=0x0001, seq=29/74
211.69.32.100	10.1.1.1	ICMP	Echo (ping) request id=0x0001, seq=30/76

ARP协议的工作过程



《计算机网络》第8版 P132

- 主机H1和H2通信，报文经过路由器R1和R2。结合路由表、IP地址、MAC地址、ARP协议，分析通信过程。



三、认识交换机

——组建局域网的关键设备



认识交换机

□ 不同的交换机



华为S5720S企业级48口千兆以太网交换机



思科（Cisco）SF95D 8口百兆交换机

认识交换机

□ 不同的交换机



华为S9300系列的交换机



48口千兆板卡

认识交换机

□ 交换机规格参数

- 品牌（华为、思科、……）
- 接口速率（百兆、千兆、万兆……）
- 接口数量（8、16、24、48……）
- 可管理性（网管型/非网管型）
- 二层交换机、三层交换机
- 各种功能参数
- ……

认识交换机

□ 如何选择交换机？



小型办公室组网



计算机机房组网



园区组网

认识交换机

□ 如何选择交换机？

■ 在建设网络时，应该依据

- 网络规模大小
- 需要起到的作用
- 经费预算
- 设备性价比
-

■ 去选择交换机。



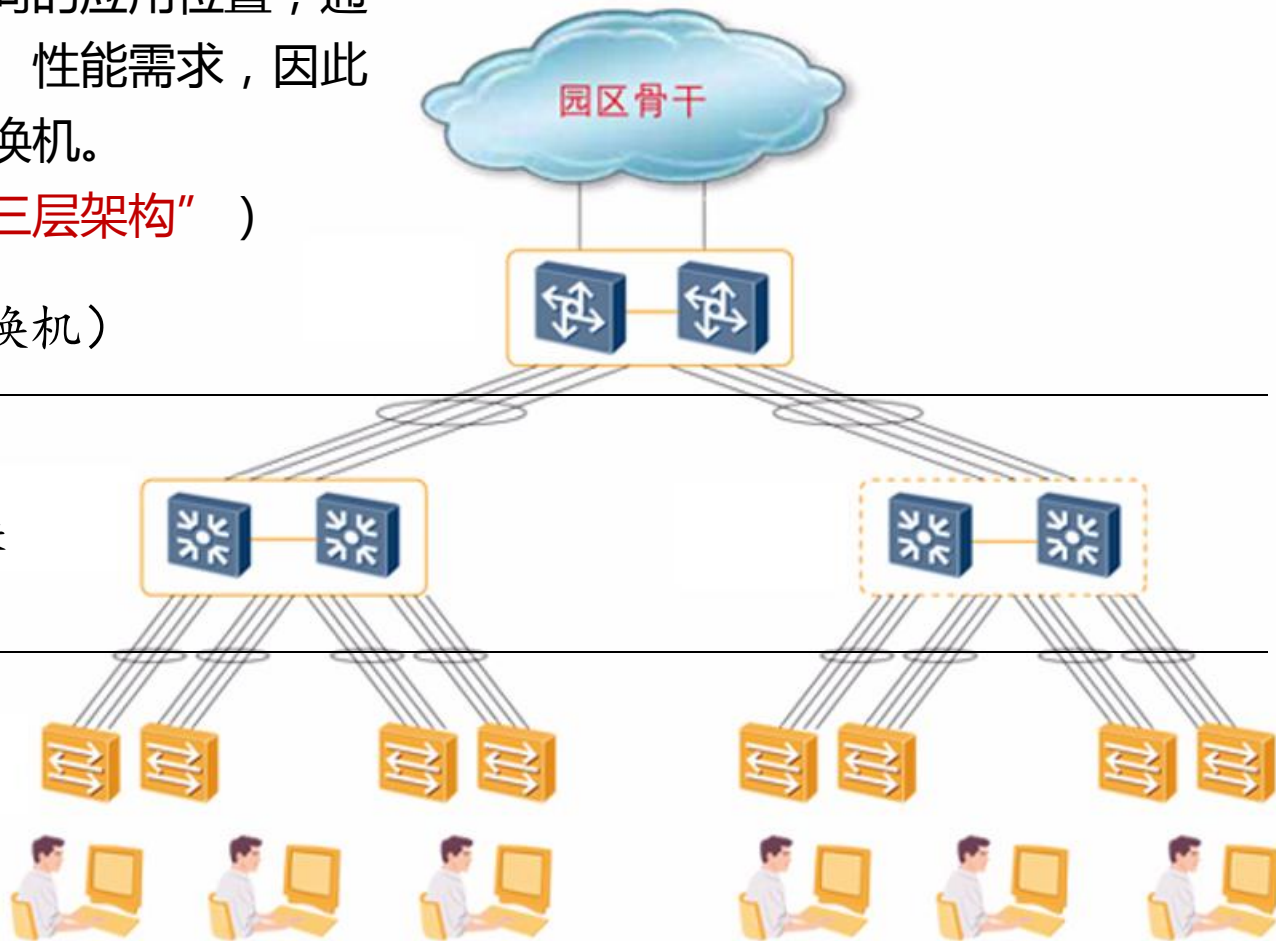
园区网建设中，不同的应用位置，通常会有不同的功能、性能需求，因此选择不同规格的交换机。

（园区网常见的“三层架构”）

核心层（三层交换机）

汇聚层（三层交换机）

接入层（二层交换机）



四、交换机的工作原理



交换机的工作原理

□ 1、依据MAC地址表进行帧的转发

- 交换机是数据链路层设备，它能够读取报文首部中所封装的MAC地址信息；
- 交换机内部会形成一个目的MAC地址与交换机接口之间的对应表，叫做MAC地址表。
- 当交换机收到一个数据帧后，会读取帧首部的目的MAC地址，并根据MAC地址表实现帧的转发，即从对应的接口发送出去。

交换机的工作原理

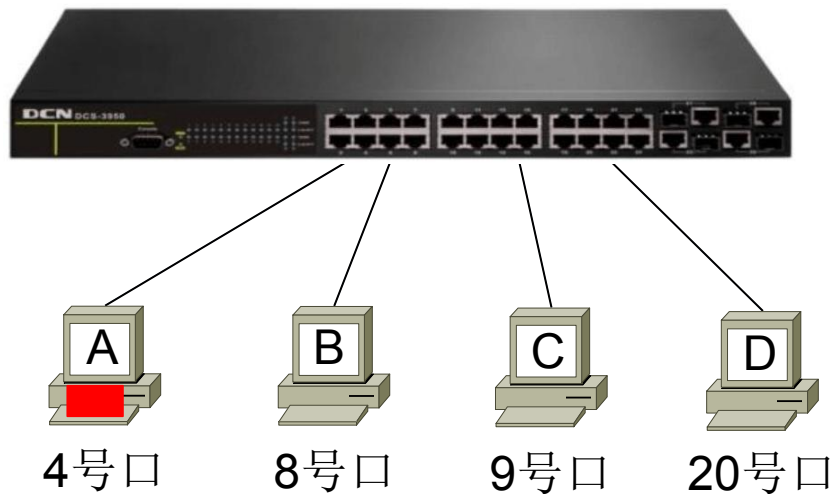
□ 交换机MAC地址表应用举例

交换机的MAC地址表

MAC地址	端口号
MAC_A	4
MAC_B	8
MAC_C	9

A访问C，A在封装报文时，首部中目的MAC是MAC_C。

报文从4号口进入交换机，交换机读取目的MAC，然后查看MAC地址表，从9号口发出该报文。



交换机的工作原理

□ 交换机的MAC地址表是怎样建立起来的？

■ 交换机刚买回来时，不可能知道网络中各主机的MAC地址，也就是说在交换机刚刚打开电源时，其MAC地址表是一片空白。那么，交换机的地址表是怎样建立起来的呢？

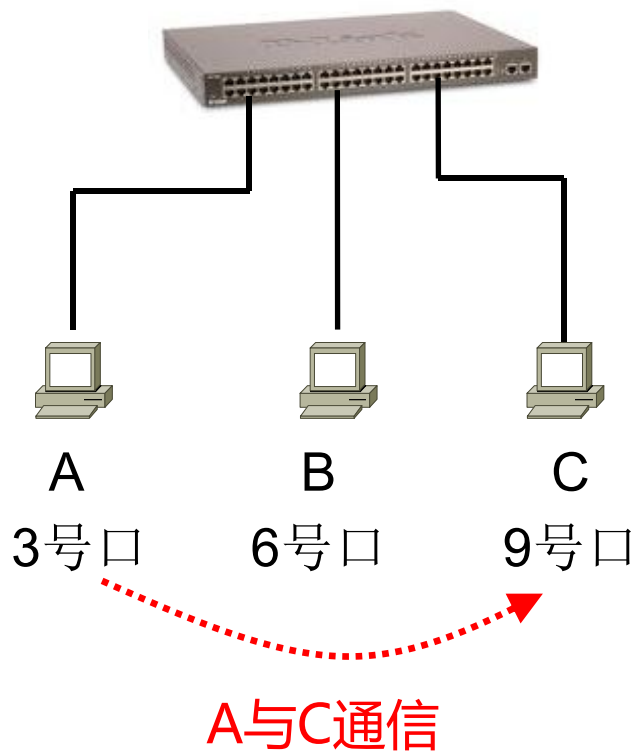
■ 方法1：手工建立

➤ 用户登录交换机，输入接入交换机的主机MAC地址信息以及所对应的接口信息，然后保存配置，又叫“MAC地址绑定”。

■ 方法2：动态生成

➤ 通过“MAC地址学习”功能，自动生成动态的MAC地址表。

◆ 演示：MAC地址学习过程（1）



MAC地址表（刚开机时）

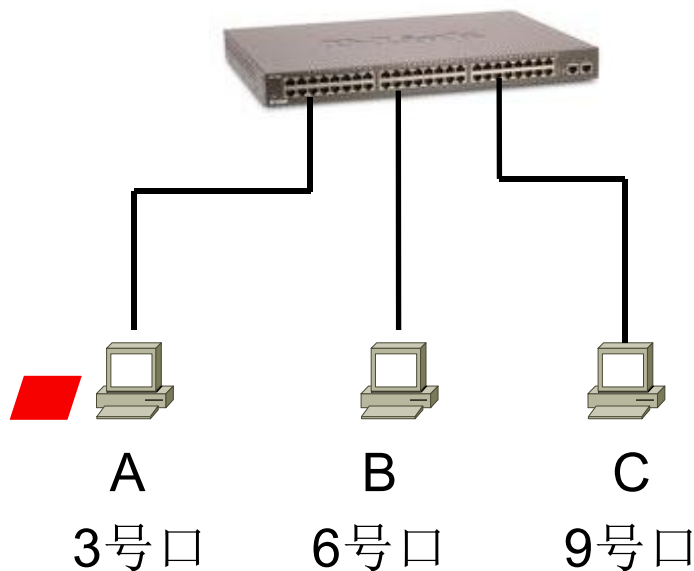
MAC地址	接口

A : 00-01-22-45-e1-03

B : 00-01-22-45-e1-06

C : 00-01-22-45-e1-09

◆ 演示：MAC地址学习过程（2）

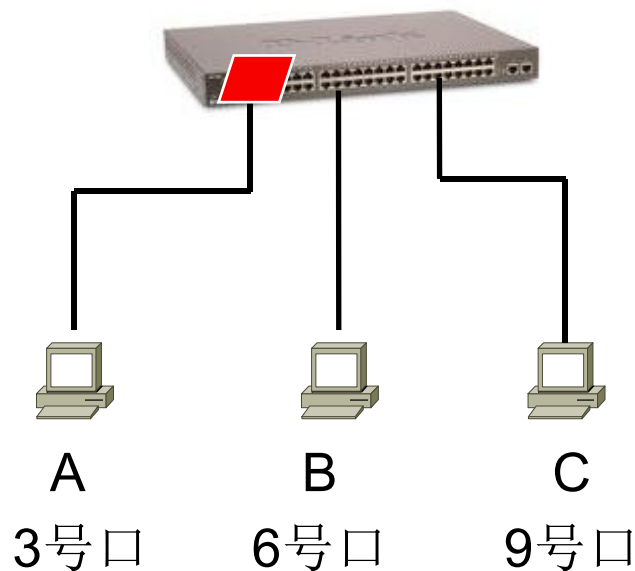


MAC地址表

MAC地址	接口
00-01-22-45-e1-03	3

1. 交换机的3号口收到A发来的数据帧，里面包含有源MAC地址(…-03)和目的MAC地址(…-09)
2. 此时，交换机就知道了3号接口对应的MAC地址(即源MAC地址)。
3. 于是，交换机的MAC表中就有了第1条信息。

◆ 演示：MAC地址学习过程（3）



MAC地址表

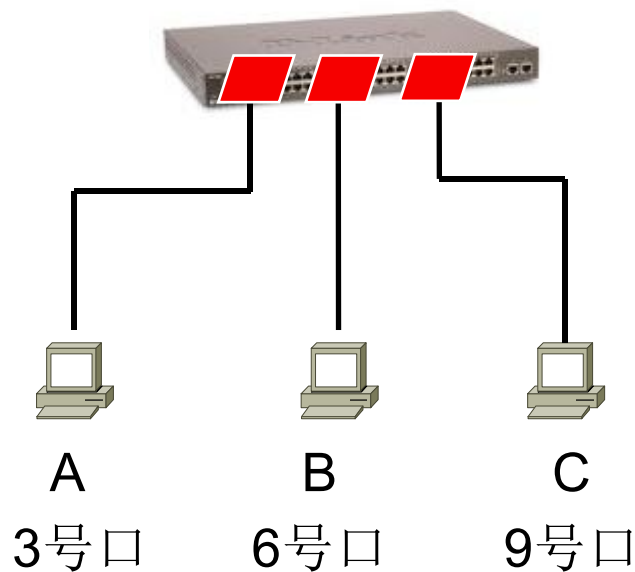
MAC地址	接口
00-01-22-45-e1-03	3

4. 但是，交换机此时不知道目的MAC地址（...-09）对应哪个端口，**接下来**怎么办呢？

采用广播！

注意：若交换机收到的是广播报文，采用同样的做法

◆ 演示：MAC地址学习过程（4）

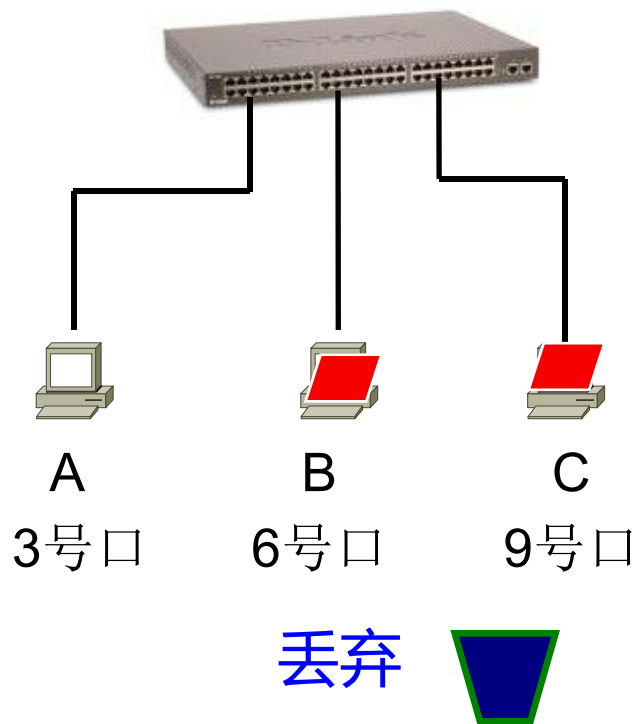


MAC地址表

MAC地址	接口
00-01-22-45-e1-03	3

5. 交换机把帧发到除来源接口外的所有接口，于是B和C都收到了A发来的数据帧。

◆ 演示：MAC地址学习过程（5）

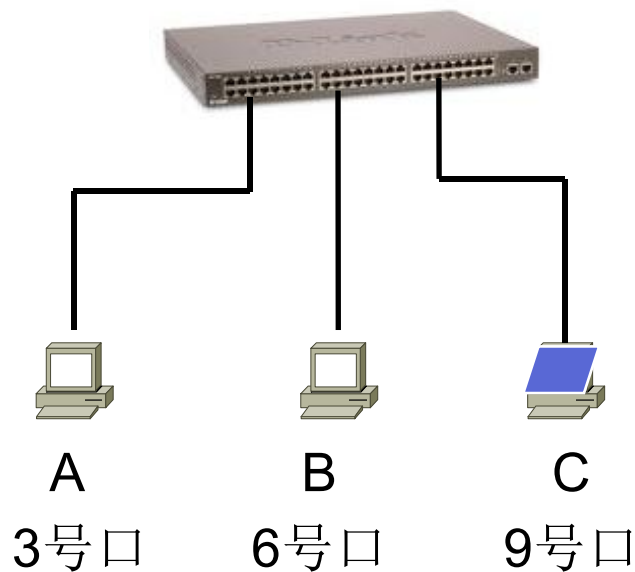


MAC地址表

MAC地址	接口
00-01-22-45-e1-03	3

6. B发现帧中的目的MAC不是自己，就把收到的帧丢弃了。
7. C发现帧中的目的MAC是自己，就收下。

◆ 演示：MAC地址学习过程（6）

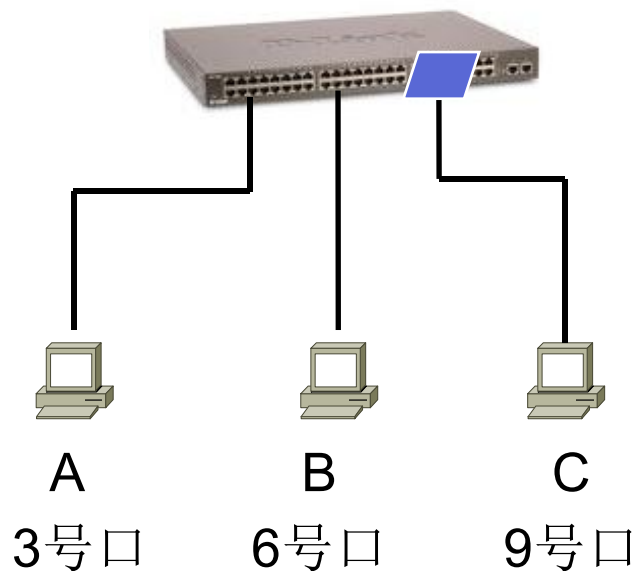


MAC地址表

MAC地址	接口
00-01-22-45-e1-03	3

8. C在接收报文后，要向来源（计算机A）发回一个确认报文。该确认消息的帧中，源MAC是C的MAC地址，目的MAC是A的MAC地址。

◆ 演示：MAC地址学习过程（7）

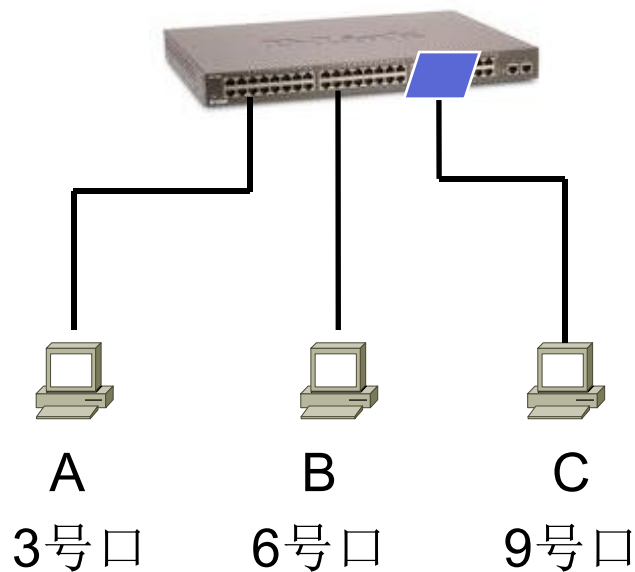


MAC地址表

MAC地址	接口
00-01-22-45-e1-03	3
00-01-22-45-e1-09	9

9. 交换机收到确认帧后，就知道了9号接口对应的MAC地址（通过源MAC地址）。于是MAC地址表就有了第2项信息。

◆ 演示：MAC地址学习过程（8）



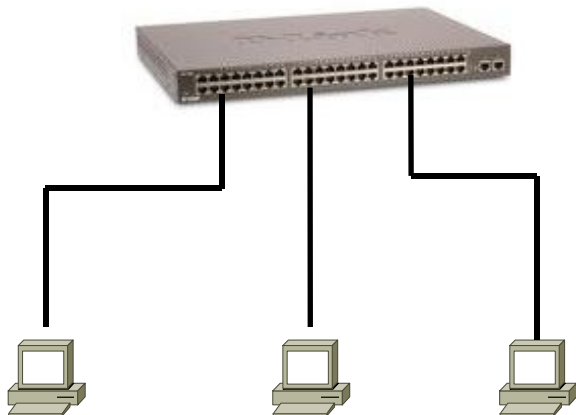
通信完毕

MAC地址表

MAC地址	接口
00-01-22-45-e1-03	3
00-01-22-45-e1-09	9

10. 交换机查询MAC地址表，发现确认帧的目的MAC对应的是3号接口，就把帧转发到3号口，帧最终到达A。

◆ 演示：MAC地址学习过程（9）



上述过程，并不需要人工干预，而是交换机自己完成的，我们把交换机自动建立MAC地址表的过程，称作“MAC地址学习”。

MAC地址表

MAC地址	接口
00-01-22-45-e1-03	3
00-01-22-45-e1-09	9
.....	...

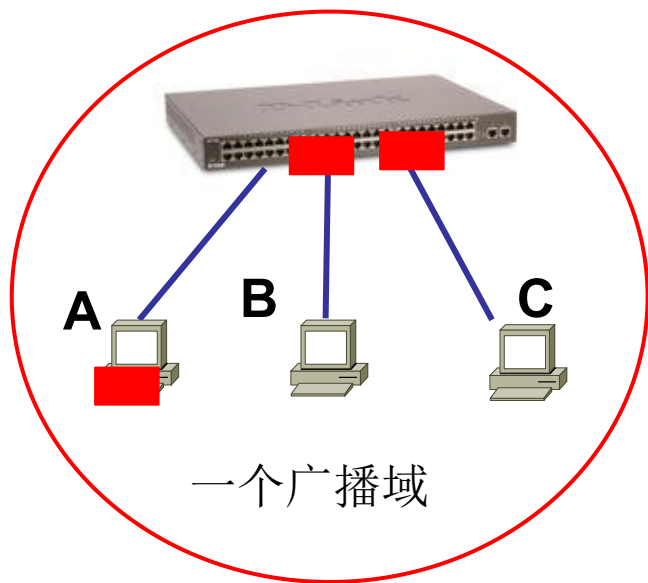
11. 现在，交换机的MAC地址表中就有了A和C的MAC地址以及对应的接口号。当A和C再次通信时，就不需要广播，可以直接单播通信了。
12. 以此类推，交换机的MAC地址表中会出现越来越多的信息

五、交换机的广播域



交换机的广播域

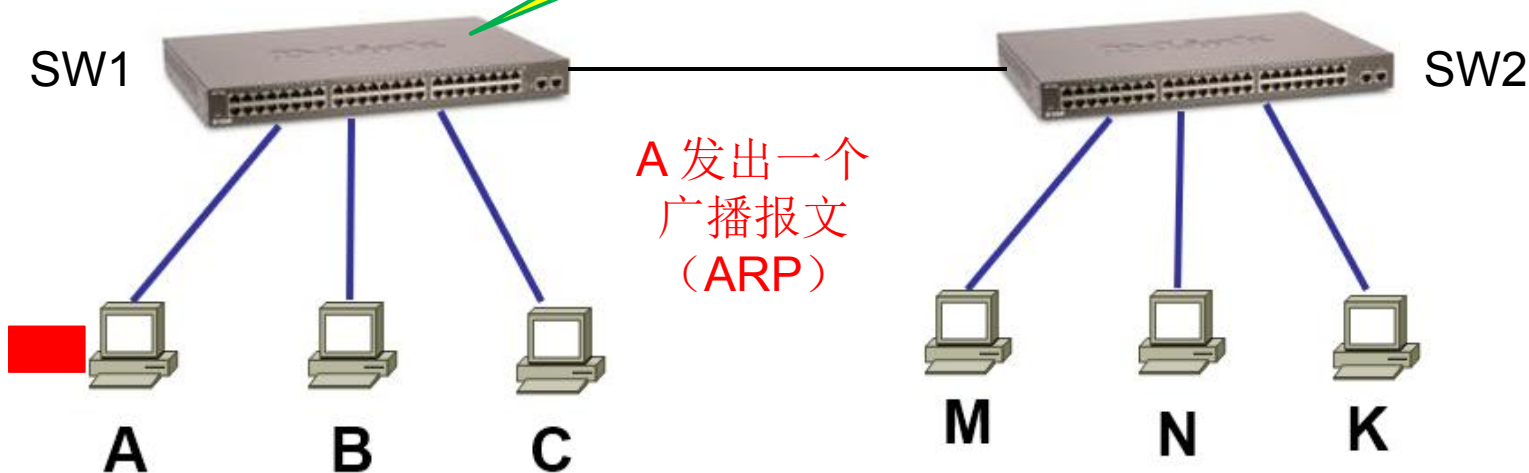
□ 一台交换机的所有接口属于同一个广播域



交换机的广播域

□ 当两台交换机级联在一起呢？

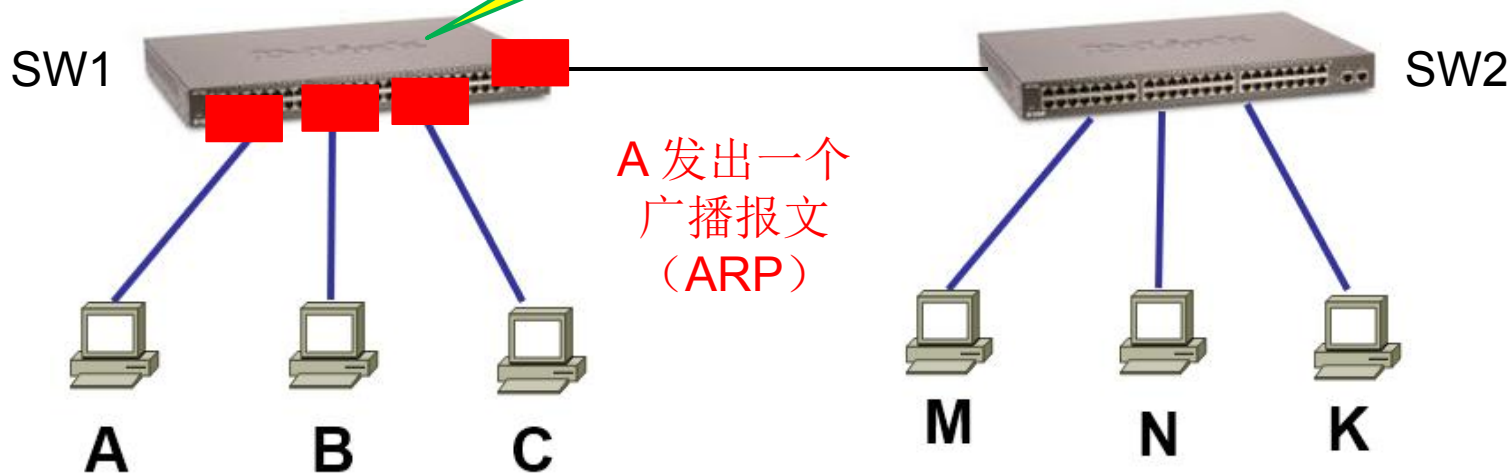
此时交换机SW1
如何处理？



交换机的广播域

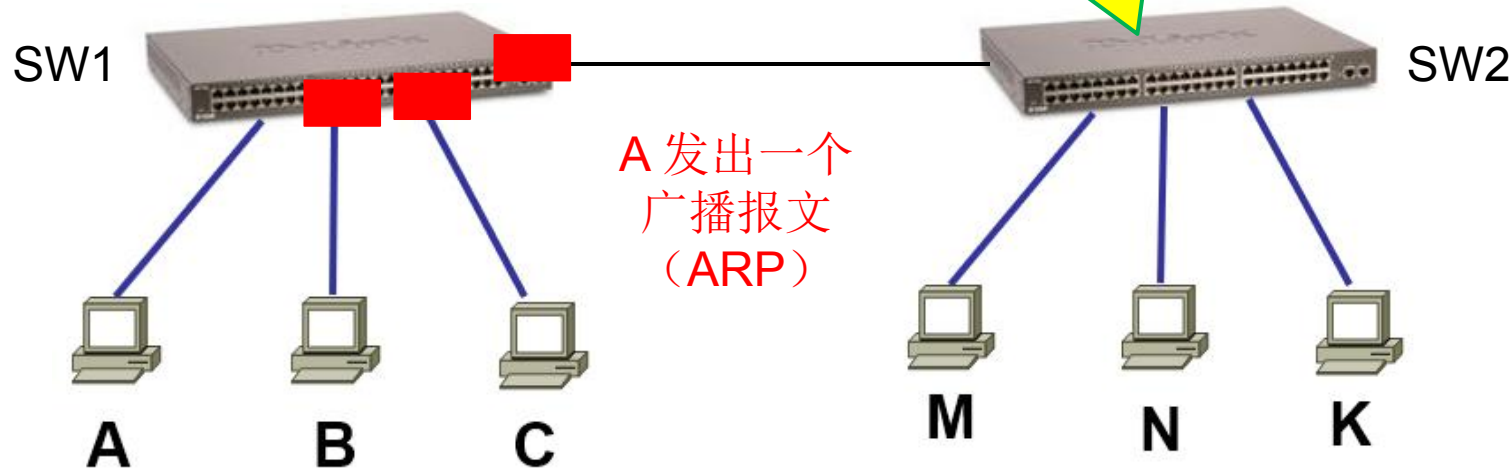
□ 当两台交换机级联在一起呢？

交换机SW1把报文广播到其他所有的接口，包括与SW2连接的接口



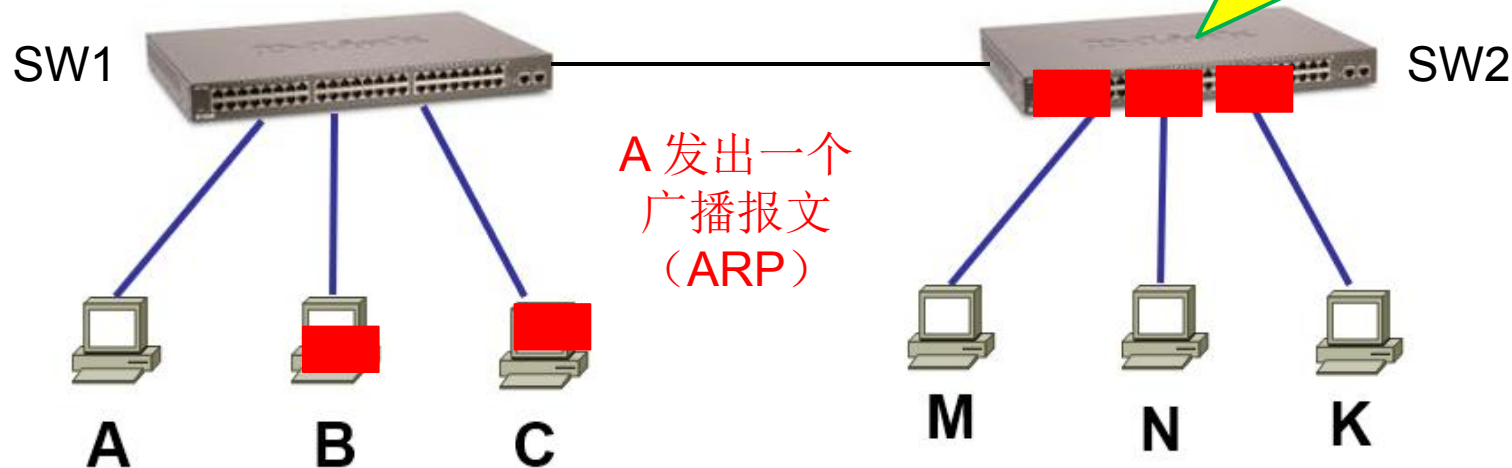
交换机的广播域

□ 当两台交换机级联在一起呢？



交换机的连接

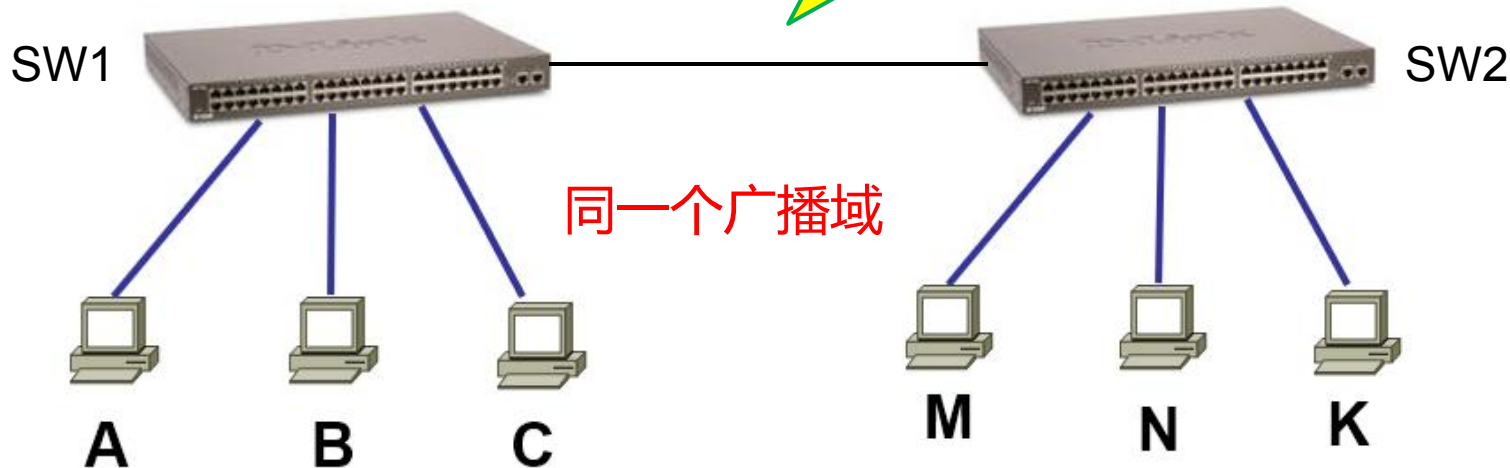
□ 当两台交换机级联在一起呢？



交换机的广播域

□ 当两台交换机级联在一起呢？

交换机级联以后，会形成一个更大的广播域。



交换机的广播域

□ 延伸思考（总结）

- 能不能把交换机无限级联下去，从而形成一个“巨大的网络”？
- 当交换机级联的数量过大时，大量的广播报文将会对整个网络的通信产生非常大的影响，甚至造成网络无法通信。

六、虚拟局域网（VLAN）的应用



虚拟局域网（VLAN）的应用

□ 什么是虚拟局域网？

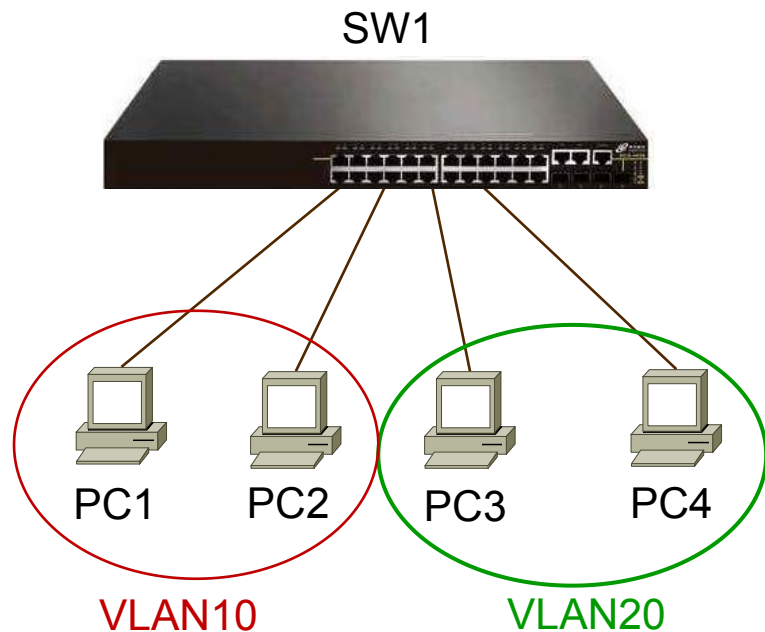
- 虚拟局域网（Virtual Local Area Network，简称VLAN），是一种应用在交换机上的**技术**。IEEE于1999年颁布了用于标准化VLAN实现方案的802.1Q协议标准草案。
- 通过VLAN技术，可以把接入同一台交换机或者接入不同交换机的设备和用户，根据其功能、部门以及应用等因素，将它们划分到不同的逻辑网络，即形成不同的、虚拟的局域网（VLAN），**即属于不同的广播域**；
- **VLAN举例**

虚拟局域网（VLAN）的应用

□ 什么是虚拟局域网？

- 虚拟局域网（Virtual Local Area Network，简称VLAN），是一种应用在交换机上的**技术**。IEEE于1999年颁布了用于标准化VLAN实现方案的802.1Q协议标准草案。
- 通过VLAN技术，可以把接入同一台交换机或者接入不同交换机的设备和用户，根据其功能、部门以及应用等因素，将它们划分到不同的逻辑网络，即形成不同的、虚拟的局域网（VLAN）；
- **VLAN举例**

◆ 例1：接入**同一交换机**的用户主机，被划分为不同的VLAN

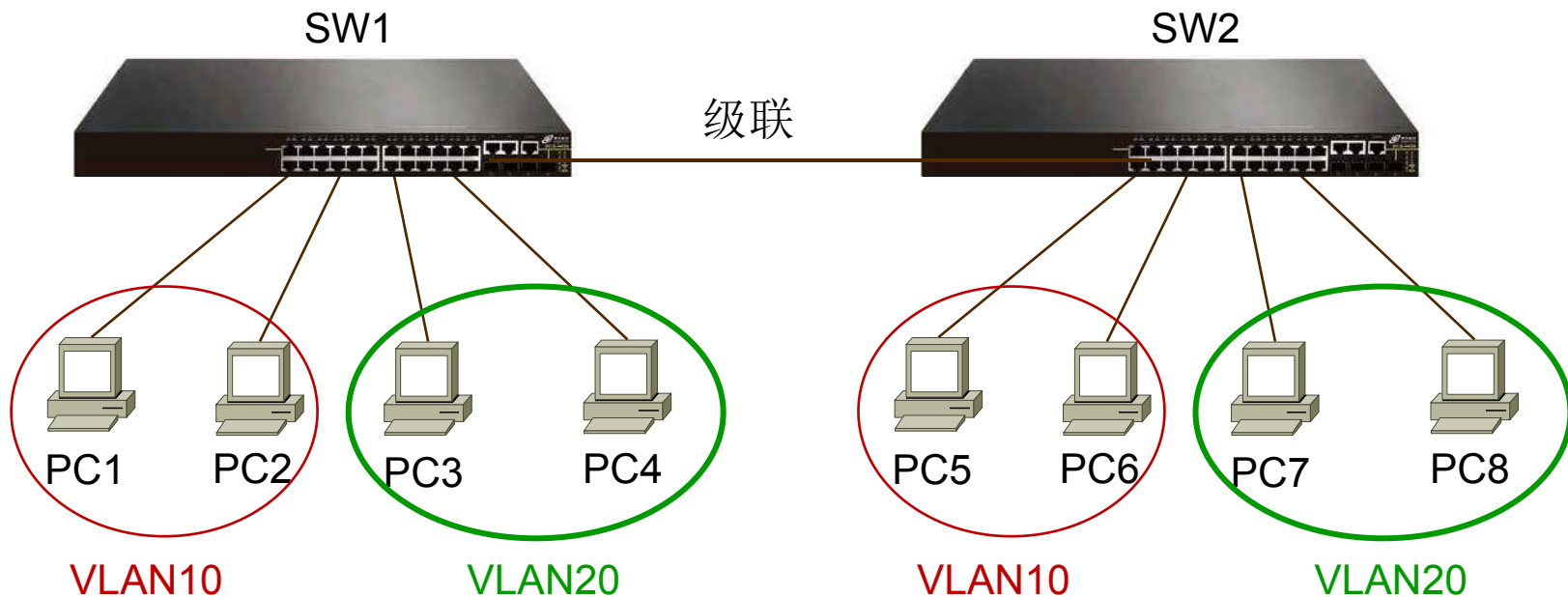


➤ 划分VLAN之后

PC1和PC2属于同一个虚拟局域网（VLAN10）

PC3和PC4属于另一个虚拟局域网（VLAN20）

◆ 例2：接入不同交换机的用户主机，被划分到同一VLAN中



- 此处，PC1、PC2、PC5、PC6属于同一个虚拟局域网（VLAN10）
- PC3、PC4、PC7、PC8属于同一个虚拟局域网（VLAN20）

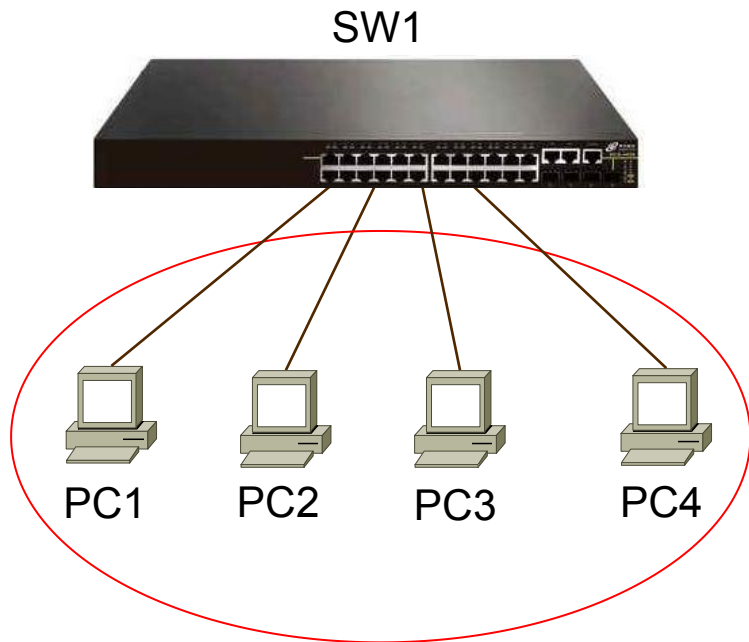
虚拟局域网（VLAN）的应用

□ 为什么使用VLAN？

■ 限制交换机的广播域范围

- 交换机默认情况下，所有接口属于同一广播域。级联的交换机，属于同一个更大的广播域。
- 在交换机上配置VLAN，可以在逻辑上划分出不同的广播域。
- 一个VLAN就是一个独立的广播域，即同一个VLAN中的设备，可以直接通信，就像它们在同一个物理网段中一样；但不同VLAN之间，是无法直接通信的，必须通过三层路由设备来完成转发。
- 虚拟局域网（VLAN）的使用，限制了交换机组成的网络中，接收广播信息的主机数，使得不会因广播域过大引起网络性能下降。
- 举例

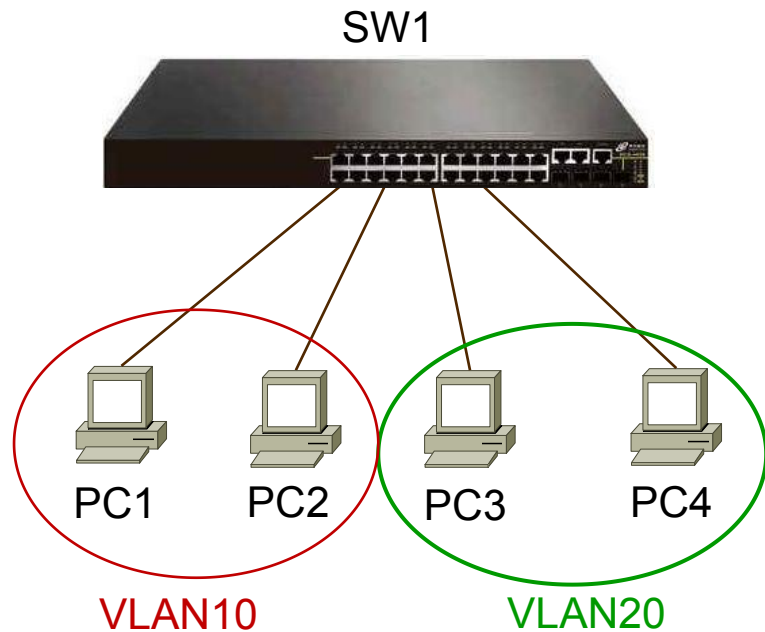
◆ 演示：VLAN限制广播域范围



➤ 划分VLAN之前

所有用户主机属于同一个广播域

◆ 演示：VLAN限制广播域范围

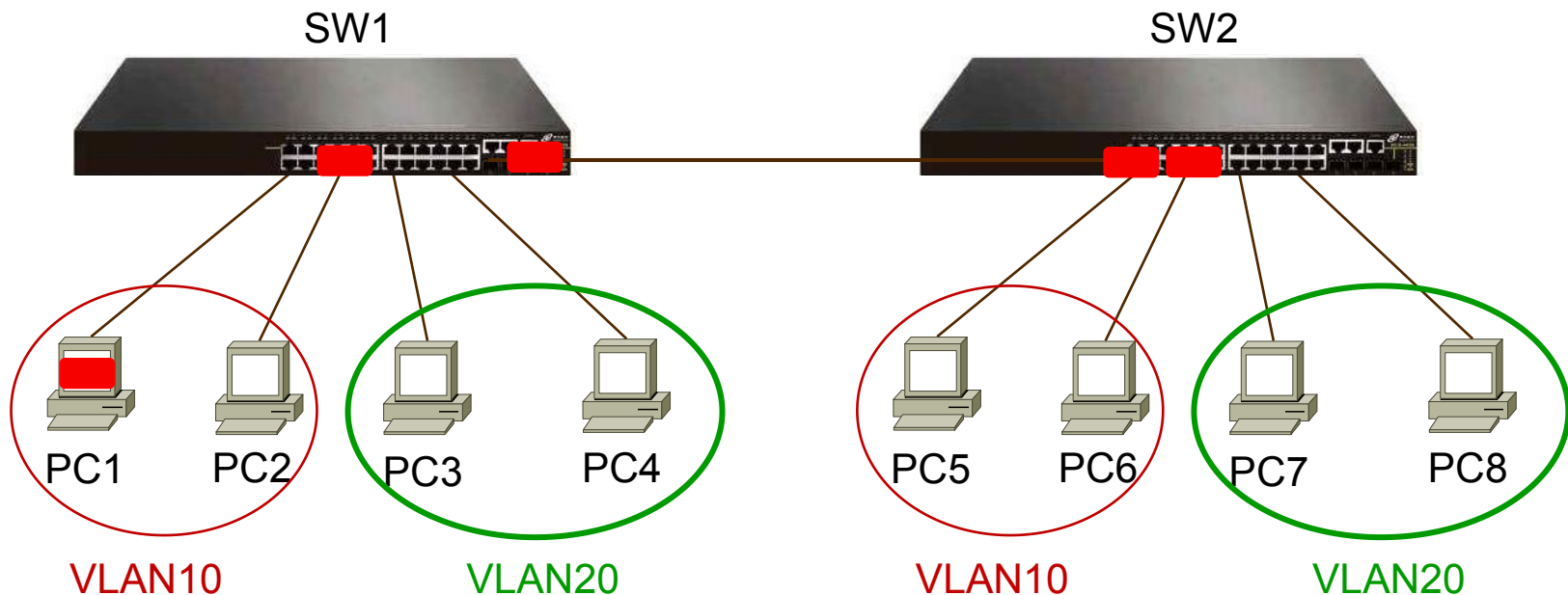


➤ 划分VLAN之后

PC1和PC2属于同一个广播域

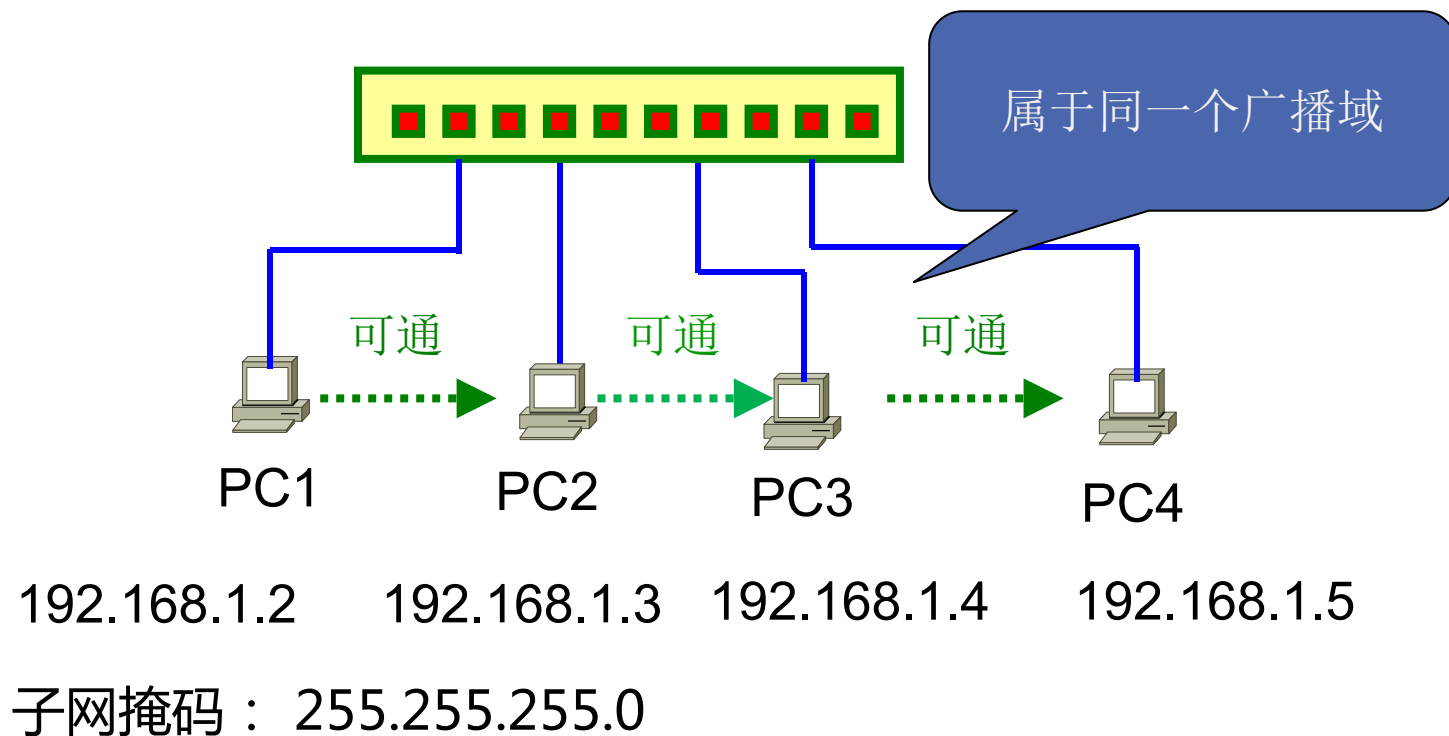
PC3和PC4属于另一个广播域

◆ 演示：VLAN限制广播域范围

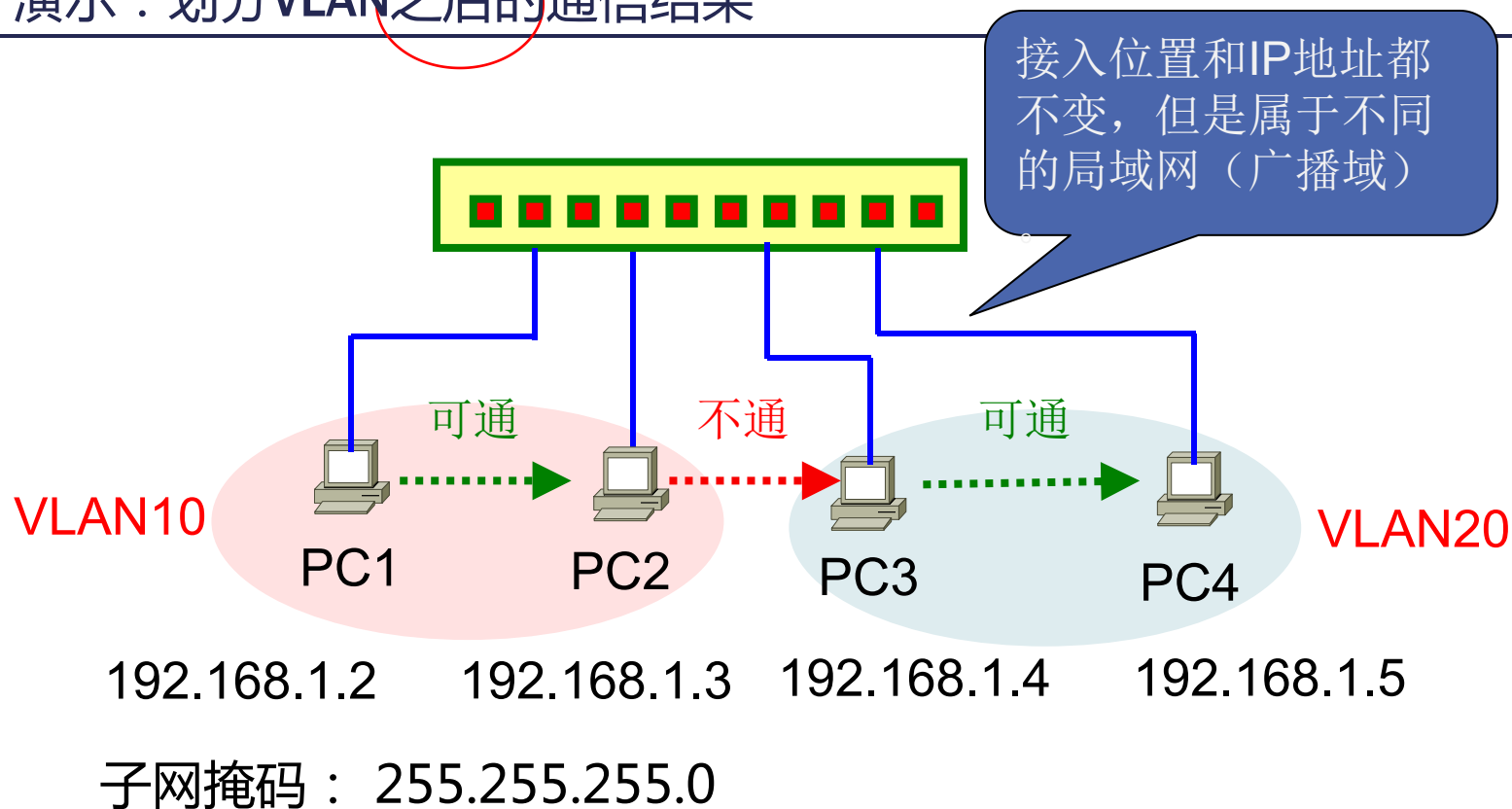


- 划分VLAN前，当PC1发出广播包时，PC2—PC8都能收到；
- 划分VLAN后，当PC1发出广播包时，只有属于同一个VLAN的设备（包括PC2、PC5、PC6）能够收到，即VLAN隔离了广播。

◆ 演示：划分VLAN之前的通信结果



◆ 演示：划分VLAN之后的通信结果



七、VLAN的划分方式

—— 如何在交换机上创建VLAN?

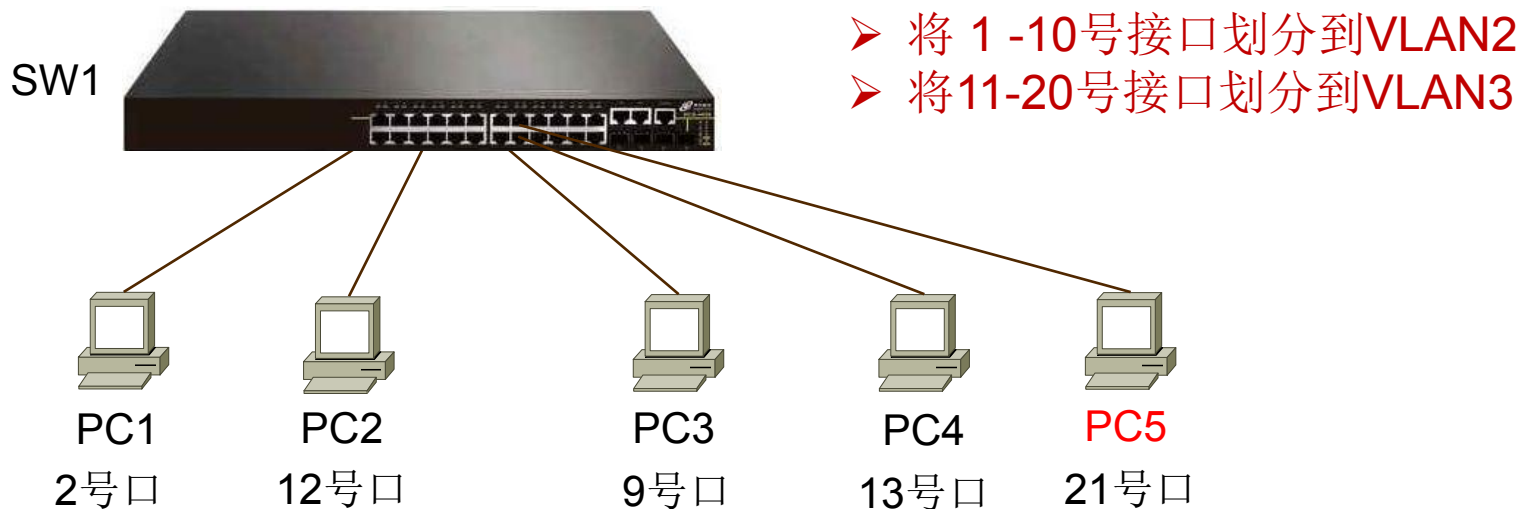
VLAN的划分方式

□ 基于接口划分VLAN

- 这是最常应用的创建VLAN的方法。
- 它在交换机上创建VLAN，然后将指定的接口划分入指定的VLAN，属于同一VLAN的接口就构成一个虚拟局域网，具有与其他接口组不同的广播域。
- 举例

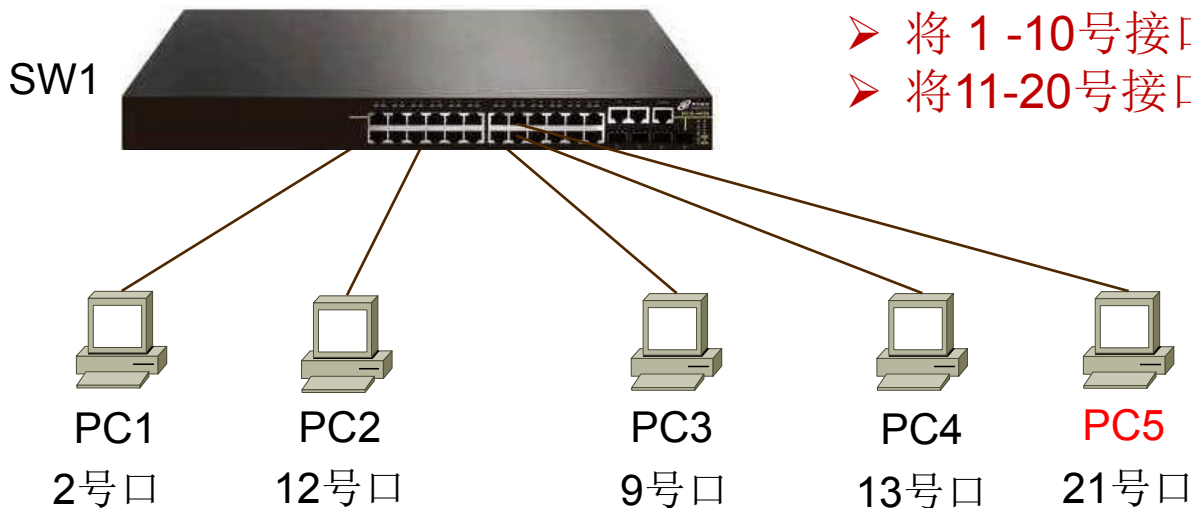
[SW-1]vlan 10	//创建VLAN10
[SW-1]interface Ethernet0/0/1	//进入接口Ethernet 0/0/1视图
[SW-1-Ethernet0/0/1]port link-type access	//配置接口类型为Access
[SW-1-Ethernet0/0/1]port default vlan 10	//将Ethernet0/0/1划分到VLAN10

◆ 示例：基于交换机接口划分VLAN —— 单交换机



- PC1和PC3属于VLAN2，在同一个广播域内，相互之间可直接通信；
- PC2和PC4属于VLAN3，在同一个广播域内，相互之间可直接通信；

◆ 示例：基于交换机接口划分VLAN —— 单交换机



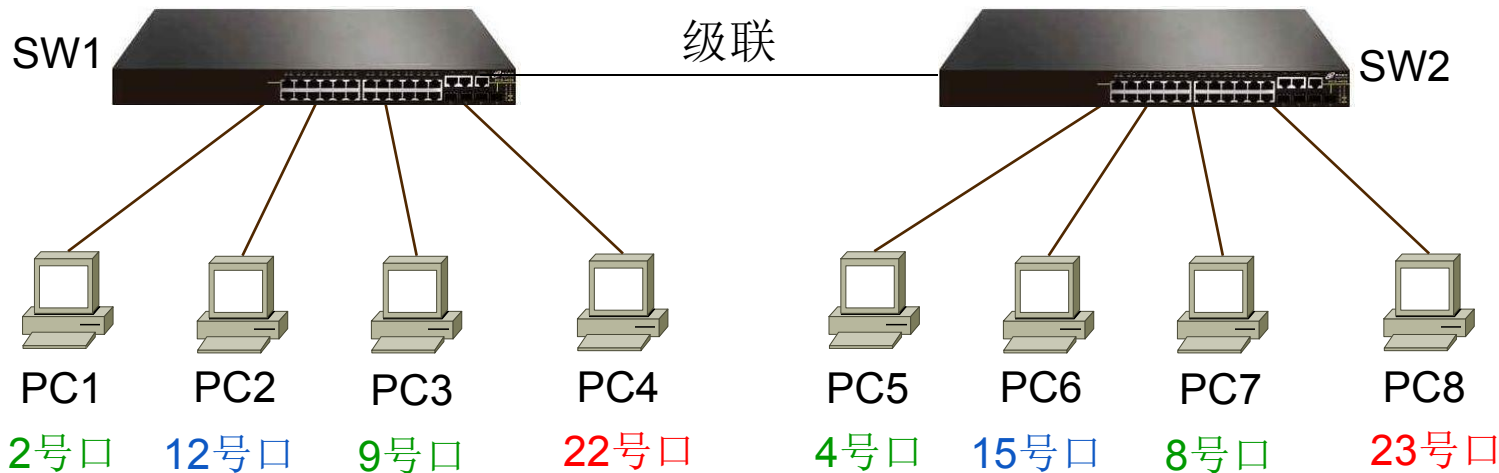
- 将 1 -10号接口划分到VLAN2
- 将11-20号接口划分到VLAN3

➤ PC5属于：VLAN1

【注意】VLAN 1是系统自带的VLAN，不需要创建，也不可以删除。在缺省情况下，交换机的所有接口都属于VLAN1。

◆ 示例：基于交换机接口划分VLAN —— 跨交换机

➤ 将每台交换机的 1-10号接口划分到VLAN2，将11-20号接口划分到VLAN3



- PC1、PC3、PC5、PC7属于VLAN2，在同一个广播域内，可直接通信；
- PC2和PC6属于VLAN3，在同一个广播域内，可直接通信；
- PC4和PC8属于VLAN1，在同一个广播域内，可直接通信；

VLAN的划分方式

□ 基于MAC地址划分VLAN（自主学习）

- 基于接口划分VLAN时，当用户主机从交换机一个接口换到另一个接口时，所属VLAN就可能发生改变。若要保持VLAN不变，就需要重新配置接口，因此，通常用于用户主机位置不变的场合；
- 当用户对安全和移动性需求较高时，可以使用基于MAC地址划分VLAN的方法，即将用户计算机的MAC地址与指定的VLAN绑定起来，用户在变换物理位置后不需要重新划分VLAN，提高了终端用户的安全性和接入的灵活性。。

VLAN的划分方式

□ 其他划分VLAN的方法（略）

- 基于协议划分VLAN
- 根据IP组播划分VLAN
- 按策略划分VLAN
- 按用户定义、非用户授权划分VLAN

注意：本课程重点讲授基于接口划分VLAN的应用

八、IEEE802.1Q帧的结构与应用

- 应用VLAN后，帧结构有何变化？
- 应用VLAN后，交换机的通信有何变化？

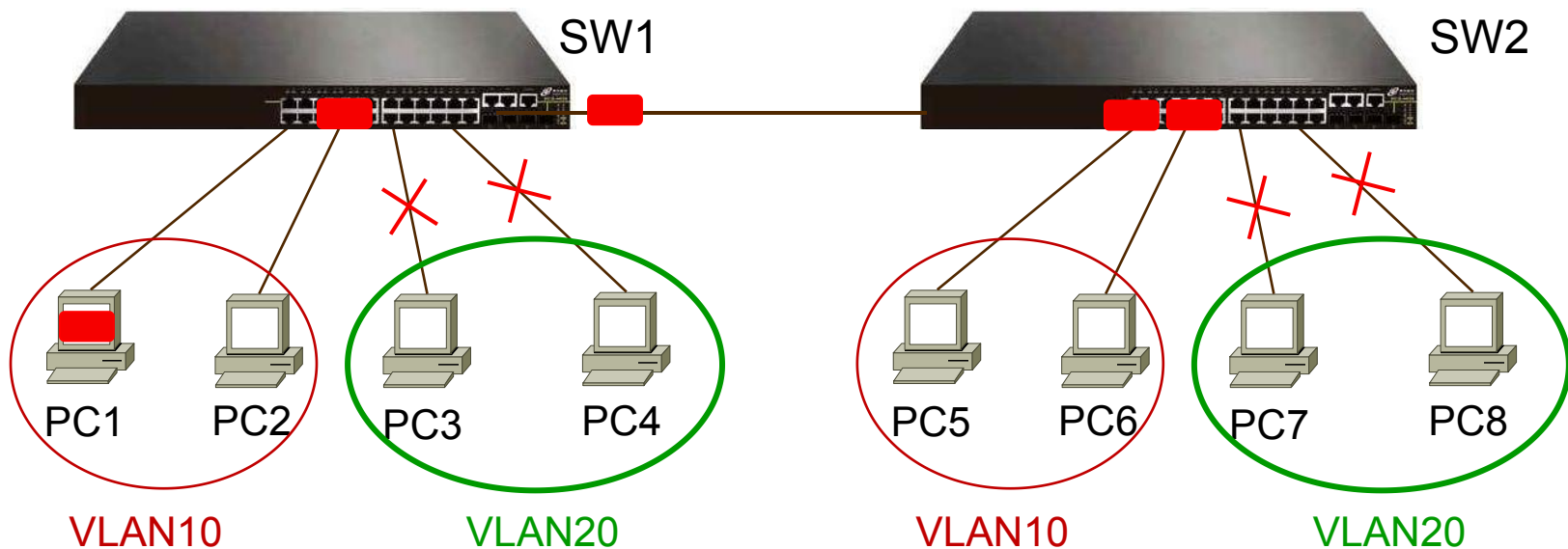
IEEE802.1Q帧的结构与应用

□ IEEE802.1Q标准

- IEEE于1999年颁布了用于标准化VLAN实现方案的802.1Q协议标准草案。
- IEEE 802.1Q标准提供了对VLAN明确的定义及在交换式网络的应用。该标准的发布，确保了不同厂商提供的产品间的互操作能力，并在业界获得了广泛的推广，成为VLAN发展史上的里程碑。
- IEEE 802.1Q的出现打破了VLAN依赖单一厂商的僵局，从而推动了VLAN技术的迅速发展。

IEEE802.1Q帧的结构与应用

- 创建了VLAN的交换机，如何知道从某一个接口进入的数据帧是属于哪个VLAN呢？（例，SW1如何知道PC1发出的帧，不能发给PC3和PC4呢？）



IEEE802.1Q帧的结构与应用

□ 创建了VLAN的交换机，如何知道从某一个接口进入的数据帧是属于哪个VLAN呢？

- 解决的方法就是：给普通帧（以太网帧）加上VLAN标签。
- IEEE 802.1Q标准规定：配置VLAN的交换机，在接收到以太网帧后，入接口会自动在帧头中的源MAC地址后增加一个4字节的802.1Q标签，用来指明该帧的VLAN属性。
- 这样，一个普通帧（untagged帧），就变成了802.1Q帧（tagged帧），会依据交换机的VLAN配置，进行传输。
- 802.1Q帧结构？（见下页）

➤ 802.1Q的帧结构

802.1Q帧



1. 2字节的协议标识符，置0x8100固定值，表明该帧带有802.1Q标记信息；
2. 2字节的标记控制信息，包含了3个域：
 - ① 表示报文优先级，占3bit，取值0到7，7为最高；
 - ② 表示规范格式指示符，占1bit，0表示规范格式，应用于以太网，1表示非规范格式，应用于Token Ring；
 - ③ VID：表示VLAN编号，占12bit，用于表示VLAN的归属，其中，VID=0用于识别帧优先级，4095 (FFF) 作为预留值，**所以有效的VLAN ID范围为1-4094。**

IEEE802.1Q帧的结构与应用

□ 划分VLAN后，交换机如何转发数据？

- **回忆：**交换机在收到数据帧之后，通常会根据帧首部的MAC地址与自身的MAC表来决定如何转发数据帧。这里我们将VLAN信息结合在一起理解。
- 引入VLAN概念后，MAC地址表项中，增加了VLAN ID属性，表示接口所属的VLAN。
- **举例说明**

➤ 举例：划分VLAN后，交换机如何转发数据？

目的 MAC地址	VLAN ID	接口
MAC_PC1	1	1
MAC_PC2	1	2
MAC_PC3	2	4
MAC_PC4	3	6

- 主机发出的数据帧是untagged帧，进入交换机后，被加上VLAN标签成为tagged帧，其中的VID值等于入接口所属的VLAN值；
- 交换机在MAC地址表中查找时，不仅要判断目的MAC是否匹配，还要判断相应接口的VID值是否与tagged帧的VID值相同，若全部匹配则转发，否则就丢弃。

例如：交换机内部的一个tagged帧，帧头中目的MAC是PC3-MAC，VLAN标签中VID=4
处理：虽然目的MAC与第3条记录对应，但因为帧的VID与对应接口的VID值不匹配，丢弃

IEEE802.1Q帧的结构与应用

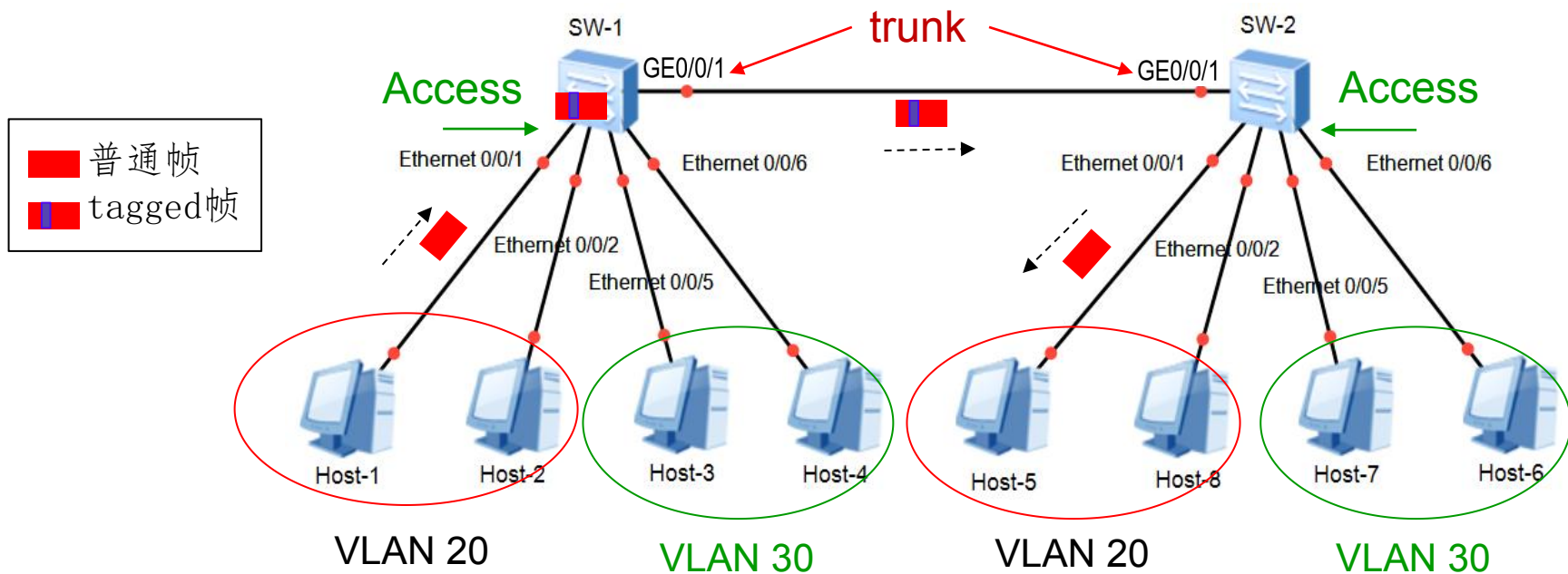
□ 802.1Q帧的传输

- 一个untagged帧进入交换机，被加上入接口的VLAN标签，变为tagged帧；
- 当tagged帧从交换机中发出时，VLAN标签是保留？还是去掉？
- 简单说，分两种情况：
 - 进行VLAN配置时，根据需要，可将接口配置成Access类型或者Trunk类型
 - 从Access口发出时，去掉VLAN标签；从Trunk口发出时，保留VLAN标签；
 - 将连接主机的接口设为Access口，因为主机无法识别tagged帧；
 - 交换机互连接口设为Trunk口，因为对端交换机需要根据VLAN标签判断下一步的转发；

IEEE802.1Q帧的结构与应用

802.1Q帧的传输

- 将连接主机的接口设为Access口，交换机互连接口设为Trunk口



操作案例：Access接口和Trunk接口的配置（华为交换机为例）

【在SW1上进行配置】（SW2的配置同理）

//创建VLAN10和VLAN20

```
[SW-1]vlan batch 10 20 //创建VLAN20和VLAN30
```

//将Ethernet0/0/1和Ethernet0/0/2接口设置成Access类型并划入VLAN10

```
[SW-1]interface Ethernet 0/0/1
```

```
[SW-1-Ethernet0/0/1]port link-type access
```

```
[SW-1-Ethernet0/0/1]port default vlan 10
```

```
[SW-1]interface Ethernet0/0/2
```

```
[SW-1-Ethernet0/0/2]port link-type access
```

```
[SW-1-Ethernet0/0/2]port default vlan 10
```

//将Ethernet0/0/5和Ethernet0/0/6设成Access类型并划入VLAN20，操作同理

//将GEO/0/1接口设置成Trunk类型并允许VLAN10和VLAN20的数据帧通过

```
[SW-1]interface GigabitEthernet 0/0/1
```

```
[SW-1-GigabitEthernet0/0/1]port link-type trunk
```

```
[SW-1-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
```

九、路由交换机实现不同VLAN之间的通信

——路由交换机的应用

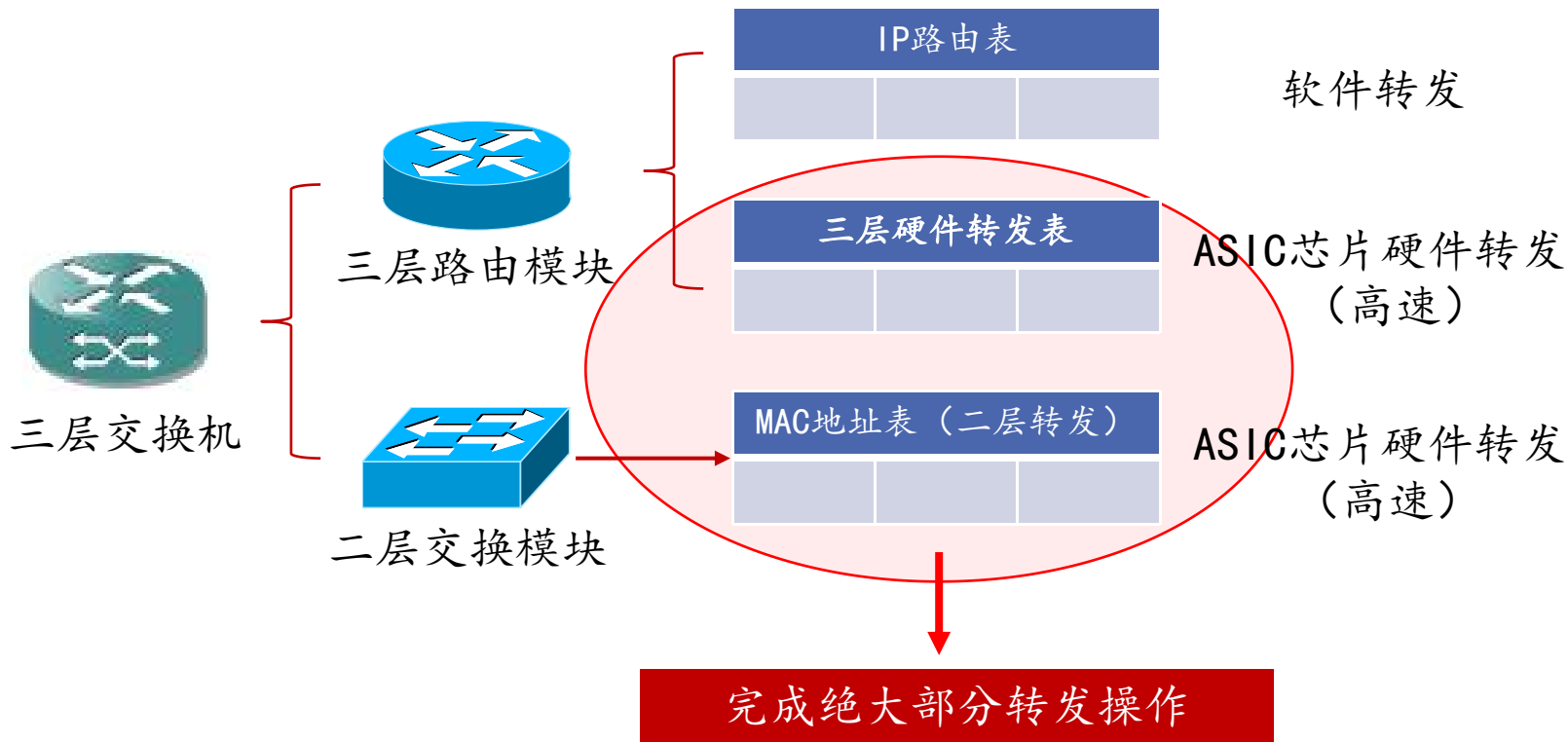
路由交换机实现不同VLAN之间的通信

□ 为什么使用路由交换机？

- 在**实际应用**中，通常使用**路由交换机实现VLAN间的通信**。路由交换机又叫**三层交换机**，除了二层交换机的功能之外，还具有第三层路由功能，即可以像路由器一样实现不同子网（主要指不同VLAN）之间的通信；
- 在一些园区网中，会将三层交换机用在网络的核心层，用三层交换机上的千兆接口或百兆接口连接不同的子网或VLAN，从而实现不同VLAN（子网）之间的高速转发。
- 与**路由器**主要通过**软件方式**进行**路由转发**不同，三层交换机在工作中主要使用硬件芯片进行IP的路由功能，因此路由过程效率大大提高，解决了传统路由器软件路由的速度问题；

三层交换机如何转发报文？

□ 三层交换机内部的“三张表”

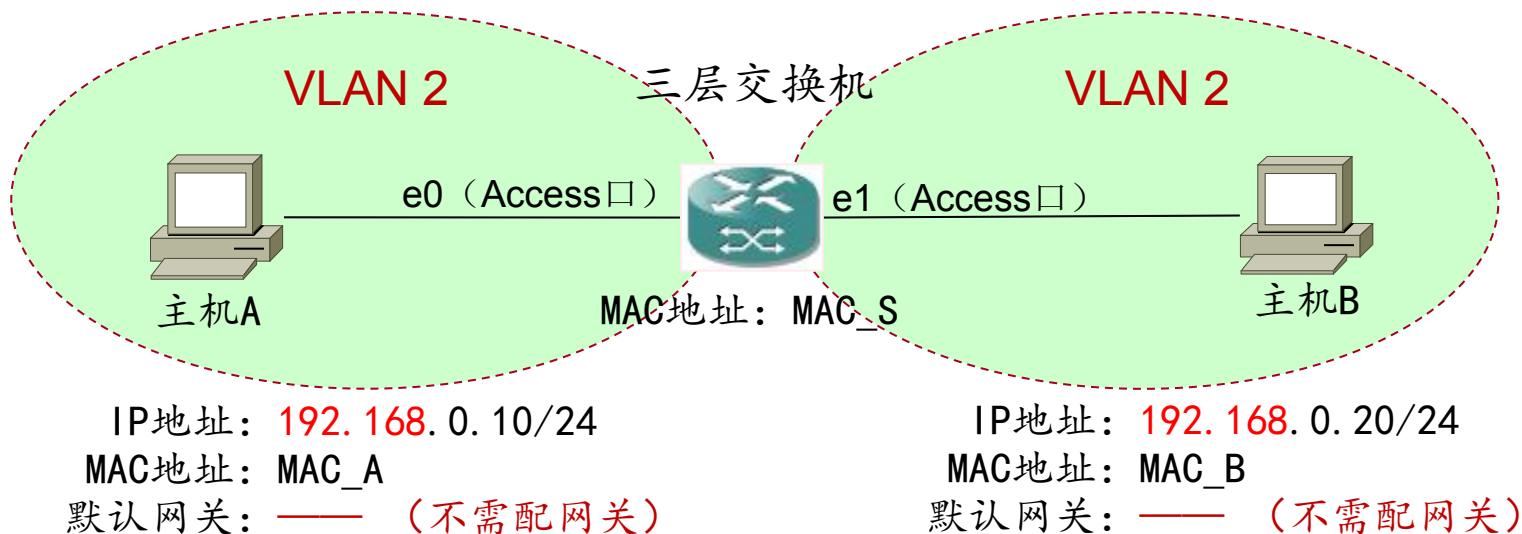


三层交换机如何转发报文？

□ 情况1：同一网络（即同一VLAN）内部，不同主机间的通信

■ 同二层交换机，查看帧首部的目的MAC地址，并根据MAC地址表进行转发

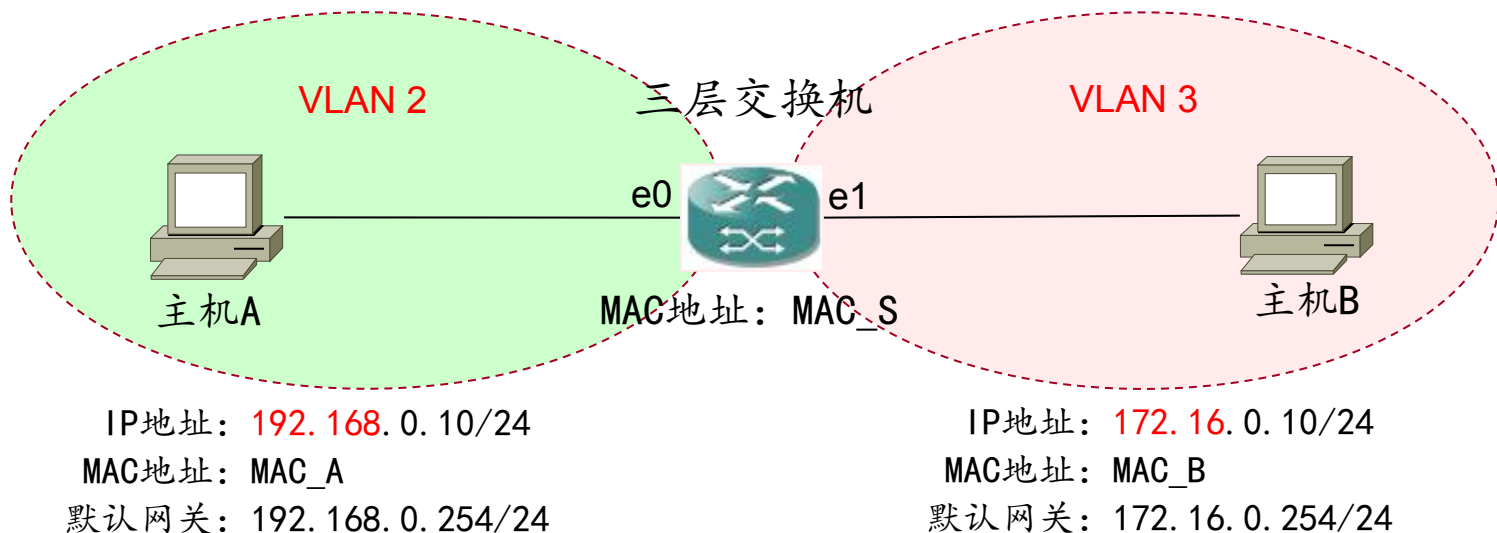
➤ 若A不知道B的MAC地址，直接ARP即可。



三层交换机如何转发报文？

□ 情况2：属于不同网络（即不同VLAN）的主机之间进行通信

- 启用三层路由模块！在三层交换机上配置所连接VLAN的默认网关（生成直连路由），读取所收到报文的IP地址，查询（匹配）路由表，完成报文在不同网络（VLAN）间转发。



三层交换机如何转发报文？

□ 进一步分析：三层交换机上如何进行路由配置？

■ 三层交换机和路由器不同！

- 三层交换机上的接口默认属于二层接口，因此无法像路由器那样直接给某个接口配置IP地址，并且接口也不具有独立的MAC地址（三层交换机上所有接口共用一个MAC地址）。
- 因此，三层交换机不能像路由器那样，通过直接给一个物理接口配置IP地址，使其成为所直连网络的默认网关，或者使其成为与其他路由互连的“下一跳”。

■ 怎么办？

华为三层交换机采用“三层虚拟接口”的方式解决上述问题

三层交换机如何转发报文？

□ 华为三层交换机上的“三层虚拟接口”

■ SVI (Switch Virtual Interface, 交换机虚拟接口)

➤ SVI接口多用于三层交换机，是一种三层逻辑（即虚拟）接口。通常用于两个地方：

1. 作为三层交换机直连VLAN的默认网关，又叫“VLAN接口”（注意，不是属于某个VLAN的接口）
2. 作为与其他路由设备互连的、下一跳的虚拟路由接口。

➤ 接下来，分别谈谈这两种应用的实现方式。

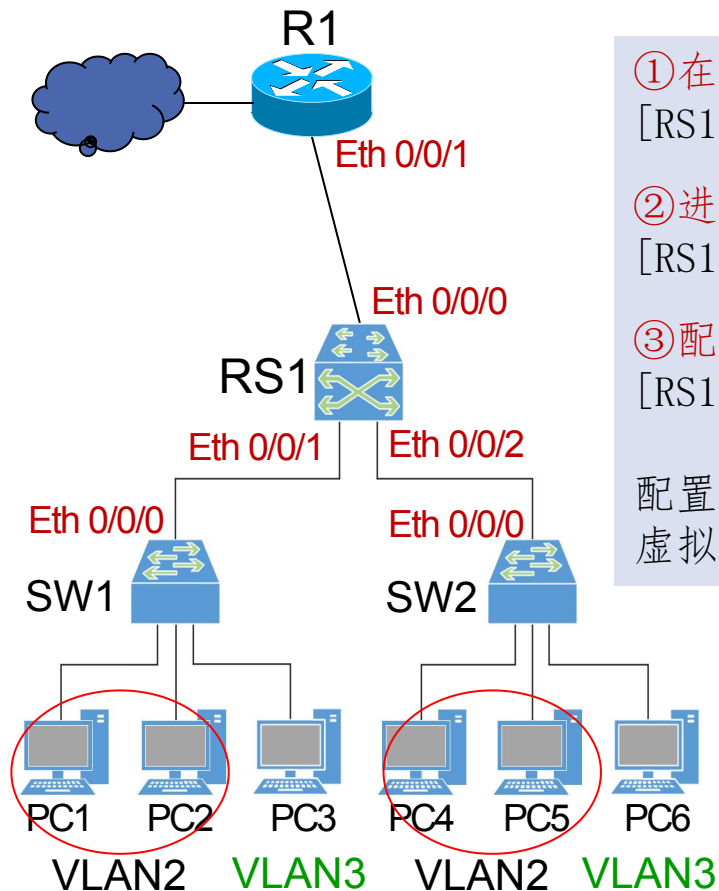
三层交换机如何转发报文？

□ 华为三层交换机上的“三层虚拟接口”

■ 应用1：作为三层交换机直连网络（即直连VLAN）的“默认网关”

- 三层交换机的一个重要应用，就是实现VLAN之间（例如VLAN2和VLAN3之间）的通信。此时就要在三层交换机上分别配置相应VLAN的默认网关。
- 例如，在三层交换机上配置VLAN2的默认网关，包含3步操作：
 1. 首先在三层交换机上创建相应的VLAN（即VLAN2）
 2. 进入VLAN2的接口视图，即进入VLAN2的SVI接口
 3. 给VLAN2的SVI接口配置IP地址/掩码
- 然后，将属于VLAN2的各主机的默认网关地址，配置成三层交换机上VLAN2的SVI接口地址即可。
- 举例

案例1：在三层交换机上配置SVI接口，并作为VLAN2的默认网关



①在三层交换机上创建VLAN2

```
[RS1]vlan 2
```

②进入VLAN2的接口视图，即创建VLAN2的SVI接口

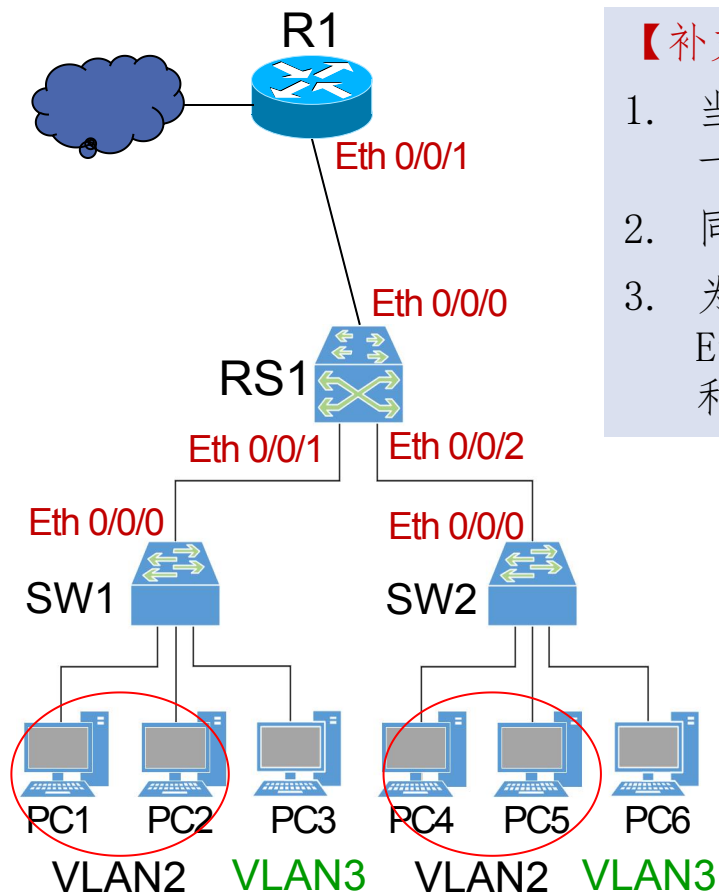
```
[RS1]interface vlanif 2
```

③配置VLAN2的SVI接口IP地址/掩码（假设172.16.1.254/24）

```
[RS1-Vlanif2]ip address 172.16.1.254 255.255.255.0
```

配置完毕！在RS1上有了VLAN2的默认网关，它其实是一个三层虚拟接口，其地址是172.16.1.254/24。

案例1：在三层交换机上配置SVI接口，并作为VLAN2的默认网关



【补充说明】

1. 当完成前面配置后，在三层交换机的路由表中会自动生成一条直连路由记录。其目的网络是172.16.1.0/24；
2. 同理，也可以在RS1配置VLAN3的默认网关；
3. 为实现VLAN2和VLAN3之间的通信，还需要将RS1的Eth0/0/1和Eth0/0/2接口都设置成trunk类，并允许VLAN2和VLAN3的帧流量通过。

【转发描述】 PC1 ping PC6

1. PC1发现和PC6不是同一网络，因此首先将报文发给默认网关（172.16.1.254），并通过ARP获取到默认网关的MAC地址（即RS1的MAC）；
2. 报文到达RS1上的VLANif 2接口（VLAN2的SVI接口，即默认网关），通过查看路由表，匹配到达VLAN3的直连路由；
3. 报文从RS1上的VLANif 3接口（VLAN3的SVI接口）发出，最终到达PC6。（返程略）

三层交换机如何转发报文？

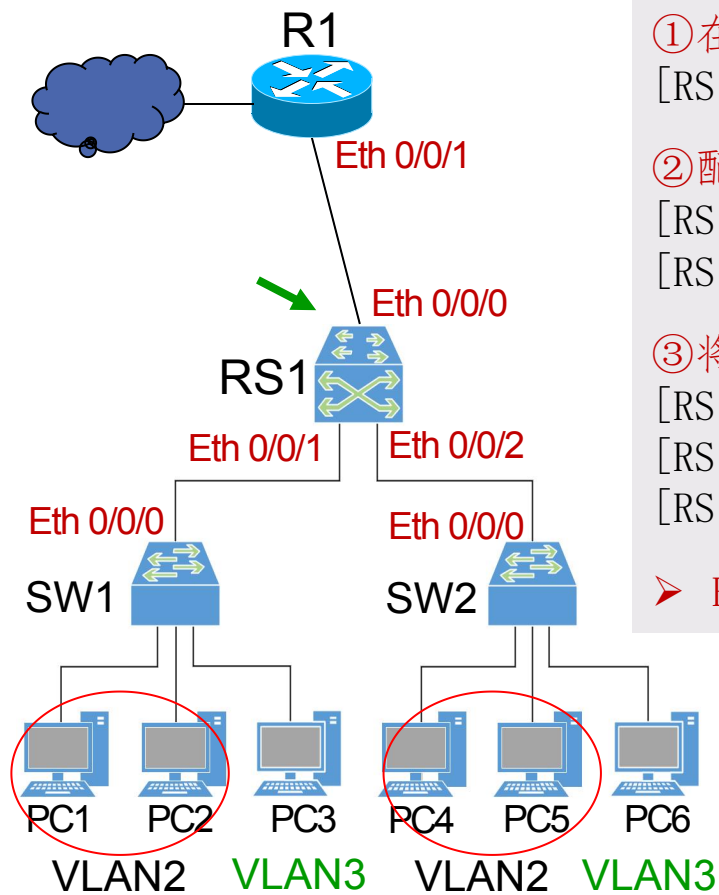
□ 三层交换机上的“三层虚拟接口”

■ 应用2：作为与其他路由设备互连的、下一跳的虚拟路由接口

► 配置三层交换机与其他路由设备相连的SVI接口时，分为三步：

1. 在路三层交换机上创建一个VLAN（例如VLAN100）；
2. 给该VLAN配置接口地址；
3. 将连接其他路由设备的物理接口（例如Eth0/0/0）配置成Access模式，并划入该VLAN中。
4. 完毕

案例2：配置三层交换机连接路由器R1的SVI接口



①在三层交换机上创建用于上连的VLAN，例如VLAN100
[RS1]vlan 100

②配置VLAN100的接口地址

[RS1]interface vlanif 100

[RS1-Vlanif100]ip address 10.0.1.1 255.255.255.252

③将上连R1的物理接口设置成Access类型，并划入VLAN100

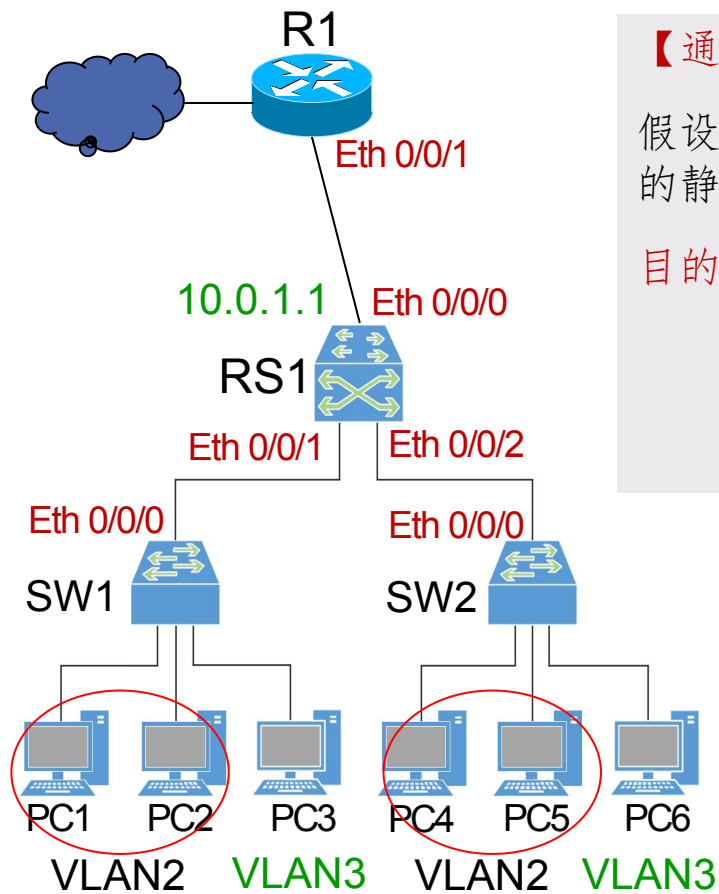
[RS1]interface Ethernet 0/0/0

[RS1-Ethernet0/0/0]port link-type access

[RS1-Ethernet0/0/0]port default vlan 100

➤ RS1与R1互联的三层虚拟接口（SVI）地址是10.0.1.1/30

案例2：配置三层交换机连接路由器R1的SVI接口



【通信描述】

假设在路由器R1的路由表中，有一条指向图中VLAN2所属网络的静态路由记录。则该路由记录中：

目的网络/掩码： 172.16.1.0/24

下一跳： 10.0.1.1（即RS1的上连SVI接口）

出接口： Eth0/0/1

三层交换机如何转发报文？

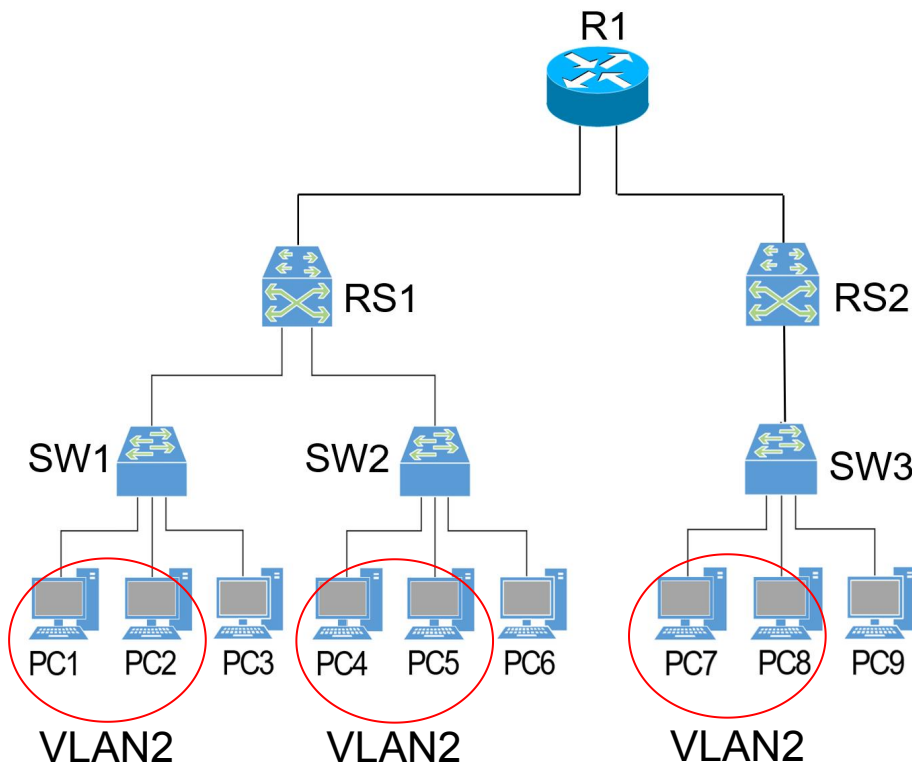
□ 此VLAN2，非彼VLAN2

■ VLAN2（PC1）和VLAN2（PC4）是同一个VLAN吗？

➤ 是，因为它们是同一个默认网关，配置在RS1上。

■ VLAN2（PC1）和VLAN2（PC7）是同一个VLAN吗？

➤ 不是，因为它们的默认网关不同！
VLAN2（PC1）的默认网关在RS1上，
VLAN2（PC7）的默认网关在RS2。

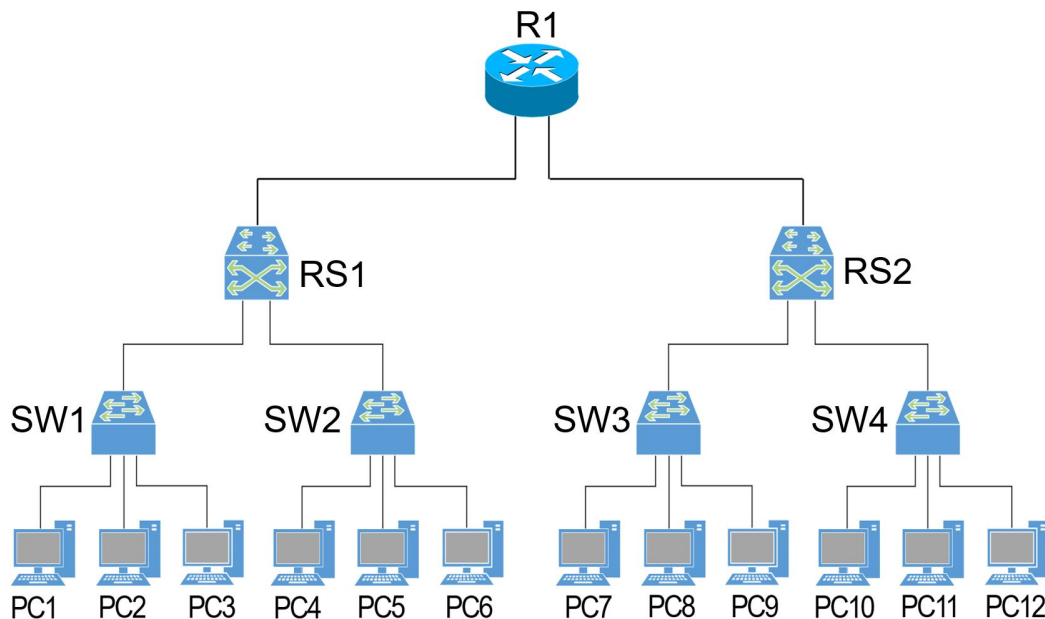


三层交换机如何转发报文？

□ 在三层交换机上配置静态/动态路由

- 配置方式与路由器相同

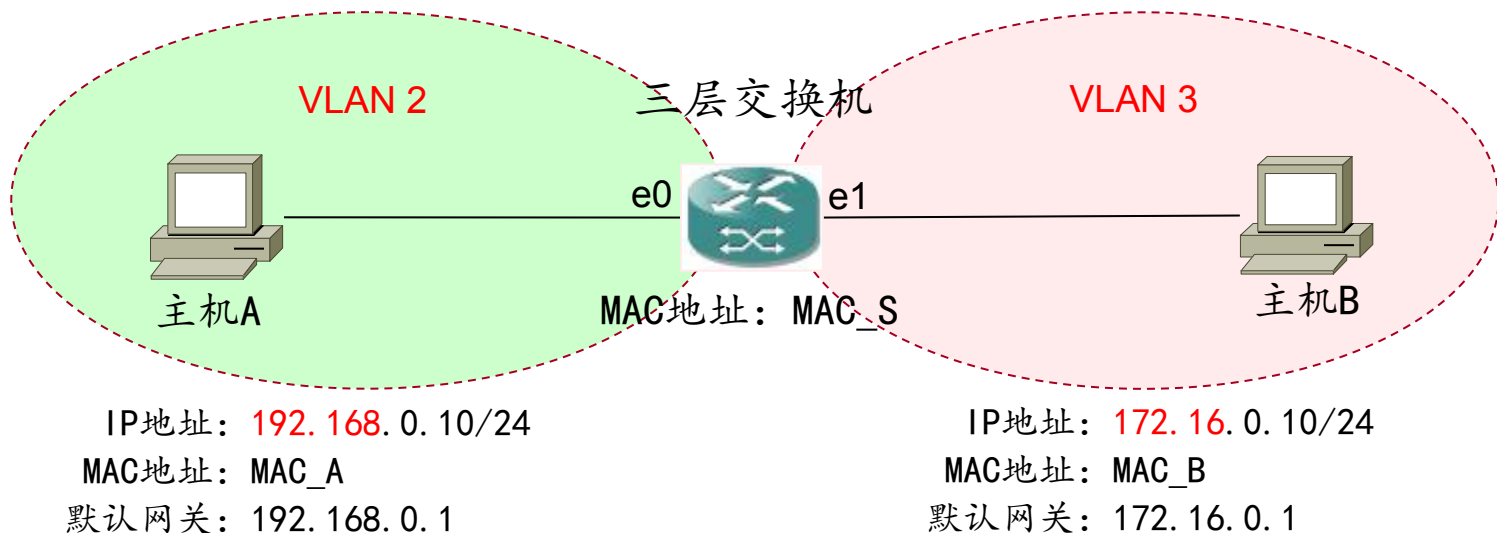
- 略



三层交换机如何转发报文？

□ 三层交换机的转发特点 —— 一次路由，多次交换

- 三层交换机在不同网络间转发报文时，与路由器最大的不同，在于其采用的是“一次路由，多次交换”的方式！

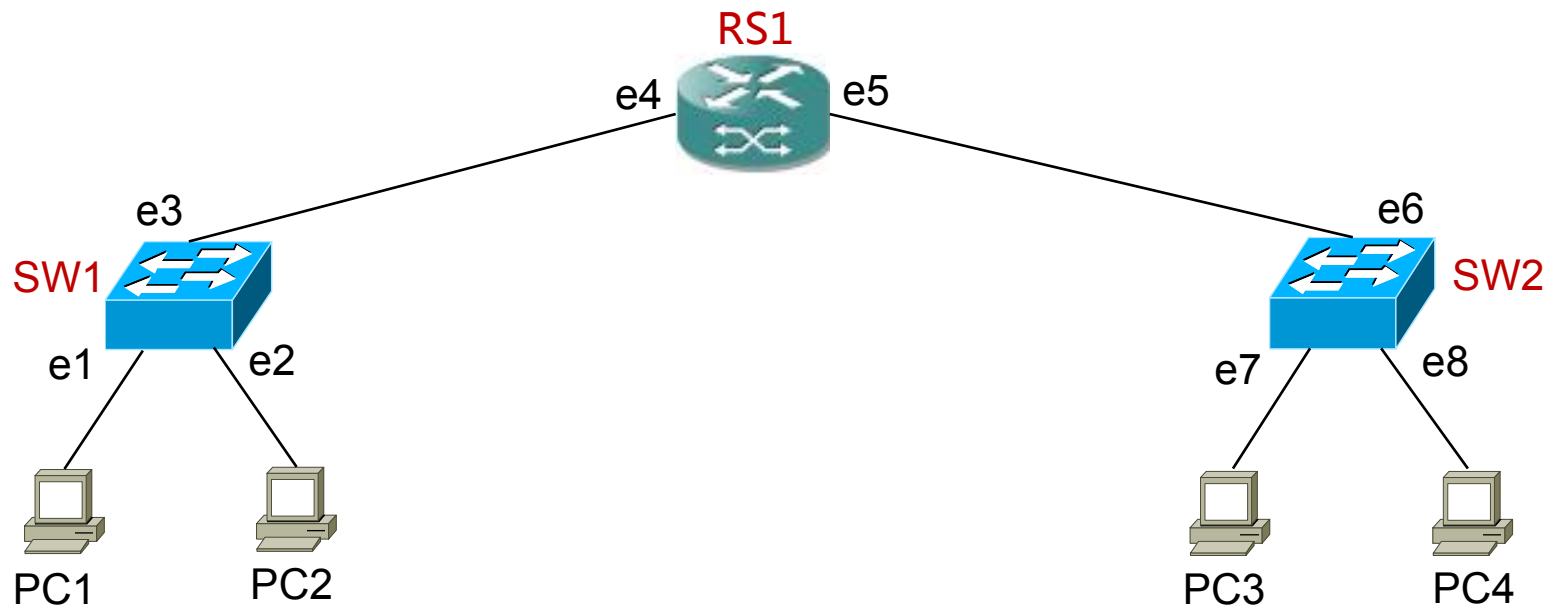


三层交换机如何转发报文？

□ “一次路由，多次交换”（结合上页图例）

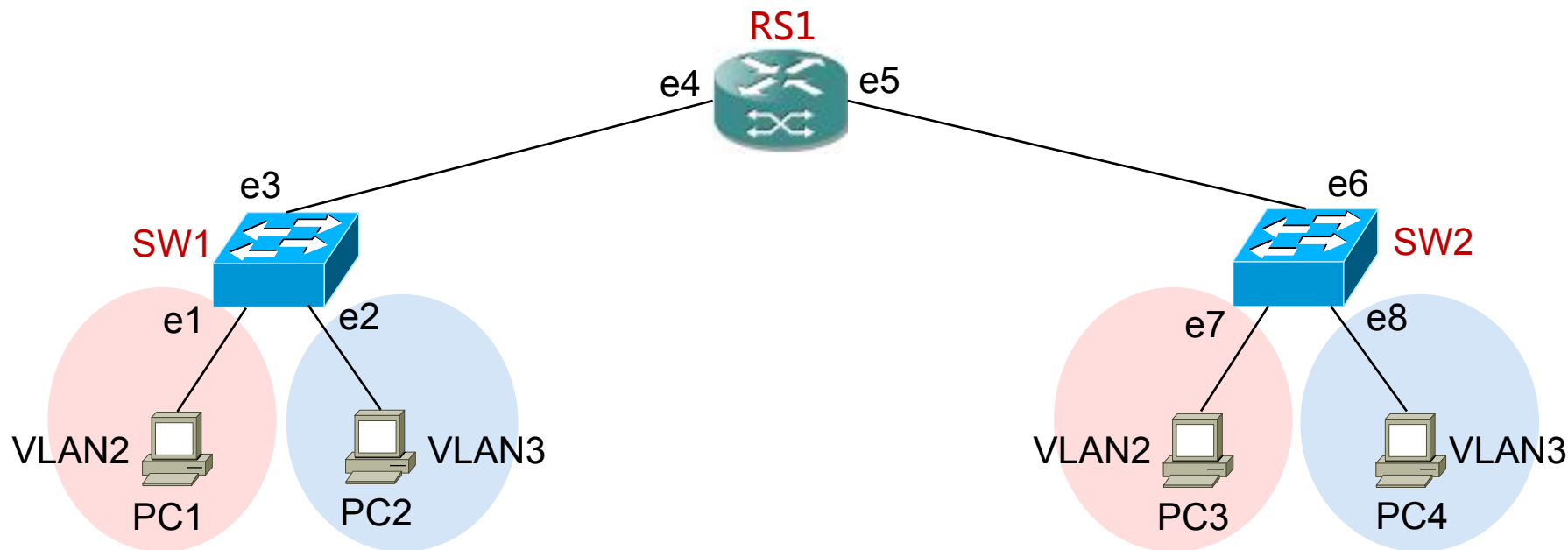
- **首次数据包**的路由处理：当三层交换机**首次**接收到某个数据流（例如主机A访问B）的数据包时，它会像路由器一样，通过查找自己的**IP路由表**，确定数据包的转发路径，并获取下一跳的**MAC地址**。然后，重新封装数据包，将源**MAC地址**改为三层交换机的**MAC地址（MAC_S）**，将目的**MAC地址**改为下一跳的**MAC地址**。转发出去。
- 构建**三层硬件转发表**：在转发第1个数据包的过程中，三层交换机会将主机A和主机B的信息（包括IP地址、MAC地址、接口号、VLAN ID）添加在自己的三层硬件转发表中；
- **后续数据包**的快速交换：从数据流的**第二个数据包**开始，三层交换机会利用之前建立的三层硬件转发表进行**快速转发**。由于直接在硬件中完成转发，不再查看IP路由表，这种方式大大提高了数据包的转发效率，降低了网络延迟。
- 这就是“一次路由，多次交换”的含义。

十、三层交换机通信实例分析



说明1：拓扑描述

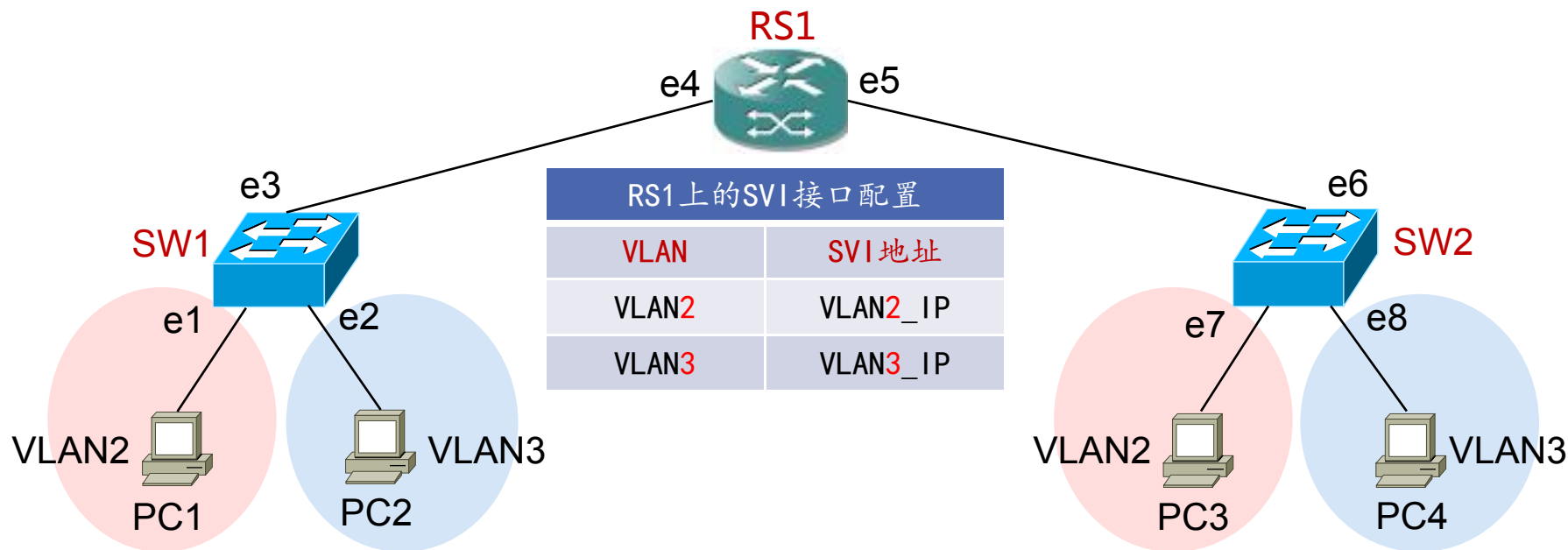
RS1是三层交换机，SW1和SW2是二层交换机，
PC1~PC4是用户主机；
e1~e8是各设备之间连接的接口。



说明2：二层交换机的配置

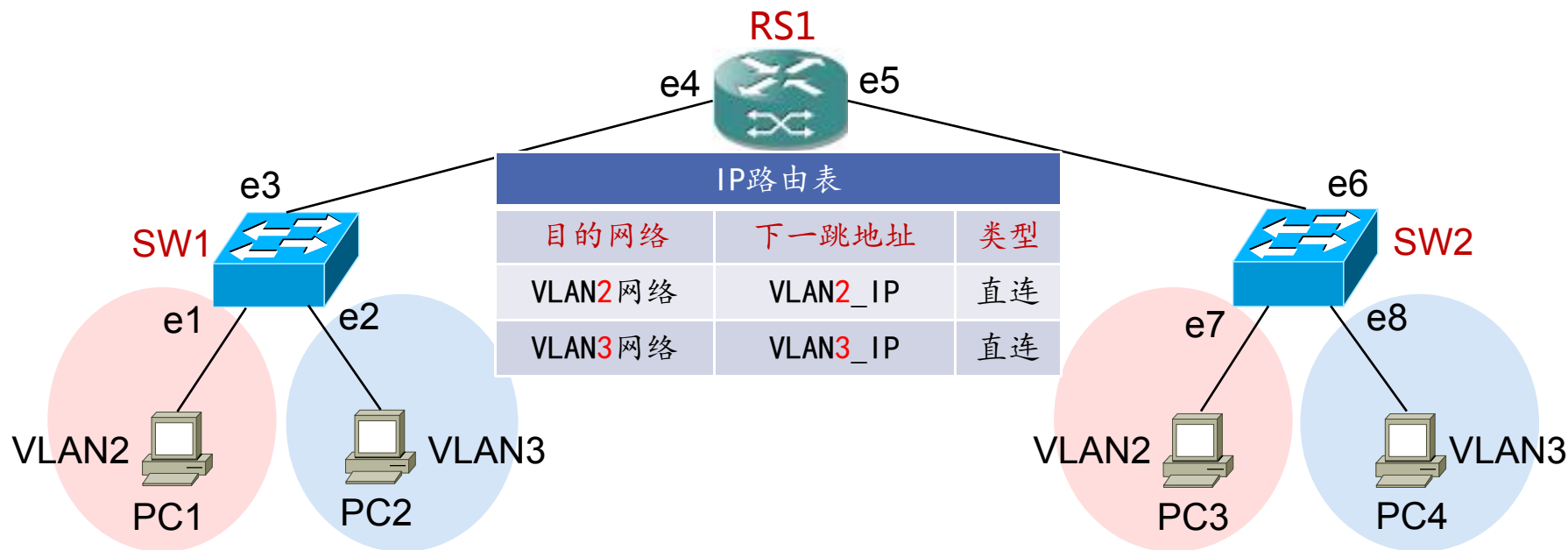
SW1和SW2上都创建了VLAN2和VLAN3；

e1和e7是Access接口，属于VLAN2。e2和e8是Access接口，属于VLAN3。



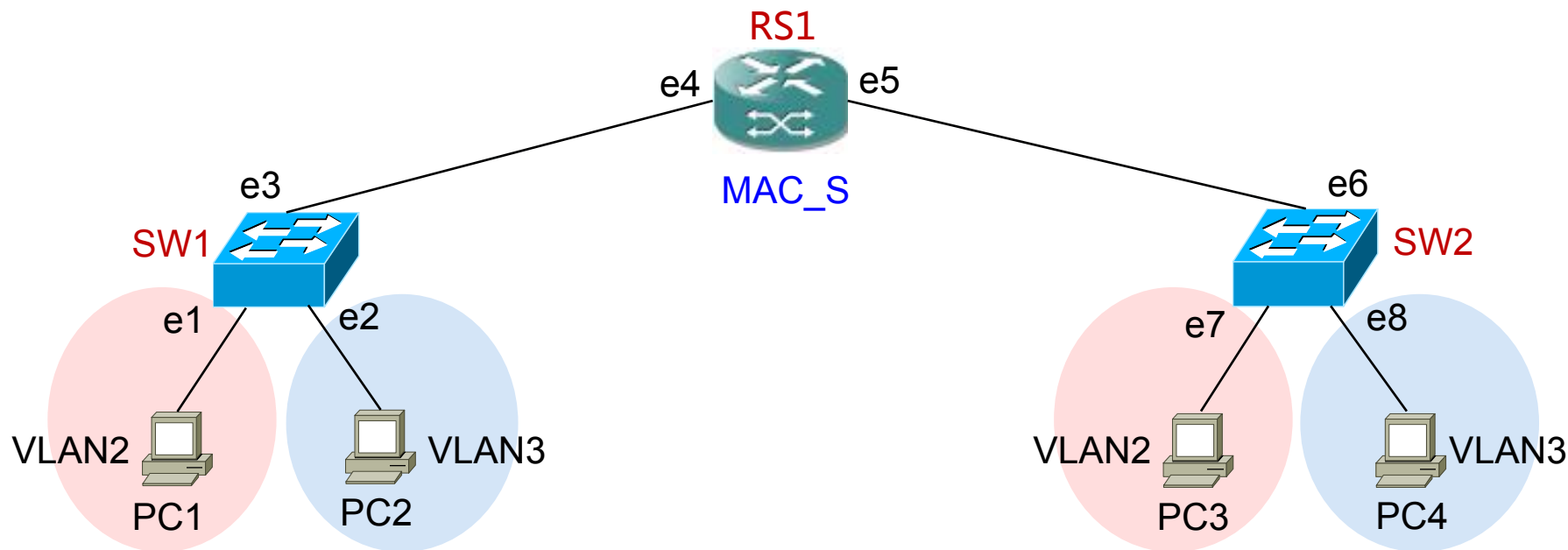
说明3：在三层交换机上配置SVI

在RS1中创建VLAN2和VLAN3，并配置了VLAN2和VLAN3的接口地址（即SVI地址），分别设为VLAN2_IP，VLAN3_IP；



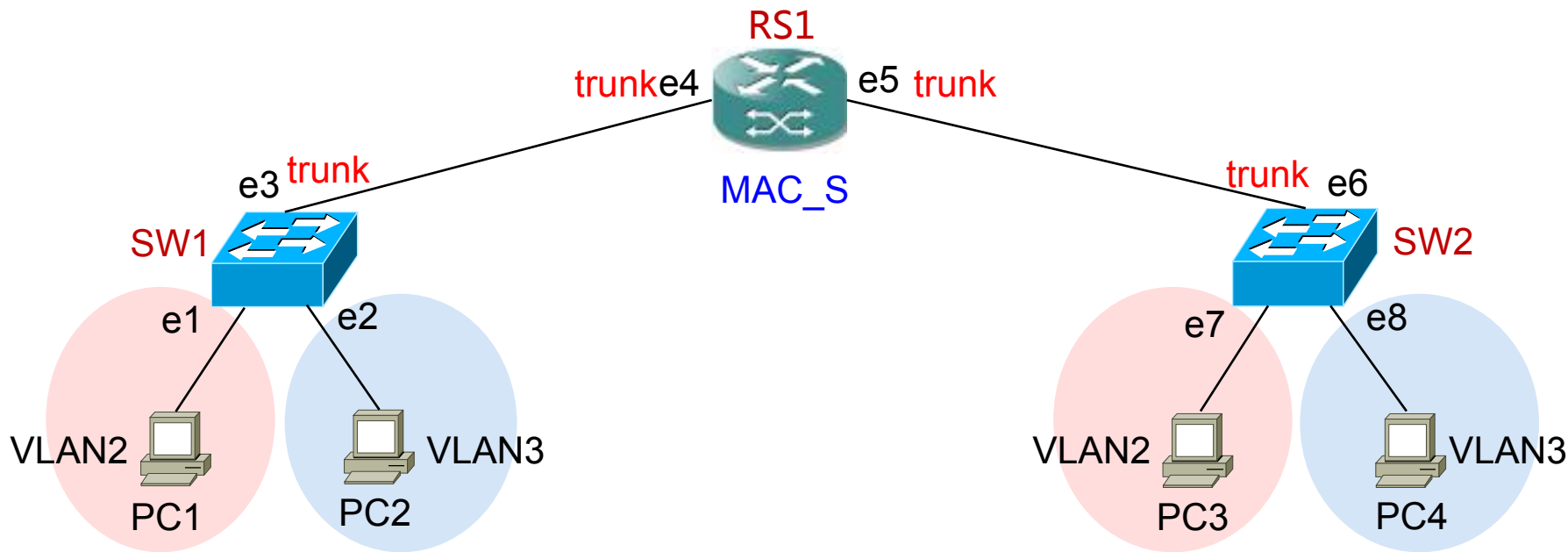
说明4：三层交换机上形成IP路由表

由于RS1中创建了VLAN2和VLAN3的SVI地址，所以RS1中的IP路由表（软件路由表）里有相应的直连路由；



说明5：三层交换机的MAC地址

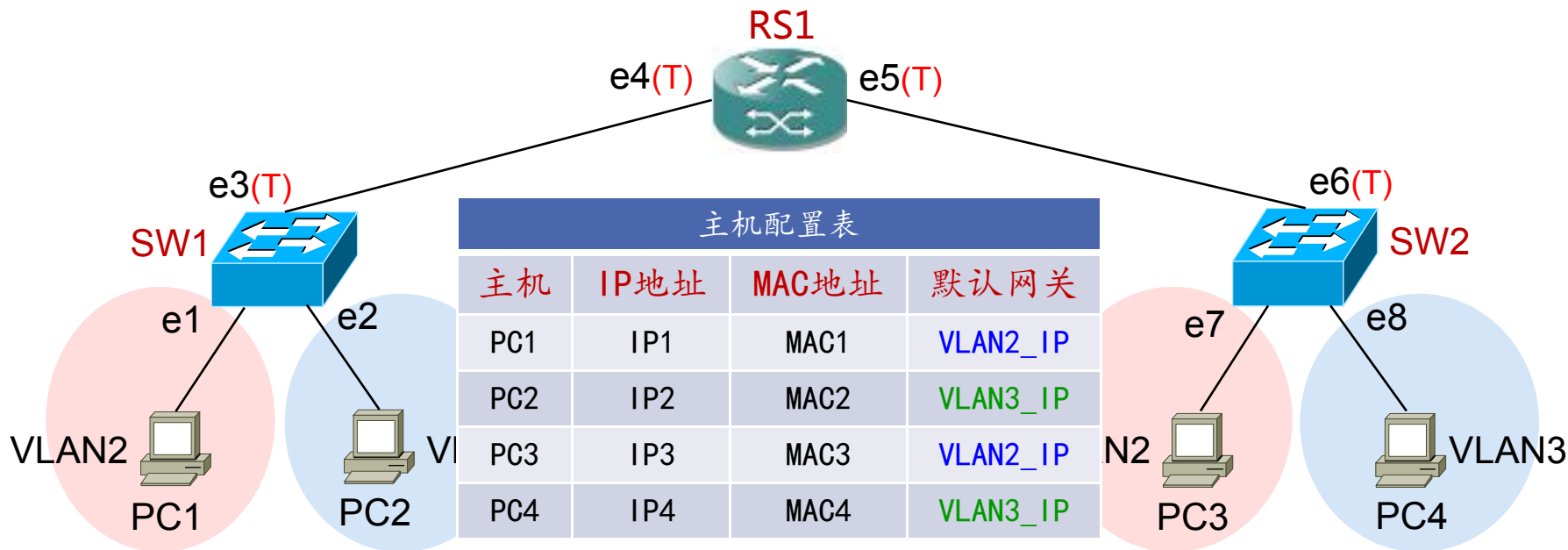
注意：三层交换机上各接口、各VLAN接口通常是共享一个MAC地址的，此处设为MAC_S。即VLAN2 SVI接口的MAC地址与VLAN3 SVI接口的MAC地址都是MAC_S。



说明6：交换机互连接口配置成Trunk类型

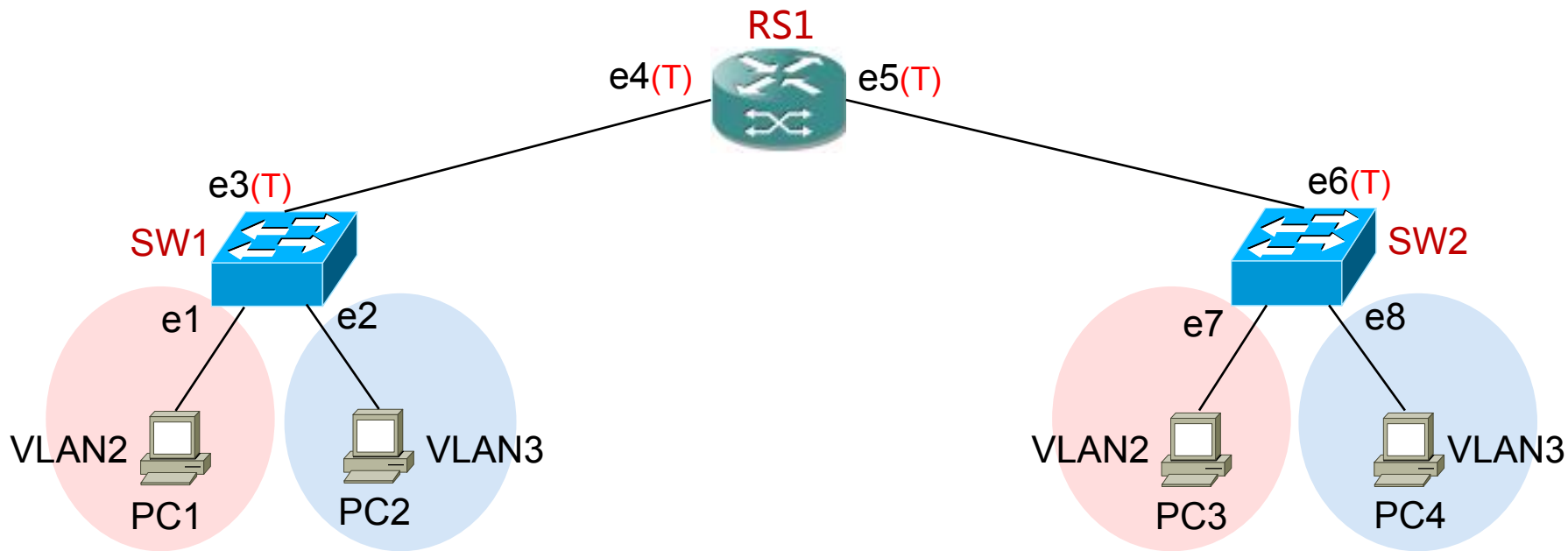
对于SW1与RS1之间的链路，由于其既要传输VLAN2的数据帧，也要传输VLAN3的数据帧，所以此处将其设置为Trunk链路，即e3接口和e4接口要设置为Trunk类型（PVID=1），并允许VLAN2和VLAN3的数据帧通过；SW2和RS1之间的链路同理。

三层交换机通信实例分析——网络基本说明（7）



说明7：用户主机配置IP地址

见“主机配置表”，注意，VLAN2和VLAN3使用的是不同网段，例如，VLAN2使用的IP地址段为192.168.0.0/24，VLAN3使用的IP地址段为172.16.0.0/24。

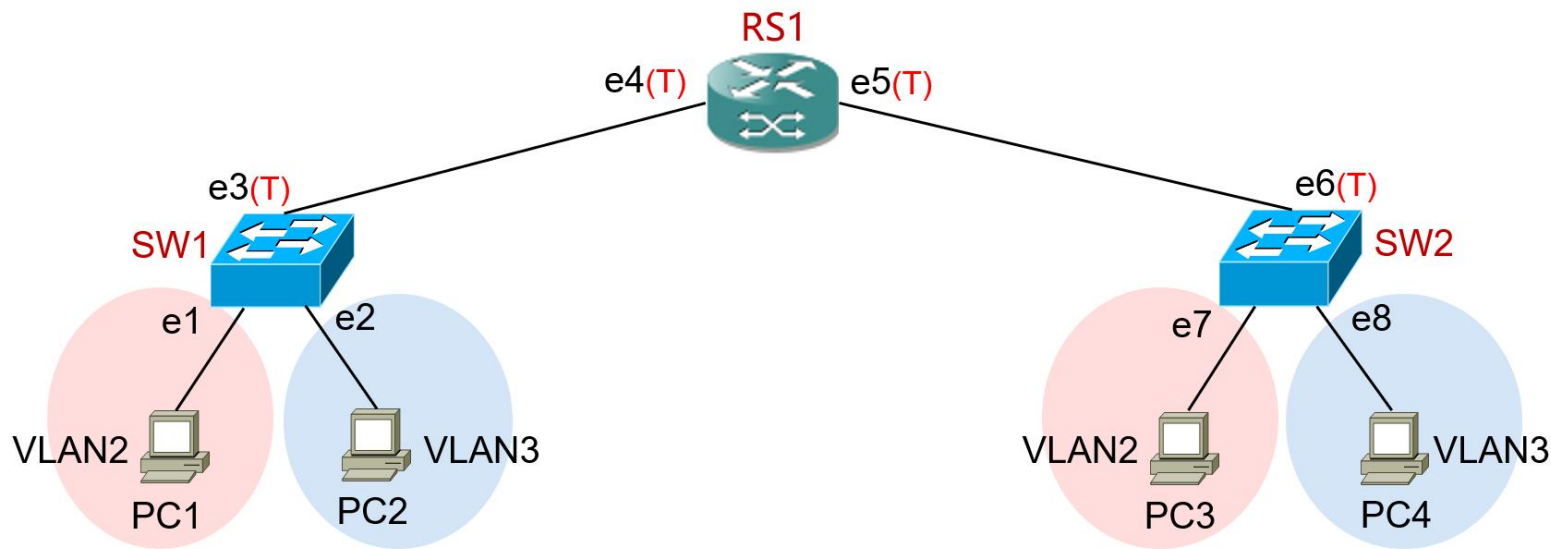


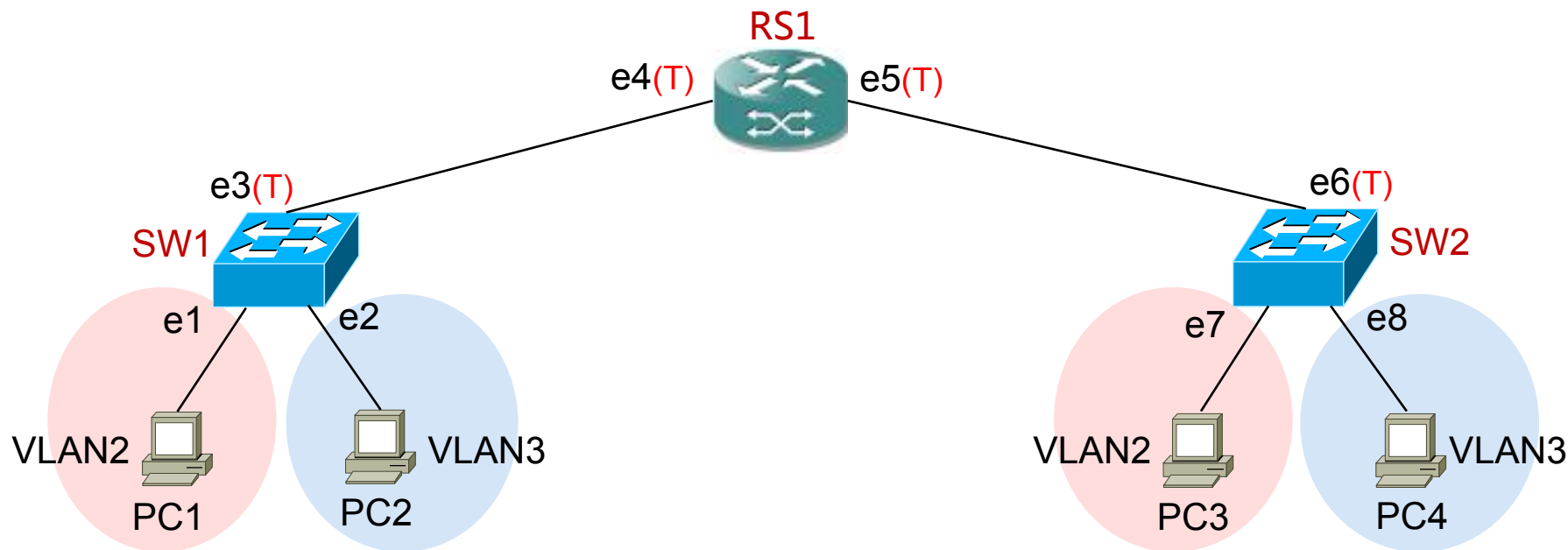
说明8: 本案例中, 需要通过三层交换机实现:

- 不同交换机中，不同VLAN内主机通信，例如PC1访问PC4
- 同交换机中，不同VLAN主机之间通信，例如PC1访问PC2；
- 不同交换机中，同一VLAN内部主机通信，例如PC1访问PC3（都属于VLAN2）；

分析1：跨交换机，不同VLAN主机之间的通信

PC1 ping PC4（完整通信过程）

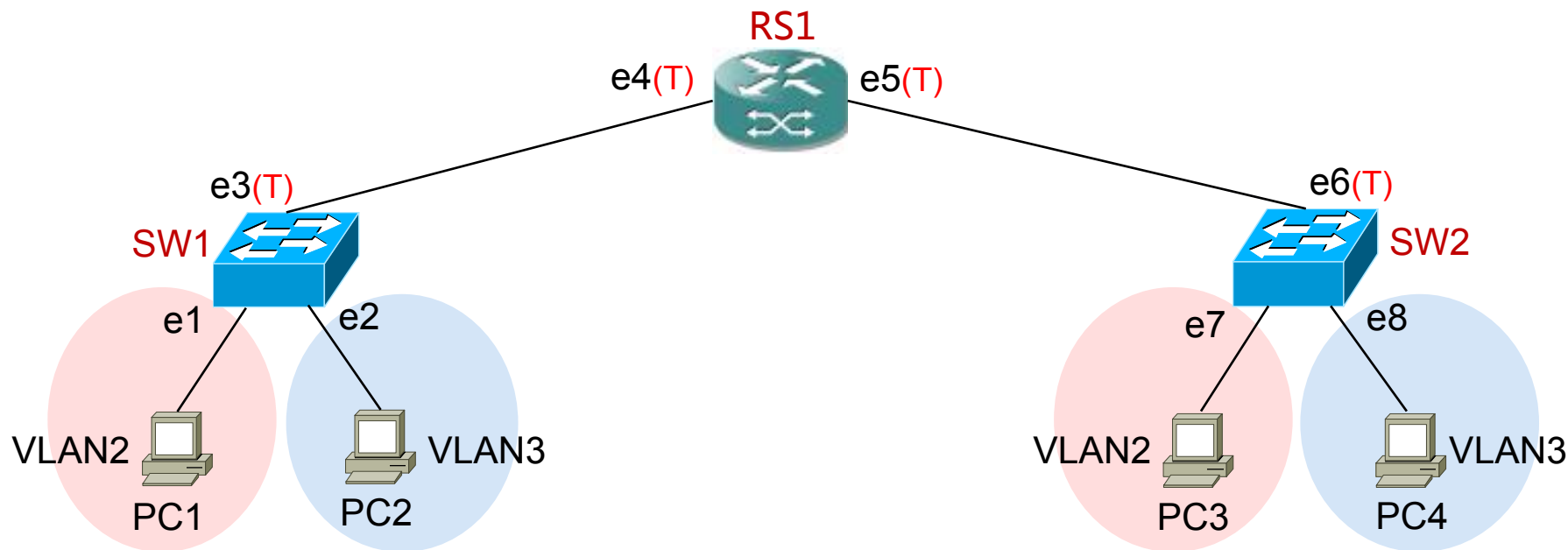




特别说明

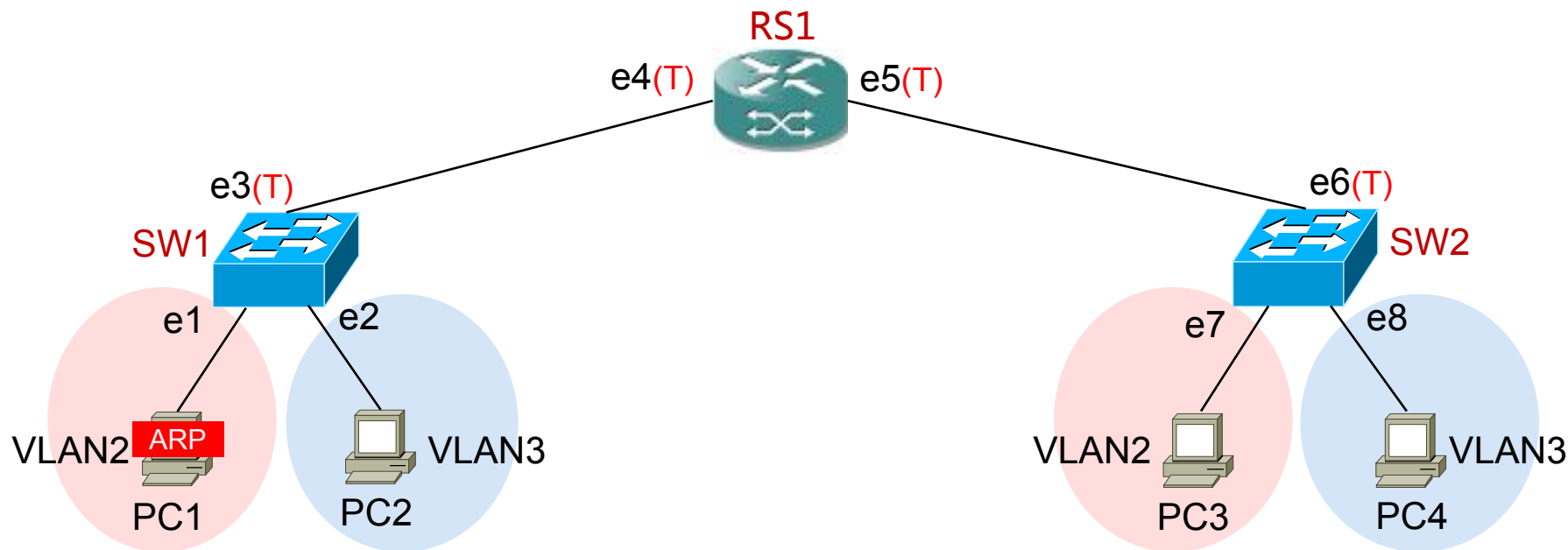
PC1是首次访问PC4！

首先分析“首报文”从PC1到达PC4的情况



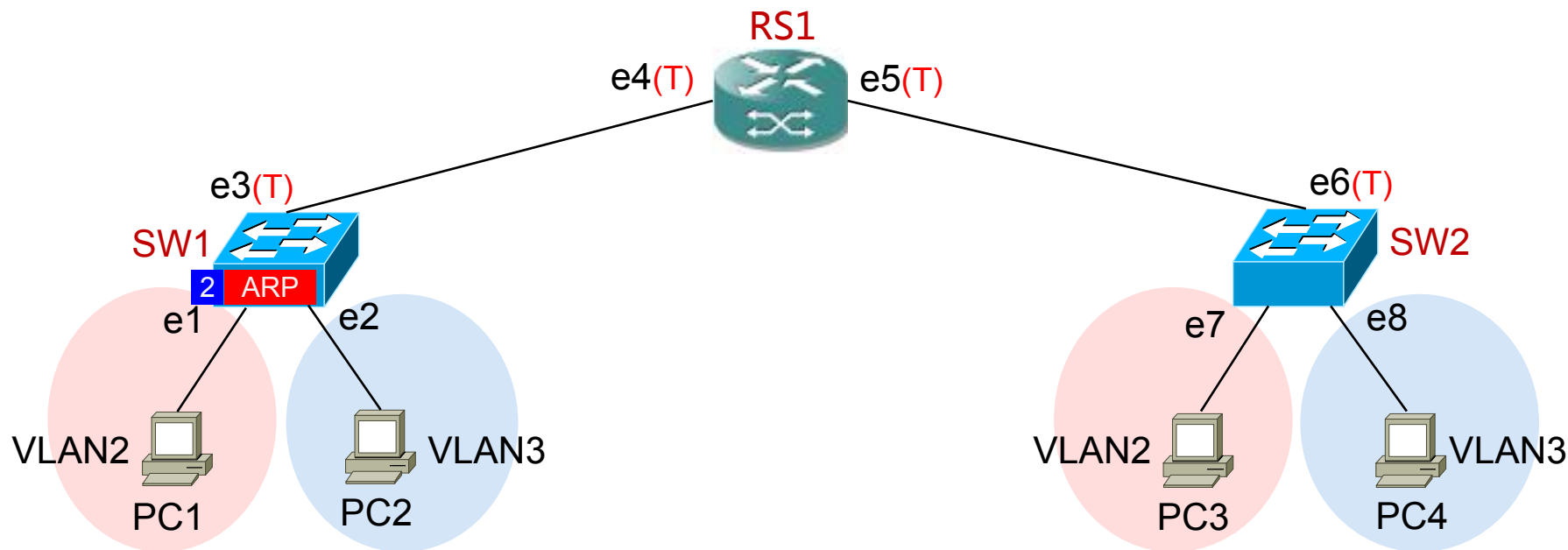
步骤1：PC1获取默认网关的MAC地址（1）—— 基本说明

PC1发现目的IP（即IP4）与自己不在同一网段，于是要先把自己的数据包发给自己的默认网关（即三层交换机上VLAN2的SVI接口）。假设，PC1此时不知道默认网关的MAC地址，必须先通过ARP协议获取到默认网关的MAC地址（即RS1的MAC地址MAC_S）。



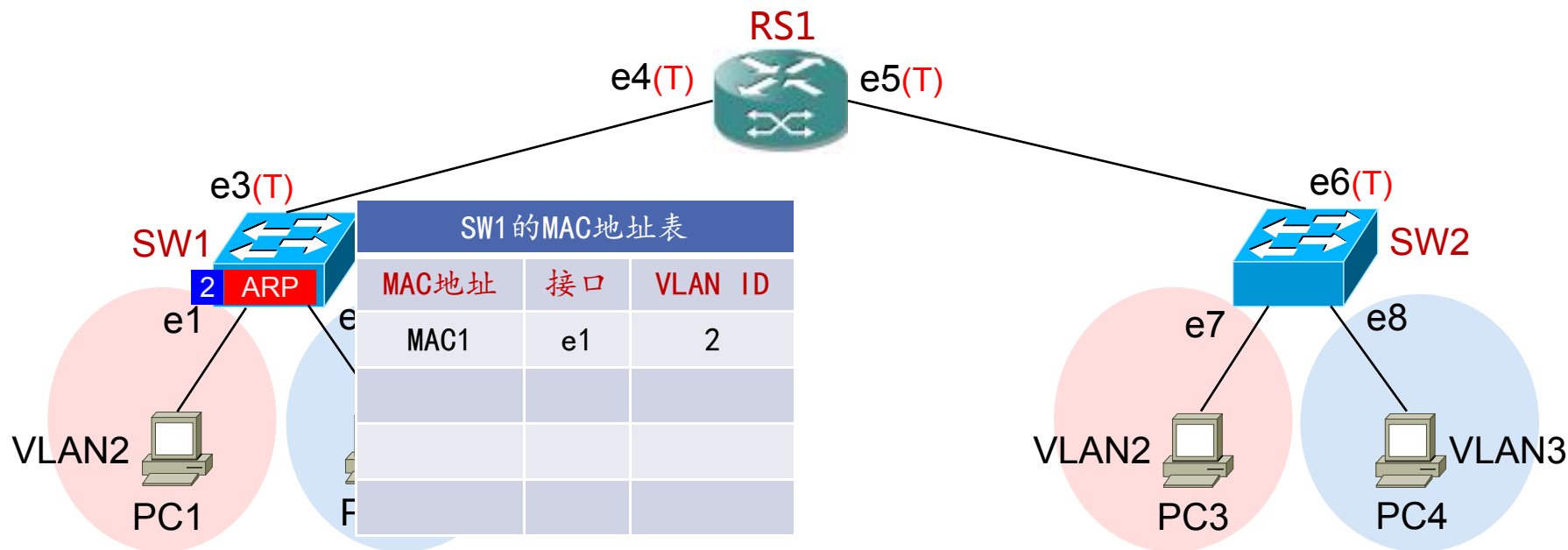
步骤1: PC1获取默认网关的MAC地址 (2) —— PC1发出ARP请求报文

于是, PC1发出ARP请求报文 (广播报文), 在封装报文时, 源MAC是MAC1, 目的MAC是ff-ff-ff-ff-ff-ff。

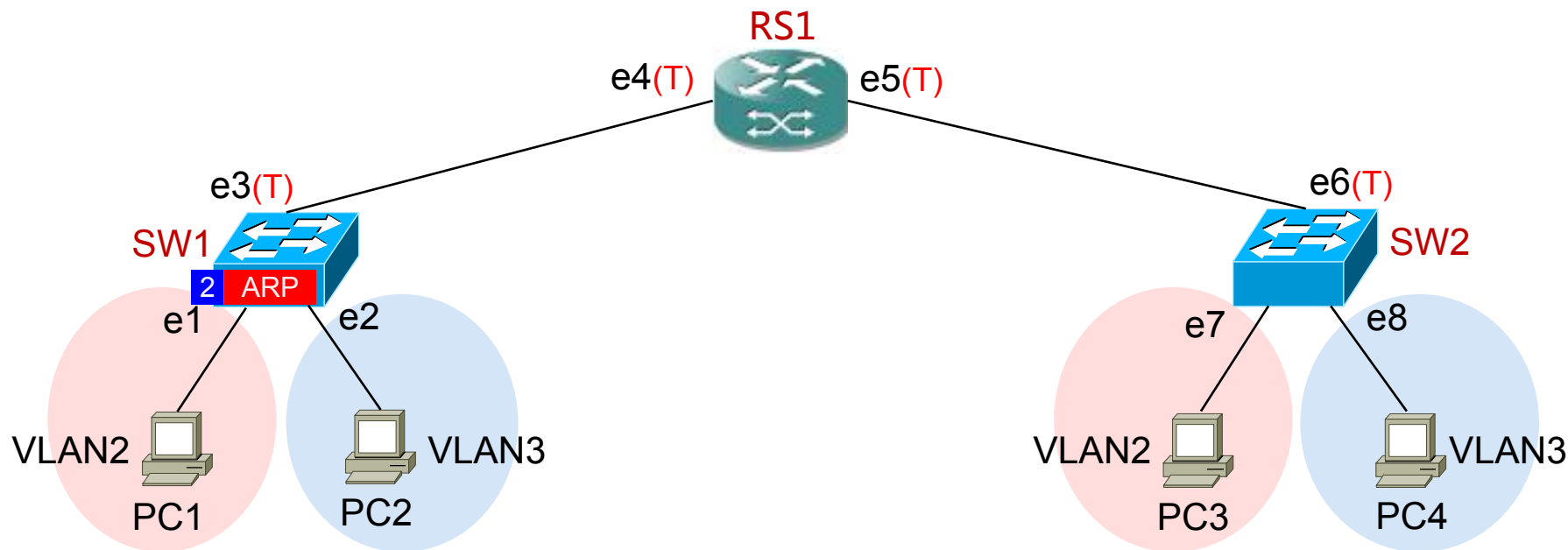


步骤1：PC1获取默认网关的MAC地址（3）——SW1的处理1：添加VLAN标签

交换机SW1的e1接口（access接口）收到ARP报文，添加VLAN标签，由于e1属于VLAN2，所以此处帧头中添加VLAN2的标签。

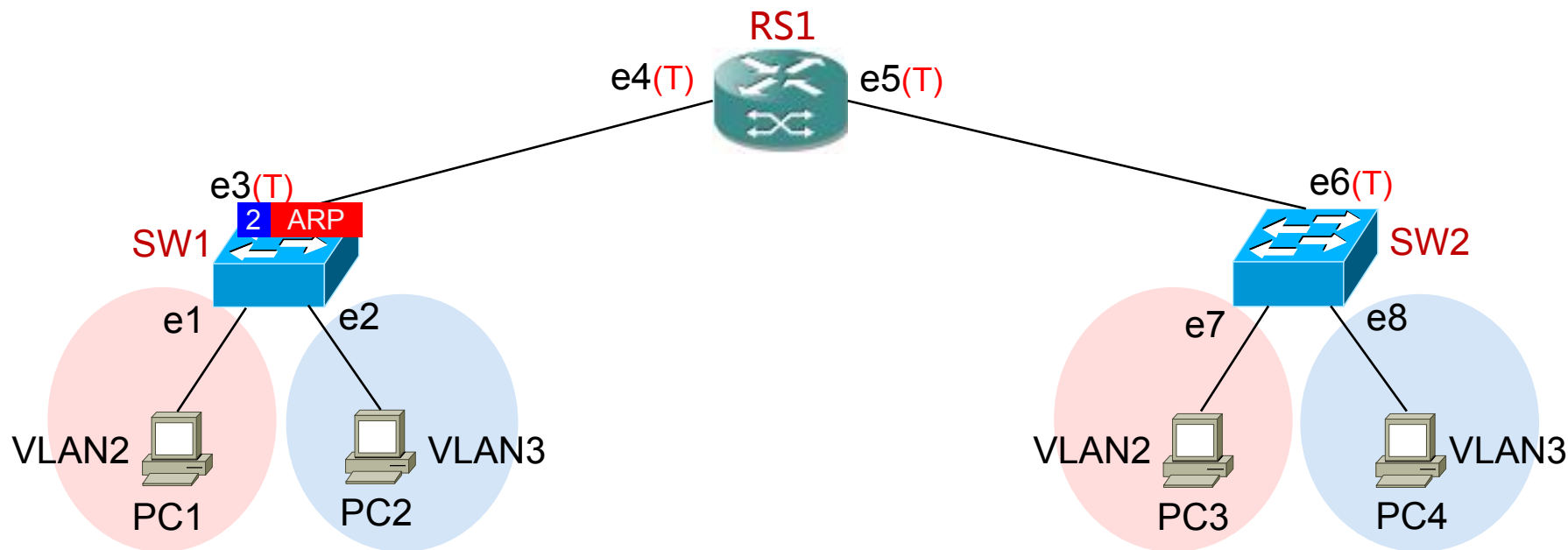


步骤1: PC1获取默认网关的MAC地址 (4) ——SW1的处理2: 添加MAC地址表记录
SW1根据ARP报文的源MAC地址, 在自己的MAC地址表中添加主机PC1的相关记录。

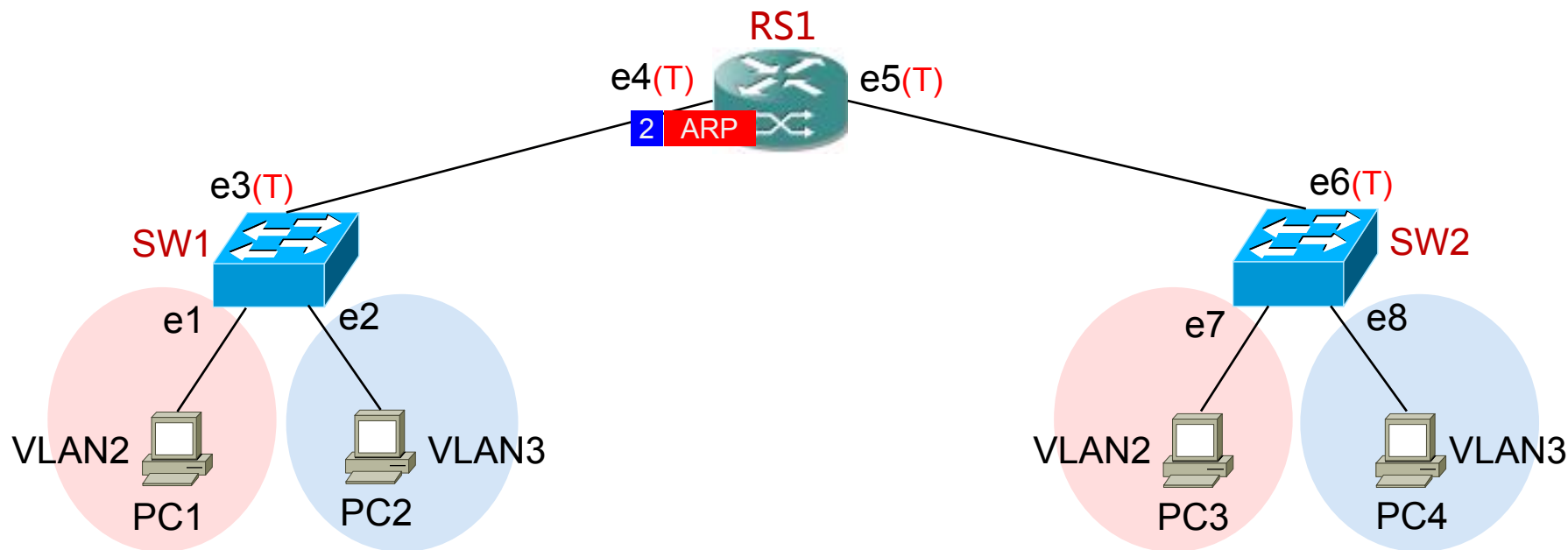


步骤1: PC1获取默认网关的MAC地址 (5) ——SW1的处理3: 转发数据帧到e3接口

由于ARP报文的目的MAC是广播地址，所以SW1会把该报文转发到SW1上所以属于VLAN2的接口，由于e3接口是trunk类型，所以该ARP报文也会转发到e3接口（在交换机内部）；



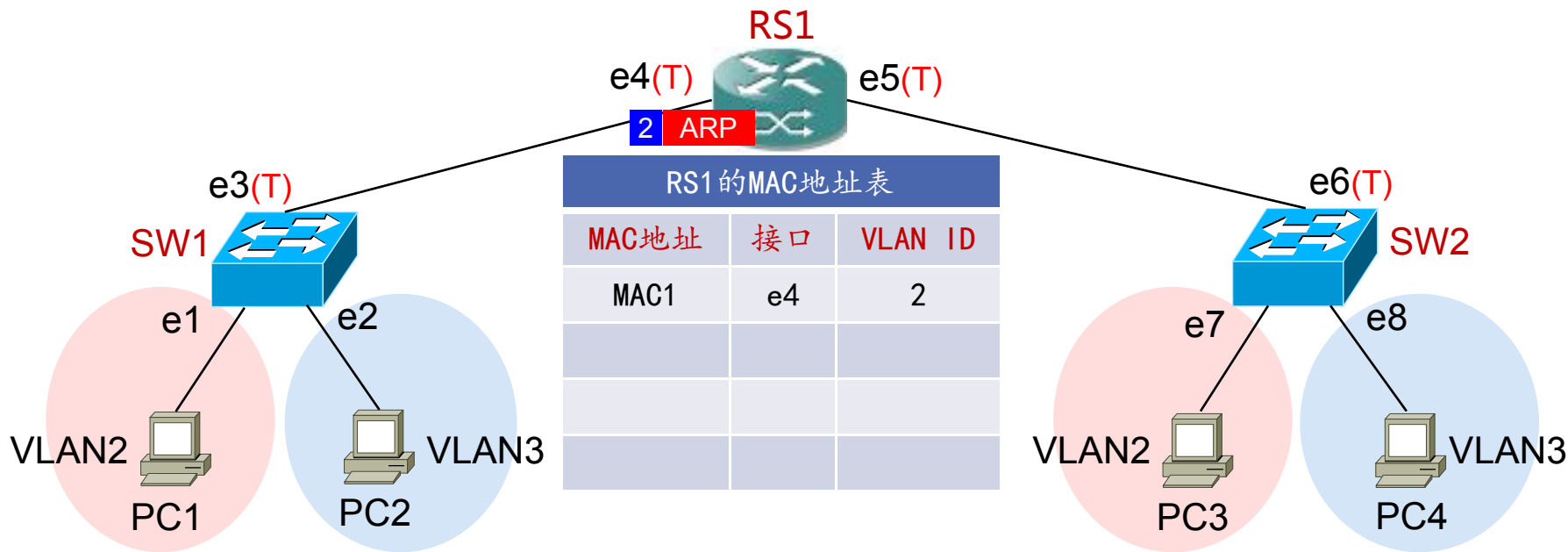
步骤1: PC1获取默认网关的MAC地址 (6) ——SW1的处理4: 从e3接口发出
由于e3接口是trunk类型, 且接口的PVID≠报文的VID, 所以, 该报文会携带VLAN2的标签, 从e3接口发出, 到达RS1的e4接口。



步骤1：PC1获取默认网关的MAC地址（7）——RS1的处理1：接收tagged帧

由于e4接口是trunk类型，所以会保留VLAN2的标签并接收该报文。进一步分析报文内容，发现报文中被请求的IP地址是自己的三层接口（即VLAN2的SVI接口）IP地址，RS1收下该报文，并进行下一步处理。

三层交换机通信实例分析——PC1 ping PC4 (8)

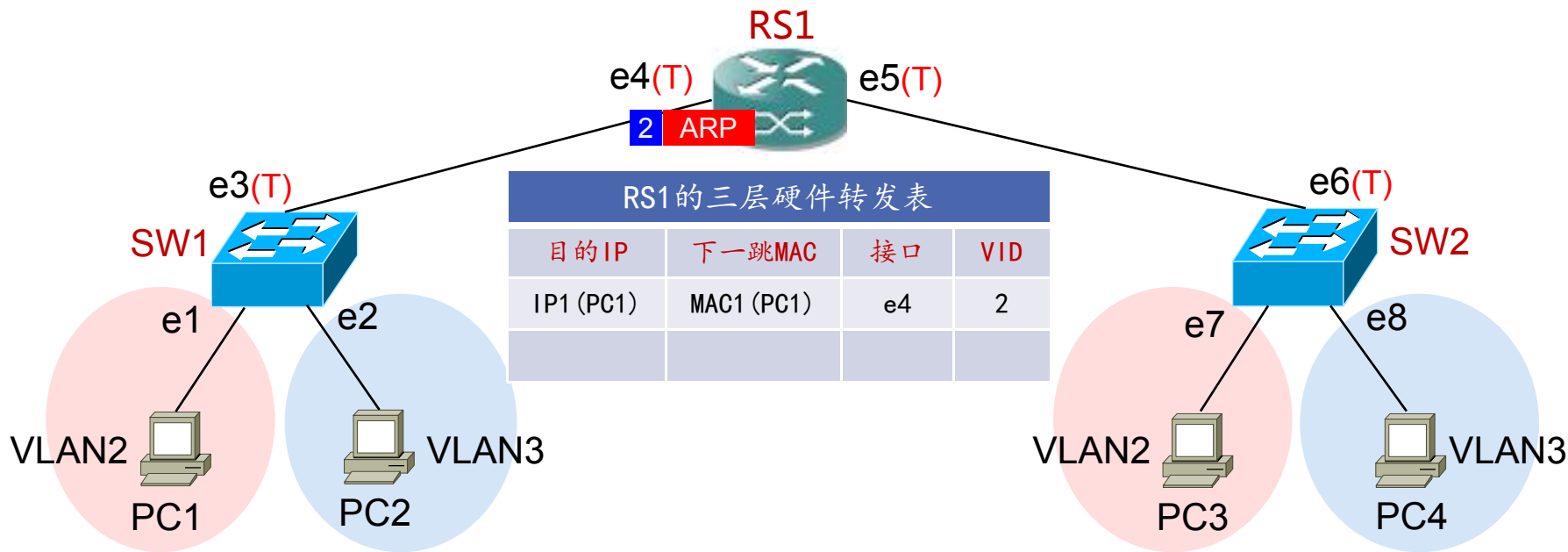


步骤1: PC1获取默认网关的MAC地址 (8) ——RS1的处理2: 在MAC地址表中添加记录

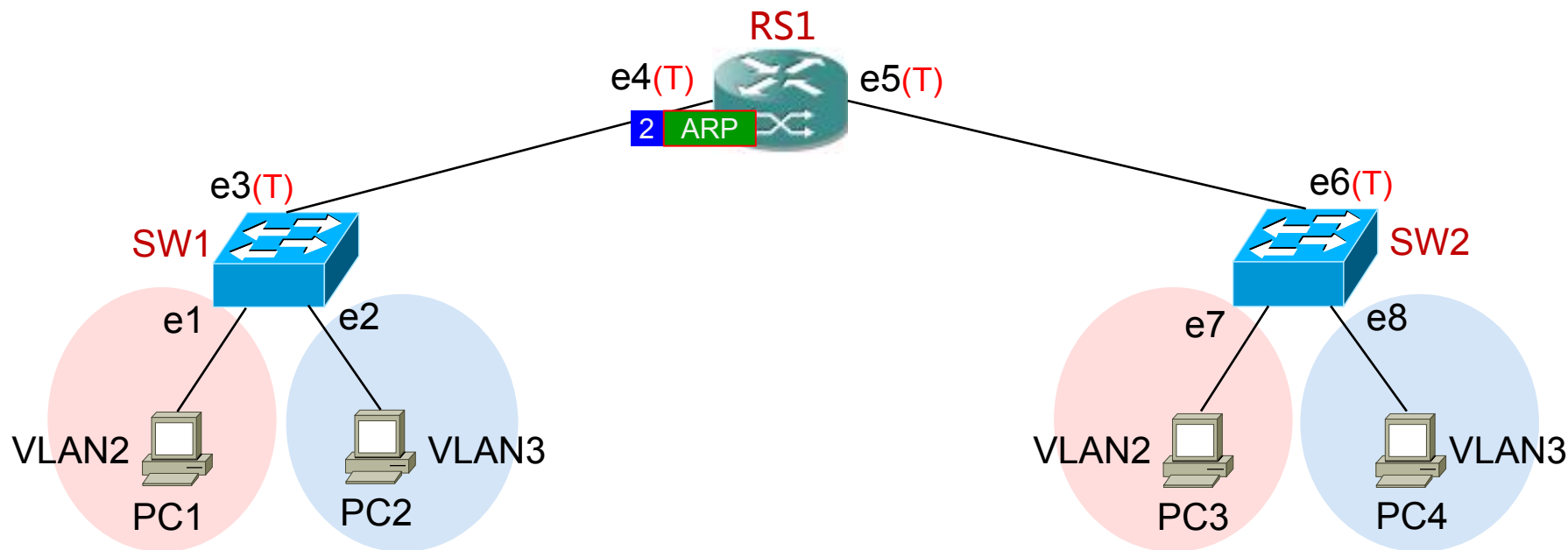
RS1根据所收到报文的来源信息, 在自己的MAC地址表中, 添加PC1相关记录。

注: RS1也会在自己的ARP表中添加PC1的IP地址和MAC地址的信息。

三层交换机通信实例分析—— PC1 ping PC4 (9)



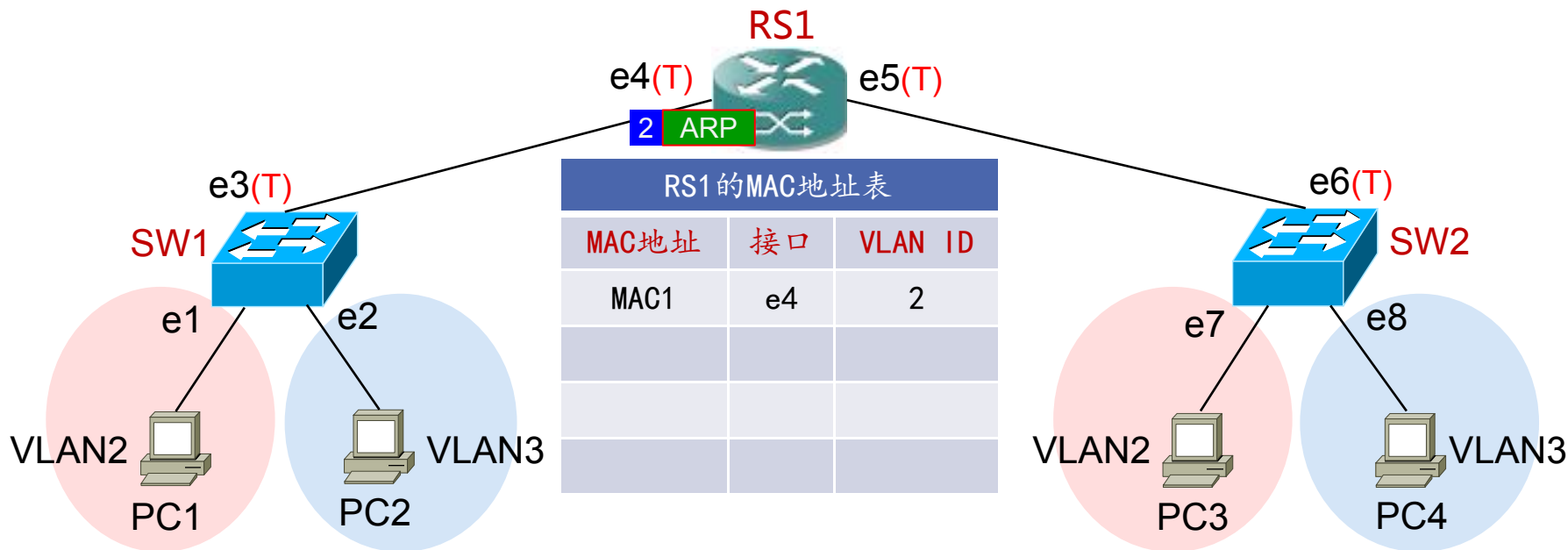
步骤1：PC1获取默认网关的MAC地址 (9) ——RS1的处理3：在三层硬件转发表中添加记录
RS1分析ARP请求报文，然后将PC1（即来源）的信息添加在交换机ASIC芯片的三层硬件转发表中，包含：目的IP地址（即IP1地址）、下一跳MAC地址（即MAC1）、接口号（即e4）、VLAN ID（即2）。以后，其他网段的主机想访问PC1时，RS1的ASIC芯片就会直接把包从本表指定的接口（即e4）转发出去（即硬件转发），而不必再交给CPU进行路由处理，即不必要再查看IP路由表（软件路由）。



步骤1：PC1获取默认网关的MAC地址（10）——RS1的处理4：构建ARP响应报文

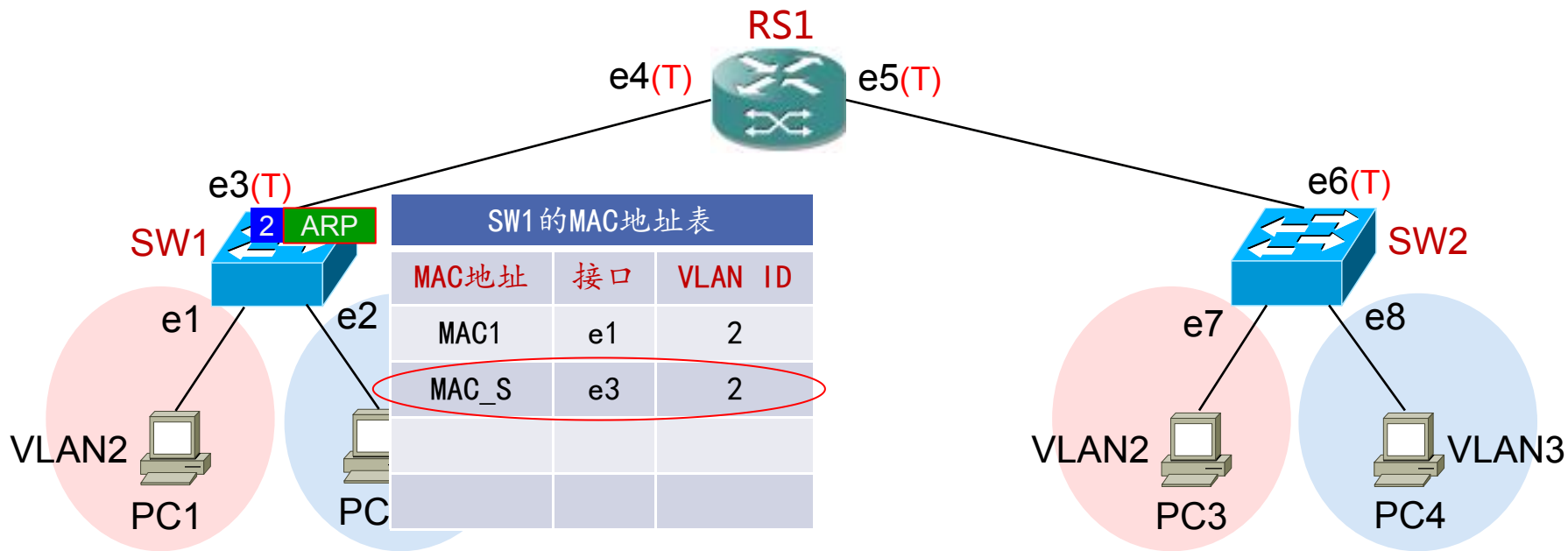
RS1收到ARP请求报文后，发现报文中请求的是自己的三层接口VLANif2（即VLAN2的SVI接口）的MAC地址，于是发回ARP响应报文。该报文的目的是MAC1，源MAC是MAC_S。

三层交换机通信实例分析—— PC1 ping PC4 (11)



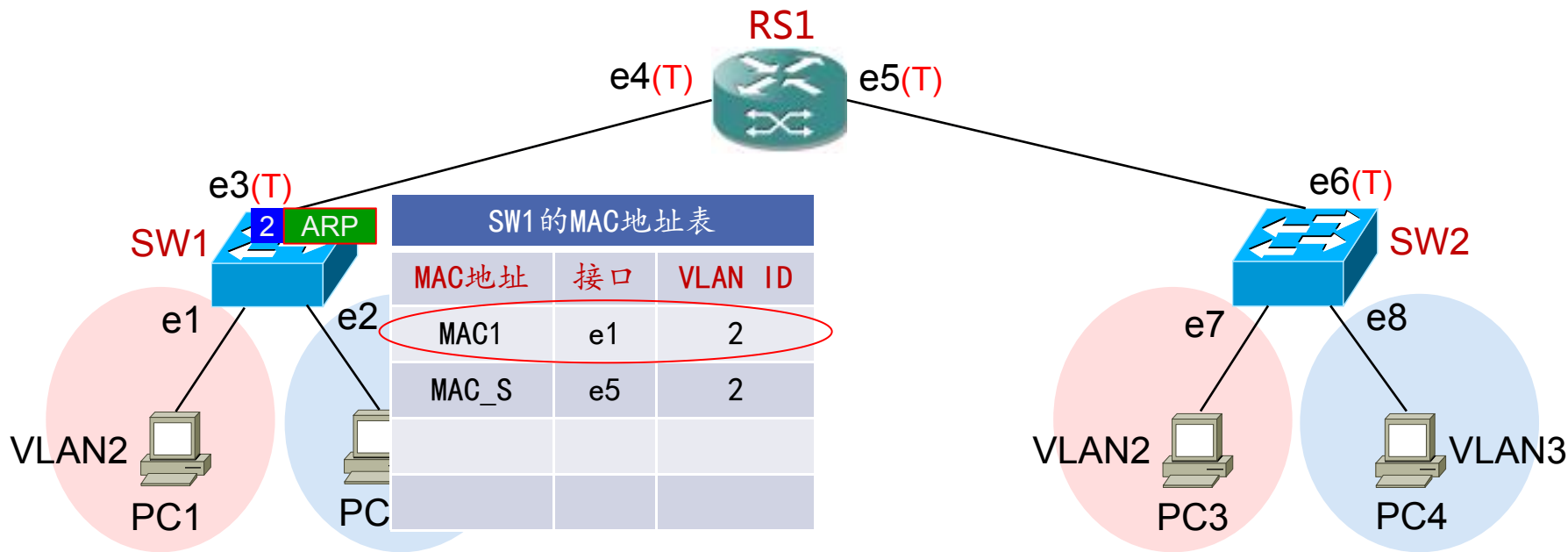
步骤1：PC1获取默认网关的MAC地址（11）——RS1的处理5：VLANif2发回ARP响应报文
此处可理解为：RS1上的虚拟接口VLANif2发出ARP响应报文，该接口发出的报文中直接带有VLAN2的标签。经过查看RS1的MAC地址表，发现目的MAC地址对应的是e4接口，并且对应VLAN2，于是从e4接口发出去。
由于e4是Trunk口，且PVID=1，所以不去掉VLAN2的标签。

三层交换机通信实例分析—— PC1 ping PC4 (12)



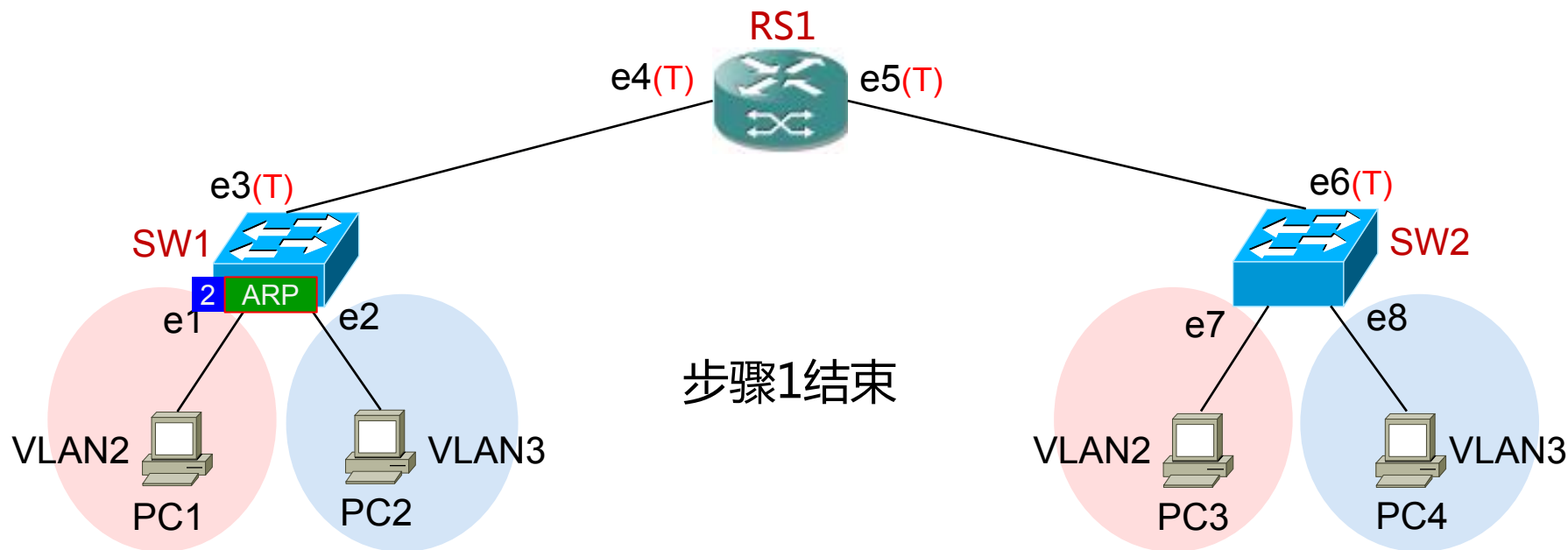
步骤1: PC1获取默认网关的MAC地址 (12) ——SW1的处理1: 接收, 在MAC地址表中添加记录
SW1的e3接口收到ARP响应报文, 由于e3是trunk口, 所以接收时不去掉帧头中的VLAN2标签。
SW1在自己的MAC地址表中添加默认网关的MAC地址 (即RS1的MAC地址) 与接收接口 (e3) 的对应关系。

三层交换机通信实例分析—— PC1 ping PC4 (13)



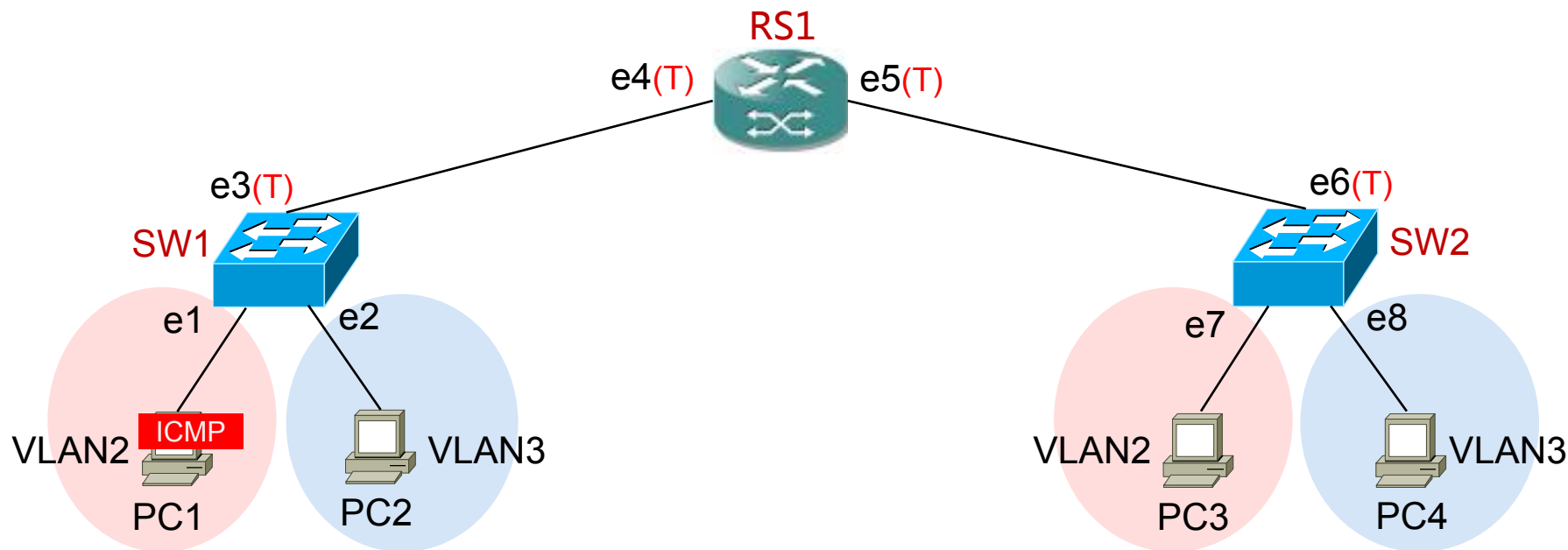
步骤1: PC1获取默认网关的MAC地址 (13) ——SW1的处理2: 转发至e1接口

SW1查看自己的MAC地址表, 发现目的MAC地址对应的是e1接口, VLAN ID也能对应上, 于是转发至e1接口。



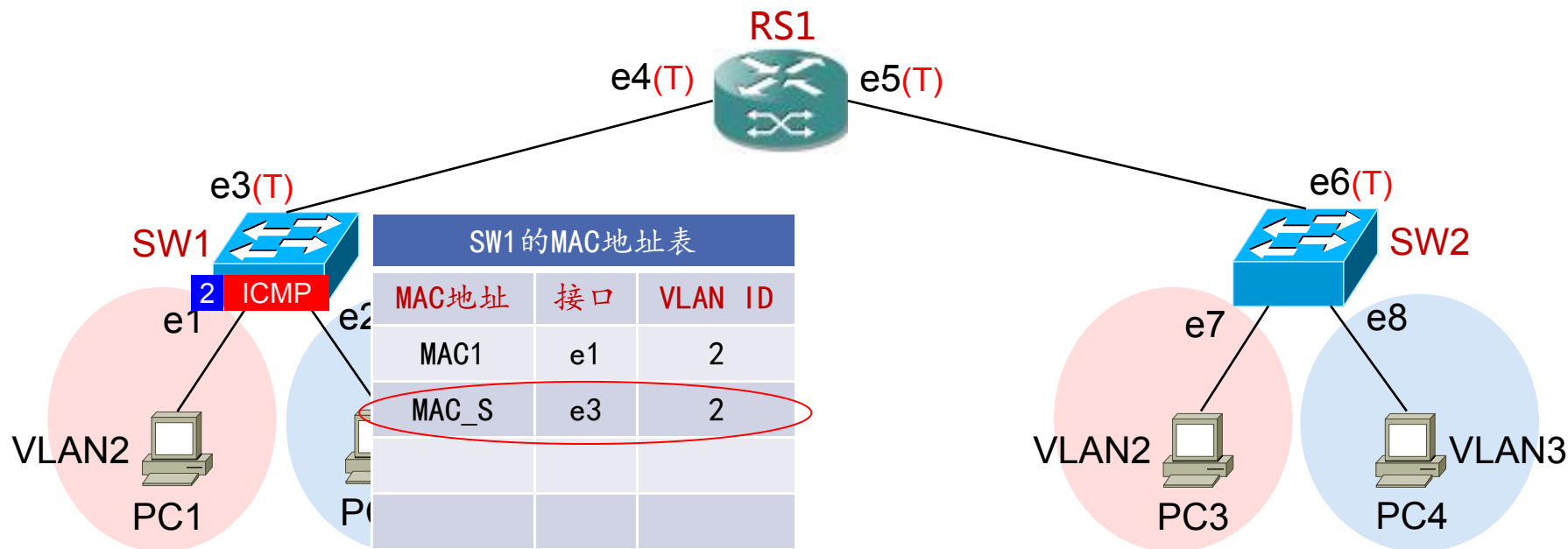
步骤1：PC1获取默认网关的MAC地址（14）——SW1的处理3：从e1接口发出去
由于e1是access接口，所以去掉帧头中的VLAN2标签，然后将普通帧（ARP响应报文）发送至目的主机PC1。

至此，PC1获得了默认网关（即RS1上VLAN2的SVI接口）的MAC地址。

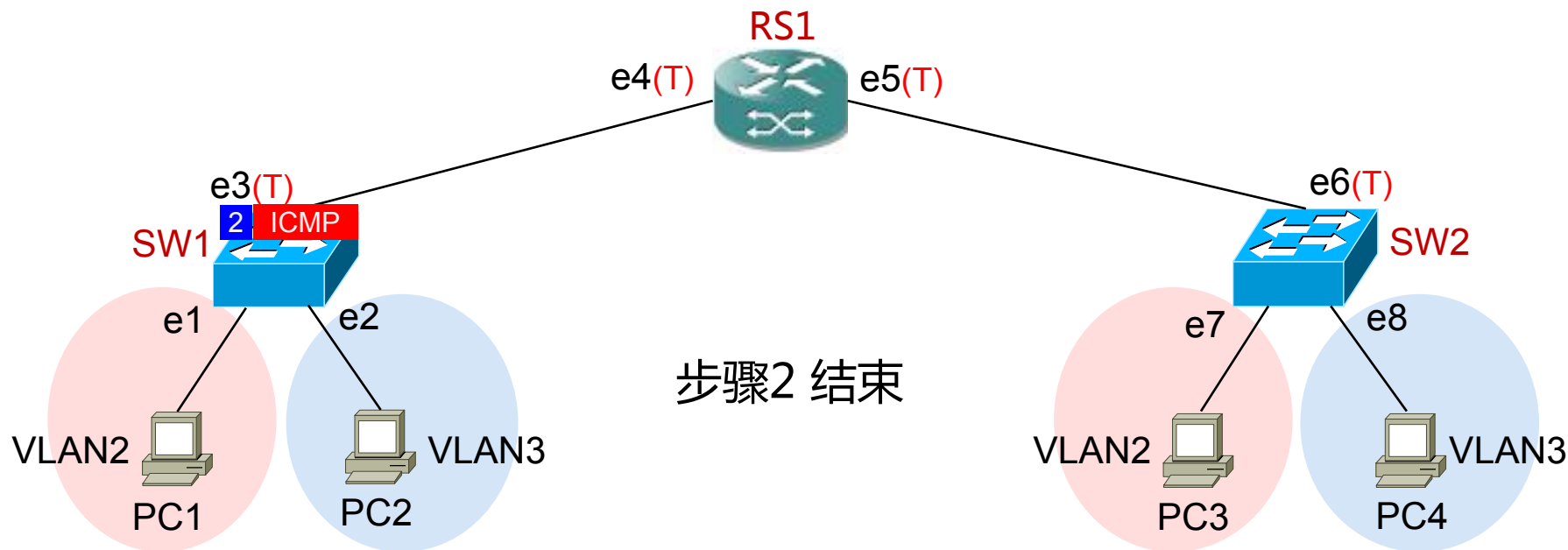


步骤2: PC1发送ICMP请求报文至RS1 (1) ——PC1封装ICMP请求报文

PC1发出ICMP请求报文，由于目的IP与自己不在同一网段，所以要先发给默认网关（即RS1的VLAN2的SVI接口）。于是在封装报文时，源MAC是MAC1，目的MAC是MAC_S。源IP是IP1，目的IP是PC4。报文先到达交换机SW1。



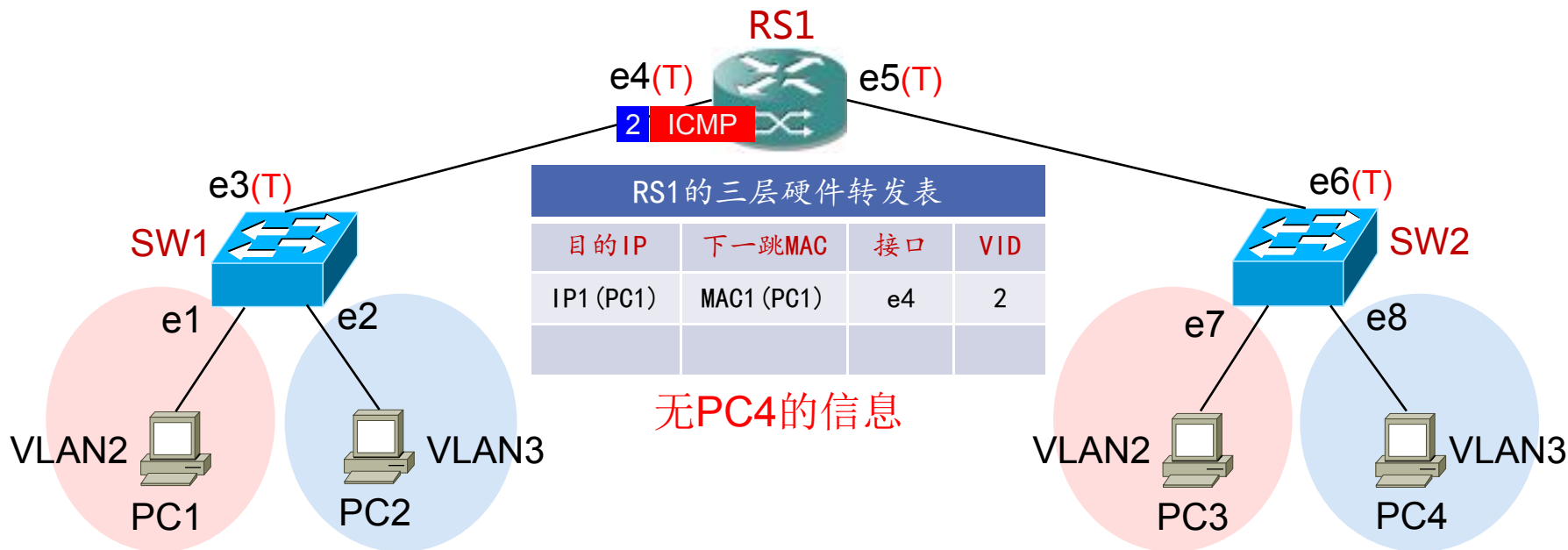
步骤2: PC1发送ICMP请求报文至RS1 (2) ——SW1处理报文: 加标签、转发
SW1的e1接口收到报文, 由于e1接口的PVID=2, 所以添加VLAN2的标签;
查找MAC地址表, 发现目的MAC (MAC_S) 对应e3接口, 并且也属于VLAN2, 于是转发至e3口;



步骤2: PC1发送ICMP请求报文至RS1 (3) ——SW1处理报文: 从e3接口发出
由于e3是trunk接口, 并且接口PVID≠帧VID, 所以保留VLAN2标签, 发送出去。

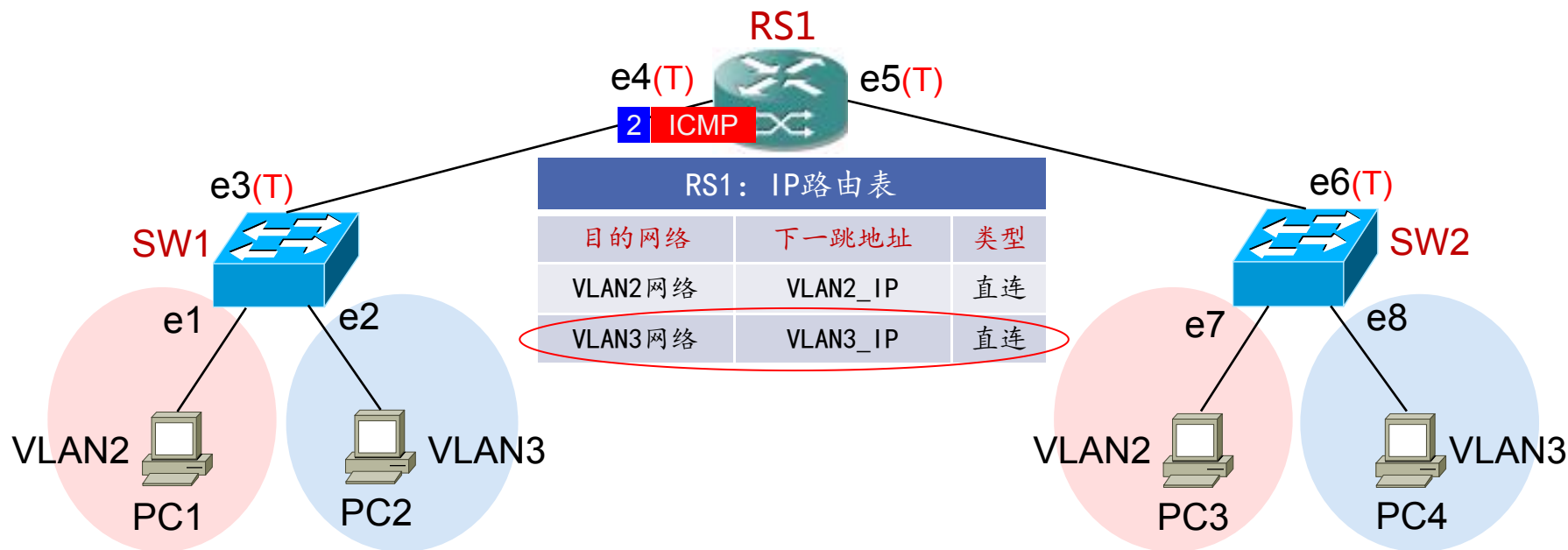
至此, PC1发出的ICMP请求报文, 到达了默认网关 (即RS1的VLAN2 的SVI)

三层交换机通信实例分析—— PC1 ping PC4 (17)



步骤3: RS1处理ICMP请求报文 (1) ——接收报文, 查看三层硬件转发表

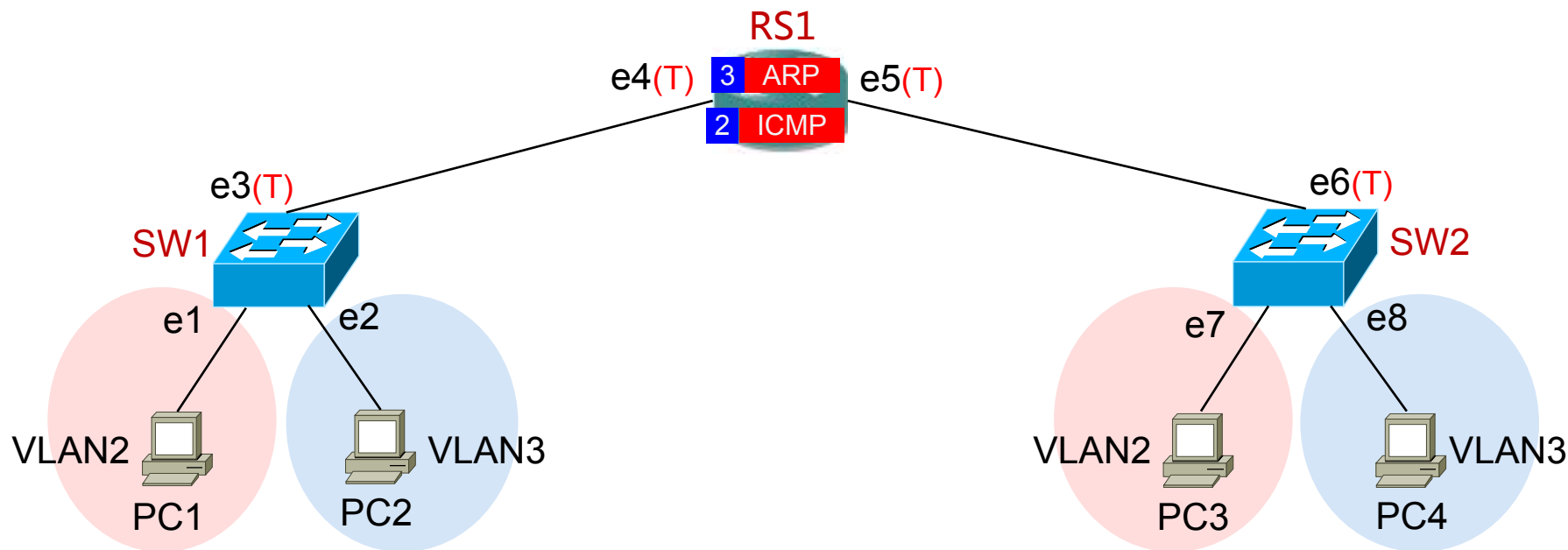
RS1的e4接口收到报文, 由于e4是trunk接口, 所以保留标签接收, 并送给VLAN2的SVI接口; 由于该报文被RS1上的三层虚拟接口 (即VLAN2 的SVI接口) 接收, 所以启用三层路由模块, 首先查询三层硬件转发表, 查看转发表中是否有目的IP地址 (即PC4的IP地址) 的信息。由于是首发数据包, 所以RS1的三层硬件转发表中, 此时并没有PC4的记录信息;



步骤3: RS1处理ICMP请求报文 (2) ——查看IP路由表 (软件路由)

由于三层硬件转发表中没有PC4的对应表项，于是CPU会根据数据包中的目的IP地址 (IP4)，进一步查看IP路由表 (软件路由表)。

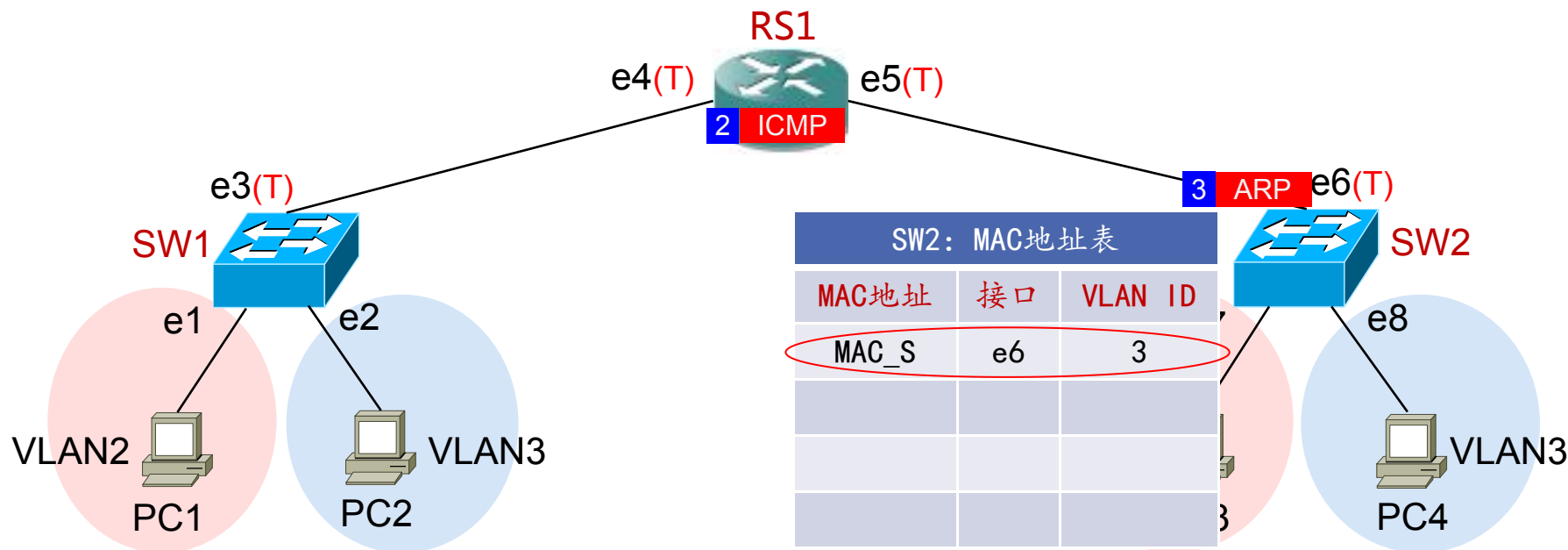
在路由表中，发现匹配了一个直连网段 (即VLAN3网络)，其下一跳是VLAN3的SVI接口IP地址 (VLAN3_IP)。于是，CPU依据直连路由，将数据包转给VLAN3的SVI接口。



步骤3: RS1处理ICMP请求报文 (3) ——获取PC4的MAC地址: 封装ARP请求报文

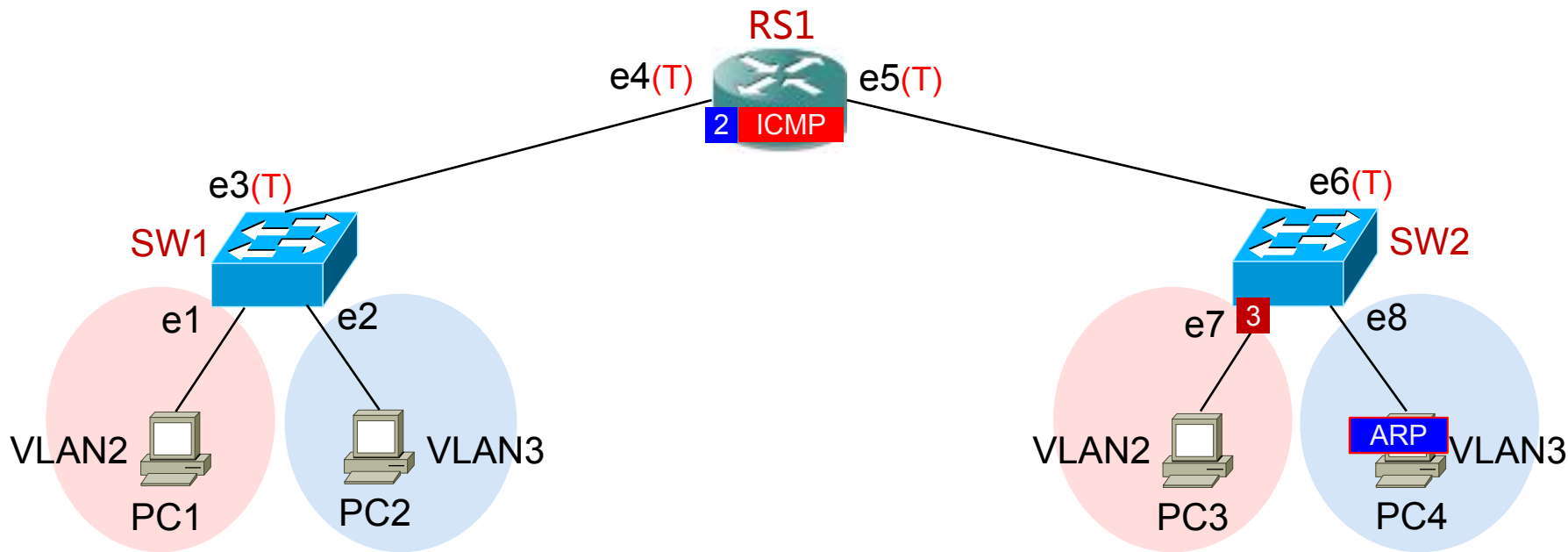
接下来VLAN3的SVI接口要将ICMP请求报文直接发给PC4, 假设此时它发现自己还不知道PC4的MAC地址。于是发出ARP请求, 报文中源MAC是MAC_S, 目的MAC是全1。

注意, 此处封装ARP报文时, 可看成是VLAN3的SVI接口封装报文, 因此要在帧头中添加VLAN3的标签, 此ARP请求报文会发至PC2和PC4, 且从e4或e5发出时不去掉VLAN标签。



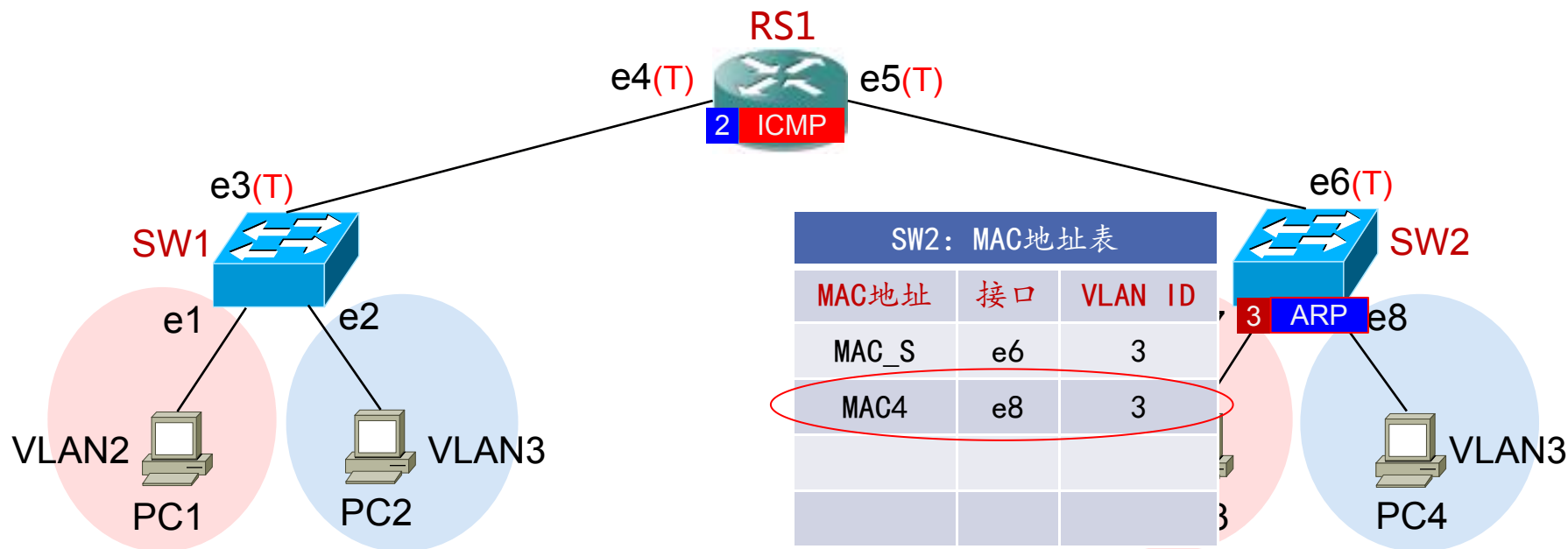
步骤3: RS1处理ICMP请求报文 (4) ——获取PC4的MAC地址: SW2转发ARP请求报文

- ARP请求报文到达e6, e6是trunk接口, 所以接收报文并保留标签;
- SW1在MAC地址表中添加VLAN3的SVI接口的记录;
- SW1将报文转发至所有属于VLAN3的接口 (来源接口除外), 包括e8接口;
- 由于e8是access接口, 所以从e8发出时, 去掉VLAN3标签, 然后到达PC4。



步骤3: RS1处理ICMP请求报文 (5) ——获取PC4的MAC地址: PC4返回ARP响应报文

- PC4返回ARP响应报文, 报文中源MAC是MAC2, 目的MAC是MAC_S;
- 响应报文到达e8, 因为e8属于VLAN3, 所以添加VLAN3标签;

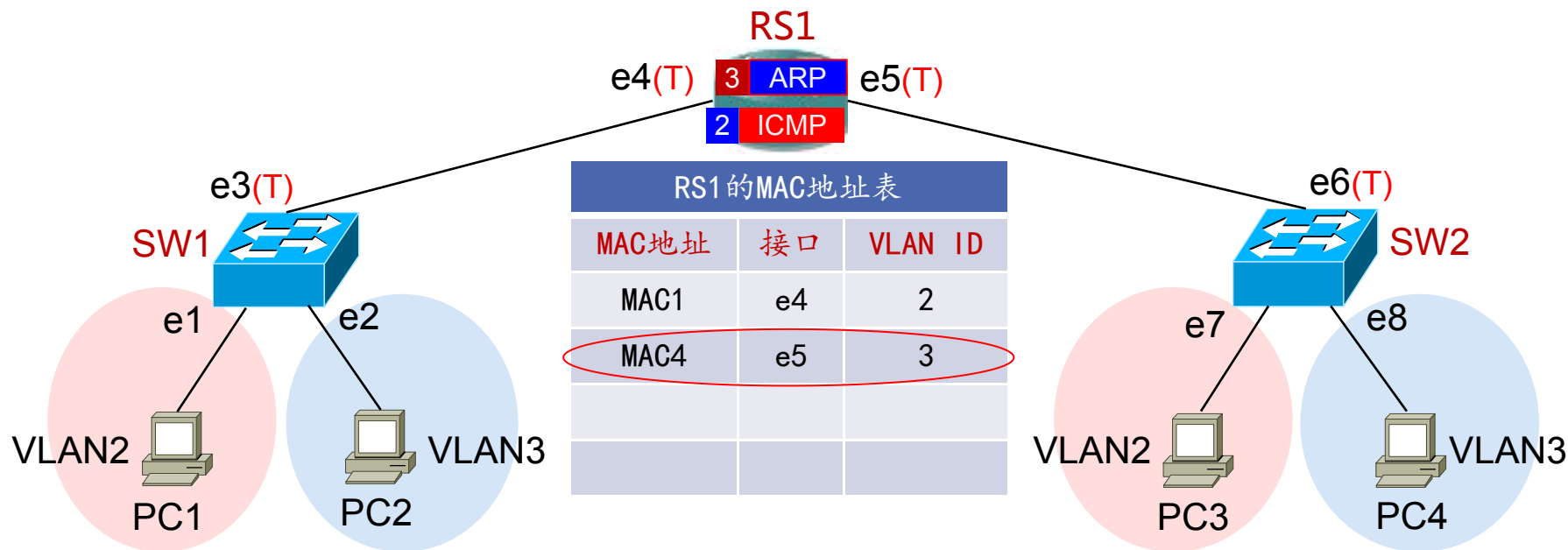


步骤3: RS1处理ICMP请求报文 (6) ——获取PC4的MAC地址: SW2转发ARP响应报文

SW2在MAC地址表中, 添加PC4的MAC地址的对应记录;

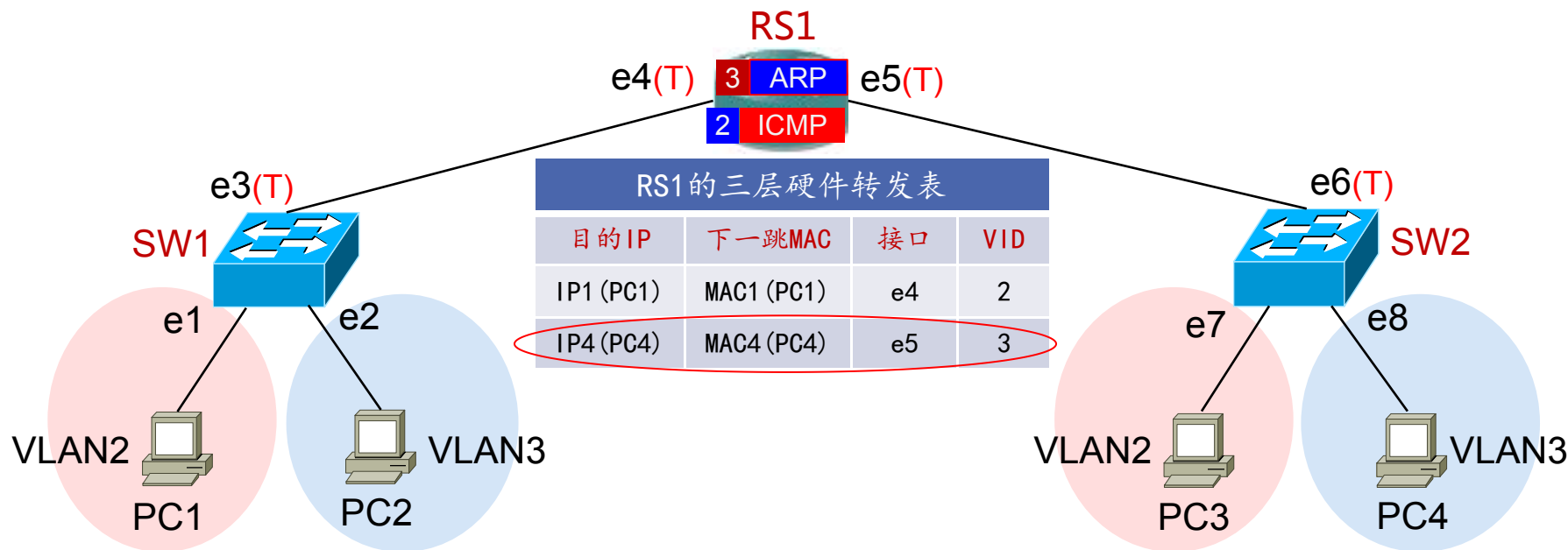
依据MAC地址表, 将报文转发至e6接口;

由于e6是trunk接口, 所以保留VLAN3标签发送至RS1。



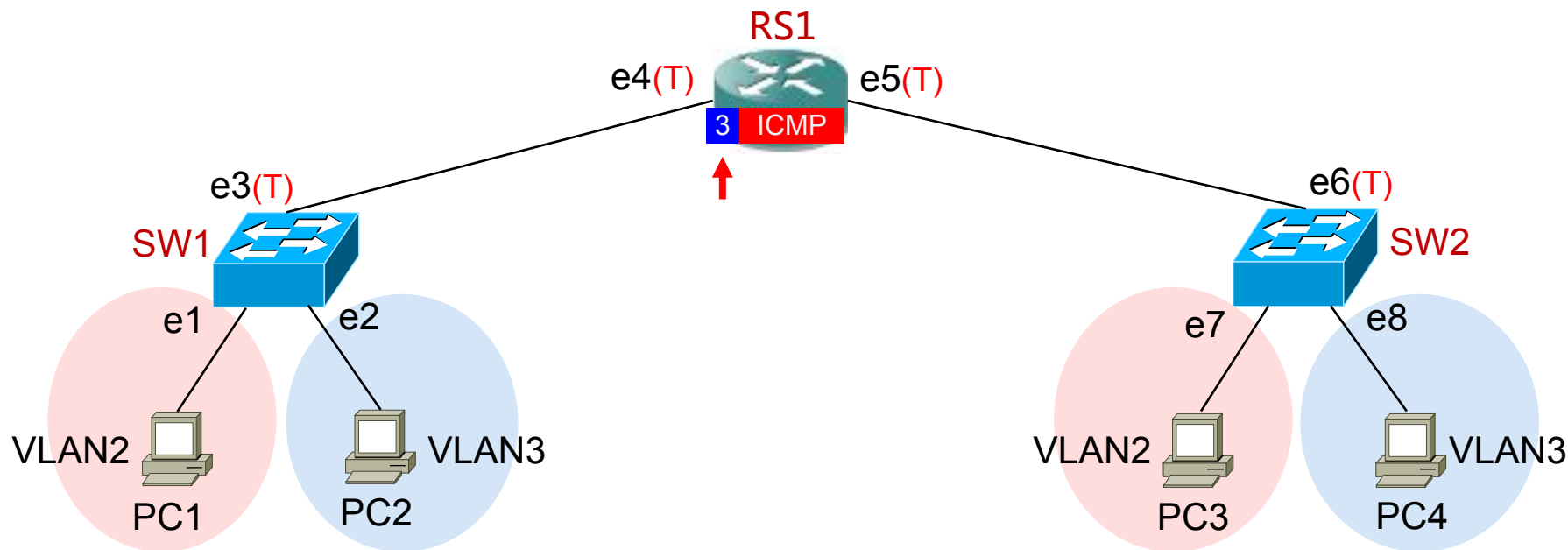
步骤3: RS1处理ICMP请求报文 (7) ——RS1在MAC地址表中添加PC4的记录

- RS1的e5接口收到PC4发来的ARP响应报文（保留VLAN3标签），获取到PC4的MAC地址，于是在自己的MAC地址表中，添加PC4的MAC地址的相关记录。



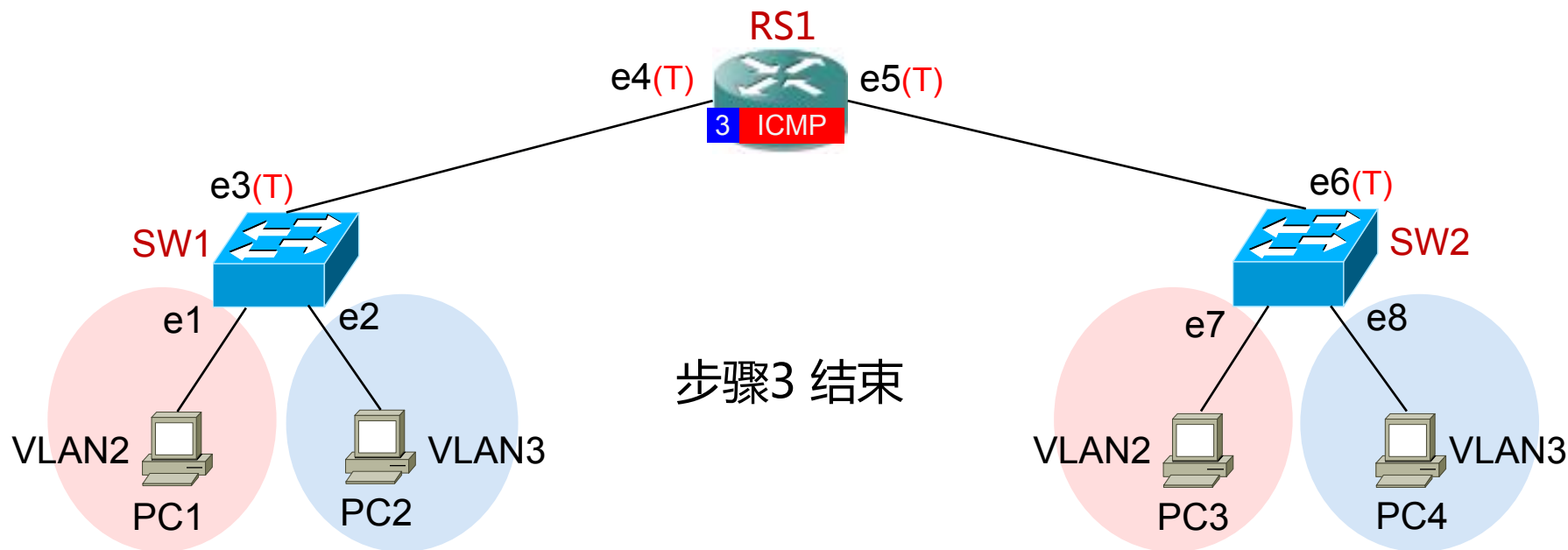
步骤3: RS1处理ICMP请求报文 (8) ——RS1在三层硬件转发表中添加PC4的记录

- RS1分析ARP响应报文的内容, 获取到PC4的相关信息, 然后在自己的三层硬件转发表中, 添加PC4的相关记录, 于是三层硬件转发表中有了第2条记录。
- 以后其他网段主机与PC4通信时, RS1的ASIC芯片会直接把数据包从本表指定的接口 (即 e5) 转发出去 (硬件转发), 不必再查看IP路由表 (软件路由)。



步骤3: RS1处理ICMP请求报文 (9) ——RS1重新封装ICMP请求报文

- 此时，RS1已经知道PC4的MAC地址，于是将PC1发来的ICMP请求报文（此时已经通过直连路由转发至VLAN3的SVI接口）重新封装。
- 在封装时，源IP（IP1）和目的IP（IP4）保持不变，MAC4为目的MAC，将VLAN3的SVI接口的MAC（即MAC_S）作为源MAC地址，并且VLAN标签变为VLAN3的标签

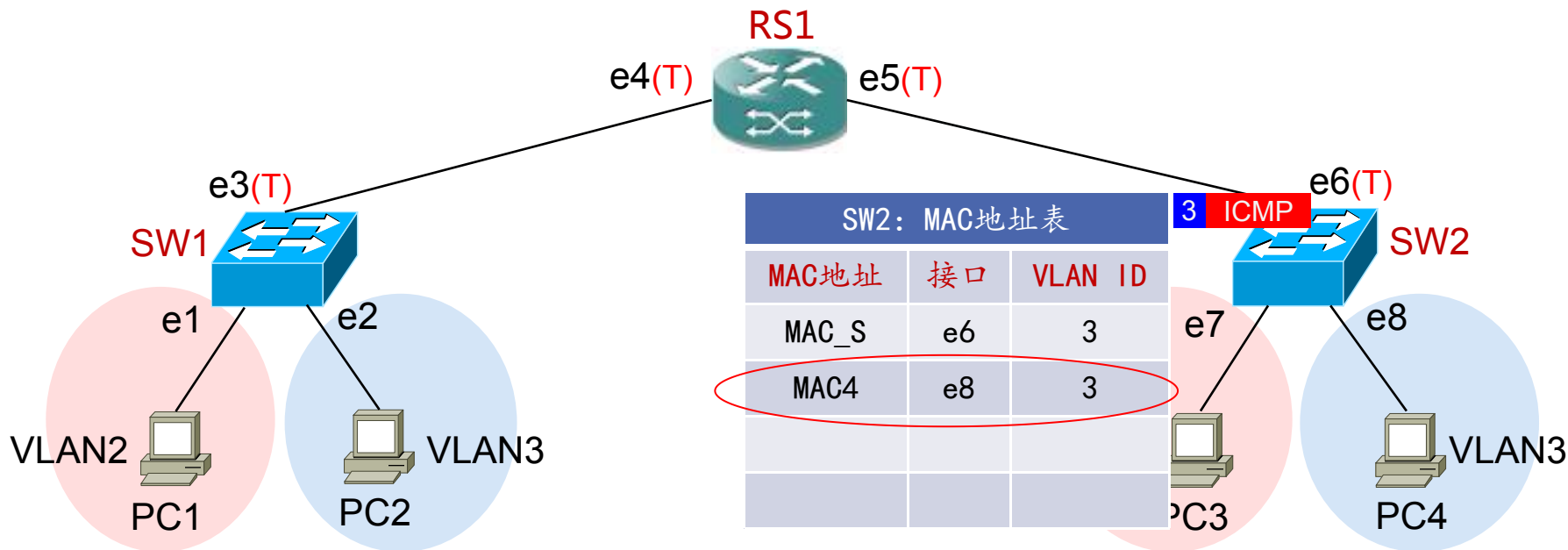


步骤3: RS1处理ICMP请求报文 (10) ——RS1转发ICMP请求报文

- RS1根据前面查看路由表得出的路由结果, 将重新封装的ICMP请求报文, 从e5接口发出;
- 由于e5接口是Trunk接口, 所以会保留VLAN3标签然后发出, 到达SW2。

至此, PC1 (VLAN2) 发出的ICMP请求报文, 经过RS1的处理, 到达了VLAN3

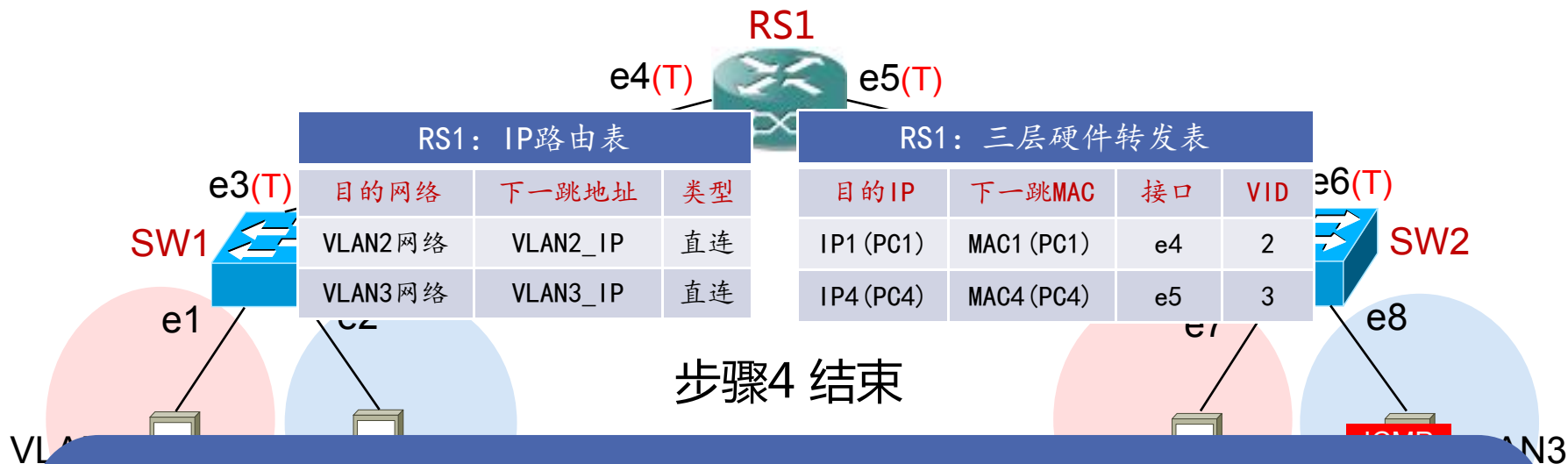
三层交换机通信实例分析—— PC1 ping PC4 (27)



步骤4: SW2处理ICMP请求报文

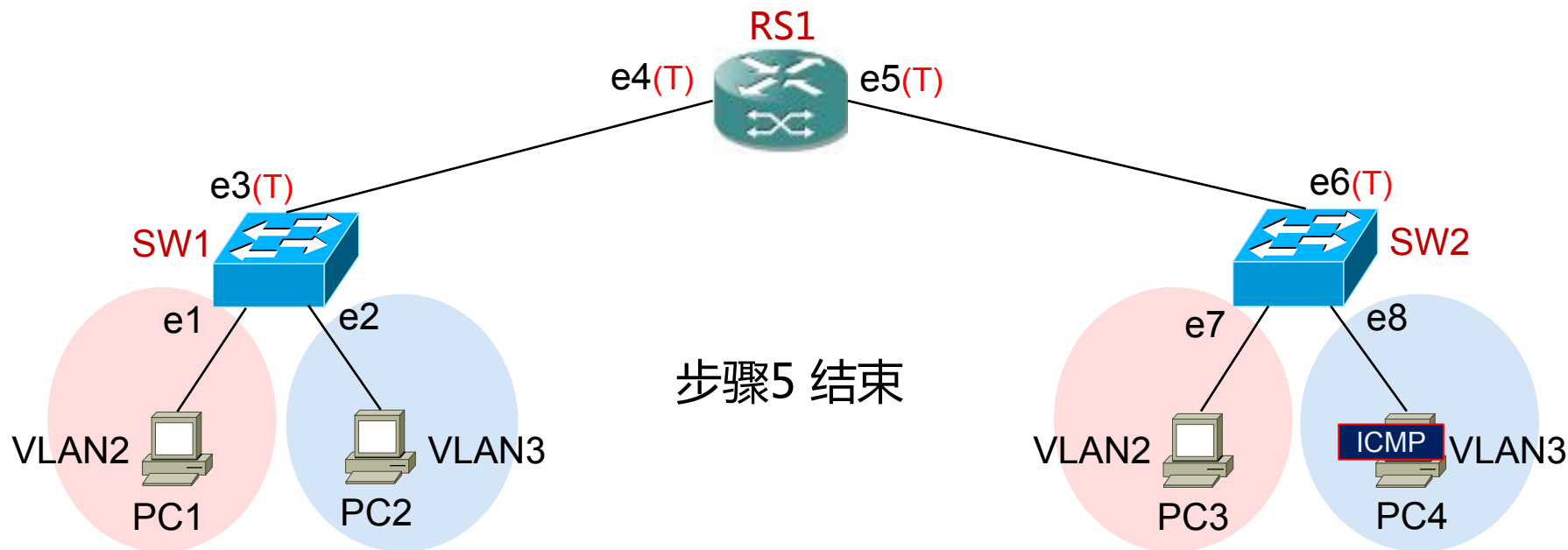
- SW2的e6接口收到ICMP请求报文，由于e6是trunk接口，所以接收报文并保留VLAN3标签。
- SW2依据自己的MAC地址表，将ICMP请求报文转发至e8接口。
- 由于e8接口是access接口，所以会去掉VLAN3标签然后发出，最终到达PC4。

三层交换机通信实例分析—— PC1 ping PC4 (28)



至此，PC1 (VLAN2) 发出的ICMP请求报文，经过三层交换机RS1的转发，到达了目的主机PC4 (VLAN3)。注意，由于这是首报文，所以在通过RS1时，依据IP路由表转发（软件转发）。

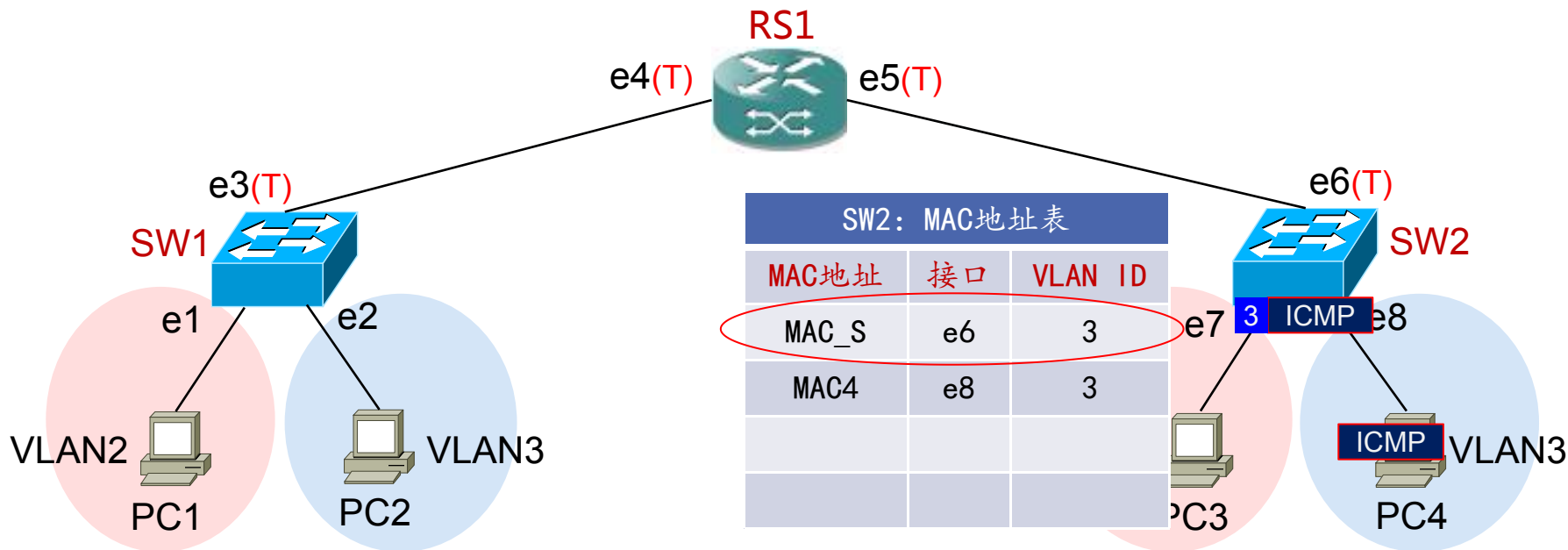
同时，RS1在转发时，也在自己的三层硬件转发表中，添加了PC1和PC4的相关记录。后续，RS1再收到发给PC1或PC4的报文，就不再查询路由表，直接通过三层硬件转发表，进行硬件转发，这就是“一次路由，多次交换”！



步骤5: PC4发出ICMP响应报文

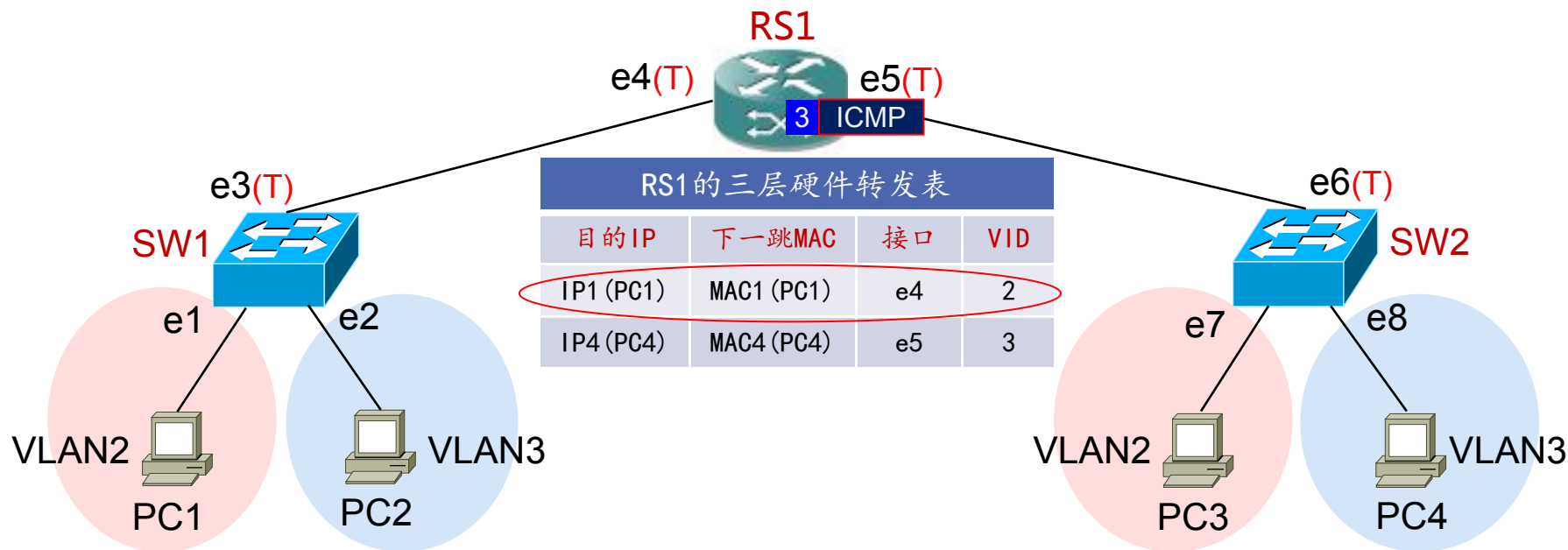
- PC4收到PC1发来的ICMP请求报文，要向PC1发回ICMP响应报文。由于目的IP与源IP不在同一网段，所以PC4先将响应报文发给自己的默认网关，即RS1中VLAN3的SVI接口；
- PC4封装ICMP响应报文，该报文的源IP为IP4，目的IP为IP1，源MAC为MAC4，目的MAC为MAC_S。注意，此时PC4已经知道默认网关的MAC地址是MAC_S。

三层交换机通信实例分析—— PC1 ping PC4 (30)



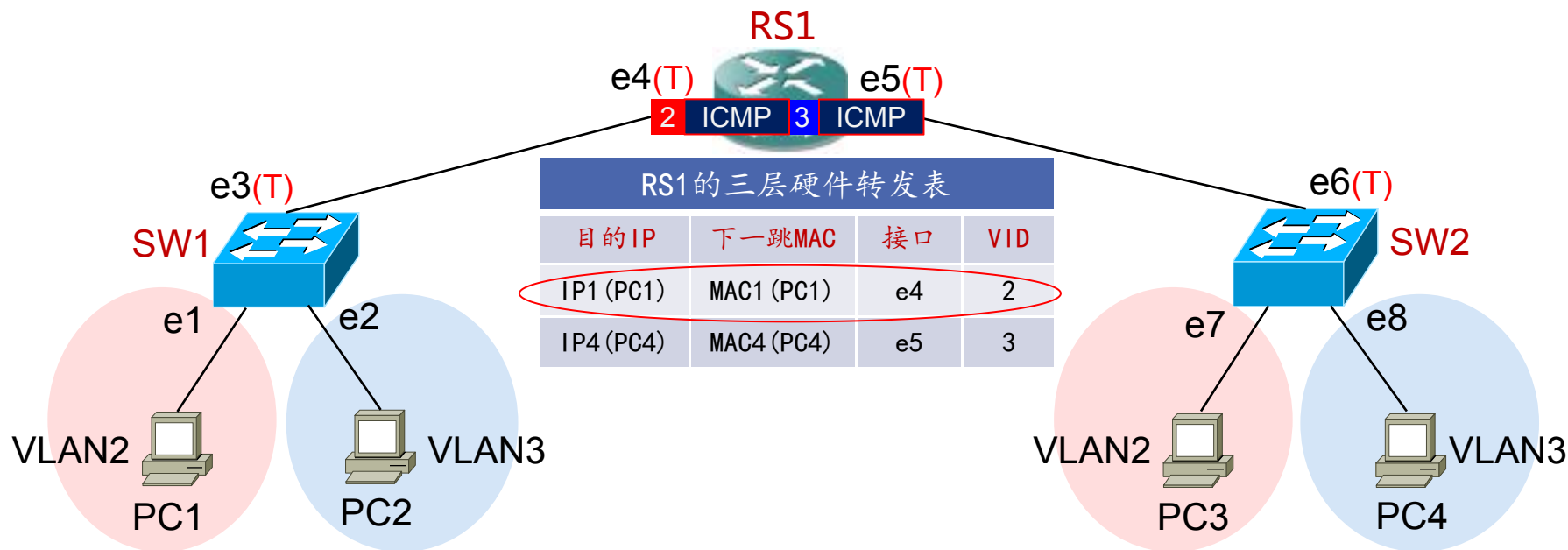
步骤6: SW2处理ICMP响应报文

- ICMP响应报文发送到SW2的e8接口，被加上VLAN3的标签；
- SW2依据MAC地址表，将ICMP响应报文转发至e6接口；
- 由于e6接口是trunk接口，所以保留VLAN3标签，发出ICMP响应报文；



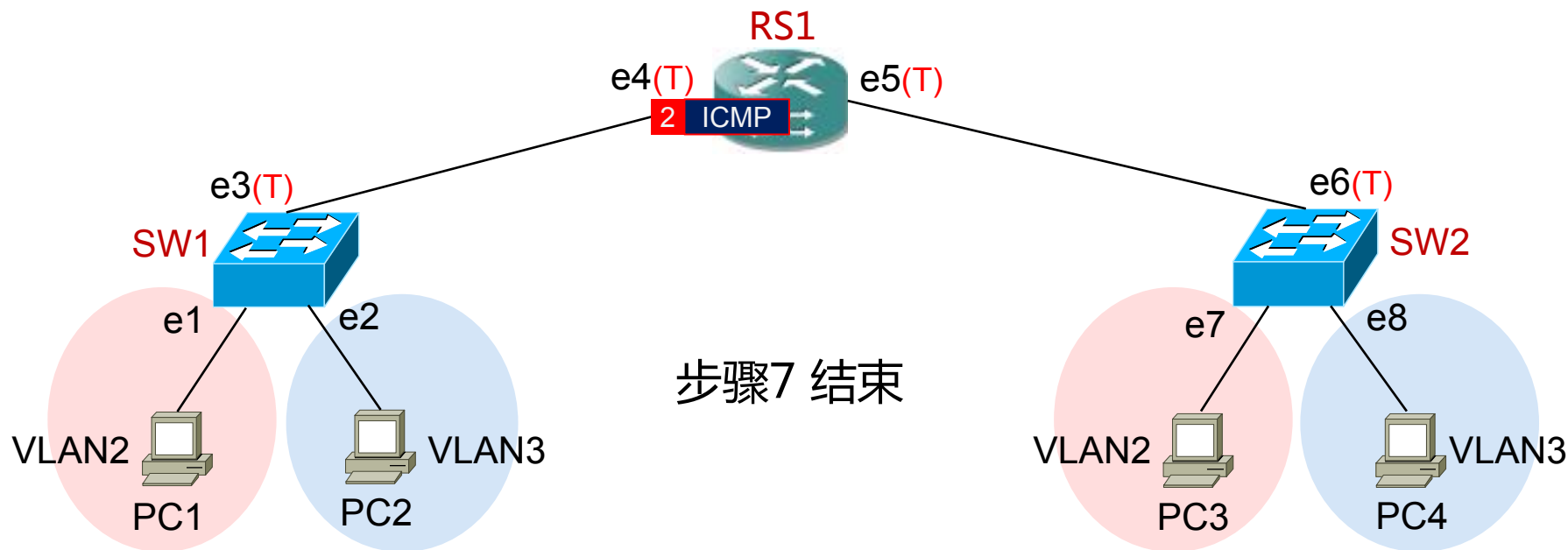
步骤7: RS1转发ICMP响应报文 (1) ——查看三层硬件转发表

- RS1收到ICMP响应报文，由于该报文是发给VLAN3的三层虚拟接口的，所以RS1启用三层路由模块，首先在ASIC芯片中的三层硬件转发表中查看。
- 注意**，此时三层硬件转发表中有PC1的记录，意味着RS1可以直接进行转发（硬件转发）该报文，并且在转发前要重新封装ICMP响应报文。



步骤7: RS1转发ICMP响应报文 (2) ——RS1重新封装ICMP响应报文

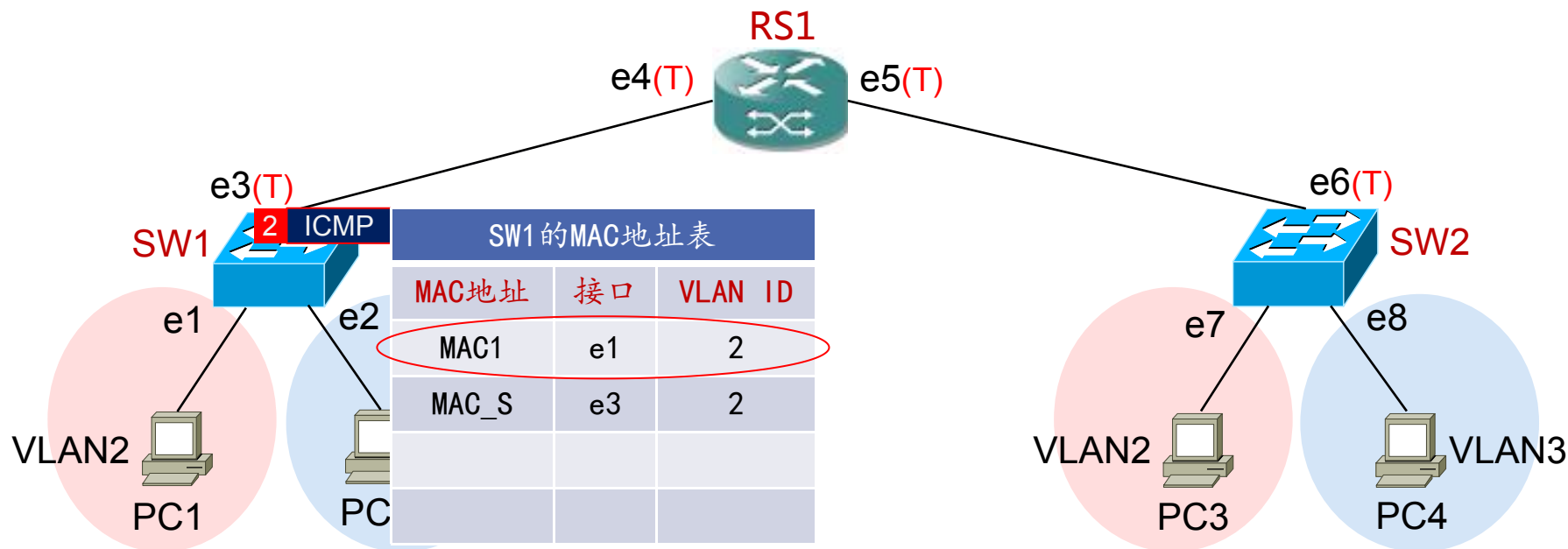
- RS1根据在三层硬件转发表中的查找结果, 重新封装ICMP响应报文。具体为: 目的IP (IP1) 和源IP (IP4) 保持不变, 目的MAC为MAC1, 源MAC为MAC_S;
- 注意: 由于IP1对应的VID值=2, 所以报文首部的VLAN标签变为VLAN2的标签;
- 根据三层硬件转发表, 重新封装的ICMP响应报文被转发到e4接口;



步骤7: RS1转发ICMP响应报文 (3) ——RS1发出ICMP响应报文

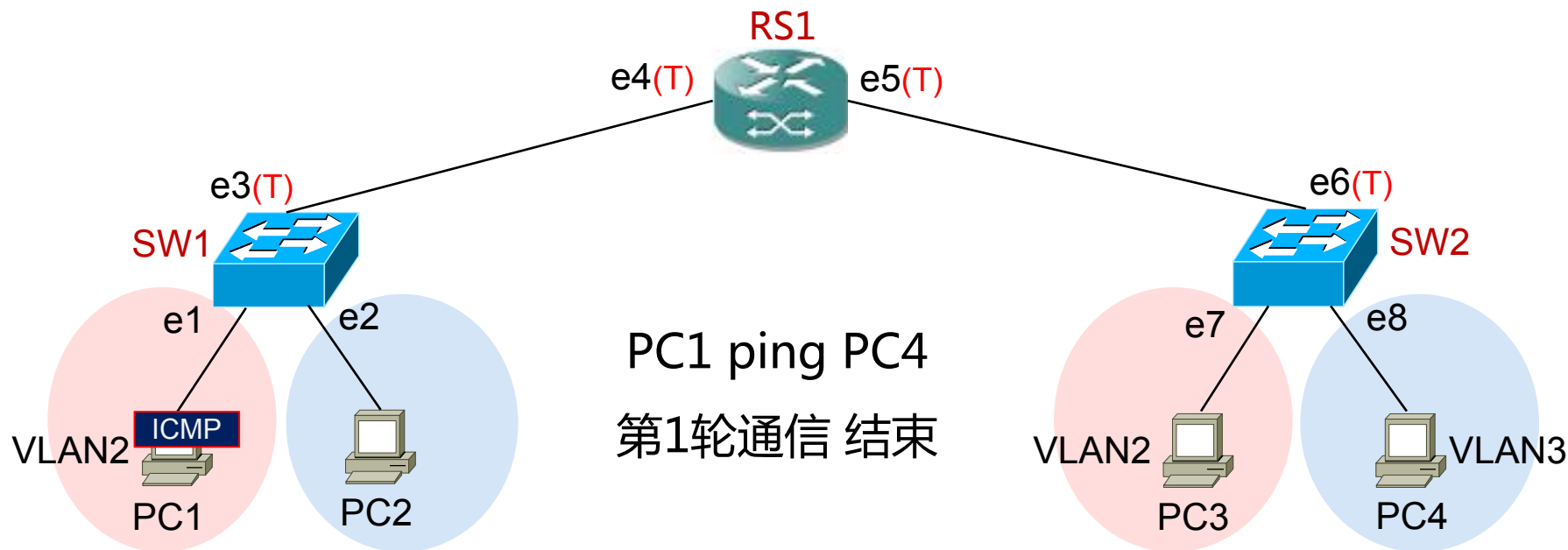
- 从e4接口发出，由于e4是trunk接口，且接口PVID≠帧VID，所以在发出ICMP响应报文时，保留VLAN2标签。

至此，PC4发出的ICMP响应报文，经过三层交换机的转发，从VLAN3转到VLAN2。注意，由于不是首报文，所以在通过RS1时，依据三层硬件转发表，是硬件转发。



步骤8: SW1转发ICMP响应报文

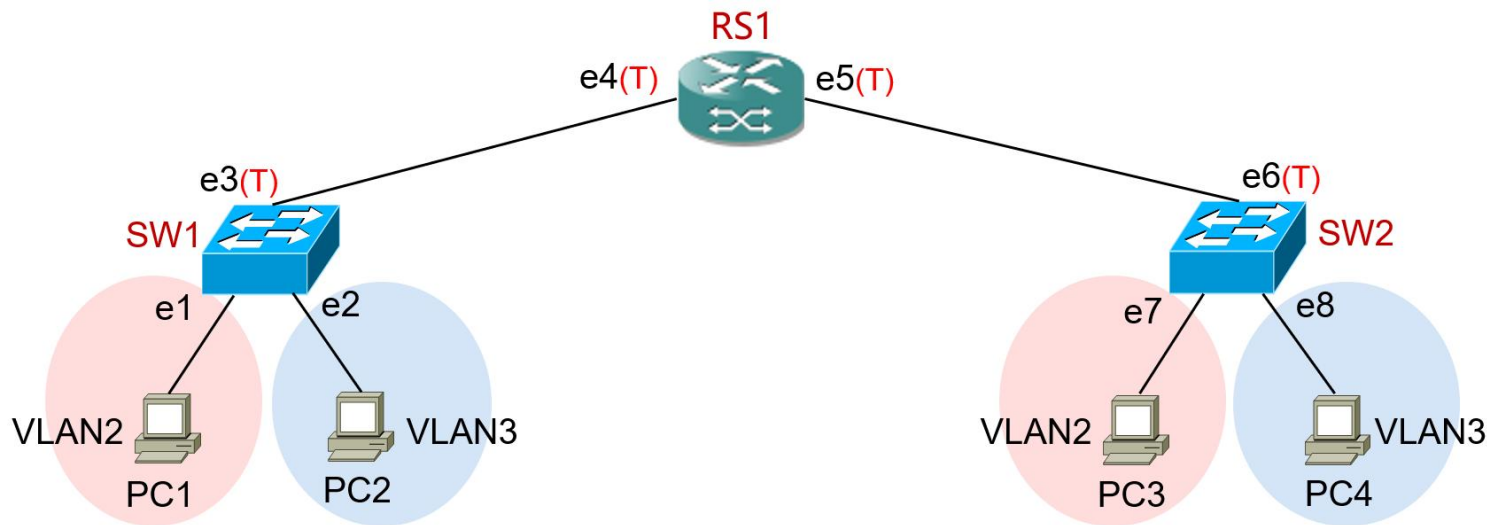
- SW1收到ICMP响应报文，依据自己的MAC地址表，将报文转发至e1接口。
- 由于e1接口是access类型，所以去掉VLAN2标签后，将ICMP响应报文发送出去，最终到达PC1。



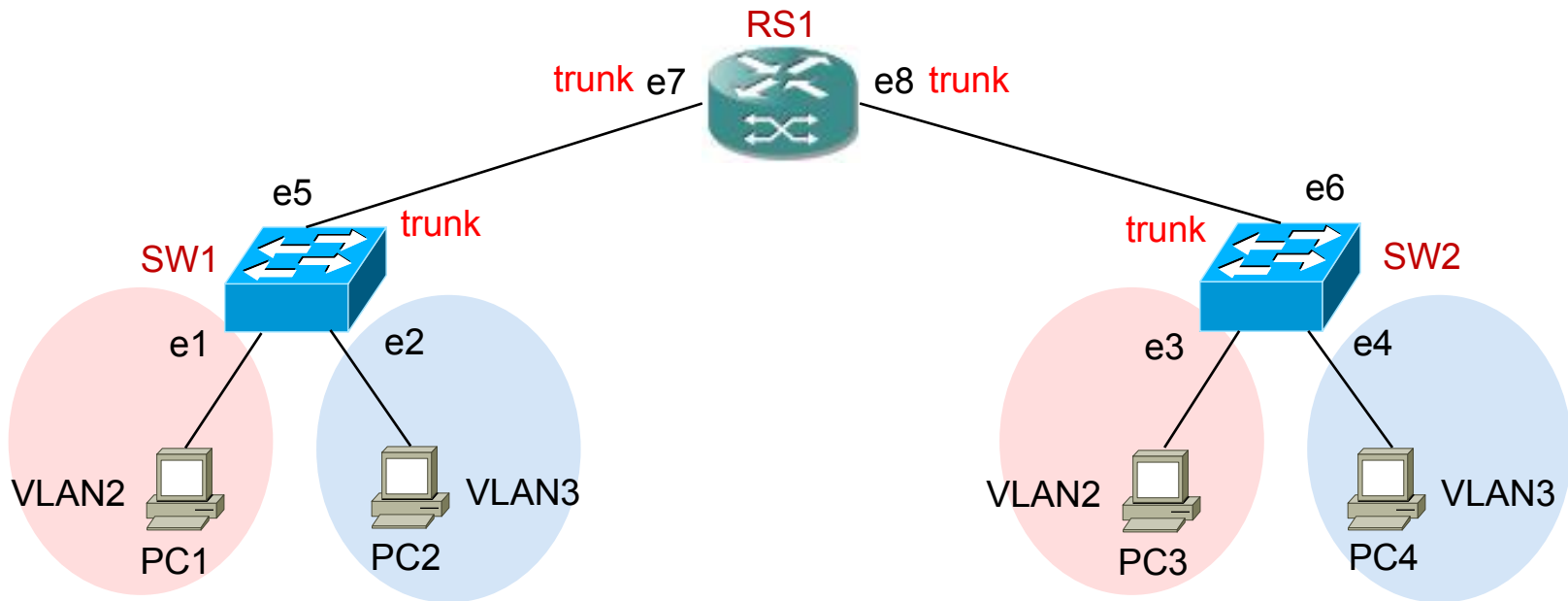
至此，PC1 ping PC4的第1轮通信结束，由于RS1中的三层硬件转发表中已经有了PC1和PC4的信息，所以后续PC1和PC4之间的访问在经过RS1时，都是依据三层硬件转发表进行硬件转发，效率更高。

分析2：同交换机中，不同VLAN主机之间通信

PC1 ping PC2 （自主）



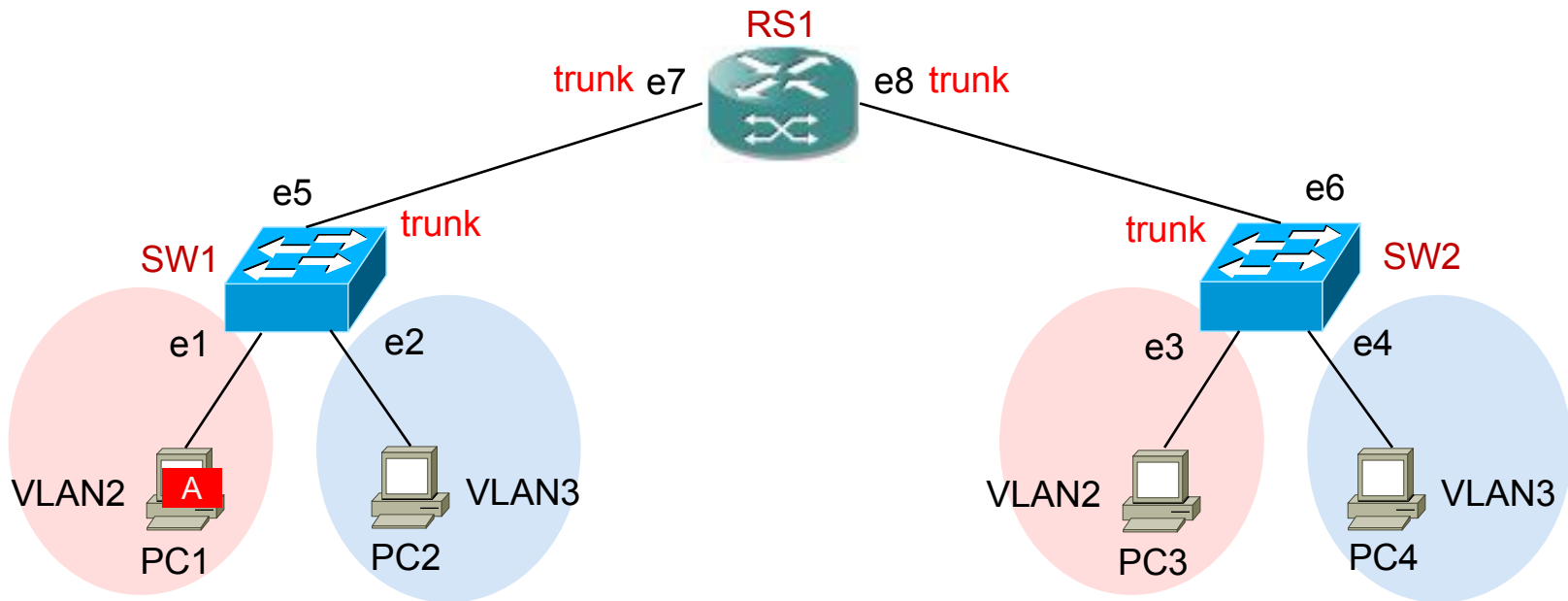
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（1）说明

PC1发现目的IP（即IP2）与自己不在同一网段，于是要先把自己的数据包发给自己的默认网关（即三层交换机上VLAN2的SVI接口）。但是，PC1此时不知道默认网关的MAC地址，必须先通过ARP协议获取到默认网关的MAC地址。

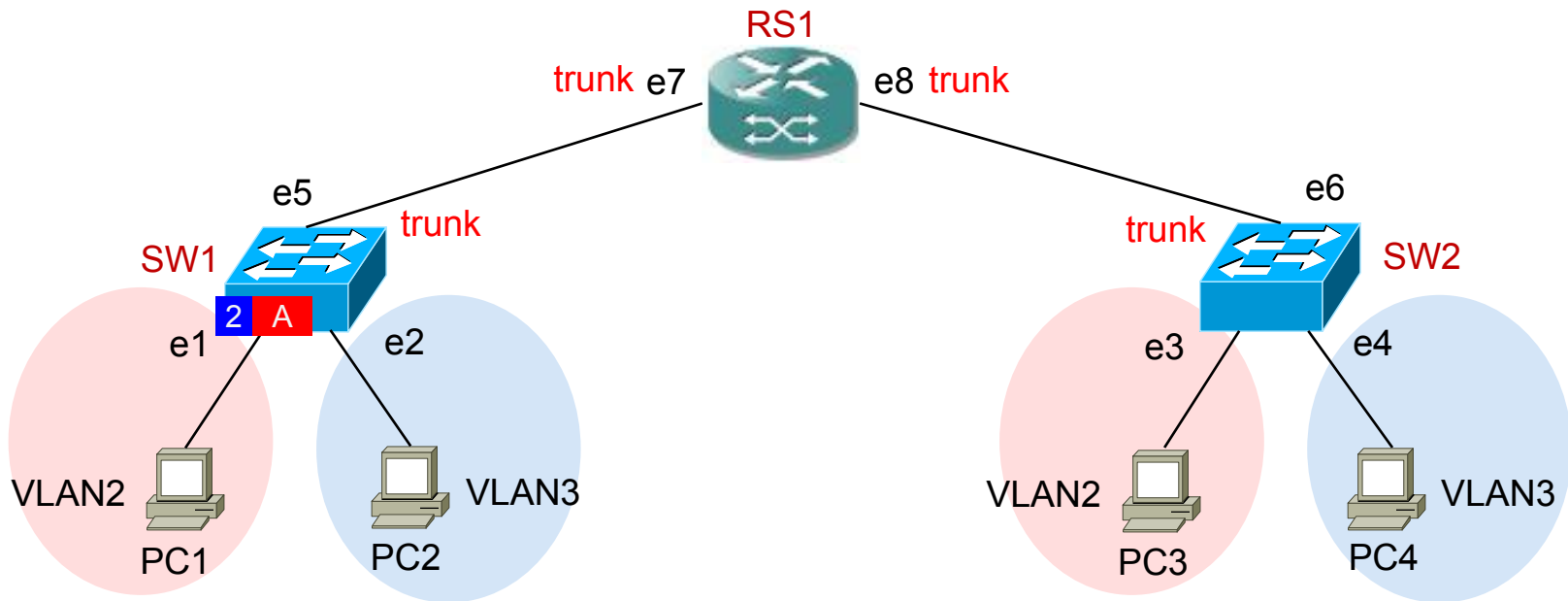
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（2）PC1封装ARP请求报文

于是，PC1发出ARP请求报文（广播报文），在封装报文时，源MAC是MAC1，目的MAC是ff-ff-ff-ff-ff-ff。

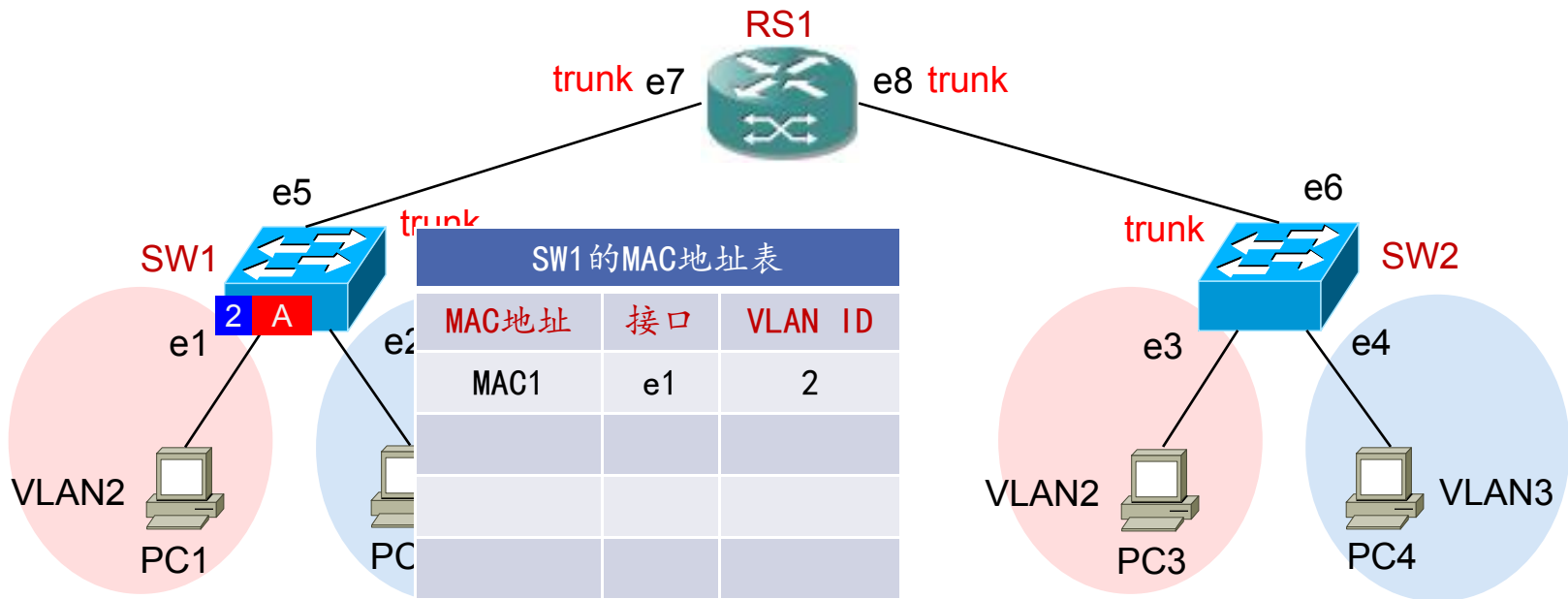
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（3）SW1的处理——添加VLAN标签

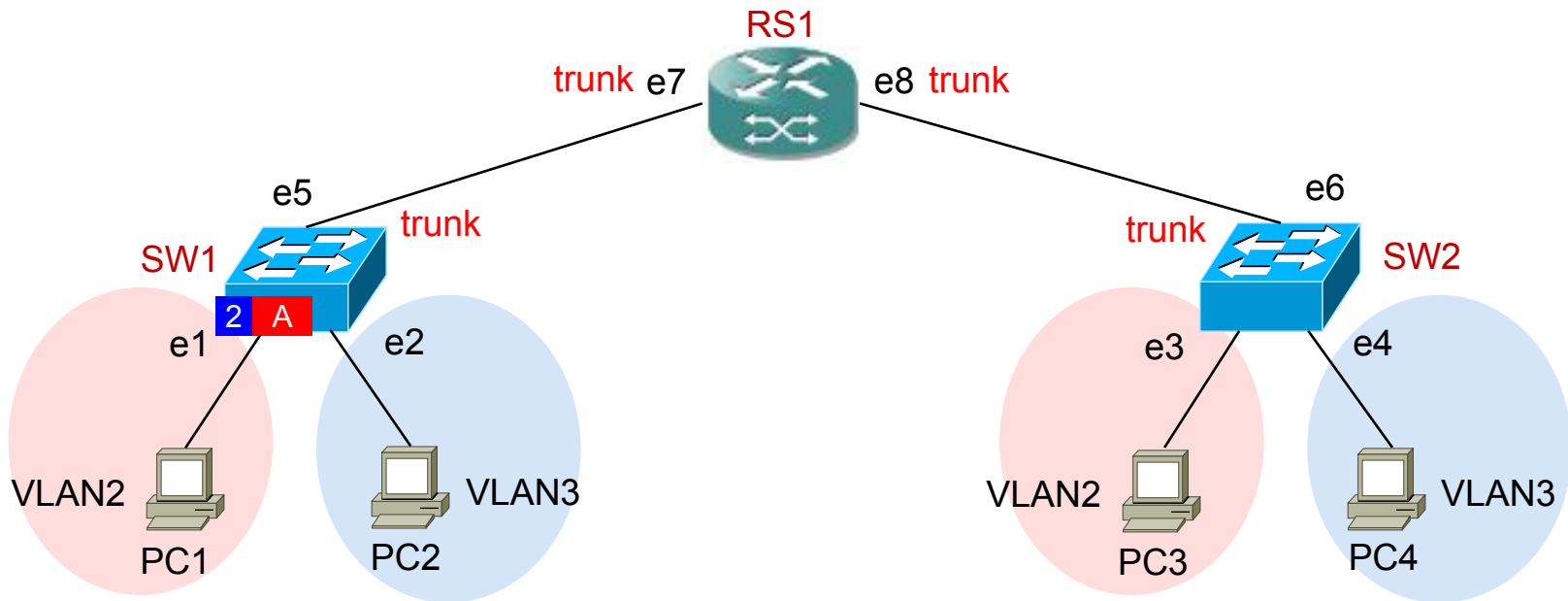
交换机SW1的e1接口（access接口）收到ARP报文，添加VLAN标签，由于e1属于VLAN2，所以此处在此帧头中添加VLAN2的标签。

三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（3）SW1的处理——添加MAC地址表记录
SW1在自己的MAC地址表中添加主机PC1的相关记录。

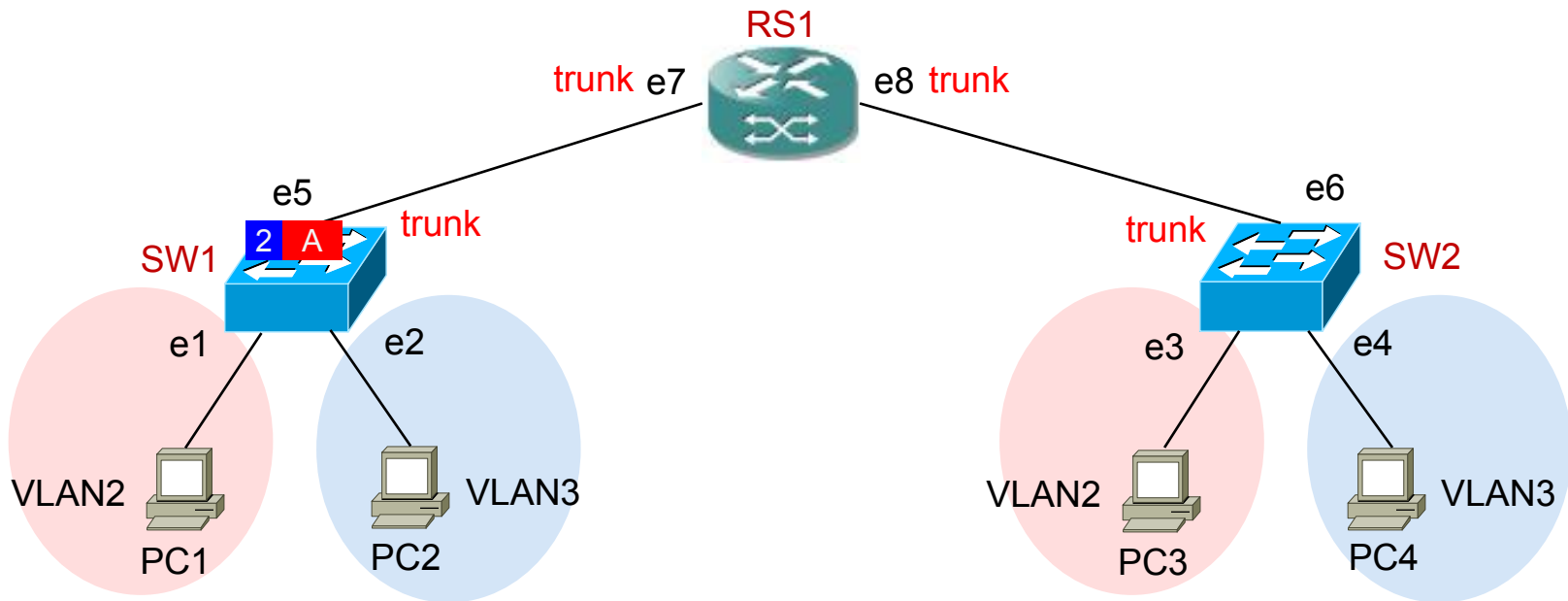
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（3）SW1的处理——转发数据帧

由于ARP报文的目的MAC是广播地址，所以SW1会把该报文转发到SW1上所以属于VLAN2的接口，由于e5接口是trunk类型，所以该ARP报文也会转发到e5接口；

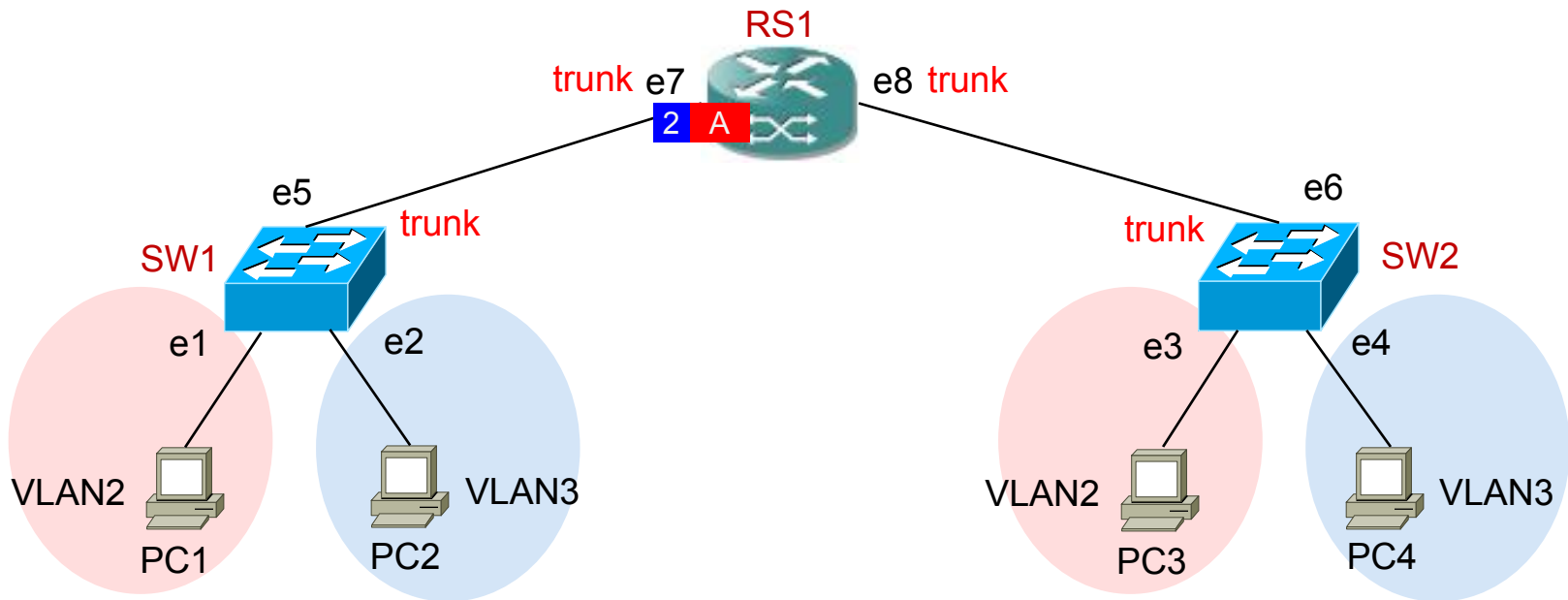
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（3）SW1的处理——从e5接口发出

由于e5接口是trunk类型，且接口的PVID≠报文的VID，所以，该报文会携带VLAN2的标签，从e5接口发出，到达RS1的e7接口。

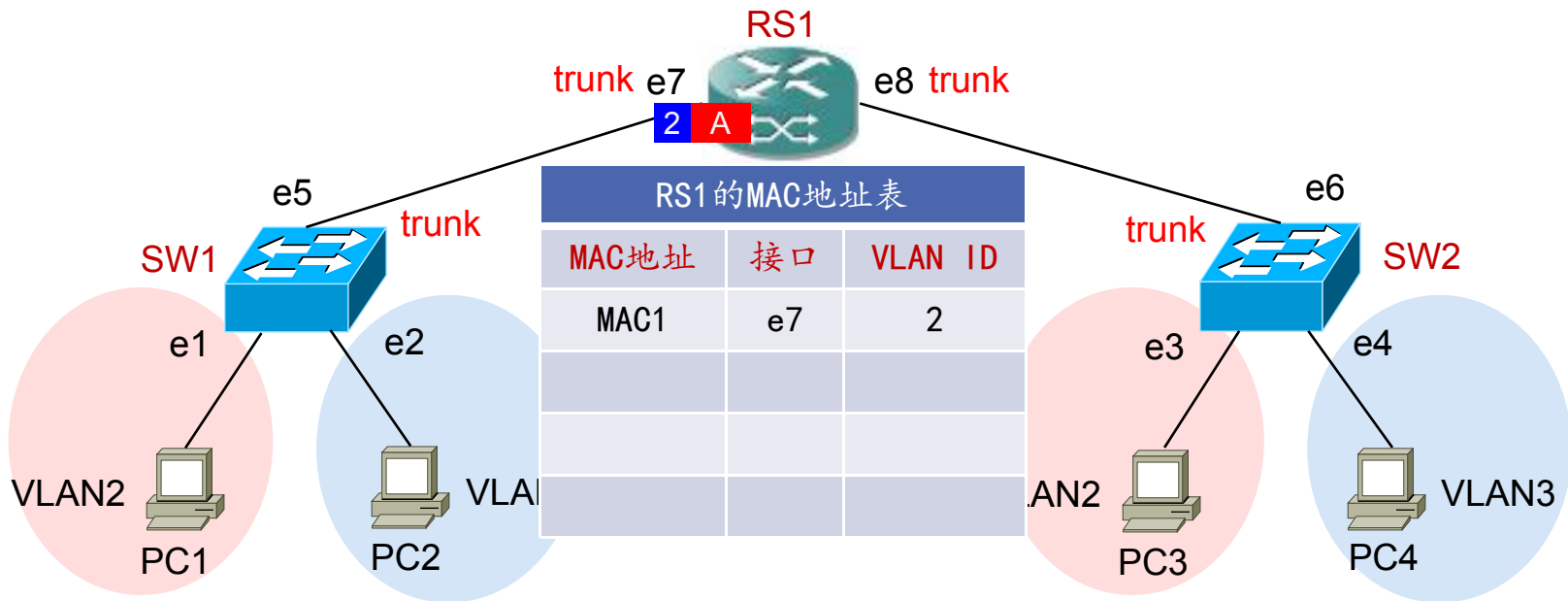
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（4）RS1的处理——接收报文

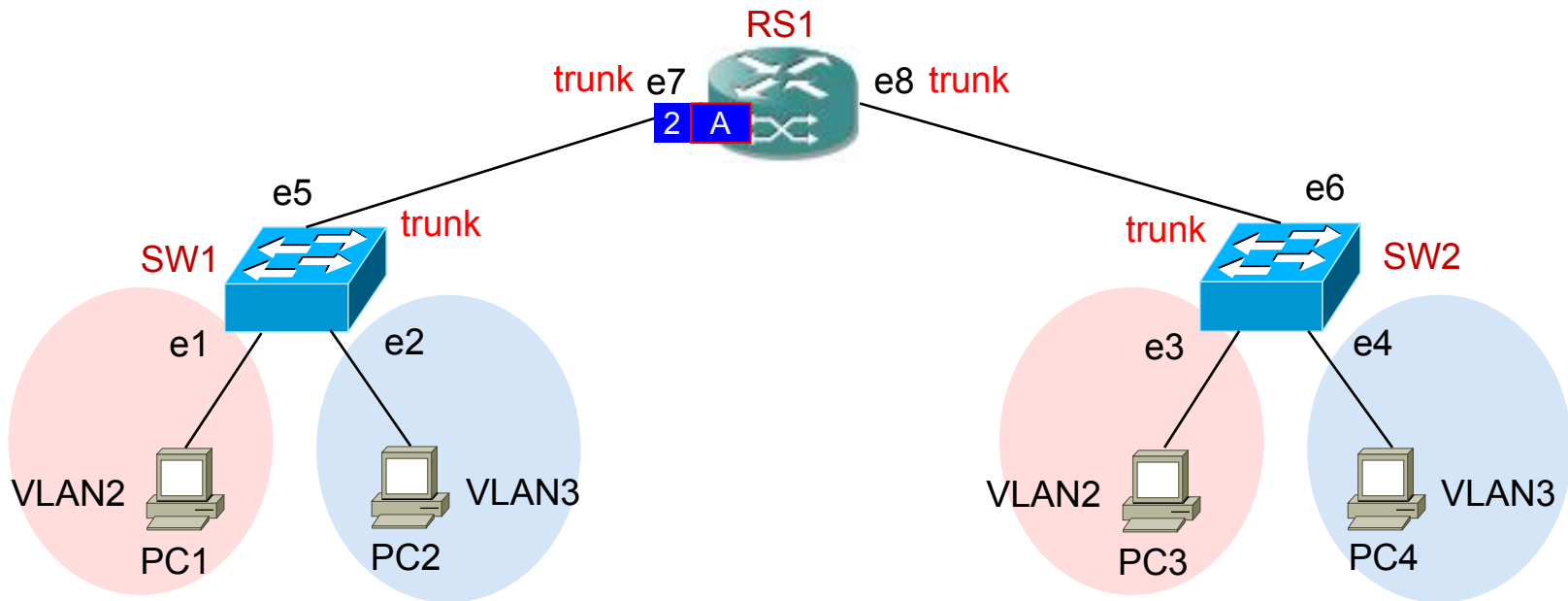
由于e7接口是trunk类型，所以会保留VLAN2的标签并接收该报文。

三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（4）RS1的处理——在MAC地址表中添加记录
RS1根据所收到报文的来源信息，在自己的MAC地址表中，添加PC1的相关记录。

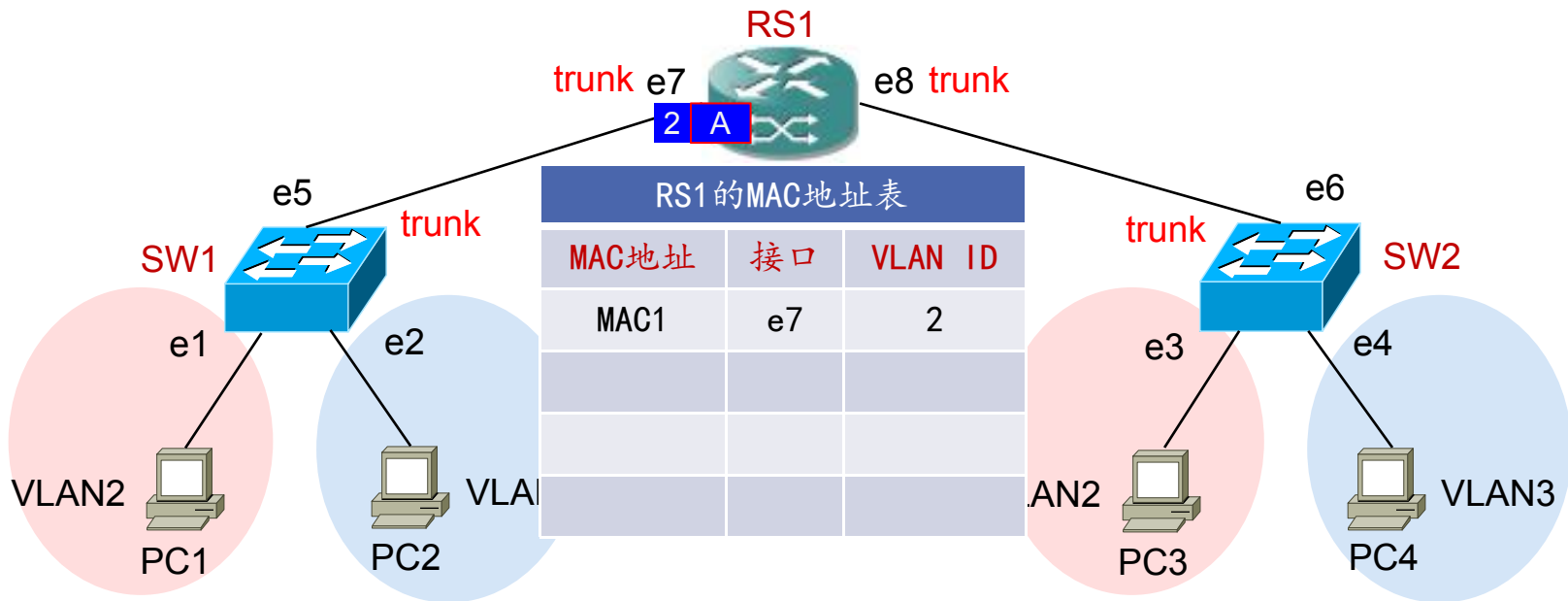
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（4）RS1的处理——发ARP响应报文

RS1收到ARP请求报文后，分析报文内容，发现报文中被请求的IP地址是自己的三层接口（即VLAN2的SVI接口）IP地址，于是发回ARP响应报文。该报文的目的MAC是MAC1，源MAC是MAC_S。注意，该报文也有VLAN标签，VID=2。

三层交换机组网实例分析——PC1访问PC2 (Ping)

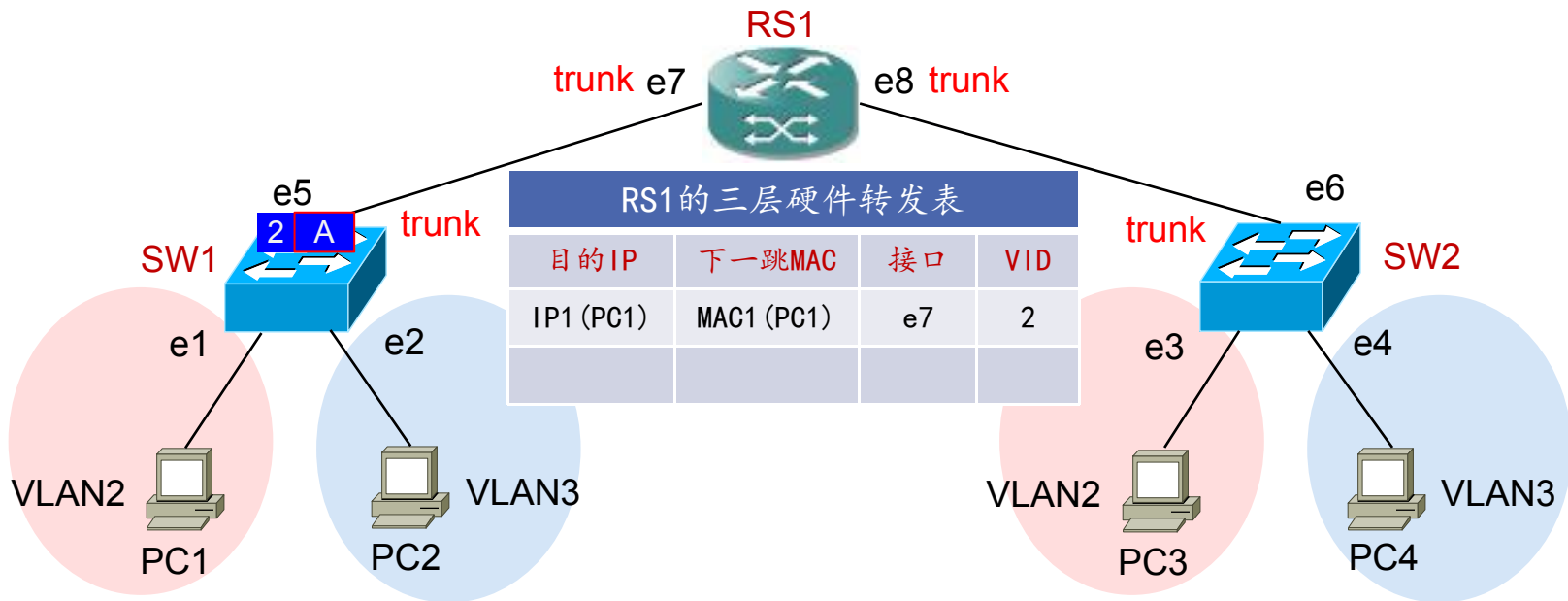


1. PC1获取默认网关的MAC地址——（4）RS1的处理——从e7接口发出

RS1封装好ARP响应报文后，查看自己的MAC地址表，发现目的MAC地址对应的是e7接口，于是从e7接口发出报文。

由于e7接口是trunk口，所以不去掉VLAN2的标签。

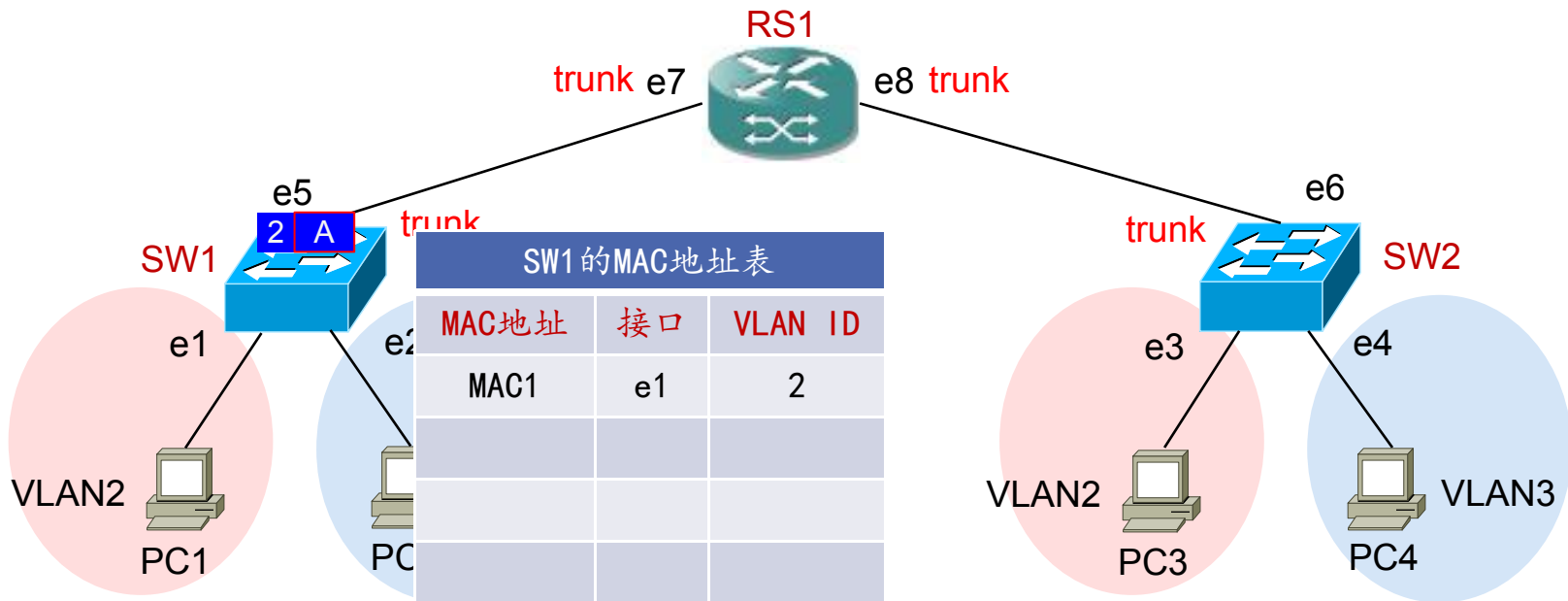
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（4）RS1的处理——在三层硬件转发表中添加记录

同时，RS1会在三层硬件转发表中添加一条到达主机PC1的记录，包含：目的IP地址（即IP1）、下一跳MAC地址（即MAC1）、接口号（即e7）、VLAN ID（即2）。以后，其他网段的主机想与PC1通信时，RS1的ASIC芯片就会直接把包从本表指定的接口（即e7）转发出去（即硬件转发），而不必再交给查看IP路由表（软件路由）。

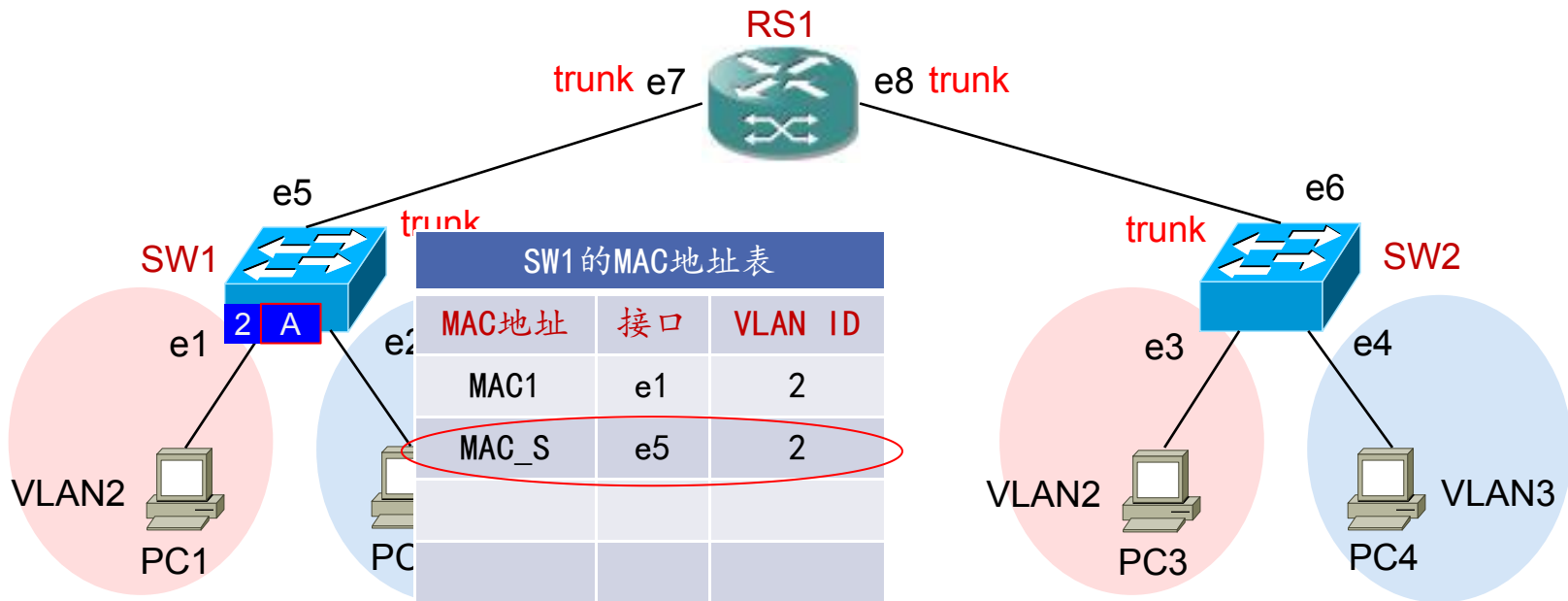
三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址—— (5) SW1的处理——接收并转发至e1接口

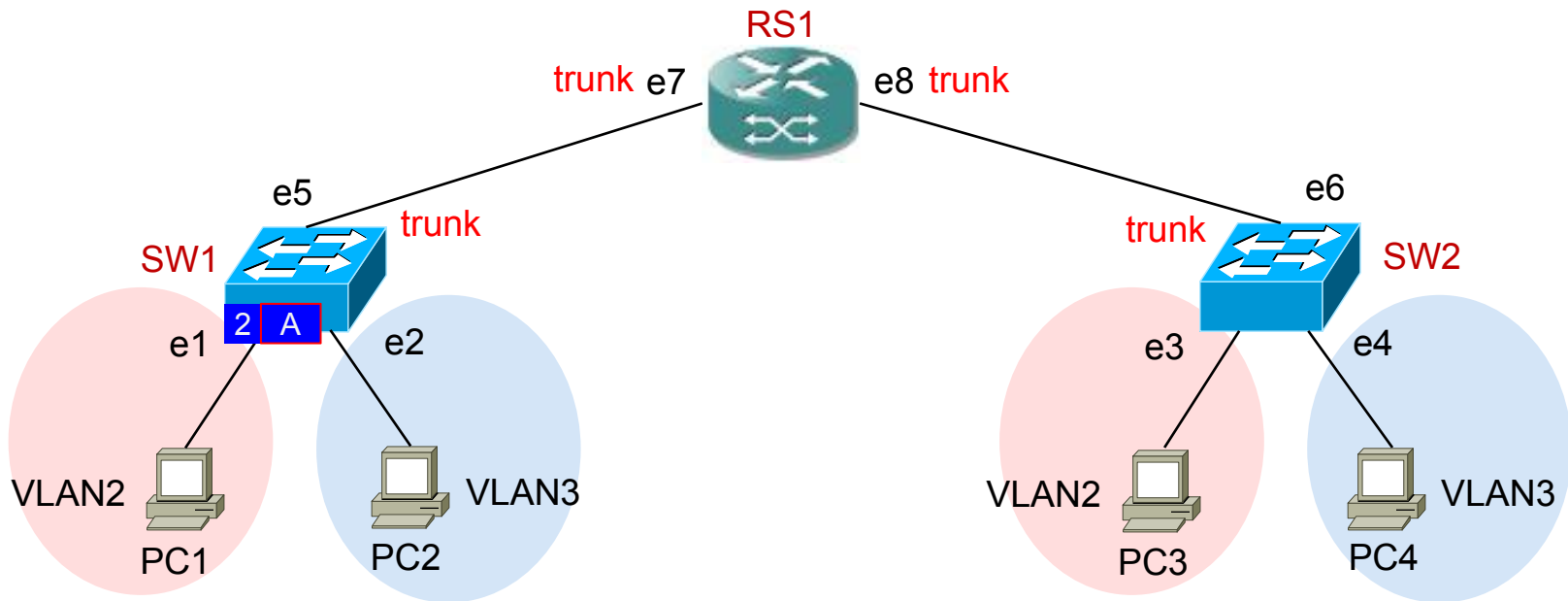
SW1的e5接口收到ARP响应报文，由于e5是trunk口，所以不去掉帧头中的VLAN2标签。SW1查看自己的MAC地址表，发现目的MAC地址对应的是e1接口，于是转发至e1接口。

三层交换机组网实例分析—— PC1访问PC2 (Ping)



1. PC1获取默认网关的MAC地址——（5）SW1的处理——在MAC地址表中添加记录
SW1在自己的MAC地址表中添加默认网关的相关记录。

三层交换机组网实例分析—— PC1访问PC2 (Ping)

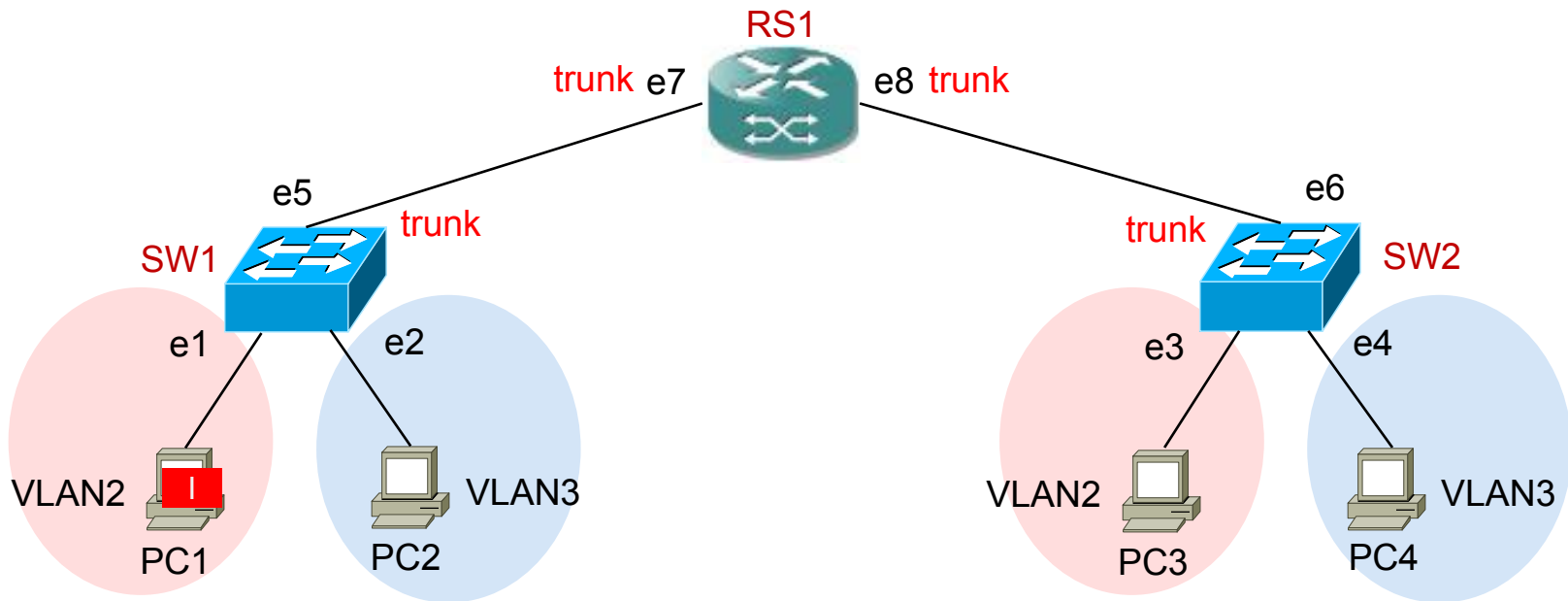


1. PC1获取默认网关的MAC地址——（5）SW1的处理——从e1接口发出至PC1

由于e1是access接口，所以去掉帧头中的VLAN2标签，然后将普通帧（ARP响应报文）发送至目的主机PC1。

至此，PC1获得了默认网关（即RS1上VLAN2的SVI接口）的MAC地址。

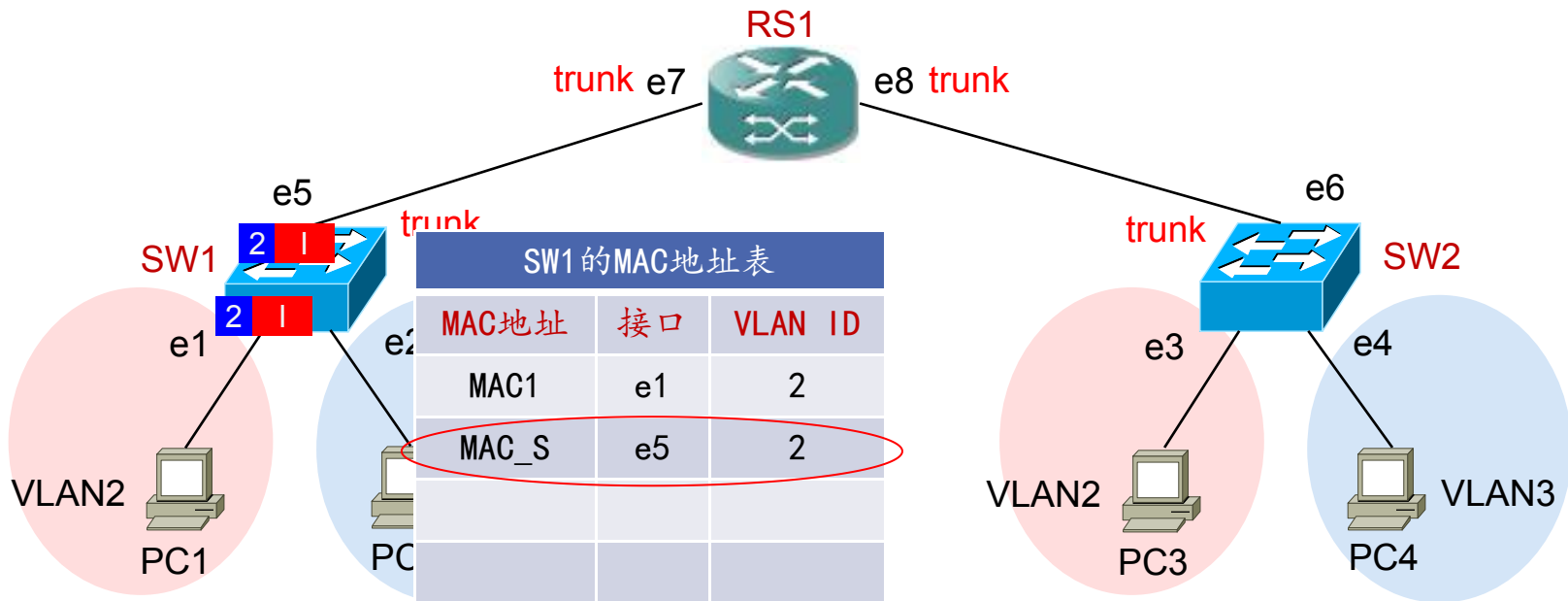
三层交换机组网实例分析—— PC1访问PC2 (Ping)



2. PC1发送ICMP请求报文至RS1—— (1) PC1封装ICMP请求报文

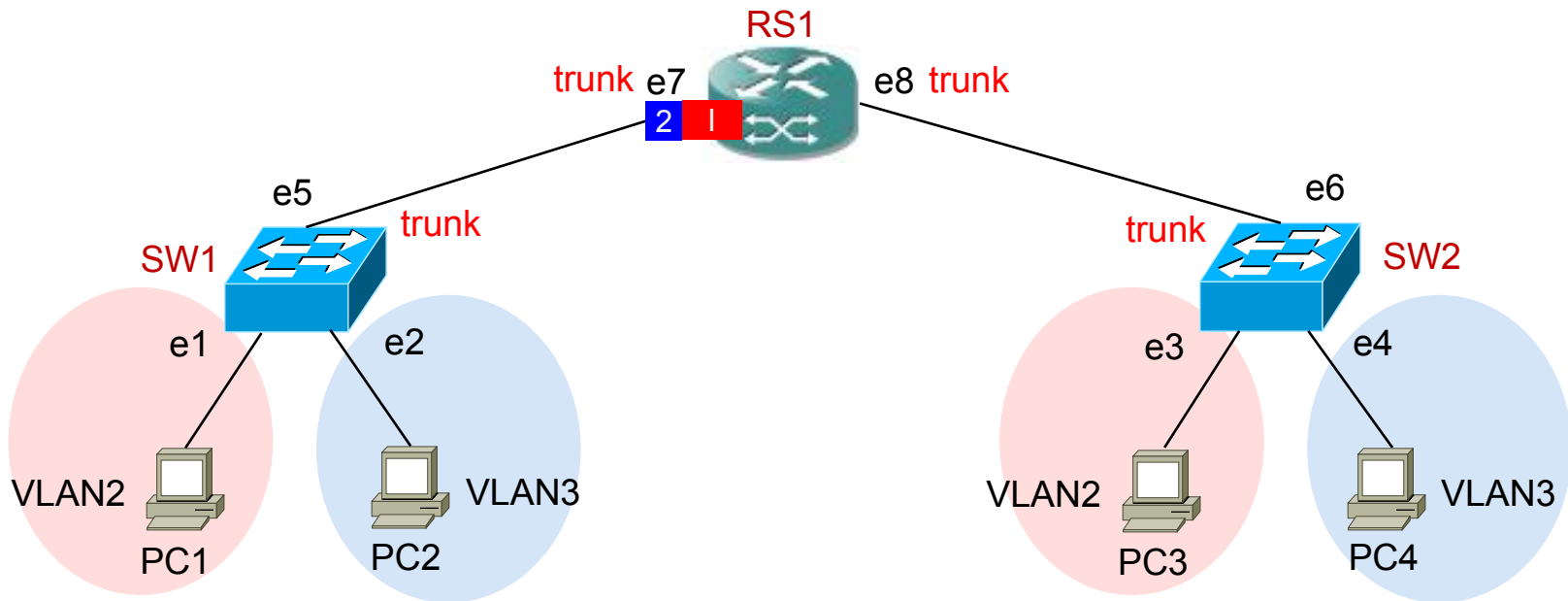
PC1发出ICMP请求报文，由于目的IP与自己不在同一网段，所以要先发给默认网关。于是在封装报文时，源MAC是MAC1，目的MAC是MAC_S。源IP是IP1，目的IP是PC2。报文先到达交换机SW1。

三层交换机组网实例分析—— PC1访问PC2 (Ping)



2. PC1发送ICMP请求报文至RS1—— (2) SW1处理报文——加标签、转发
- SW1的e1接口收到报文，由于e1接口的PVID=2，所以添加VLAN2的标签；
查找MAC地址表，发现目的MAC对应e5接口，于是转发至e5接口；
由于e5是trunk接口，所以保留VLAN2标签，发送出去。

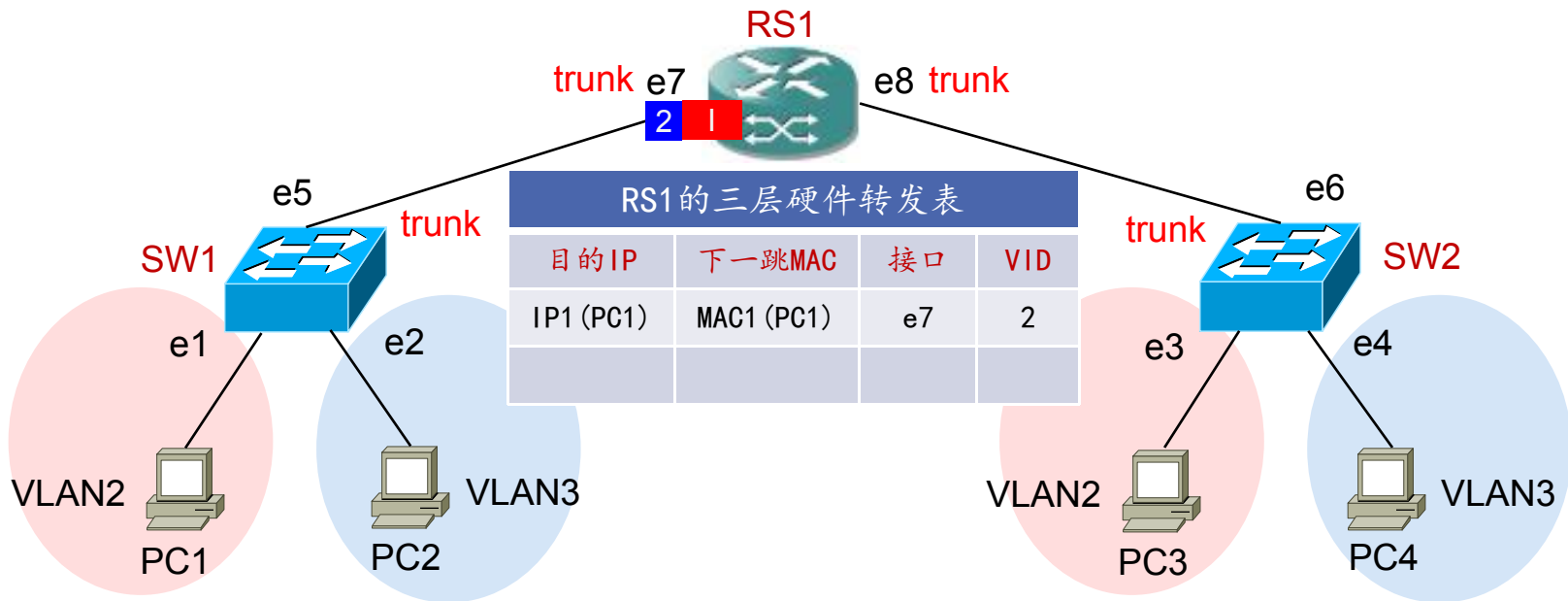
三层交换机组网实例分析—— PC1访问PC2 (Ping)



3. RS1处理ICMP请求报文——（1）RS1接收报文

RS1的e7接口收到报文，由于e7是trunk接口，所以保留标签接收；
由于该报文中目的MAC是RS1的三层虚拟接口（即VLAN2的SVI接口），且目的IP与源IP不在同一网段，所以直接提交三层硬件转发表。

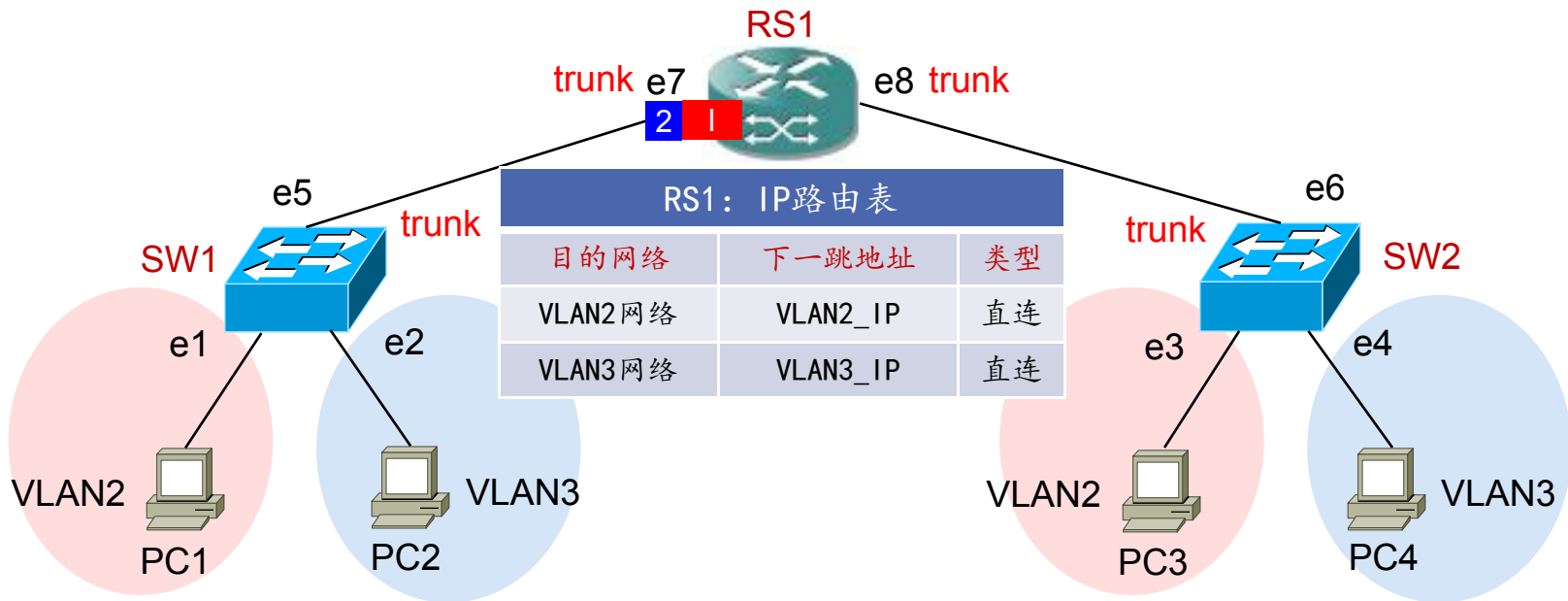
三层交换机组网实例分析—— PC1访问PC2 (Ping)



3. RS1处理ICMP请求报文——（2）查看三层硬件转发表

RS1查看自己的三层硬件转发表，此时表中没有PC2的记录信息；

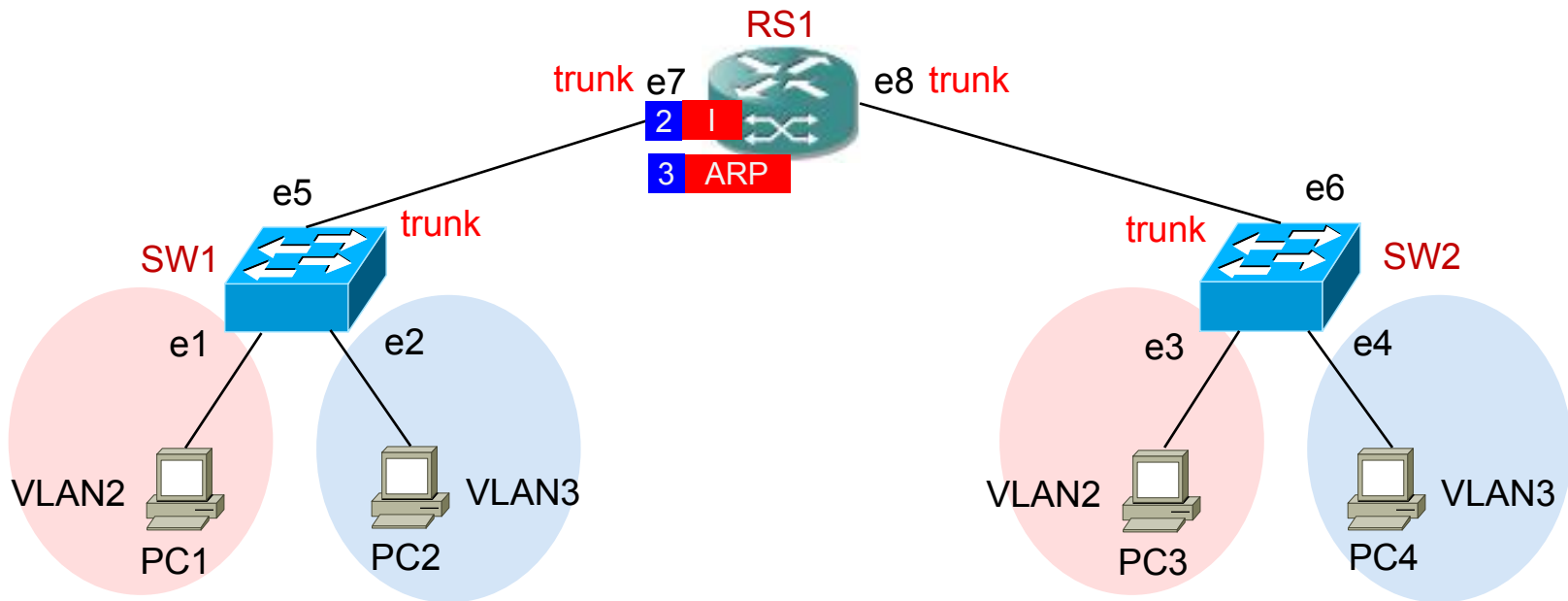
三层交换机组网实例分析—— PC1访问PC2 (Ping)



3. RS1处理ICMP请求报文——（3）查看IP路由表（软件路由）

由于三层硬件转发表中没有PC2的对应表项，于是CPU会根据数据包中的目的IP地址（IP2），进一步查看IP路由表（软件路由表），发现匹配了一个直连网段（即VLAN3网络），其下一跳是VLAN3的SVI接口IP地址（VLAN3_IP）。于是，CPU依据直连路由，将数据包转给VLAN3的SVI接口。

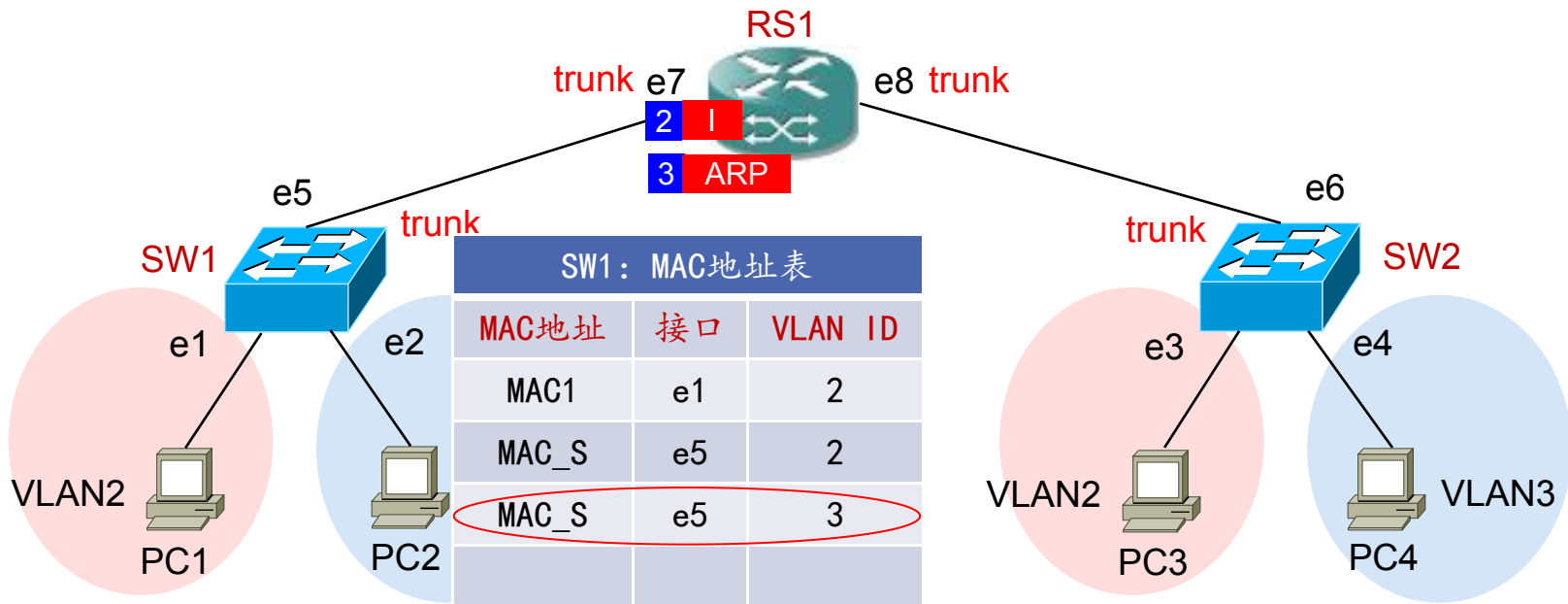
三层交换机组网实例分析—— PC1访问PC2 (Ping)



3. RS1处理ICMP请求报文——（4）获取PC2的MAC地址——封装ARP请求报文

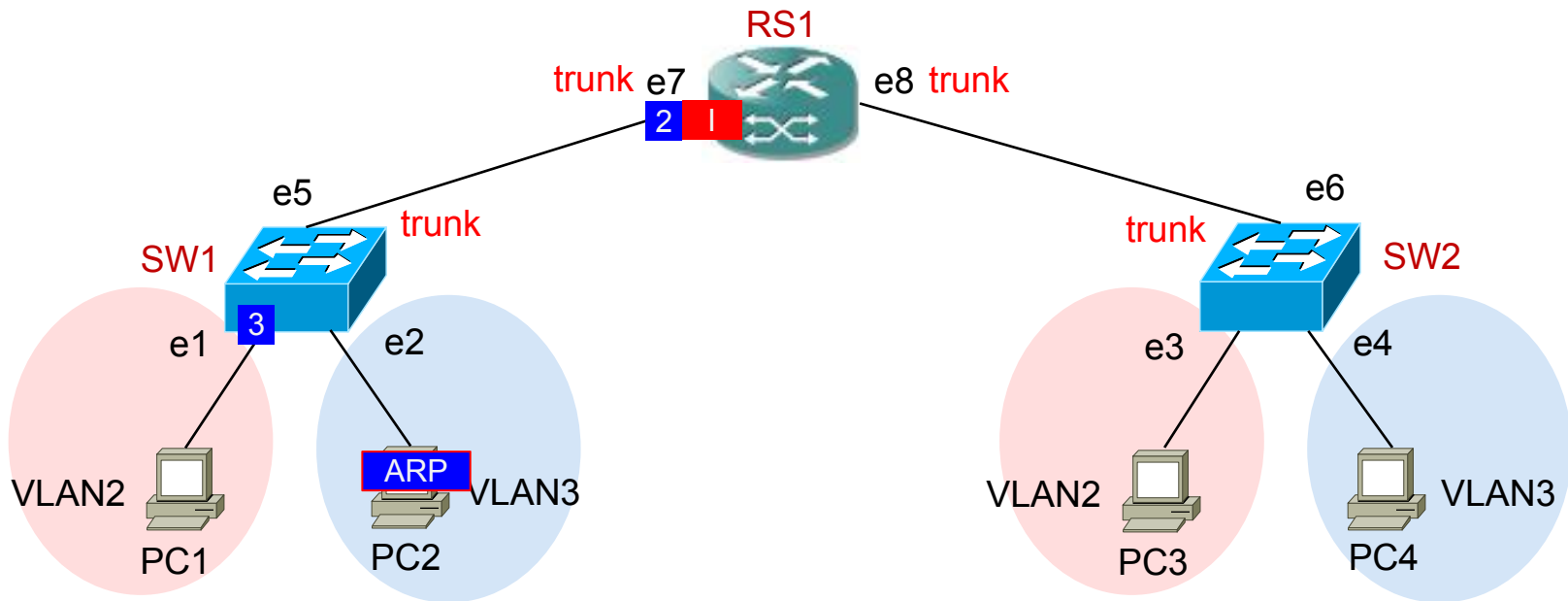
接下来VLAN3的SVI接口要将ICMP请求报文直接发给PC2，但它发现目前还不知道PC2的MAC地址。于是发出ARP请求，报文中源MAC是MAC_S，目的MAC是全1，请求的目的IP地址是IP2。注意，此处封装报文时，可看成是VLAN3的SVI接口封装报文，因此要在帧头中添加VLAN3的标签，且从e7发出时不去掉标签。

三层交换机组网实例分析—— PC1访问PC2 (Ping)



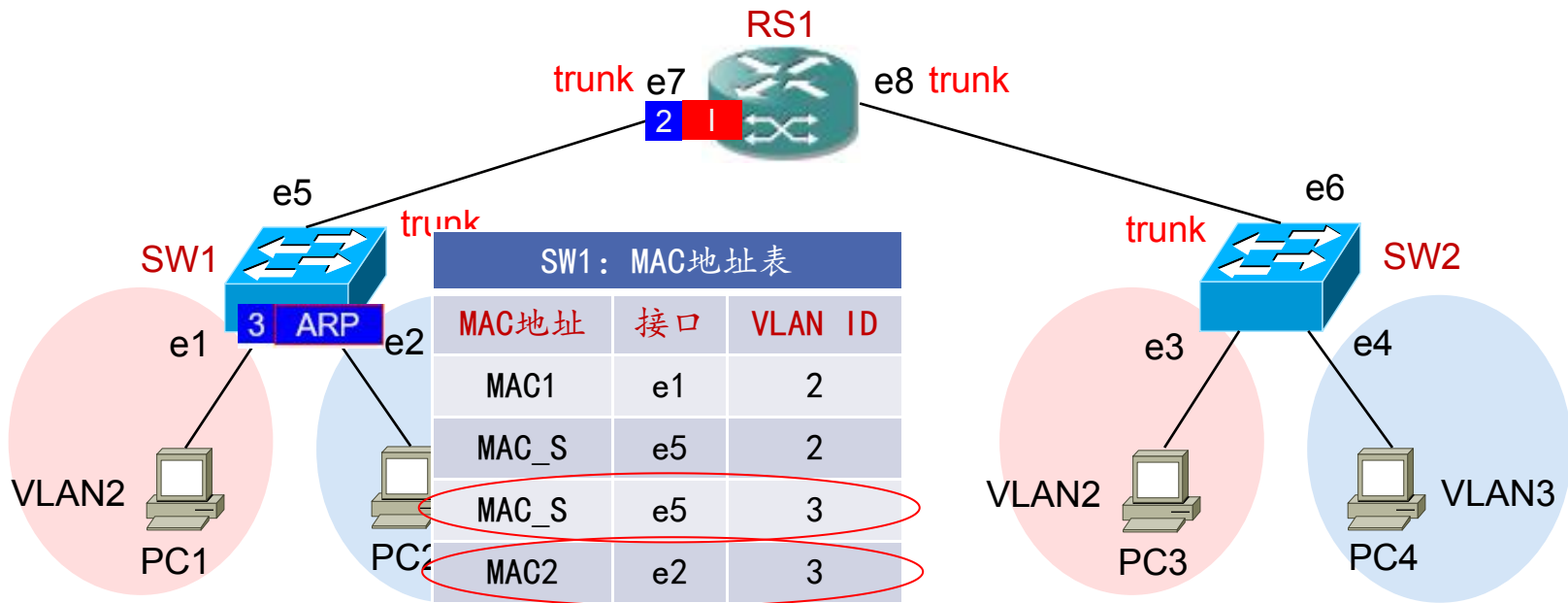
3. RS1处理ICMP请求报文—— (4) 获取PC2的MAC地址——SW1转发ARP请求报文
- ARP请求报文到达e5，e5是trunk接口，所以接收报文并保留标签；
 SW1将报文转发至所有属于VLAN3的接口（来源接口除外），包括e2接口；
 SW1在MAC地址表中添加VLAN3的SVI接口的记录；
 由于e2是access接口，所以从e2发出时，去掉VLAN3标签，然后到达PC2。

三层交换机组网实例分析—— PC1访问PC2 (Ping)



3. RS1处理ICMP请求报文——（4）获取PC2的MAC地址——PC2返回ARP响应报文
PC2返回ARP响应报文，报文中源MAC是MAC2，目的MAC是MAC_S；
响应报文到达e2，因为e2属于VLAN3，所以添加VLAN3标签；

三层交换机组网实例分析—— PC1访问PC2 (Ping)



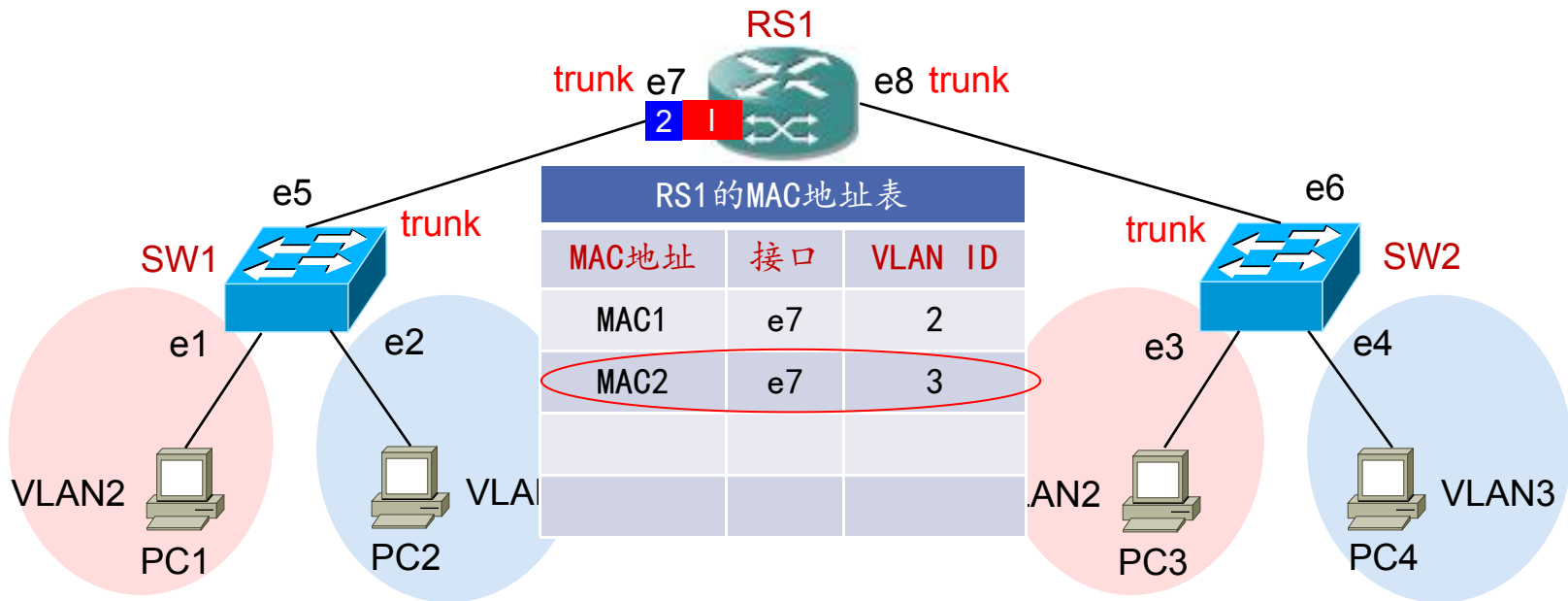
3. RS1处理ICMP请求报文——（4）获取PC2的MAC地址——SW1转发ARP响应报文

SW1在MAC地址表中，添加PC2的记录；

依据MAC地址表，将报文转发至e5接口；

由于e5是trunk接口，所以保留VLAN3标签发送至RS1。

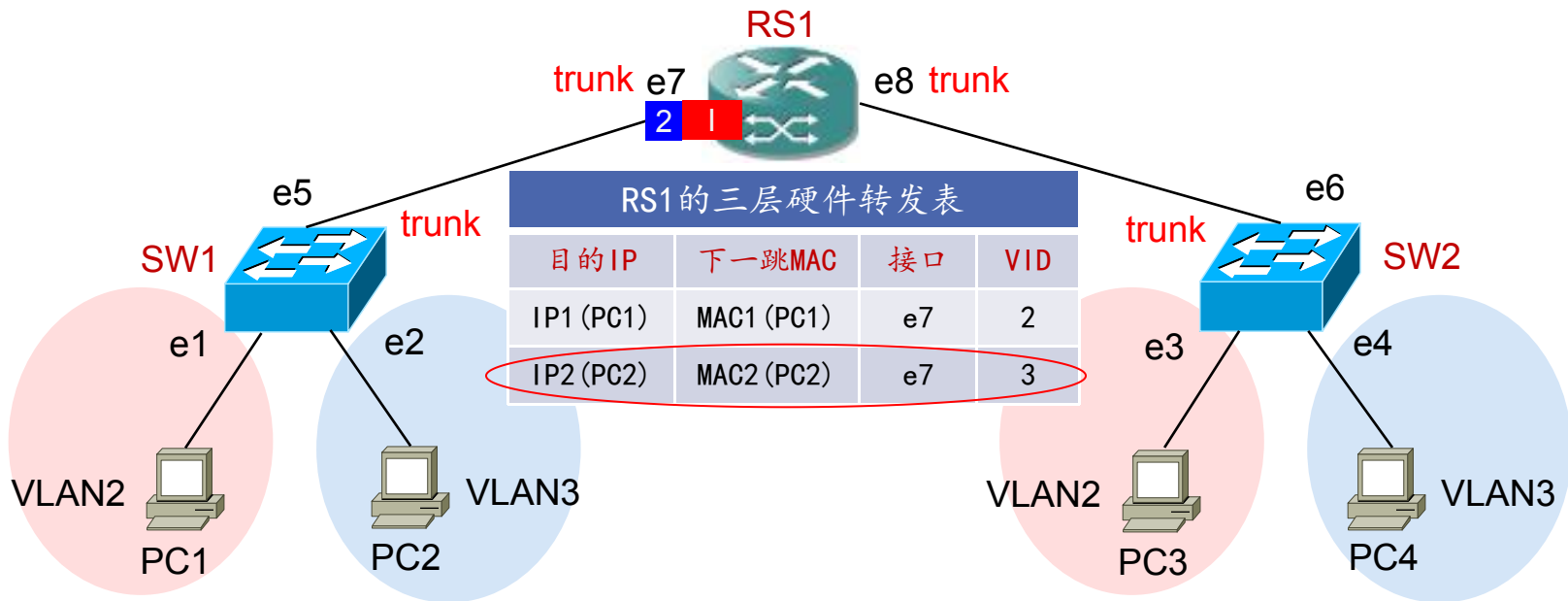
三层交换机组网实例分析—— PC1访问PC2 (Ping)



3. RS1处理ICMP请求报文—— (5) RS1在MAC地址表中添加记录

RS1的e7接口收到PC2发来的ARP响应报文（保留VLAN3标签），获取到PC2的MAC地址，于是在自己的MAC地址表中，添加PC2的相关记录。

三层交换机组网实例分析—— PC1访问PC2 (Ping)

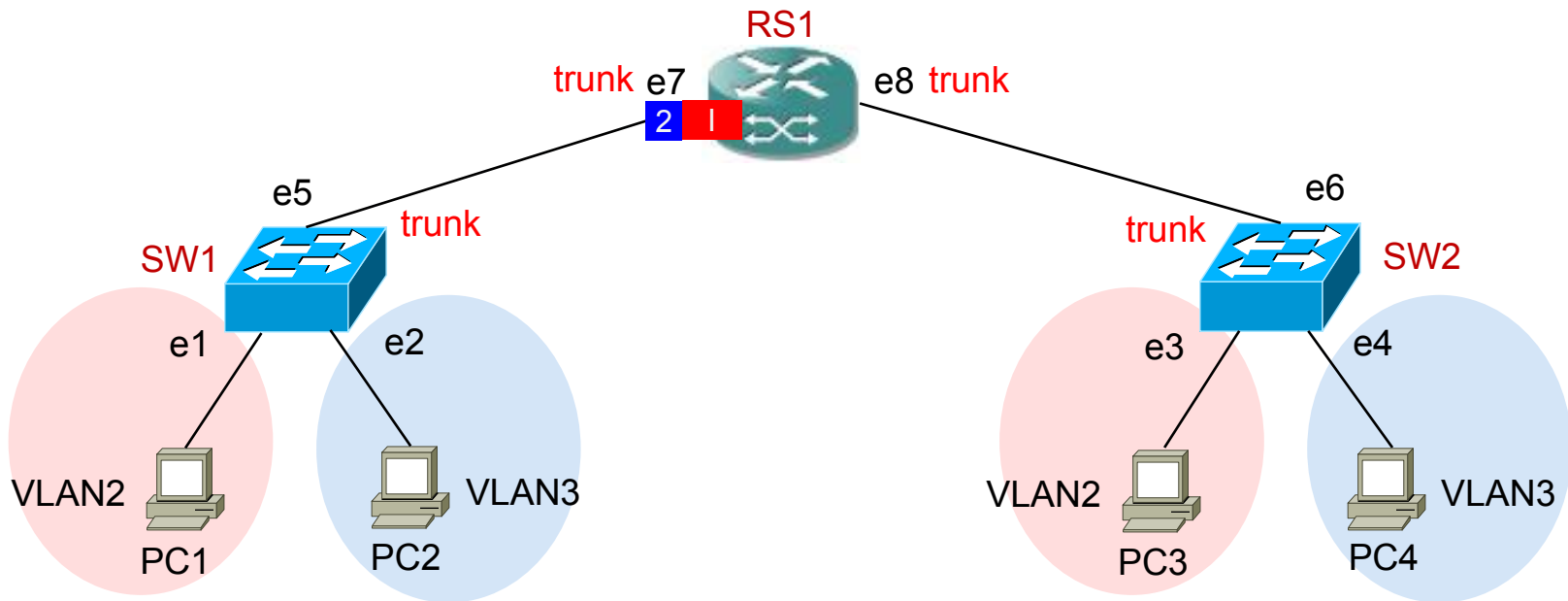


3. RS1处理ICMP请求报文——（6）RS1在三层硬件转发表中添加记录

RS1分析ARP响应报文的内容，获取到PC2的相关信息，然后在自己的三层硬件转发表中，添加PC2的相关记录。

以后其他网段主机与PC2通信时，RS1的ASIC芯片会直接把包从本表指定的接口（即e7）转发出去（硬件转发），不必再查看IP路由表（软件路由）。

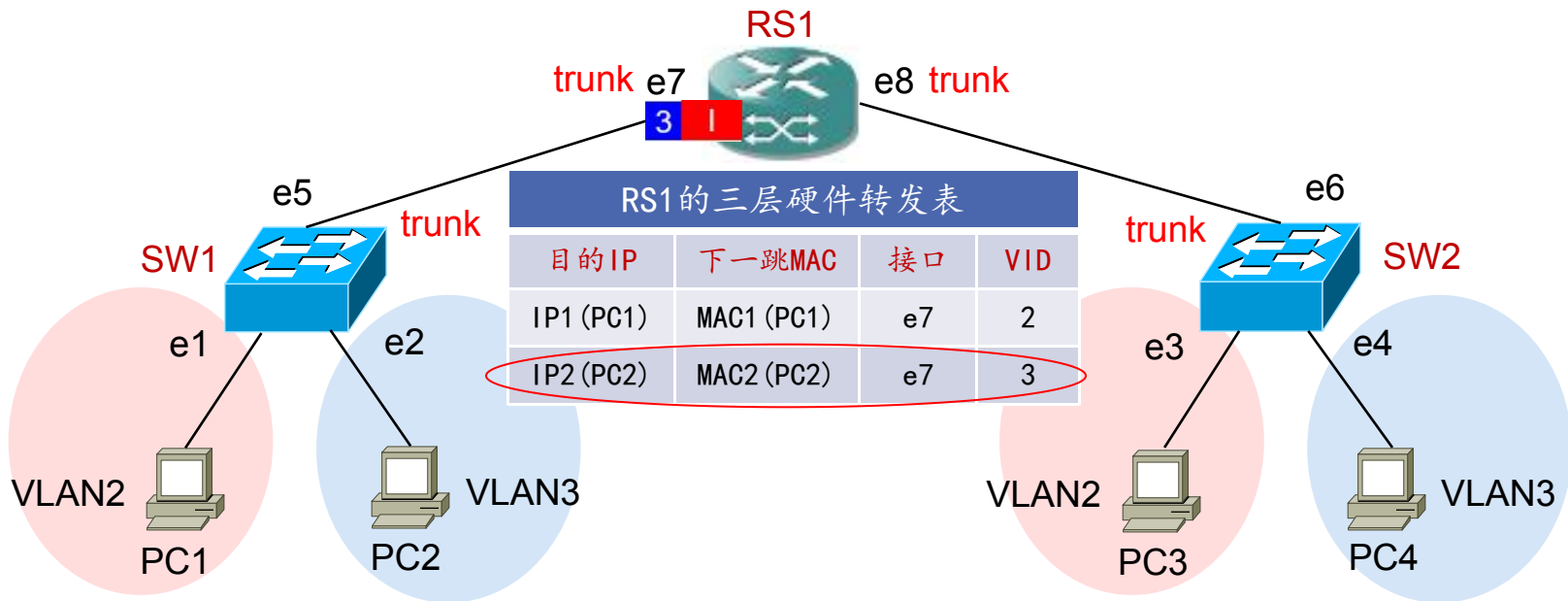
三层交换机组网实例分析—— PC1访问PC2 (Ping)



3. RS1处理ICMP请求报文——（7）RS1重新封装ICMP请求报文

此时，RS1已经知道PC2的MAC地址，于是将PC1发来的ICMP请求报文（此时已经通过直连路由转发至VLAN3的SVI接口）重新封装，在封装时，源IP（IP1）和目的IP（IP2）保持不变，MAC2为目的MAC，将VLAN3的SVI接口的MAC（即MAC_S）作为源MAC地址。

三层交换机组网实例分析—— PC1访问PC2 (Ping)

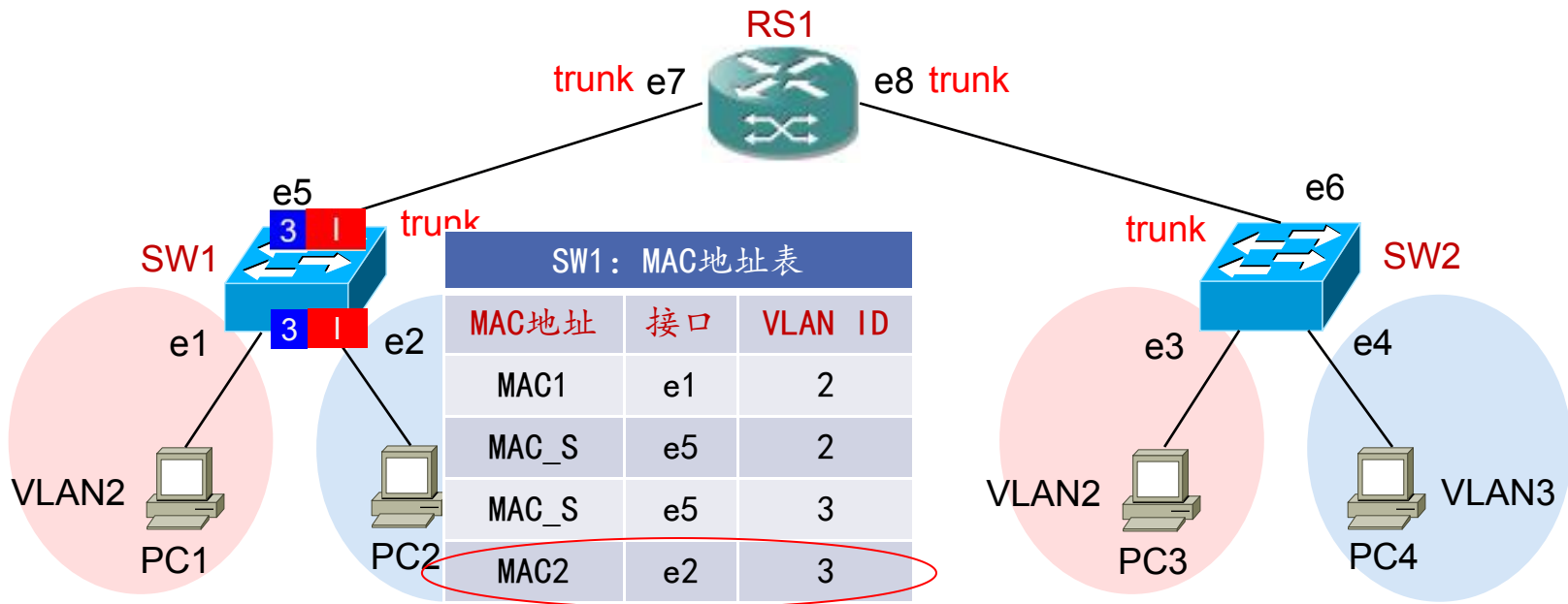


3. RS1处理ICMP请求报文—— (7) RS1重新封装ICMP请求报文

RS1根据自己的三层硬件转发表，把ICMP请求报文从e7接口转发出去，并且在报文的帧头添加VLAN3的标签。

由于e7接口是Trunk接口，所以会保留VLAN3标签然后发出，到达SW1。

三层交换机组网实例分析——PC1访问PC2 (Ping)



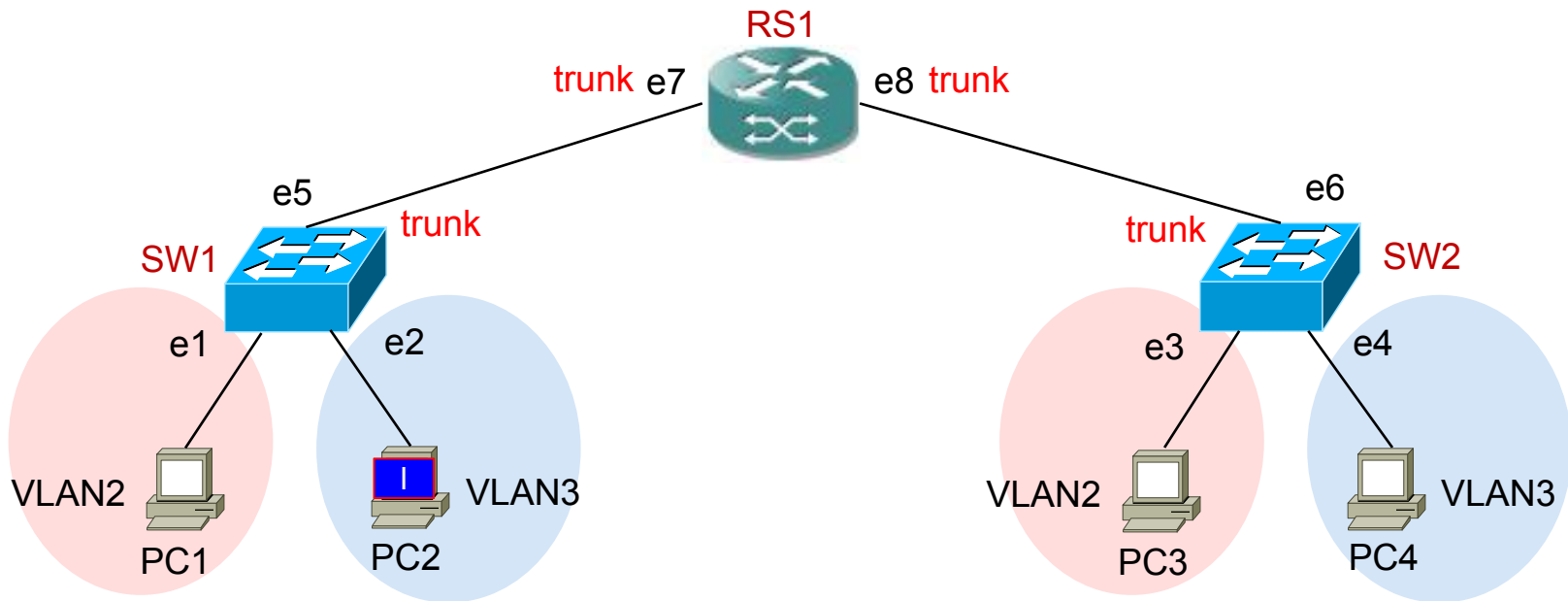
4. SW1处理ICMP请求报文

SW1的e5接口收到ICMP请求报文，由于e5是trunk接口，所以接收报文并保留VLAN3标签。

SW1依据自己的MAC地址表，将ICMP请求报文转发至e2接口。

由于e2接口是access接口，所以会去掉VLAN3标签然后发出，最终到达PC2。

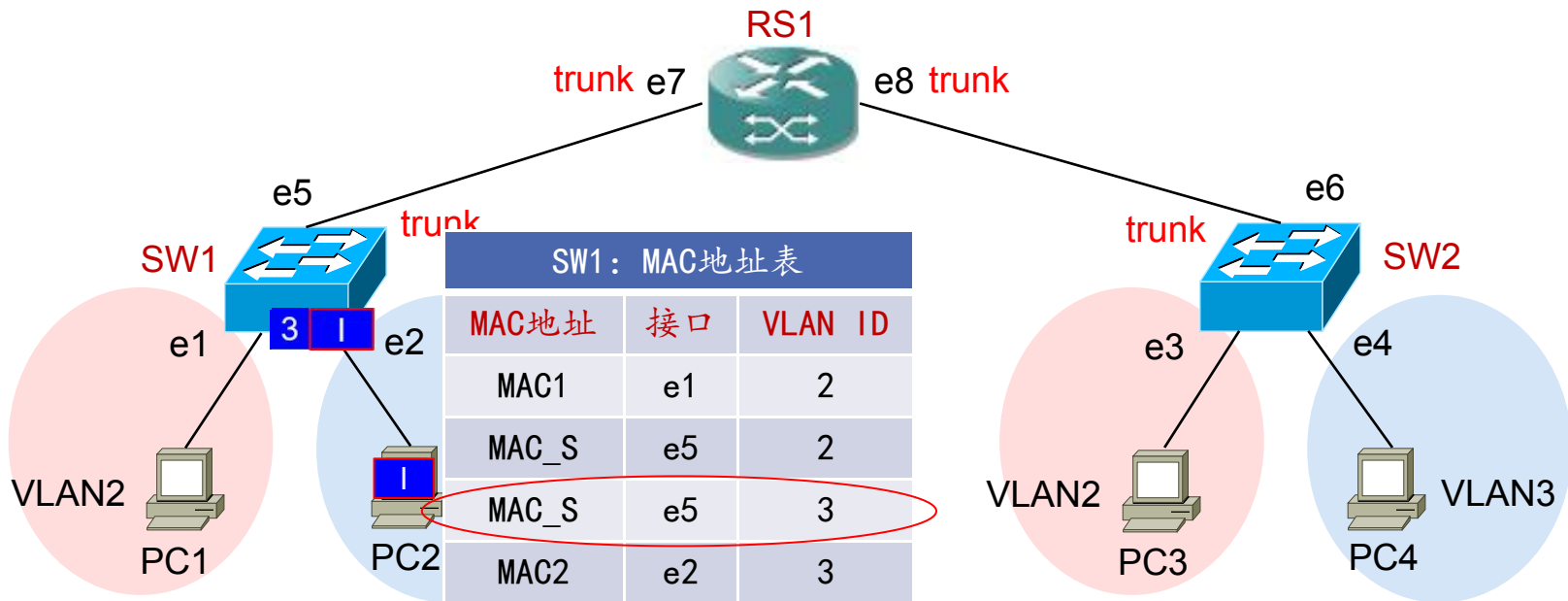
三层交换机组网实例分析—— PC1访问PC2 (Ping)



5. PC2返回ICMP响应报文

PC2收到PC1发来的ICMP请求报文，要向PC1发回ICMP响应报文；
由于目的IP与源IP不在同一网段，所以PC2先将响应报文发给默认网关；
PC2封装ICMP响应报文，该报文的源IP为IP2，目的IP为IP1，源MAC为MAC2，目的MAC为MAC_S。注意，此时PC2已经知道默认网关的MAC地址是MAC_S。

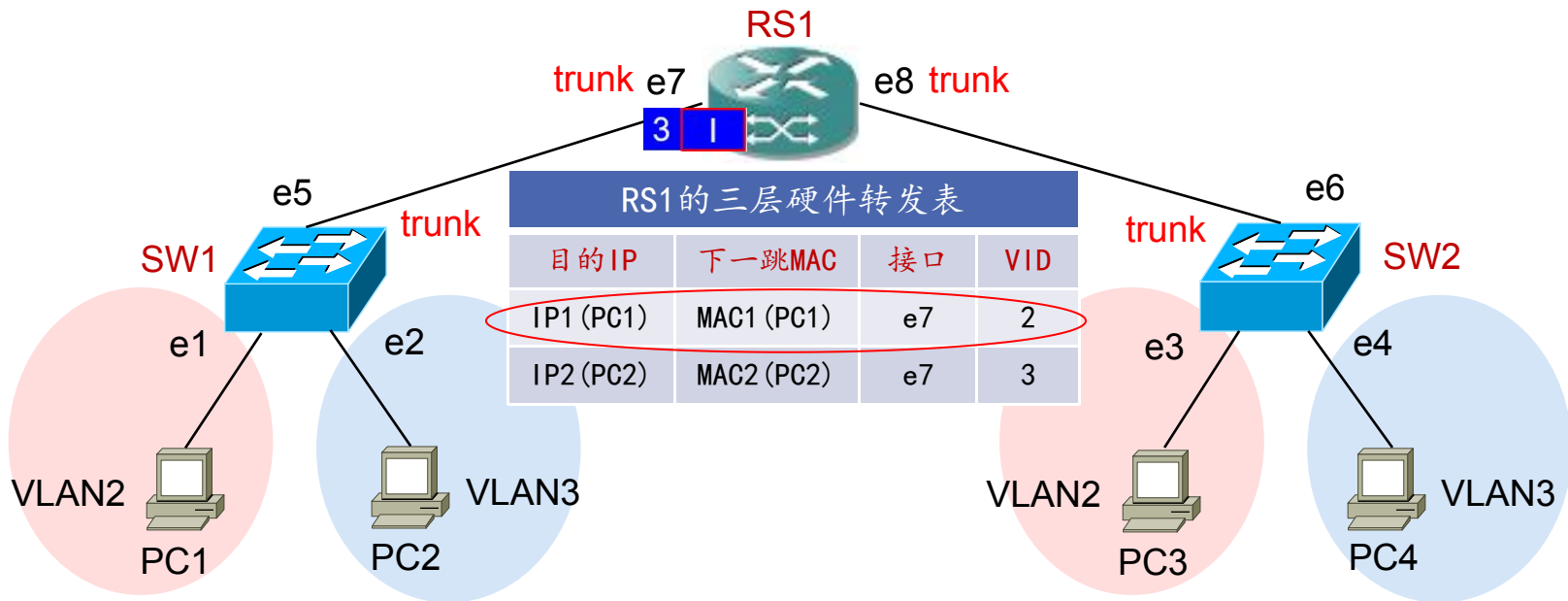
三层交换机组网实例分析—— PC1访问PC2 (Ping)



6. SW1转发ICMP响应报文

ICMP响应报文发送到SW1的e2接口，被加上VLAN3的标签；
 SW1依据MAC地址表，将ICMP响应报文转发至e5接口；
 由于e5接口是trunk接口，所以保留VLAN3标签，发出ICMP响应报文；

三层交换机组网实例分析—— PC1访问PC2 (Ping)

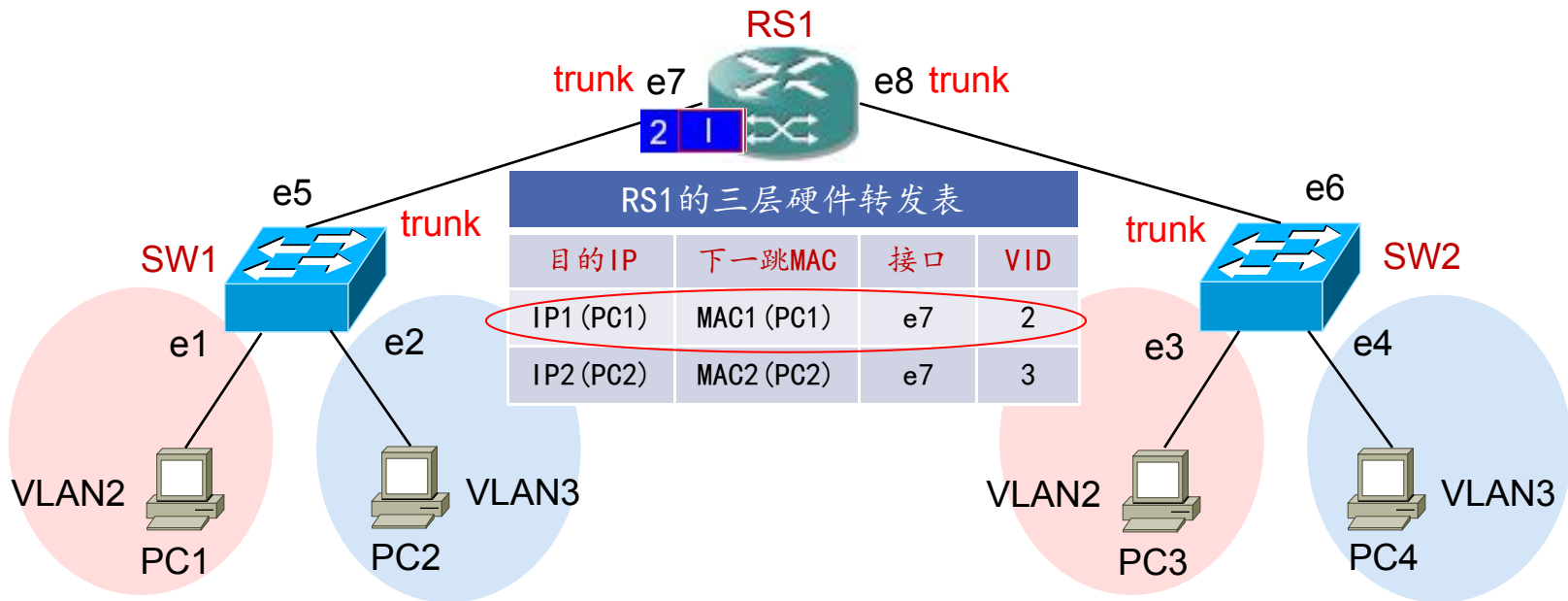


7. RS1转发ICMP响应报文——（1）查看三层硬件转发表

RS1收到ICMP响应报文，发现报文中源IP地址与目的IP地址不在同一网段，首先在三层硬件转发表中查看。

三层硬件转发表中有PC1的记录，于是RS1直接进行转发（硬件转发）；

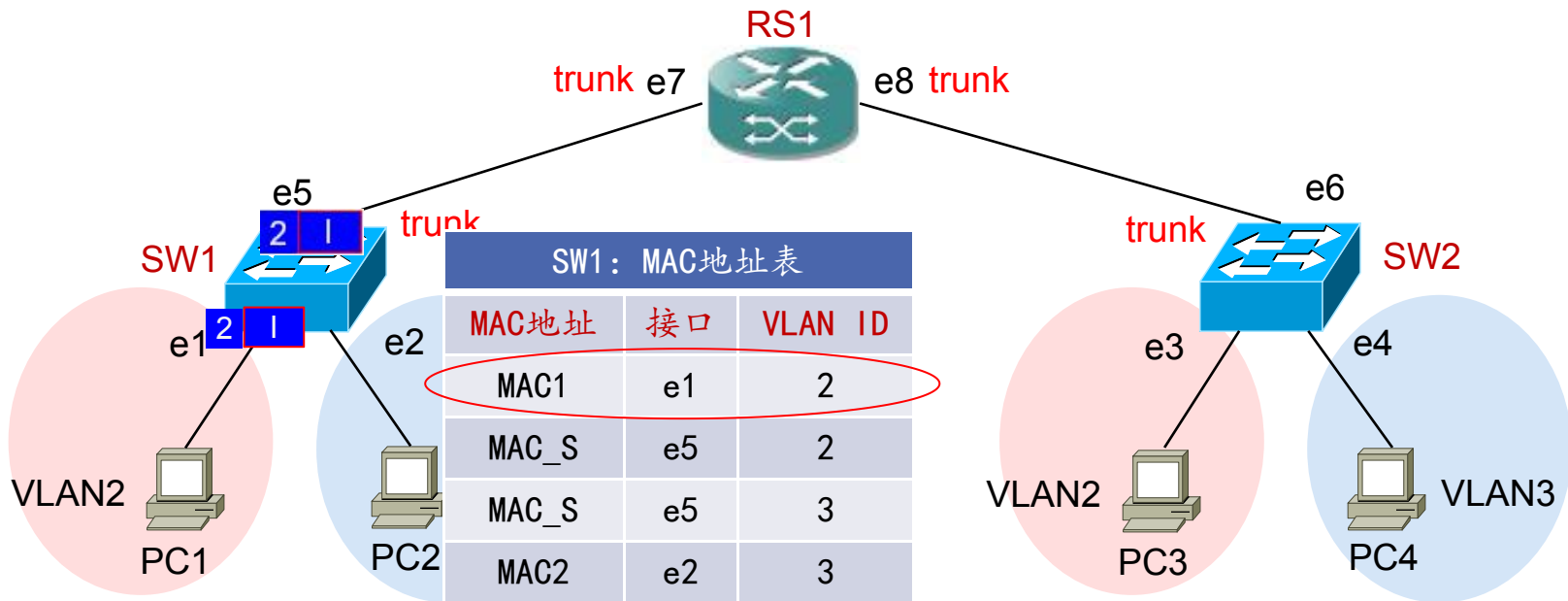
三层交换机组网实例分析—— PC1访问PC2 (Ping)



7. RS1转发ICMP响应报文——（2）重新封装ICMP响应报文

RS1根据在三层硬件转发表中的查找结果，重新封装ICMP响应报文；
目的IP（IP1）和源IP（IP2）保持不变，目的MAC为MAC1，源MAC为MAC_S；
在数据链路层，报文被添加上VLAN2的标签；
从e7接口发出，由于e7是trunk接口，所以保留VLAN2标签；

三层交换机组网实例分析—— PC1访问PC2 (Ping)

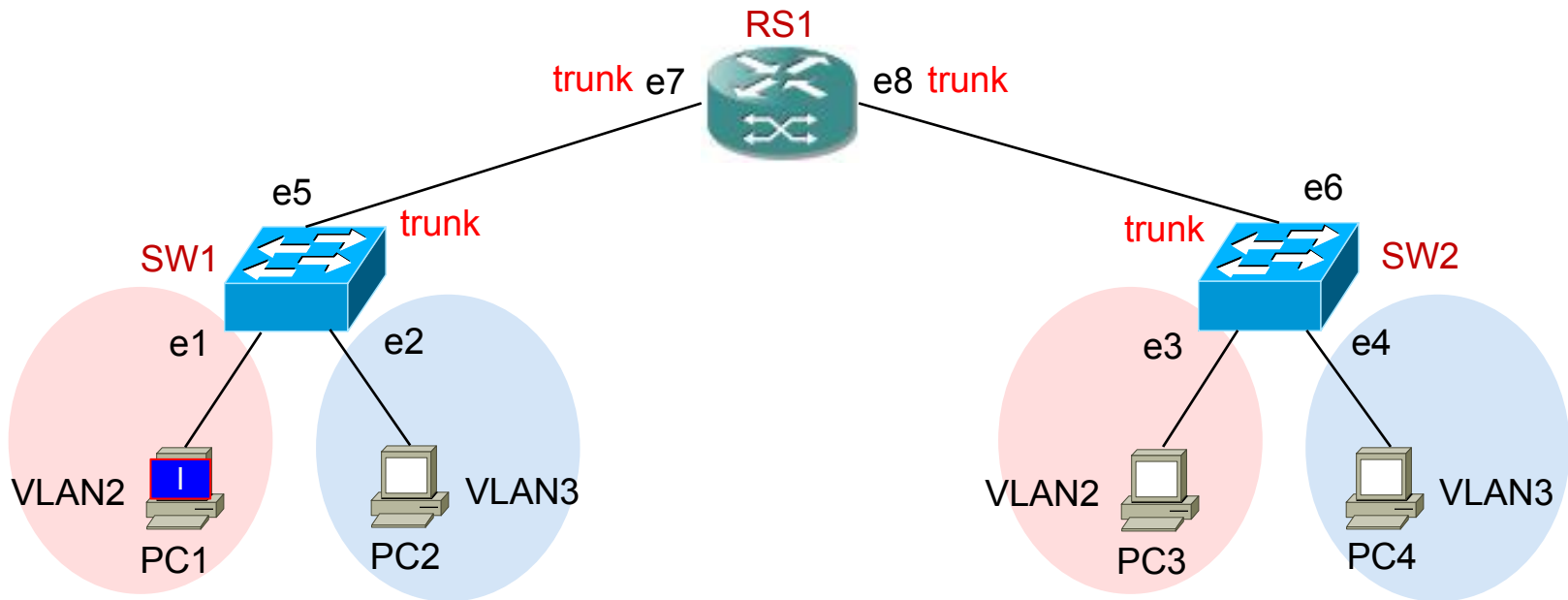


8. SW1转发ICMP响应报文

SW1收到ICMP响应报文，依据自己的MAC地址表，将报文转发至e1接口。

由于e1接口是access类型，所以去掉VLAN2标签后，将ICMP响应报文发送出去，最终到达PC1。

三层交换机组网实例分析—— PC1访问PC2 (Ping)

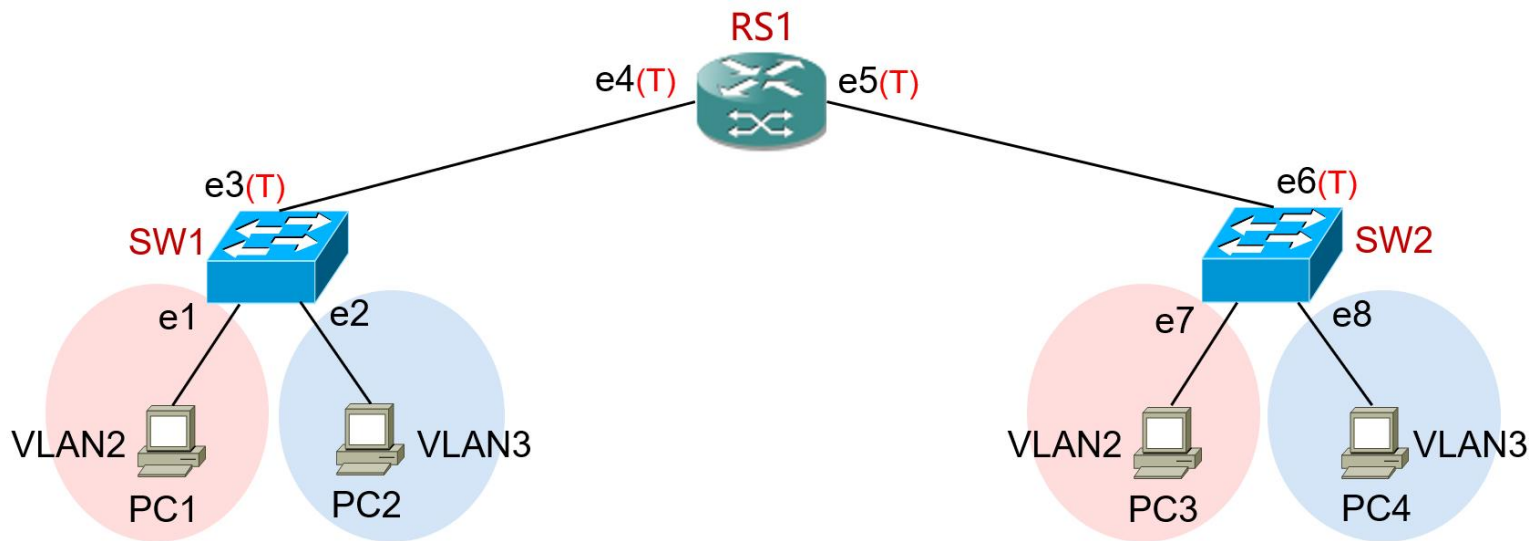


PC1访问PC2 (Ping)

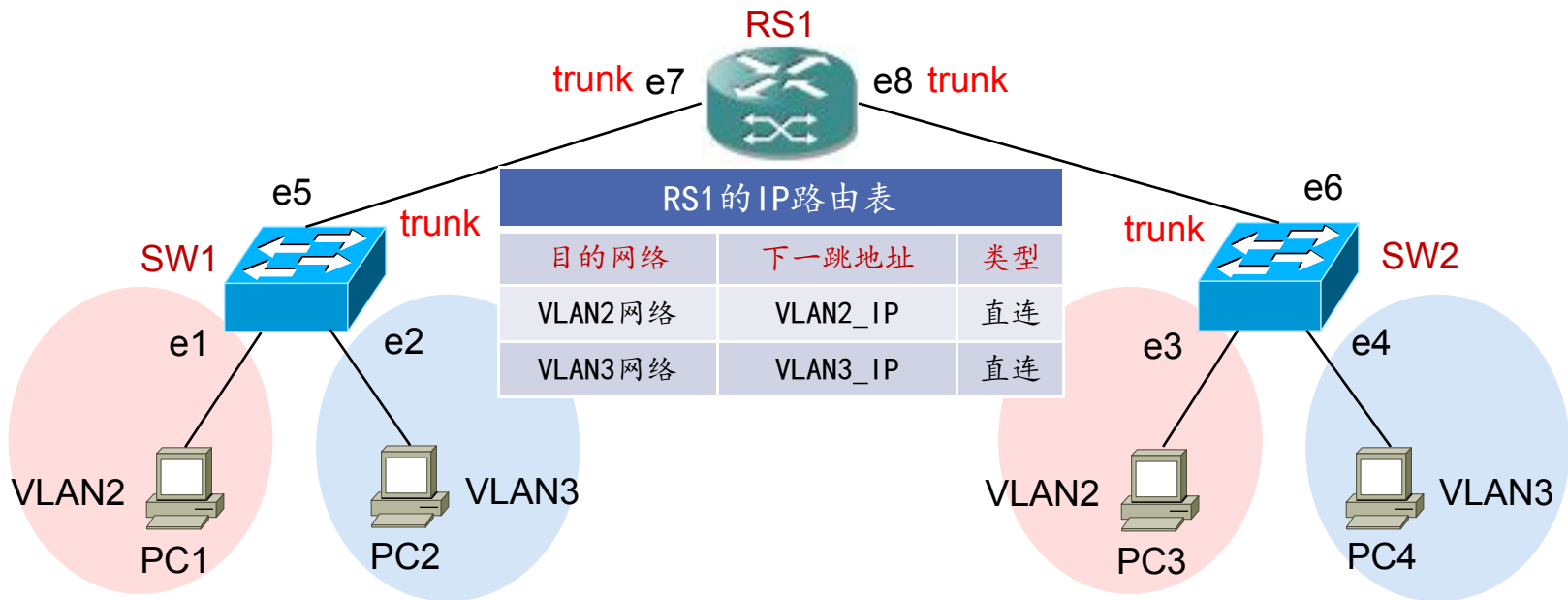
通信完毕

分析3：同一VLAN主机之间的通信

PC1 ping PC3 （自主）



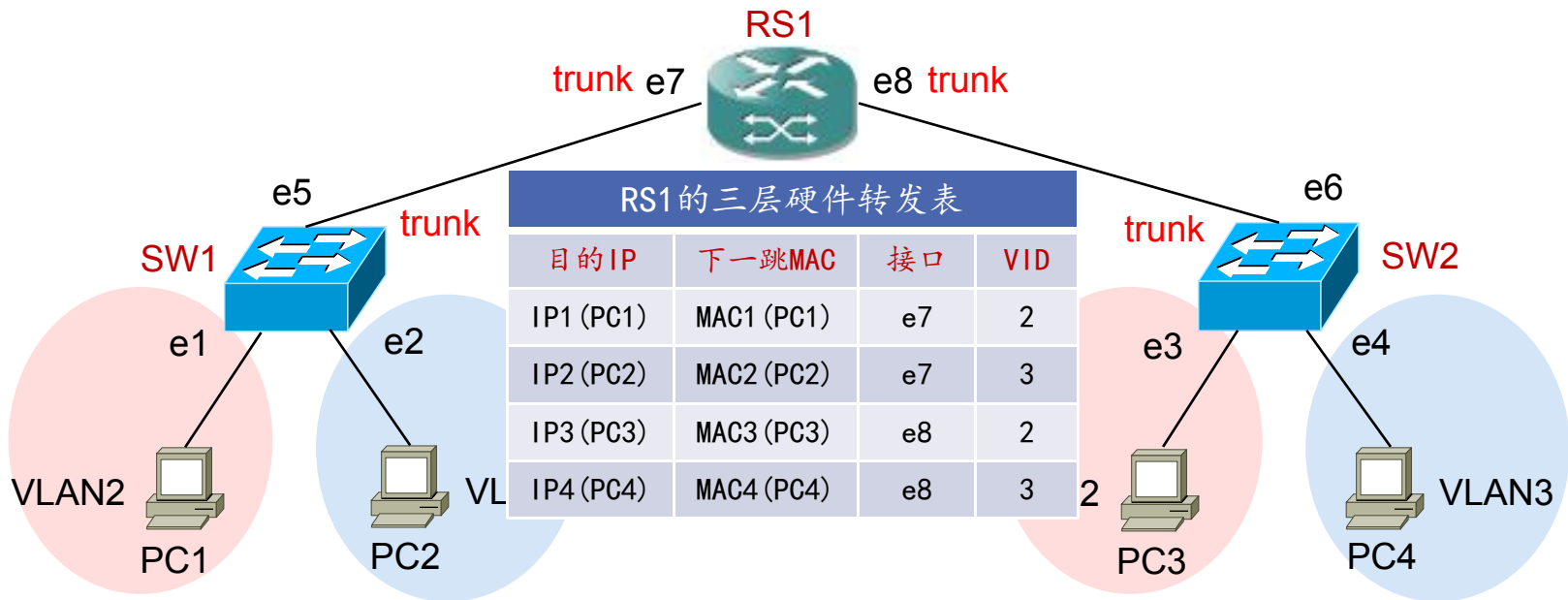
三层交换机组网实例分析——PC1访问PC2 (Ping)



假设1:

三层交换机RS1的IP路由表（软件路由）中，已经具有到达VLAN2网络和VLAN3的直连路由

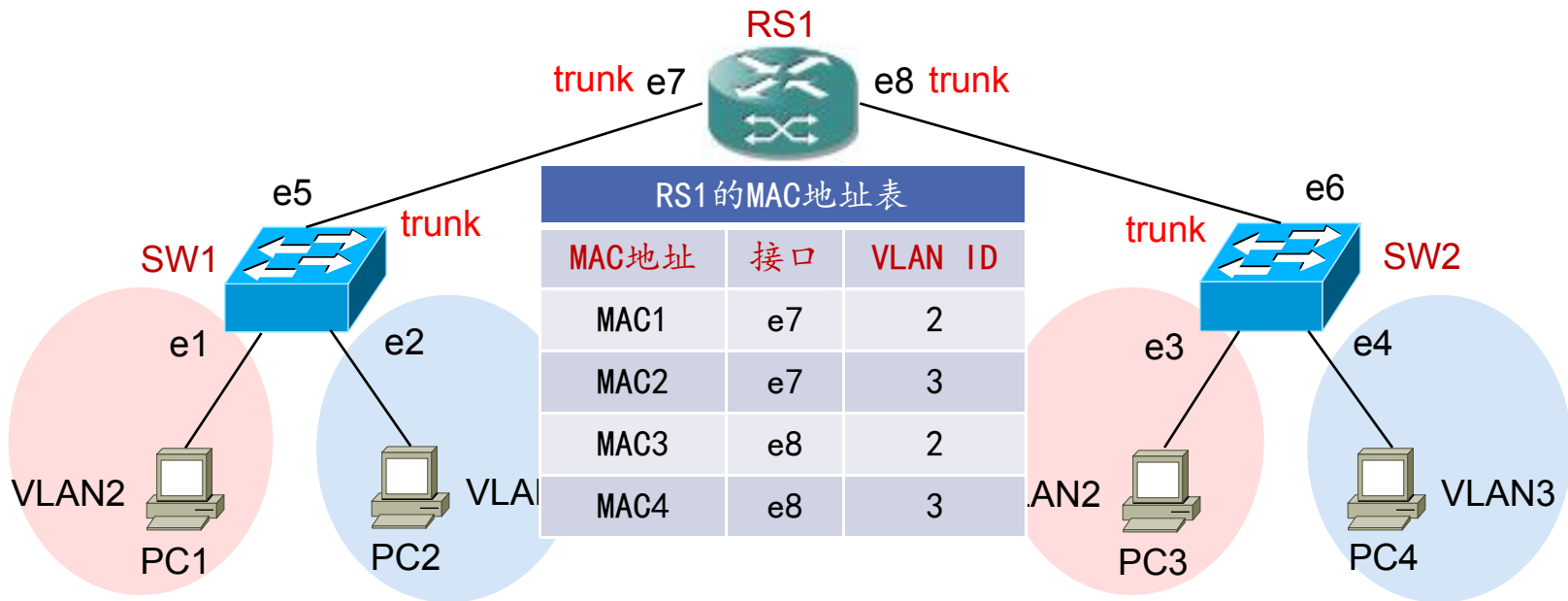
三层交换机组网实例分析—— PC1访问PC2 (Ping)



假设2:

三层交换机RS1的三层硬件转发表中, 已经具有PC1、PC2、PC3、PC4的记录

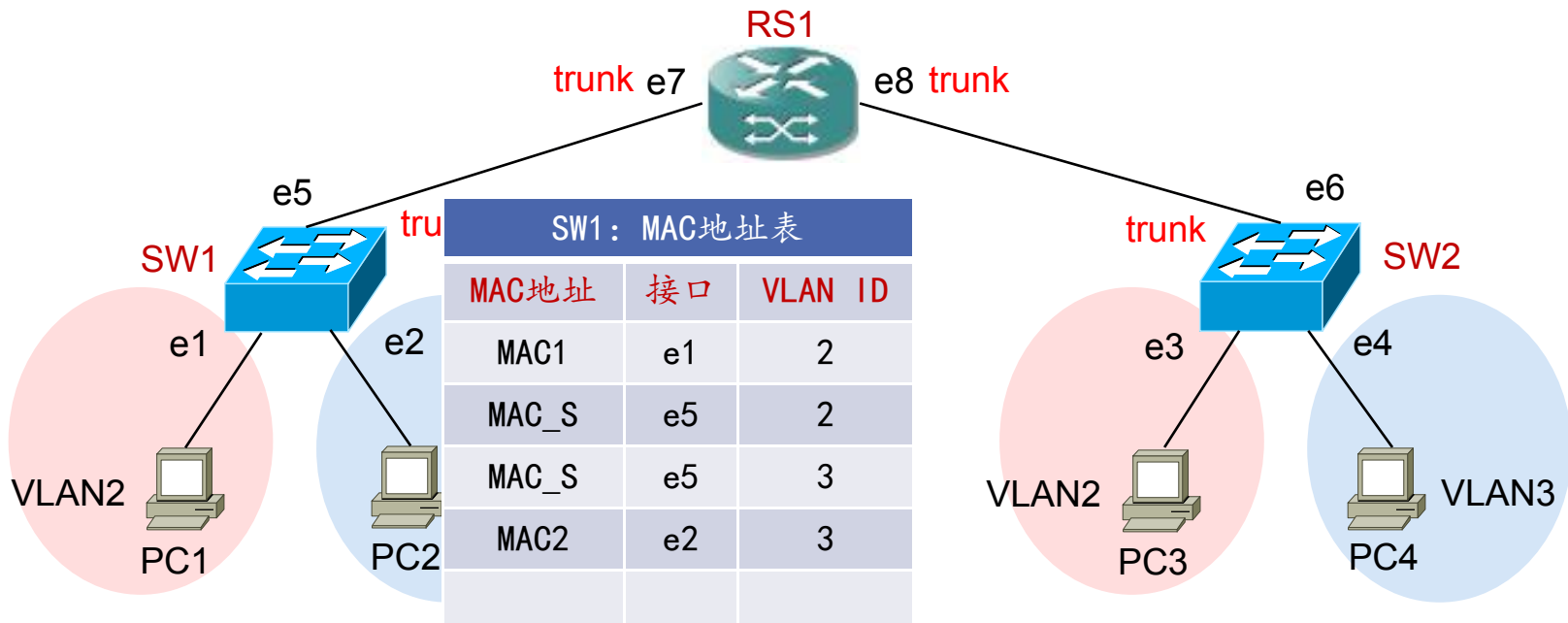
三层交换机组网实例分析——PC1访问PC2 (Ping)



假设3:

三层交换机RS1的MAC地址表中, 已经具有PC1、PC2、PC3、PC4的记录

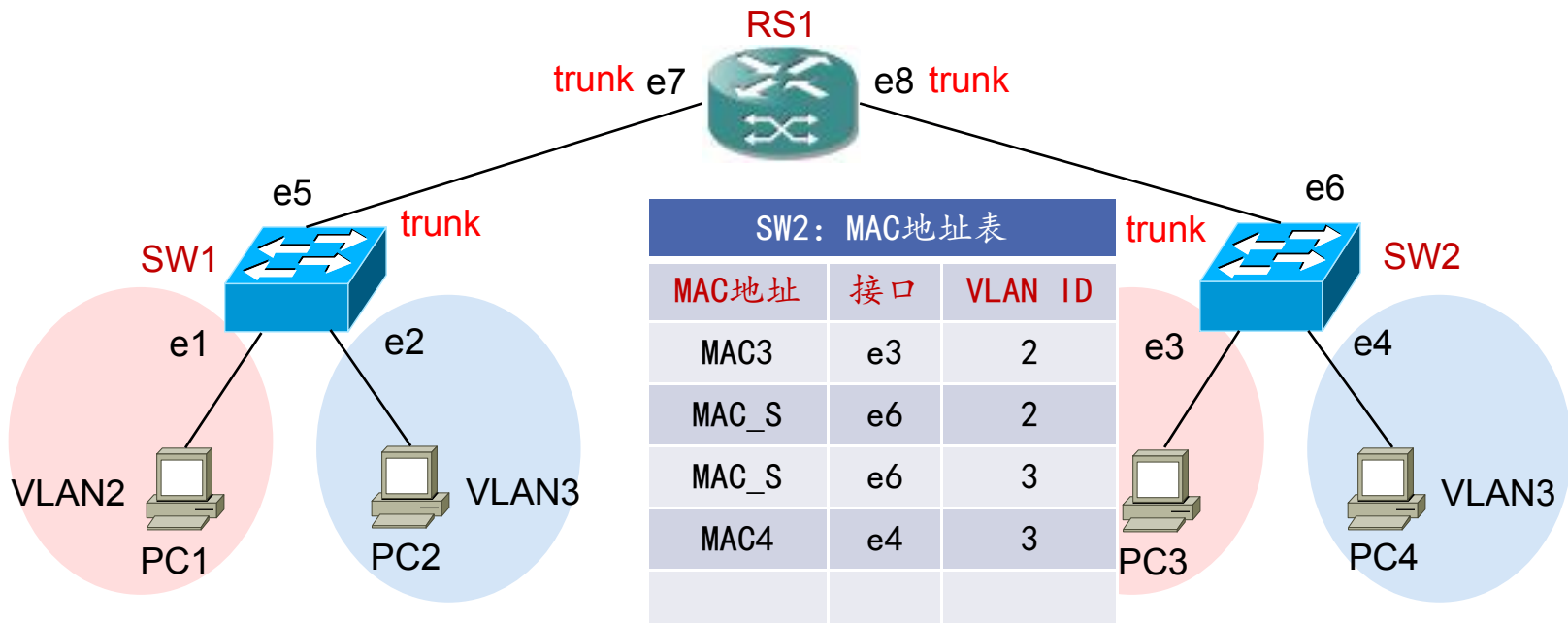
三层交换机组网实例分析——PC1访问PC3 (Ping)



假设4:

SW1的MAC地址表中, 已经具有PC1、PC2、VLAN2的SVI接口、VLAN3的SVI接口的记录。

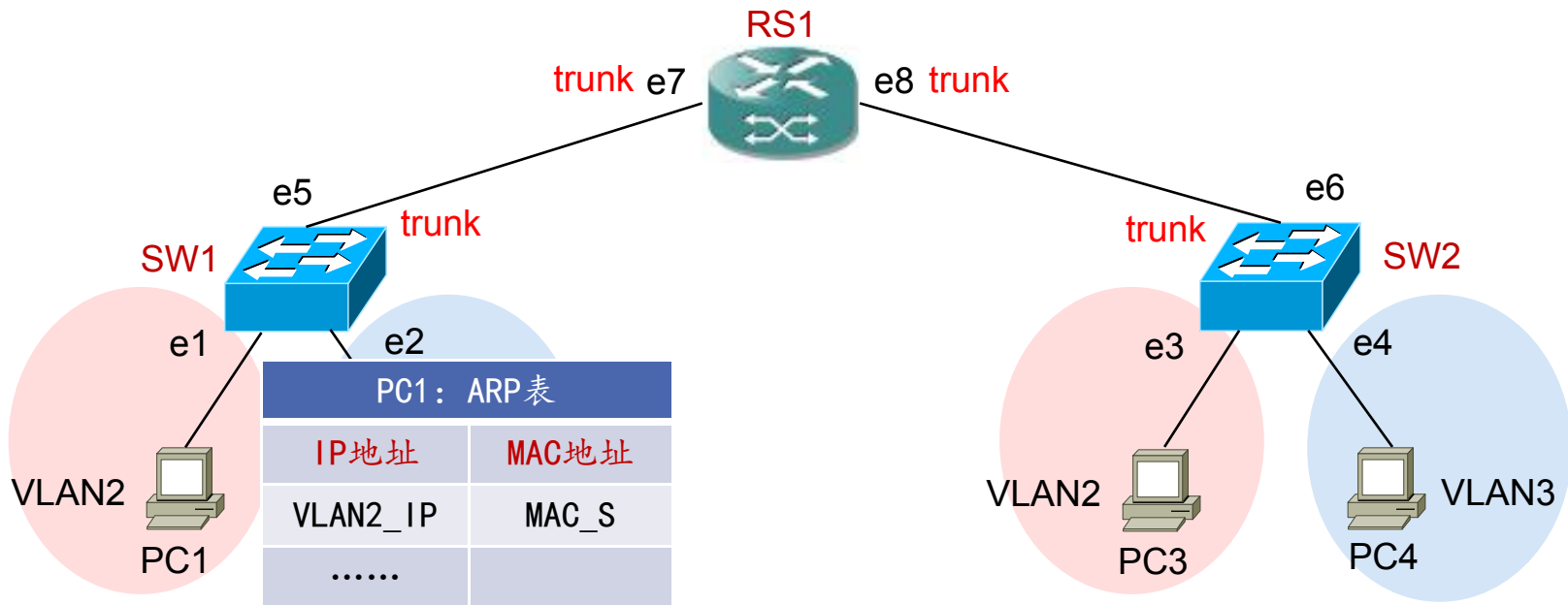
三层交换机组网实例分析——PC1访问PC3 (Ping)



假设5:

SW2的MAC地址表中, 已经具有PC3、PC4、VLAN2的SVI接口、VLAN3的SVI接口的记录。

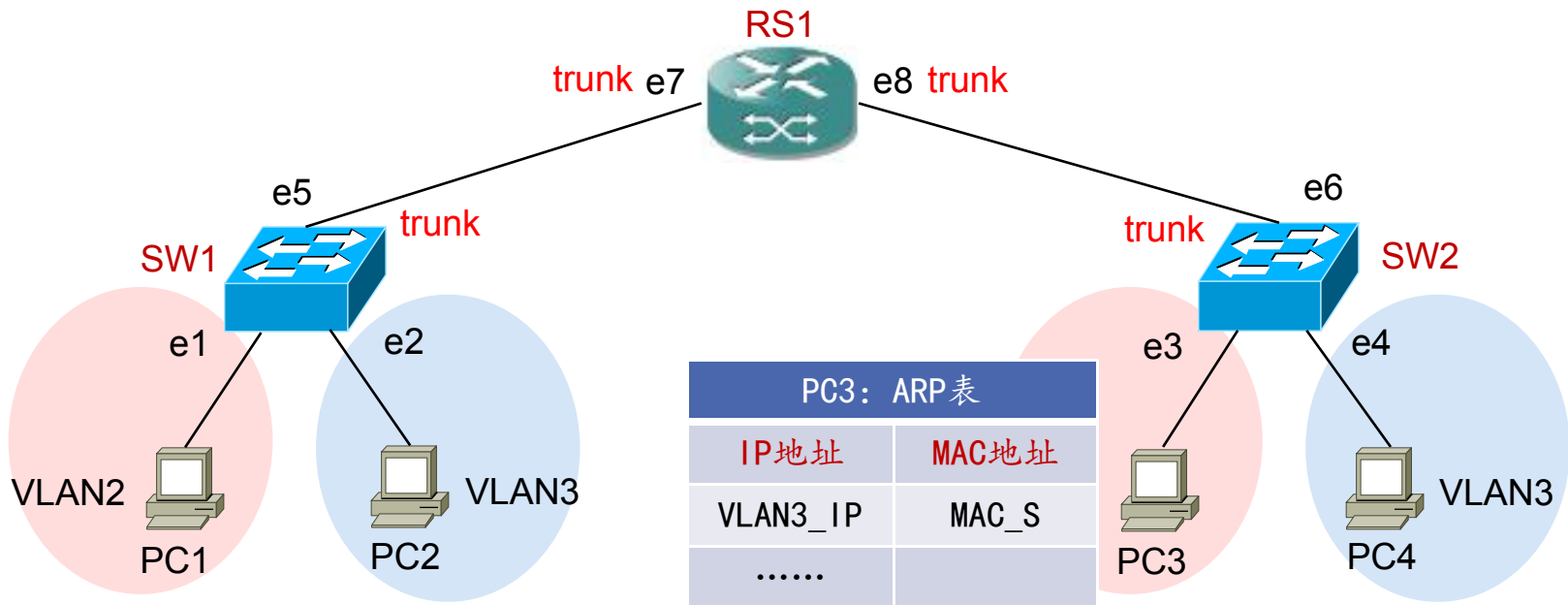
三层交换机组网实例分析—— PC1访问PC3 (Ping)



假设6:

PC1已经知道自己默认网关的MAC地址 (即MAC_S);
注意, 该记录在PC1的ARP表中。

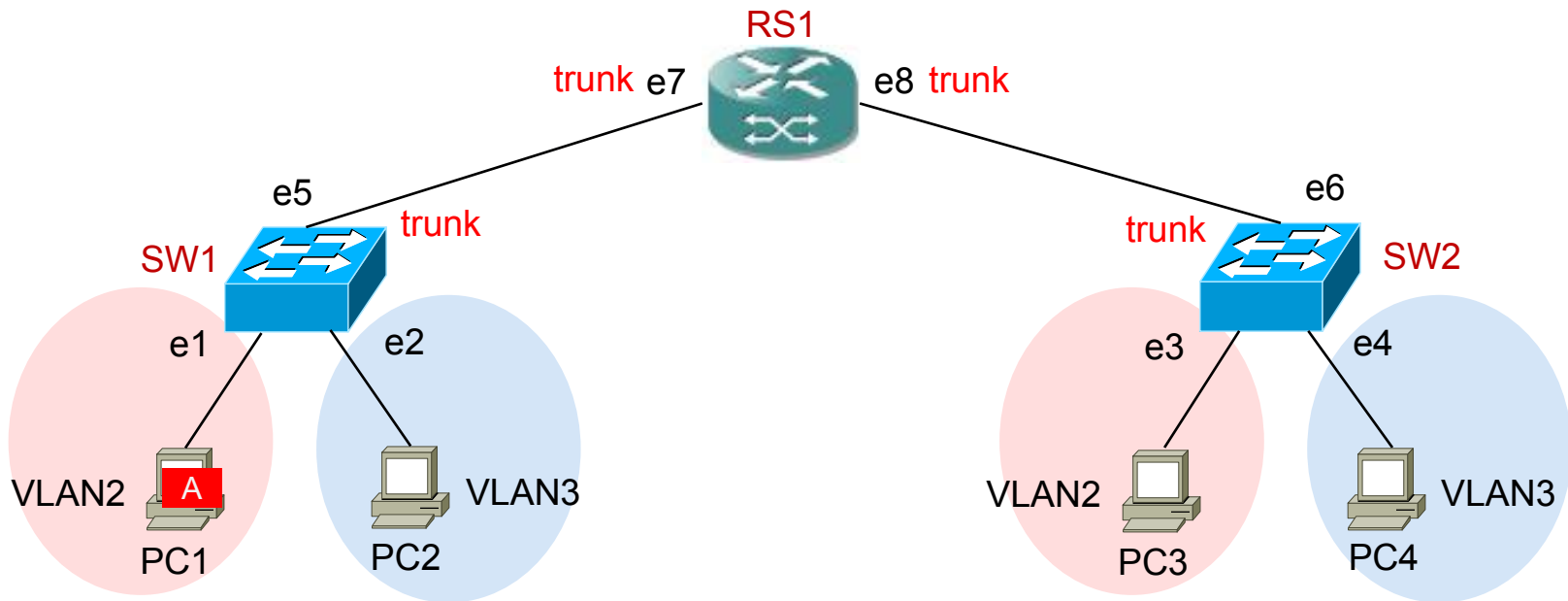
三层交换机组网实例分析—— PC1访问PC3 (Ping)



假设7:

PC3已经知道自己默认网关的MAC地址 (即MAC_S);
注意, 该记录在PC3的ARP表中。

三层交换机组网实例分析—— PC1访问PC3 (Ping)

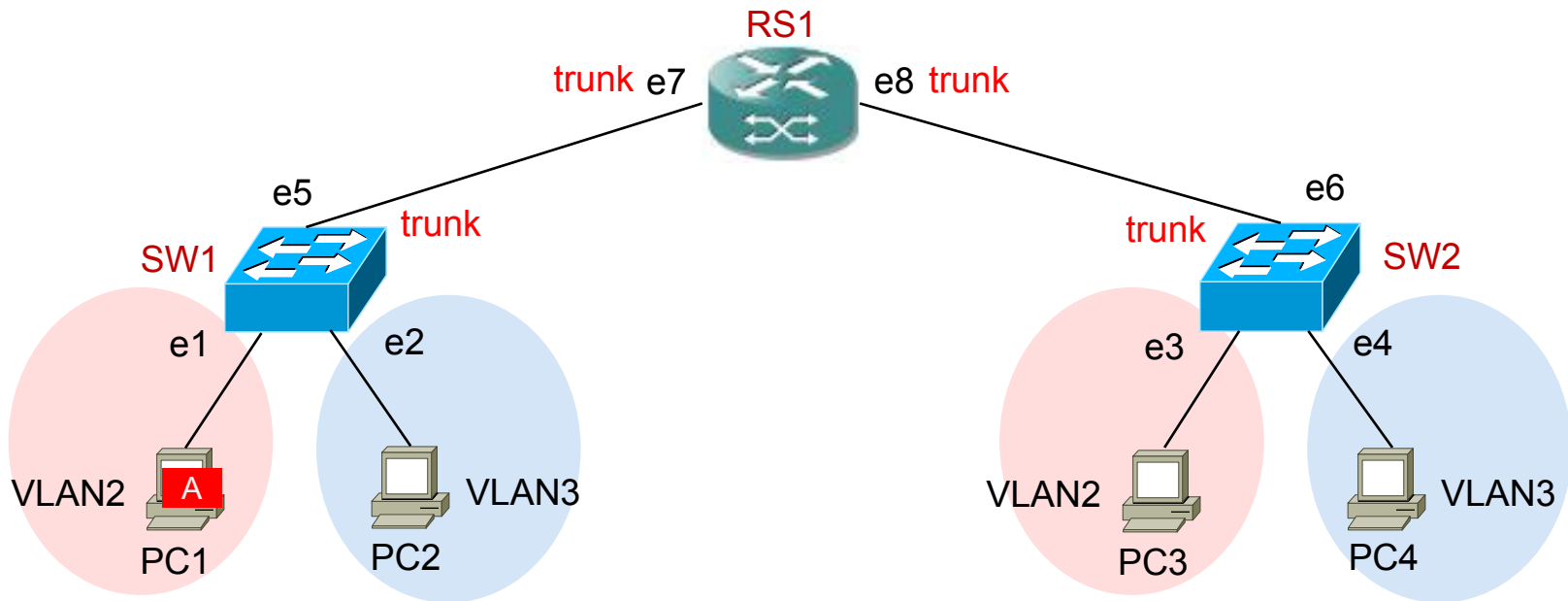


1. PC1获取PC3的MAC地址——（1）发送ARP请求报文

由于目的IP与源IP在**同一网段**，所以可以将ICMP请求报文直接发给PC3。

但是，PC1发现自己还不知道PC3的MAC地址，所以先发出ARP请求，询问PC3的MAC地址。

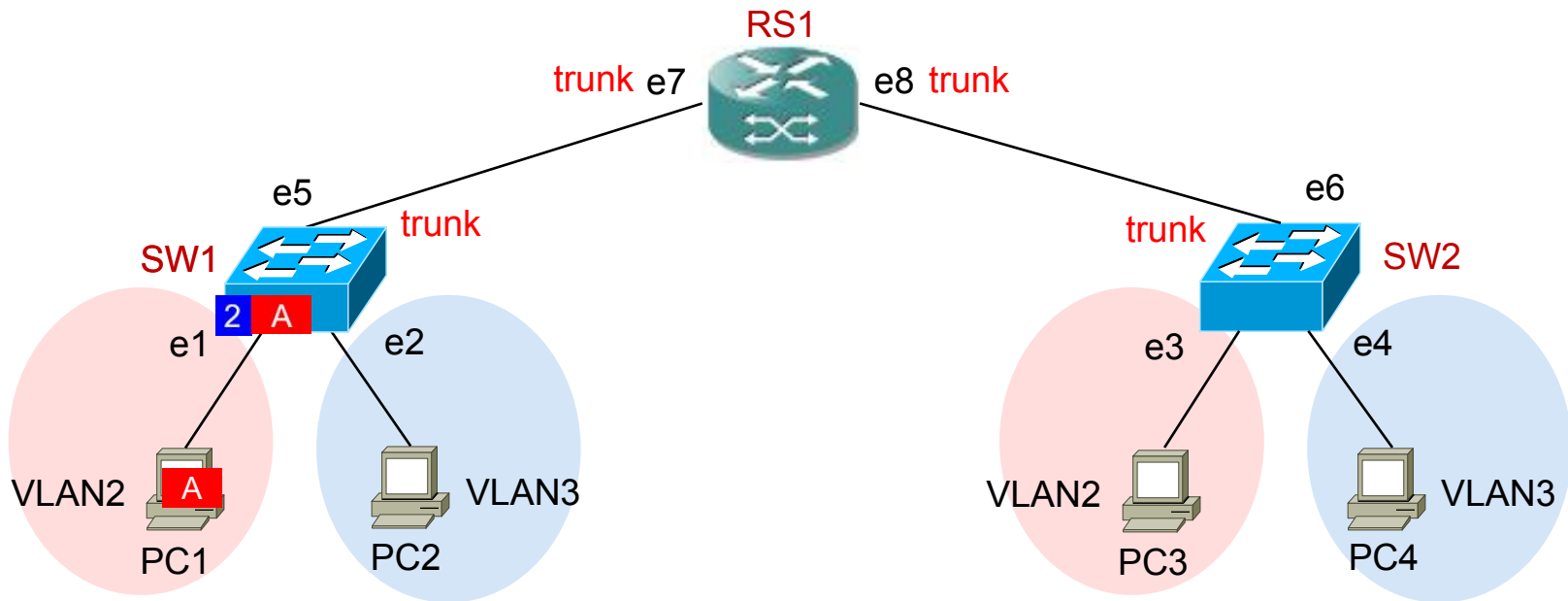
三层交换机组网实例分析—— PC1访问PC3 (Ping)



1. PC1获取PC3的MAC地址——（1）PC1发送ARP请求报文

在封装报文时，源MAC是MAC1，目的MAC是ff-ff-ff-ff-ff-ff。源IP是IP1，目的IP是PC3。报文先到达交换机SW1。

三层交换机组网实例分析—— PC1访问PC3 (Ping)



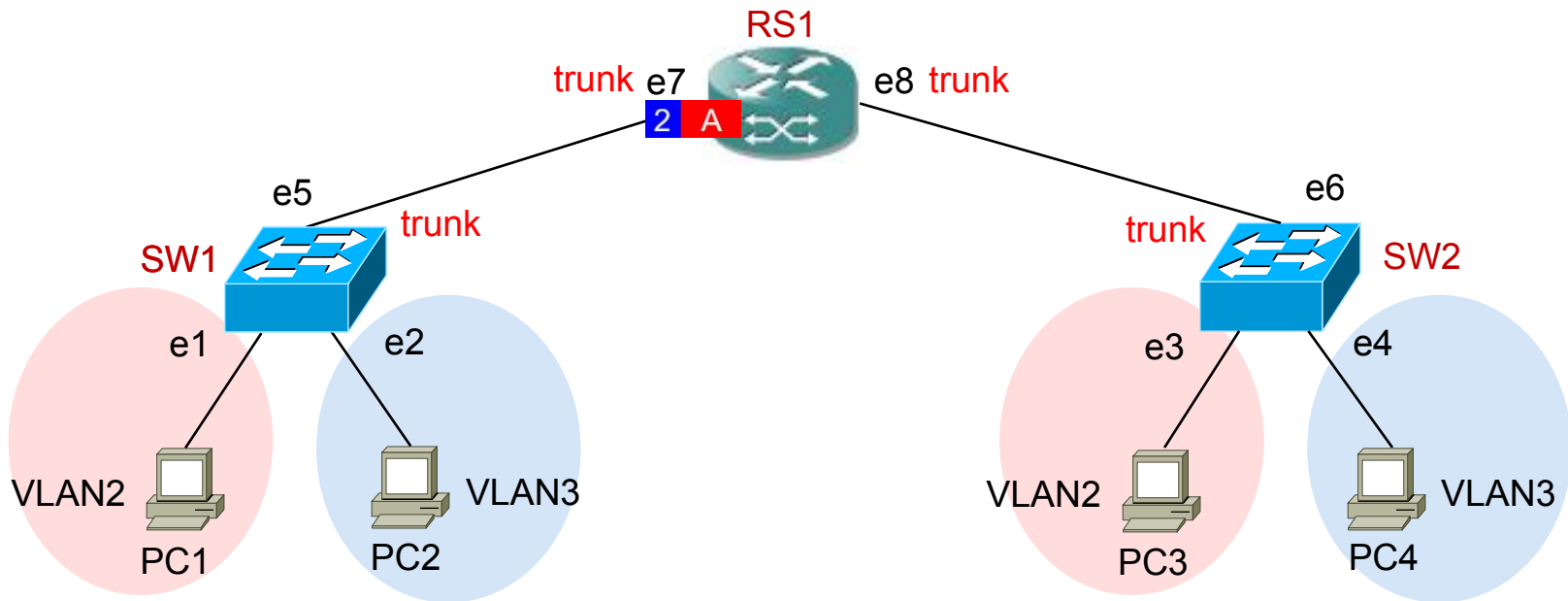
1. PC1获取PC3的MAC地址—— (2) SW1处理ARP请求报文

ARP请求报文到达e1接口，被添加VLAN2标签；

SW1将该广播报文转发至VLAN2当中的所有接口，包括e5接口；

由于e5接口是trunk接口，所以保留VLAN2标签发送出去，到达RS1的e7接口。

三层交换机组网实例分析—— PC1访问PC3 (Ping)

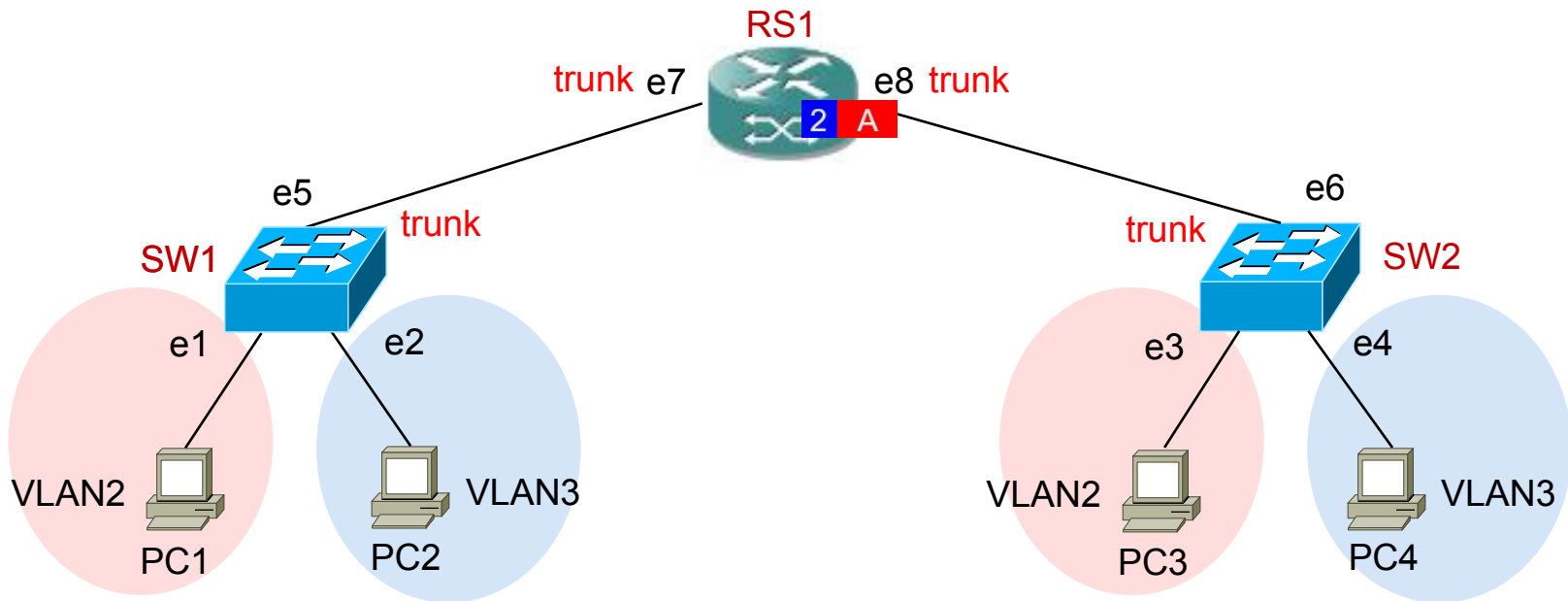


1. PC1获取PC3的MAC地址——（3）RS1转发ARP请求报文

RS1的e7接口是trunk接口，所以接收报文并保留VLAN2的标签；

由于目的MAC是广播地址，因此RS1将ARP请求报文转发至属于VLAN2的所有接口（来源接口除外），包括e8接口（trunk接口）。

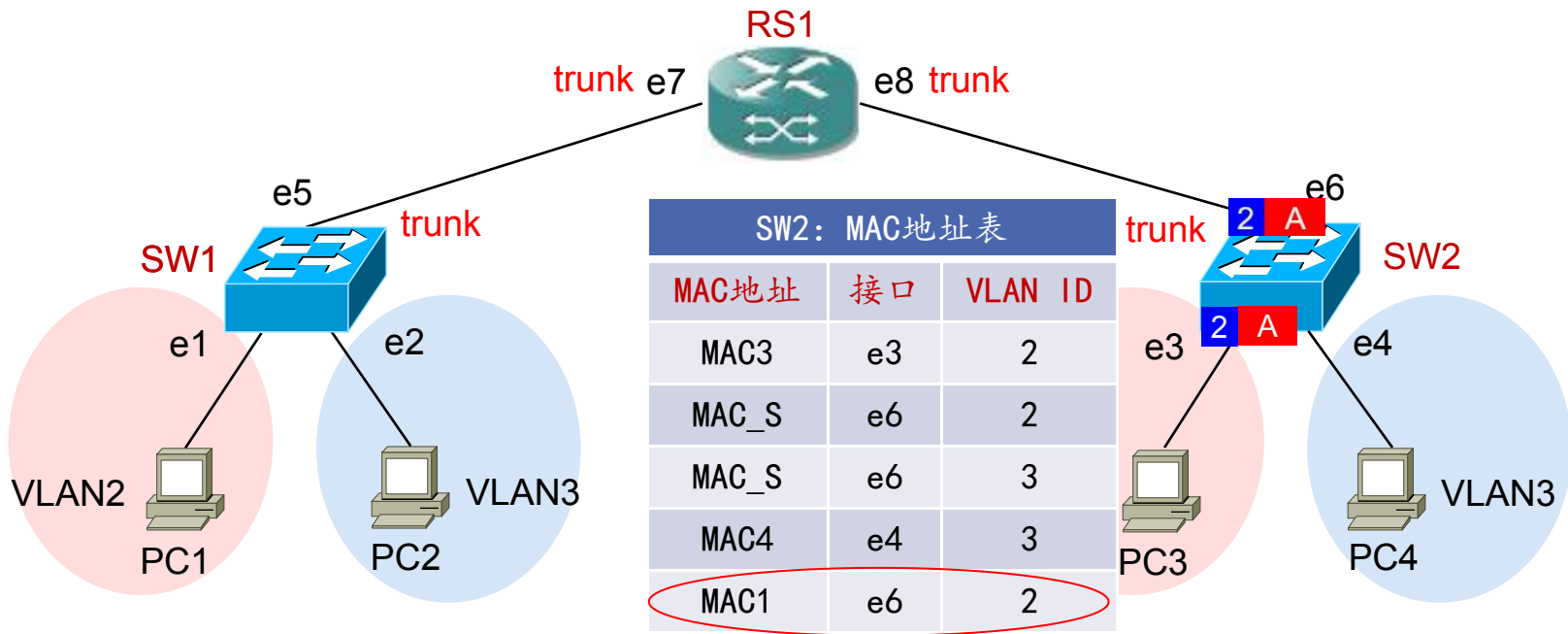
三层交换机组网实例分析—— PC1访问PC3 (Ping)



1. PC1获取PC3的MAC地址—— (3) RS1转发ARP请求报文

RS1的e8接口是trunk接口，所以发出ARP报文时保留VLAN2的标签；

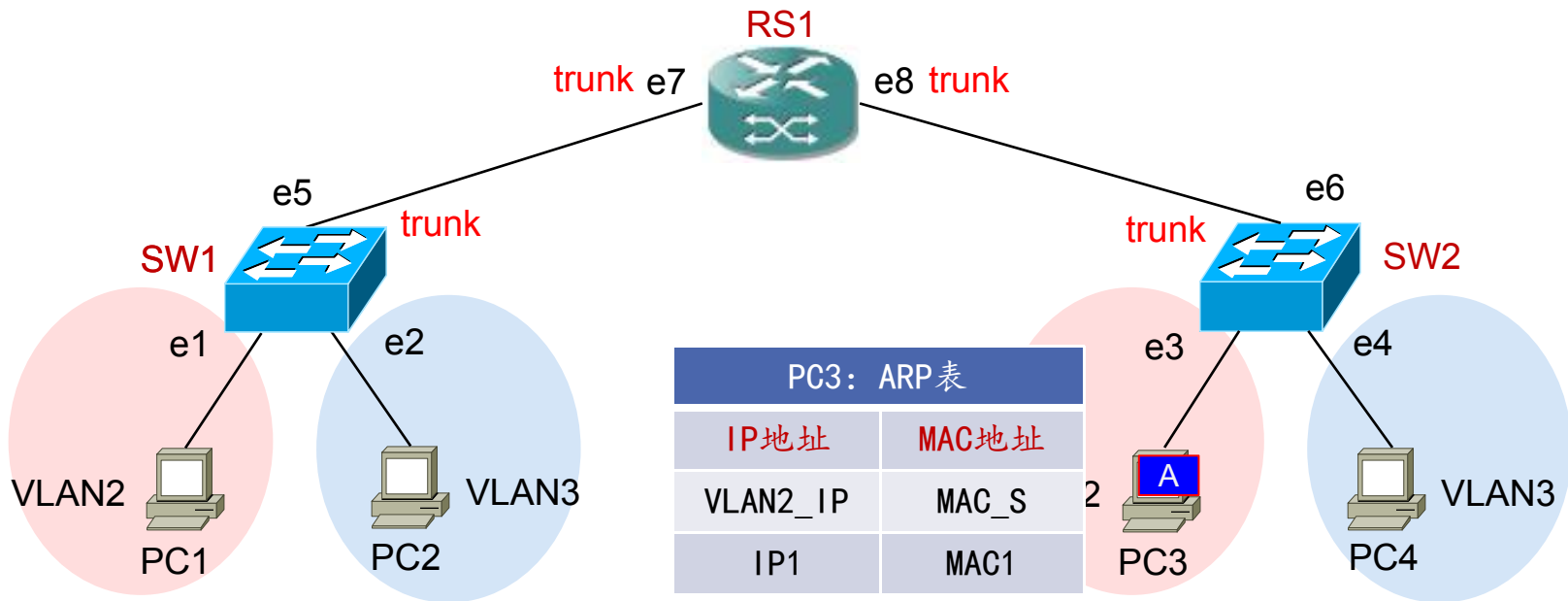
三层交换机组网实例分析—— PC1访问PC3 (Ping)



1. PC1获取PC3的MAC地址—— (4) SW2转发ARP请求报文

SW2的e6接口是trunk接口，所以接收ARP报文时保留VLAN2的标签；
 SW2将ARP报文转发至所有属于VLAN2的接口（除来源接口），包括e3接口；
 SW2根据ARP报文的来源，在MAC地址表中添加PC1的MAC地址记录；
 由于e3接口是access接口，所以去掉VLAN2标签后，将ARP请求报文发出

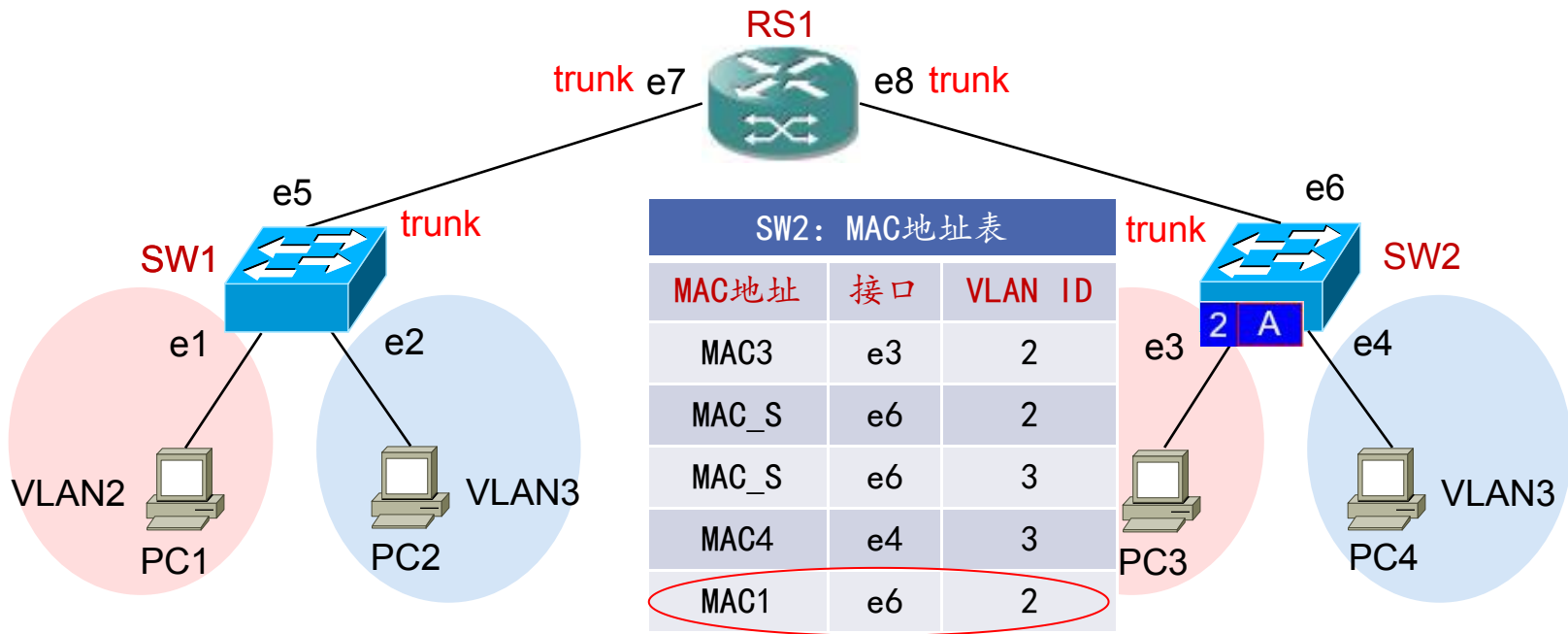
三层交换机组网实例分析—— PC1访问PC3 (Ping)



1. PC1获取PC3的MAC地址—— (5) PC3发回ARP响应报文

PC3从收到的ARP请求报文中，获取到PC1的MAC，将其记录在自己的ARP表中；
PC3发回ARP响应报文（单播报文）；
报文中源IP为IP3，目的IP为IP1，源MAC为MAC3，目的MAC为MAC1。

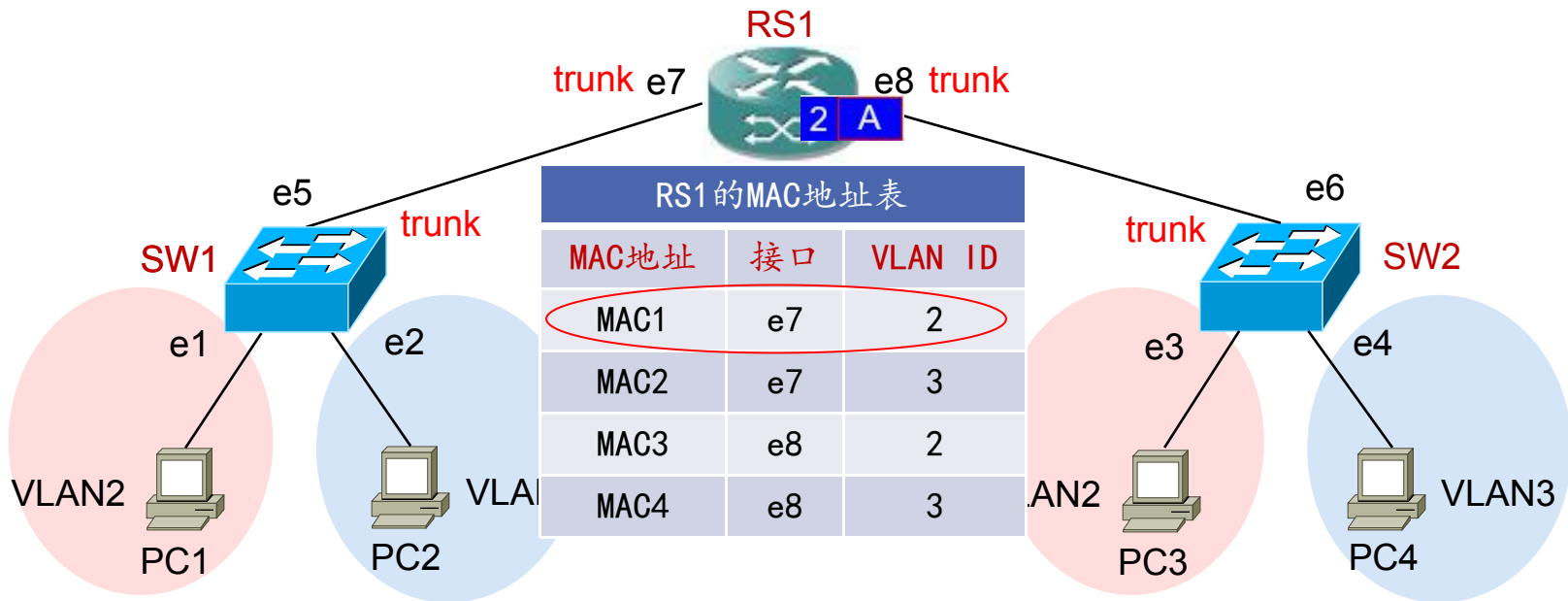
三层交换机组网实例分析—— PC1访问PC3 (Ping)



1. PC1获取PC3的MAC地址—— (6) SW2转发ARP响应报文

SW2的e3接口收到PC3发回ARP响应报文，添加上VLAN2的标签；
 SW2依据自己的MAC地址表，将报文转发至e6接口；
 由于e6是trunk接口，所以将报文保留VLAN2标签发送出去。

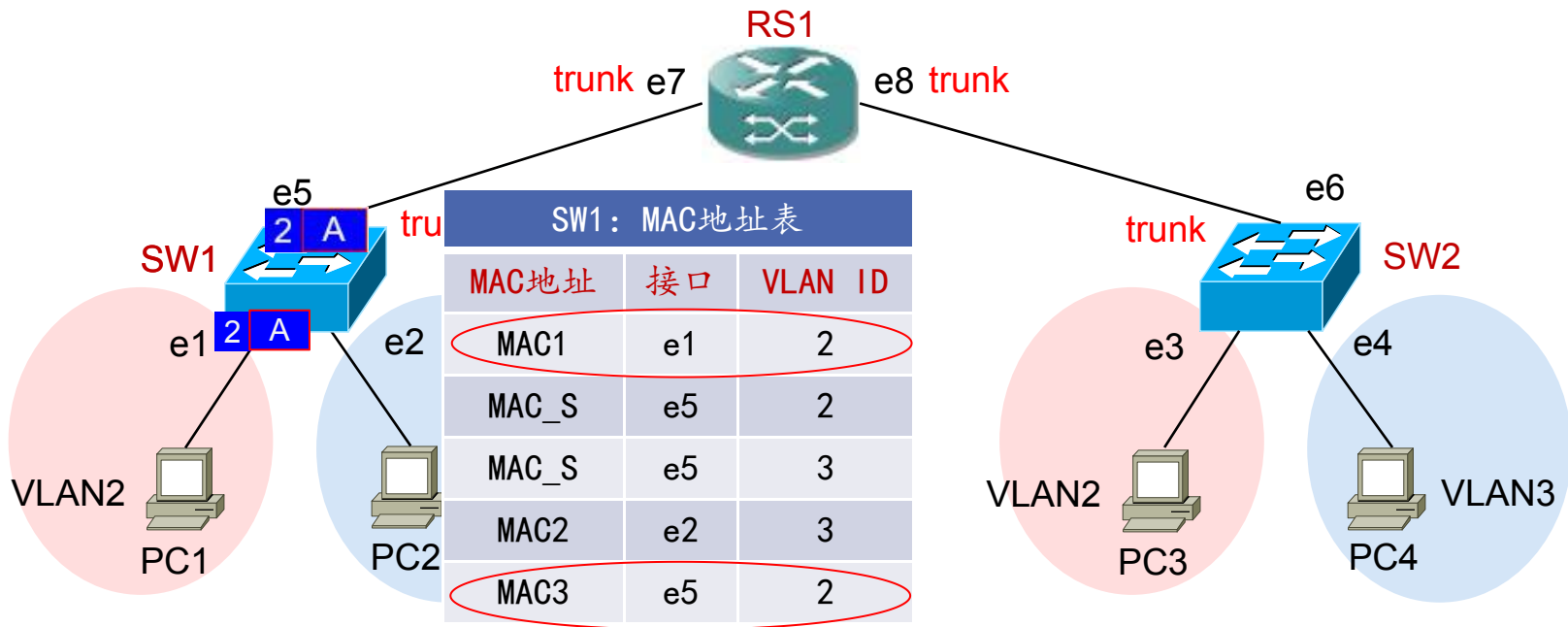
三层交换机组网实例分析—— PC1访问PC3 (Ping)



1. PC1获取PC3的MAC地址—— (7) RS1转发ARP响应报文

RS1的e8接口收到ARP响应报文，因为e8是trunk接口，所以保留VLAN2标签；因为属于同VLAN内部转发，因此依据MAC地址表即可进行；RS1依据自己的MAC地址表，将报文转发至e7接口；由于e7是trunk接口，所以将报文保留VLAN2标签发送出去。

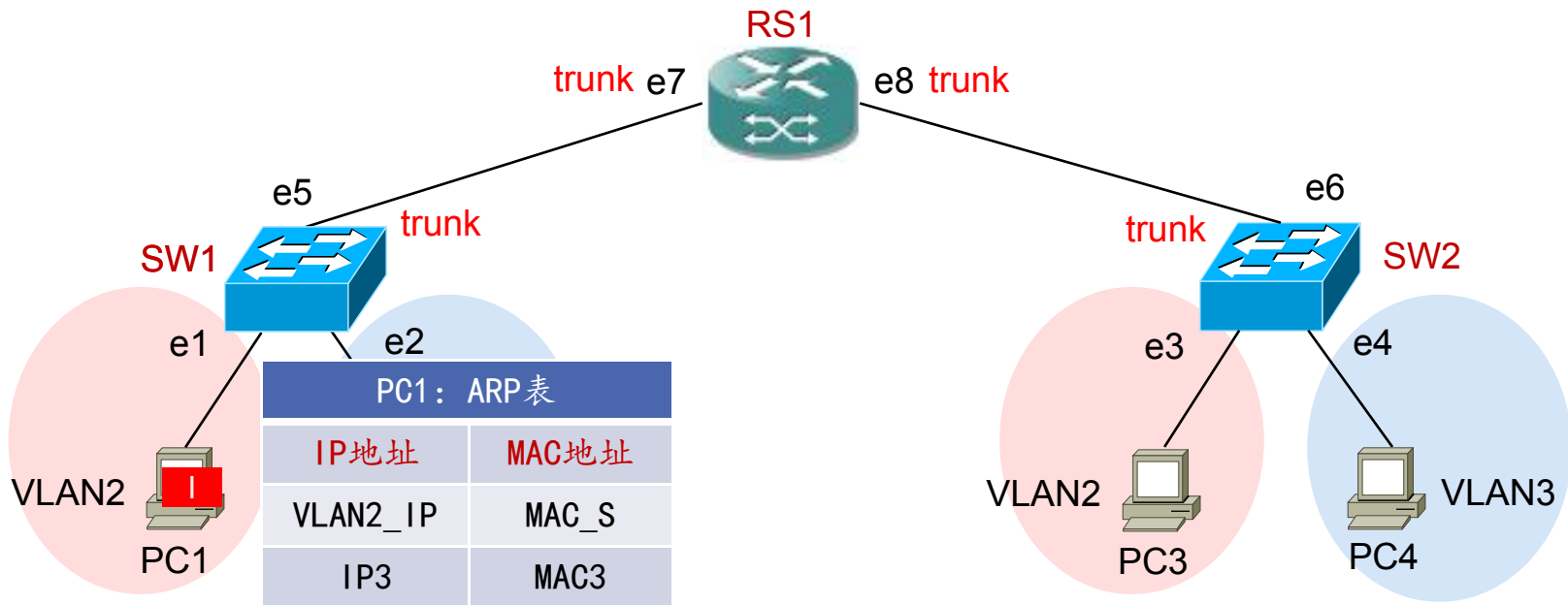
三层交换机组网实例分析—— PC1访问PC3 (Ping)



1. PC1获取PC3的MAC地址—— (8) SW1转发ARP响应报文

SW1的e5接口收到ARP响应报文，因为e5是trunk接口，所以保留VLAN2标签；
 SW1依据报文来源信息，在MAC地址表中添加PC3的信息；
 SW1依据MAC地址表将报文转发至e1接口；
 由于e1是access接口，所以将报文去掉VLAN2标签发送出去。

三层交换机组网实例分析—— PC1访问PC3 (Ping)

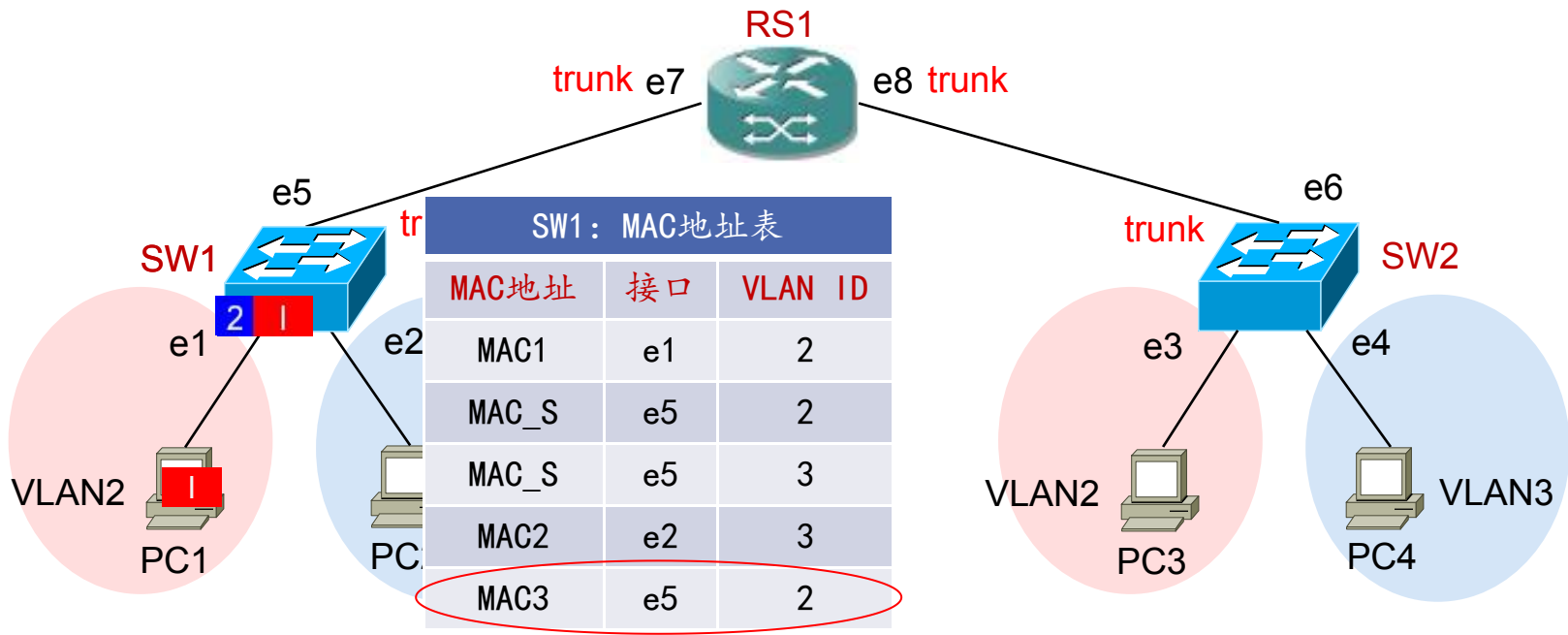


2. PC1向PC3发送ICMP请求报文—— (1) PC1封装ICMP请求报文

PC1获得PC3的MAC地址后，记录在自己的ARP表中；

PC1封装ICMP请求报文，其源IP是IP1、目的IP是IP3、源MAC是MAC1、目的MAC是MAC3；

三层交换机组网实例分析—— PC1访问PC3 (Ping)



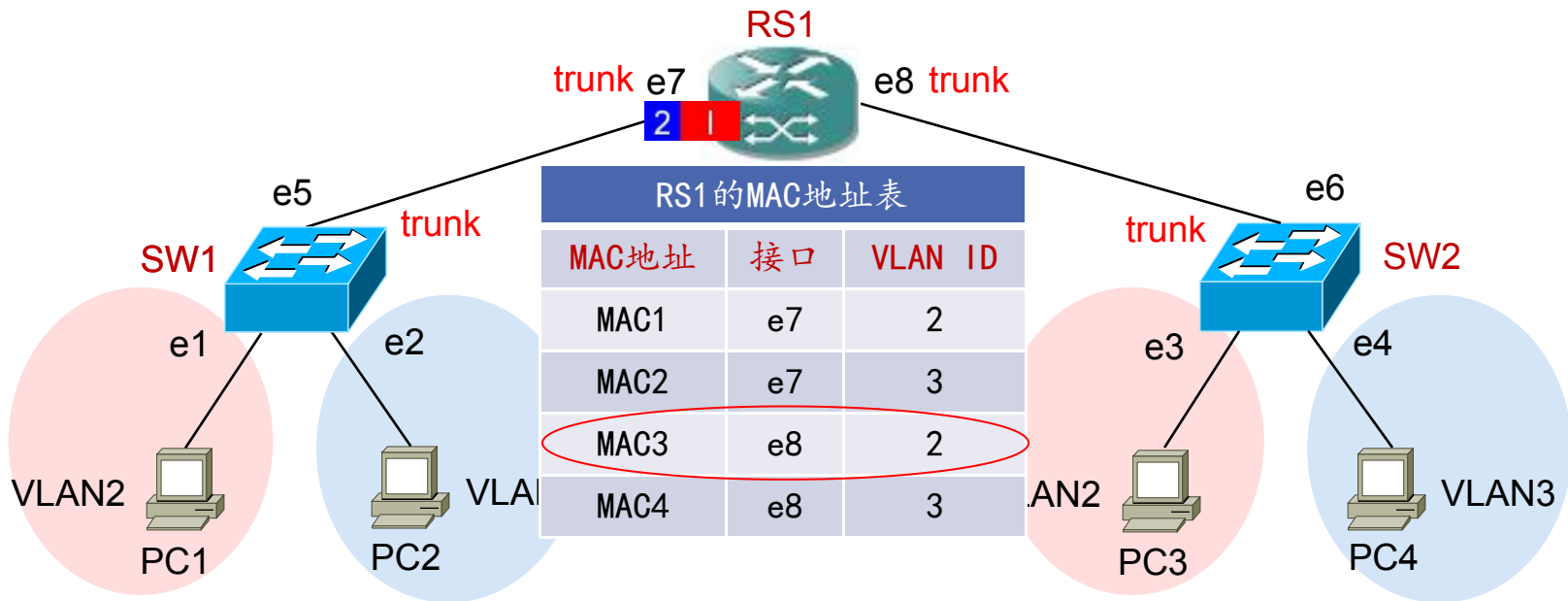
2. PC1向PC3发送ICMP请求报文—— (2) SW1转发ICMP请求报文

ICMP请求报文到达SW1的e1接口，被添加VLAN2标签；

SW1依据MAC地址表，将该报文转发至e5接口；

由于e5接口是trunk接口，所以保留VLAN2标签发送出去；

三层交换机组网实例分析—— PC1访问PC3 (Ping)

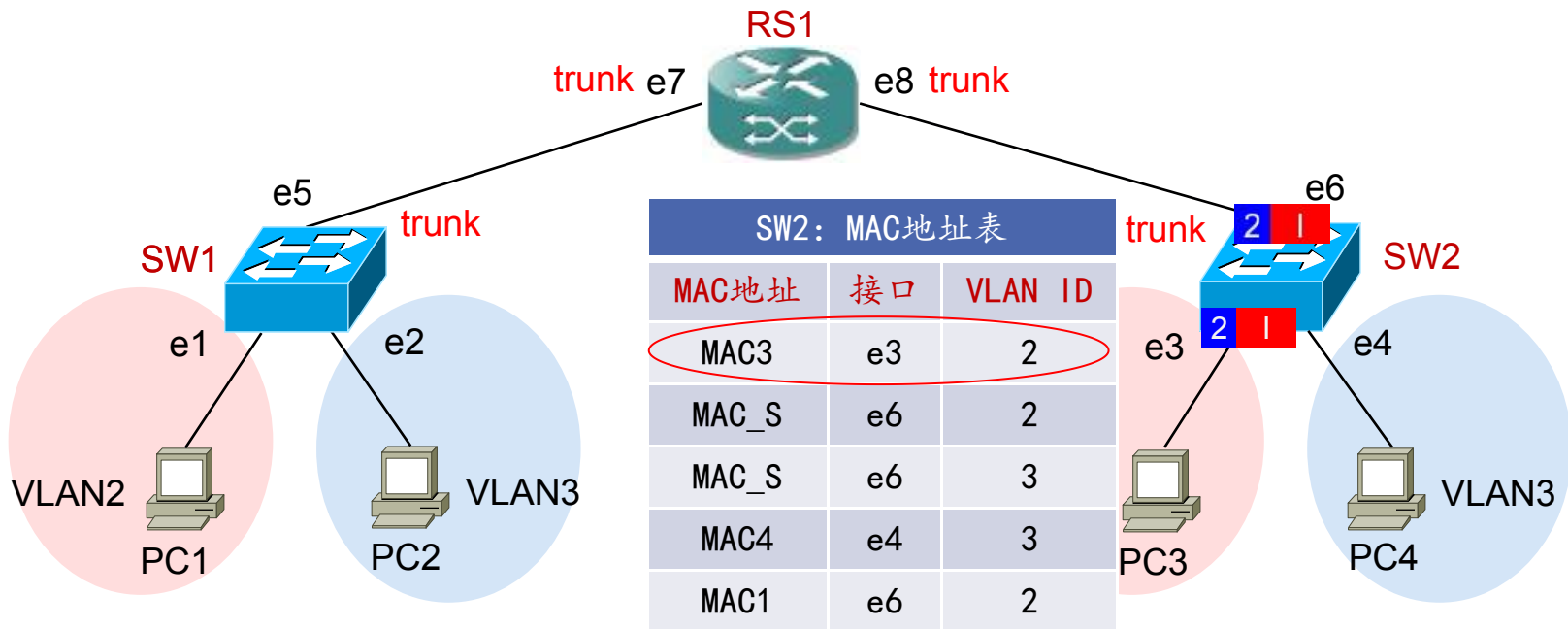


2. PC1向PC3发送ICMP请求报文—— (3) RS1转发ICMP请求报文

RS1的e7接口是trunk接口，所以接收报文并保留VLAN2的标签；由于源IP和目的IP在同一网段，所以不需启用三层路由模块，依据MAC地址表进行转发。

将ICMP请求报文转发至e8接口（trunk接口），保留VLAN2标签并发送出去。

三层交换机组网实例分析—— PC1访问PC3 (Ping)



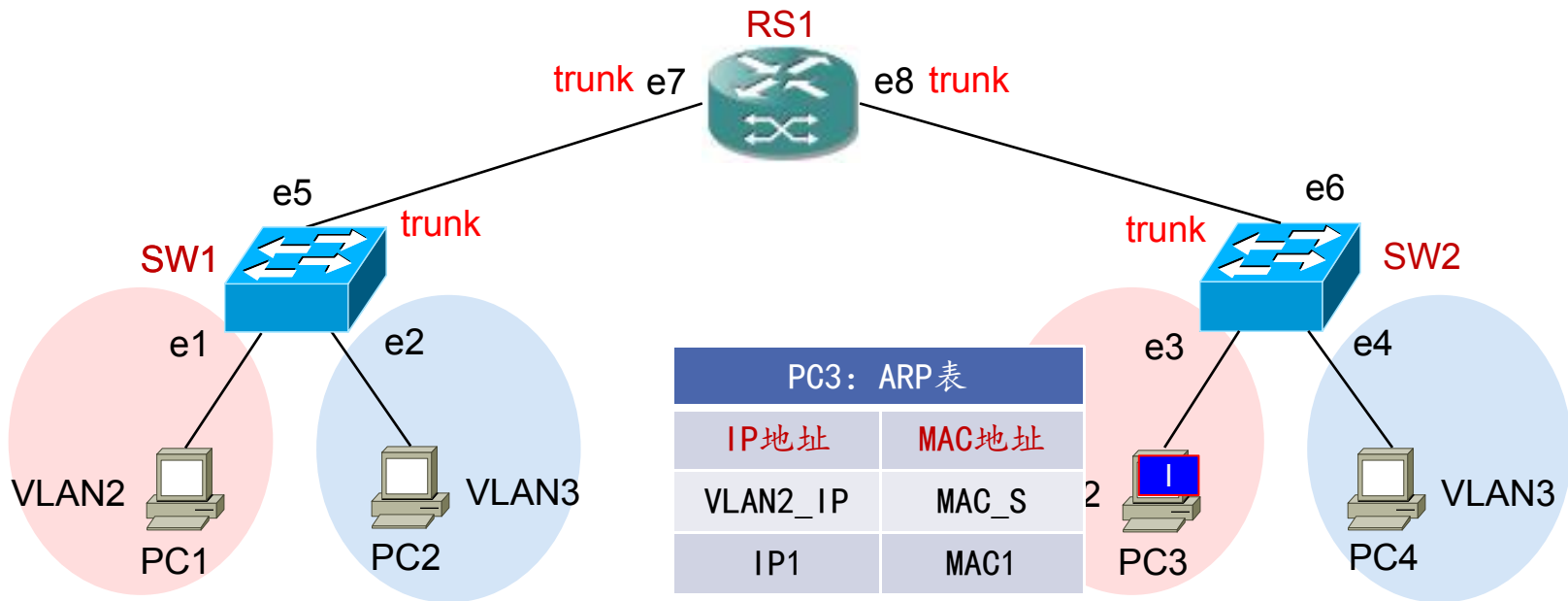
2. PC1向PC3发送ICMP请求报文——（4）SW2转发ICMP请求报文

SW2的e6接口是trunk接口，所以接收ICMP请求报文时保留VLAN2的标签；

SW2依据MAC地址表，将ICMP请求报文转发至e3接口；

由于e3接口是access接口，所以去掉VLAN2标签后，将ICMP请求报文发出

三层交换机组网实例分析—— PC1访问PC3 (Ping)



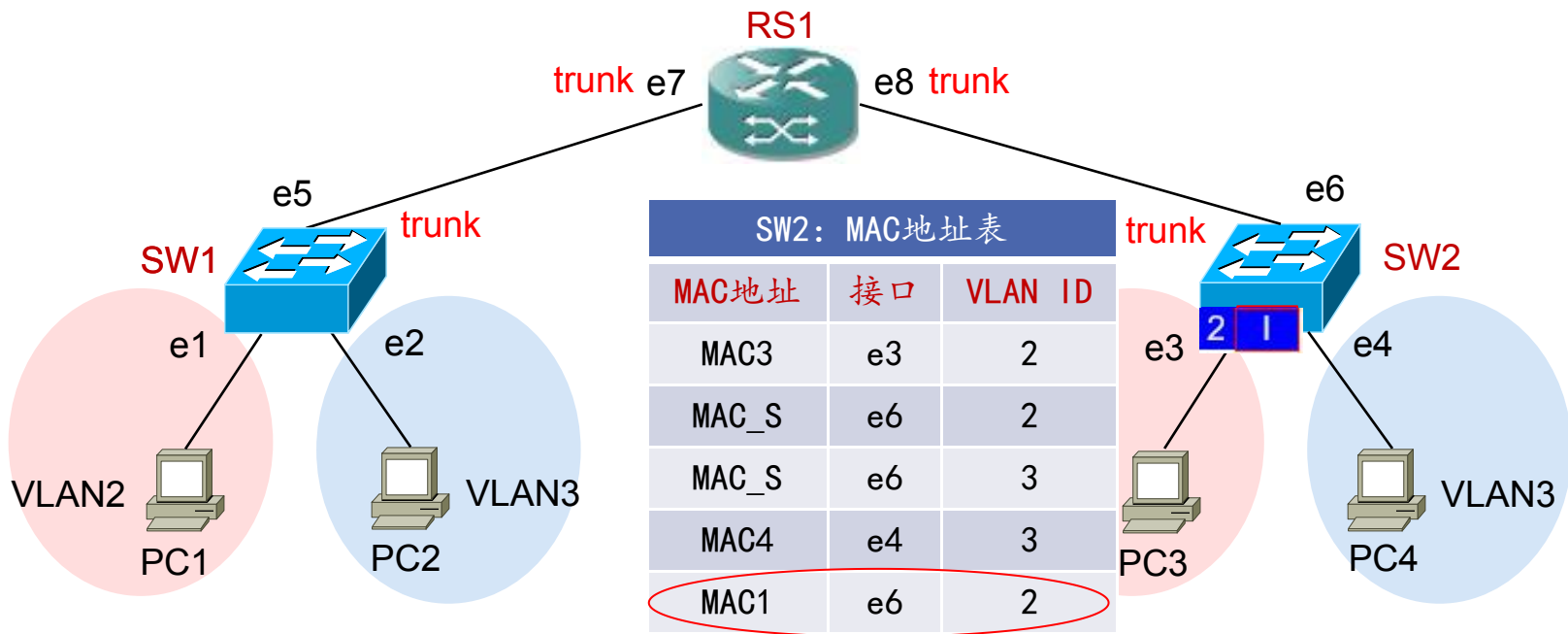
3. PC3向PC1发回ICMP响应报文——（1）PC3封装ICMP响应报文

PC3发回ICMP响应报文（单播报文）；

PC3从自己的ARP表中查到PC1的MAC地址是MAC1；

报文中源IP为IP3，目的IP为IP1，源MAC为MAC3，目的MAC为MAC1。

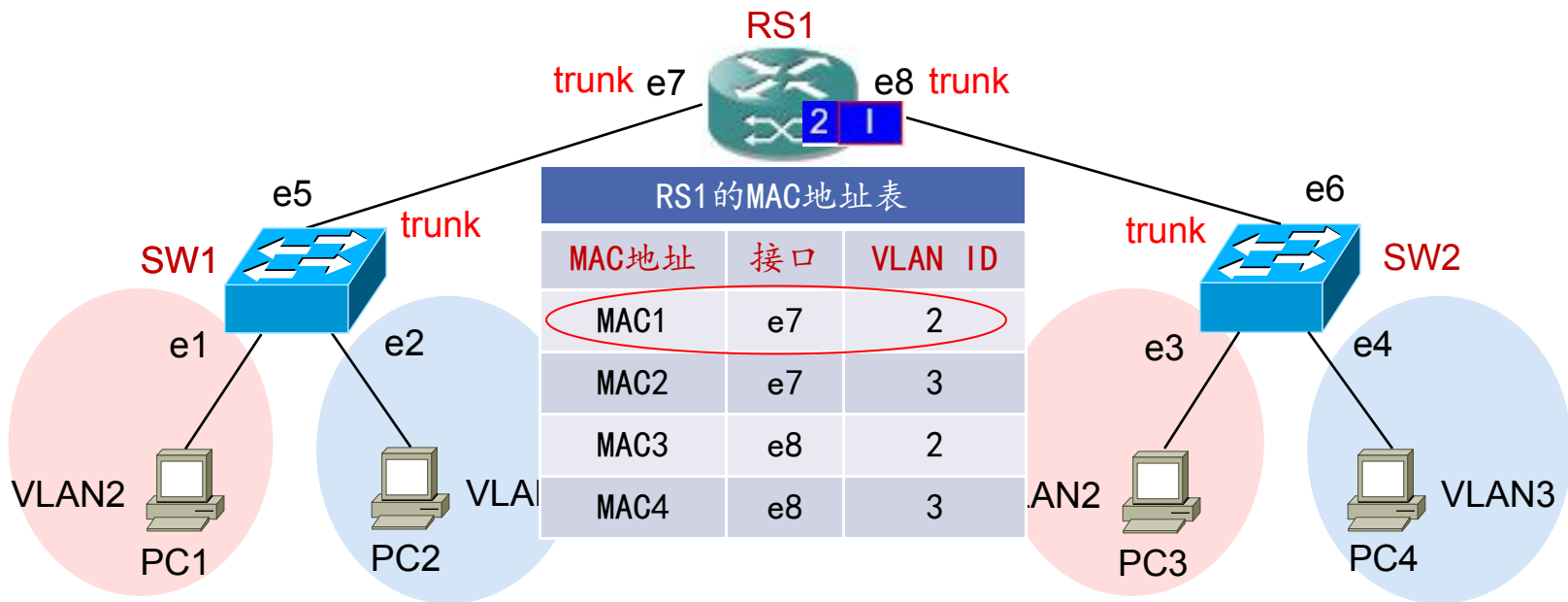
三层交换机组网实例分析—— PC1访问PC3 (Ping)



3. PC3向PC1发回ICMP响应报文—— (2) SW2转发ICMP响应报文

SW2的e3接口收到PC3发回ICMP响应报文，添加上VLAN2的标签；
SW2依据自己的MAC地址表，将报文转发至e6接口；
由于e6是trunk接口，所以将报文保留VLAN2标签发送出去。

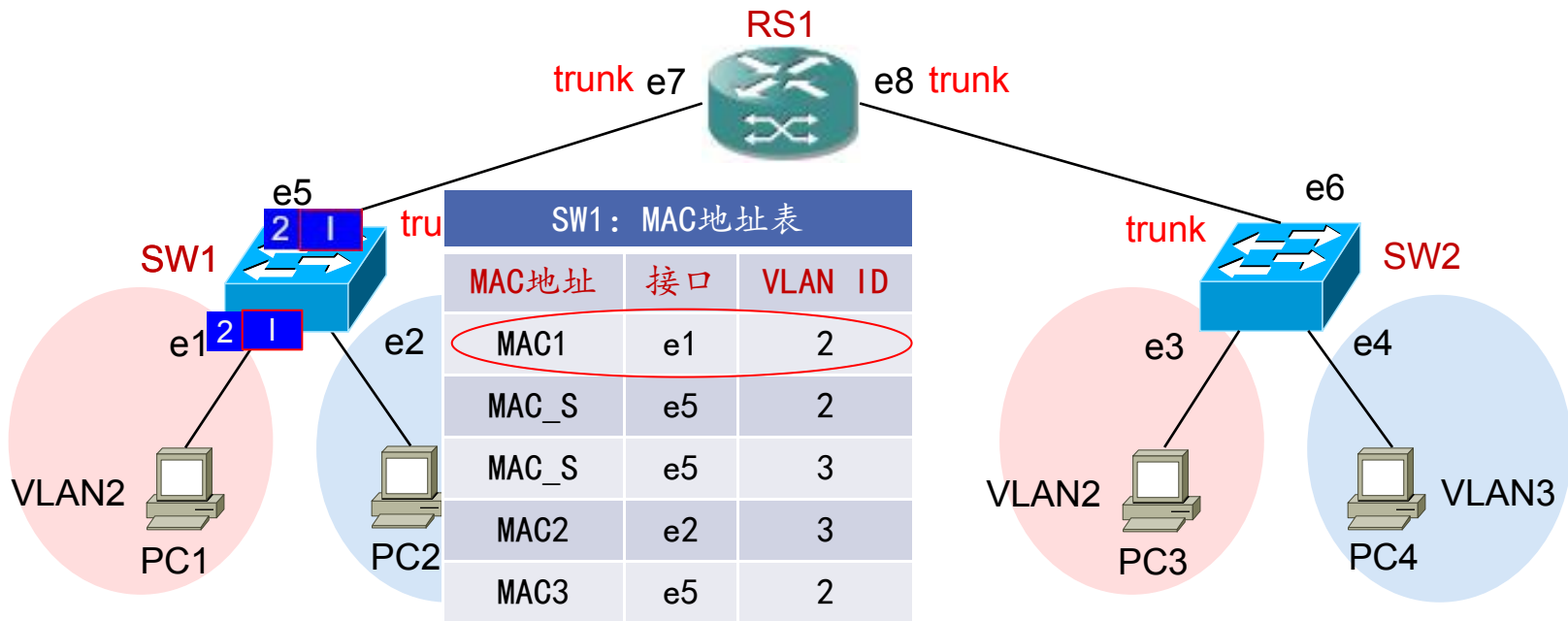
三层交换机组网实例分析—— PC1访问PC3 (Ping)



3. PC3向PC1发回ICMP响应报文—— (3) RS1转发ICMP响应报文

RS1的e8口收到ICMP响应报文，因为e8是trunk接口，所以保留VLAN2标签；
 因为属于同VLAN内部转发，因此依据MAC地址表即可进行；RS1依据自己的
 MAC地址表，将报文转发至e7接口；由于e7是trunk接口，所以将报文保留VLAN2标
 签发送出去。

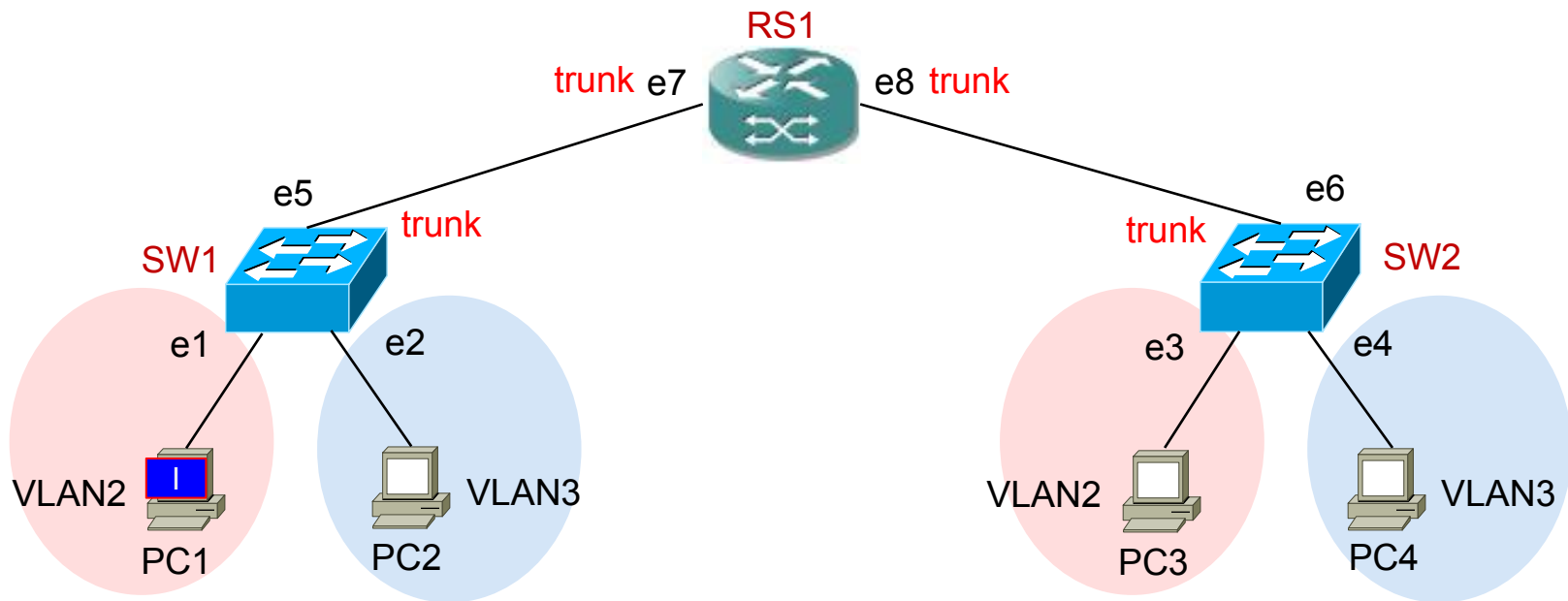
三层交换机组网实例分析—— PC1访问PC3 (Ping)



3. PC3向PC1发回ICMP响应报文——（4）SW1转发ICMP响应报文

SW1的e5接口收到ARP响应报文，因为e5是trunk接口，所以保留VLAN2标签；
SW1依据MAC地址表将报文转发至e1接口；
由于e1是access接口，所以将报文去掉VLAN2标签发送出去。

三层交换机组网实例分析—— PC1访问PC3 (Ping)



PC1访问PC3 (Ping)

通信完毕

第一讲 构建局域网

完