

网络运维管理



第1讲：构建有线/无线混合的园区网

目录

1. 以太网基础
2. 交换机组网
3. 虚拟局域网 (VLAN) 的应用
4. 三层交换机的应用
5. 路由器实现网络互联
6. 划分子网与构建超网
7. IP地址的管理 (DHCP)
8. 无线局域网的部署
9. 混合园区网建设案例分析

1. 以太网基础

以太网基础

网络标准: IEEE802.3 (CSMA/CD)

技术发展: 传统、快速、千兆、万兆

拓扑结构: 从总线型到星型

传输介质: 双绞线、光纤等

组网设备: 交换机、路由器

关于地址: MAC地址与IP地址

2. 交换机组网

- 交换机组网
- 工作原理：依据MAC地址进行转发
 - MAC地址表：MAC地址自动学习、手工配置
 - 广播域：所有接口属于同一个广播域
 - 交换机管理：带外、带内
 - 交换机连接：级联、堆叠

3. 虚拟局域网VLAN

虚拟局域网
VLAN

工作特点： 限制广播

划分方式： 基于接口、基于MAC地址等

帧结构： IEEE802.1Q, VLAN标记

接口类型： Access、Trunk、Hybrid

两种操作： 加标签与去标签



➤ 802.1Q的帧结构

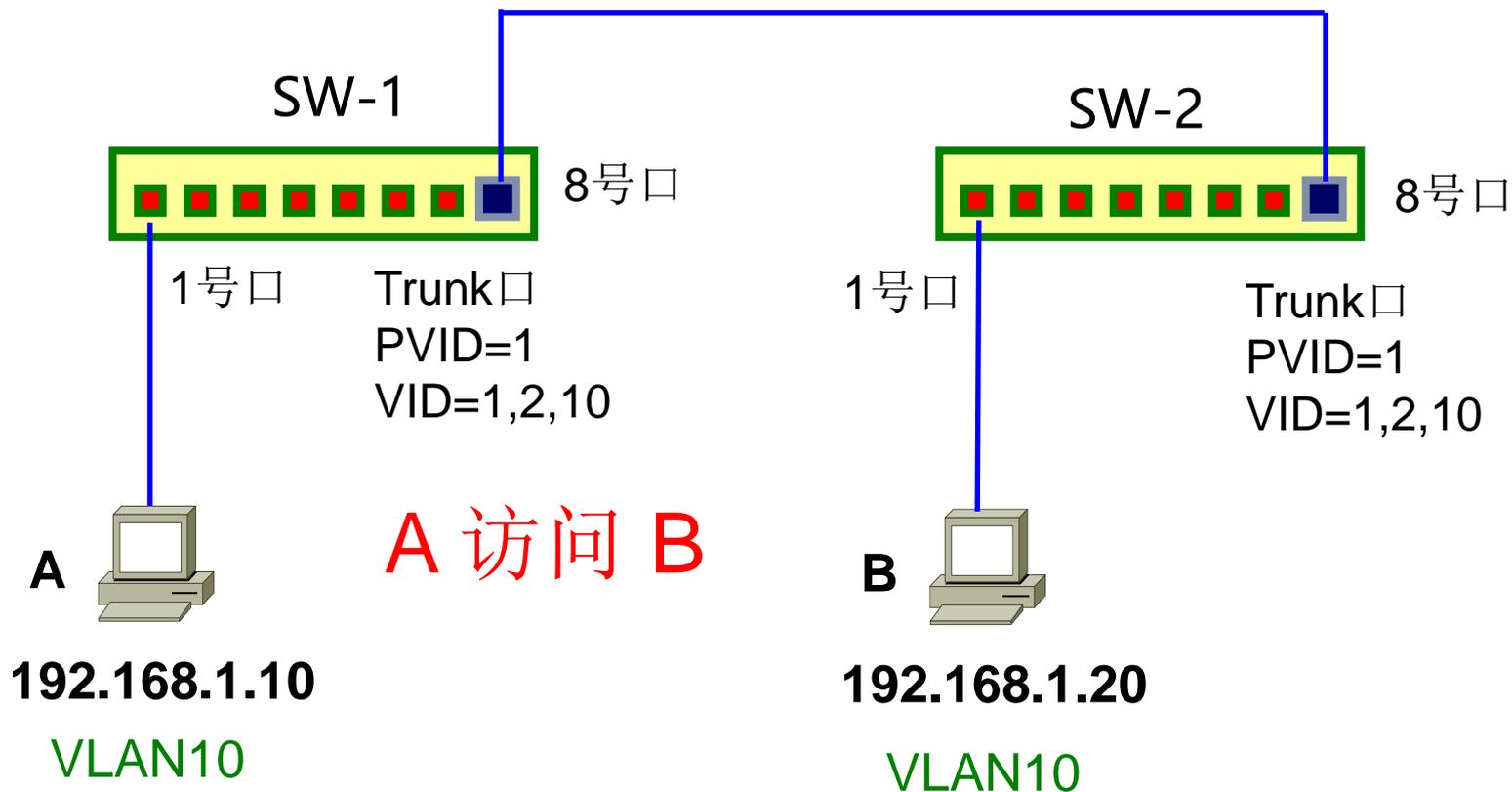


- 2字节的协议标识符，置0x8100固定值，表明该帧带有802.1Q标记信息；
- 2字节的标记控制信息，包含了3个域：
 - ① 表示报文优先级，占3bit，取值0到7，7为最高；
 - ② 表示规范格式指示符，占1bit，0表示规范格式，应用于以太网，1表示非规范格式，应用于Token Ring；
 - ③ 表示VLAN ID，占12bit，用于表示VLAN的归属，其中，VID=0用于识别帧优先级，4095 (FFF) 作为预留值，**所以有效的VLAN ID范围为1-4094。**

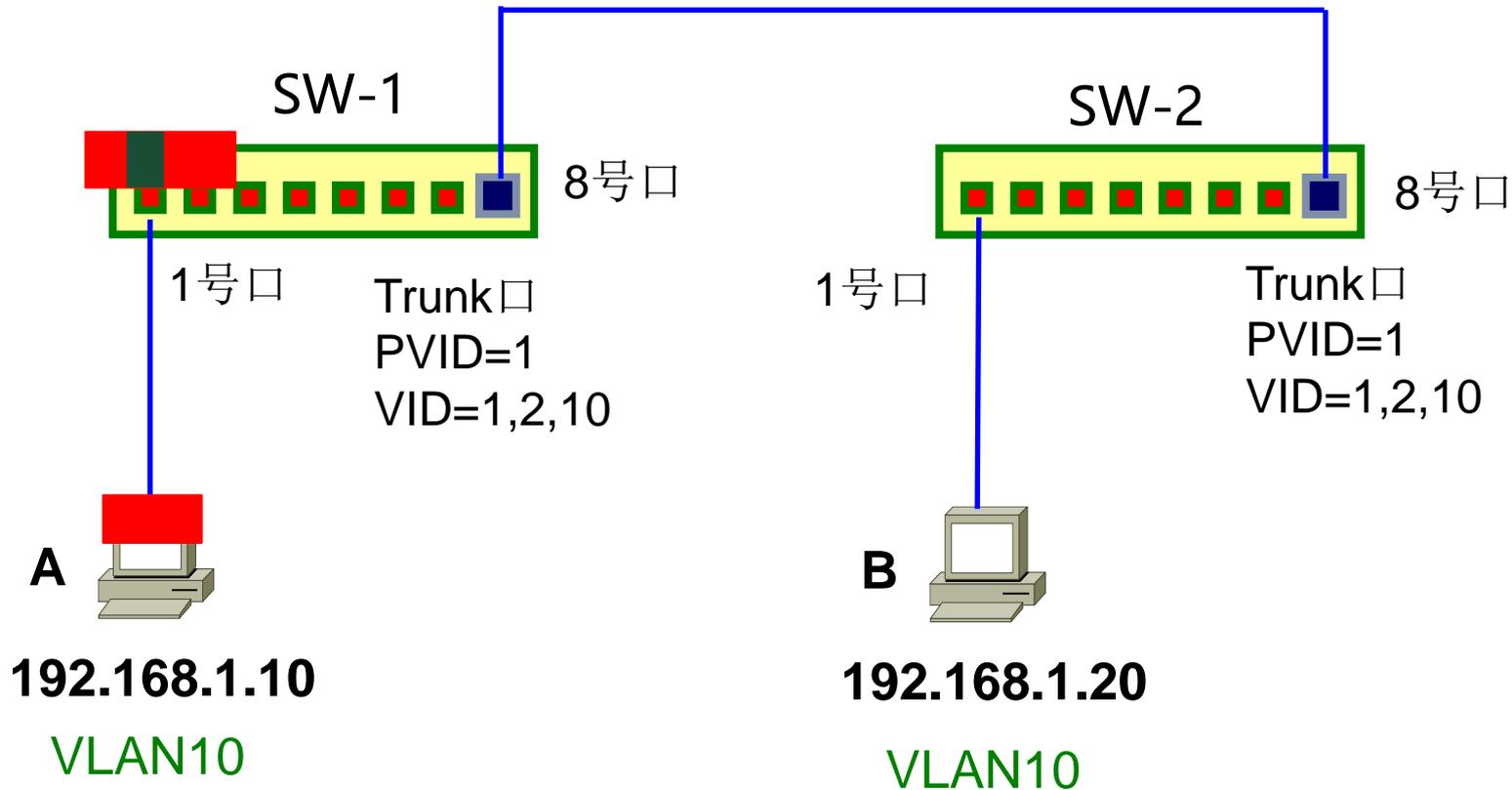


帧 接口	802.1Q数据帧 (tagged帧)		普通数据帧 (untagged帧)	
	In	Out	In	Out
Trunk 接口	接收，保持原有标签	<p>若本接口的PVID=帧VID，则去掉帧中的VLAN标签，然后发出。</p> <p>若本接口的PVID \neq 帧VID值，则直接发出，不去掉VLAN标签</p>	按接口PVID值封装帧	无此情况
Access 接口	VID=VID收 否则丢	去掉标签	按接口PVID值封装帧	无此情况

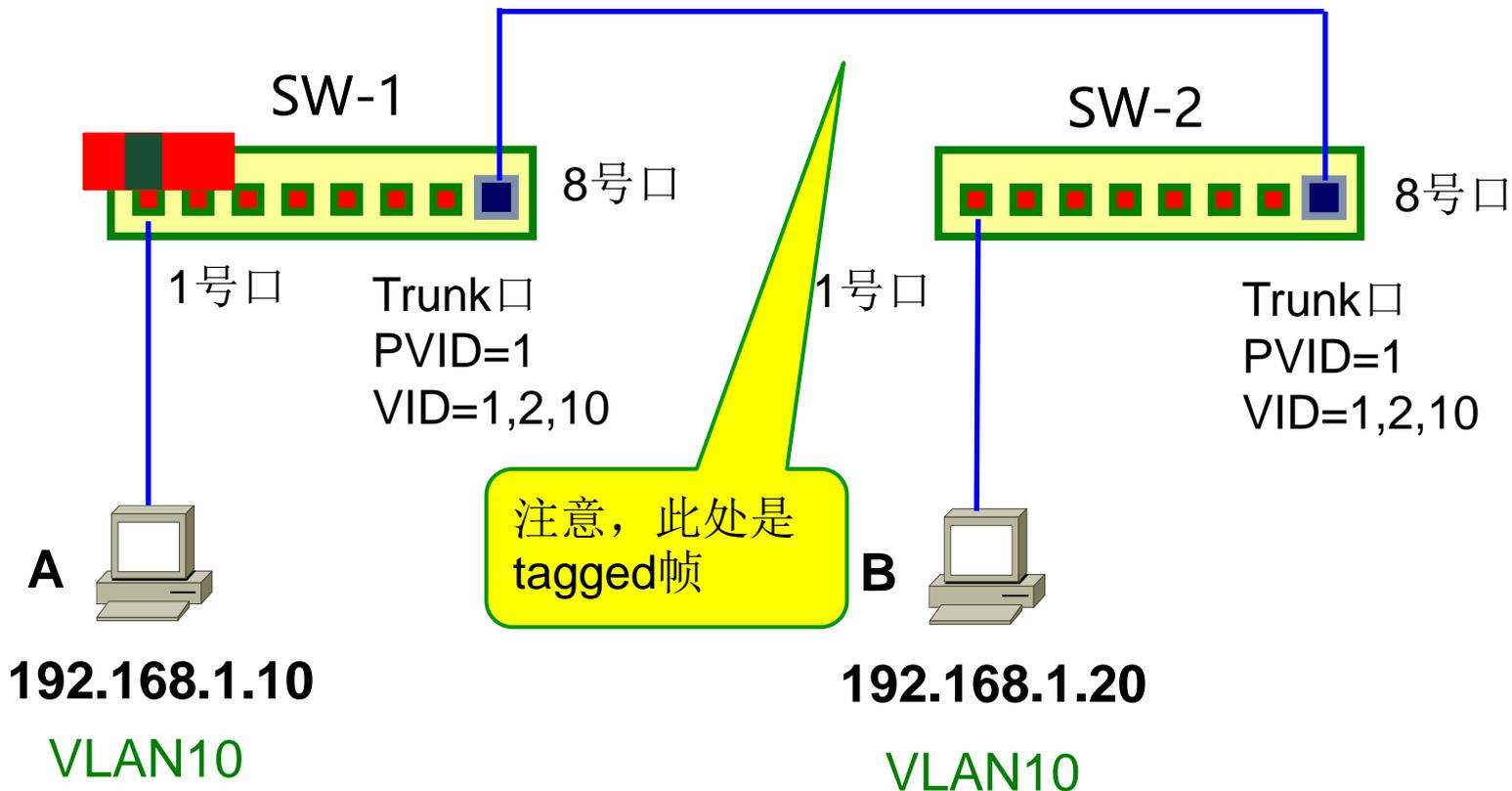
- 1号口都是Access口，属于VLAN10，其PVID值=VID值=10
- 8号口都是Trunk口，PVID值=1，允许VLAN 1、VLAN 2、VLAN 10的帧通过



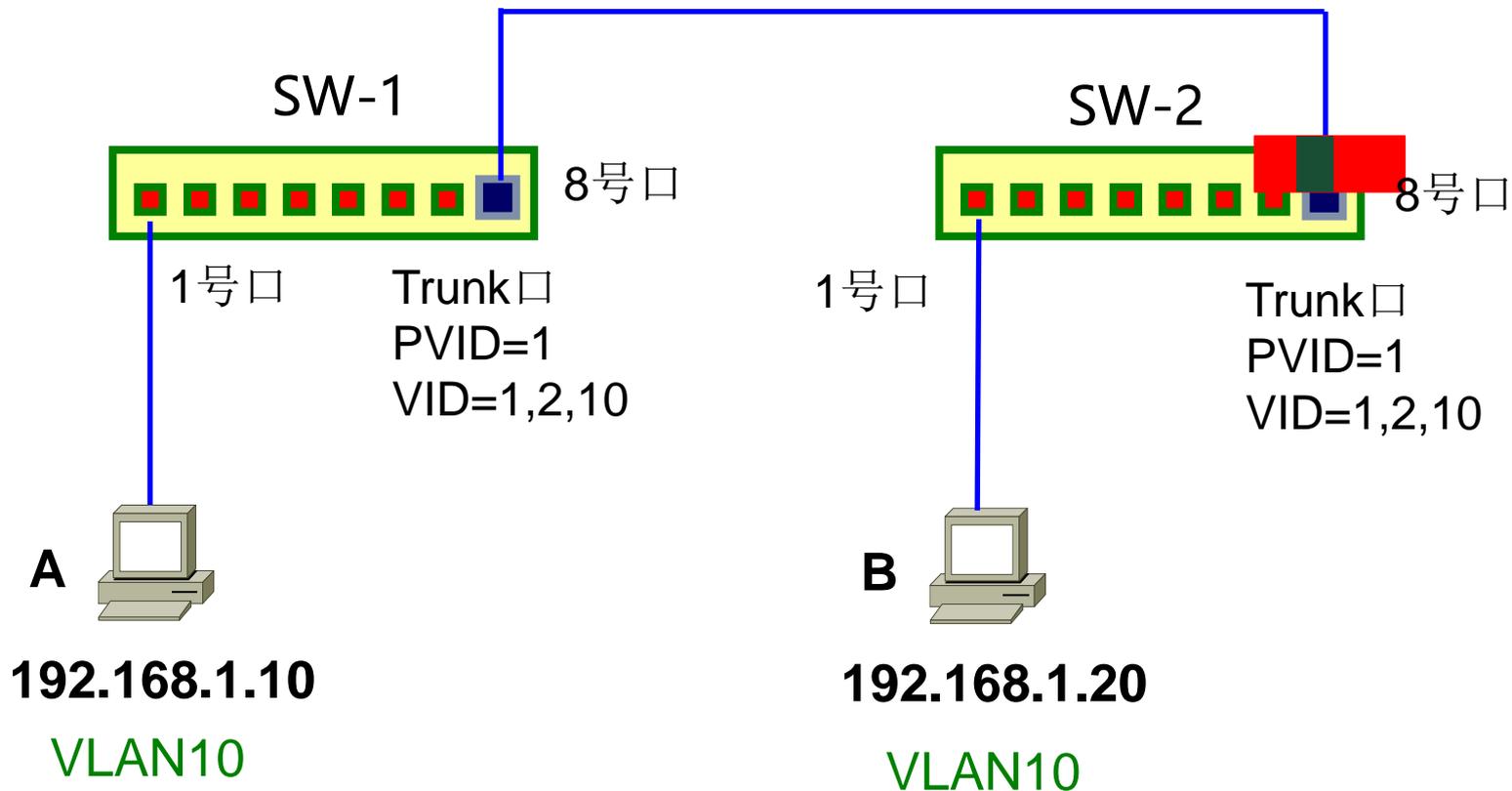
➤ PC-A发出普通帧，进入SW-1的1号口，普通帧被加上VLAN10的标签，使得该帧的VID=10



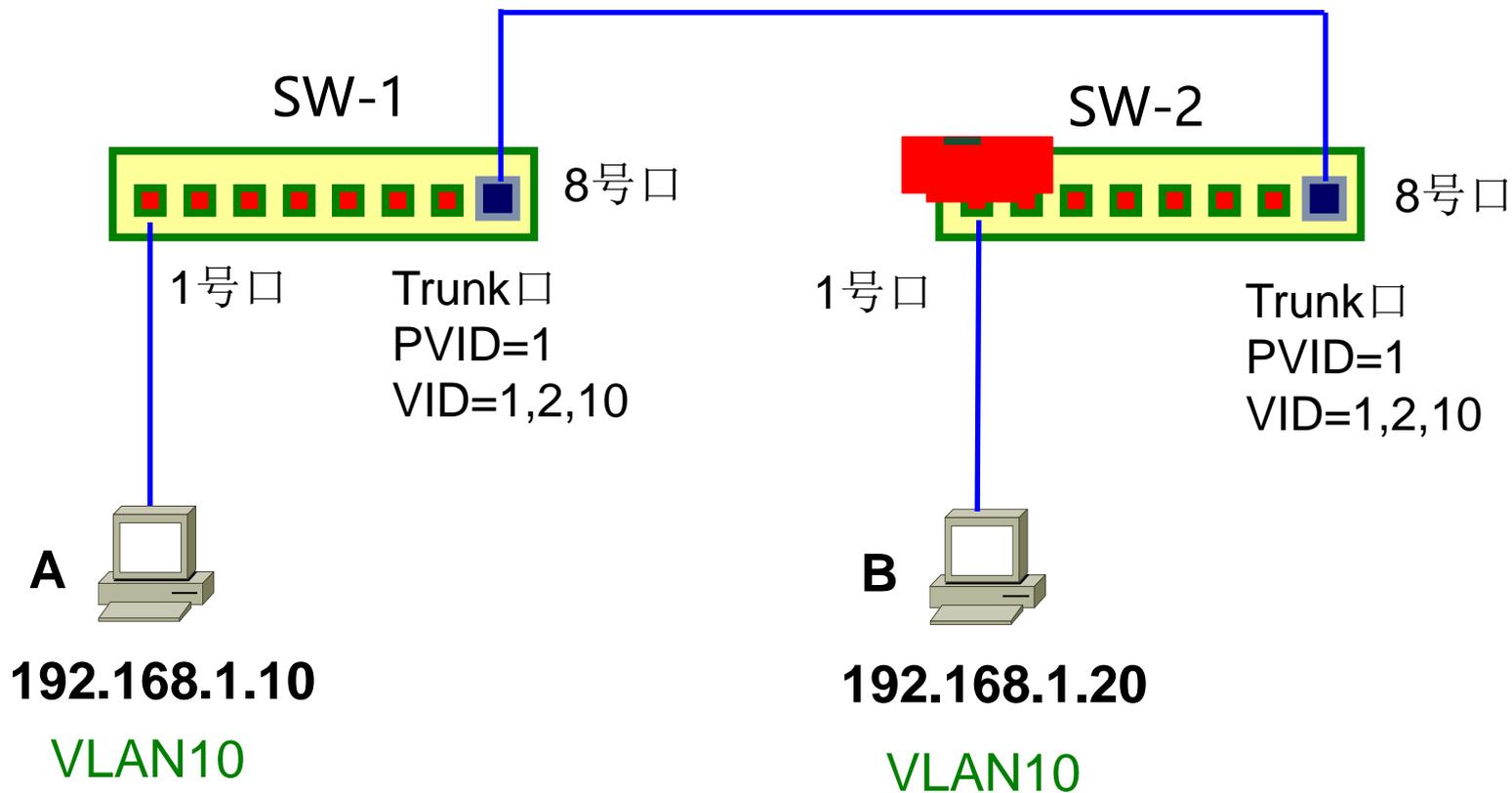
➤ 该tagged帧被转发至SW-1的8号口，由于8号口是Trunk口，且允许VLAN10的帧通过，且8号口PVID≠该帧的VID，因此，该帧被从8号口直接发出，不去掉标签。



- SW-2的8号口收到该tagged帧，由于8号口是Trunk口，因此8号口不去掉该帧的VLAN标签，直接将其转发至VLAN10的接口，通过查询MAC地址表，将其发送到1号口。



➤ 该tagged帧从1号口发出，由于1号口是Access口，因此该tagged帧发出时，被去掉VLAN标签，变成普通帧，到达PC-B。



4. 三层交换机的应用

三层交换机

主要用途： 实现VLAN间互访

SVI接口： 交换机三层虚拟接口，VLAN的默认网关

工作特点： 一次路由、多次交换

部署： 汇聚、核心

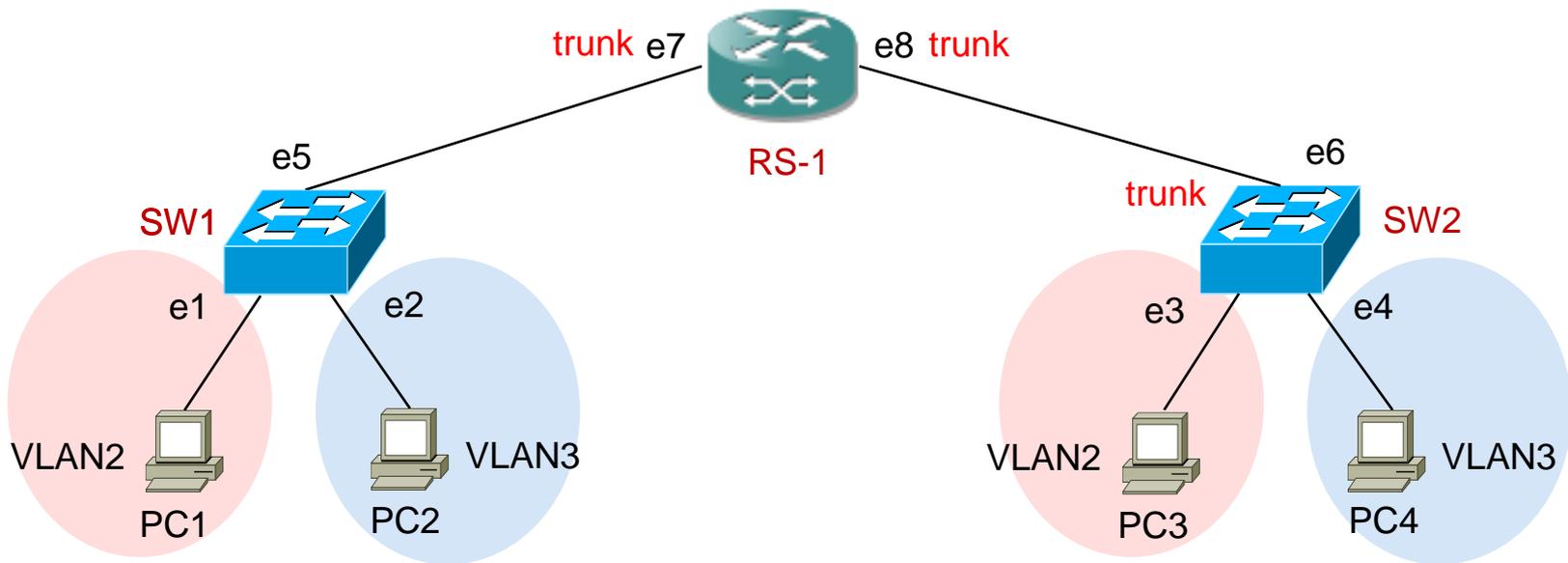


➤ 在三层交换机上配置三层虚拟接口，用作vlan 2 的默认网关

vlan 2

```
Interface vlanif 2
```

```
ip address 192.168.1.254 24
```

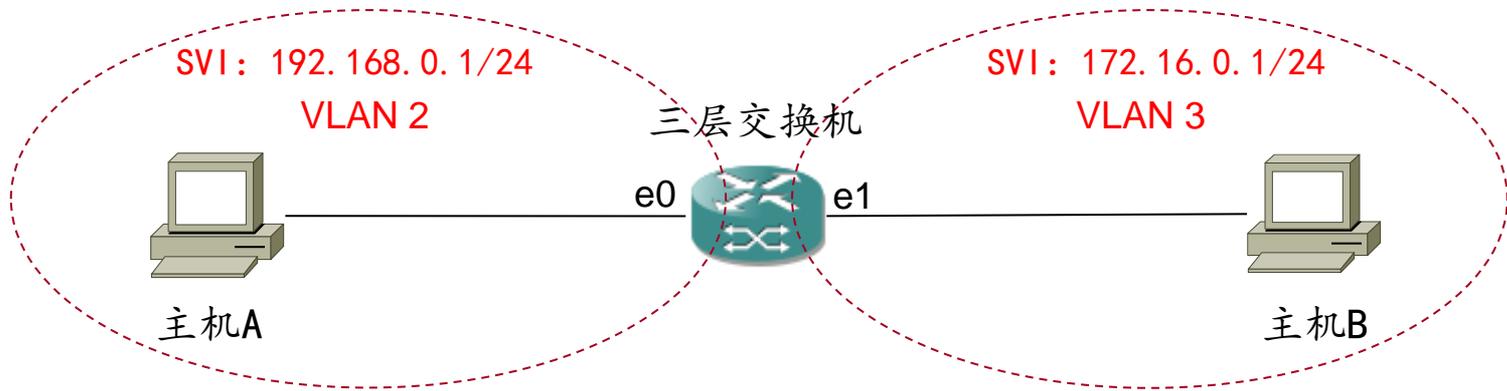


三层交换机组网

- 三层交换机的通信过程分析

 - 不同VLAN间主机通信

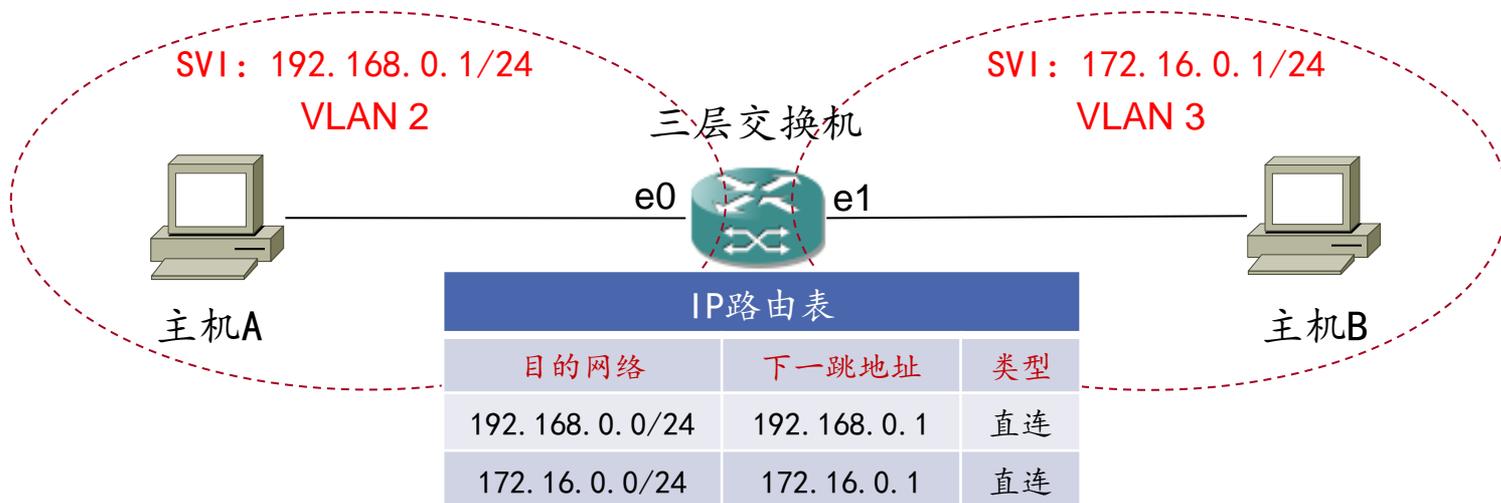
三层交换机的通信过程——不同VLAN间主机通信



➤ 网络拓扑说明：

- ① 三层交换机上创建了VLAN2、VLAN3，A属于VLAN2，B属于VLAN3；
- ② 在三层交换机上配置VLAN2和VLAN3的接口地址（即SVI地址），VLAN2接口的IP设置为192.168.0.1/24，VLAN3接口的IP设置为172.16.0.1/24

三层交换机的通信过程——不同VLAN间主机通信

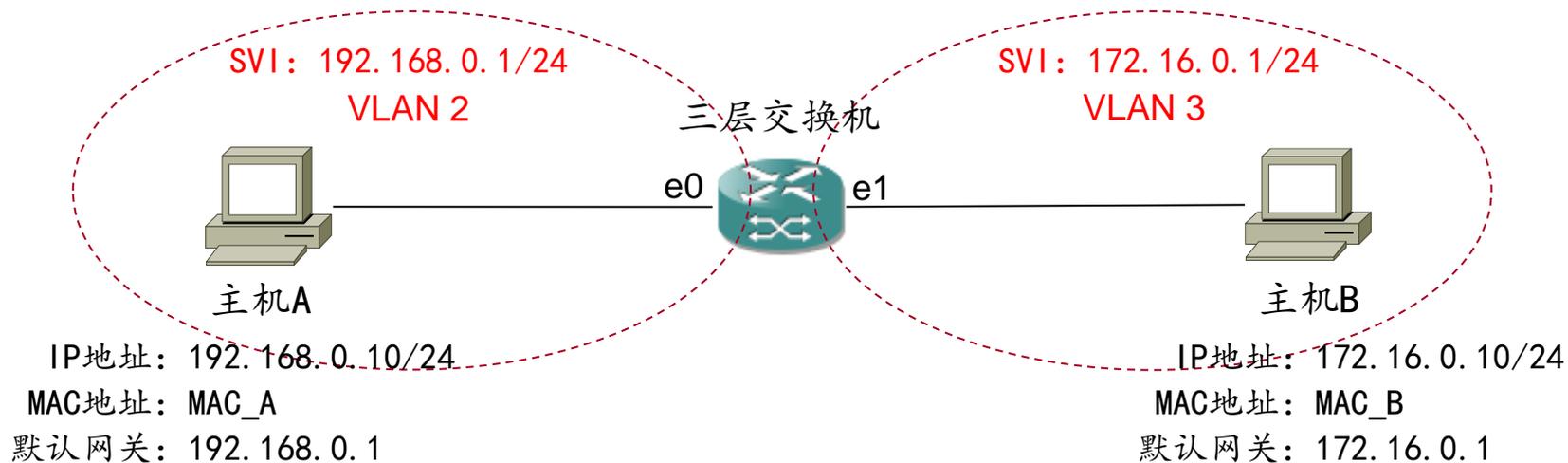


注意:

对于三层交换机来说,当配置完VLAN接口(SVI)地址后,三层交换机的IP路由表(软件路由表)中就有了相应的直连路由。



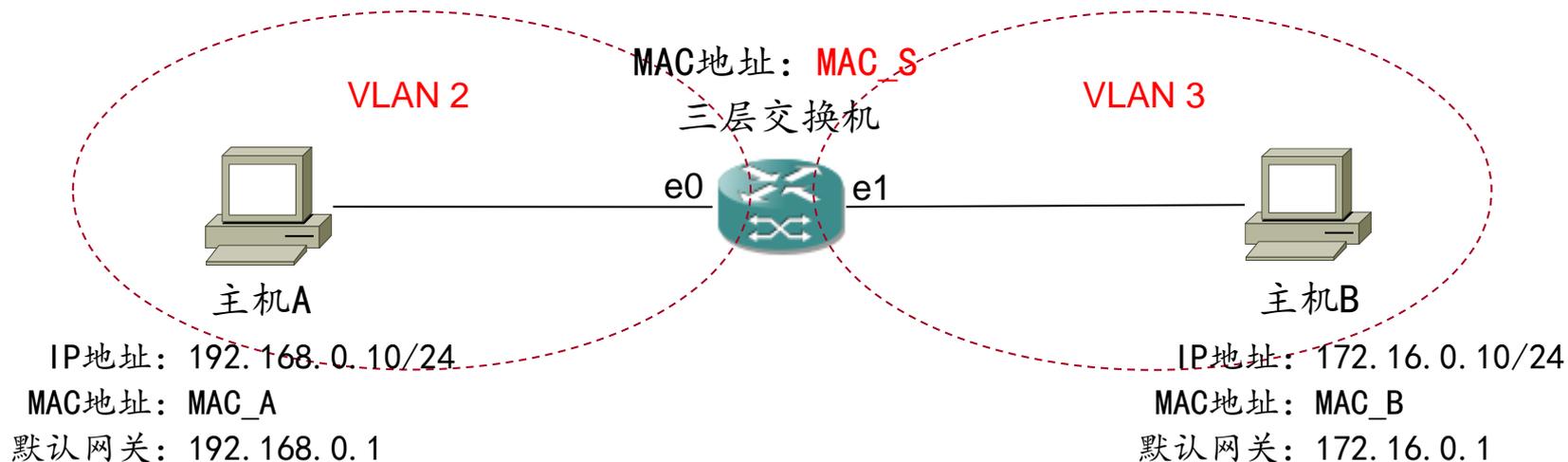
三层交换机的通信过程——不同VLAN间主机通信



➤ 网络拓扑说明:

- ③ 主机的IP地址和MAC地址如图所示，主机A的默认网关设置为三层交换机的VLAN2接口地址（192.168.0.1），主机B的默认网关设置为三层交换机的VLAN3接口地址（172.16.0.1）。

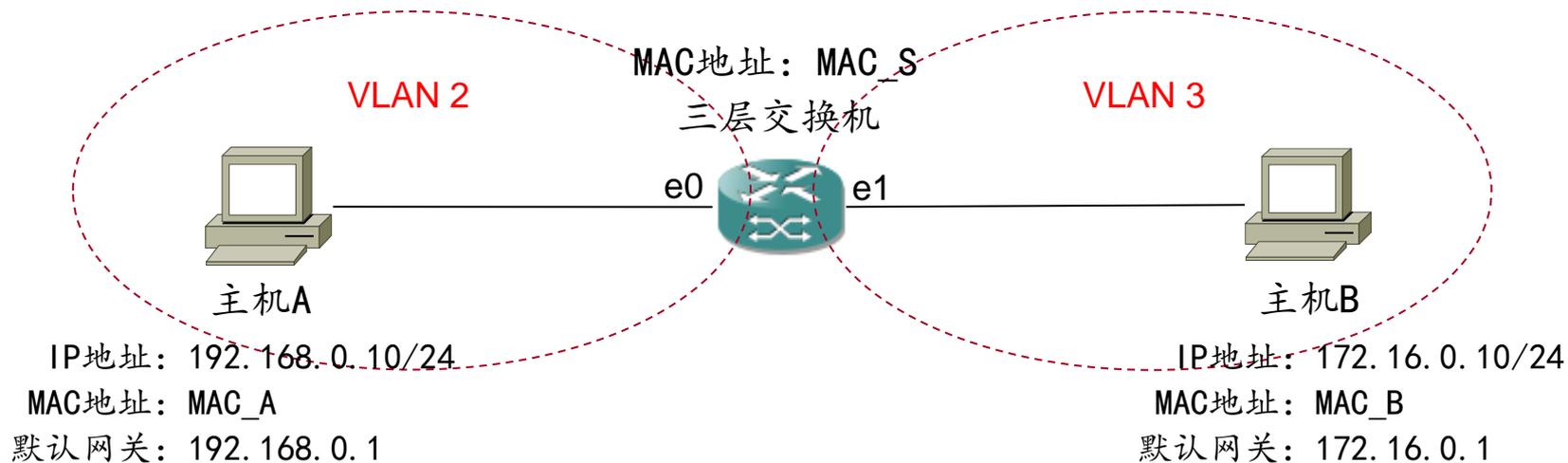
三层交换机的通信过程——不同VLAN间主机通信



➤ 网络拓扑说明:

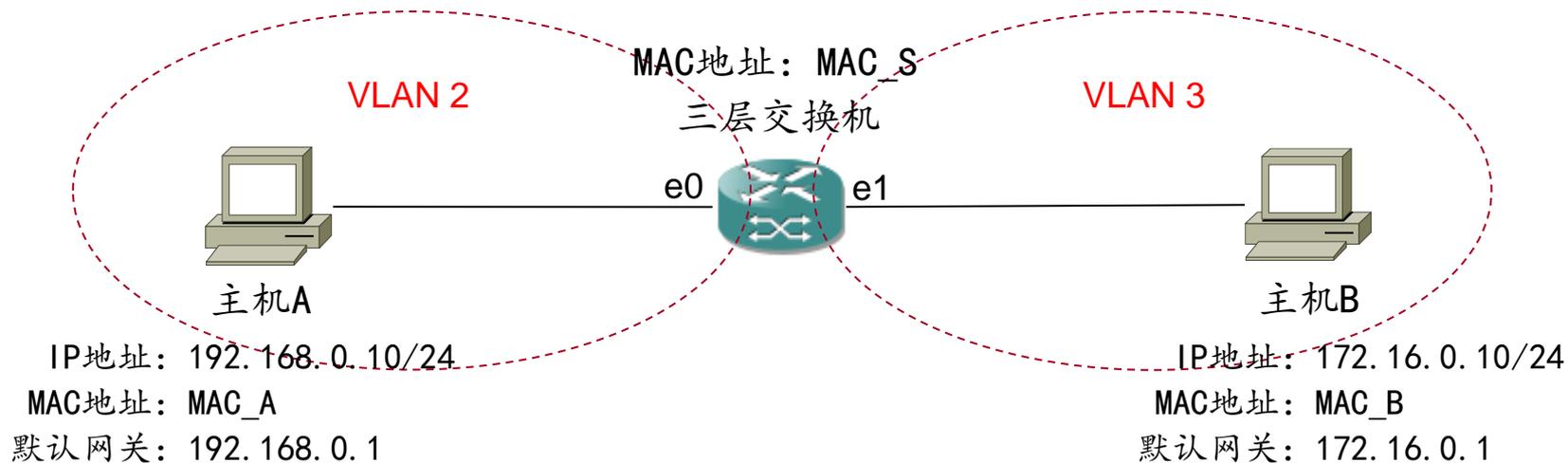
- ④ **注意:** 三层交换机上各接口、各VLAN接口通常是共享一个MAC地址的, 此处设为MAC_S。即VLAN2接口的MAC地址与VLAN3接口的MAC地址都是MAC_S。

三层交换机的通信过程——不同VLAN间主机通信



主机A Ping 主机B (第一次)

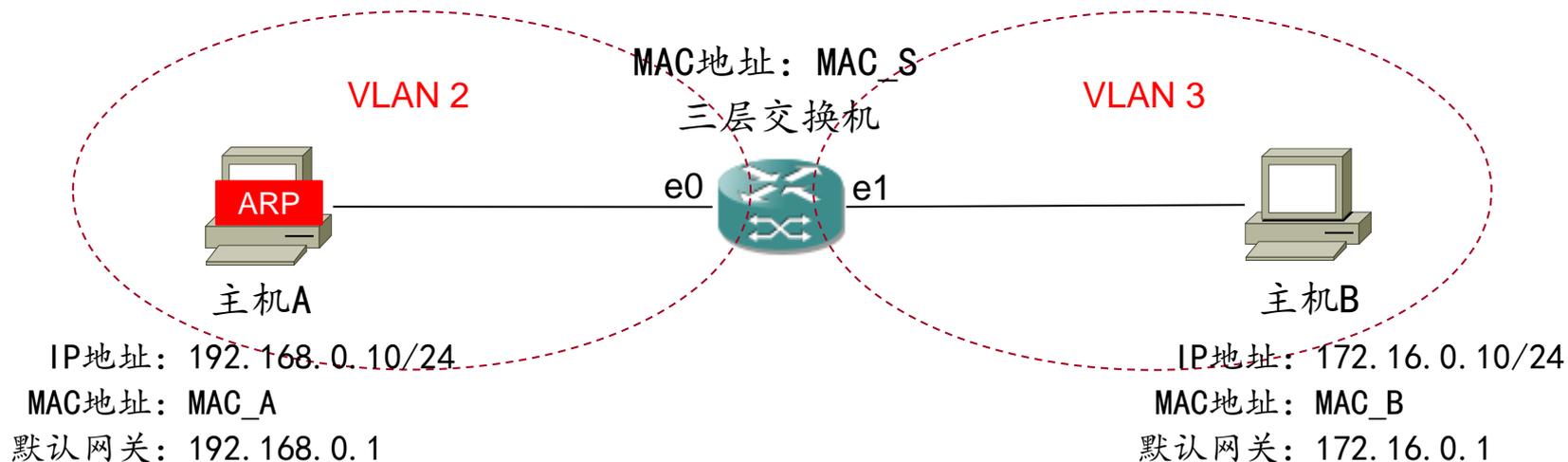
三层交换机的通信过程——不同VLAN间主机通信



1. 主机A → 默认网关 (ARP请求)

主机A发现目的IP (主机B的IP) 与自己不在同一网段, 于是要先把数据包发给自己的默认网关 (即三层交换机上VLAN2的SVI)。但是, 主机A此时不知道默认网关的MAC地址。

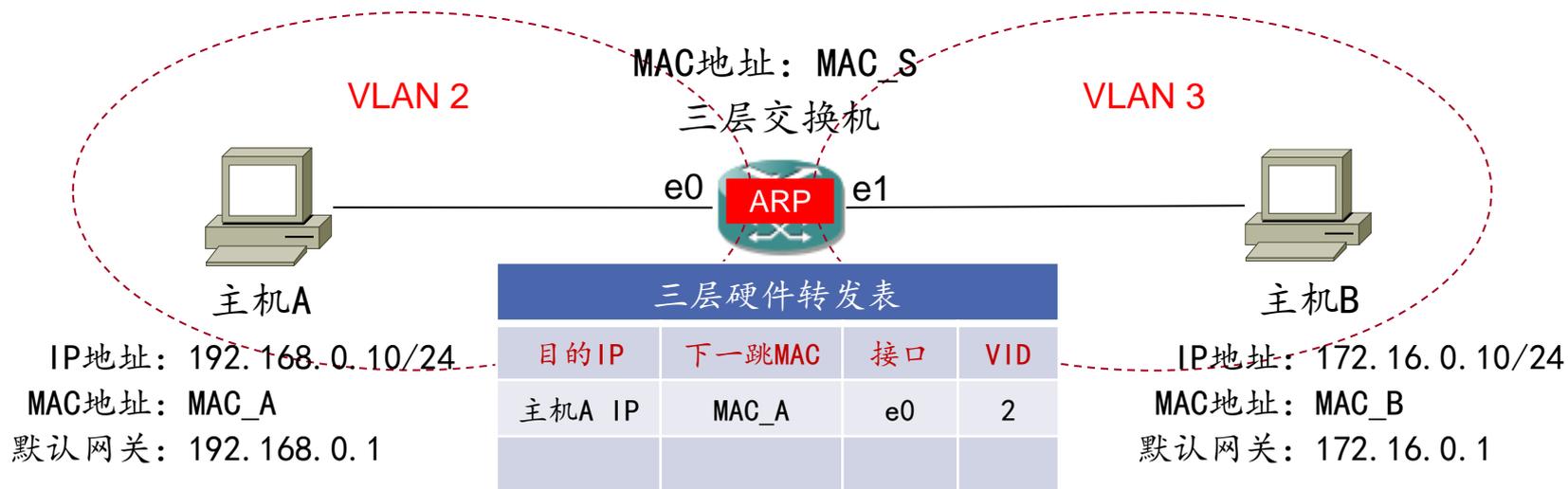
三层交换机的通信过程——不同VLAN间主机通信



1. 主机A → 默认网关 (ARP请求)

于是, 主机A发出ARP请求 (寻找默认网关的MAC地址), ARP报文中, 源MAC是MAC_A, 目的MAC是ff-ff-ff-ff-ff-ff, VLAN2内所有节点都收到了ARP请求, 包括三层交换机的VLAN2接口 (SVI虚拟接口)。

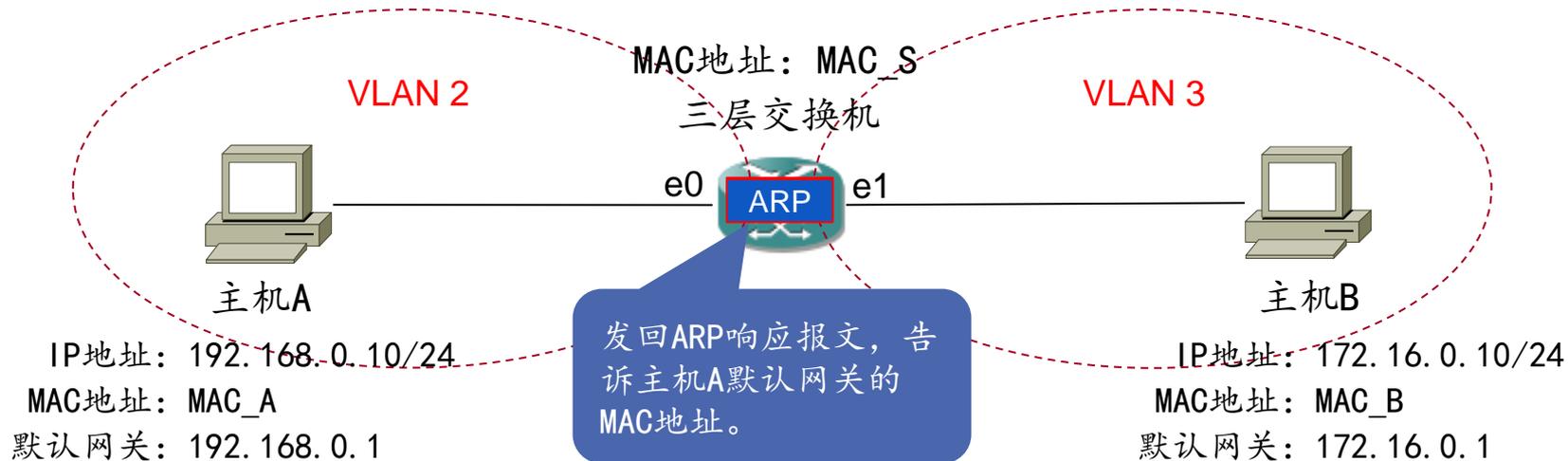
三层交换机的通信过程 —— 不同VLAN间主机通信



2. 三层交换机的处理 —— 在三层硬件转发表中添加主机A的记录

三层交换机收到主机A发来的ARP请求后，发现是给自己的VLAN2接口（SVI）的，于是就收下，并且把主机A的IP地址、MAC地址、接入交换机的接口号、VLAN ID信息，添加到三层交换机ASIC芯片中的三层硬件转发表。此时在三层硬件转发表中就有了第一个转发表项，即主机A的转发表项。

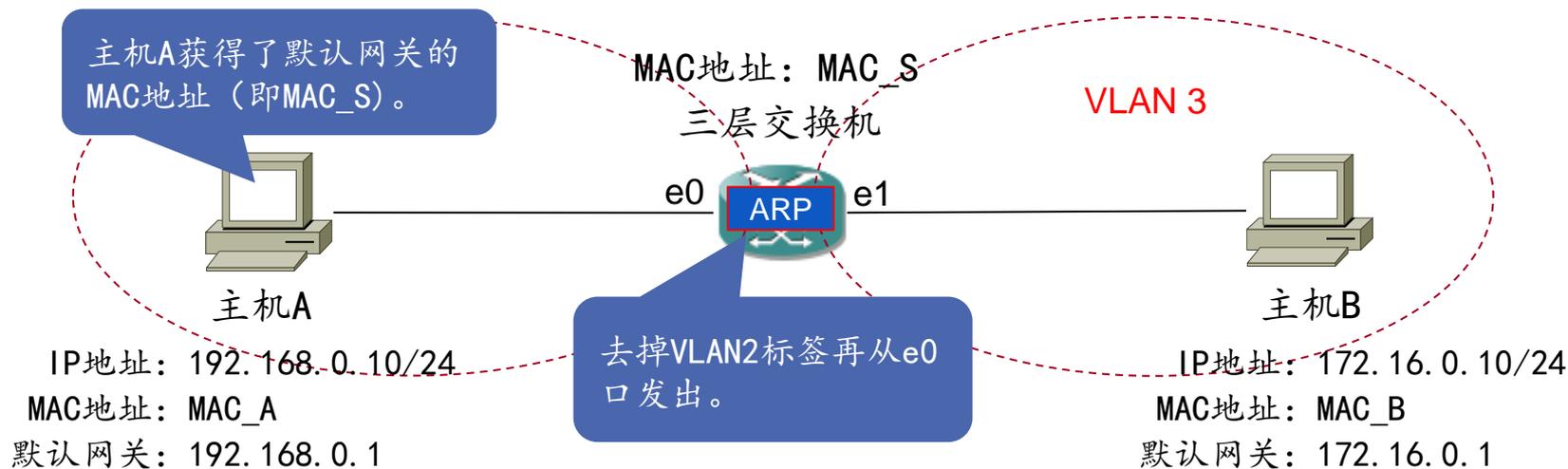
三层交换机的通信过程 —— 不同VLAN间主机通信



3. 三层交换机的处理 —— 向主机A发回ARP响应

同时, 由于e0接口是Access接口, 所以收下该报文时还要添加VLAN2标签, 然后, 三层交换机还要向主机A发回一个ARP响应报文, 在封装该报文时, 将MAC_A作为目的MAC, 将VLAN2接口的MAC (即MAC_S) 作为源MAC地址。

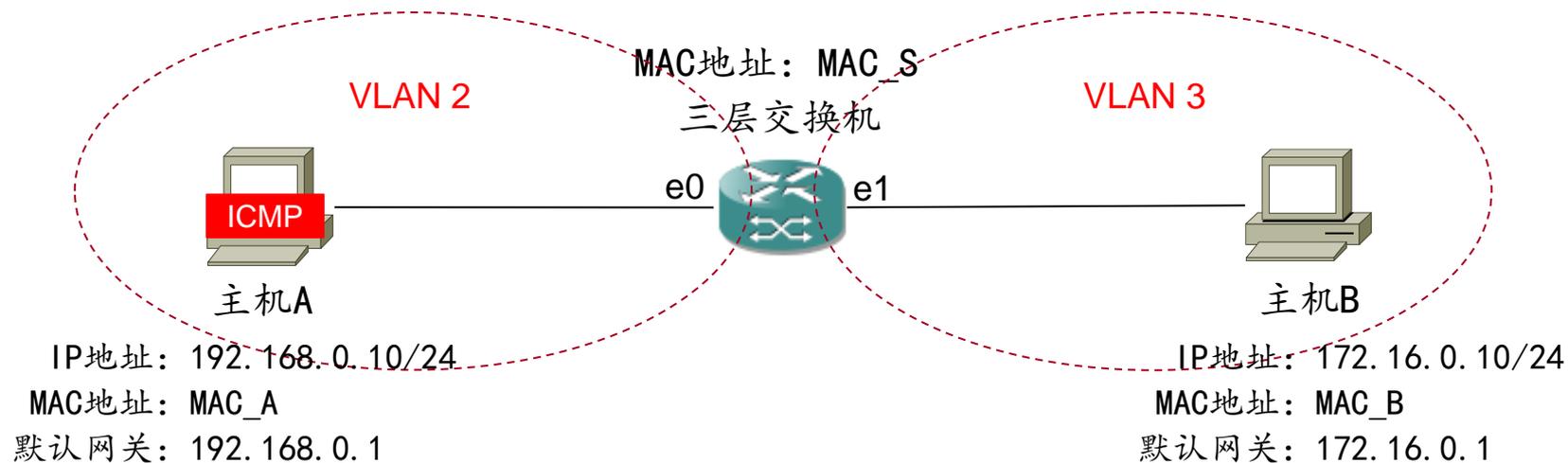
三层交换机的通信过程 —— 不同VLAN间主机通信



3. 三层交换机的处理 —— 向主机A发回ARP响应

注意，此处三层交换机在封装ARP响应报文时，可以理解为是交换机中的VLAN2接口在封装报文，因此在进行数据帧封装时，VLAN2标签保持不变，但是，由于此例中e0接口是Access接口，所以从e0口发出时会去掉VLAN标签然后发出，最终到达主机A。

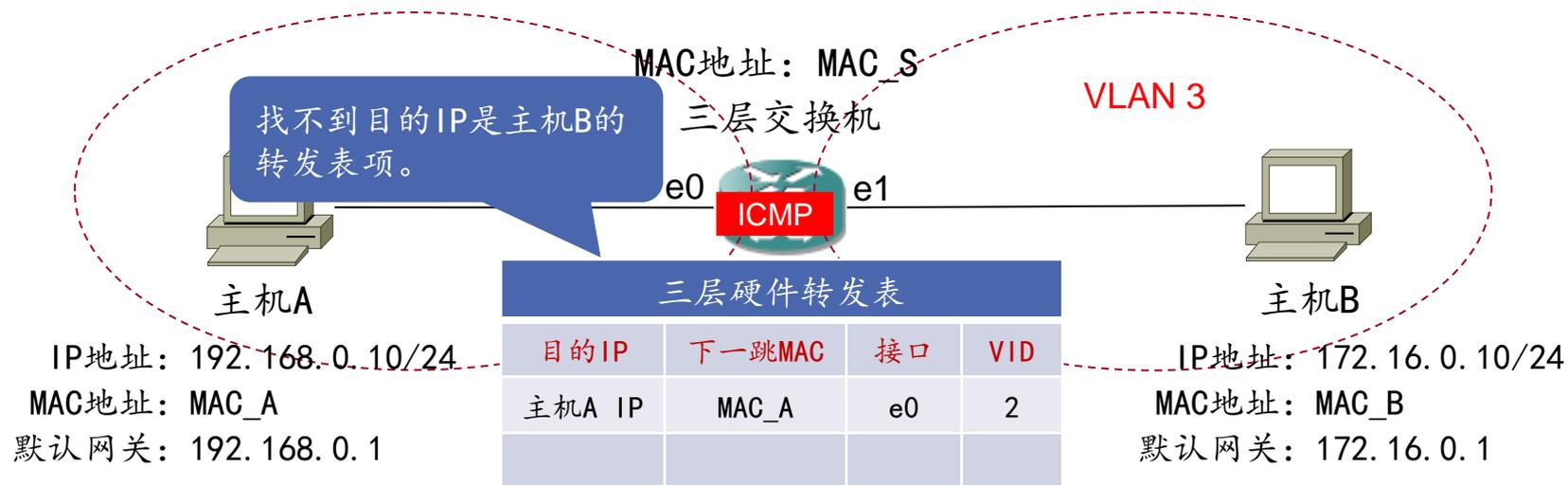
三层交换机的通信过程——不同VLAN间主机通信



4. 主机A → 默认网关 (ICMP请求)

主机A获得默认网关的MAC地址后, 就可以进行后续的ICMP报文发送了。首先封装要发给主机B的ICMP请求报文, 注意, 报文中的源IP是主机A的IP, 目的IP是主机B的IP, 源MAC是MAC_A, 目的MAC是默认网关的MAC (即MAC_S)。然后将ICMP请求报文发给默认网关。

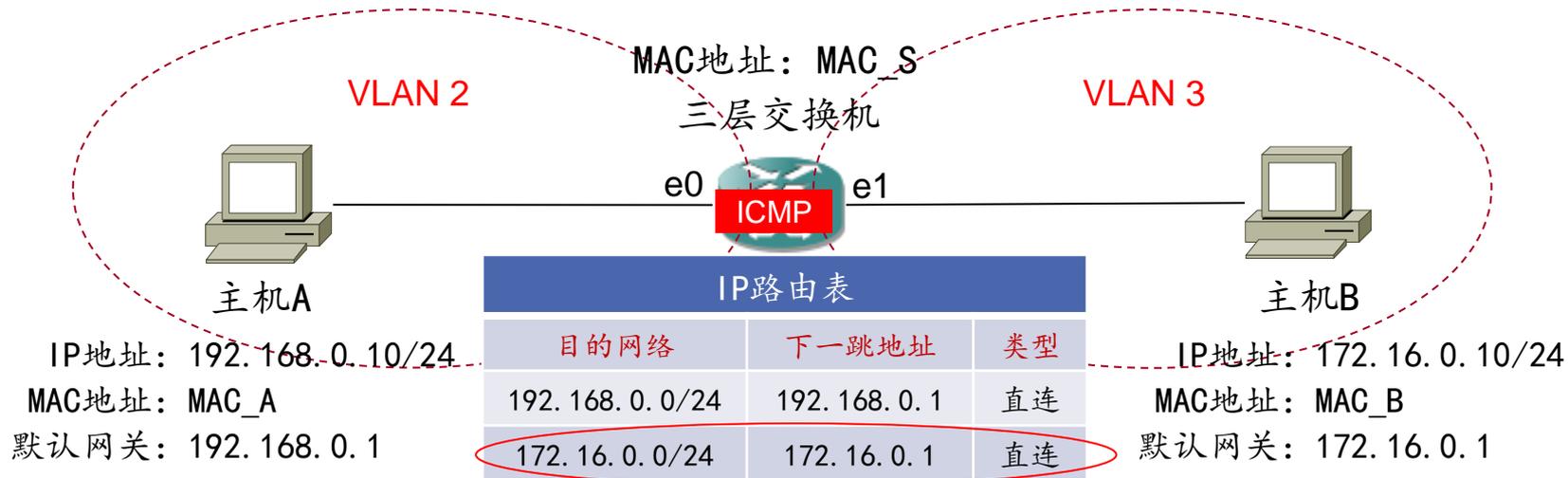
三层交换机的通信过程——不同VLAN间主机通信



5. 三层交换机的处理——查找三层硬件转发表（硬件转发）

三层交换机收下这个数据包（因为目的MAC=MAC_S），进一步分析发现，源IP与目的IP不在同一网段，于是首先提交给负责三层转发的ASIC芯片，根据数据包中的目的IP地址（主机B的IP），在三层硬件转发表中查看有无对应表项。此处因为是第一次通信，所以查找失败。

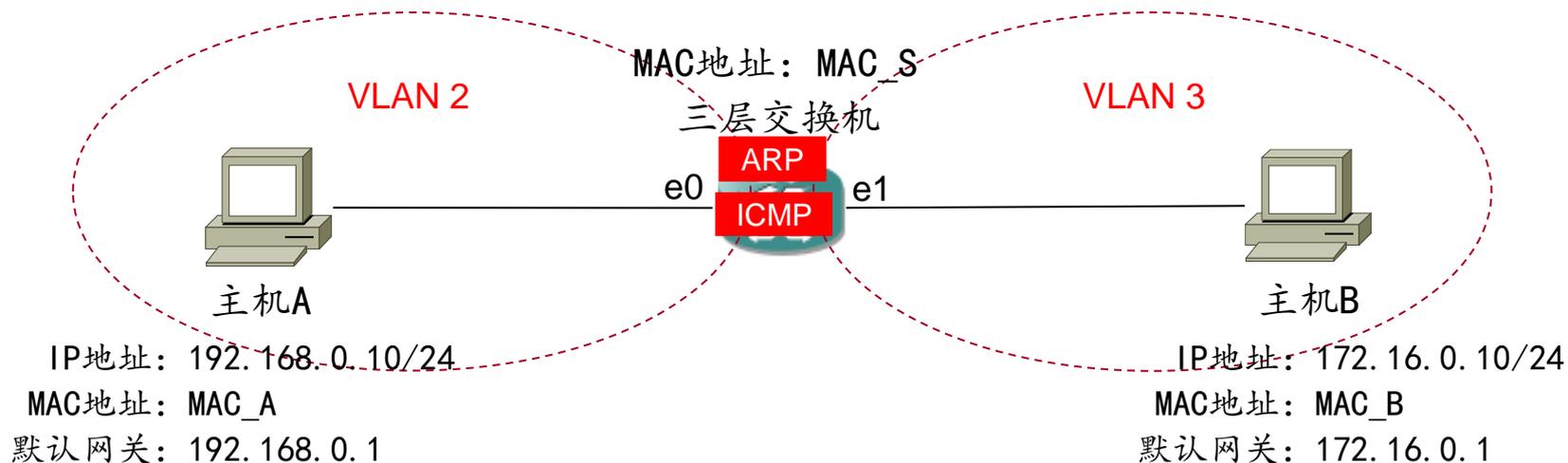
三层交换机的通信过程——不同VLAN间主机通信



6. 三层交换机的处理——查找IP路由表（软件路由）

由于三层硬件转发表中没有目的IP的对应表项，于是CPU会根据数据包中的目的IP地址（172.16.0.10），进一步查找IP路由表（软件路由表），发现匹配了一个直连网段（即VLAN3的网段），其下一跳是VLAN3的接口。于是，CPU依据直连路由，将数据包转给VLAN3接口。

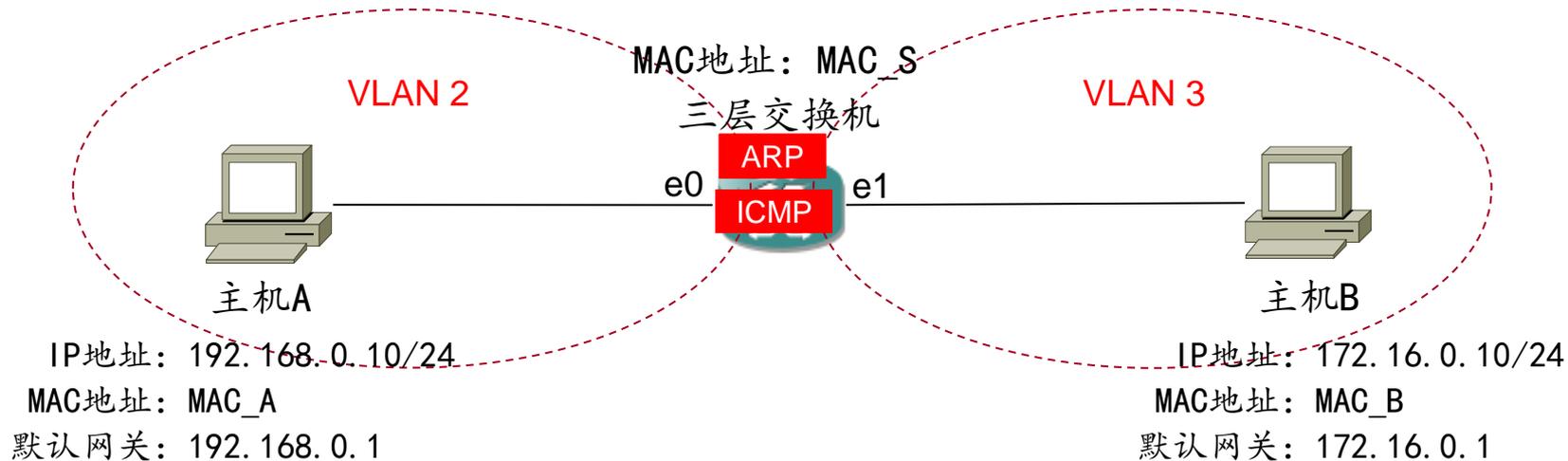
三层交换机的通信过程——不同VLAN间主机通信



7. 三层交换机的处理——向目的主机B发出ARP请求

由于目的主机B在三层交换机的直连网络中，因此三层交换机可以直接把ICMP请求报文转发给主机B。但是三层交换机发现自己当前并不知道主机B的MAC地址，于是向主机B发出ARP请求。此处三层交换机在封装ARP报文时，源MAC是MAC_S，目的MAC是ff-ff-ff-ff-ff-ff，即广播报文。

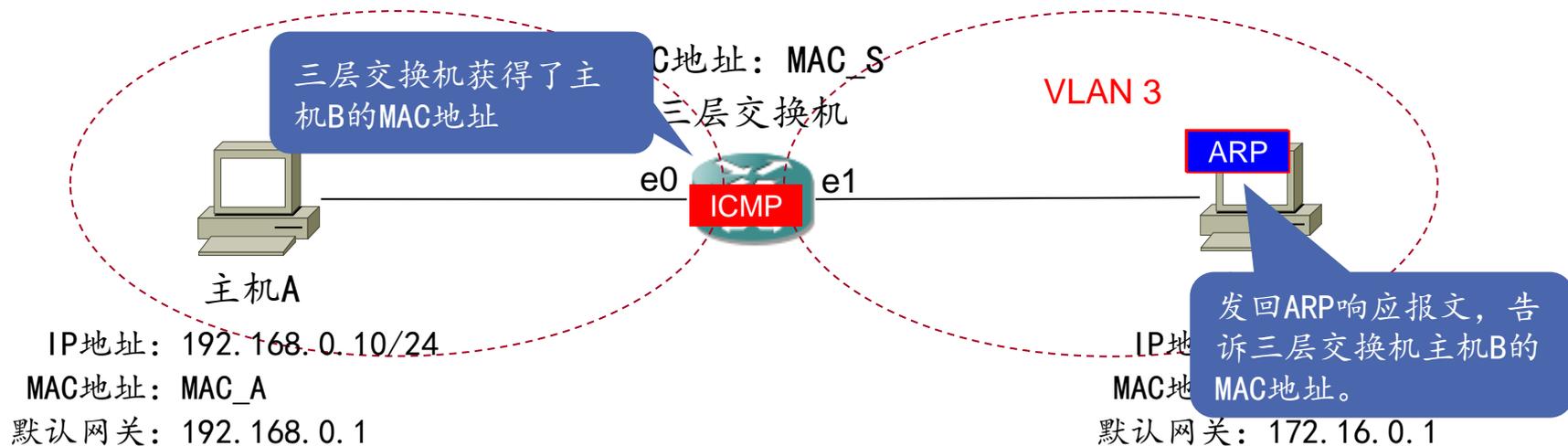
三层交换机的通信过程——不同VLAN间主机通信



7. 三层交换机的处理——向目的主机B发出ARP请求

注意，此处三层交换机在封装ARP报文时，可以理解为是交换机中的VLAN3接口在封装报文，因此在进行数据帧封装时，需要添加VLAN3的标签。即该ARP请求报文，将被广播发送至三层交换机上属于VLAN3的所有接口，包括主机B连接的e1接口。但由于此例中e1接口是Access接口，所以会去掉VLAN标签然后发出，最终到达主机B。

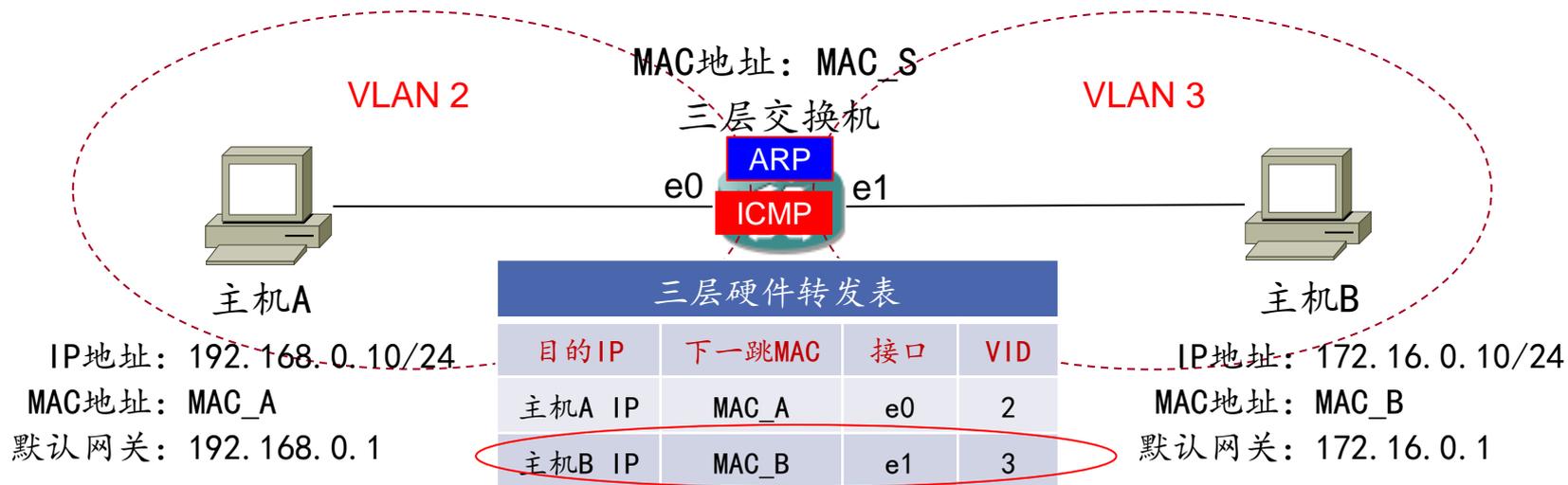
三层交换机的通信过程——不同VLAN间主机通信



8. 主机B → 三层交换机 (ARP响应)

主机B收下三层交换机VLAN3接口发来的ARP请求报文, 并发回ARP响应报文。在封装报文时, 将MAC_B作为源MAC, 将三层交换机VLAN3接口的MAC (即MAC_S) 作为目的MAC地址。然后发给三层交换机 (VLAN3接口)。

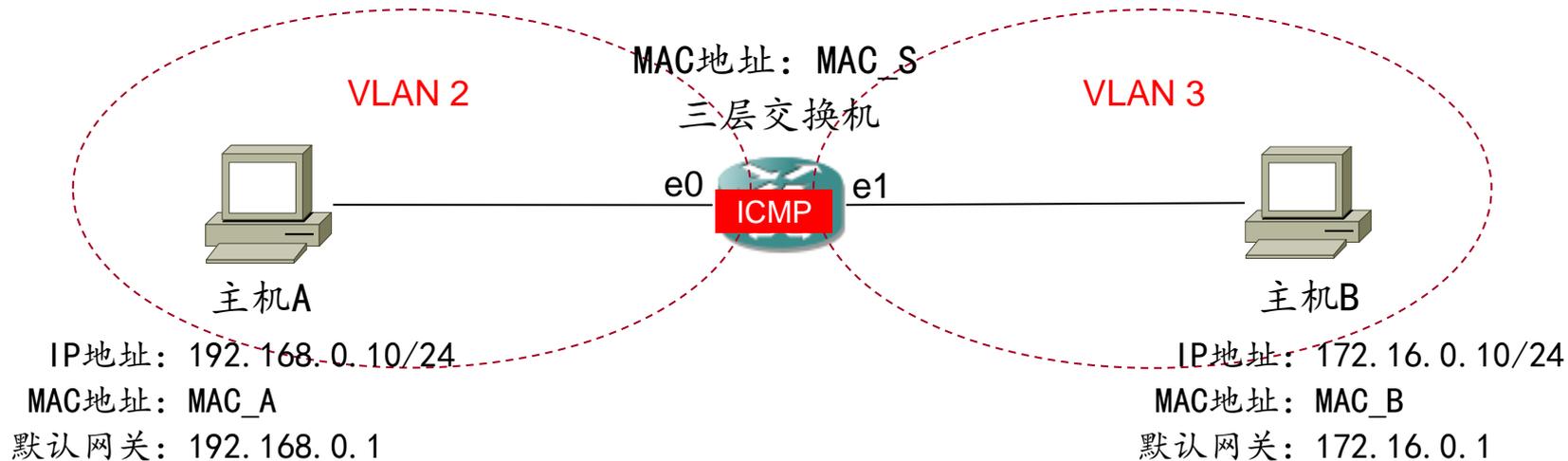
三层交换机的通信过程——不同VLAN间主机通信



9. 三层交换机的处理——在三层硬件转发表中添加主机B的记录

三层交换机收到主机B发来的ARP响应报文，并且把主机B的IP地址、MAC地址、接入交换机的接口号、VLAN ID信息，添加到三层交换机ASIC芯片中的三层硬件转发表。此时在三层硬件转发表中就有了第2个转发表项，即主机B的转发表项。

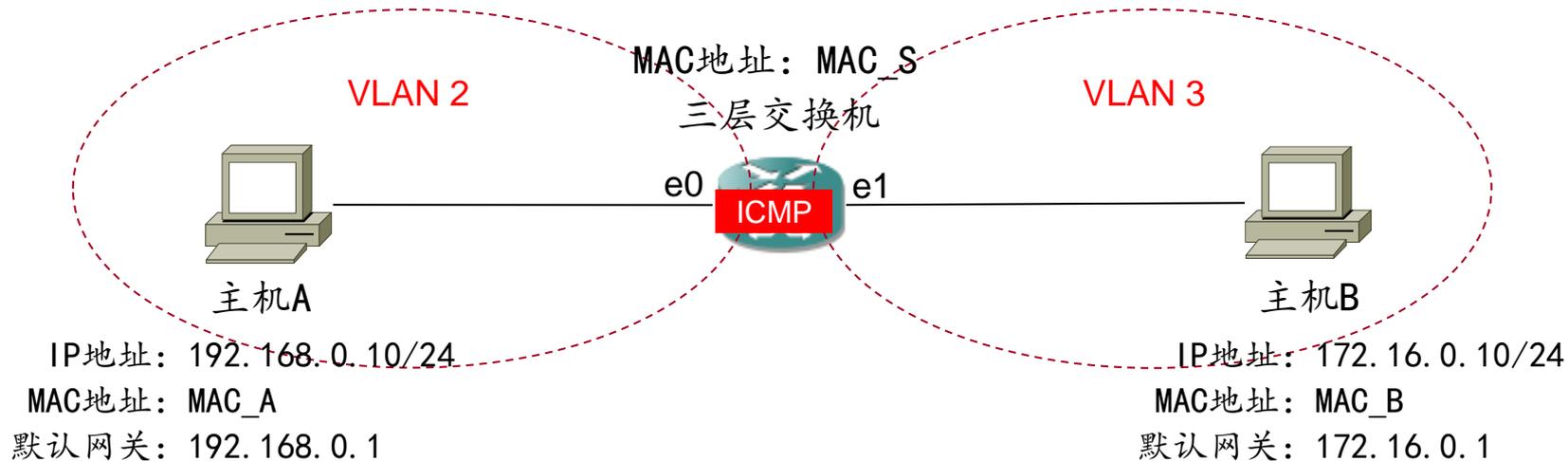
三层交换机的通信过程——不同VLAN间主机通信



10. 三层交换机的处理——向主机B发送ICMP请求报文

此时，三层交换机已经知道主机B的MAC地址。于是将主机A发来的ICMP请求报文（此时已经通过直连路由转发至VLAN3接口），重新封装，在封装时，源IP（主机A）和目的IP（主机B）保持不变，MAC_B为目的MAC，将VLAN3接口的MAC（即MAC_S）作为源MAC地址。

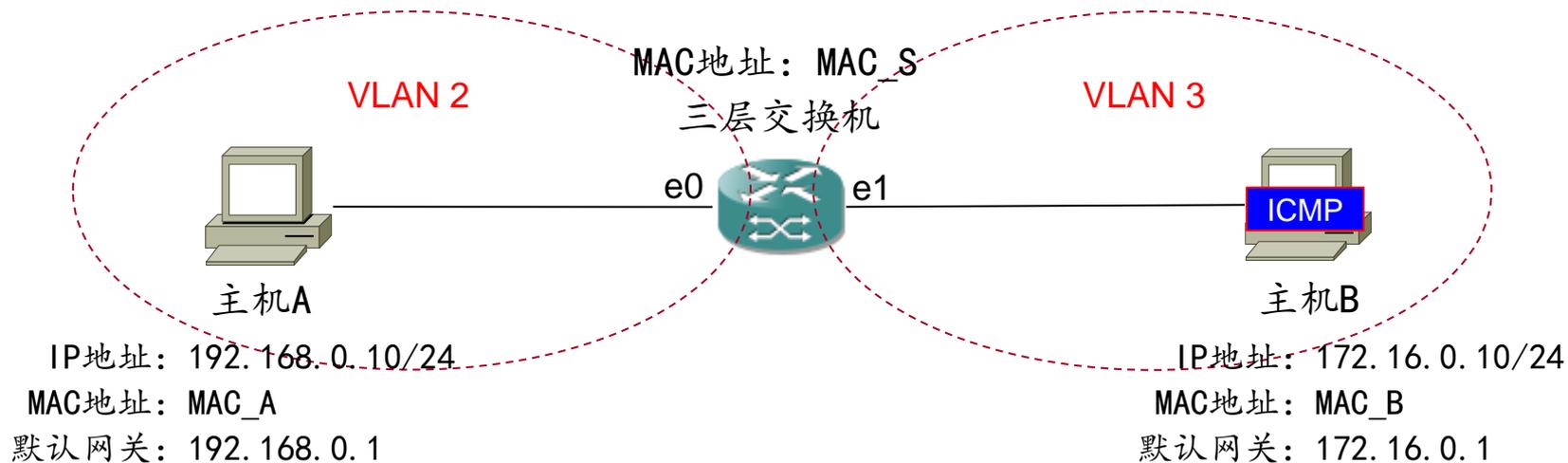
三层交换机的通信过程——不同VLAN间主机通信



10. 三层交换机的处理——向主机B发送ICMP请求报文

注意，此处三层交换机在封装报文时，可以理解为是交换机中的VLAN3接口在封装报文，因此在进行数据帧封装时，需要添加VLAN3的标签。但由于此例中e1接口是Access接口，所以会去掉VLAN标签然后发出，最终到达主机B。

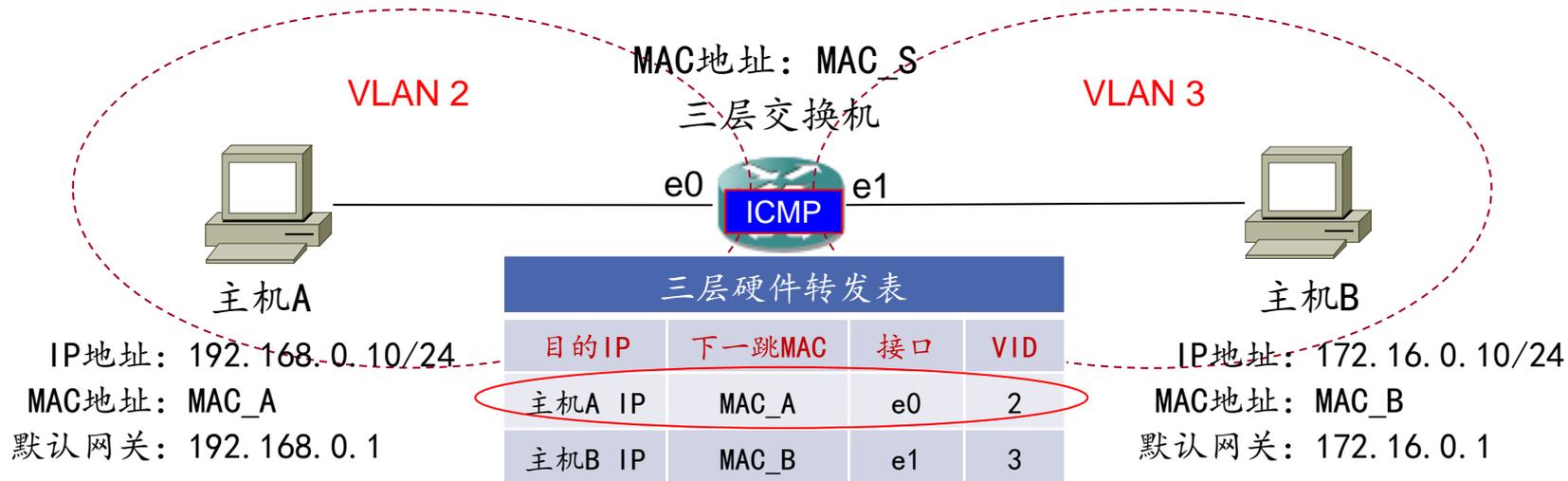
三层交换机的通信过程——不同VLAN间主机通信



11. 主机B → 三层交换机 (ICMP响应)

主机B向主机A发送ICMP响应报文。由于与主机A不在同一网段，主机B先把报文发给默认网关，即三层交换机中的VLAN3接口。主机B封装ICMP响应报文，其源IP为主机B的IP，目的IP为主机A的IP，源MAC为MAC_B，目的MAC为默认网关的MAC（即MAC_S），此时主机B已经知道默认网关的MAC地址。

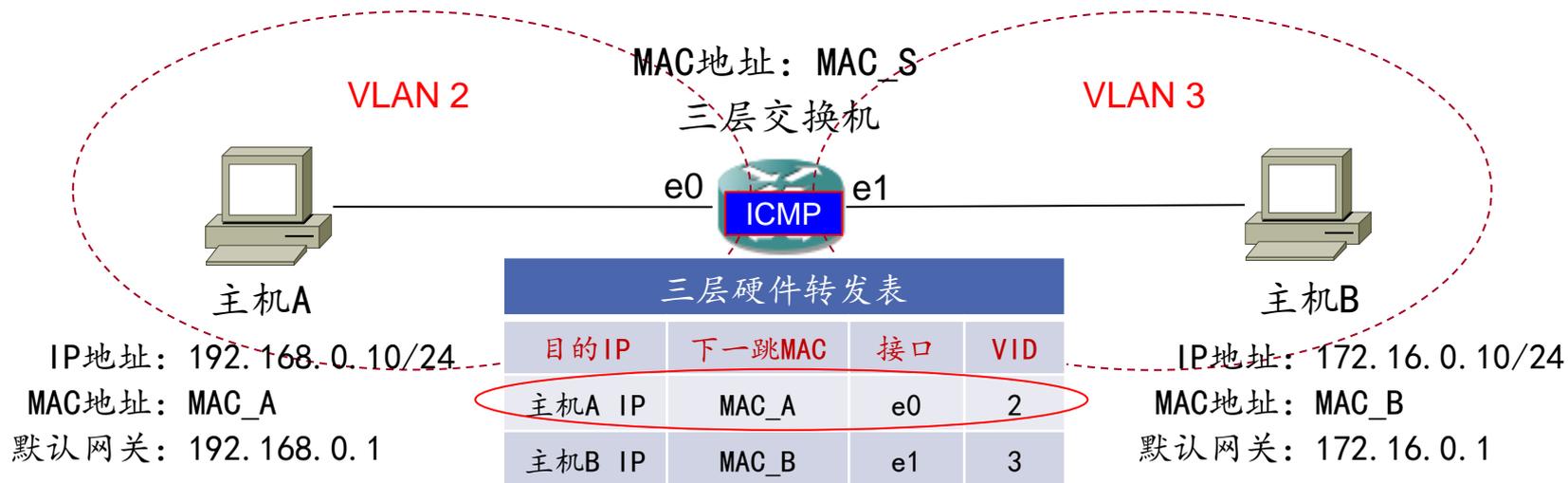
三层交换机的通信过程 —— 不同VLAN间主机通信



12. 三层交换机的处理 —— 查找三层硬件转发表（硬件转发）

数据包到达默认网关，三层交换机发现目的IP和源IP不在同一网段，此时它会先查看三层硬件转发表，发现有主机A的记录，于是直接依据三层硬件转发表进行转发（硬件转发），不再去查看IP路由表（软件路由）

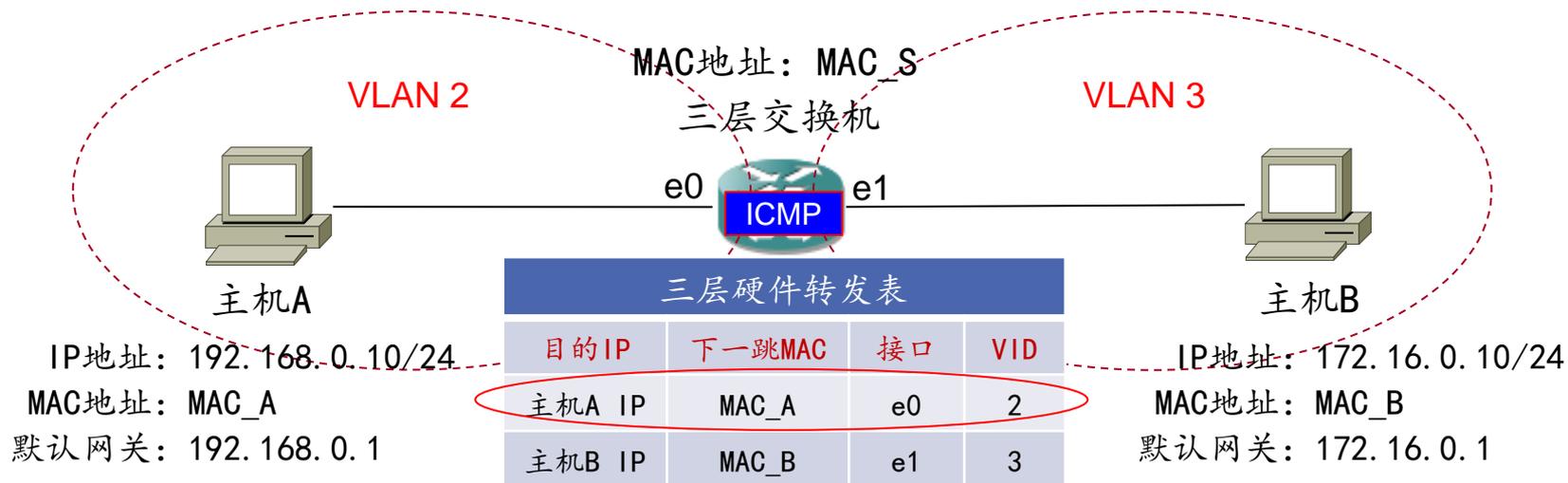
三层交换机的通信过程 —— 不同VLAN间主机通信



13. 三层交换机的处理 —— 重新封装ICMP响应报文

三层交换机在重新封包时，源IP（主机B）和目的IP（主机A）保持不变，源MAC为MAC_S，目的MAC为MAC_A（从三层硬件转发表中查到），并且数据帧头添加VLAN2的标签（从三层硬件转发表中查到）。

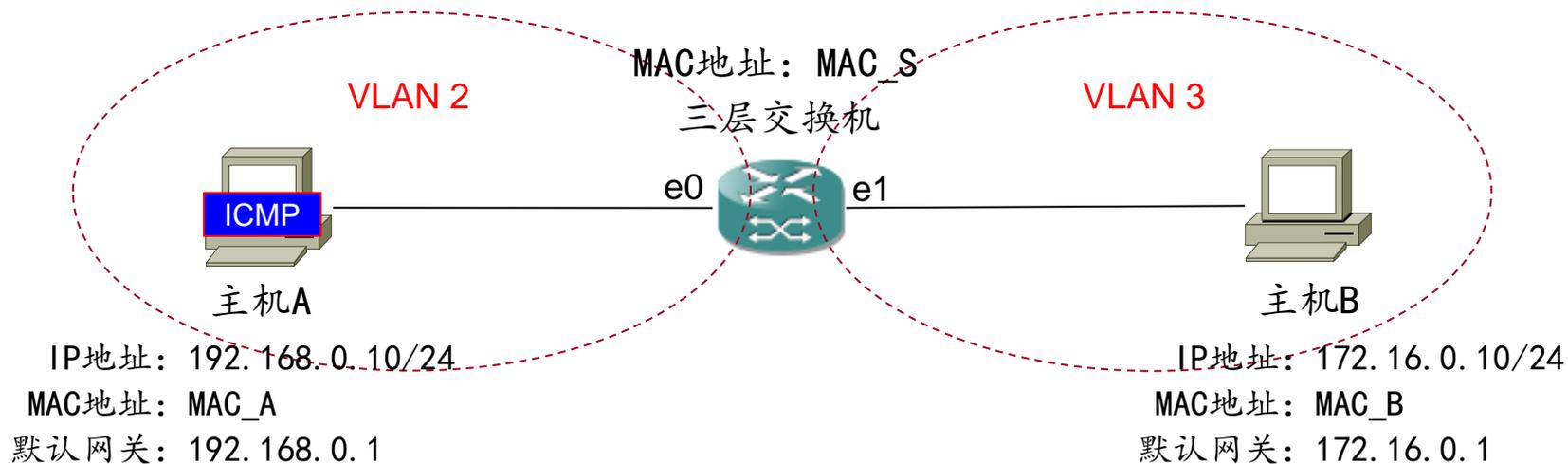
三层交换机的通信过程 —— 不同VLAN间主机通信



14. 三层交换机的处理 —— 向主机A发送封装好的ICMP响应报文

三层交换机将重新封装好的数据包，从e0接口发出（从三层硬件转发表中查到）。但由于此例中e0接口是Access接口，所以从e0接口发出前先去掉VLAN2标签然后发出，最终到达主机A。

三层交换机的通信过程——不同VLAN间主机通信



通信完成



5. 路由器实现网络互联

路由器
组网

用途: 网络互连

路由表: 目的网络、Proto、Pre、Cost、下一跳

路由器接口: 默认网关、下一跳

直连路由: 接口地址

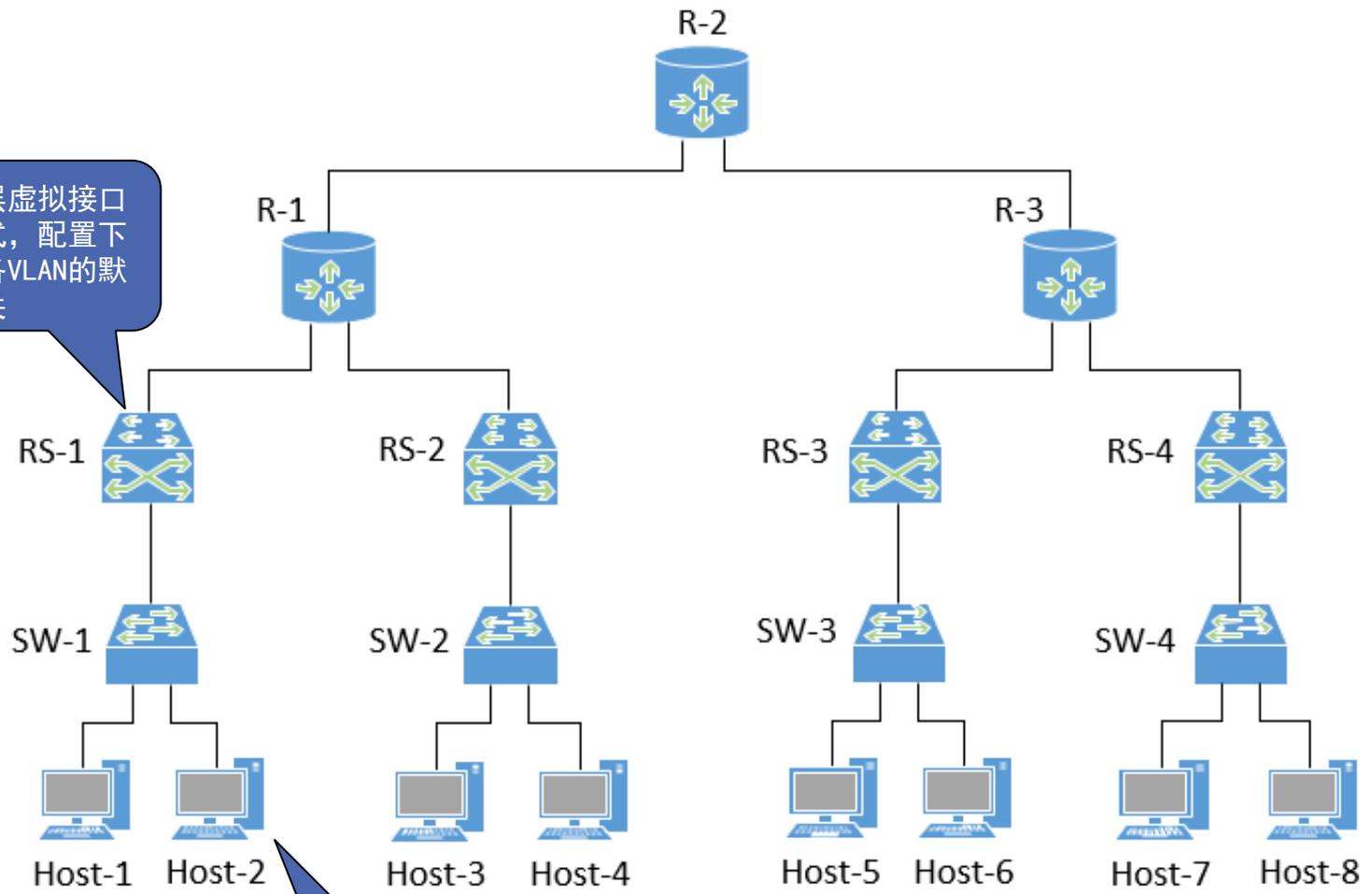
静态路由: 单向、固定、缺省路由

动态路由: 路由协议、RIP、OSPF

路由通信过程分析



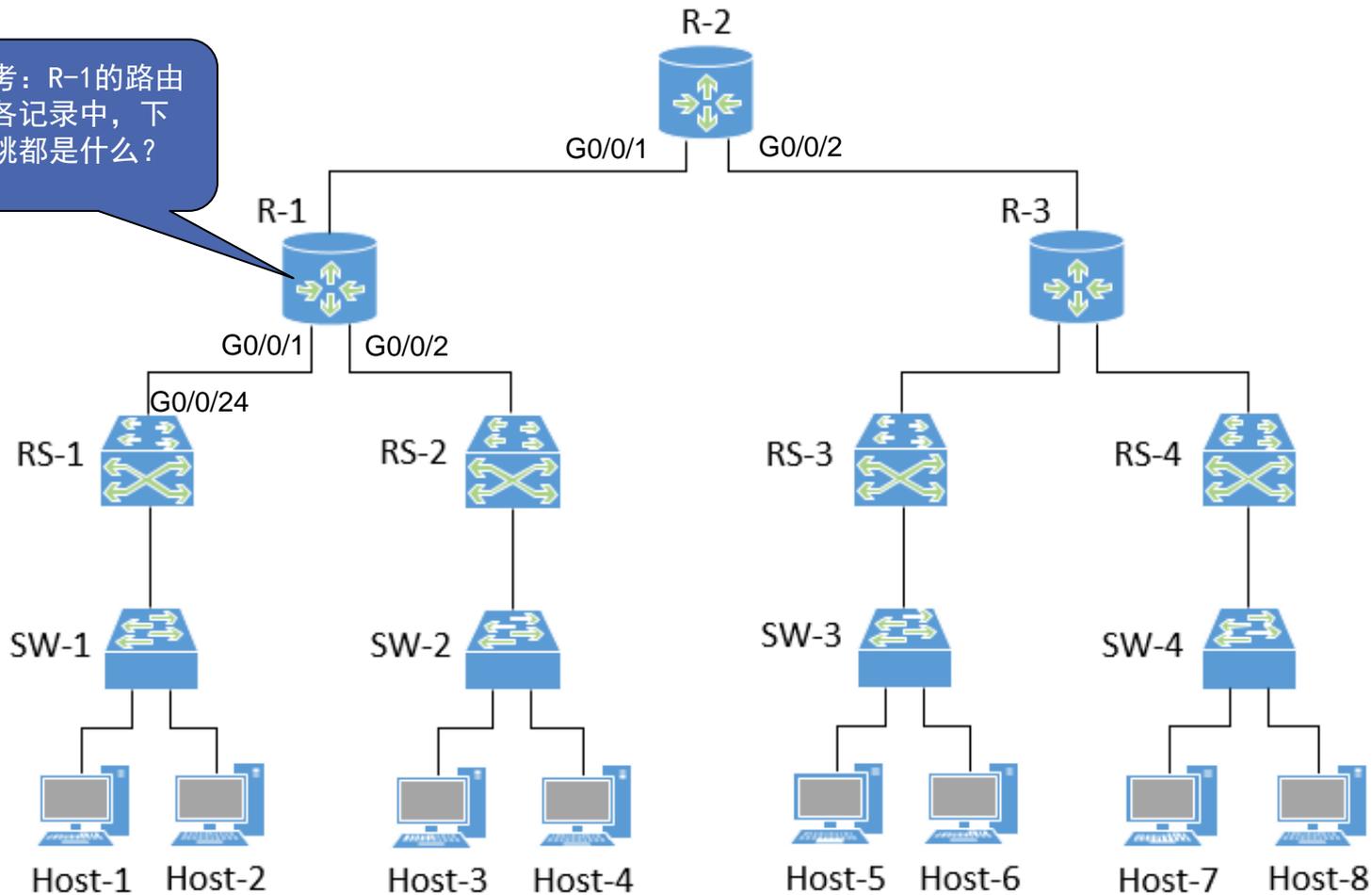
以三层虚拟接口的方式，配置下联的各VLAN的默认网关

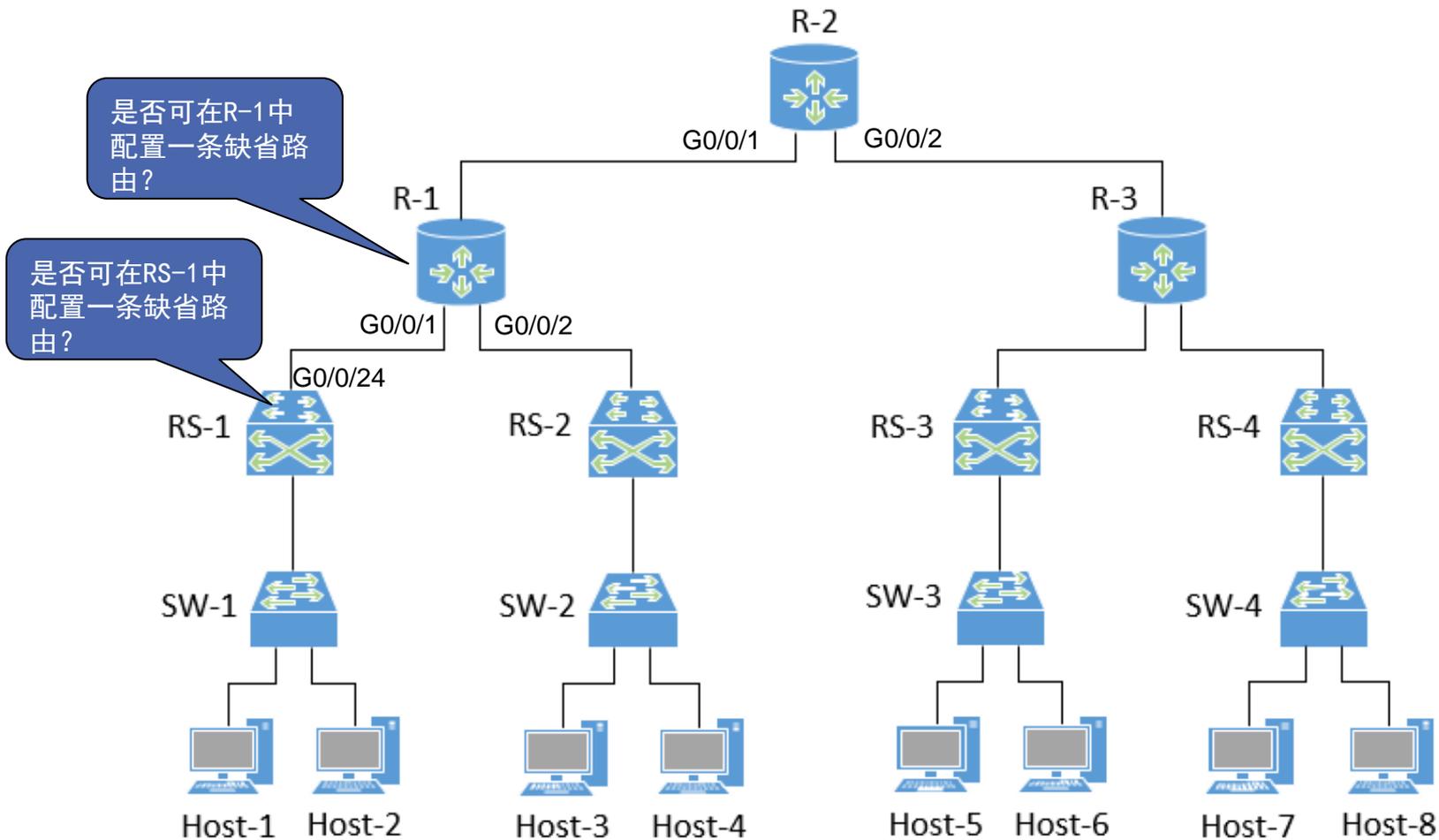


网关在哪？



思考：R-1的路由表各记录中，下一跳都是什么？

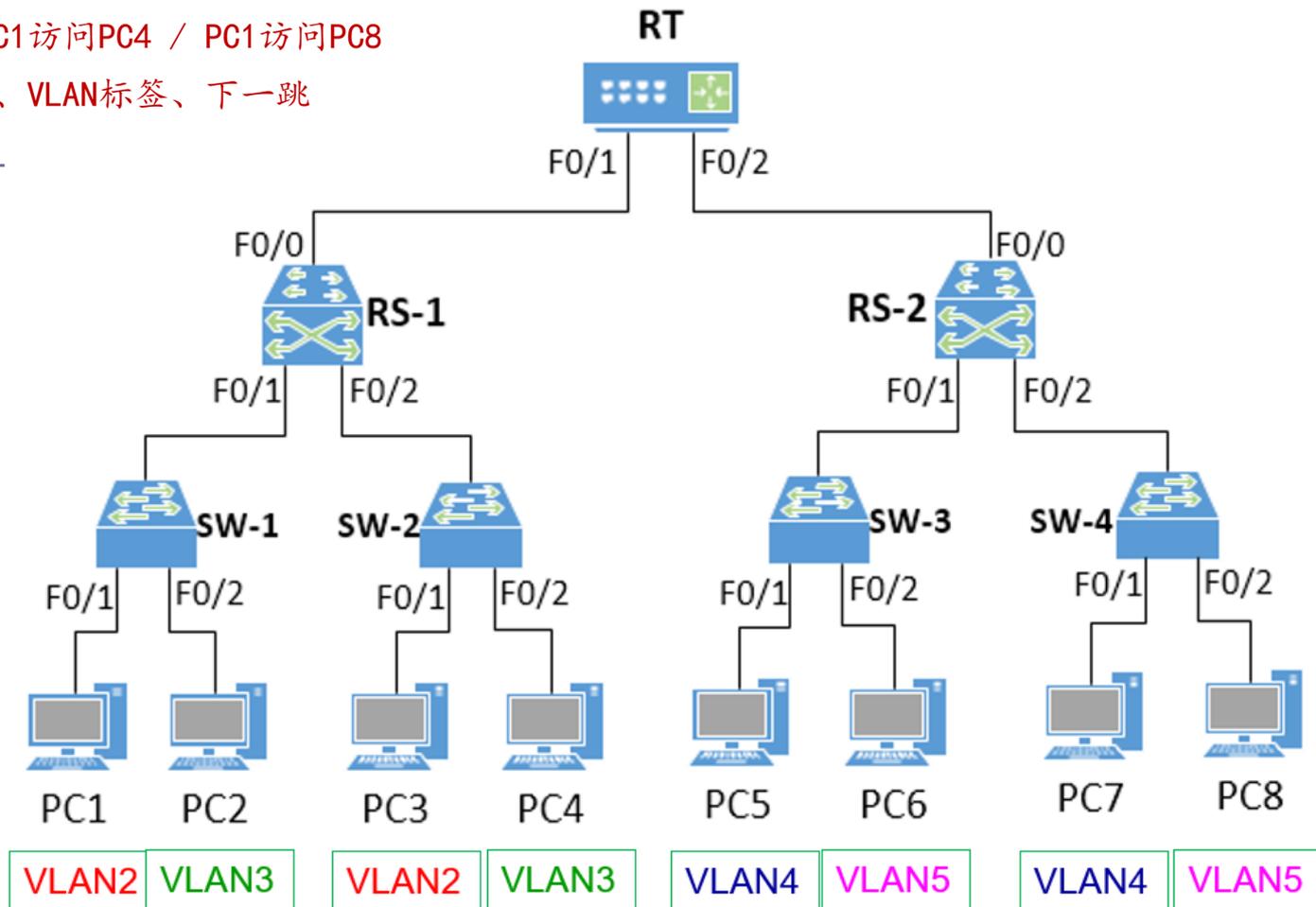


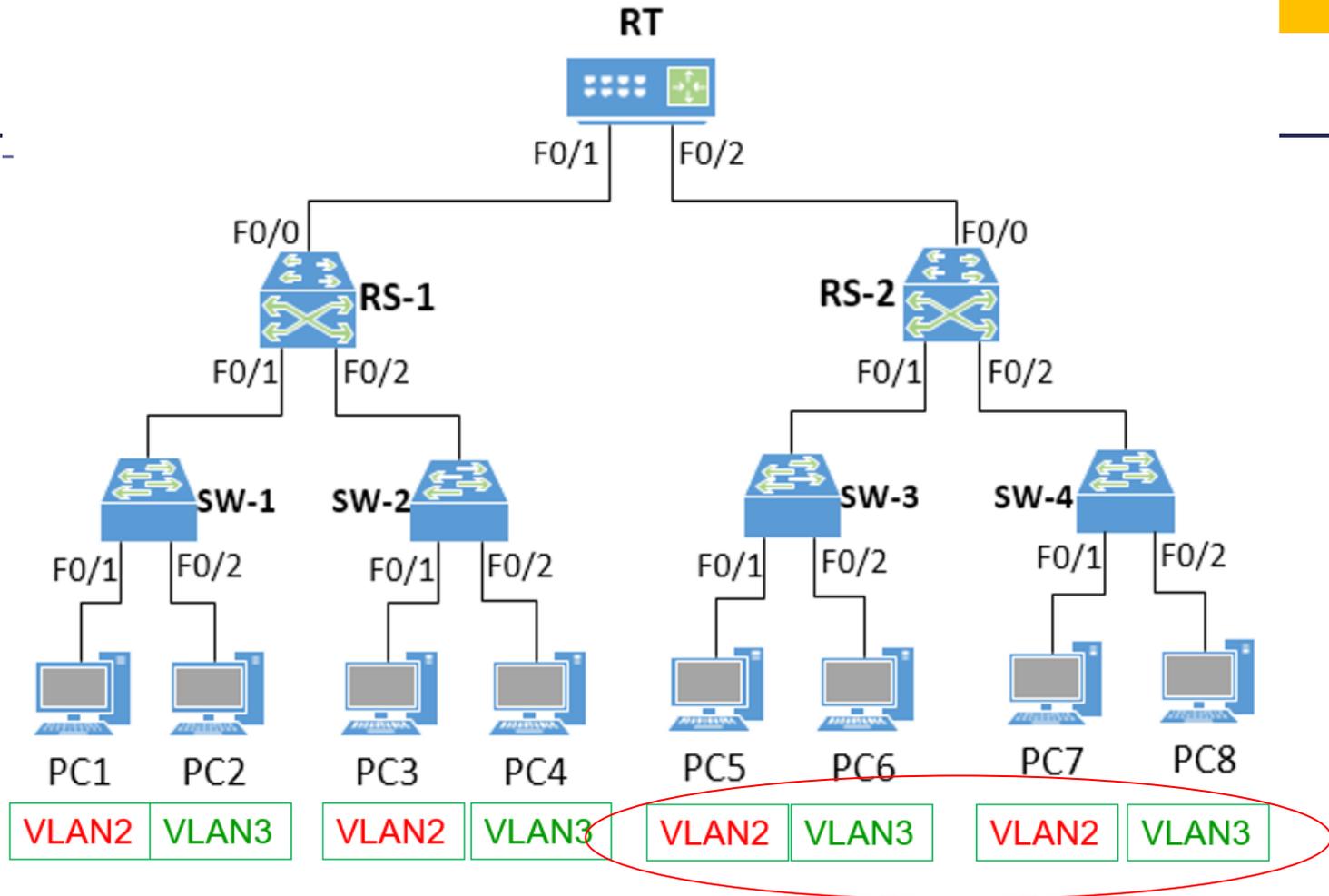


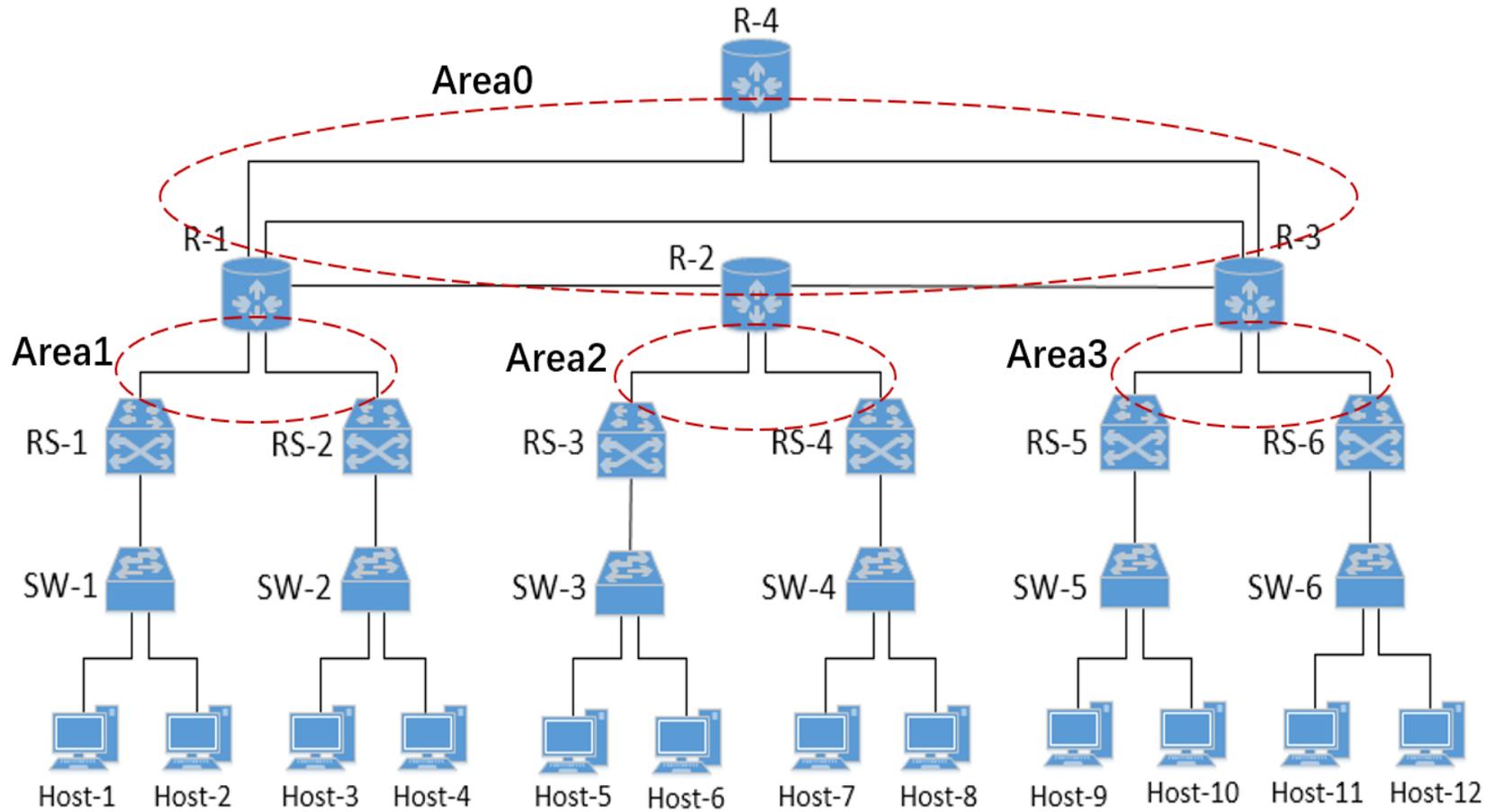
分别分析：

PC1访问PC3 / PC1访问PC4 / PC1访问PC8

网关、首部地址、VLAN标签、下一跳







6. 划分子网与构建超网

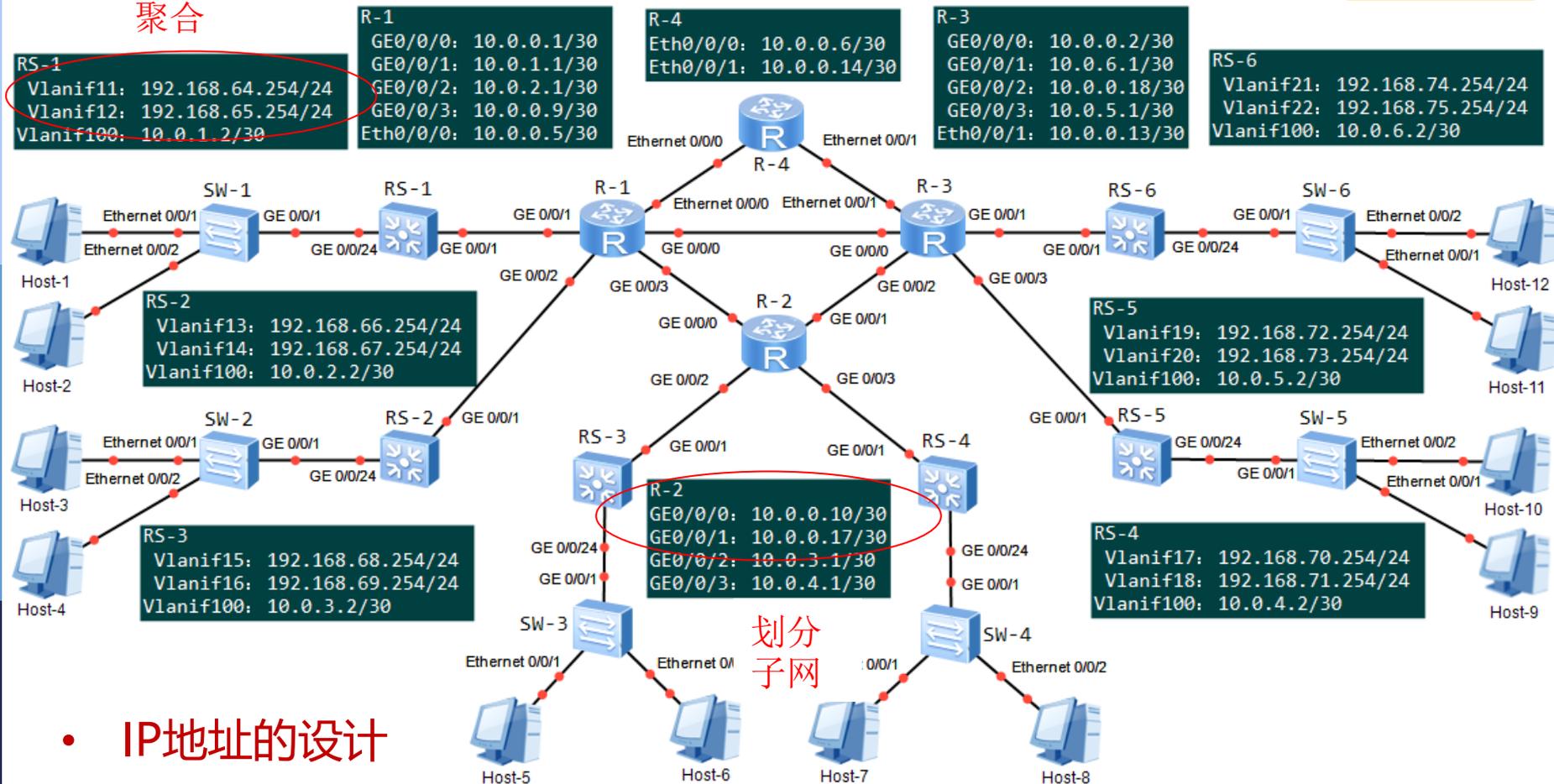
划分子网
构建超网

划分子网: 外统内分、大变小

构建超网: 路由聚合、小变大

案例分析

聚合



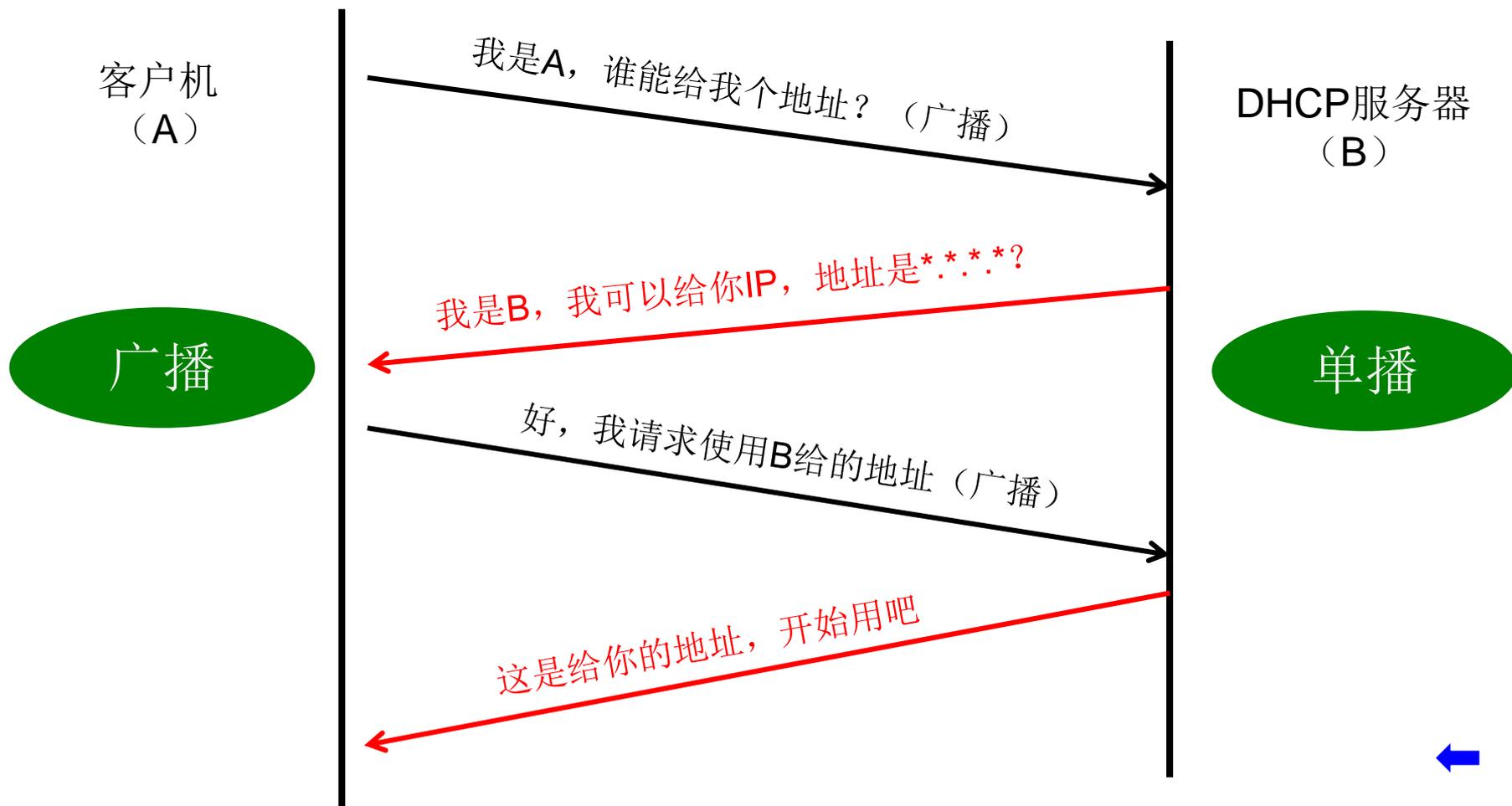
- IP地址的设计

7. IP地址的管理 (DHCP)

- DHCP {
- 功能: 动态分配IP地址
 - 报文类型: Discover、offer、request、ACK
 - DHCP客户端获取IP地址的过程: [图例](#)
 - DHCP中继: [通信过程](#)



客户端获取IP地址的过程——总结



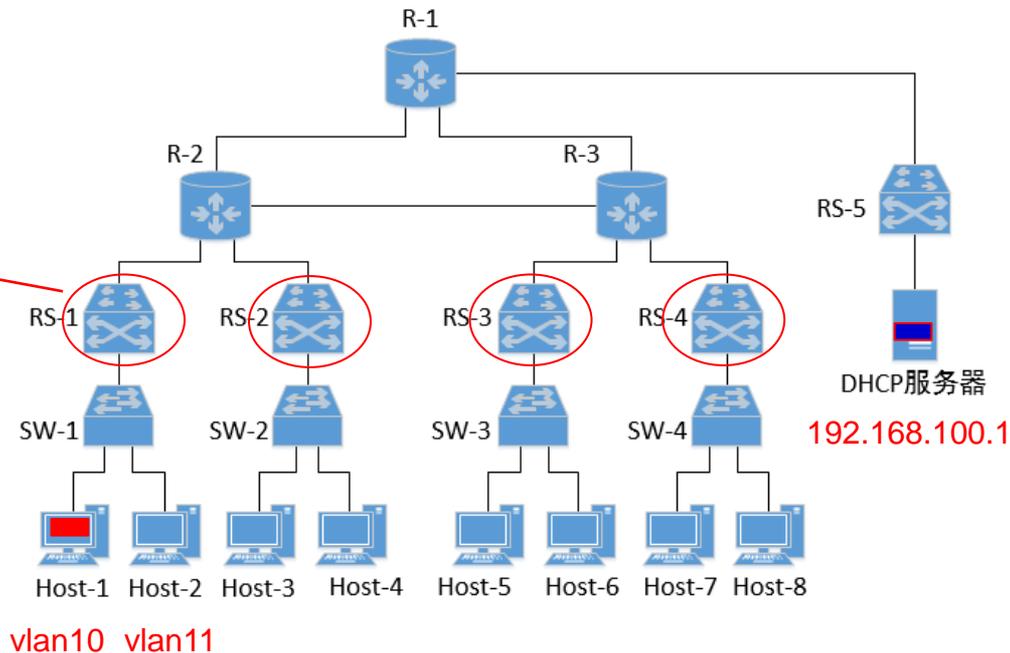
DHCP 中继代理

➤ DHCP中继的配置举例（华为s5700）：

```
[RS-1] dhcp enable
[RS-1] interface vlanif 10
[RS-1-Vlanif10] dhcp select relay
[RS-1-Vlanif10] dhcp relay server-ip 192.168.100.1
[RS-1-Vlanif10] quit

[RS-1] interface vlanif 11
[RS-1-Vlanif11] dhcp select relay
[RS-1-Vlanif11] dhcp relay server-ip 192.168.100.1
[RS-1-Vlanif11] quit
```

针对每个用户VLAN，在
网关处配置DHCP中继。



8. 无线局域网 (WLAN)

无线局域网

无线电频谱是关键资源

标准: IEEE802.11, 802.11a、802.11b、802.11g、
802.11n、802.11ac

WLAN的组成: 分布式系统、无线媒介、AP、工作站

WLAN的拓扑结构: BSS、ESS

WLAN的认证与加密

WLAN的部署: 胖AP (FAT)、瘦AP (FIT)

华为WLAN的模板配置

认识无线电频谱

□ 无线电频谱是关键资源

- 无线设备被限定在某个特定频带上工作，每个频带都有相应的带宽，即该频带可供使用的频率空间总和。带宽是评价链路（link）数据传输能力的基准
- 无线电频谱的使用受到主管当局的严格控制，主要是通过核发许可证的方式。例如，在美国的主管机关是联邦通信委员会，欧洲的主管机关是欧洲无线电通信局。其他地区，则由国际电信联盟（ITU）把关。

认识无线电频谱

□ 美国地区常用频带（部分）

频带	频率范围
UHF, ISM	902~928 MHz
S - 频带	2~4 GHz
S - 频带, ISM	2.4 ~2.5 GHz
C - 频带, 卫星下行链路	3.7 ~4.2 GHz
C - 频带, 雷达 (气象)	5.25 ~5.925 GHz
C - 频带, ISM	5.725 ~5.875 GHz
C - 频带, 卫星上行链路	5.925 ~6.425 GHz

认识无线电频谱

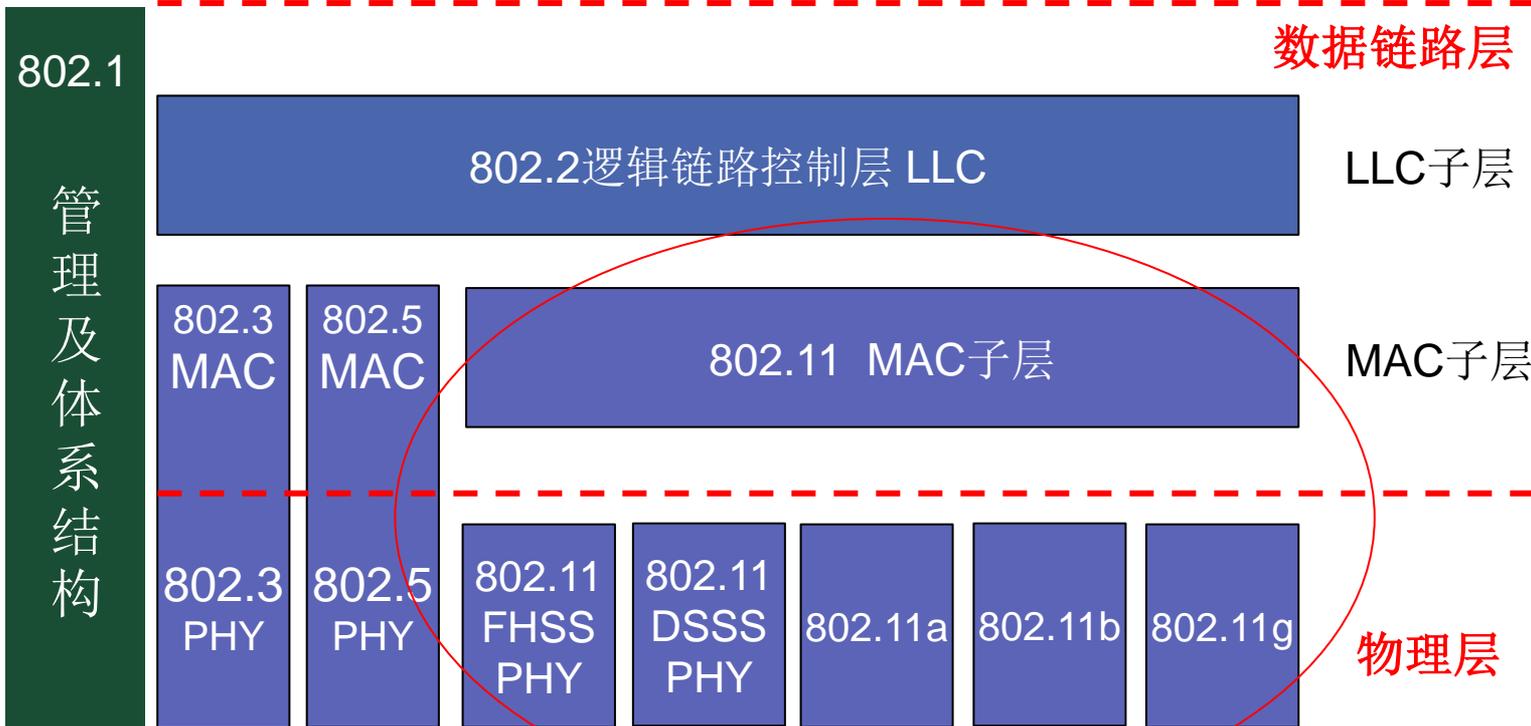
□ 关于ISM频带

- 上表中，有三个标示为ISM的频带，即工业（industrial）、科学（scientific）、医疗（medical）。大致而言，ISM频带是保留给工业、科学或医疗设备使用的。
- 例如，微波炉就属于ISM设备，使用的是2.4G ~ 2.5GHz ISM频带，因为该频段内的电磁辐射特别有利于加热含水物质。
- 之所以提到ISM，因为该频段的使用不需要申请许可证。802.11和许多其他设备均使用ISM频带。



寻址及网际互连

网络层



标准	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11i
发布时间	1999	1999	2003	2009	2012	2003
工作频段	5GHz	2.4GHz	2.4GHz	2.4/5GHz	5GHz	无线网络 安全方面 的补充
非重叠信道数	12或24	3	3	15	8	
最高接入速率	54Mb/s	11Mb/s	54Mb/s	600Mb/s	3.2Gb/s	
调制方式	OFDM	CCK/DSSS	CCK/DSSS/OFDM	4*4MIMO-OFDM/DSSS/CCK	8*8MIMO-OFDM/16~256 QAM	
兼容性	802.11a	802.11b	802.11b/g	802.11a/b/g/n	802.11a/b/g/n	

无线局域网的标准



无线局域网的组成

DS: 分布式系统，负责将帧传送到目的地

DS

AP



无线
媒介

AP



工作站

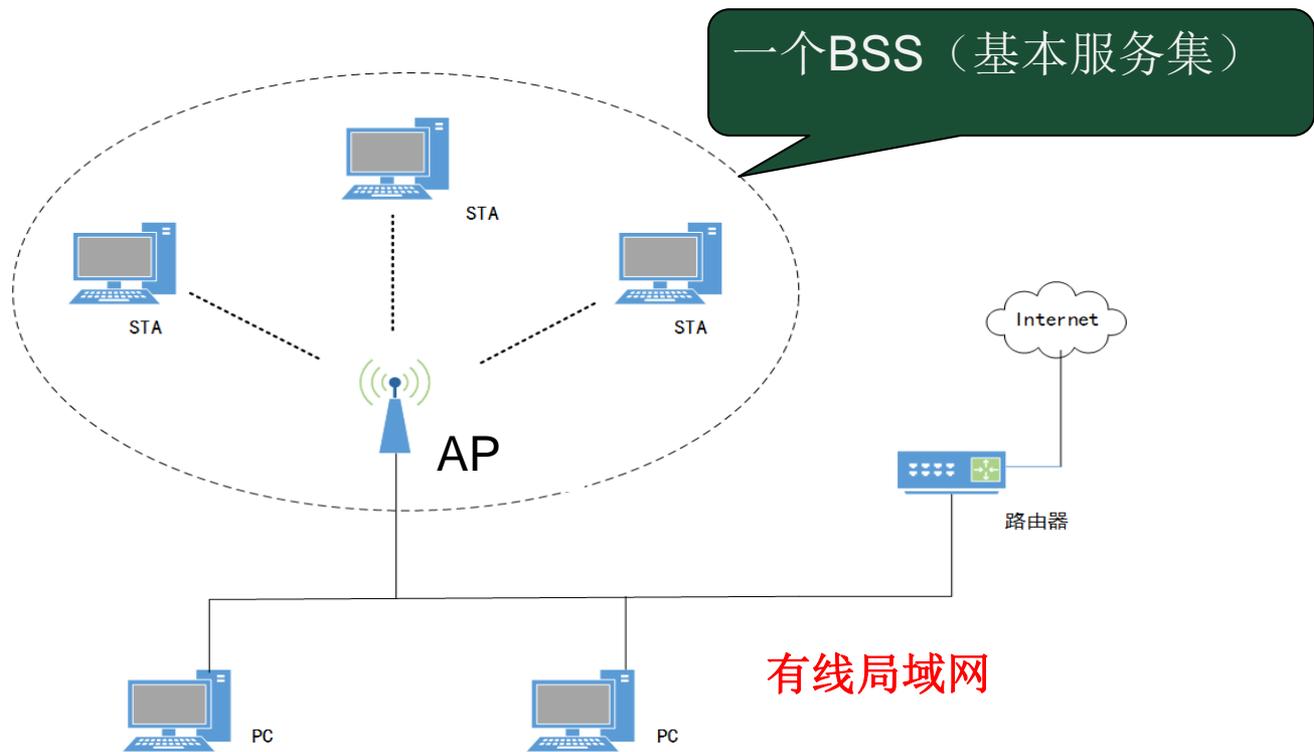


AP: 接入点，管理员在安装配置AP时，
需要为该AP配置至少一个服务集标识符
(又叫网络标识符) SSID和一个信道。



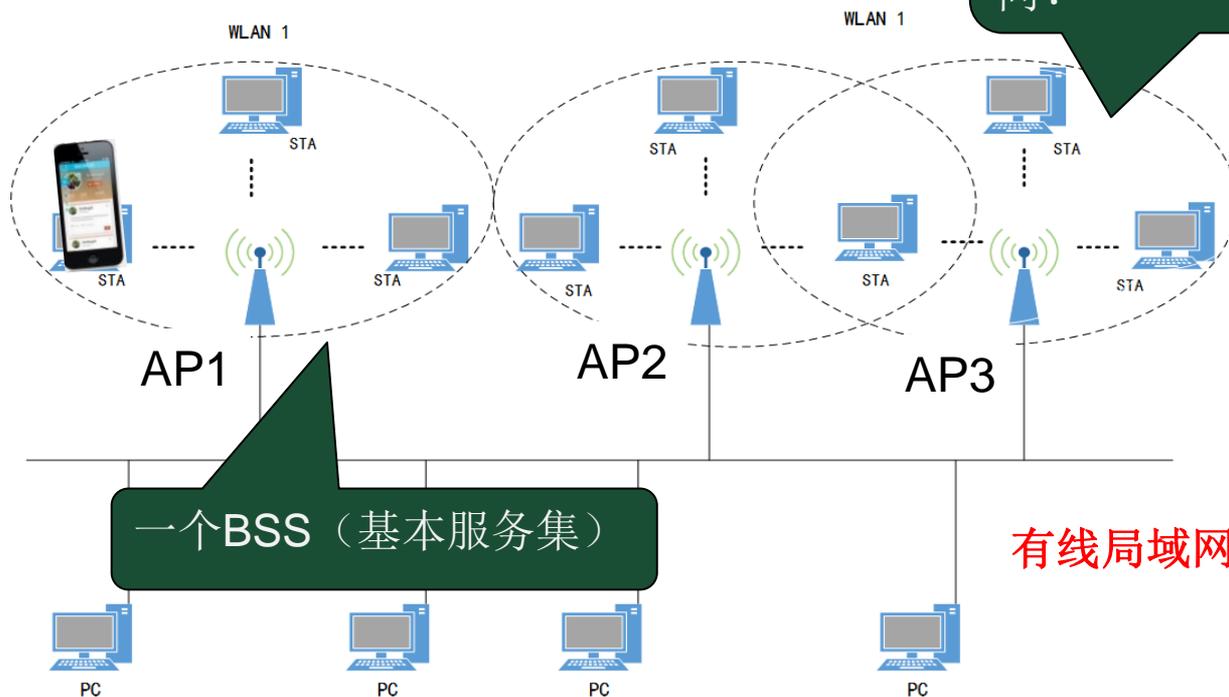
无线局域网的拓扑结构

□ 基础架构模式 (BSS)



无线局域网的拓扑结构

多AP模式 (扩展服务集ESS)



从AP1漫游到AP3
SSID相同? 接入密码相同?

一个BSS (基本服务集)

有线局域网



无线局域网的接入认证

□ 为什么需要认证？

- 认证提供了关于用户的身份保证，这意味着当用户声称具有一个特别的身份时，认证将提供某种方法来证实这一声明是正确的。
- 用户在访问无线局域网之前，首先需要经过认证验证身份以决定其是否具有相关权限，再对用户进行授权，允许用户接入网络，访问权限内的资源。

无线局域网的接入认证

□ 802.11的认证方式及其缺陷

■ 802.11规定了两种认证方式：开放系统认证和共享密钥认证。

- **开放系统认证**。根据802.11规范的描述，开放系统认证实质上是空认证，采用这种认证方式的任何用户都可以成功认证并接入WLAN。
- **WEP共享密钥身份验证**。WEP (Wired Equivalent Privacy) 叫做有线等效加密，用来提供访问控制、数据加密和安全性检验等功能，是无线领域第一个安全协议。WEP推出以后，很快就被安全人员及黑客发现很多漏洞，因此已被802.11i拒用（不建议使用）

无线局域网的接入认证

□ Web接入认证

- 客户机在认证页面中输入用户名和密码等认证信息，提交认证请求。
- 认证服务器提取客户机**认证请求信息**，访问后台数据库进行用户信息核对。如果通过认证，客户机则可以访问网络资源；否则，系统要求客户机重新认证。

无线通信加密

□ 802.11i对802.11安全性的改进

- 由于802.11标准存在公认的安全漏洞，严重威胁到无线局域网的进一步应用。2003年，IEEE又制定了IEEE802.11i标准，以增强IEEE802.11的媒体接入控制功能，改进无线局域网的安全性。
- 802.11i是围绕IEEE 802.1X用户端口身份验证和设备验证制定的，主要包括两项内容：
 - Wi-Fi保护存取（简称 WPA）技术
 - 强健安全网络（简称 RSN）

无线通信加密

- 由于WEP加密技术在安全方面存在缺陷，于是出现了新的WLAN加密技术WPA（Wi-Fi Protected Access, Wi-Fi保护访问）和WPA2。
 -
- WPA/WPA2主要解决WEP在共享密钥上的漏洞，添加了数据完整性检查和用户级的认证措施。

无线通信加密

□ WPA加密认证方式

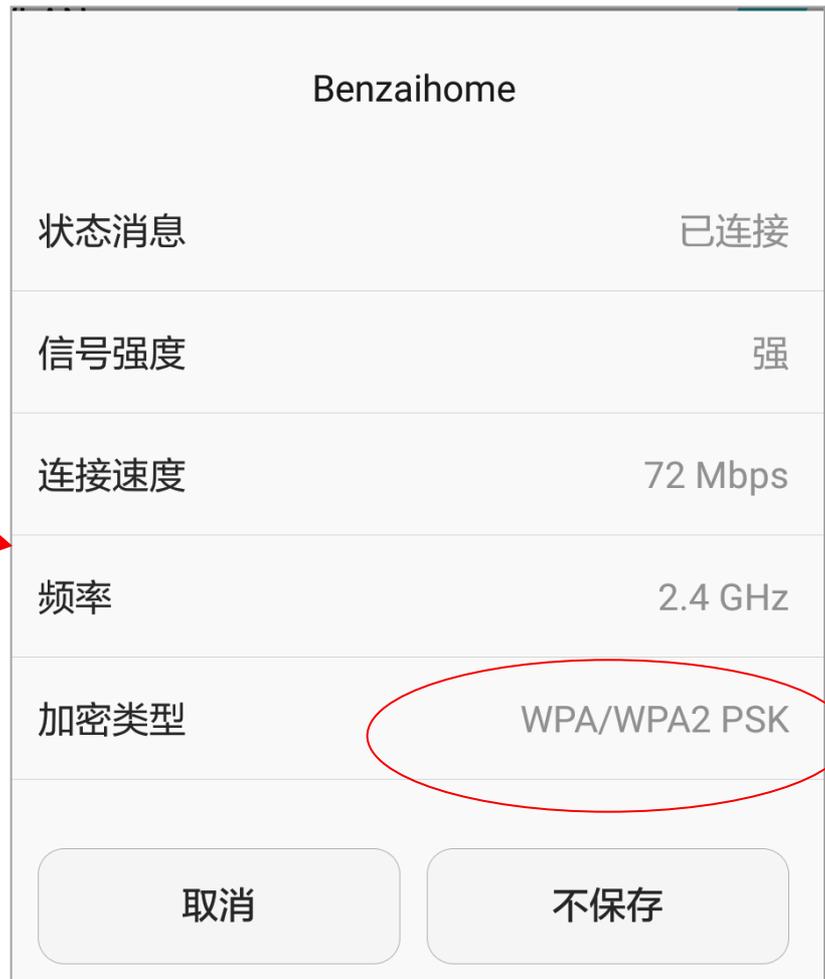
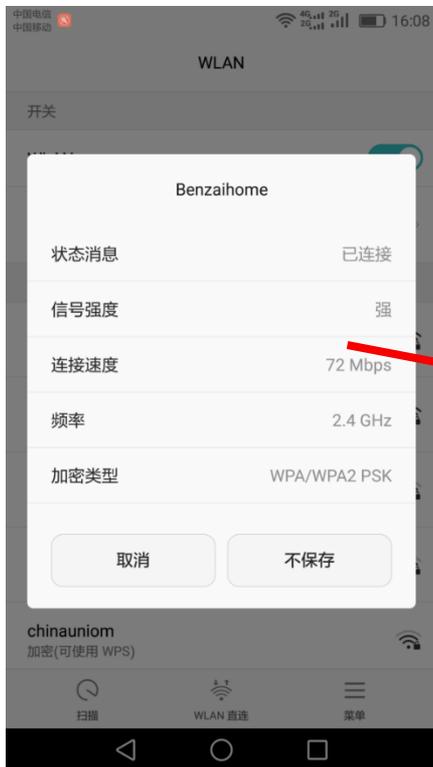
- Wi-Fi联盟给出的WPA定义为：WPA = 802.1x + EAP + TKIP + MIC。
其中：
 - 802.1x是指IEEE的802.1x身份认证标准；EAP（Extensible Authentication Protocol，扩展身份认证协议）是一种扩展身份认证协议。这两者就是新添加的用户级身份认证方案。
 - TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）是一种密钥管理协议，即一种加密算法；
 - MIC（Message Integrity Code，消息完整性编码）是用来对消息进行完整性检查的，用来防止攻击者拦截、篡改甚至重发数据封包。
- 由此可见，WPA已不再是单一的链路加密，还包括了身份认证和完整性检查两个重要方面。

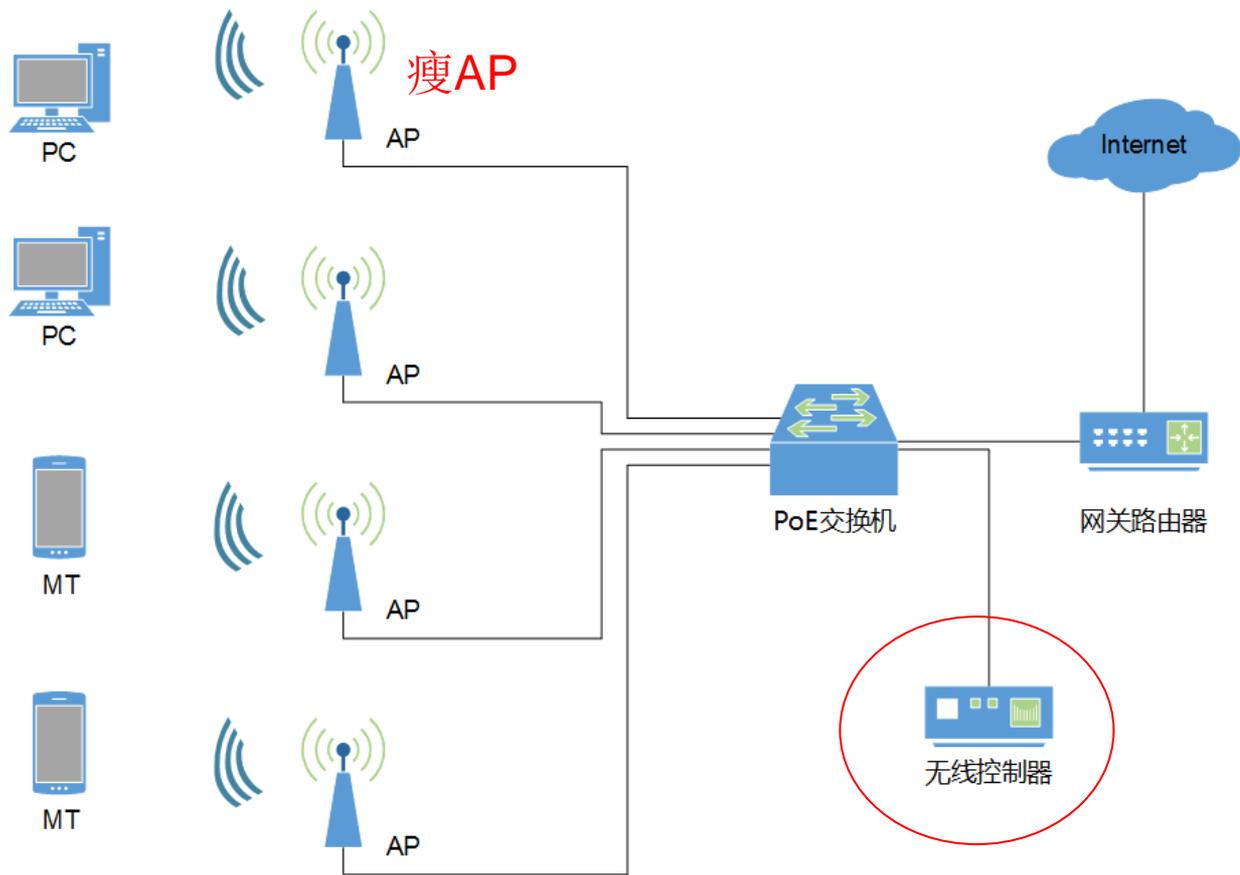
无线通信加密

□ WPA加密认证方式

- WPA2是WPA的后续版本，支持“AES”加密方式。除此之外，与过去的WPA相比在功能方面没有大的区别。
- 在WPA的设计中要用到一个802.1X认证服务器来散布不同的钥匙给各个用户；不过它也可以用在较不保险的“pre-shared key”(PSK)模式，让每个用户都用同一个密语。Wi-Fi联盟把这个使用pre-shared key的版本叫做WPA个人版或WPA2个人版，用802.1X认证的版本叫做WPA企业版或WPA2企业版。

查看手机连接WLAN的加密认证方式





➤ 无线网络规划

模板设计

给各个AP配置模板信息。可将各AP的模板信息配置成一样的内容，使得无线终端在不同AP间漫游时，可以自动接入。通过AC进行统一配置。

(1) 域管理模板

域管理模板用来进行AP的国家码、调优信道集合和调优带宽的配置。

国家码是AP射频所在国家的标识，规定了AP射频特性，包括AP的发送功率、支持的信道等。国家码的配置使AP的射频特性符合不同国家或区域的法律法规要求。

(2) 安全模板

安全模板用来配置WLAN安全策略，对无线终端接入进行身份验证，对用户报文进行加密，为WLAN网络 and 用户提供安全保障。WLAN安全策略包括开放认证、WEP、WPA/WPA2-PSK、WPA/WPA2-802.1X、WAPI-PSK和WAPI-证书，配置安全模板时可选择其中一种。

➤ 无线网络规划

模板设计

(3) SSID模板

SSID模板主要用来配置SSID名称，即无线网络标识。

(4) VAP模板

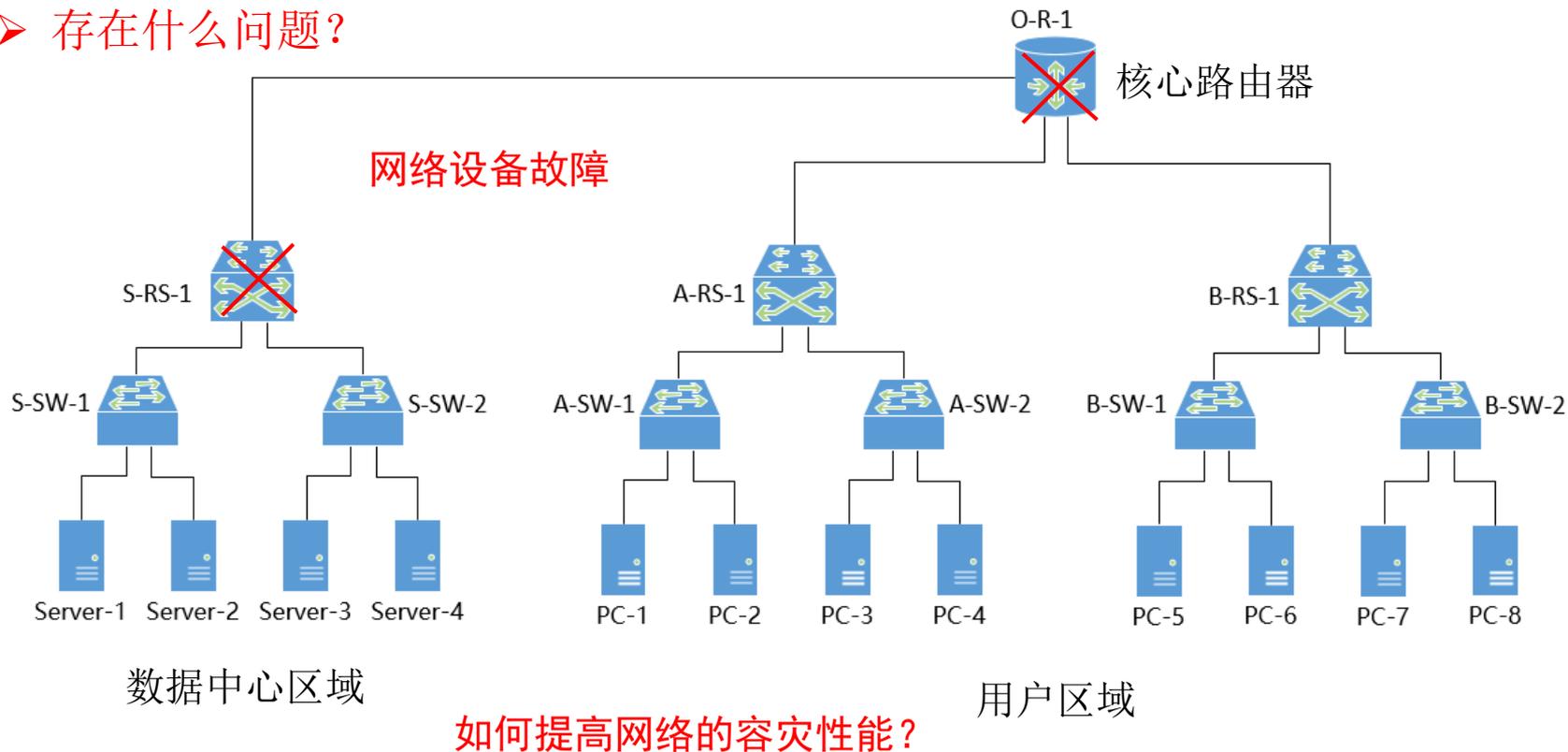
在VAP模板中配置各项参数、引用模板，然后引用到AP或AP组，AP上就会创建VAP，为STA提供无线接入服务。通过VAP模板中的各项参数配置可以实现AP的管理。例如：可以在VAP模板中设置业务数据报文转发方式、业务VLAN，引用SSID模板、安全模板。



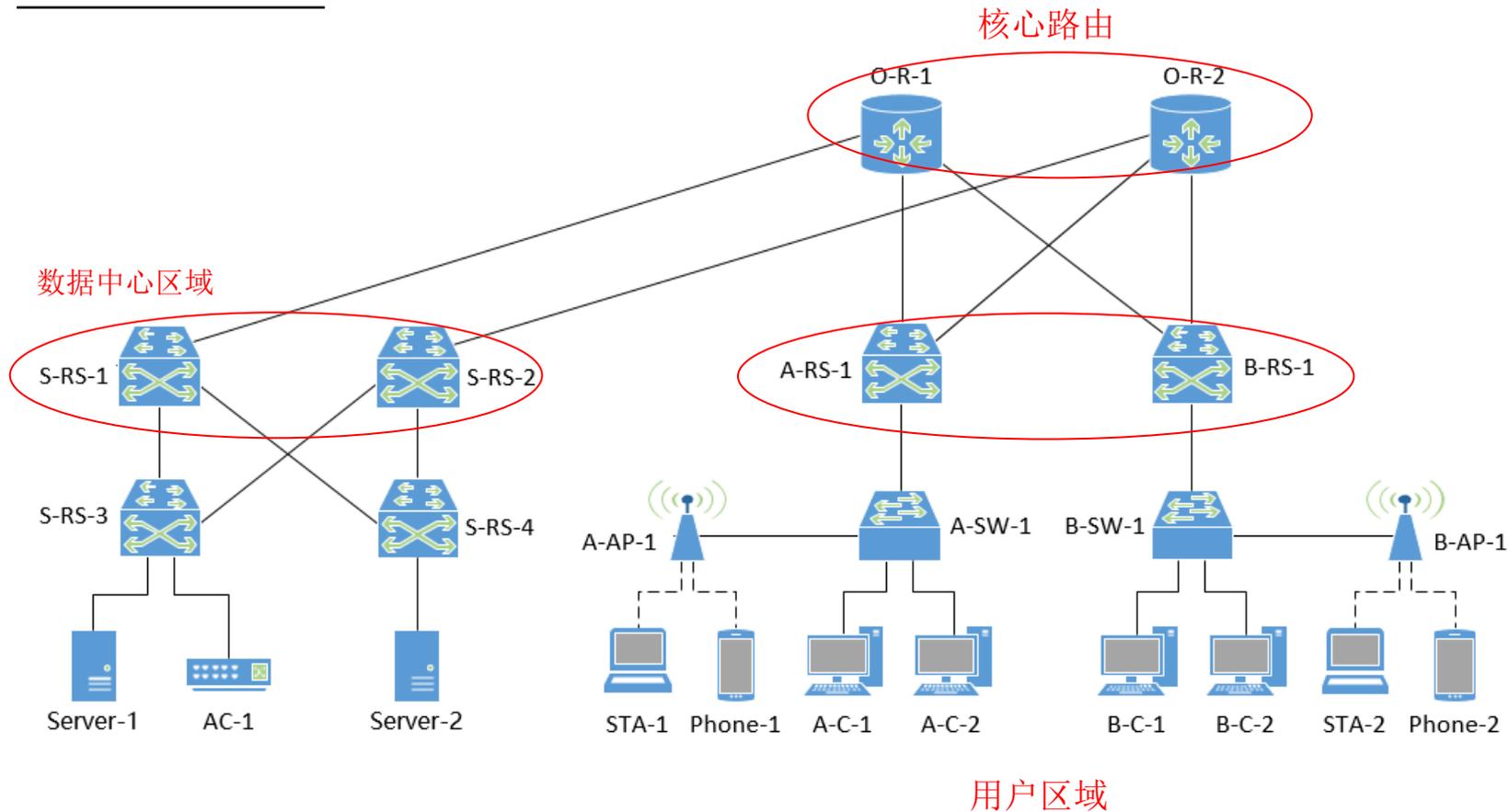
9. 混合园区网建设案例分析

9. 混合园区网建设案例分析

➤ 存在什么问题？

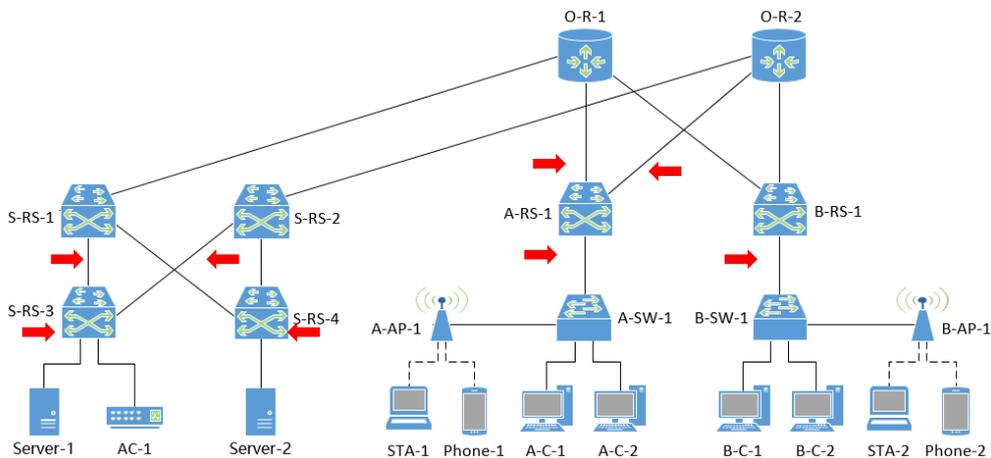


➤ 网络容灾部署



1. 拓扑结构分析

- 用户区域拓扑中，三层交换机A-RS-1和B-RS-1下面可根据需要接入多台二层交换机，此处简化为各接入一台二层交换机，用于接入用户主机。
- 三层交换机A-RS-1和B-RS-1分别同时接入路由器O-R-1和O-R-2，实现了通信链路冗余，起到了网络容灾作用。
- 数据中心区域拓扑中，三层交换机S-RS-1和S-RS-2作为汇聚交换机，其下面可根据需要接入多台三层交换机，此处简化为各接入一台三层交换机，即S-RS-3和S-RS-4，用于接入服务器。
- 数据中心中，所有的接入交换机（此处指S-RS-3和S-RS-4）分别同时接入汇聚交换机S-RS-1和S-RS-2，实现了通信链路冗余，起到了网络容灾作用。



2. 设备类型分析

➤ 路由器：

✓ O-R-1、O-R-2

➤ 三层交换机

✓ S-RS-1、S-RS-2

✓ S-RS-3、S-RS-4

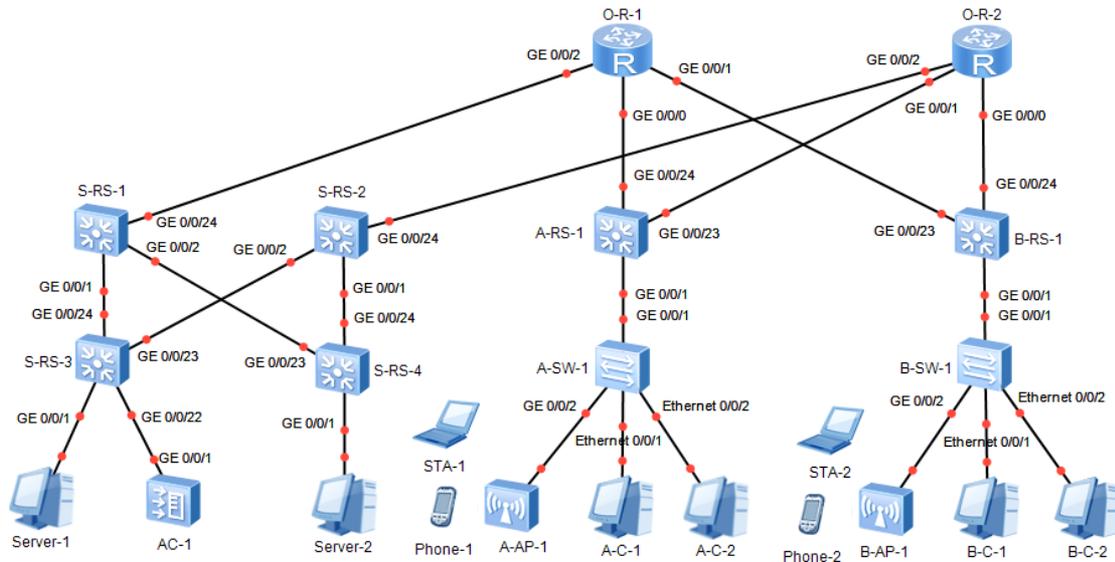
✓ A-RS-1、B-RS-1

➤ 二层交换机

✓ A-SW-1、B-SW-2

➤ 无线通信设备

✓ AC-1、A-AP-1、B-AP-1



问题：

1. 用户区域中的A-SW-1和B-SW-1，能否换成三层交换机？
2. 用户区域中的A-RS-1和B-RS-1，能否换成二层交换机？
3. 数据中心区域中的S-RS-3和S-RS-4，能否换成二层交换机？

3. 主机IP地址规划分析

➤ 用户区域的用户主机

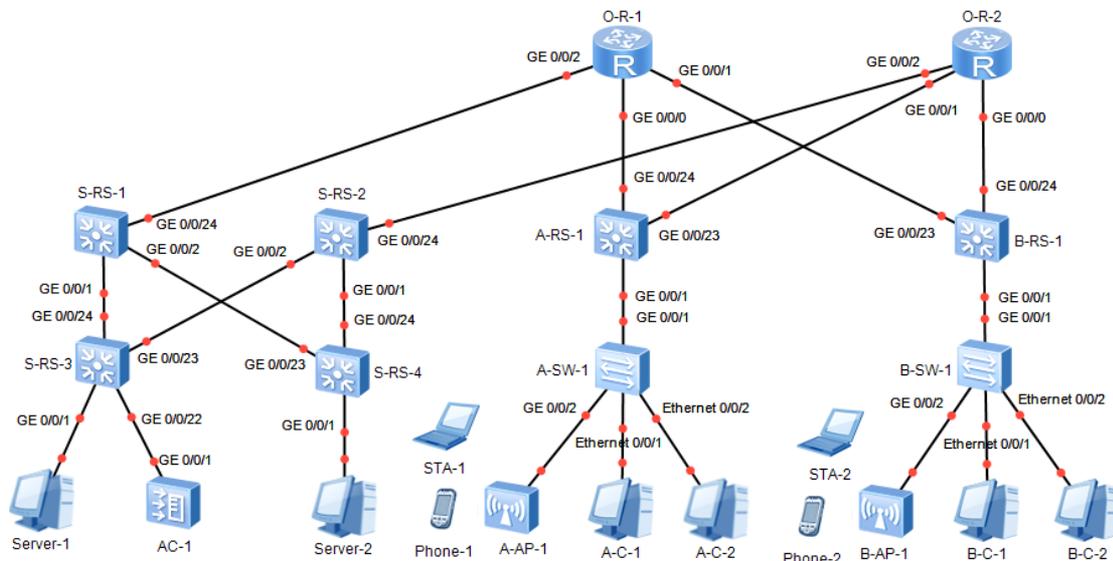
- 有线用户
- 无线用户

➤ 数据中心区域服务器

- S-RS-3下连的服务器
- S-RS-4下连的服务器

➤ 无线通信设备

- A-SW-1下连的AP
- B-SW-1下连的AP
- AC



问题：

1. 有线用户和无线用户的IP地址是同一个网段，还是设计成不同网段？例如STA-1和A-C-1。
2. 能否给AC-1、A-AP-1、B-AP-1全部配置10.0.200.*段的IP地址？
3. 假设园区网中所有AP以及AC的IP地址都属于10.0.200.*，你如何设计它们的子网掩码？默认网关？
4. 数据中心区域中的服务器，你如何设计IP地址？
5. 无线移动终端的IP地址如何获得？AP的IP地址如何获得？

4. VLAN设计分析

➤ 用户区域

- 有线用户
- 无线用户

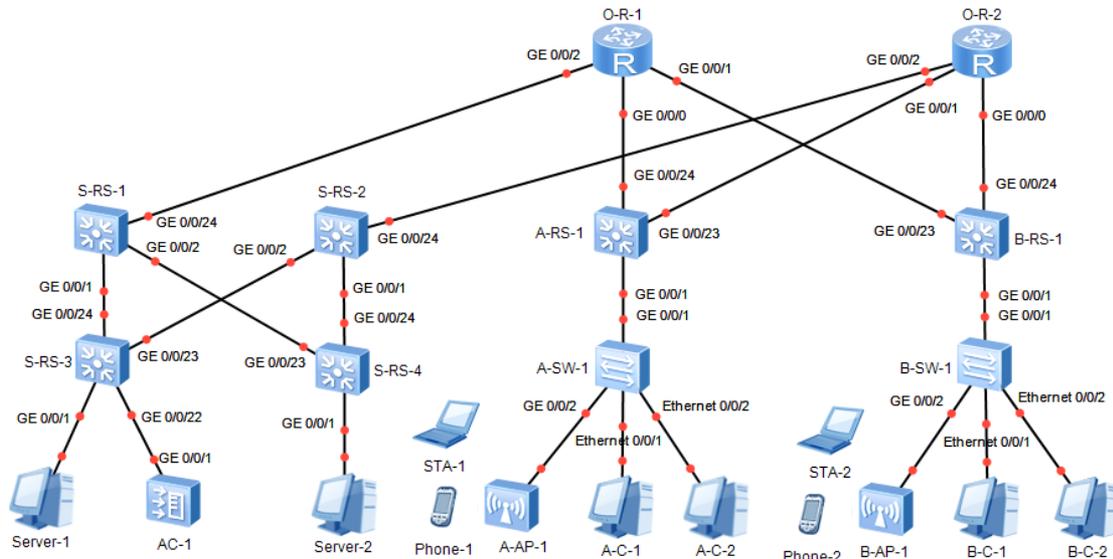
➤ 数据中心区域

➤ 无线通信设备 (AP和AC)

- AP所属的VLAN
- AC-1所属的VLAN

➤ 三层交换机路由接口的VLAN

- 此处略，具体见路由接口IP地址设计



问题:

1. 你如何设计有线用户主机所属的VLAN? 无线移动终端的VLAN呢?
2. 你如何设计A-AP-1和B-AP-1所属的VLAN? 能否将它们所属的VLAN ID值设置成相同?
3. AP接入交换机的接口, 其类型设置成access还是trunk? 为什么? 用户主机接入交换机的接口呢? 服务器接入交换机的接口呢?
4. 若AP接入交换机的接口被设置成trunk模式, 该接口的PVID值是保持缺省值吗?
5. A-SW-1的上联接口, 其类型设置成access还是trunk? 为什么?
6. AC-1的VLAN ID能否和A-AP-1或B-AP-1的VLAN ID相同? 有冲突吗?
7. 你如何设计服务器所属的VLAN?
8. A-SW-1上需要创建几个VLAN ?

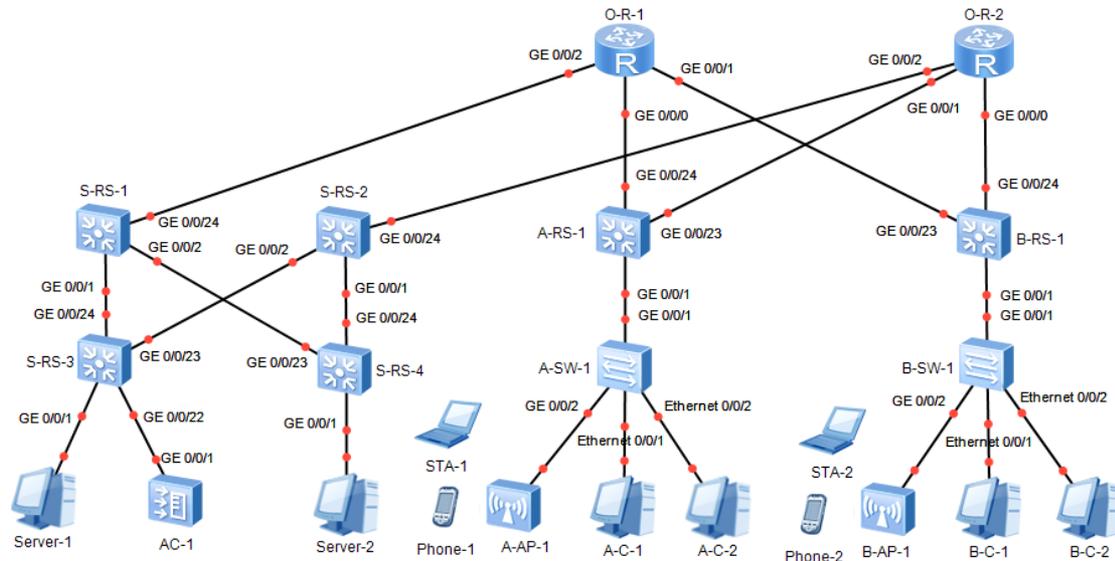
5. 路由接口IP地址规划分析

➤ 三层虚拟路由接口

- A-RS-1、B-RS-1
- S-RS-1~S-RS-4
- 注意：有些三层虚拟路由接口是用来做默认网关的，有些是用来进行路由间通信的

➤ 路由器的物理接口

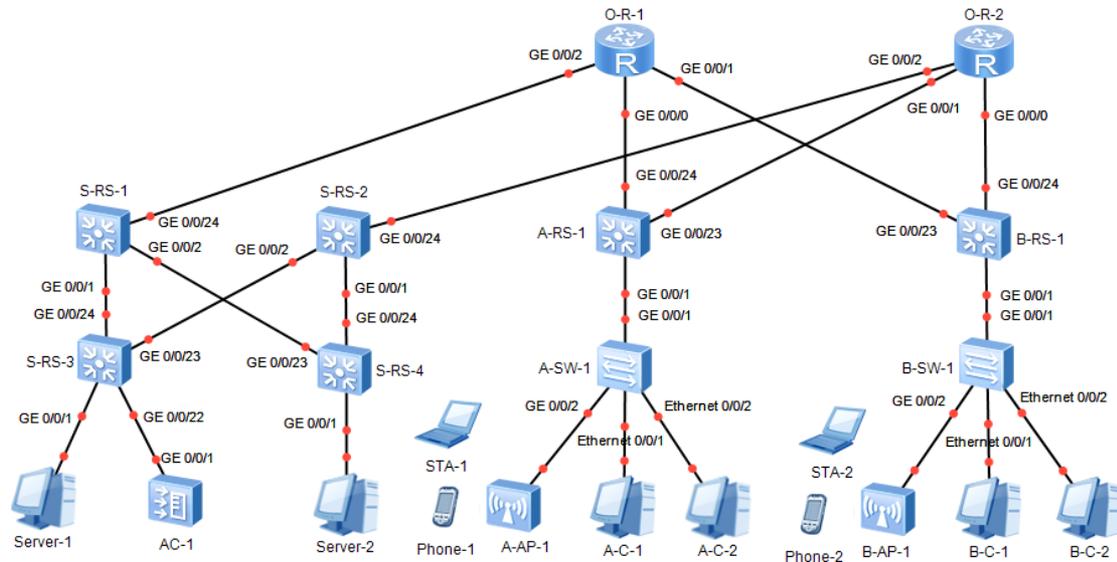
- O-R-1
- O-R-2



问题：

1. O-R-1和O-R-2上各需要配置几个路由接口地址？
2. A-RS-1上需要创建几个三层虚拟接口？分别有什么作用？B-RS-1呢？S-RS-1~S-RS-4呢？
3. A-RS-1上需要创建几个VLAN？分别有什么作用？B-RS-1呢？S-RS-1~S-RS-4呢？
4. A-RS-1上，用来作为默认网关的三层虚拟接口，其子网掩码如何设计？用来进行路由间通信的虚拟接口，其子网掩码又该如何设计？

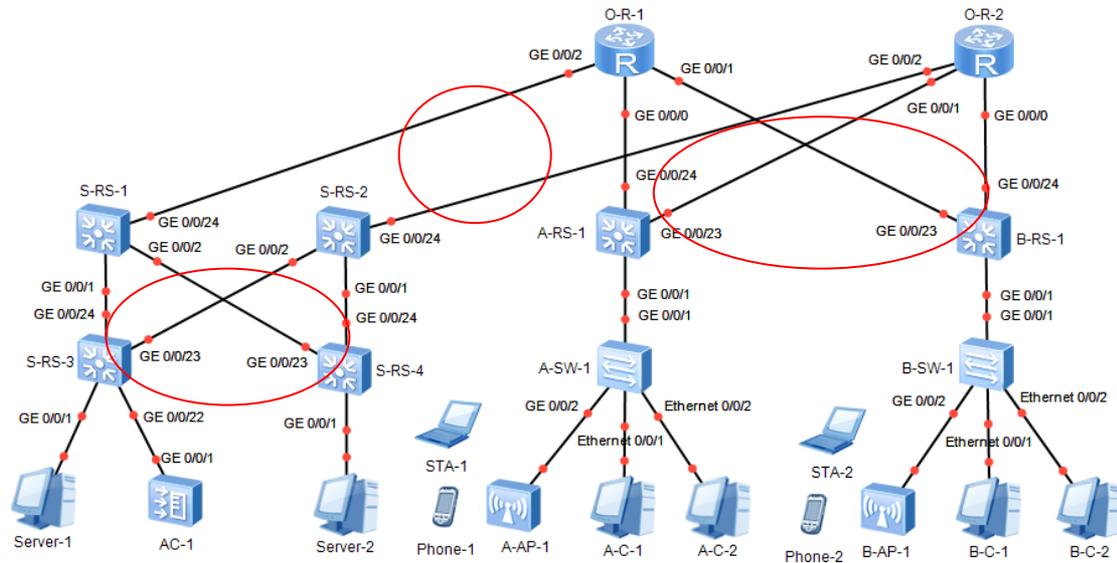
6. 路由配置分析



问题：

1. 全网使用静态路由？动态路由？
2. A-RS-1的路由表中，应该有到达哪些目的网络的路由记录？下一跳分别是什么？
3. O-R-1的路由表中，应该有到达哪些目的网络的路由记录？下一跳分别是什么？
4. S-RS-1~S-RS-4呢？分别说明
5. AC-1呢？
6. 假设全网使用OSPF协议，则A-RS-1在配置OSPF时，需要宣告哪些路由？其他设备呢？

7. OSPF区域划分分析



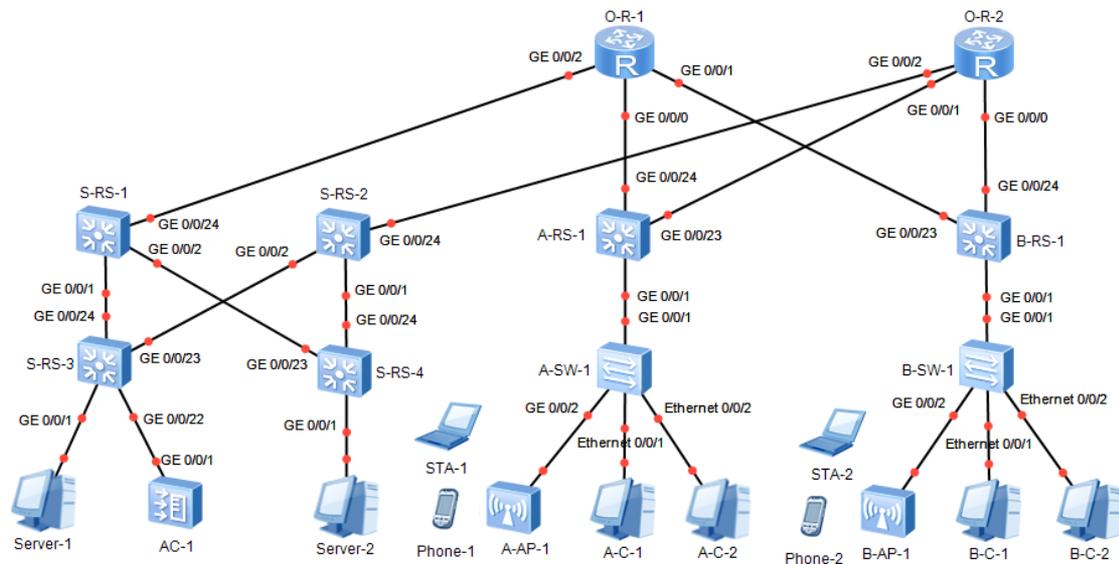
问题:

1. 右图中是划分的三个OSPF区域，谁是area0？
2. 每个OSPF区域包含哪些路由接口？

8.WLAN的配置分析

问题

1. 此处AP采用瘦AP模式，还是胖AP模式？
2. 若无线移动终端采用动态获取IP地址的方式，从何处获取IP地址？
3. 此处将DHCP中继配置在何处？
4. 当AC-1收到STA-1发来的申请获取IP地址的报文时，如何知道该从哪个网段中（地址池中）分配IP地址？
5. AP和AC之间的通信采用了何种特殊协议？（无线接入点控制与规范 CAPWAP）
6. 在配置A-AP-1的SSID和登录密码时，是配置成和B-AP-1相同，还是不同？



Thanks.