网络运维管理

第1讲：构建有线/无线混合的园区网

河南中医药大学信息技术学院
《网络运维管理》课程教学组

目录

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

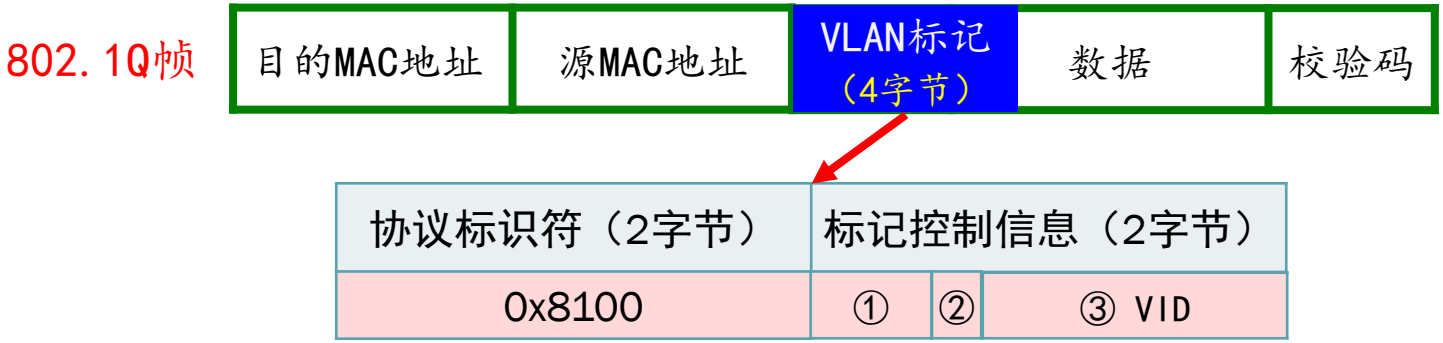
- 工作原理: 依据帧目的MAC地址进行转发
- MAC地址表：MAC地址自动学习、手工配置
- 广播域：所有接口属于同一个广播域
- 交换机管理：带外、带内
- 交换机连接：级联、堆叠

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

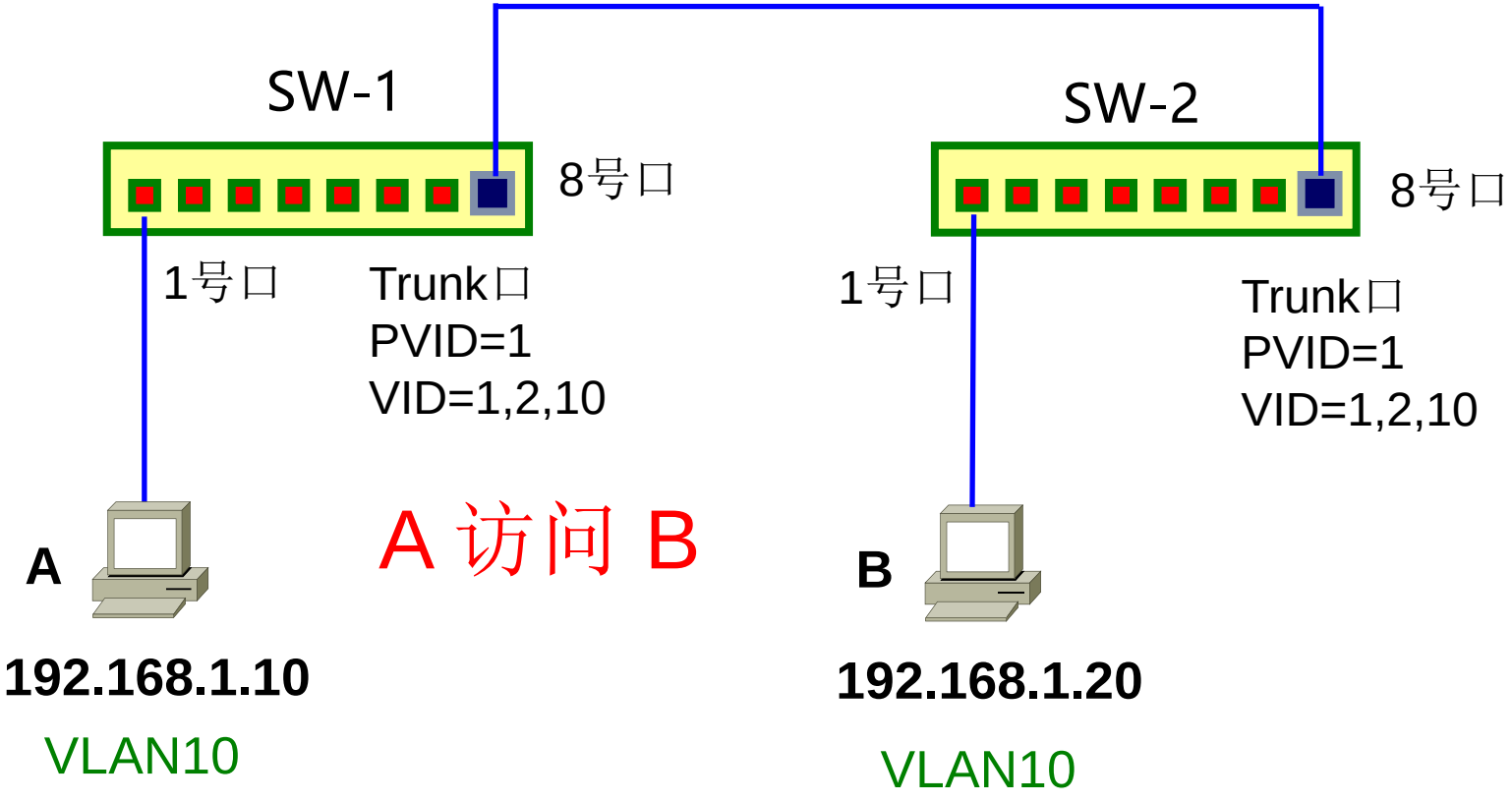
➢ 802.1Q的帧结构



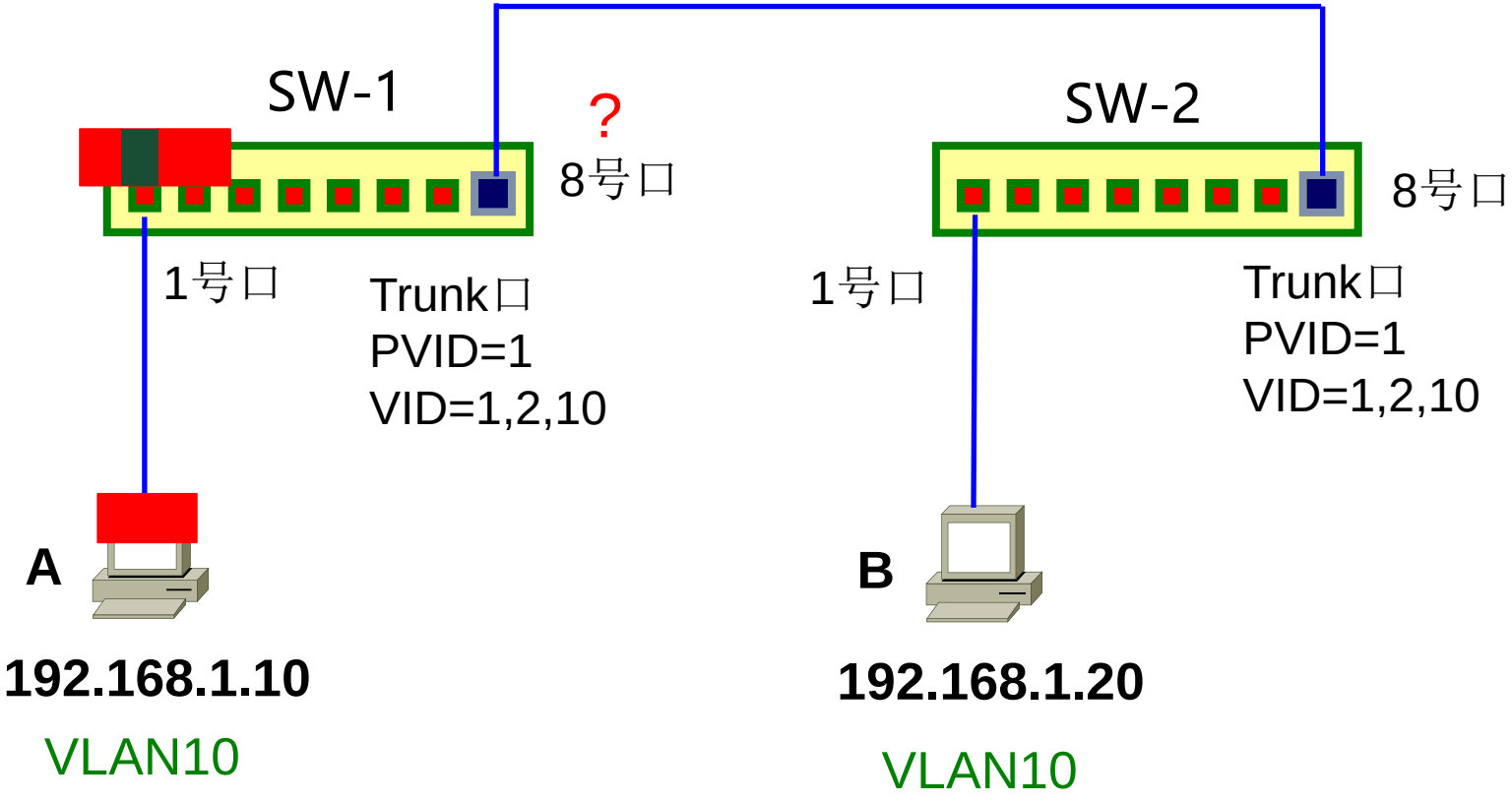
1. 2字节的协议标识符，置0x8100固定值，表明该帧带有802.1Q标记信息；
2. 2字节的标记控制信息，包含了3个域：
   - ① 表示报文优先级，占3bit，取值0到7，7为最高；
   - ② 表示规范格式指示符，占1bit，0表示规范格式，应用于以太网，1表示非规范格式，应用于Token Ring；
   - ③ 表示VLAN ID，占12bit，用于表示VLAN的归属，其中，VID＝0用于识别帧优先级，4095(FFF)作为预留值，**所以有效的VLAN ID范围为1-4094。**

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	若本接口的PVID=帧VID，则去掉帧中的VLAN标签，然后发出。 若本接口的PVID ≠ 帧VID值，则直接发出，不去掉VLAN标签	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

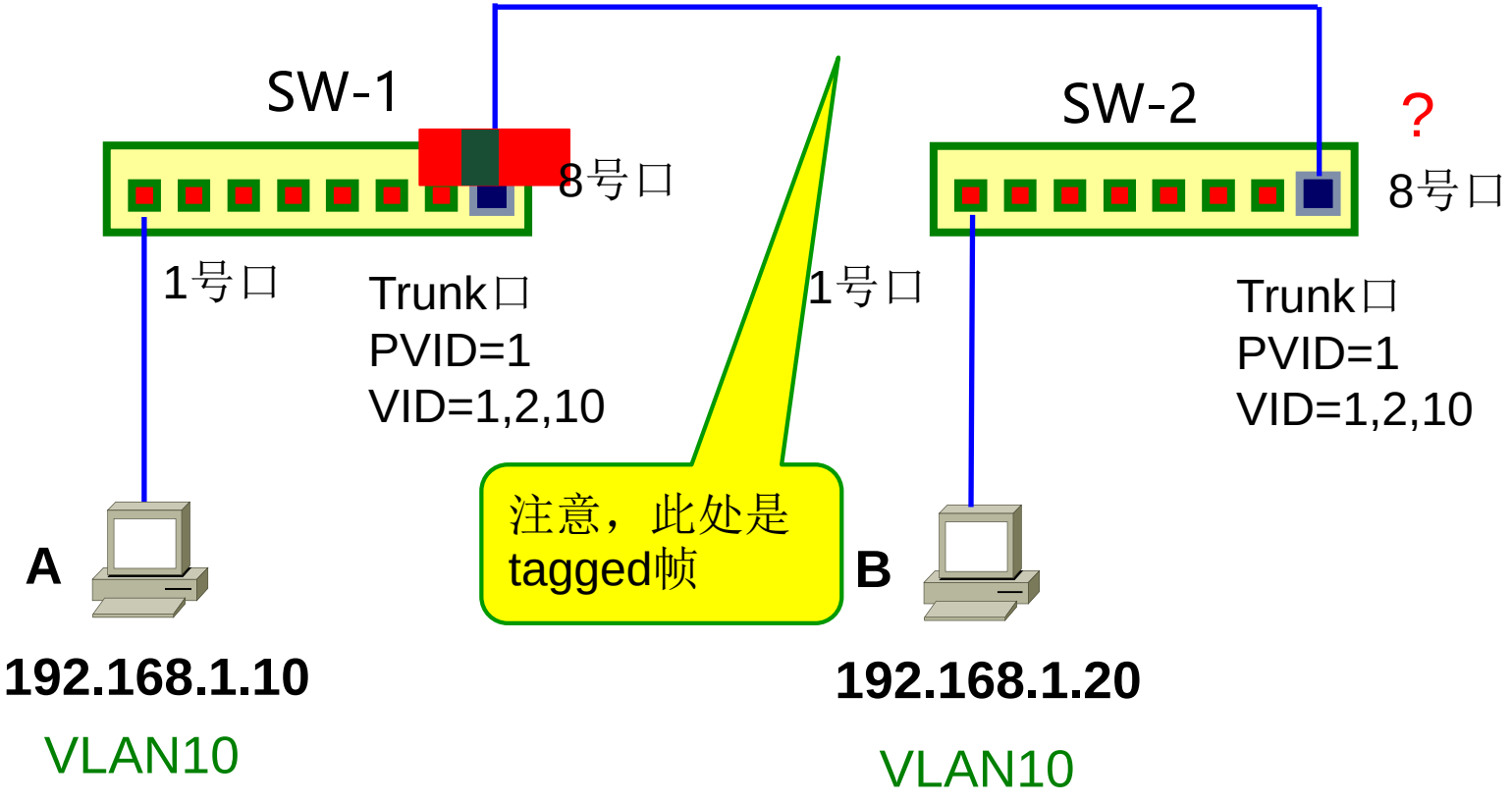
- 1号口都是Access口，属于VLAN10，其PVID值=VID值=10
- 8号口都是Trunk口，PVID值=1，允许VLAN 1、VLAN 2、VLAN 10的帧通过



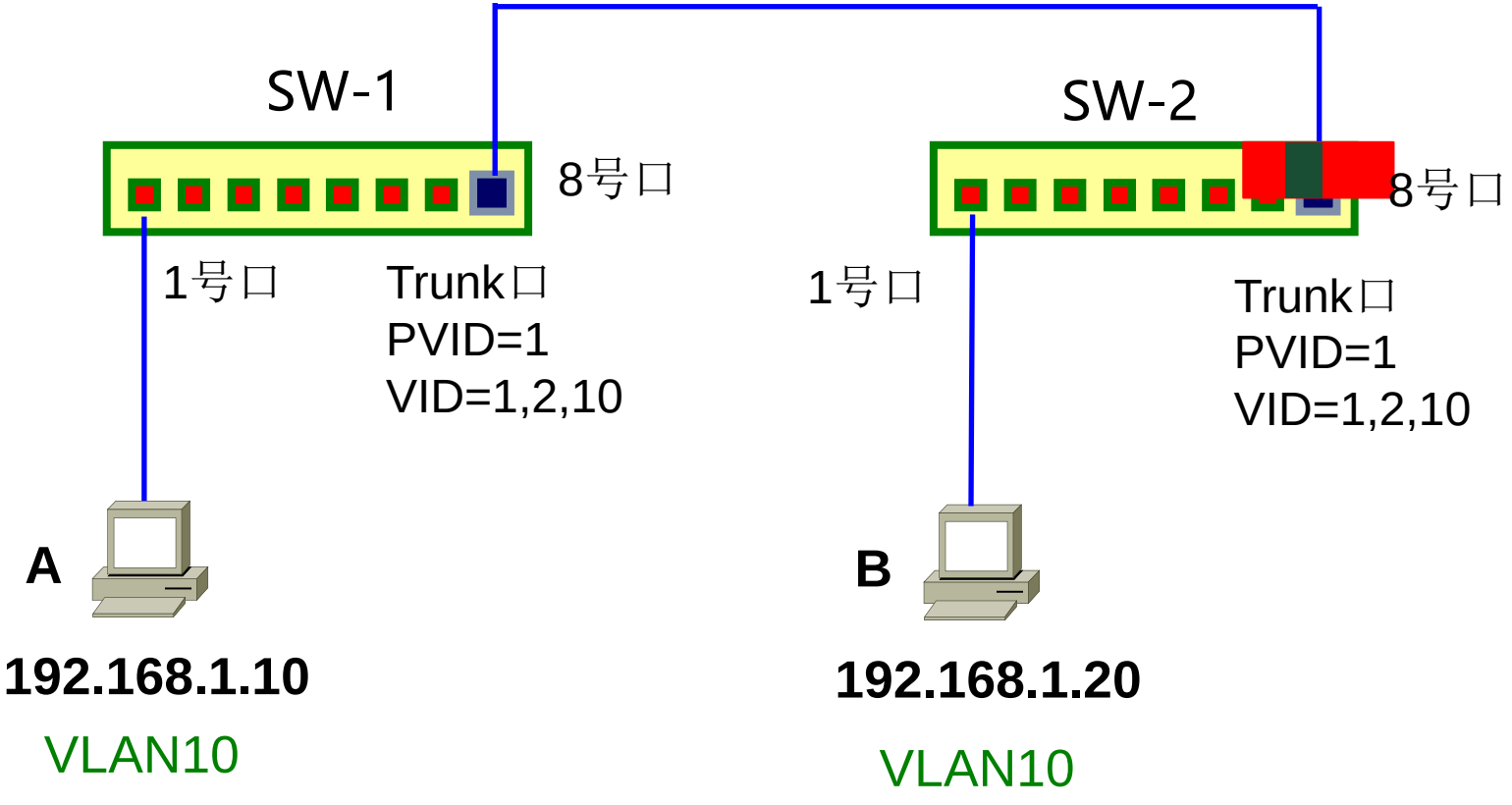
➢ PC-A发出普通帧，进入SW-1的1号口，普通帧被加上VLAN10的标签，使得该帧的VID=10



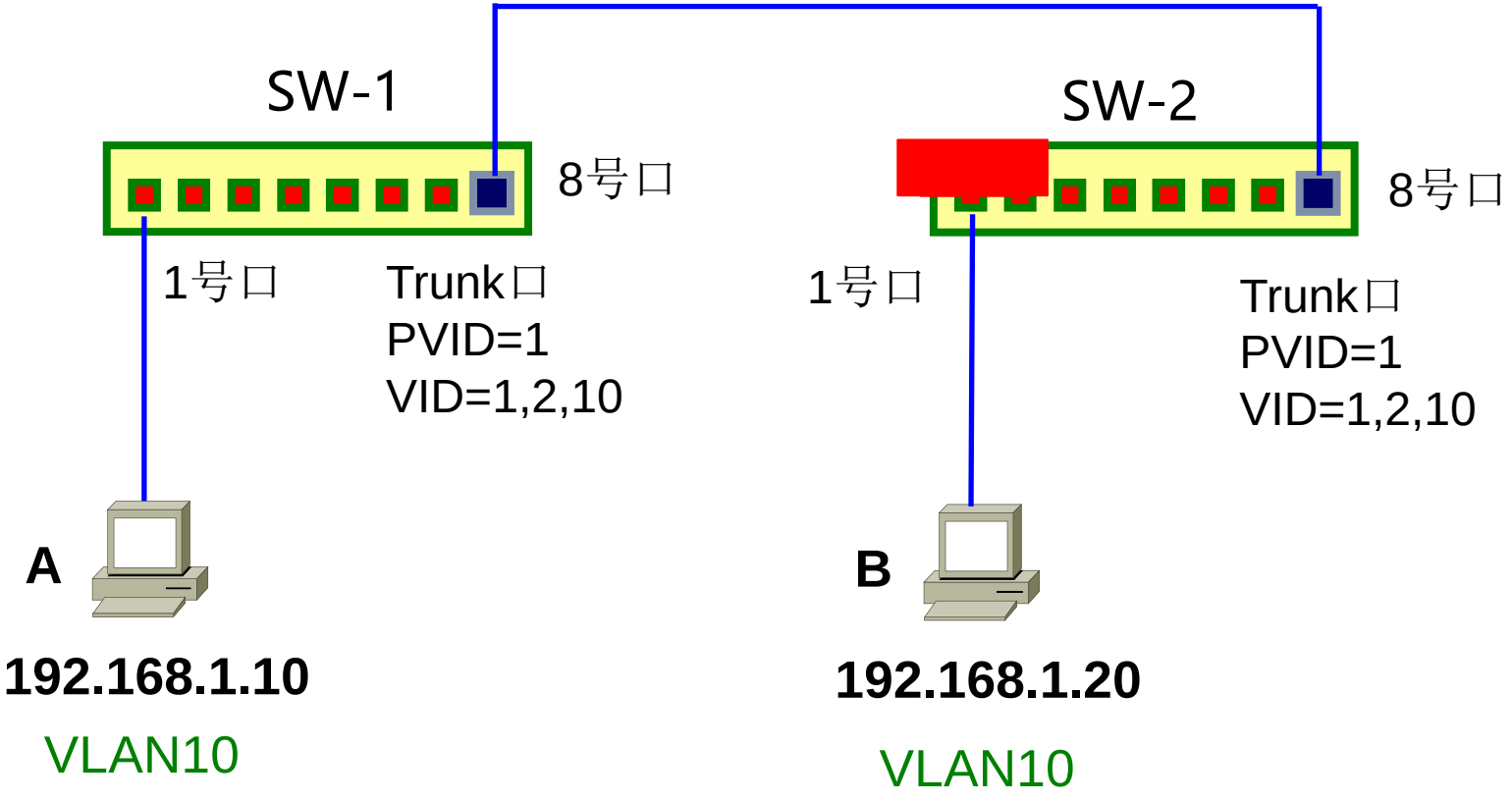
- 该tagged帧被转发至SW-1的8号口，由于8号口是Trunk口，且允许VLAN10的帧通过，且8号口PVID≠该帧的VID，因此，该帧被从8号口直接发出，不去掉标签。



- 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。



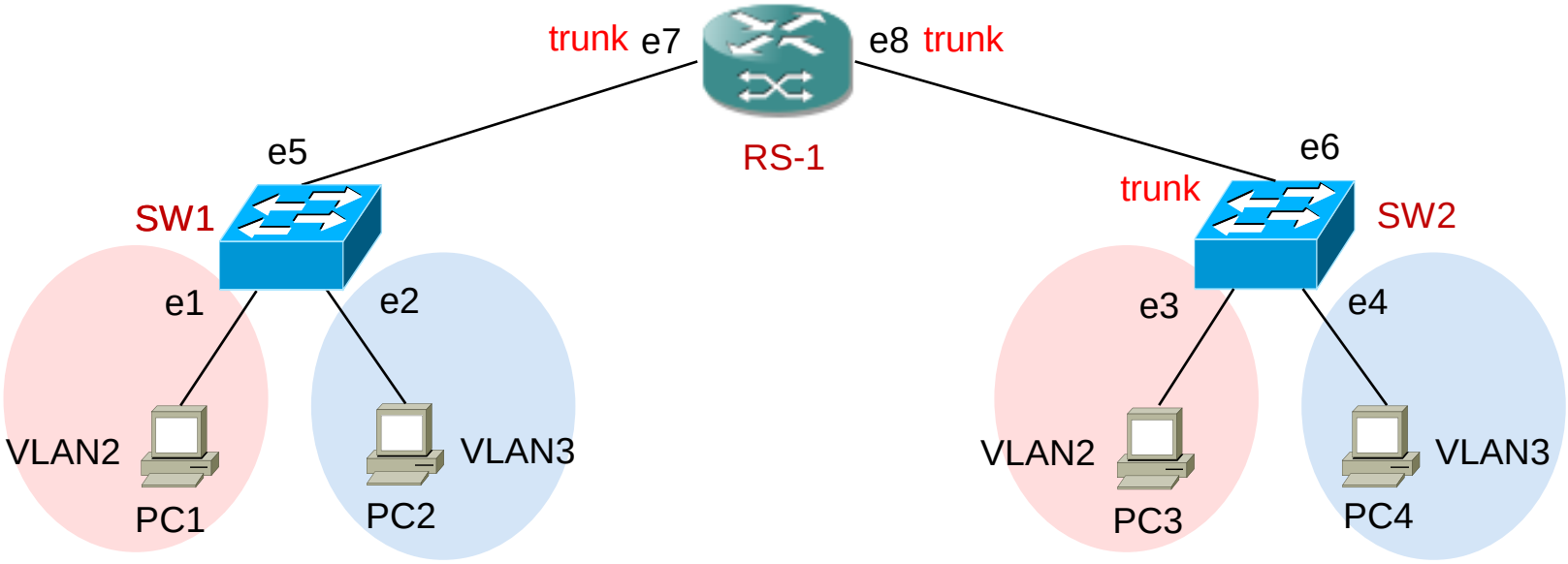
4. 三层交换机的应用

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
```

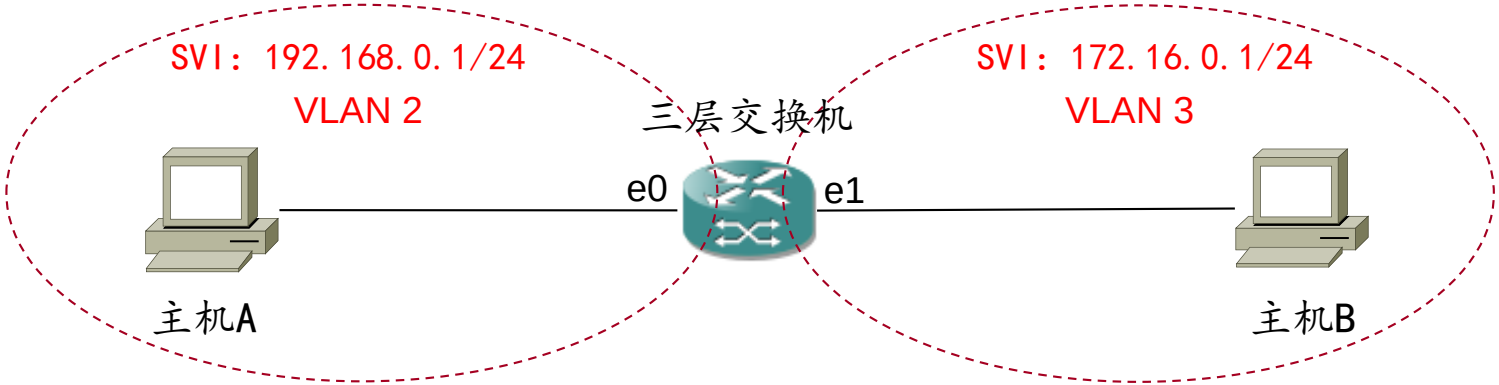


4. 三层交换机组网

- 三层交换机的通信过程分析

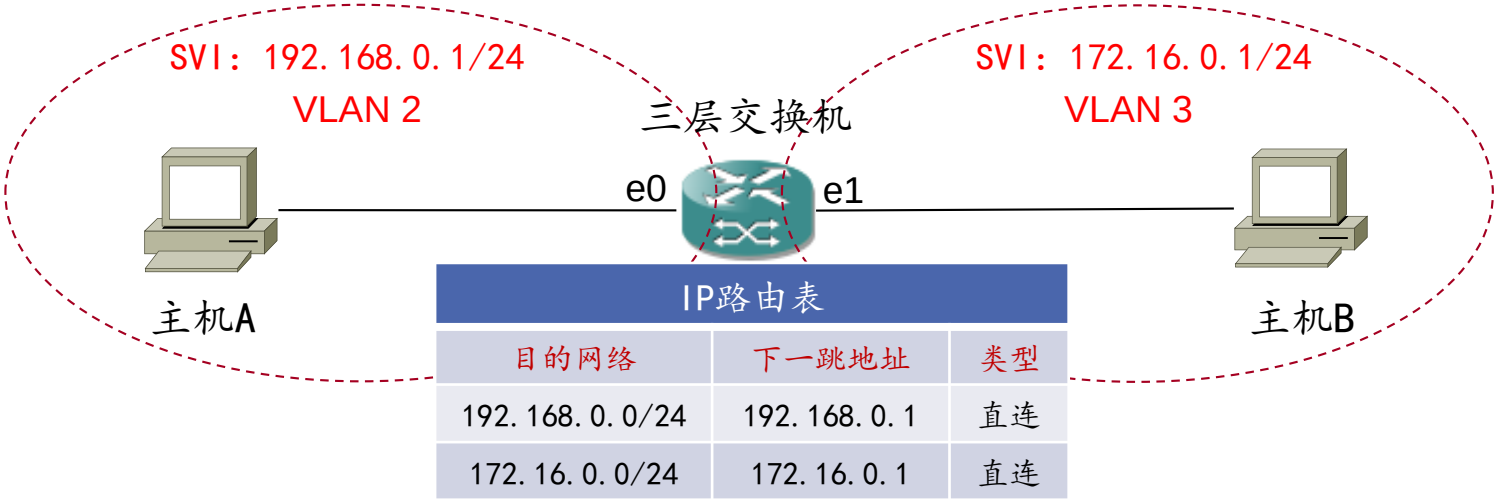
  ——不同VLAN间主机通信

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

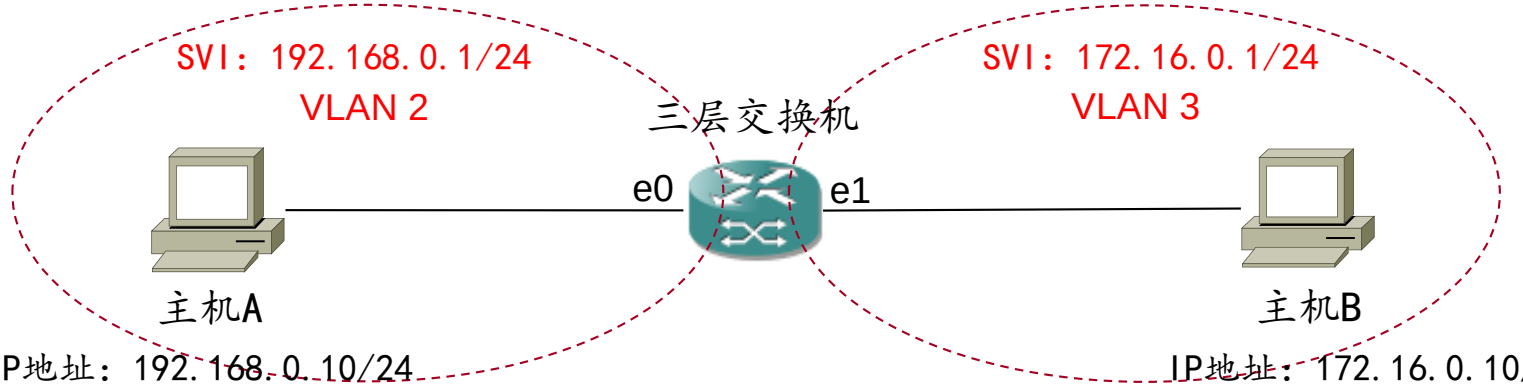


IP路由表		
目的网络	下一跳地址	类型
192.168.0.0/24	192.168.0.1	直连
172.16.0.0/24	172.16.0.1	直连

注意：

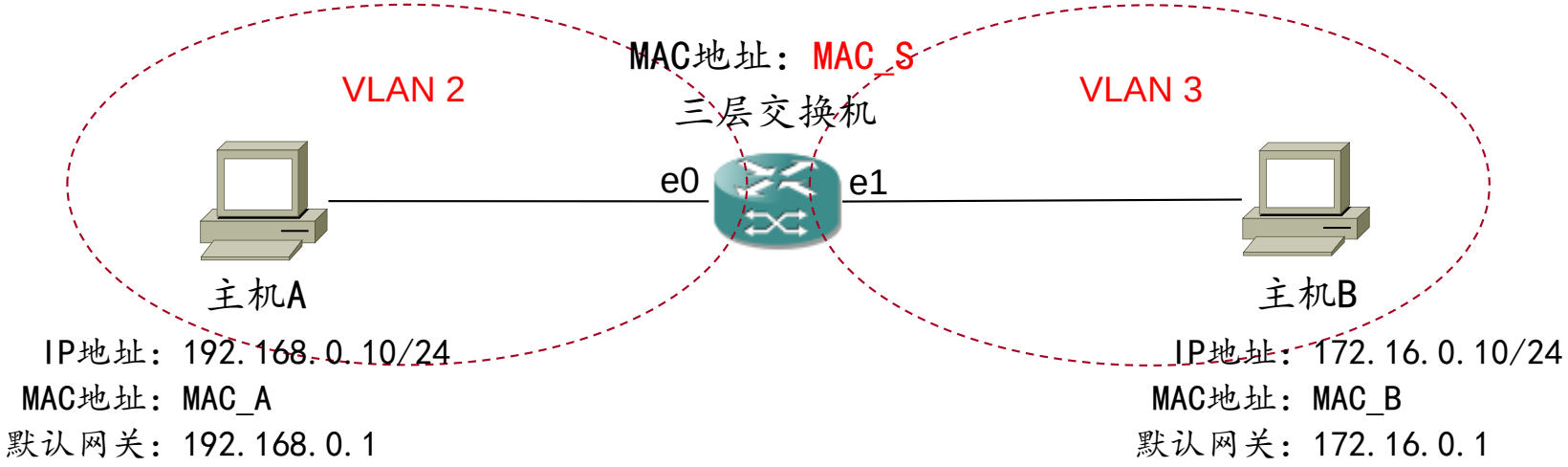
对于三层交换机来说，当配置完VLAN接口（SVI）地址后，三层交换机的IP路由表（软件路由表）中就有了相应的直连路由。

三层交换机的通信过程——不同VLAN间主机通信



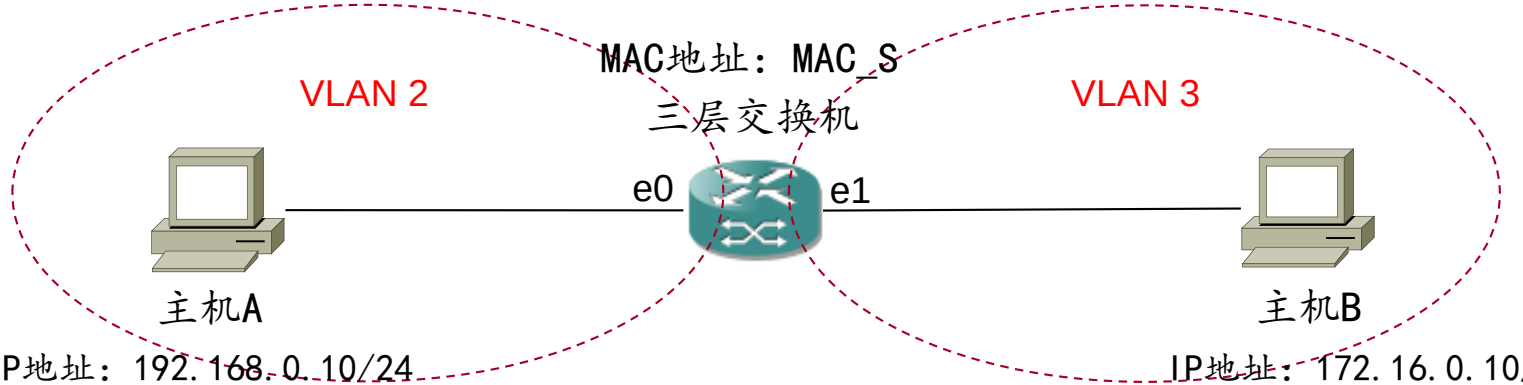
- 网络拓扑说明：
  - ③ 主机的IP地址和MAC地址如图所示，主机A的默认网关设置为三层交换机的VLAN2接口地址（192.168.0.1），主机B的默认网关设置为三层交换机的VLAN3接口地址（172.16.0.1）。

三层交换机的通信过程——不同VLAN间主机通信



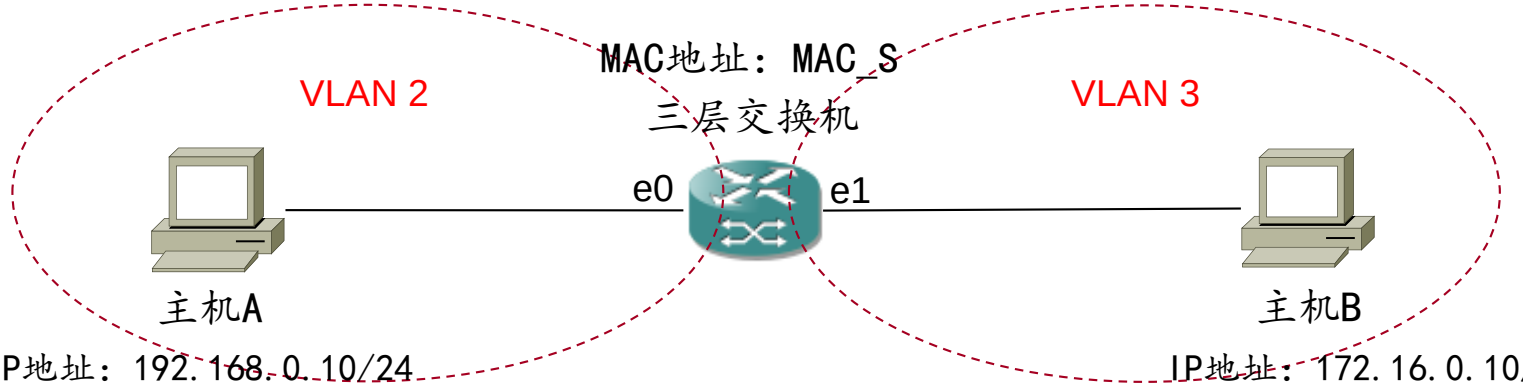
- 网络拓扑说明：
  - ④ 注意：三层交换机上各接口、各VLAN接口通常是共享一个MAC地址的，此处设为MAC_S。即VLAN2接口的MAC地址与VLAN3接口的MAC地址都是MAC_S。

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）

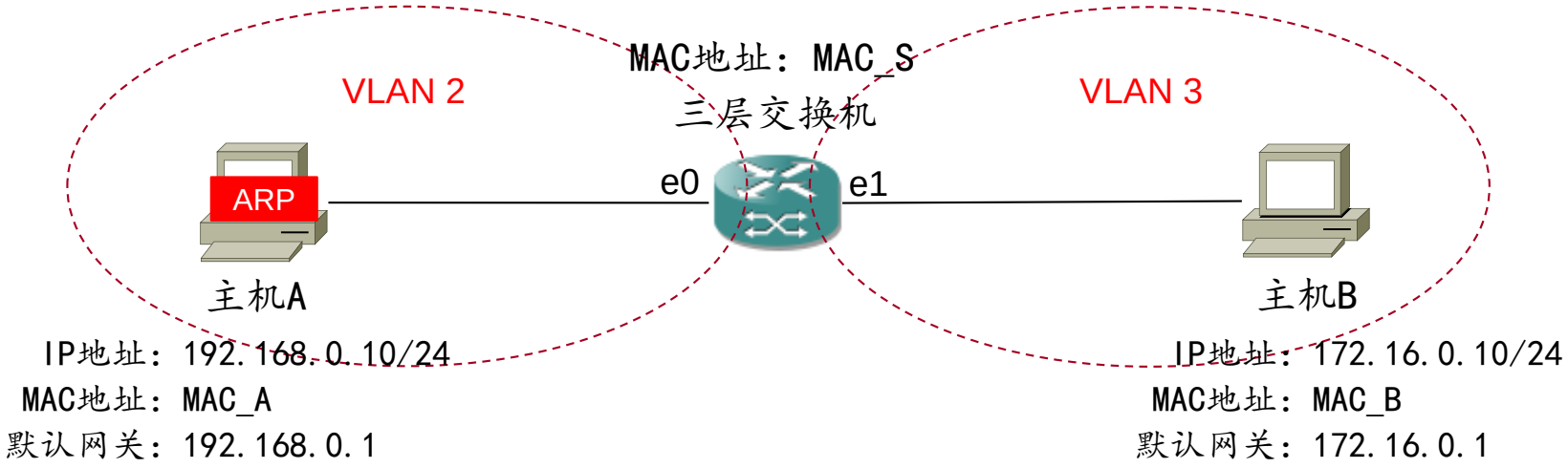
三层交换机的通信过程——不同VLAN间主机通信



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。

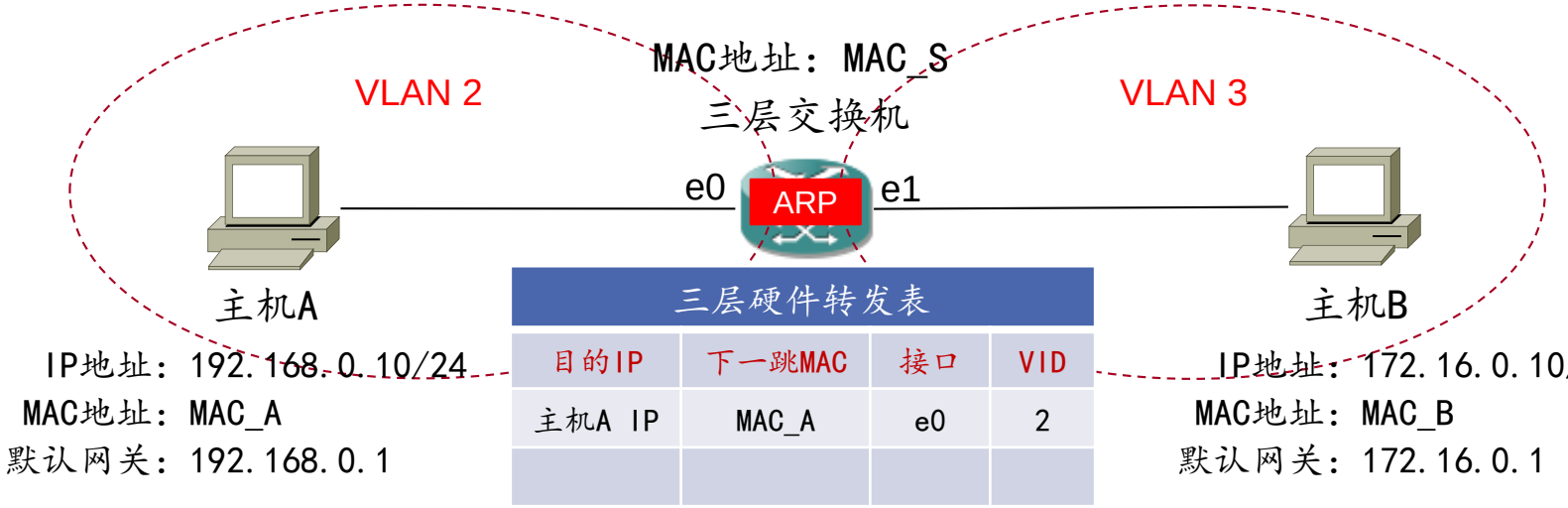
三层交换机的通信过程——不同VLAN间主机通信



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



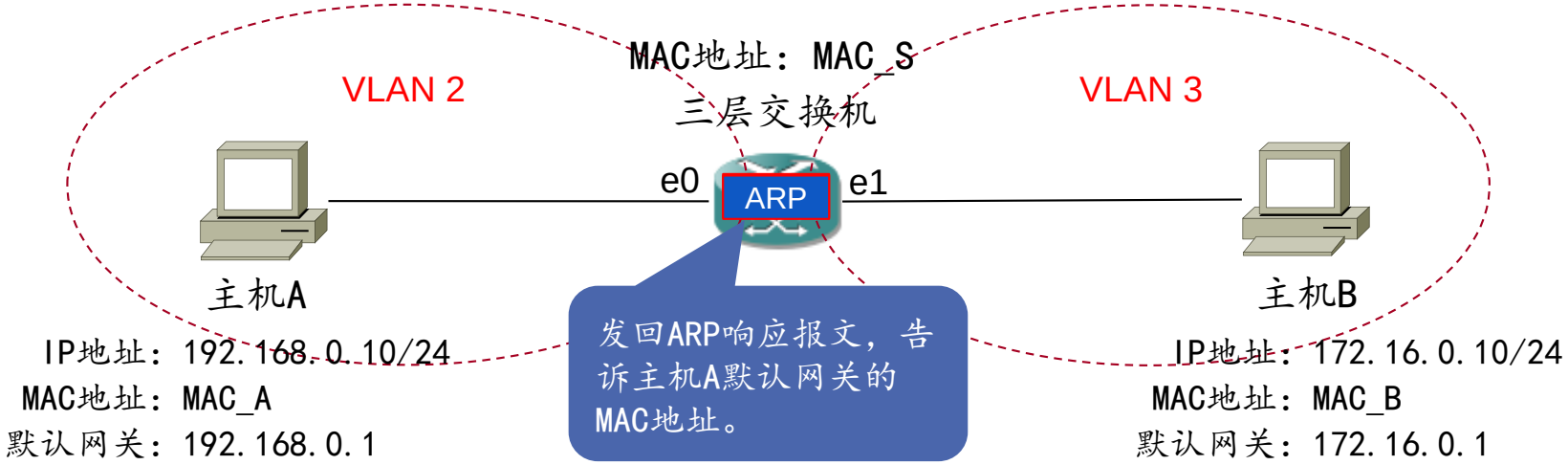
三层硬件转发表

目的IP	下一跳MAC	接口	VID
主机A IP	MAC_A	e0	2

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。

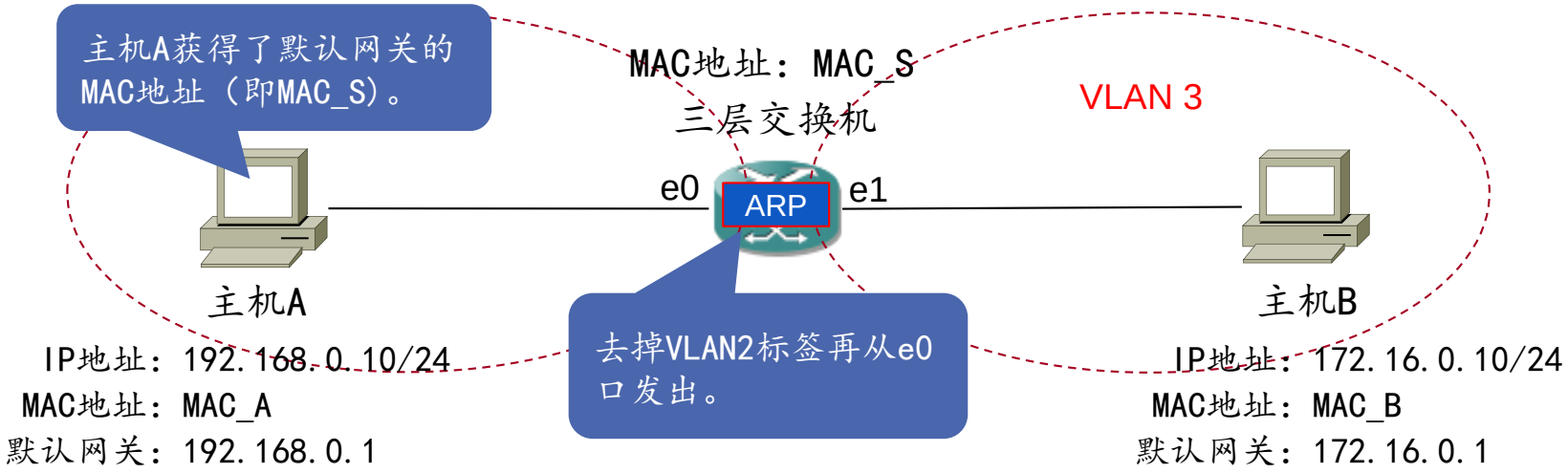
三层交换机的通信过程——不同VLAN间主机通信



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。

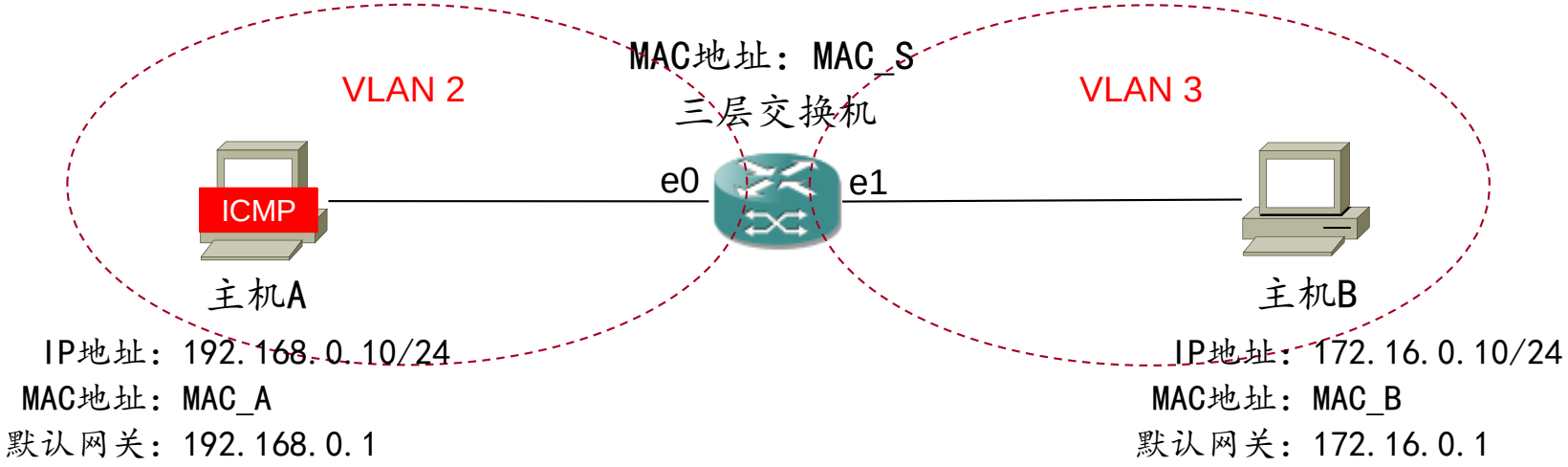
三层交换机的通信过程——不同VLAN间主机通信



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。

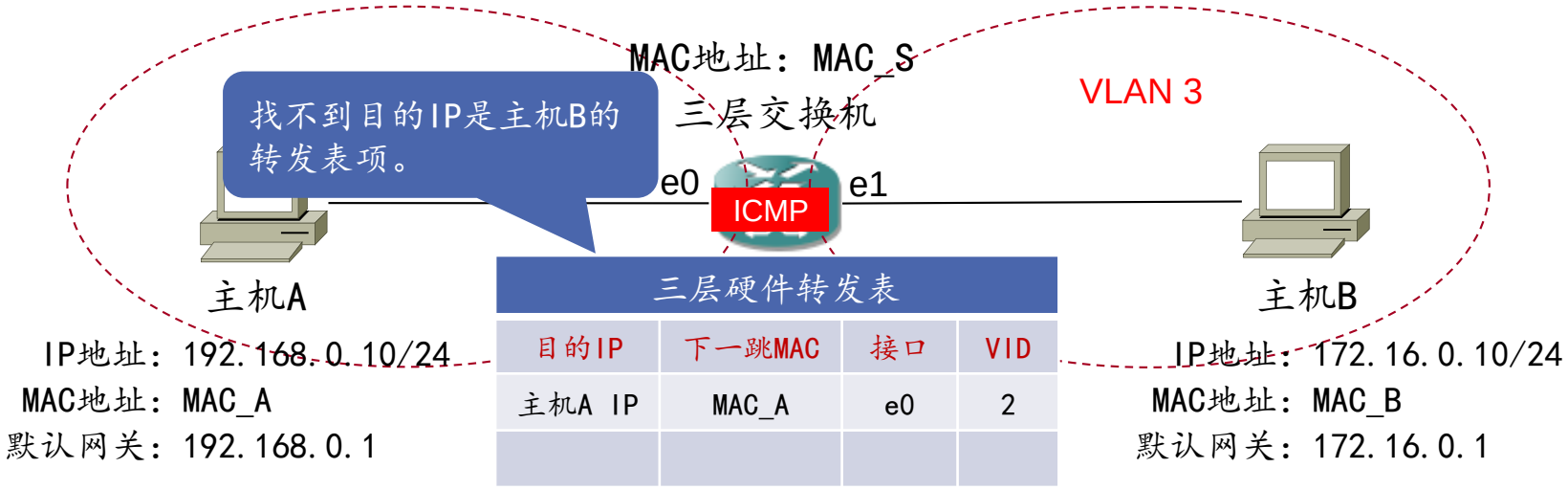
三层交换机的通信过程——不同VLAN间主机通信



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



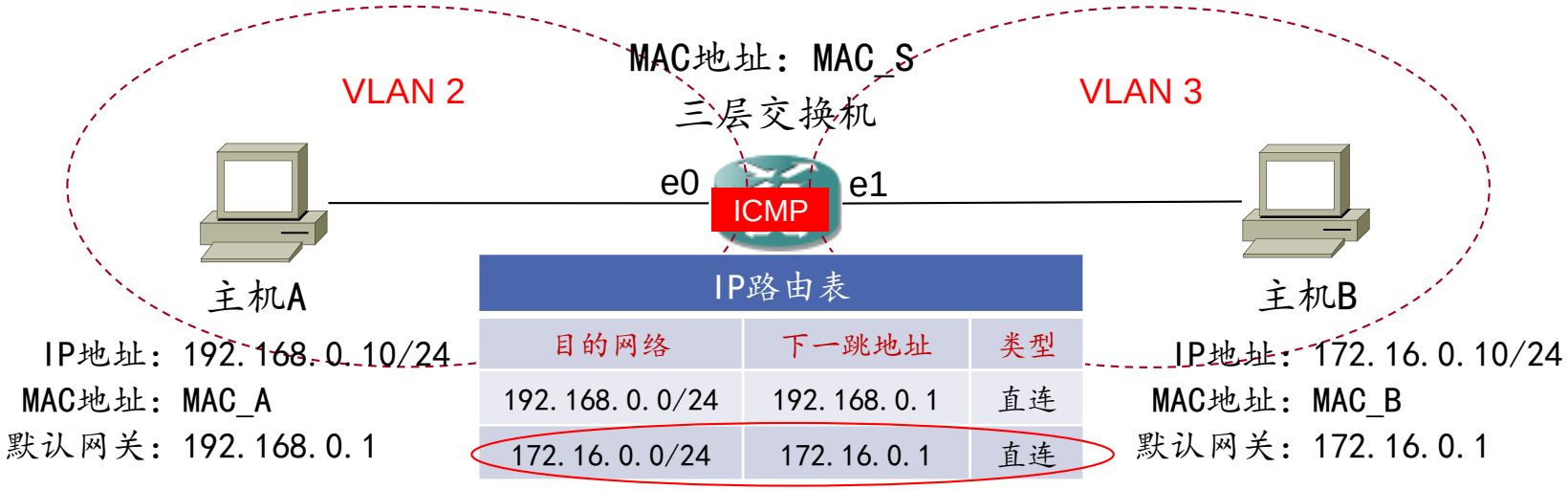
三层硬件转发表

目的IP	下一跳MAC	接口	VID
主机A IP	MAC_A	e0	2

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



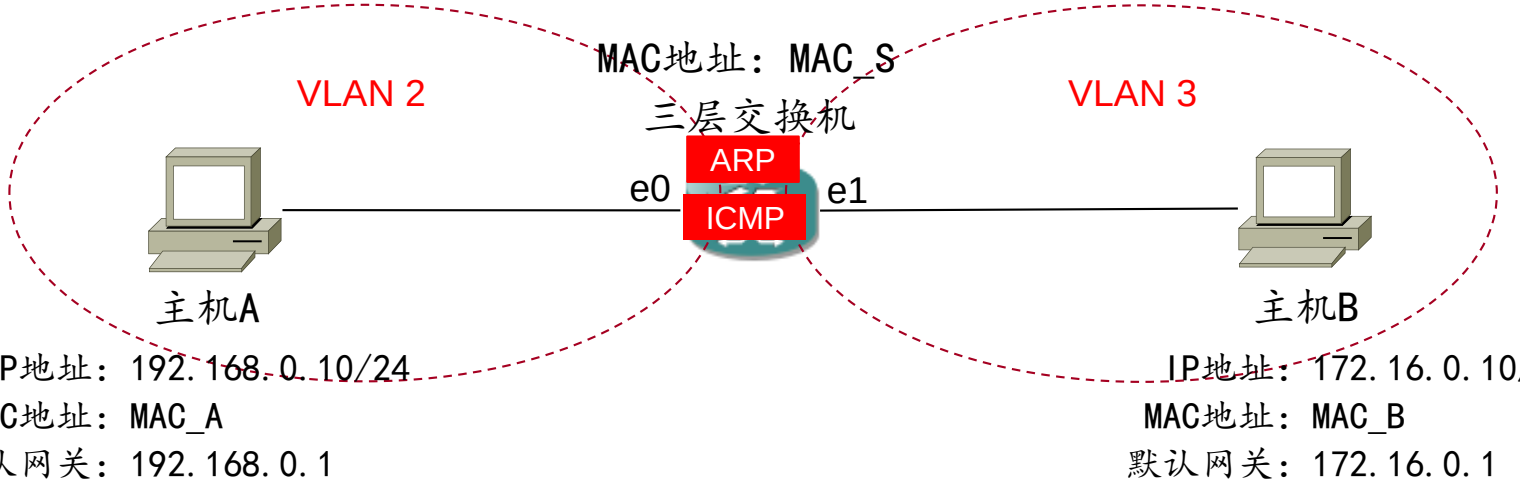
IP路由表

目的网络	下一跳地址	类型
192.168.0.0/24	192.168.0.1	直连
172.16.0.0/24	172.16.0.1	直连

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。

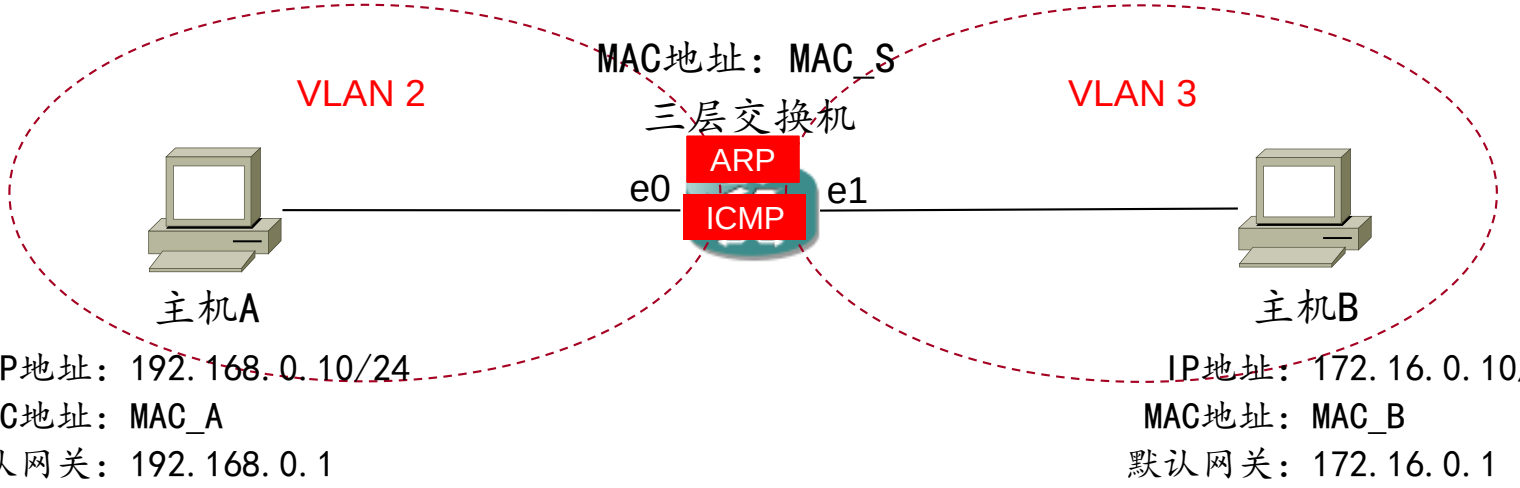
三层交换机的通信过程——不同VLAN间主机通信



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。

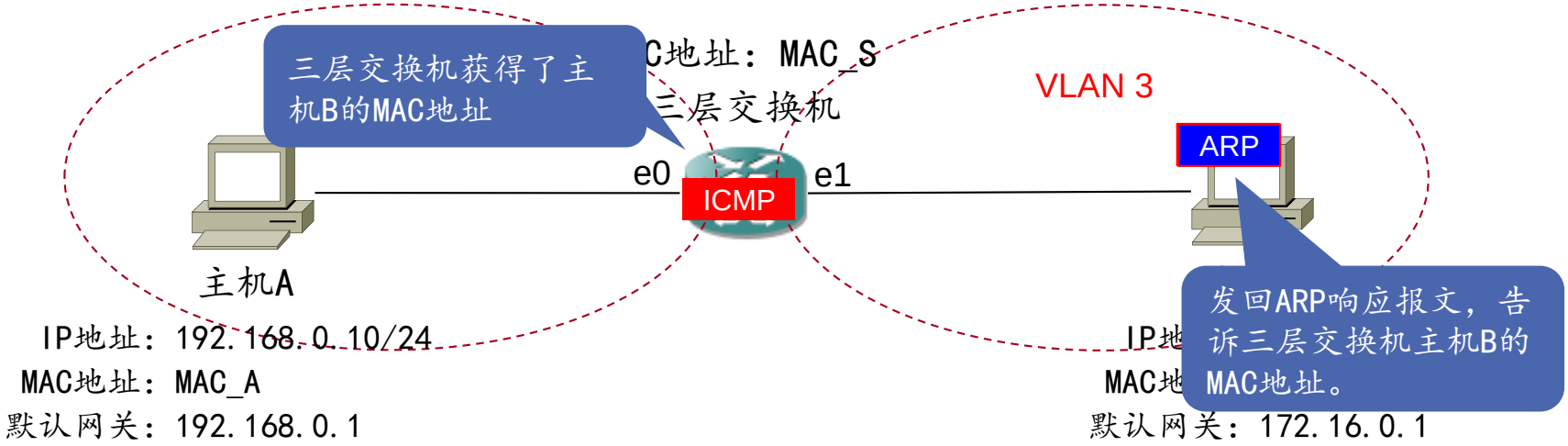
三层交换机的通信过程——不同VLAN间主机通信



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。

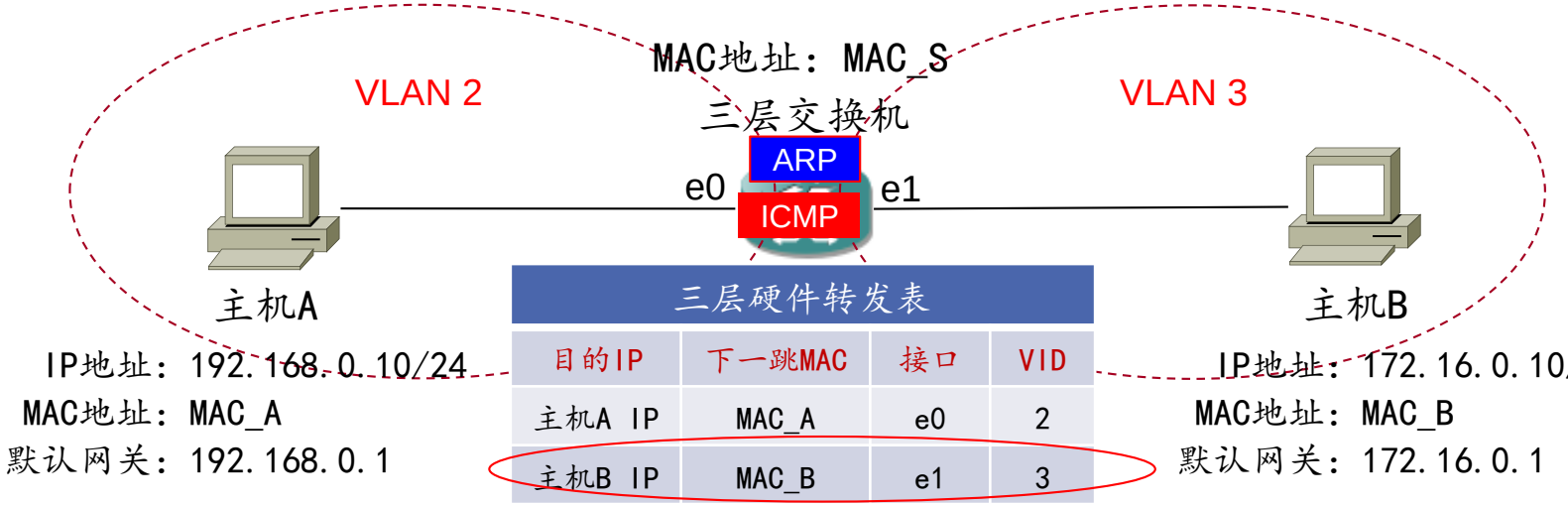
三层交换机的通信过程——不同VLAN间主机通信



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



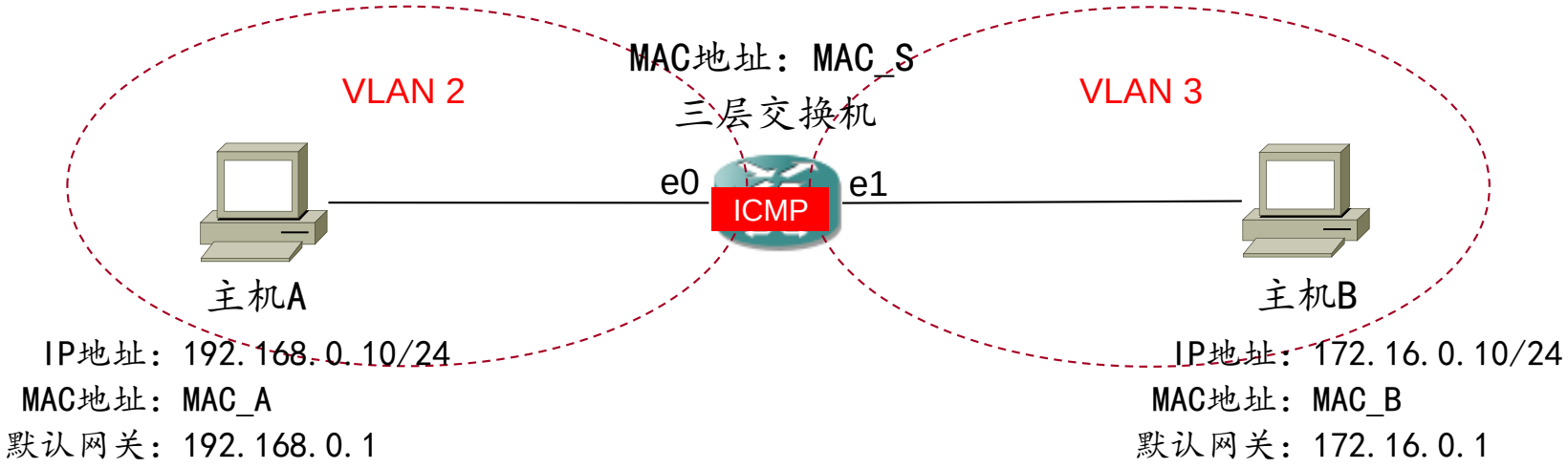
三层硬件转发表

目的IP	下一跳MAC	接口	VID
主机A IP	MAC_A	e0	2
主机B IP	MAC_B	e1	3

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。

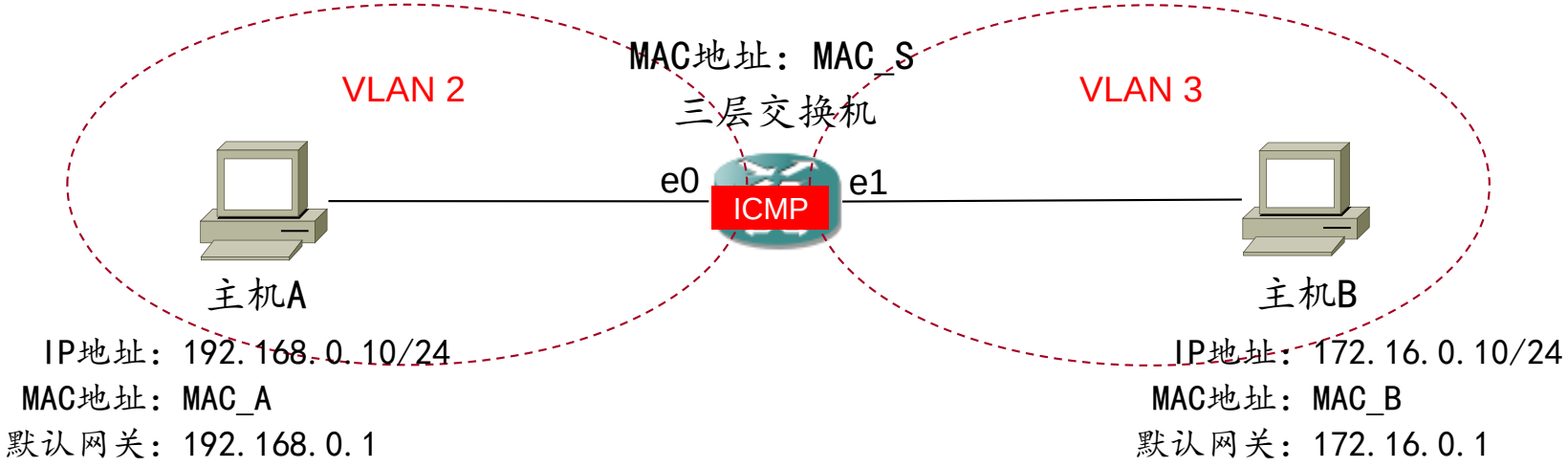
三层交换机的通信过程——不同VLAN间主机通信



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。

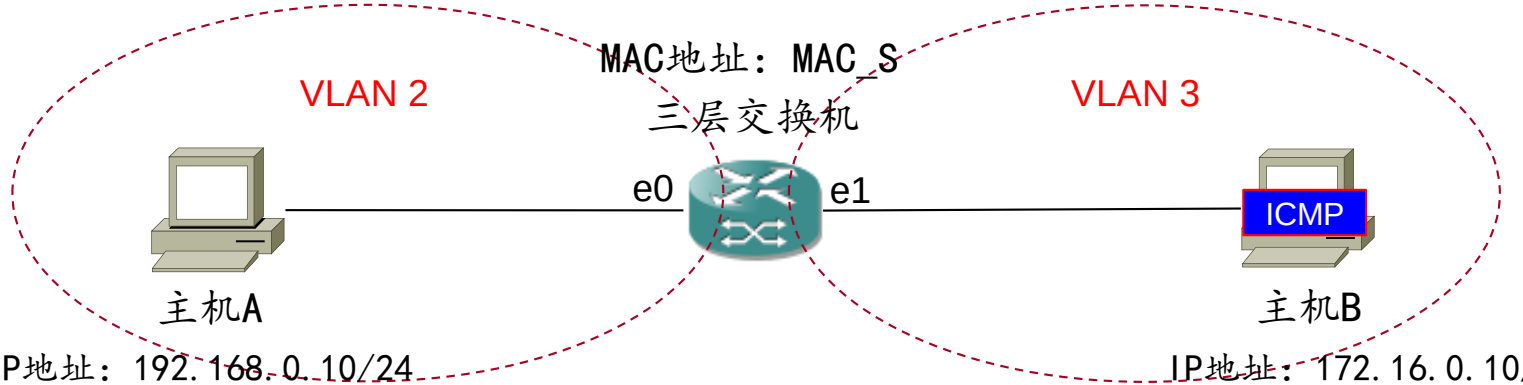
三层交换机的通信过程——不同VLAN间主机通信



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。

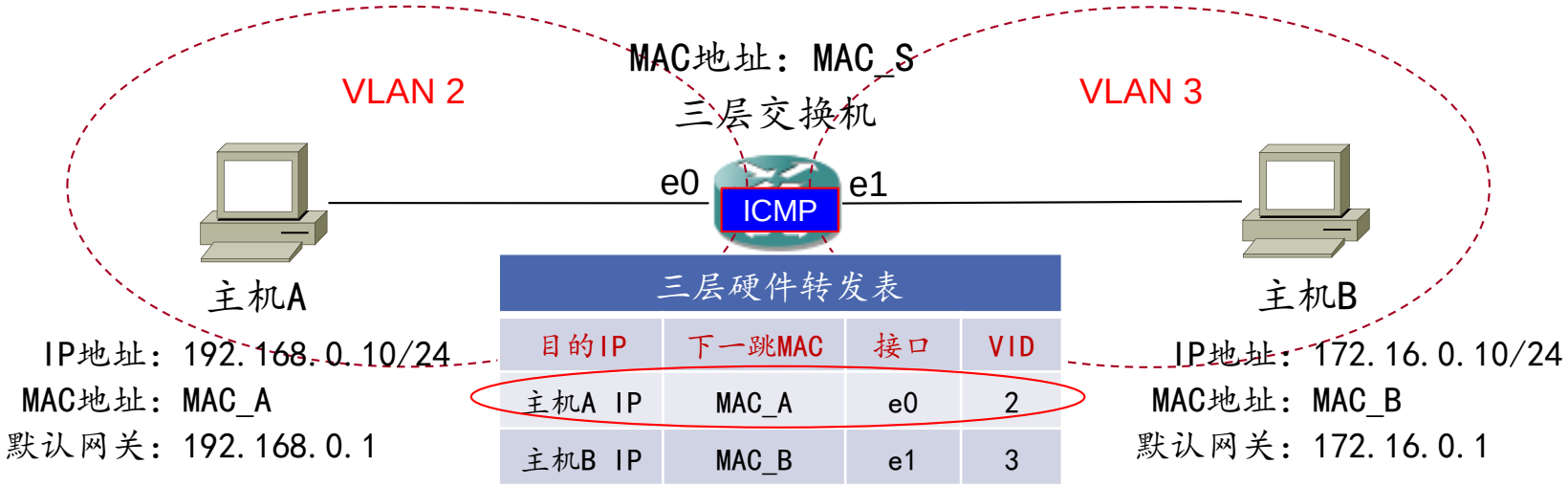
三层交换机的通信过程——不同VLAN间主机通信



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



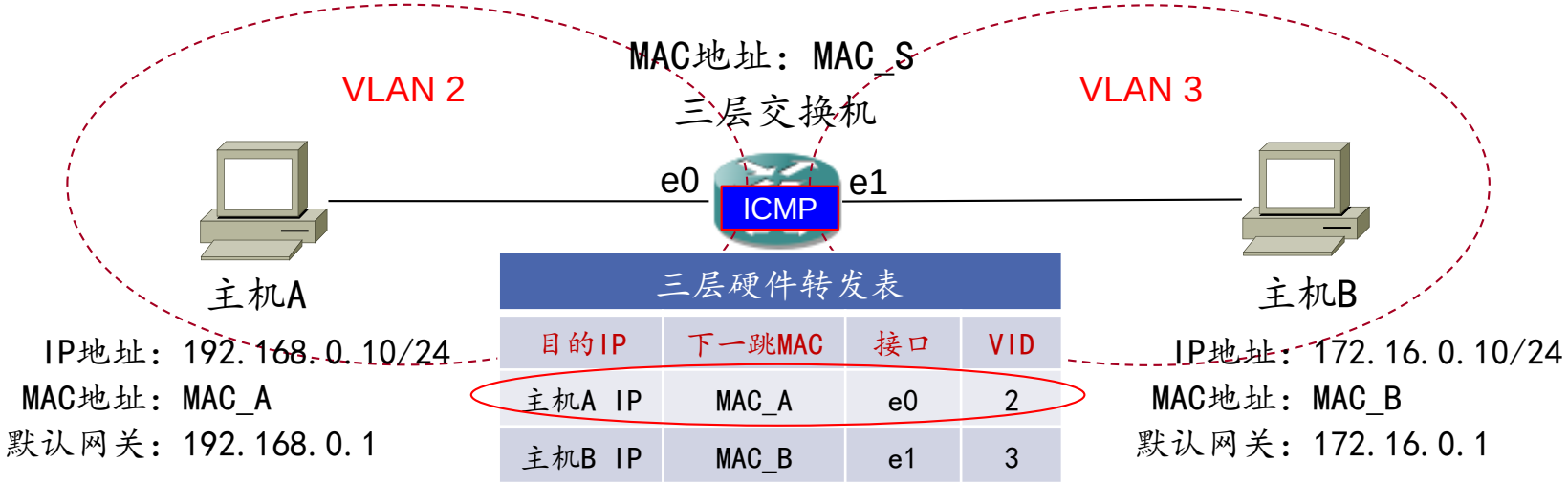
三层硬件转发表

目的IP	下一跳MAC	接口	VID
主机A IP	MAC_A	e0	2
主机B IP	MAC_B	e1	3

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



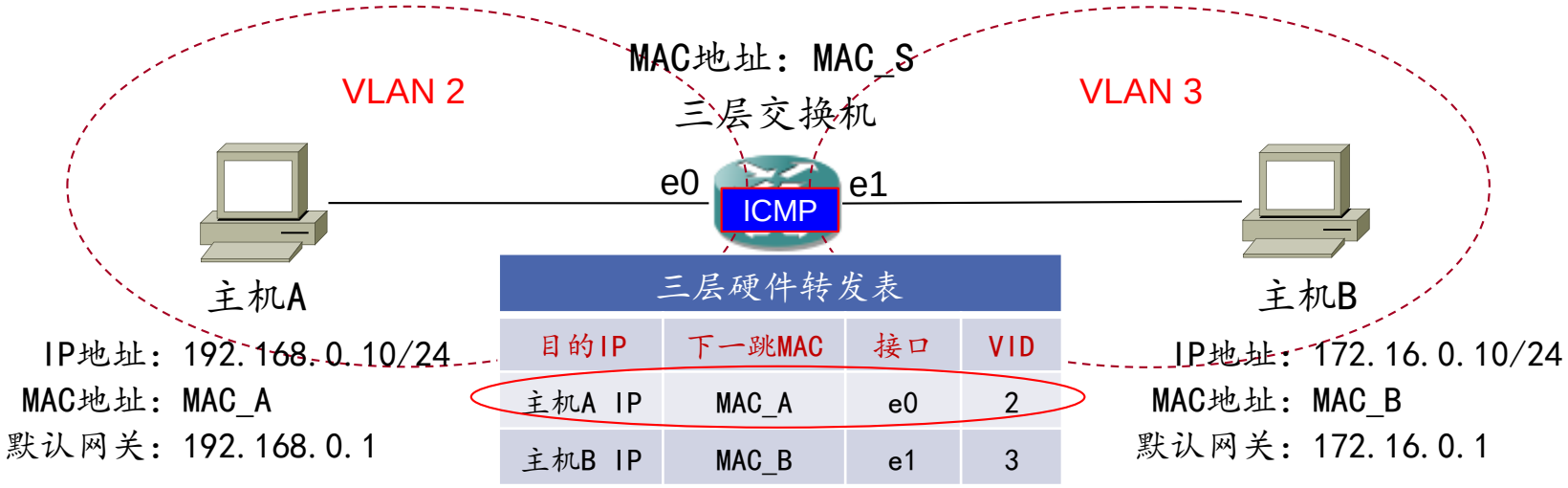
三层硬件转发表

目的IP	下一跳MAC	接口	VID
主机A IP	MAC_A	e0	2
主机B IP	MAC_B	e1	3

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



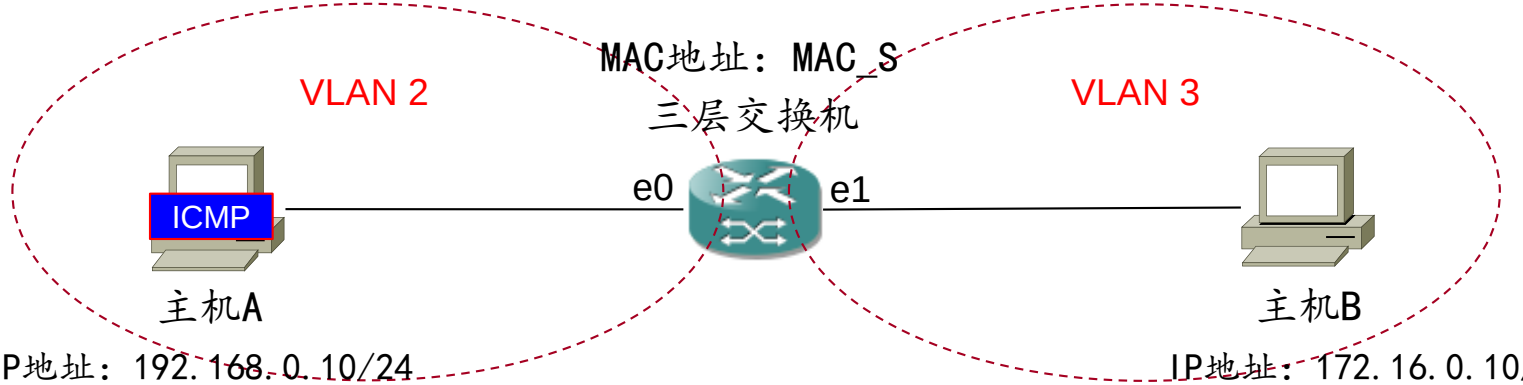
三层硬件转发表

目的IP	下一跳MAC	接口	VID
主机A IP	MAC_A	e0	2
主机B IP	MAC_B	e1	3

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

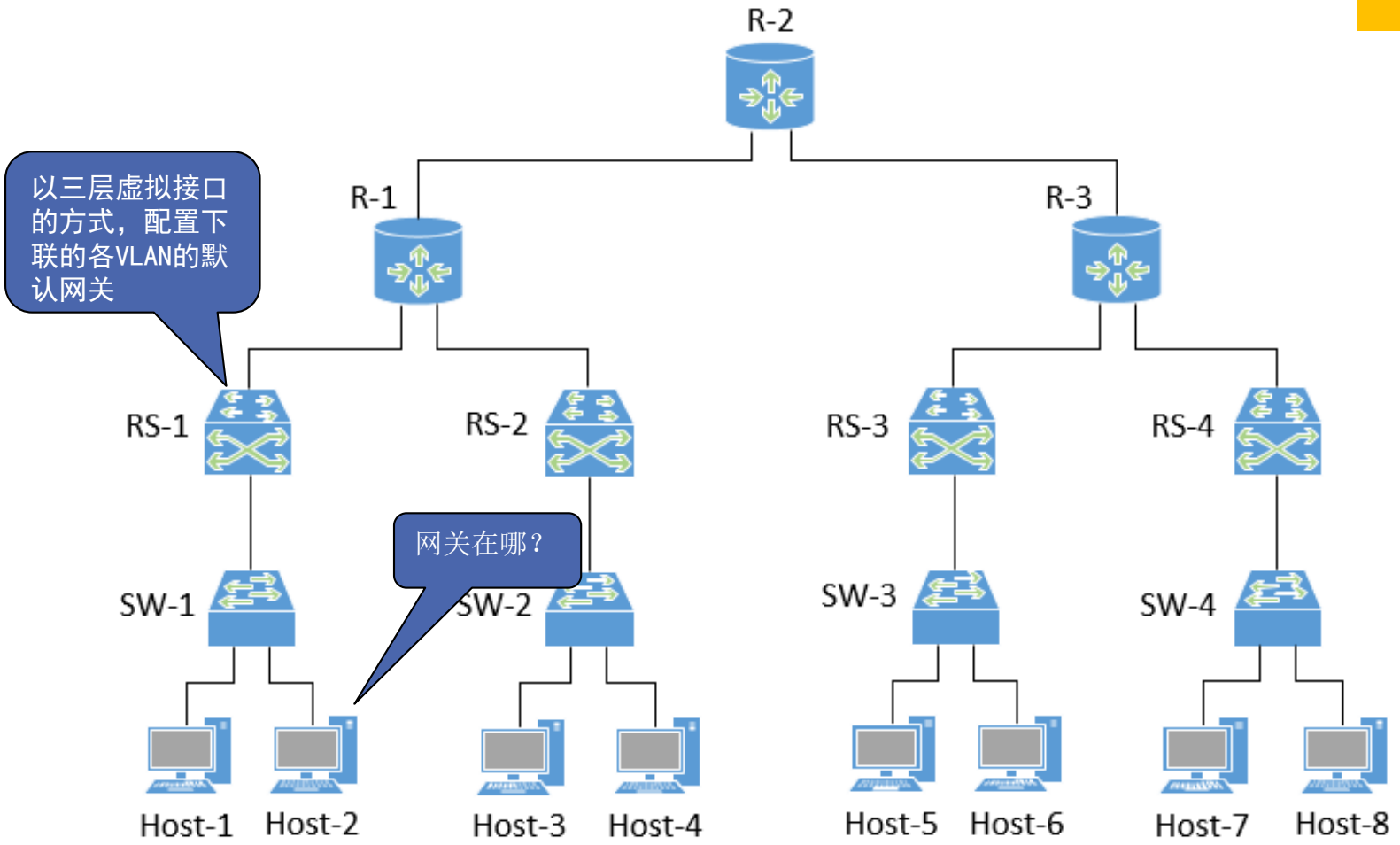


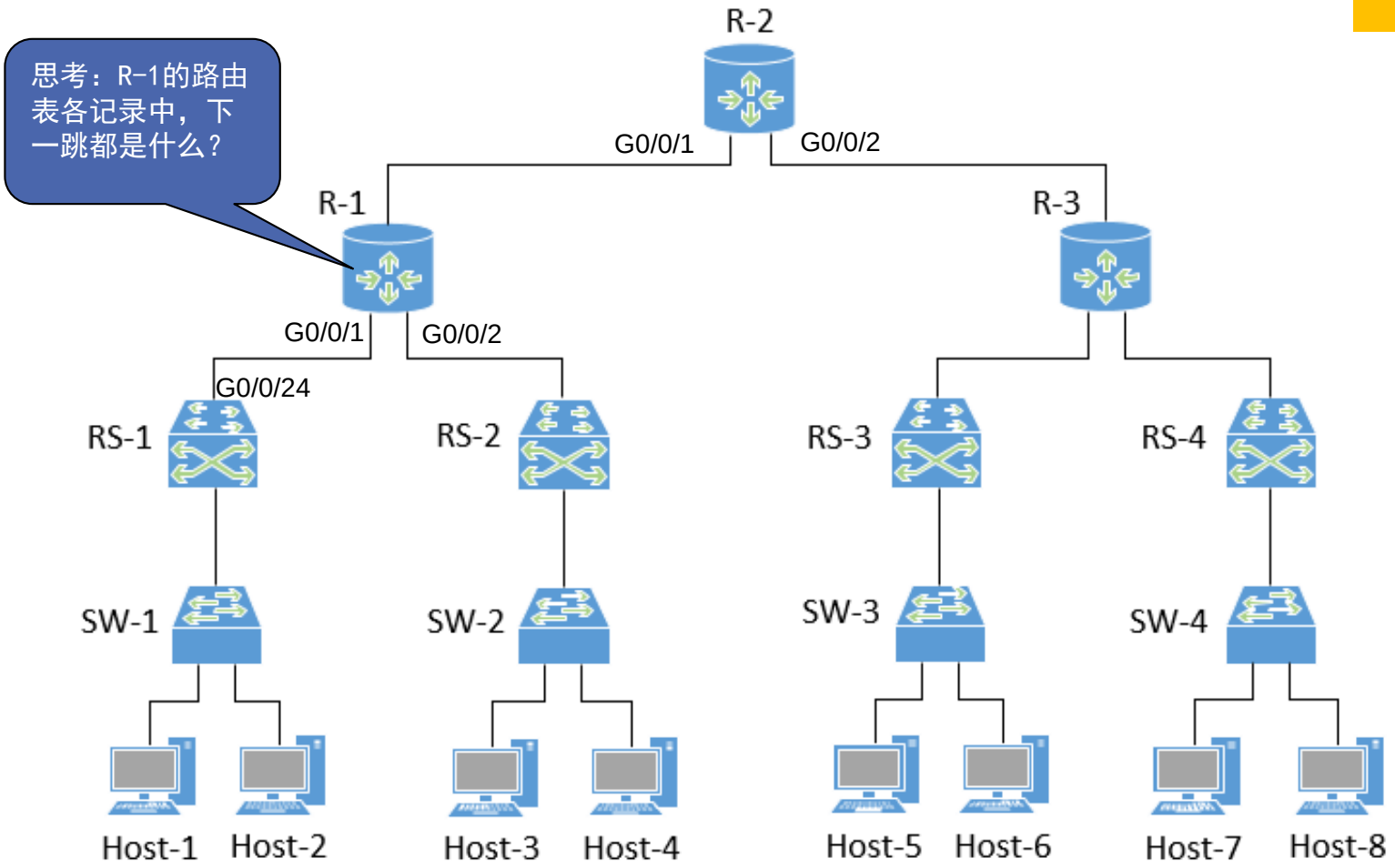
通信完成

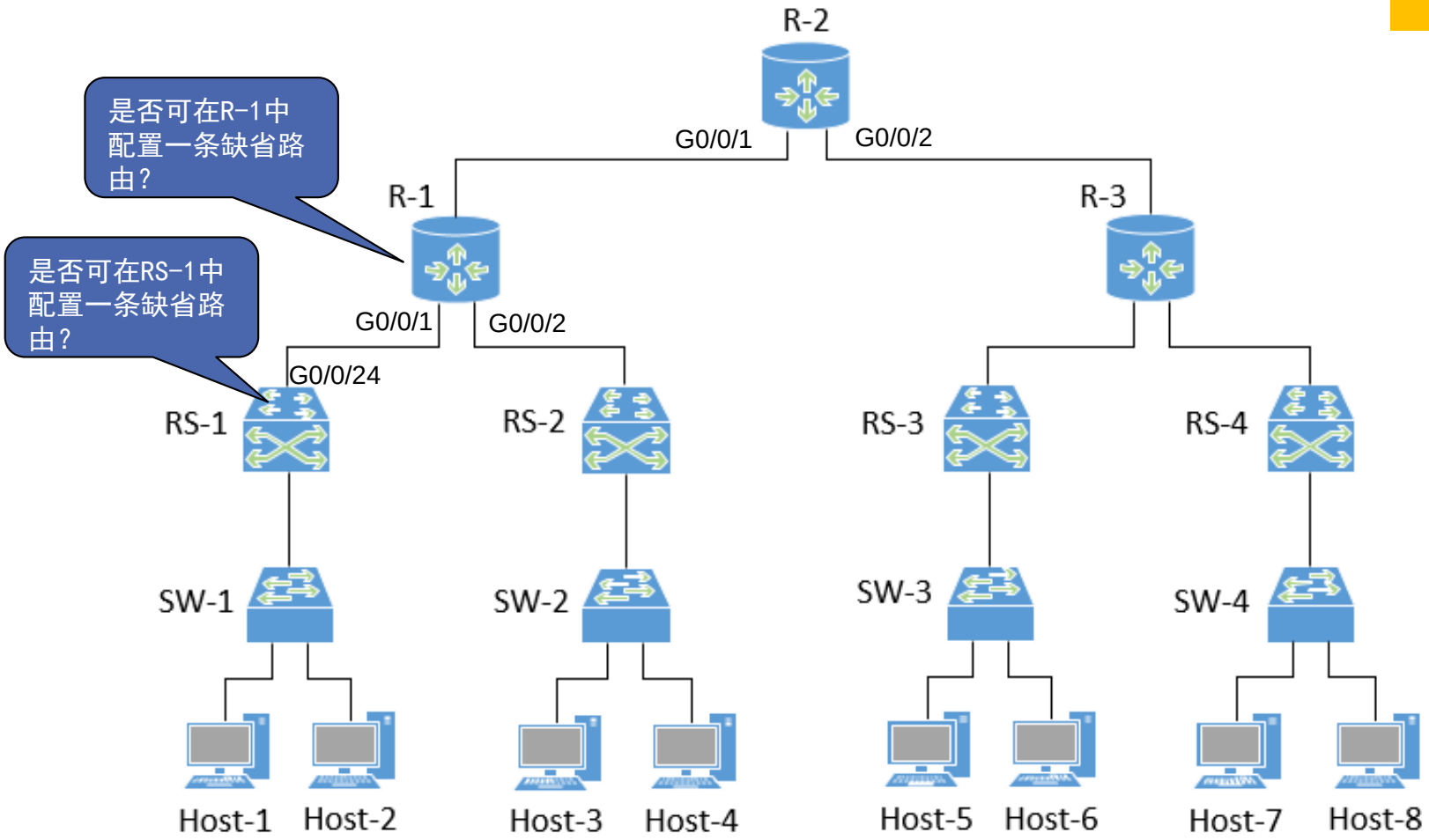
5. 路由器实现网络互联

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


R-2
R-1
R-3
以三层虚拟接口的方式，配置下联的各VLAN的默认网关
RS-1
RS-2
RS-3
RS-4
网关在哪？
SW-1
SW-2
SW-3
SW-4
Host-1
Host-2
Host-3
Host-4
Host-5
Host-6
Host-7
Host-8

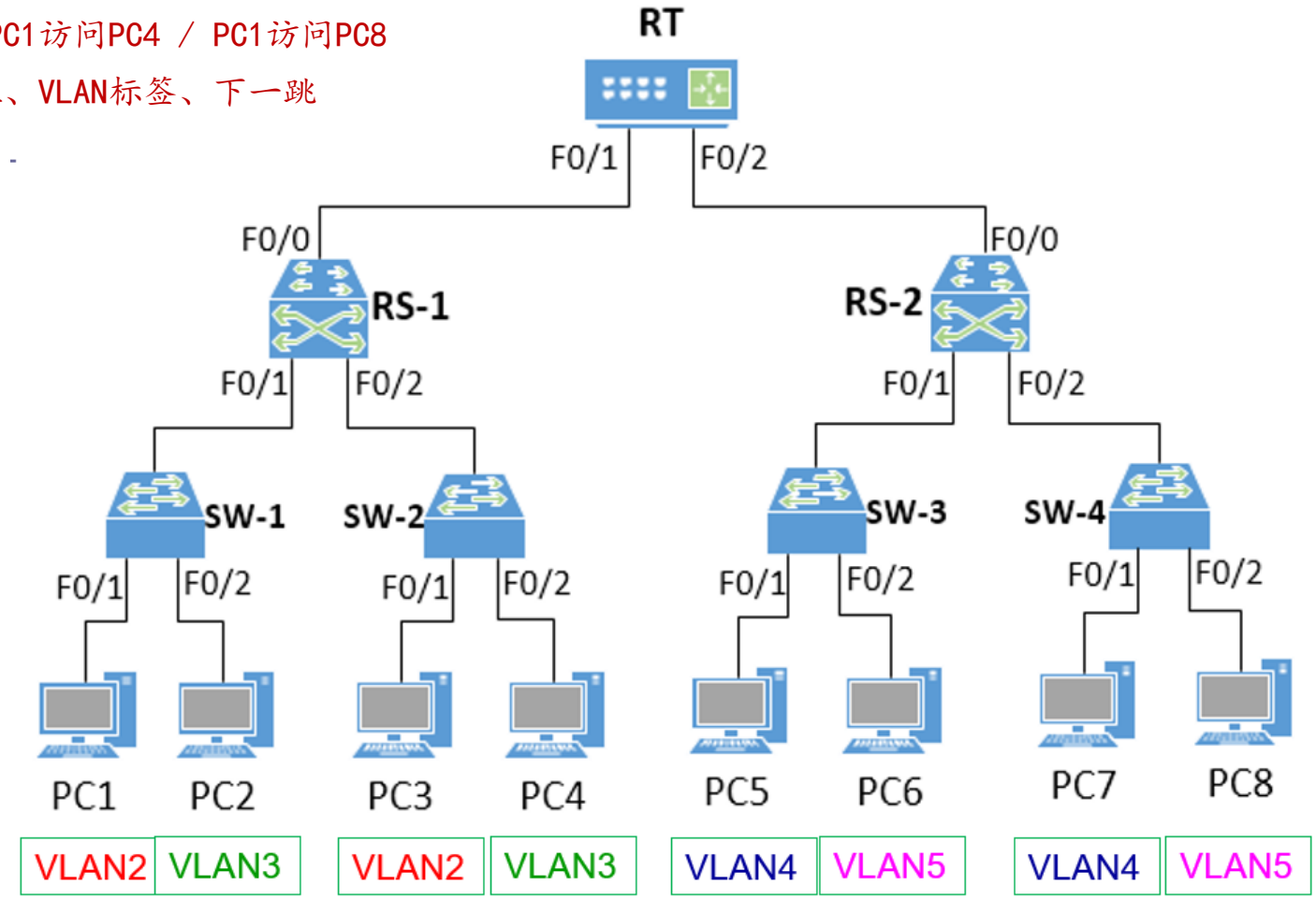

思考：R-1的路由表各记录中，下一跳都是什么？
R-2
G0/0/1
G0/0/2
R-1
R-3
G0/0/1
G0/0/2
G0/0/24
RS-1
RS-2
RS-3
RS-4
SW-1
SW-2
SW-3
SW-4
Host-1
Host-2
Host-3
Host-4
Host-5
Host-6
Host-7
Host-8


R-2
G0/0/1
G0/0/2
R-1
R-3
是否可在R-1中配置一条缺省路由？
是否可在RS-1中配置一条缺省路由？
G0/0/1
G0/0/2
G0/0/24
RS-1
RS-2
RS-3
RS-4
SW-1
SW-2
SW-3
SW-4
Host-1
Host-2
Host-3
Host-4
Host-5
Host-6
Host-7
Host-8

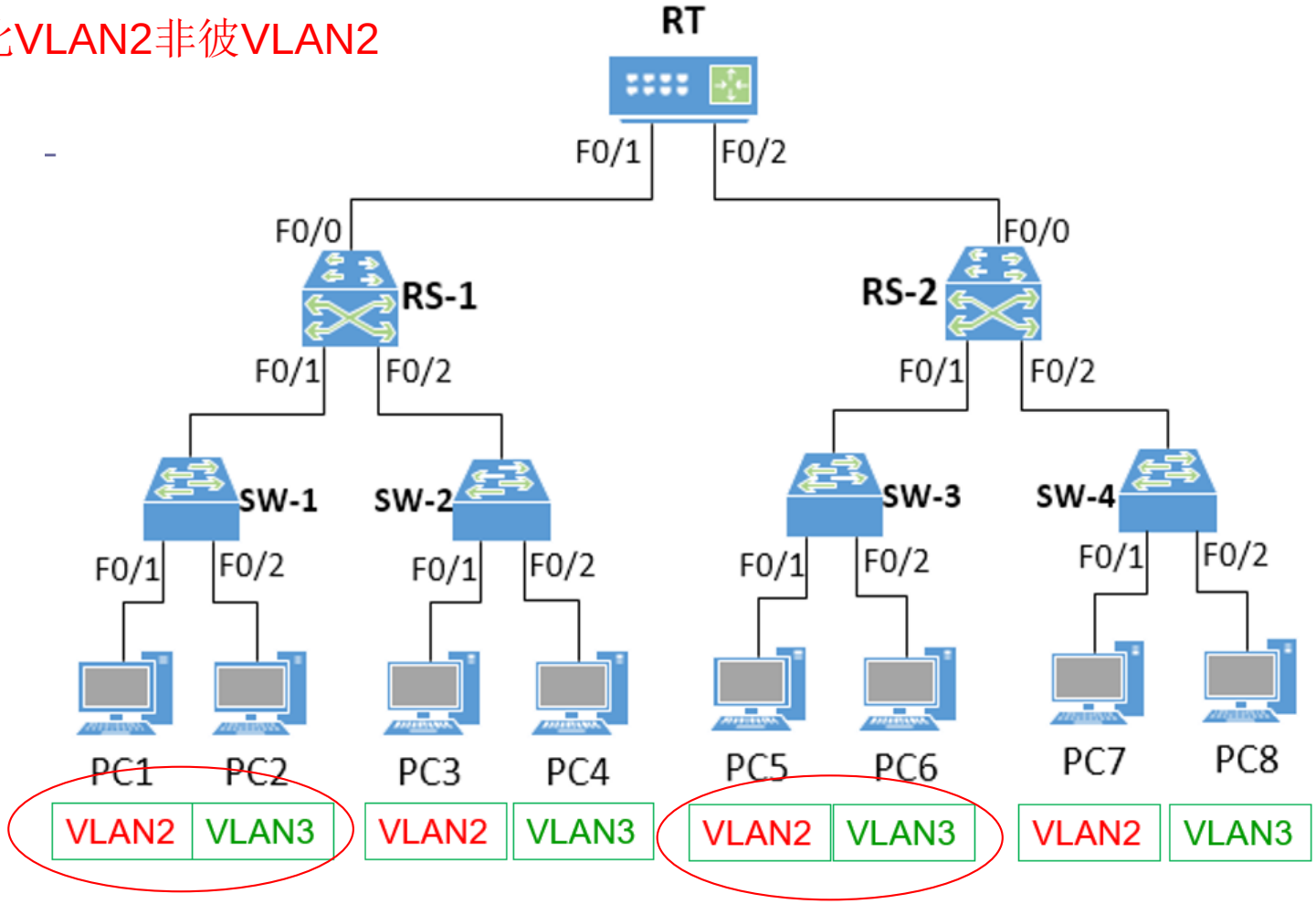
分别分析：

PC1访问PC3 / PC1访问PC4 / PC1访问PC8

网关、首部地址、VLAN标签、下一跳



此VLAN2非彼VLAN2



路由选择协议

分层次的路由选择协议

—— 互联网那么大，如何实现路由？

路由选择协议——分层次的路由选择协议

- **互联网采用自适应的（即动态的）、分布式路由选择协议。由于以下原因，互联网采用分层次的路由选择协议。**
  - （1）互联网的规模非常大。
    - 如果让所有的路由器知道所有的网络应怎样到达，则这种路由表将非常大，处理起来也太花时间。
    - 所有这些路由器之间交换路由信息所需的带宽就会使互联网的通信链路饱和。
  - （2）不仅如此，许多单位并不想让外界了解本单位网络建设的具体细节，包括网络结构以及所采用的路由选择协议，但同时还希望连接到互联网上。

路由选择协议——分层次的路由选择协议

- 自治系统（Autonomous System，AS）
  - 为此，整个互联网被划分为许多较小的自治系统（Autonomous Ssystem，简称 AS）。
  - 自治系统AS的定义：
    - 是在单一技术管理下的许多网络、IP地址以及路由器，而这些路由器使用一种自治系统内部的路由选择协议和共同的度量。每一个 AS 对其他 AS 表现出的是一个单一的和一致的路由选择策略
  - 所以，结合自治系统的概念，从路由选择协议的使用范围的角度来看，就把互联网的路由选择协议分为两大类：

路由选择协议——分层次的路由选择协议

- **互联网的两大类路由选择协议：**
  - 内部网关协议 IGP (Interior Gateway Protocol)
    - 在一个自治系统内部使用的路由选择协议。
    - 目前这类路由选择协议使用得最多，如RIP和OSPF协议。
  - 外部网关协议 EGP (External Gateway Protocol)
    - 若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中，这样的协议就是外部网关协议EGP。
    - 在外部网关协议中目前使用最多的是BGP-4。

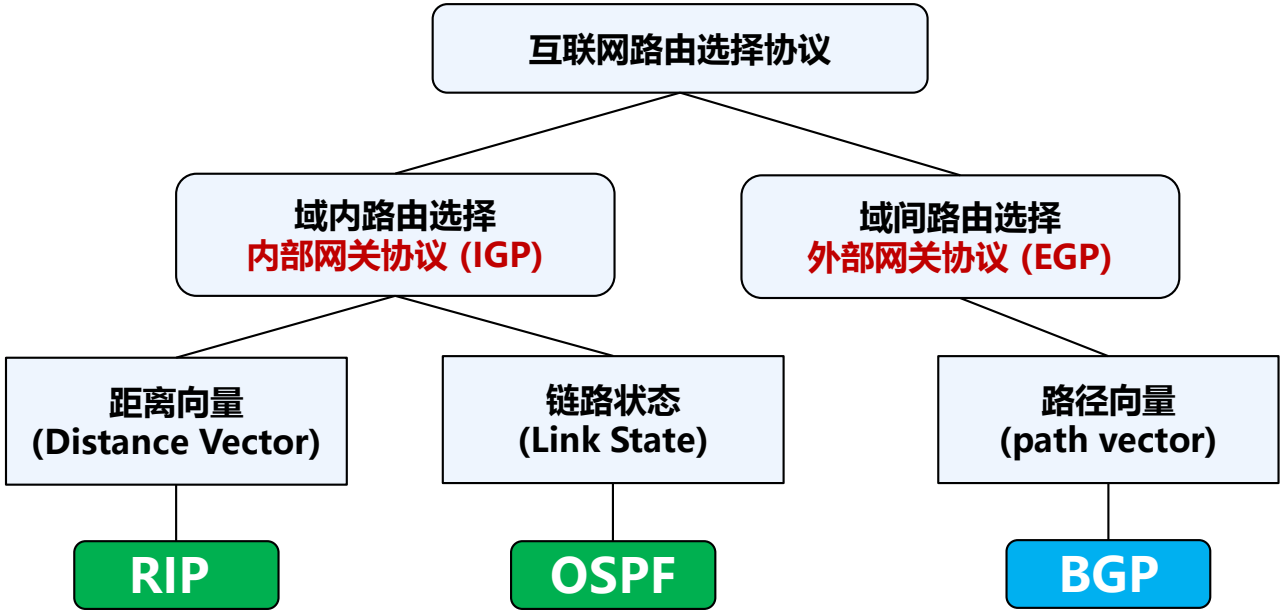
路由选择协议——分层次的路由选择协议

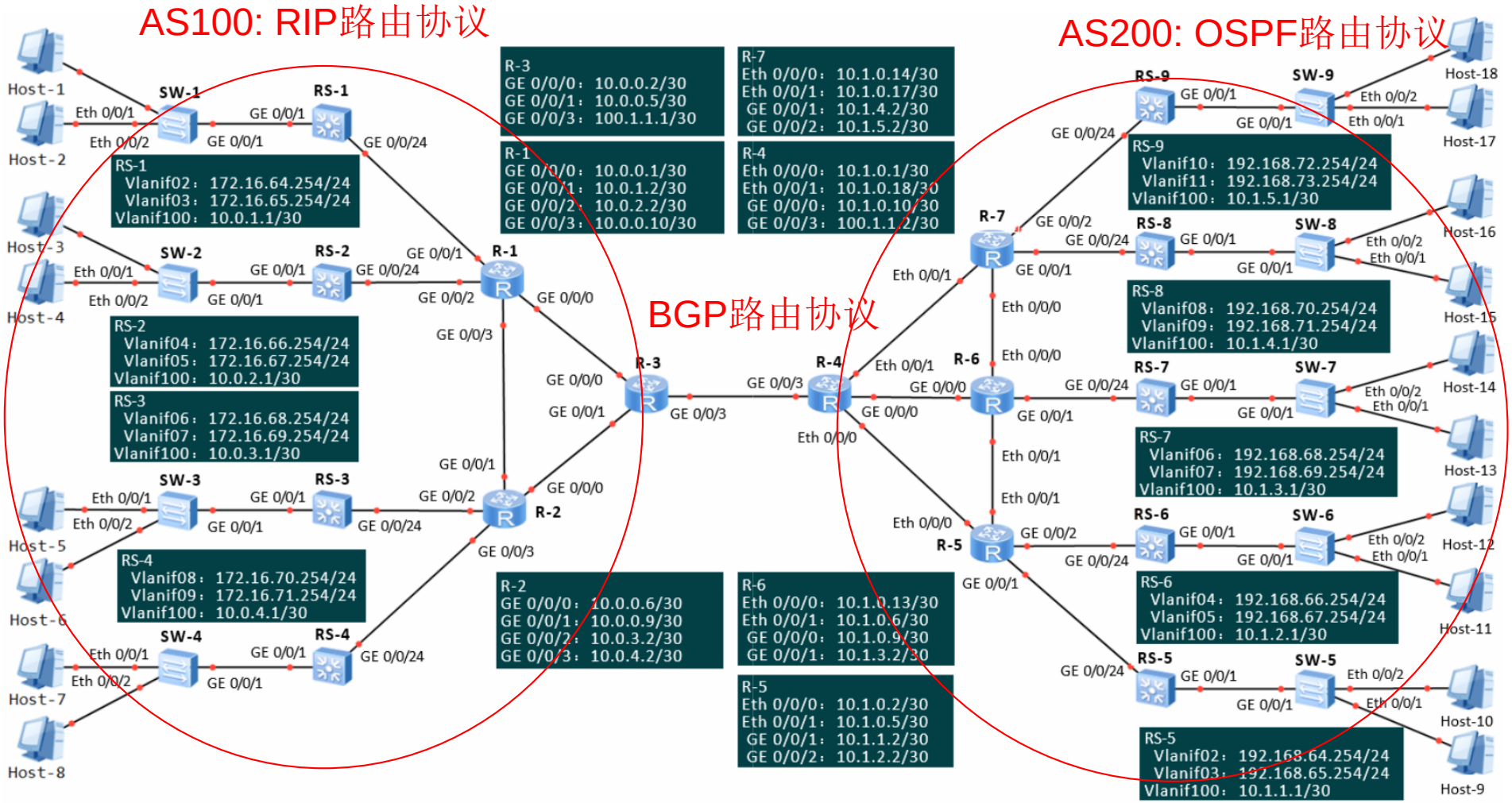
- 互联网的两大类路由选择协议：

自治系统之间的路由选择叫做域间路由选择 (interdomain routing)
自治系统内部的路由选择叫做域内路由选择 (intradomain routing)

路由选择协议——分层次的路由选择协议

- 互联网的两大类路由选择协议：




AS100: RIP路由协议
AS200: OSPF路由协议
BGP路由协议
Host-1
Host-2
Host-3
Host-4
Host-5
Host-6
Host-7
Host-8
SW-1
SW-2
SW-3
SW-4
RS-1
RS-2
RS-3
RS-4
R-1
R-2
R-3
R-4
R-5
R-6
R-7
RS-9
SW-9
RS-8
SW-8
RS-7
SW-7
RS-6
SW-6
RS-5
SW-5
Host-18
Host-17
Host-16
Host-15
Host-14
Host-13
Host-12
Host-11
Host-10
Host-9
Eth 0/0/1
Eth 0/0/2
GE 0/0/1
GE 0/0/24
GE 0/0/0
GE 0/0/1
GE 0/0/2
GE 0/0/3
Eth 0/0/0
Eth 0/0/1
RS-1
Vlanif02：172.16.64.254/24
Vlanif03：172.16.65.254/24
Vlanif100：10.0.1.1/30
RS-2
Vlanif04：172.16.66.254/24
Vlanif05：172.16.67.254/24
Vlanif100：10.0.2.1/30
RS-3
Vlanif06：172.16.68.254/24
Vlanif07：172.16.69.254/24
Vlanif100：10.0.3.1/30
RS-4
Vlanif08：172.16.70.254/24
Vlanif09：172.16.71.254/24
Vlanif100：10.0.4.1/30
R-3
GE 0/0/0：10.0.0.2/30
GE 0/0/1：10.0.0.5/30
GE 0/0/3：100.1.1.1/30
R-1
GE 0/0/0：10.0.0.1/30
GE 0/0/1：10.0.1.2/30
GE 0/0/2：10.0.2.2/30
GE 0/0/3：10.0.0.10/30
R-2
GE 0/0/0：10.0.0.6/30
GE 0/0/1：10.0.0.9/30
GE 0/0/2：10.0.3.2/30
GE 0/0/3：10.0.4.2/30
R-7
Eth 0/0/0：10.1.0.14/30
Eth 0/0/1：10.1.0.17/30
GE 0/0/1：10.1.4.2/30
GE 0/0/2：10.1.5.2/30
R-4
Eth 0/0/0：10.1.0.1/30
Eth 0/0/1：10.1.0.18/30
GE 0/0/0：10.1.0.10/30
GE 0/0/3：100.1.1.2/30
R-6
Eth 0/0/0：10.1.0.13/30
Eth 0/0/1：10.1.0.6/30
GE 0/0/0：10.1.0.9/30
GE 0/0/1：10.1.3.2/30
R-5
Eth 0/0/0：10.1.0.2/30
Eth 0/0/1：10.1.0.5/30
GE 0/0/1：10.1.1.2/30
GE 0/0/2：10.1.2.2/30
RS-9
Vlanif10：192.168.72.254/24
Vlanif11：192.168.73.254/24
Vlanif100：10.1.5.1/30
RS-8
Vlanif08：192.168.70.254/24
Vlanif09：192.168.71.254/24
Vlanif100：10.1.4.1/30
RS-7
Vlanif06：192.168.68.254/24
Vlanif07：192.168.69.254/24
Vlanif100：10.1.3.1/30
RS-6
Vlanif04：192.168.66.254/24
Vlanif05：192.168.67.254/24
Vlanif100：10.1.2.1/30
RS-5
Vlanif02：192.168.64.254/24
Vlanif03：192.168.65.254/24
Vlanif100：10.1.1.1/30

内部网关协议RIP

路由选择协议——RIP

- 路由信息协议 (Routing Information Protocol，RIP) 是内部网关协议 IGP中最先得到广泛使用的协议。
  - RIP 是一种分布式的基于距离向量的路由选择协议，是互联网的标准协议。
  - RIP 最大优点是：简单。
  - RIP 要求网络中的每个路由器都要维护从它自己到其他每一个目的网络的距离记录。

路由选择协议——RIP

- RIP 对“距离”的定义：
  - 从路由器到直接连接的网络的距离 = 1。
  - 路由器到非直接连接的网络的距离 = 所经过的路由器数 + 1。
  - RIP中的距离也称为“跳数” (hop count)，每经过一个路由器，跳数就加1。
  - 一条路径最多只能包含 15 个路由器。“距离”的最大值为 16 时即相当于不可达。
  - RIP 不能在两个网络之间同时使用多条路由，只选择距离最短”的路由。

路由选择协议——RIP

- 路由表的建立过程：
  - 首先：路由器在刚刚开始工作时，路由表是空的。
  - 然后：路由器得出到直接连接的网络的距离，距离定义为1。
  - 接着：每一个路由器也只和数目非常有限的相邻路由器交换并更新路由信息。
  - 以后：经过若干次更新后，所有的路由器最终都会知道到达本自治系统中任何一个网络的最短距离和下一跳路由器的地址。
  - RIP 的收敛(convergence)过程较快，即在自治系统中所有的结点都得到正确的路由选择信息的过程较短。

- 距离向量算法：
  - 本路由器是Y，假设相邻路由器（地址为 X）发送过来 RIP 报文，则Y：

1. 修改 RIP 报文中的所有项目（即路由）：把“下一跳”字段中的地址都改为 X，并把所有的“距离”字段的值加 1。
2. 对修改后的 RIP 报文中的每一个项目，重复以下步骤：
   ① 若路由表中没有目的网络N，则把该项目添加到路由表中。否则
   ② 若路由表中网络 N 的下一跳也是X，则用收到的项目替换原路由表中的项目。否则
   ③ 若收到项目中的距离小于路由表中的距离，则用收到项目更新原路由表中的项目。否则
   ④ 什么也不做。
3. 若 3 分钟还未收到相邻路由器的更新路由表，则把此相邻路由器记为不可达路由器，即将距离置为 16（表示不可达）。
4. 返回。

【RIP协议举例】已知路由器 R6 的路由表如表1所示。现在收到相邻路由器 R4 发来的路由更新信息（表2）。试填写更新后的R6 的路由表（见表3）

表 1：路由器 R6的路由表

目的网络	距离	下一跳路由器
Net2	3	R_4
Net3	4	R_5
…	…	…

表 2： R4 发来的路由更新信息

目的网络	距离	下一跳路由器
Net1	3	R_1
Net2	4	R_2
Net3	1	直接交付

② 计算更新 ③

① 距离+1，修改下一跳地址

表 2′ ：修改后的表2

目的网络	距离	下一跳路由器
Net1	4	R_4
Net2	5	R_4
Net3	2	R_4

表 3：路由器 R6 更新后的路由表

目的网络	距离	下一跳路由器
Net1	4	R_4
Net2	5	R_4
Net3	2	R_4
…	…	…

现场讨论：路由表更新。

从 C 来的 RIP 报文

Net2	4
Net3	8
Net6	4
Net8	3
Net9	5

对 C发来的 RIP 报文预处理
(跳数+1)

Net2	5
Net3	9
Net6	5
Net8	4
Net9	6

Net1: 没有新信息，不变
Net2: 相同的下一跳，替换
Net3: 一条新路由，增加
Net6: 不同的下一跳，新跳数小，替换
Net8: 不同的下一跳，跳数相同，不变
Net9: 不同的下一跳，新跳数大，不变

Net1	7	A
Net2	2	C
Net6	8	F
Net8	4	E
Net9	4	F

原路由表

更新算法

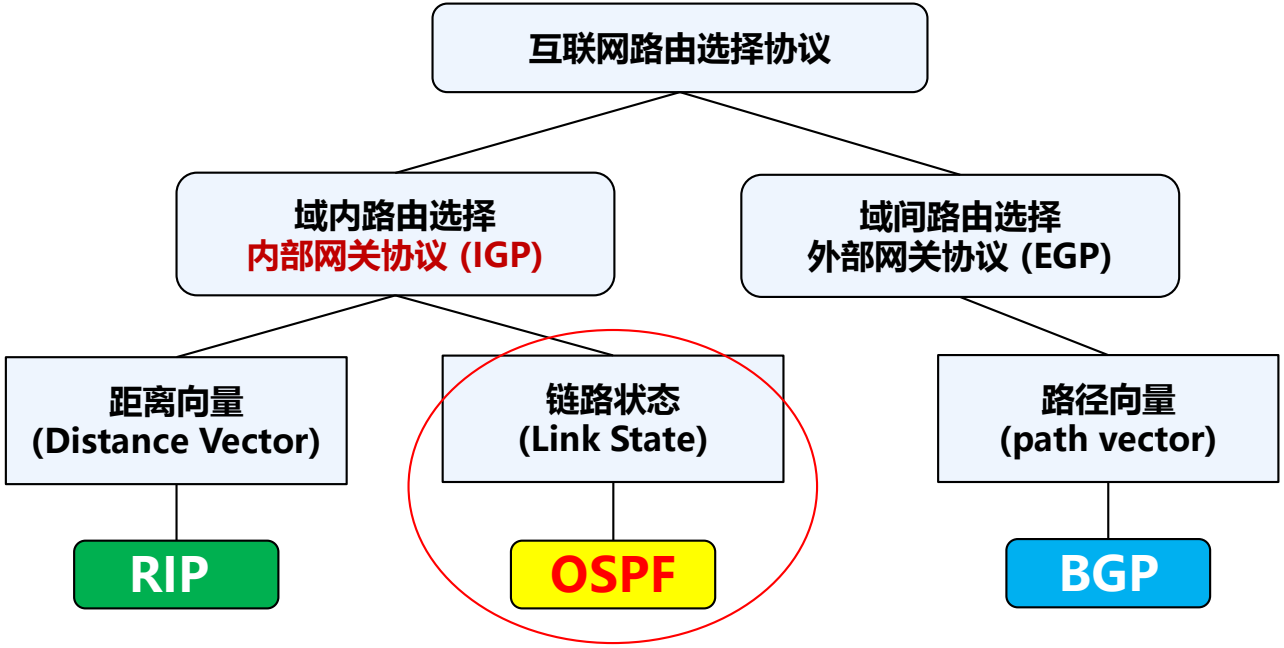
Net1	7	A
Net2	5	C
Net3	9	C
Net6	5	C
Net8	4	E
Net9	4	F

新路由表

路由选择协议

内部网关协议OSPF

路由选择协议—— OSPF


互联网路由选择协议
域内路由选择
内部网关协议 (IGP)
域间路由选择
外部网关协议 (EGP)
距离向量
(Distance Vector)
链路状态
(Link State)
路径向量
(path vector)
RIP
OSPF
BGP

路由选择协议—— OSPF

- 开放最短路径优先（Open Shortest Path First，OSPF）是为了克服 RIP的缺点，在1989年开发出来的。

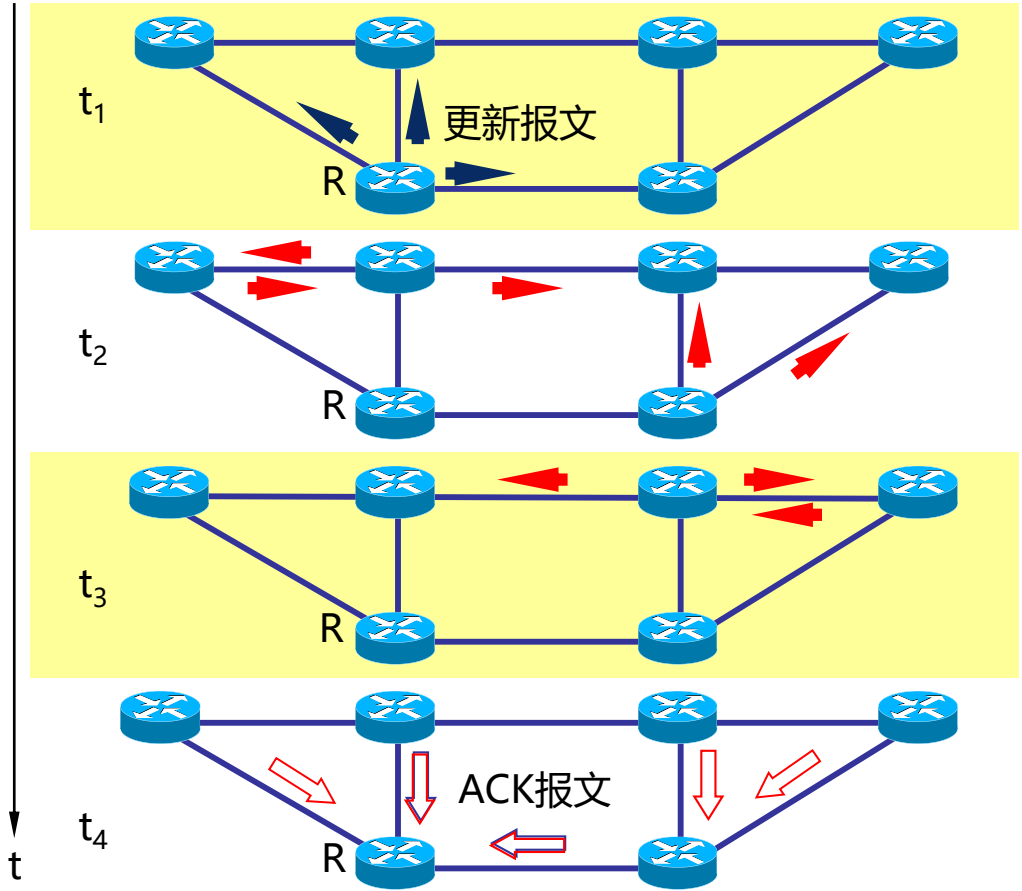
路由选择协议—— OSPF

- OSPF的三个主要特点：
  - 采用洪泛法（flooding），路由器向所有相邻路由器发送信息，而每一个相邻路由器再将此信息发往其所有的相邻路由器，最终本自治系统中所有路由器都得到了这个信息的一个副本。（RIP仅仅向自己相邻的几个路由器发送信息）
  - 发送的信息是与本路由器相邻的所有路由器的链路状态。链路状态用来说明本路由器都和哪些路由器相邻，以及该链路的度量（metric）。
    - RIP协议中，本路由器向相邻的路由器发送的是自己的路由表（到各网络的距离和下一跳路由）
  - 当链路状态发生变化或每隔一段时间（如30分钟），路由器才用洪泛法向所有路由器发送此信息。

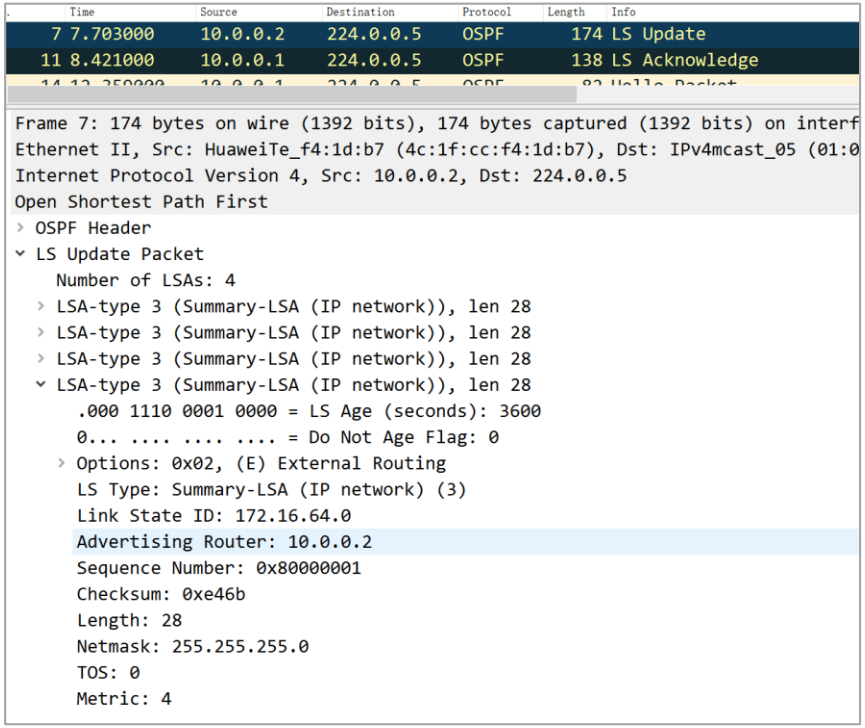
路由选择协议—— OSPF

OSPF 使用可靠的洪泛法发送更新分组

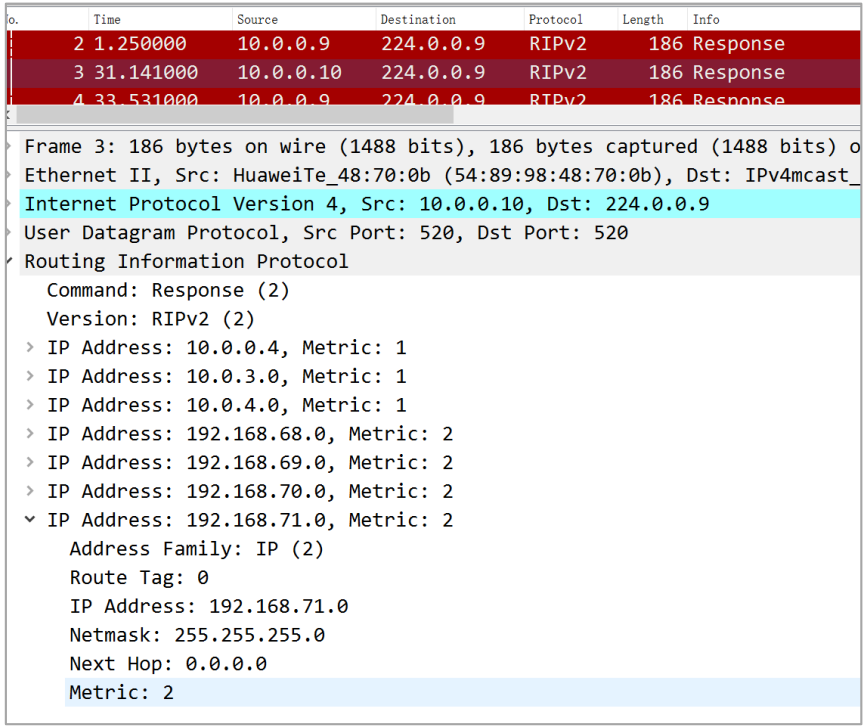
——路由器收到链路状态更新分组后，要发送确认报文（ACK报文）



OSPF与RIP的报文对比



OSPF的LSU报文



RIPv2的报文

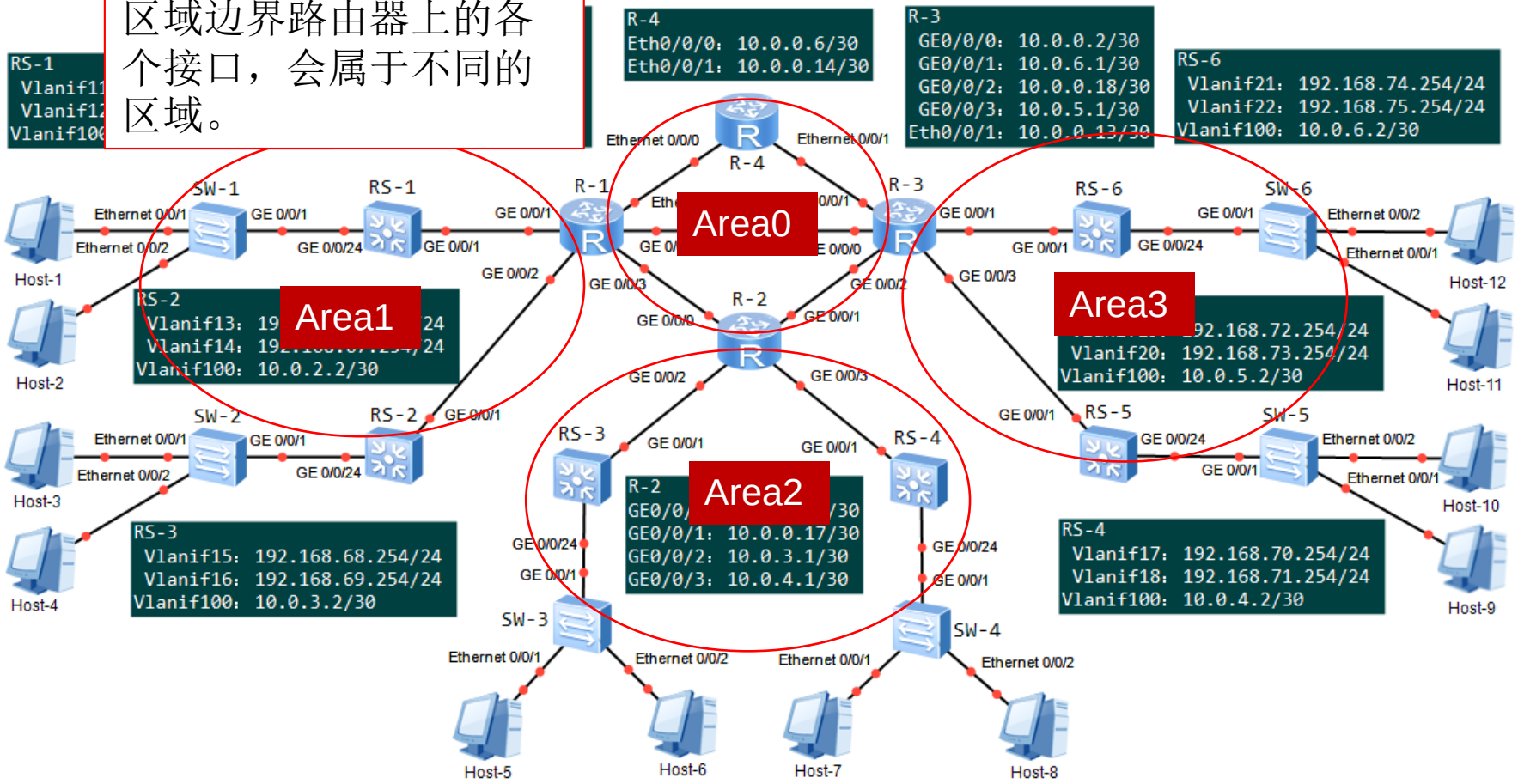
路由选择协议—— OSPF

- 链路状态数据库（Link-state Database）：
  - 由于各路由器之间频繁地交换链路状态信息，因此所有的路由器最终都能建立一个链路状态数据库，这个数据库实际上就是全网的拓扑结构图，它在全网范围内是一致的（这称为链路状态数据库的同步）。
  - 所以，每个路由器都知道全网共有多少个路由器，以及哪些路由器是相连的，其代价是多少。即各路由器的链路状态数据库是相同的
    - RIP中的每一个路由器虽然知道到所有的网络的距离以及下一跳路由器，但却不知道全网的拓扑结构（只有到了下一跳路由器，才能知道再下一跳应当怎样走）
  - 每个路由器使用链路状态数据库中的数据构造自己的路由表

路由选择协议—— OSPF

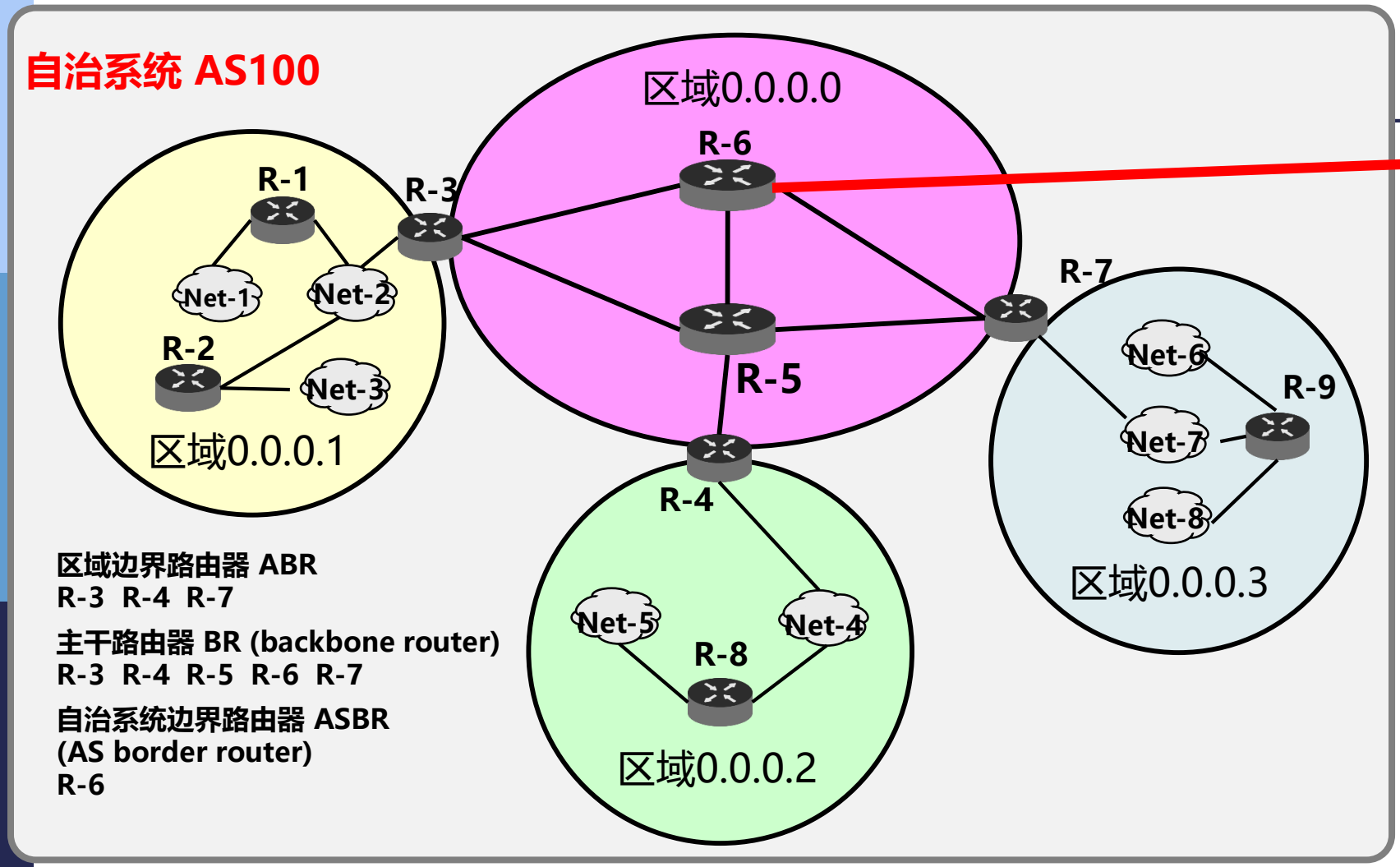
- OSPF 区域（area）：
  - RIP中“距离”等于16时即相当于不可达，只适用于小型网络。
  - 为了使OSPF能够用于规模很大的网络，OSPF 将一个自治系统再划分为若干个更小的范围，叫作区域。
  - 划分区域的好处就是将利用洪泛法交换链路状态信息的范围局限于每一个区域而不是整个的自治系统，这就减少了整个网络上的通信量。
  - 所以，在一个区域内部的路由器只知道本区域的完整网络拓扑，而不知道其他区域的网络拓扑的情况。

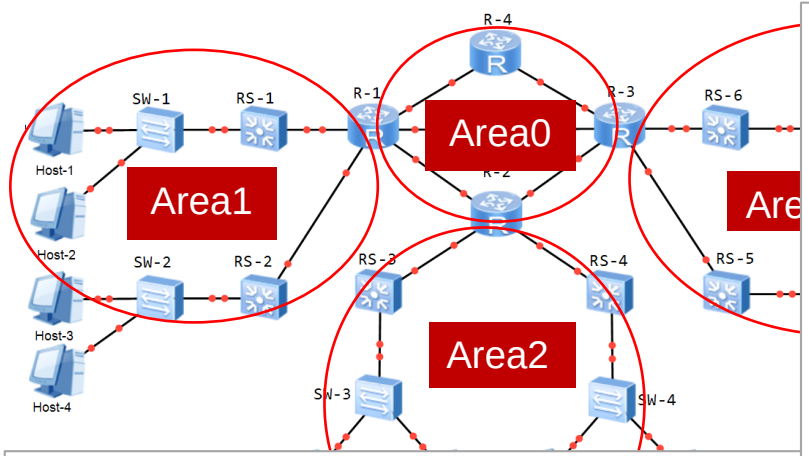
区域边界路由器上的各个接口，会属于不同的区域。



路由选择协议—— OSPF

- OSPF 区域（area）：
  - OSPF 使用层次结构的区域划分。即将区域分为主干区域（backbone area)和普通区域。
  - 每一个区域都有一个 32 位的区域标识符，用点分十进制表示。例如主干区域的标识符规定为0.0.0.0。
  - 在规划一个AS中的ospf区域时，要注意，所有普通区域必须与主干区域直接相连。主干区域的作用是用来连通其他的普通区域。
  - 从其他区域来的信息都由区域边界路由器进行概括。
  - 举例


自治系统 AS100
区域0.0.0.0
R-6
R-1
R-3
R-7
至其他自治系统
Net-1
Net-2
R-2
Net-3
区域0.0.0.1
R-5
Net-6
R-9
Net-7
Net-8
区域0.0.0.3
R-4
Net-5
Net-4
R-8
区域0.0.0.2
区域边界路由器 ABR
R-3 R-4 R-7
主干路由器 BR (backbone router)
R-3 R-4 R-5 R-6 R-7
自治系统边界路由器 ASBR
(AS border router)
R-6




```
[R-1]ospf 1
[R-1-ospf-1]area 0
[R-1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.3
[R-1-ospf-1-area-0.0.0.0]network 10.0.0.4 0.0.0.3
[R-1-ospf-1-area-0.0.0.0]network 10.0.0.8 0.0.0.3
[R-1-ospf-1-area-0.0.0.0]quit
[R-1-ospf-1]area 1
[R-1-ospf-1-area-0.0.0.1]network 10.0.1.0 0.0.0.3
[R-1-ospf-1-area-0.0.0.1]network 10.0.2.0 0.0.0.3
[R-1-ospf-1-area-0.0.0.1]quit
[R-1-ospf-1]quit
[R-1]quit
```

```
[RS-1]ospf 1
//创建并进入OSPF区域，此处是区域1
[RS-1-ospf-1]area 1
//宣告当前区域中的直连网络，注意需要配置子网掩码
[RS-1-ospf-1-area-0.0.0.1]network 192.168.64.0 0.0.0.255
[RS-1-ospf-1-area-0.0.0.1]network 192.168.65.0 0.0.0.255
[RS-1-ospf-1-area-0.0.0.1]network 10.0.1.0 0.0.0.3
[RS-1-ospf-1-area-0.0.0.1]quit
[RS-1-ospf-1]quit
<RS-1>save
```

路由选择协议—— OSPF

- OSPF 的总结：
  - 链路状态路由协议是层次式的，网络中的路由器并不向邻居传递“路由项”而是通告给邻居一些链路状态LSA (Link State Advertisement，例如接口设置的IP、掩码、开销值)
  - OSPF路由器将自己的链路状态全部转发给邻居，通过LSA的泛洪，全网中所有路由器都知道整个网络的链路状态
  - 因为所有路由器得到的链路状态信息都是一致的，就构建了统一且一致的链路状态数据库LSDB (Link-State Database)

路由选择协议—— OSPF

- OSPF 的总结：
  - LSDB 描述了路由区域内详细的网络拓扑结构
  - 所有路由器上的链路状态数据库是相同的，通过 LSDB，每台路由器计算一个以自己为根，以网络中其它节点为叶的最短路径树
  - 通过运行SPF算法，以自己为根，计算到达各目的地址的最短路径，从而形成路由表
  - 只有链路状态发生变化时，才发送更新信息
  - 减少了数据的交换，更快收敛

路由选择协议—— OSPF

- OSPF 划分区域总结：
  - OSPF区域划分为主干区域（Area0）和普通区域（Area0之外的所有区域）
  - 一个区域中可以有多个网段，即区域是一组网段的集合，
  - 划分区域可以缩小 LSDB 规模，减少网络流量
  - 区域内的详细拓扑信息不向其他区域发送，区域间传递的是抽象的路由信息，而不是详细的描述拓扑结构的链路状态信息
  - 每个区域都有自己的 LSDB，不同区域的LSDB是不同的。

路由选择协议—— OSPF

- OSPF 划分区域总结：
  - 路由器会为每一个自己所连接到的区域维护一个单独的LSDB
  - 由于详细链路状态信息不会被发布到区域以外，因此 LSDB 的规模大大缩小了
  - Area0 为主干区域，主干区域负责在非主干区域之间发布由区域边界路由器汇总的路由信息（并非详细的链路状态信息）
  - 为了避免区域间路由环路，非主干区域之间不允许直接相互发布区域间路由信息
  - 因此，所有区域边界路由器都至少有一个接口属于 Area0，即每个区域都必须连接到主干区域

路由选择协议—— OSPF

- OSPF 的五种分组（消息）类型：
  - 类型1：Hello报文（问候信息）：
    - 周期性发送，用来发现和维护OSPF邻居关系（可达性）
  - 类型2：Database Description分组（链路状态数据库描述信息）
    - 描述本地LSDB的摘要信息，用于两台设备进行数据库同步
  - 类型3：Link State Request分组（链路状态请求信息）。
    - 用于向对方请求所需要的LSA（链路状态），设备只有在OSPF邻居双方成功交换DD报文后才会向对方发出LSR报文
  - 类型4：链路状态更新 (Link State Update) 分组。
    - 用洪泛法对全网更新链路状态，向对方发送其所需要的LSA。
  - 类型5：链路状态确认 (Link State Acknowledgment) 分组。
    - 用来对收到的LSA进行确认

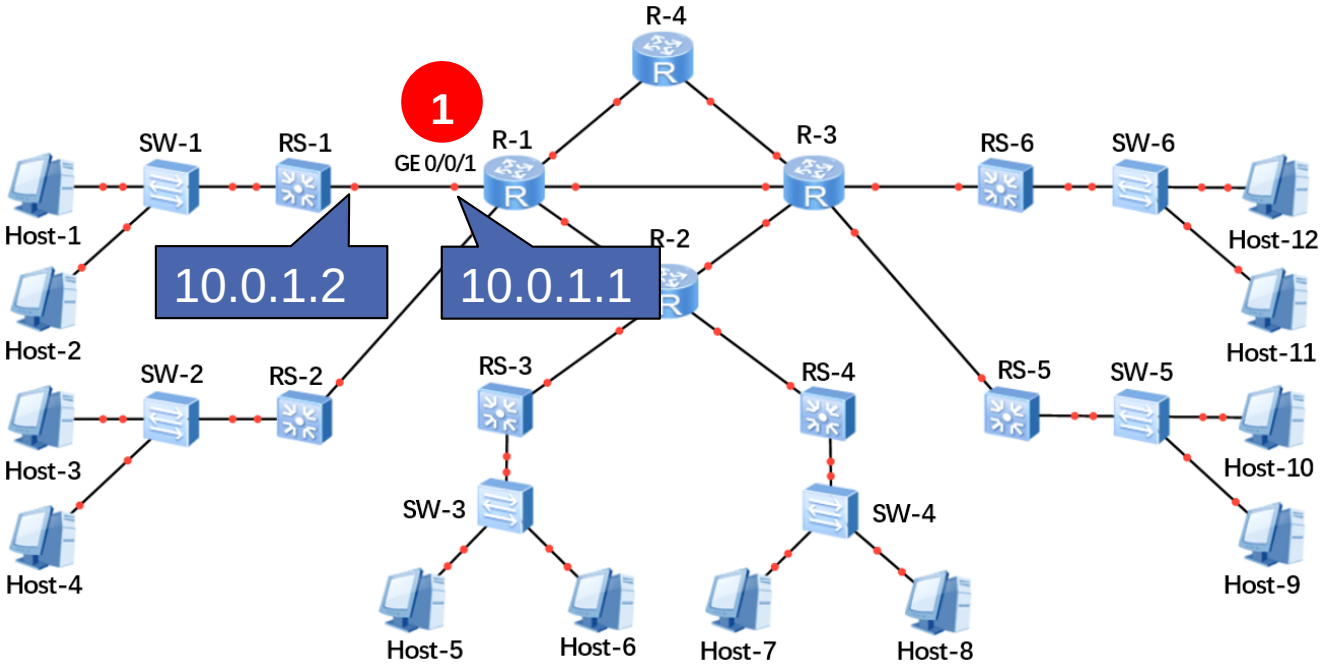
路由选择协议

- OSPF 工作过程
  - 第1：确定邻站可达。
    - 相邻路由器每隔 10 秒钟要交换一次问候分组。
    - 若有 40 秒钟没有收到某个相邻路由器发来的问候分组，则可认为该相邻路由器是不可达的，立即修改链路状态数据库，重新计算路由表。
  - 第2：同步链路状态数据库。
    - 同步：指不同路由器的链路状态数据库的内容是一样的。
    - 两个同步的路由器叫做完全邻接的（fully adjacent）路由器。
    - 不是完全邻接的路由器：虽然在物理上是相邻的，但其链路状态数据库并没有达到一致。

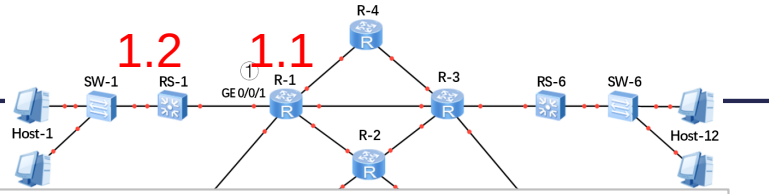
路由选择协议—— OSPF

- OSPF 工作过程
  - 第3：更新链路状态。
    - 只要链路状态发生变化，路由器就使用链路状态更新分组，采用可靠的洪泛法向全网更新链路状态。
    - 为确保链路状态数据库与全网的状态保持一致，OSPF 还规定：每隔一段时间，如 30 分钟，要刷新一次数据库中的链路状态。
    - OSPF 链路状态只涉及相邻路由器，与整个互联网的规模并无直接关系，因此当互联网规模很大时，OSPF 协议要比距离向量协议 RIP 好得多。
    - OSPF 没有“坏消息传播得慢”的问题，收敛速度快。

举例：OSPF更新链路状态



举例：OSPF更新链路状态



文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

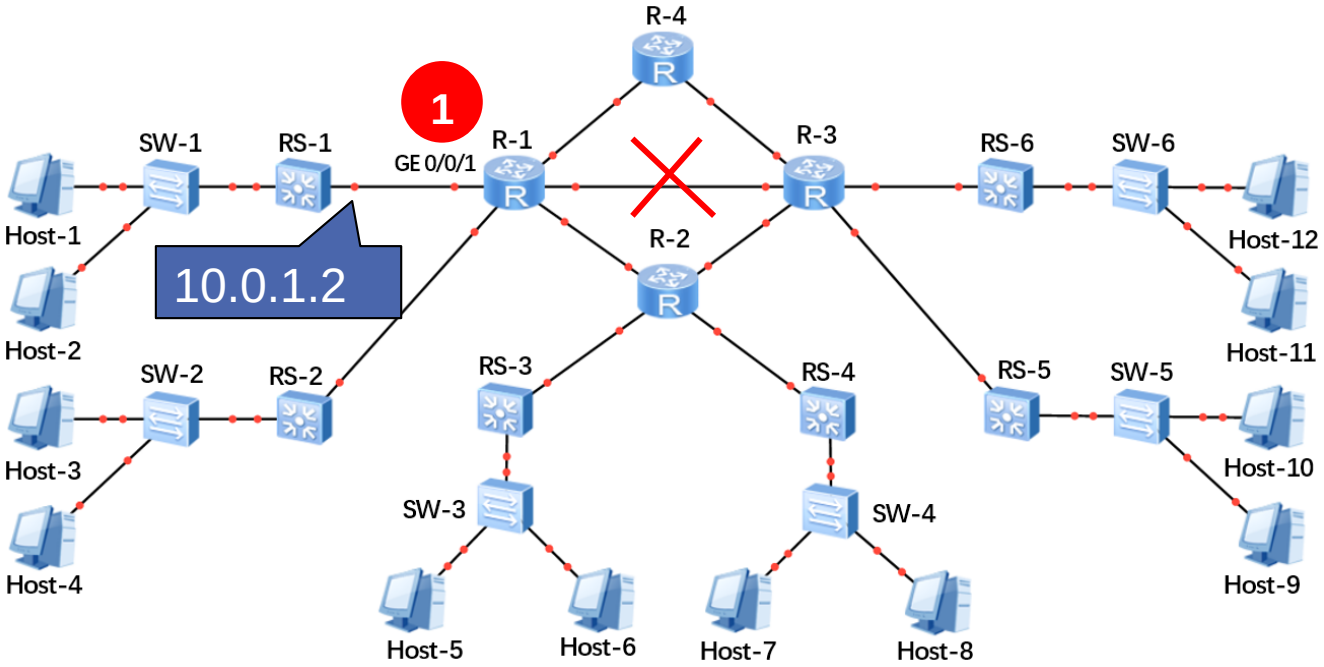
ospf

No.	Time	Source	Destination	Protocol	Info
2	1.578000	10.0.1.2	224.0.0.5	OSPF	Hello Packet
5	6.515000	10.0.1.1	224.0.0.5	OSPF	Hello Packet
8	11.125000	10.0.1.2	224.0.0.5	OSPF	Hello Packet
11	15.984000	10.0.1.1	224.0.0.5	OSPF	Hello Packet

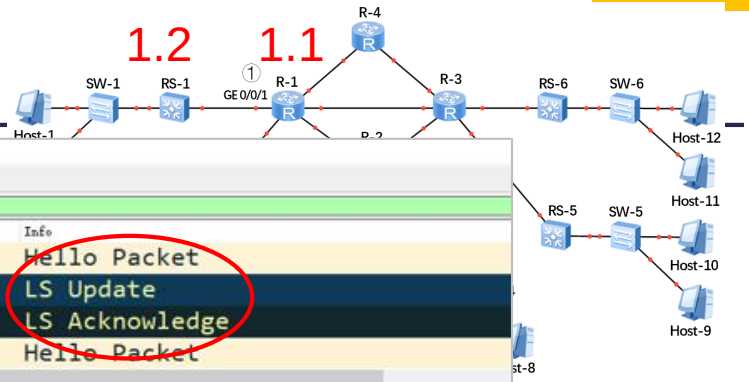
```
> Frame 2: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
> Ethernet II, Src: HuaweiTe_41:5f:7d (4c:1f:cc:41:5f:7d), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> Internet Protocol Version 4, Src: 10.0.1.2 (10.0.1.2), Dst: ospf-all.mcast.net (224.0.0.5)
> Open Shortest Path First
```

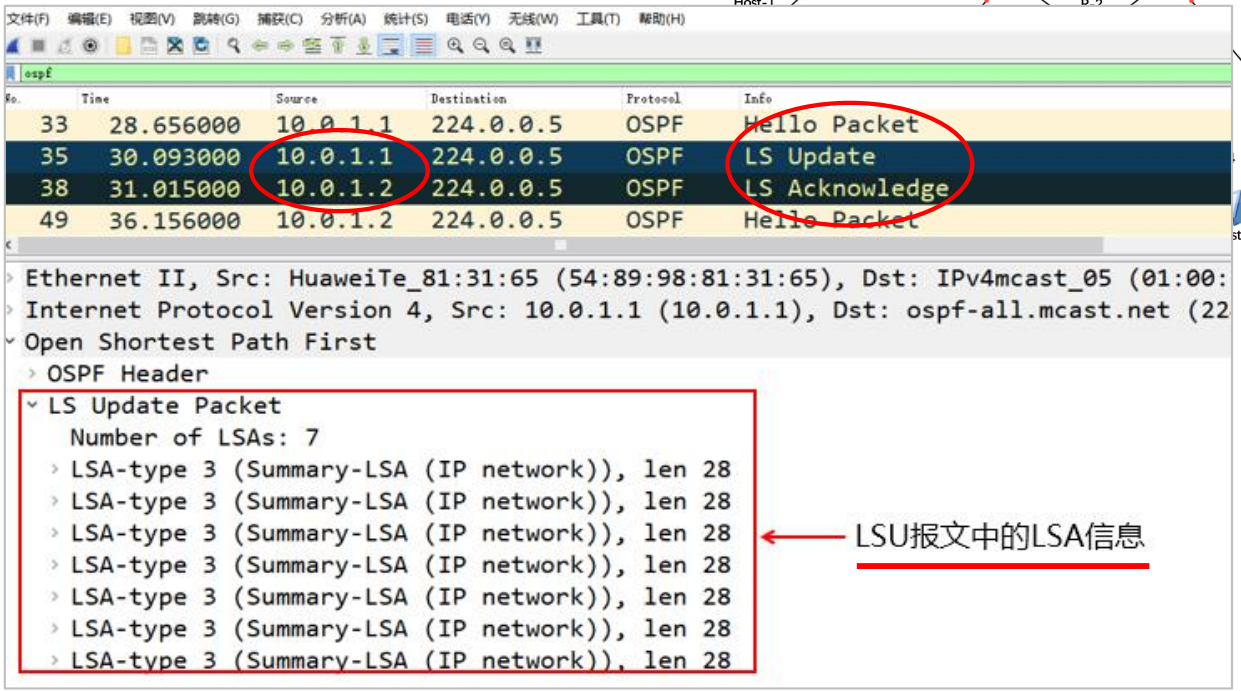
周期性发送，用来发现和维护OSPF邻居关系（可达性）

举例：OSPF更新链路状态



举例：OSPF更新链路状态

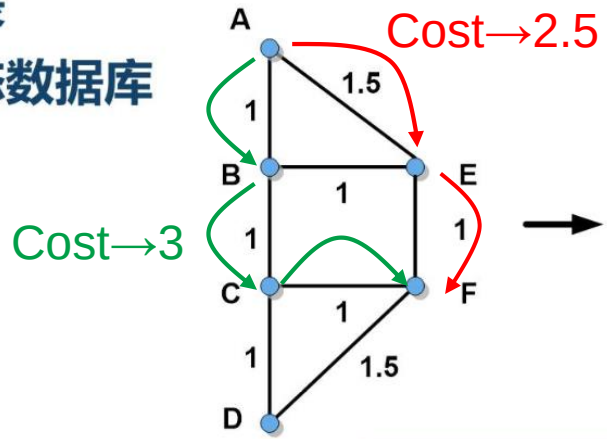




链路状态更新与链路状态确认分组

路由选择协议—— OSPF

- 邻居列表
- 链路状态数据库
- 路由表



以A为例，生成路由表的过程

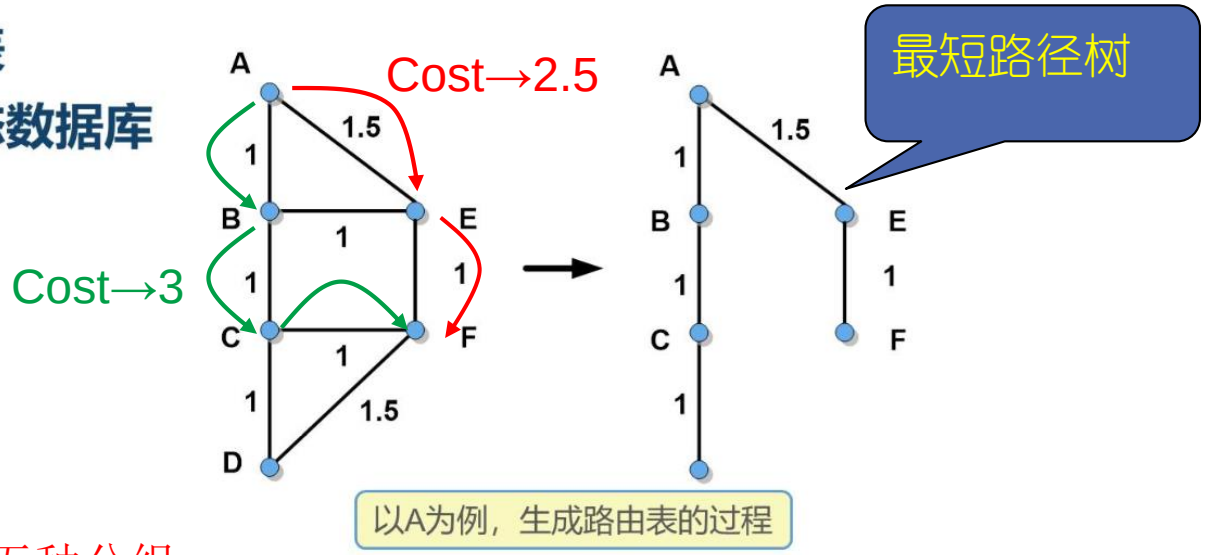
OSPF五种分组

建立邻接关系 → 链路状态数据库 → 最短路径树 → 路由表

学习链路状态信息　　Dijkstra算法

路由选择协议—— OSPF

- 邻居列表
- 链路状态数据库
- 路由表



OSPF五种分组

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

RS-1
Vlanif11：192.168.64.254/24
Vlanif12：192.168.65.254/24
Vlanif100：10.0.1.2/30

R-1
GE0/0/0：10.0.0.1/30
GE0/0/1：10.0.1.1/30
GE0/0/2：10.0.2.1/30
GE0/0/3：10.0.0.9/30
Eth0/0/0：10.0.0.5/30

R-4
Eth0/0/0：10.0.0.6/30
Eth0/0/1：10.0.0.14/30

R-3
GE0/0/0：10.0.0.2/30
GE0/0/1：10.0.6.1/30
GE0/0/2：10.0.0.18/30
GE0/0/3：10.0.5.1/30
Eth0/0/1：10.0.0.13/30

RS-6
Vlanif21：192.168.74.254/24
Vlanif22：192.168.75.254/24
Vlanif100：10.0.6.2/30

RS-2
Vlanif13：192.168.66.254/24
Vlanif14：192.168.67.254/24
Vlanif100：10.0.2.2/30

RS-5
Vlanif19：192.168.72.254/24
Vlanif20：192.168.73.254/24
Vlanif100：10.0.5.2/30

RS-3
Vlanif15：192.168.68.254/24
Vlanif16：192.168.69.254/24
Vlanif100：10.0.3.2/30

R-2
GE0/0/0：10.0.0.10/30
GE0/0/1：10.0.0.17/30
GE0/0/2：10.0.3.1/30
GE0/0/3：10.0.4.1/30

RS-4
Vlanif17：192.168.70.254/24
Vlanif18：192.168.71.254/24
Vlanif100：10.0.4.2/30

划分子网

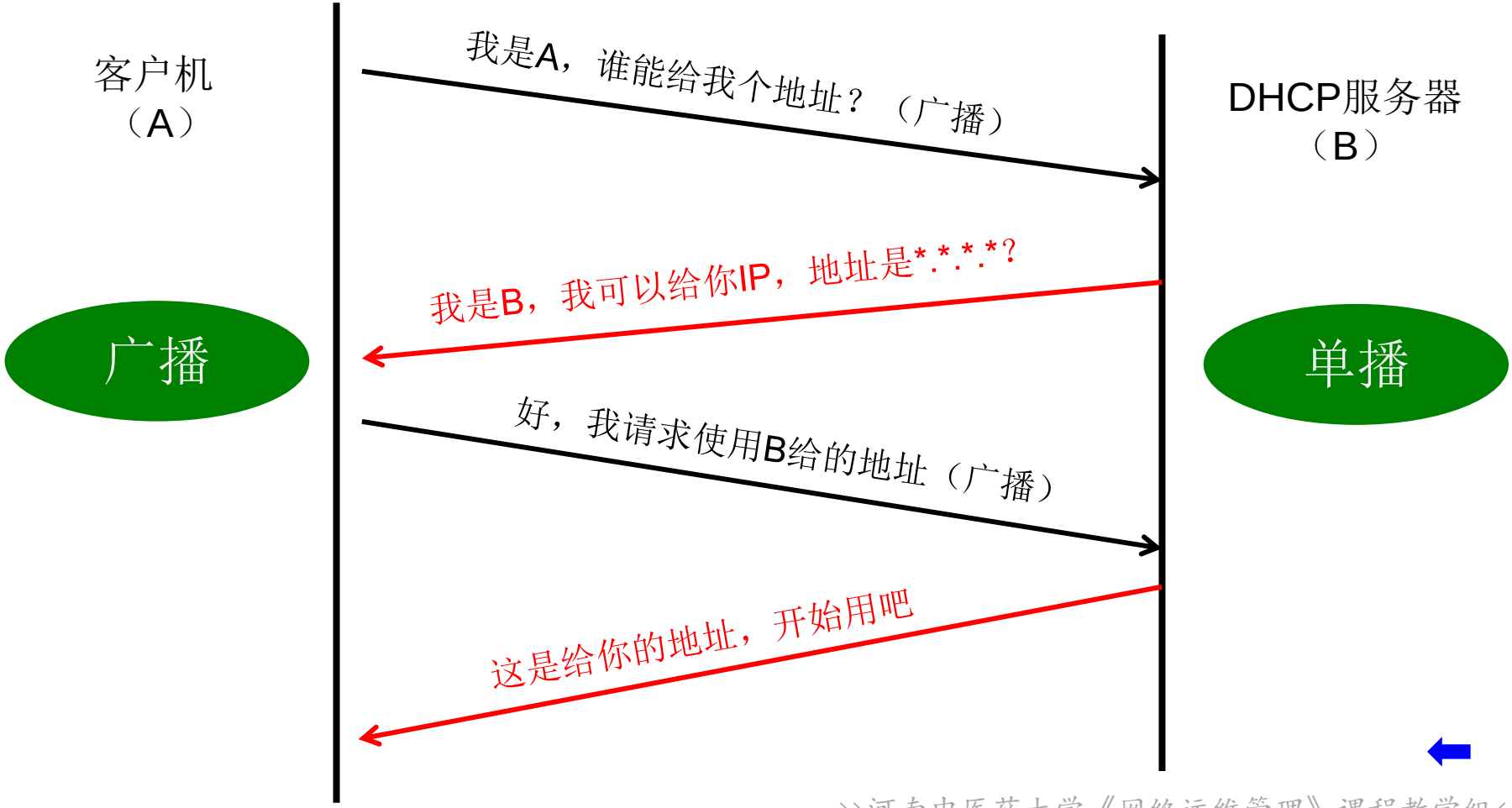
- IP地址的设计

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



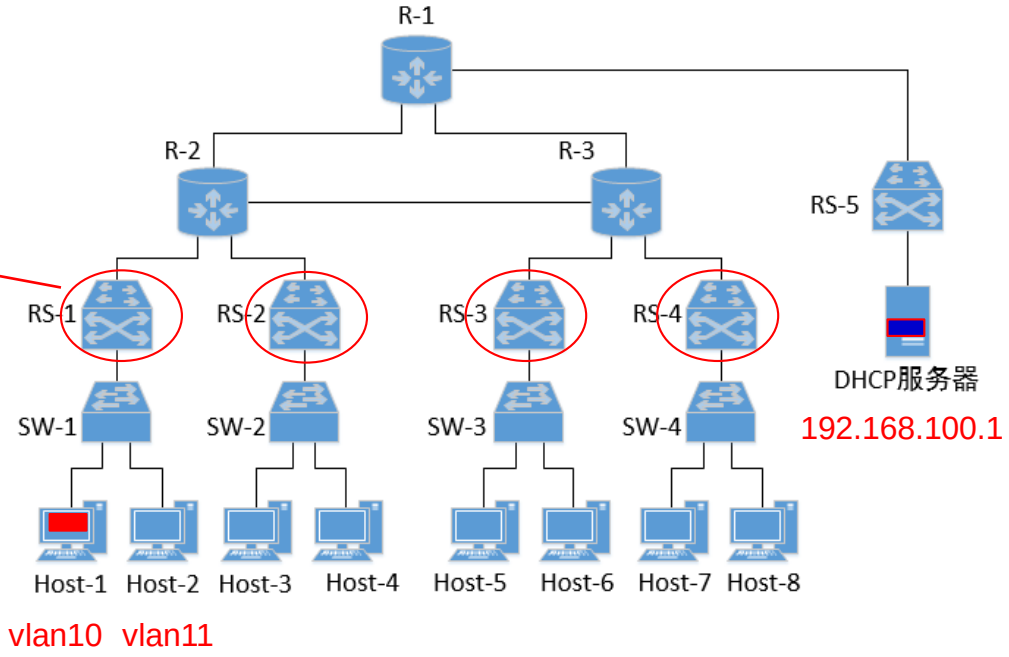
DHCP 中继代理

➢ 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

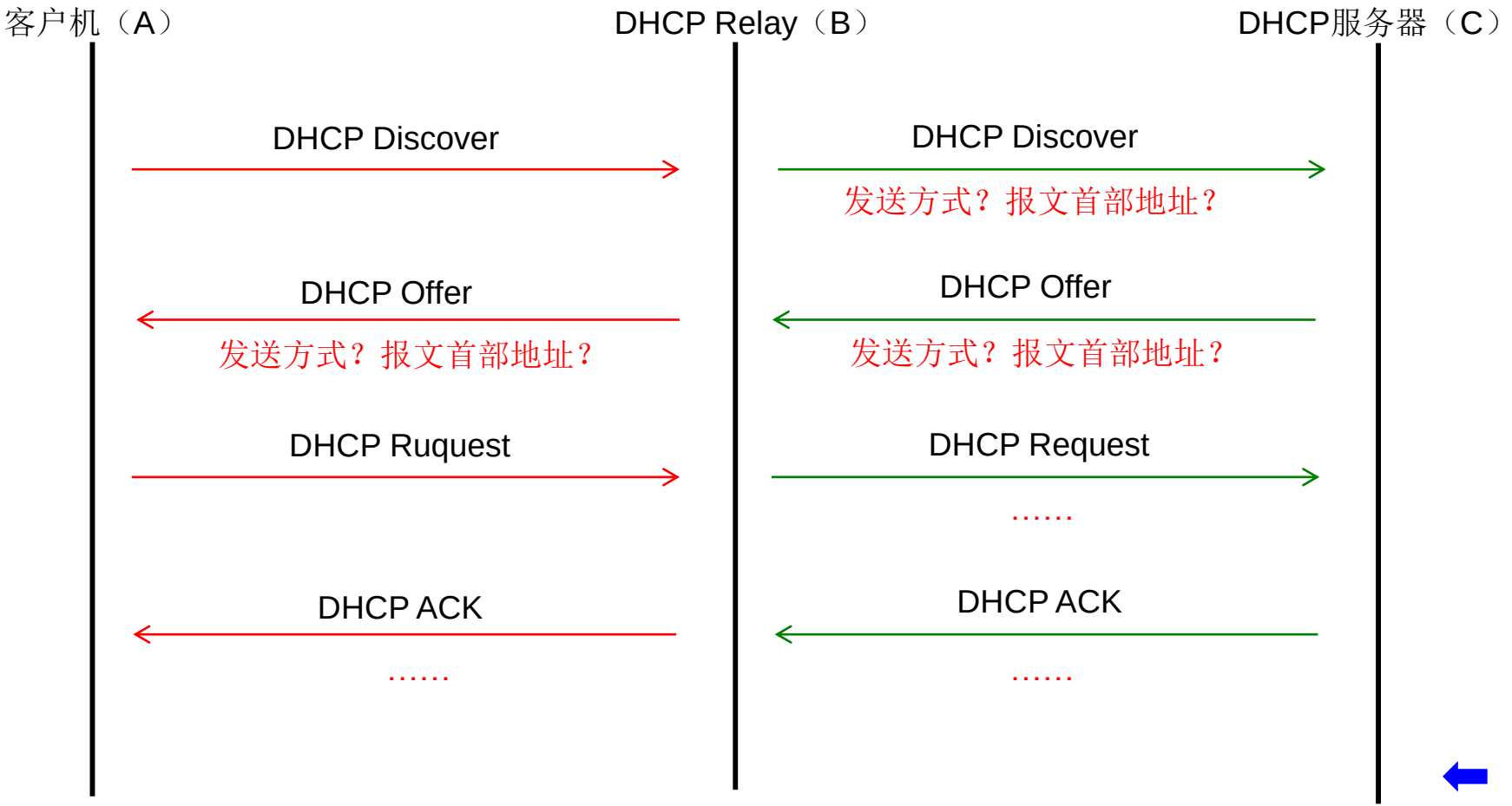
[RS-1] interface vlanif 11
[RS-1-Vlanif11] dhcp select relay
[RS-1-Vlanif11] dhcp relay server-ip 192.168.100.1
[RS-1-Vlanif11] quit

针对每个用户VLAN，在网关处配置DHCP中继。



在RS-1~RS-4上配置DHCP中继

DHCP Relay的工作过程



8. 无线局域网（WLAN）

无线局域网
（略）

- 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。

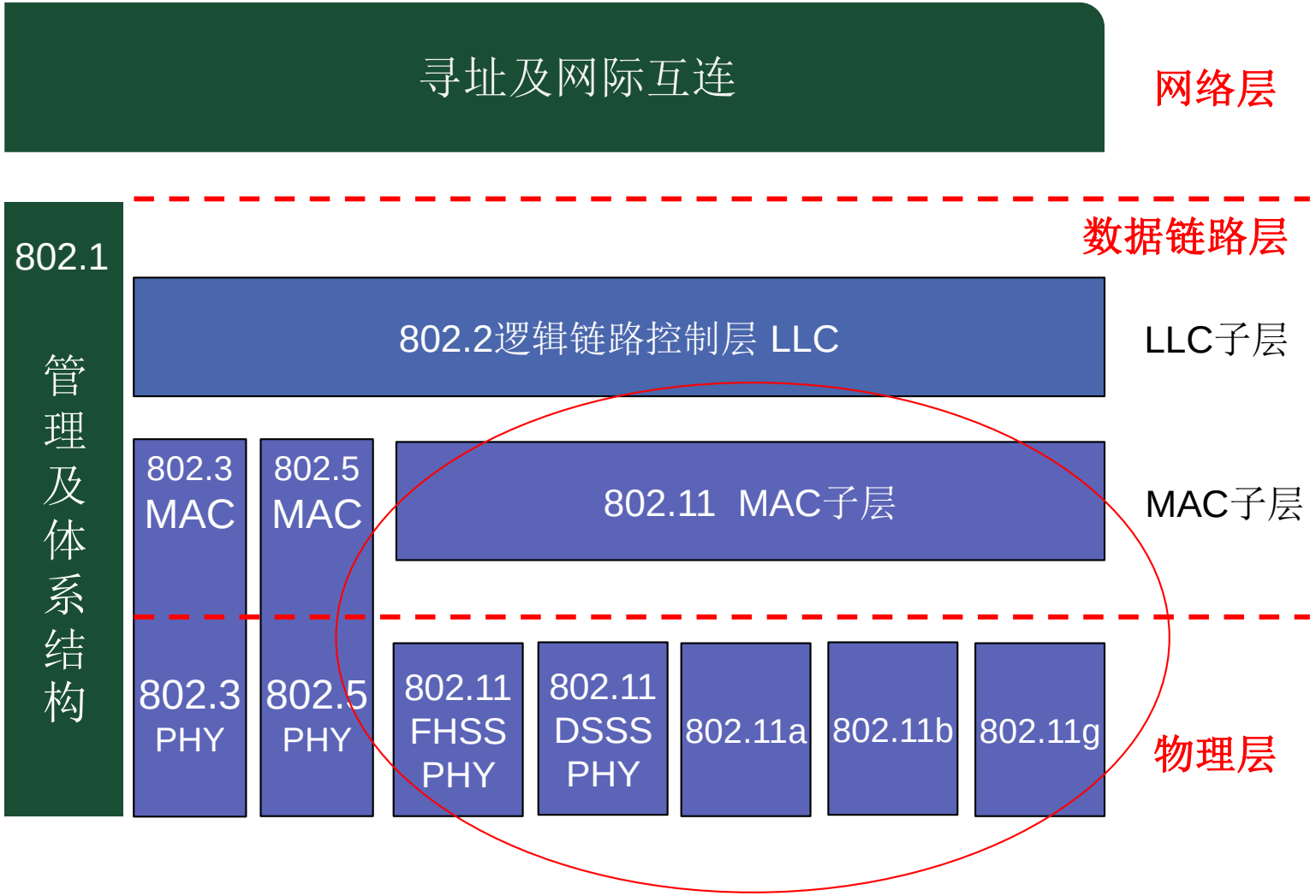
认识无线电频谱

- 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
802.1
管理及体系结构
数据链路层
802.2逻辑链路控制层 LLC
LLC子层
802.3 MAC
802.5 MAC
802.11 MAC子层
MAC子层
802.3 PHY
802.5 PHY
802.11 FHSS PHY
802.11 DSSS PHY
802.11a
802.11b
802.11g
物理层

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/CKK	8*8MIMO-OFDM/16~256QAM	
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

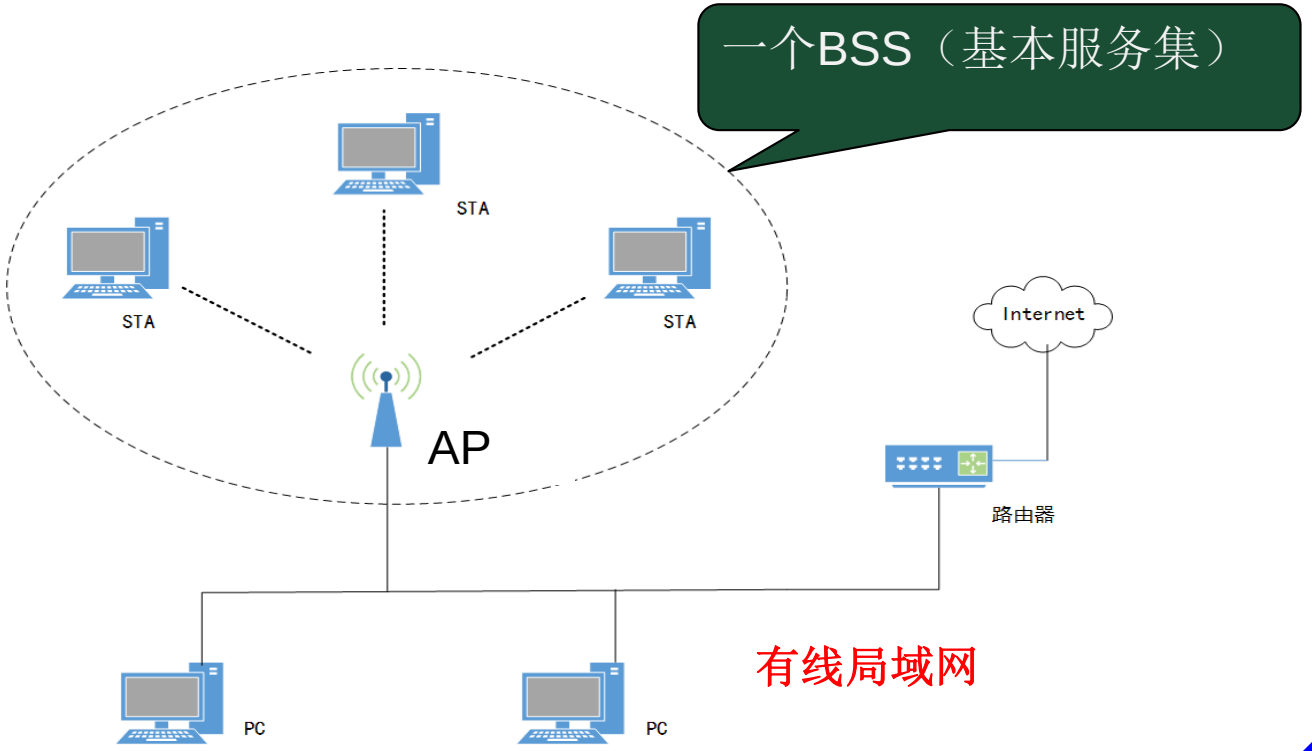
无线局域网的组成

DS：分布式系统，负责将帧传送到目的地

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。

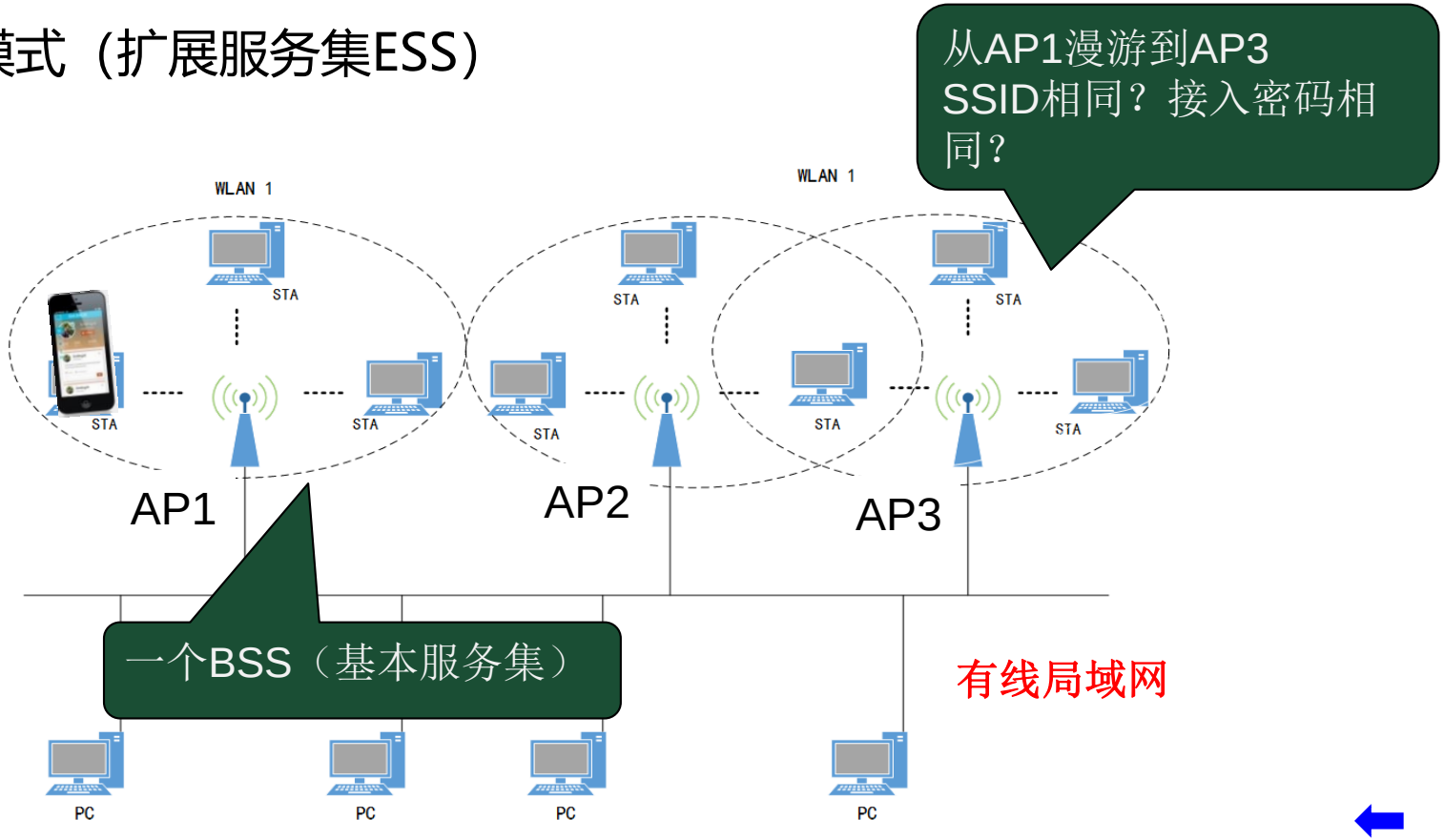
无线局域网的拓扑结构

- 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）



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在共享秘钥上的漏洞，添加了数据完整性检查和用户级的认证措施。

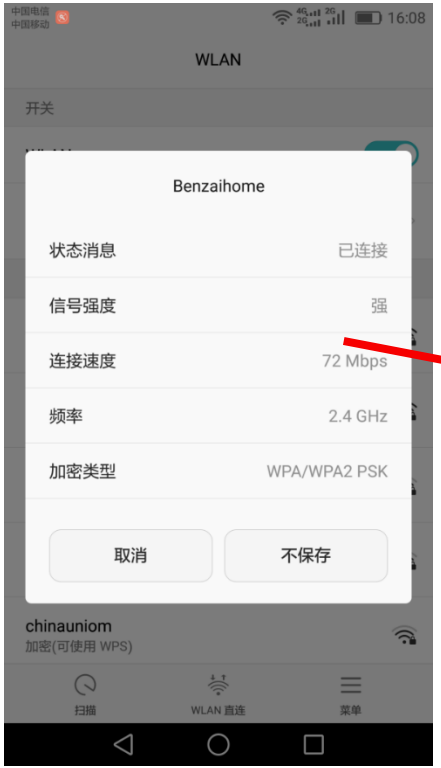
无线通信加密

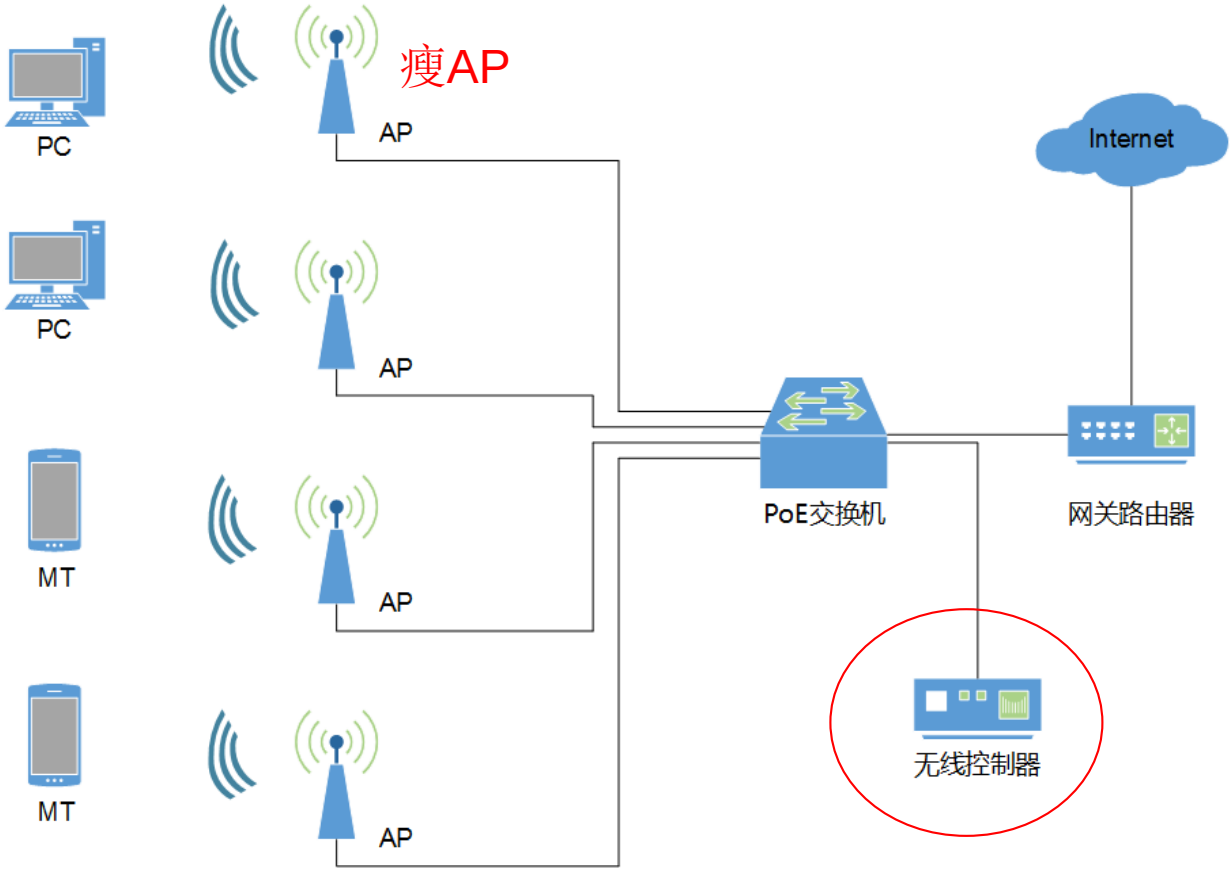
- WPA加密认证方式
  - Wi-Fi联盟给出的WPA定义为：WPA = 802.1x + EAP + TKIP + MIC。其中：
    - 802.1x是指IEEE的802.1x身份认证标准；EAP（Extensible Authentication Protocol，扩展身份认证协议）是一种扩展身份认证协议。这两者就是新添加的用户级身份认证方案。
    - TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）是一种密钥管理协议，即一种加密算法；
    - MIC（Message Integrity Code，消息完整性编码）是用来对消息进行完整性检查的，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




瘦AP
PC
PC
MT
MT
AP
AP
AP
AP
Internet
PoE交换机
网关路由器
无线控制器

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网络和用户提供安全保障。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。

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。

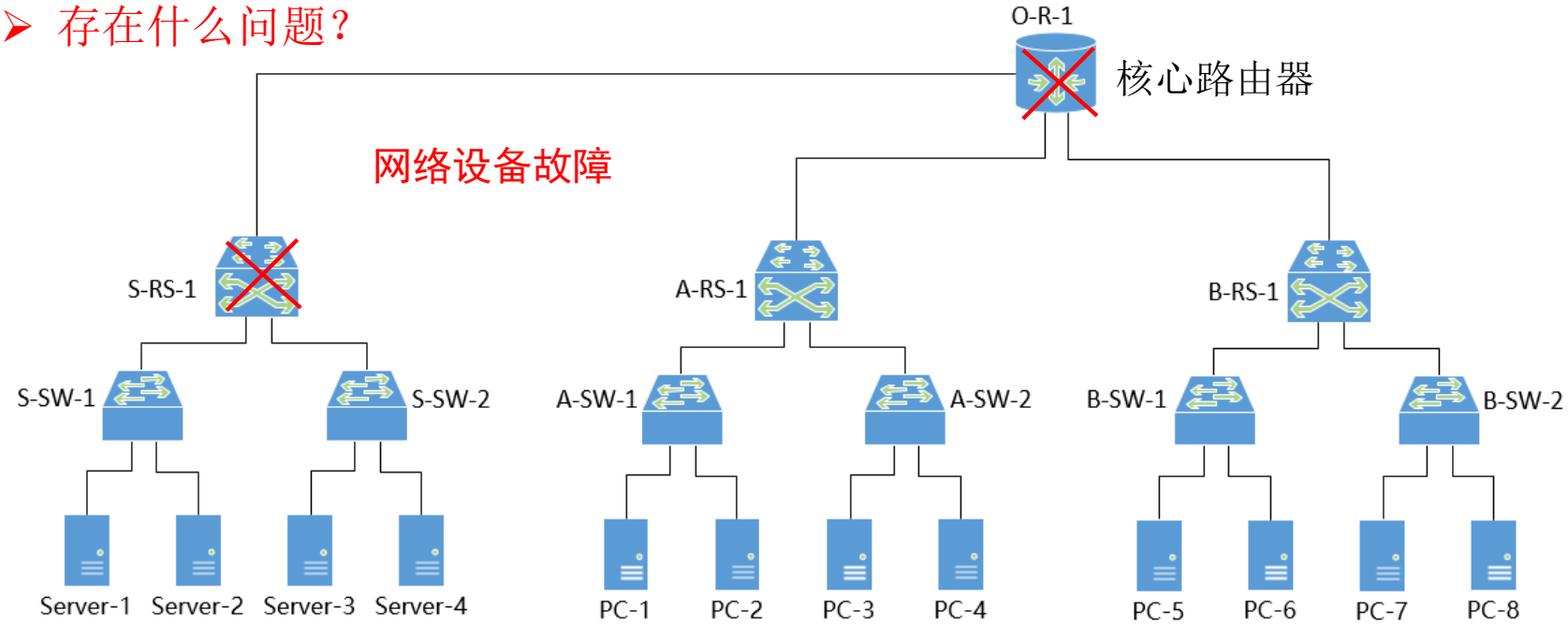
（4）VAP模板

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

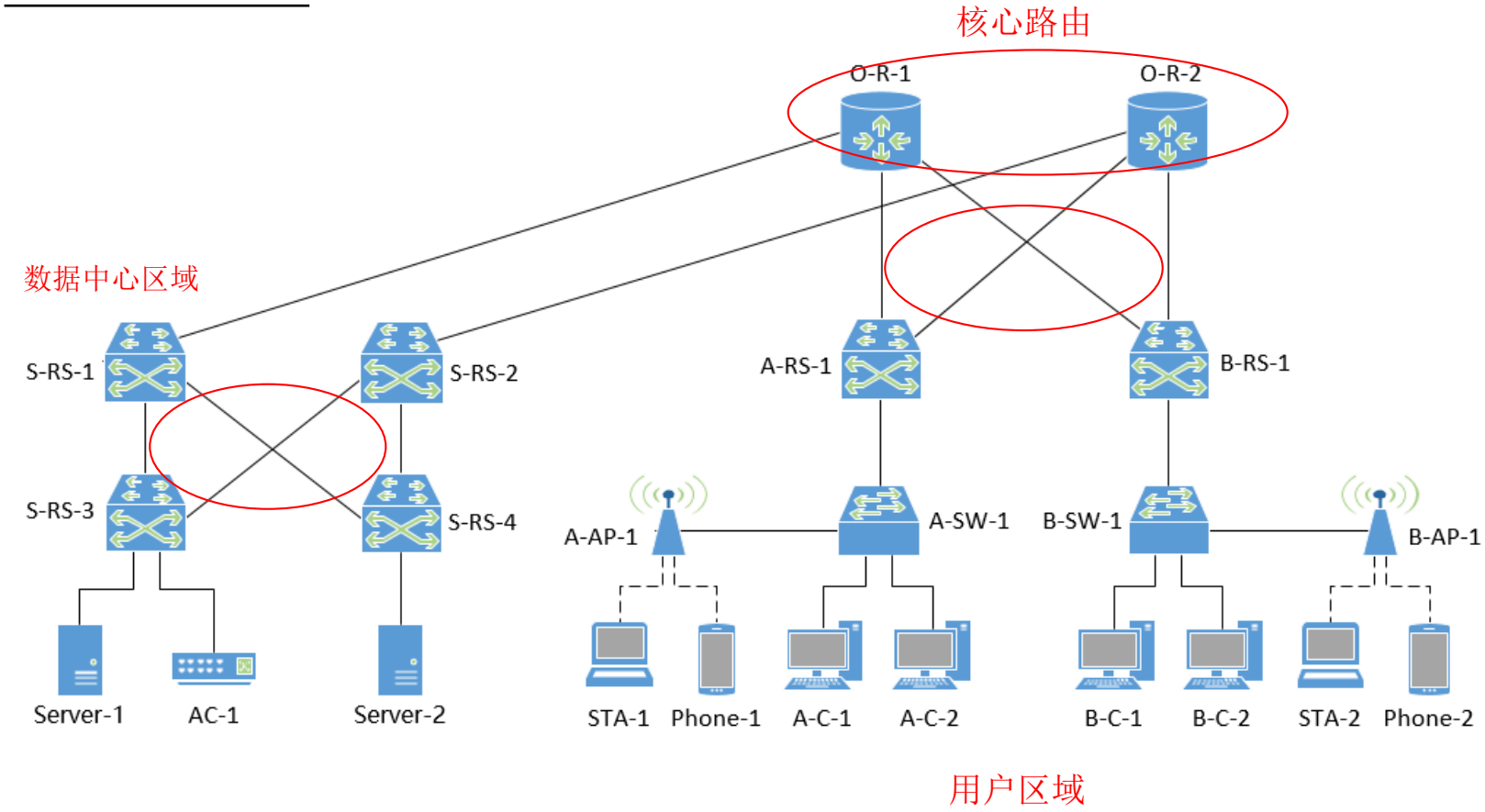
9. 混合园区网建设案例分析

➢ 存在什么问题？



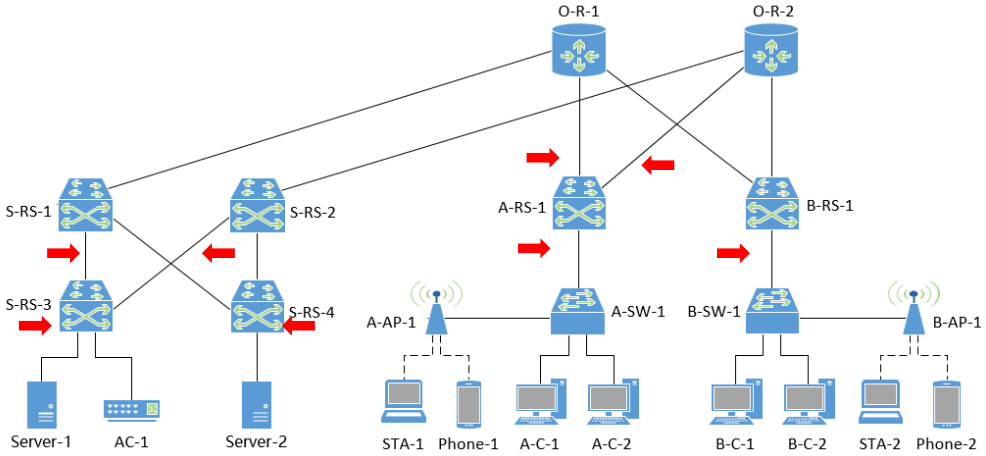
如何提高网络的容灾性能？

➢ 网络容灾部署


核心路由
O-R-1
O-R-2
数据中心区域
S-RS-1
S-RS-2
S-RS-3
S-RS-4
A-RS-1
B-RS-1
A-AP-1
A-SW-1
B-SW-1
B-AP-1
Server-1
AC-1
Server-2
STA-1
Phone-1
A-C-1
A-C-2
B-C-1
B-C-2
STA-2
Phone-2
用户区域

1. 拓扑结构分析

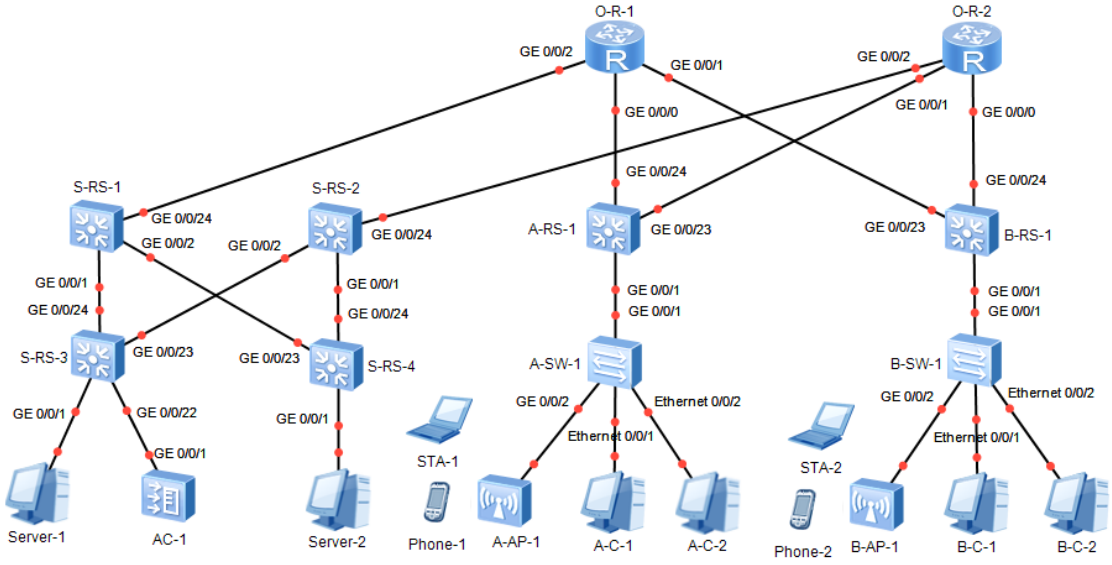
- 用户区域拓扑中，三层交换机A-RS-1和B-RS-1下面可根据需要接入多台二层交换机，此处简化为各接入一台二层交换机，用于接入用户主机。
- 三层交换机A-RS-1和B-RS-1分别同时接入路由器O-R-1和O-R-2，实现了通信链路冗余，起到了网络容灾作用。



- 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

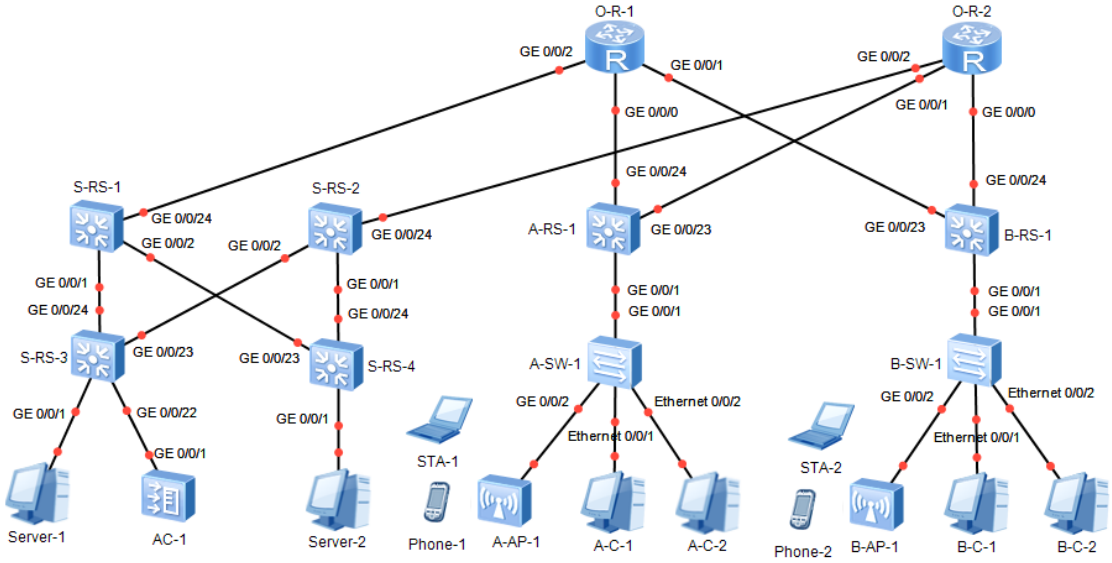


问题：

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（可以有多个）
  - B-SW-1下连的AP（可以有多个）
  - AC

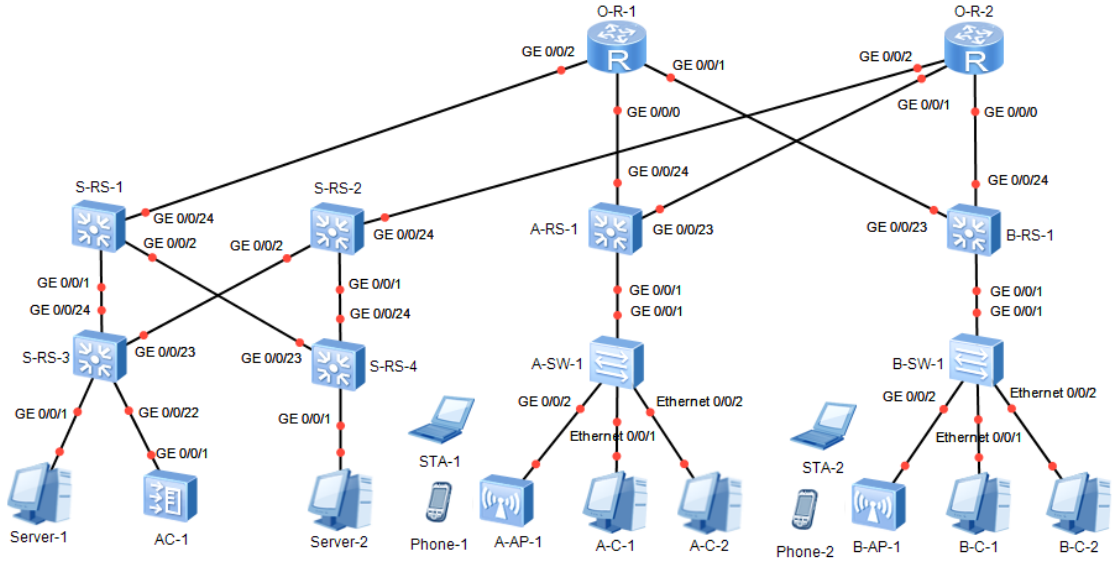


问题：

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。管理性
2. 能否给AC-1、A-AP-1、B-AP-1全部配置10.0.200.*段的IP地址？ 划分子网
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？ 多个AP
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

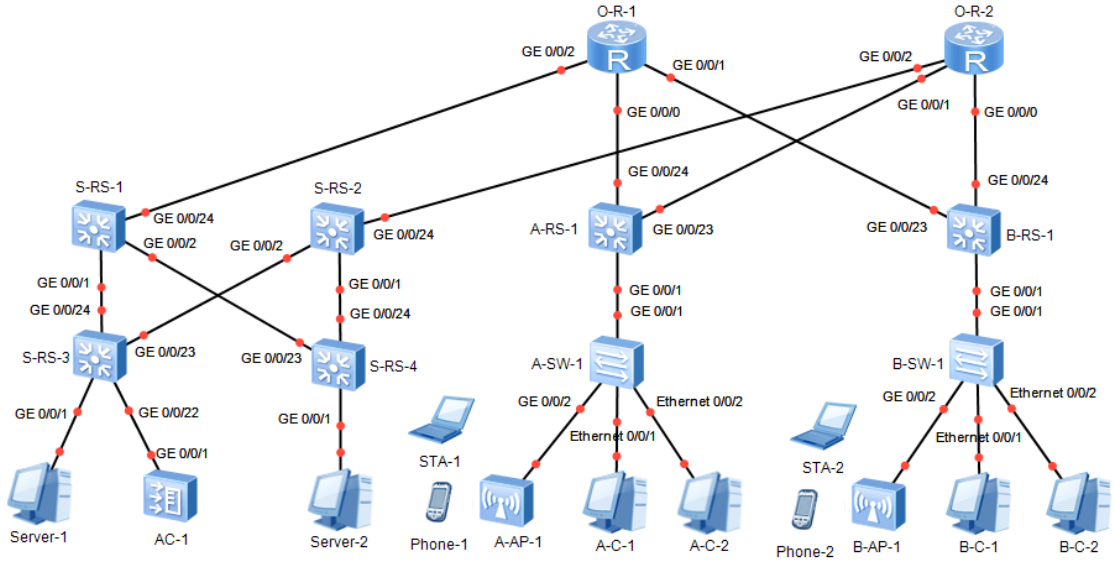


问题：

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

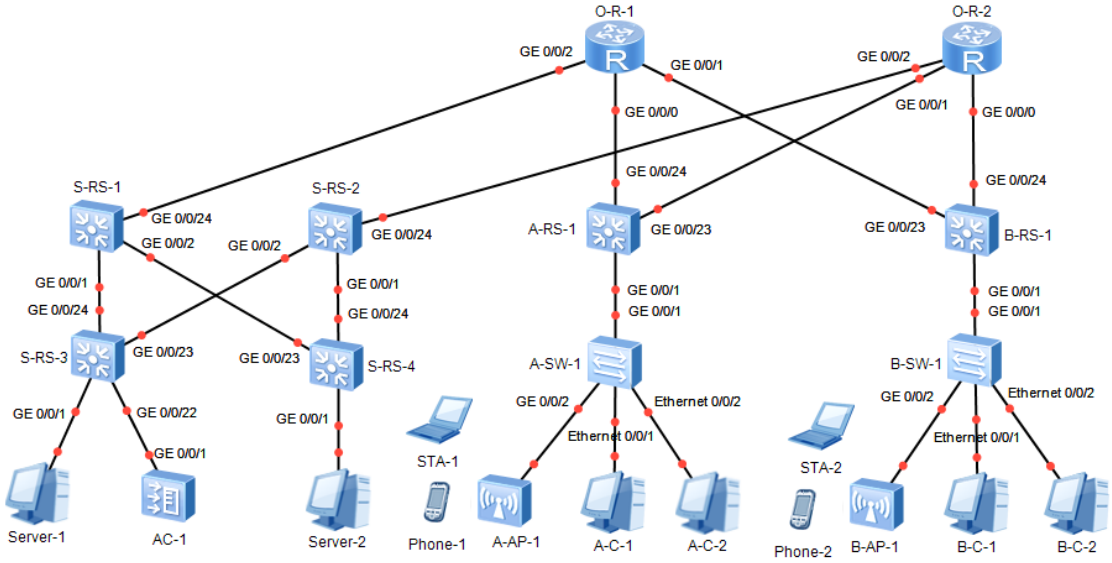
- 三层虚拟路由接口
  - A-RS-1、B-RS-1
  - S-RS-1～S-RS-4
  - 注意：有些三层虚拟路由接口是用来做默认网关的，有些是用来进行路由间通信的
- 路由器的物理接口
  - O-R-1
  - O-R-2



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？

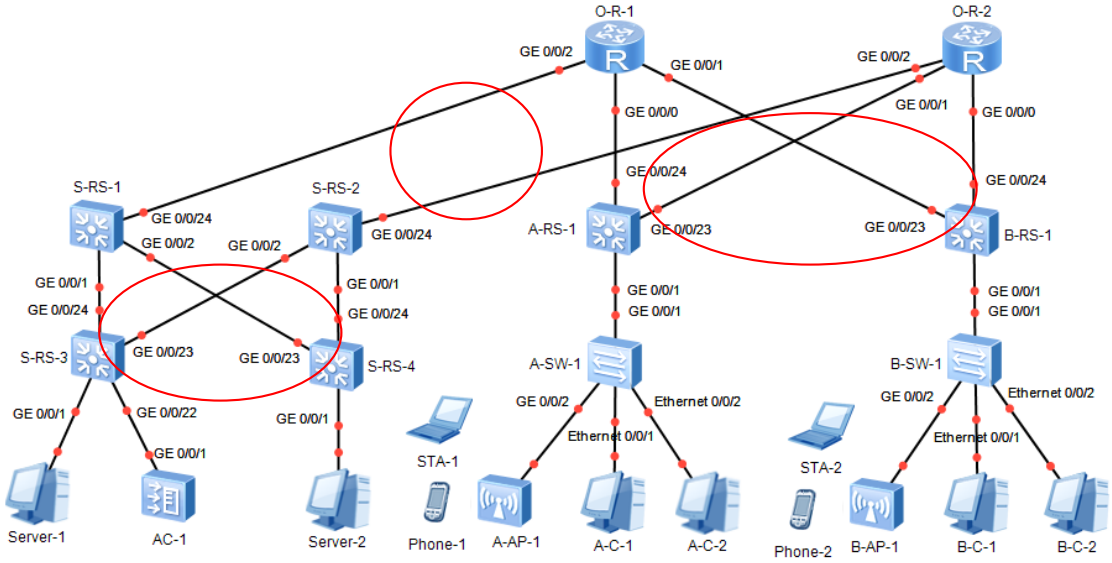
6. 路由配置分析



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



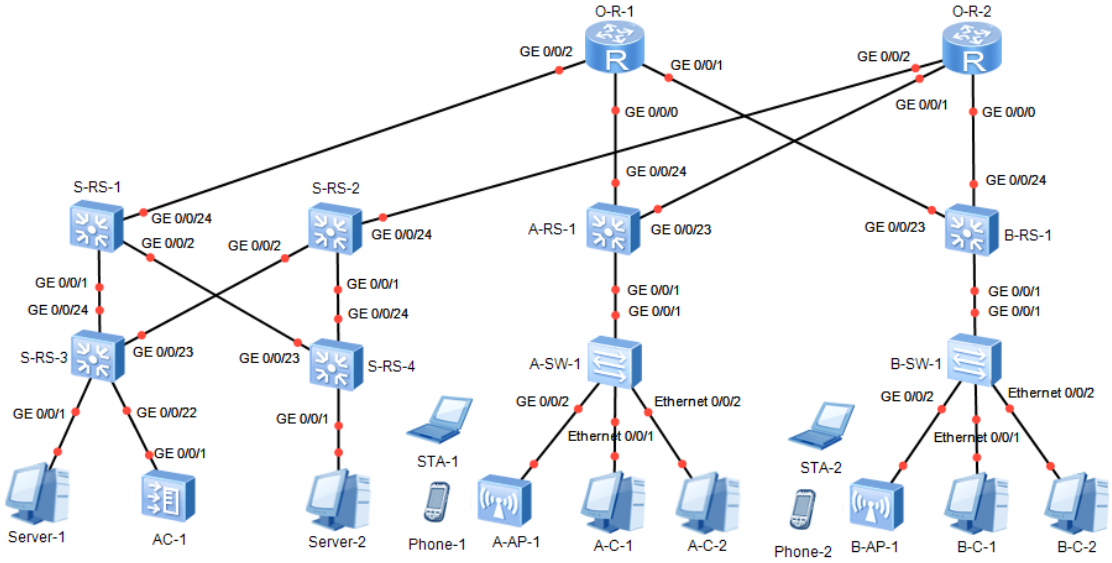
问题：

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？

实验1的IP地址设计要求

1. 所有用户主机（无线用户和有线用户）的IP地址格式为192.A.B.*，其中A为学生本人学号后2位，A≤B≤（A+4），*表示该值由学生自定。例如学生2021181011，其可以用来分配给用户主机的IP地址范围是192.11.11.0——192.11.15.255。
2. 每个网段的默认网关地址，由本网段最后一个可用单播地址表示。
3. 自行设计每个用户VLAN中的主机数量，给每个VLAN分配IP地址块，并考虑路由聚合的要求。
4. 所有路由间通信的接口（含路由器接口和路由交换机中的相关SVI接口）的IP地址格式为10.10.A.*，其中A为学生本人学号后2位，*表示该值由学生自定。
5. 所有AC、AP的IP地址，IP地址格式为10.20.A.*，其中A为学生本人学号后2位，*表示该值由学生自定

Thanks.