第四讲　交换机上VLAN的配置

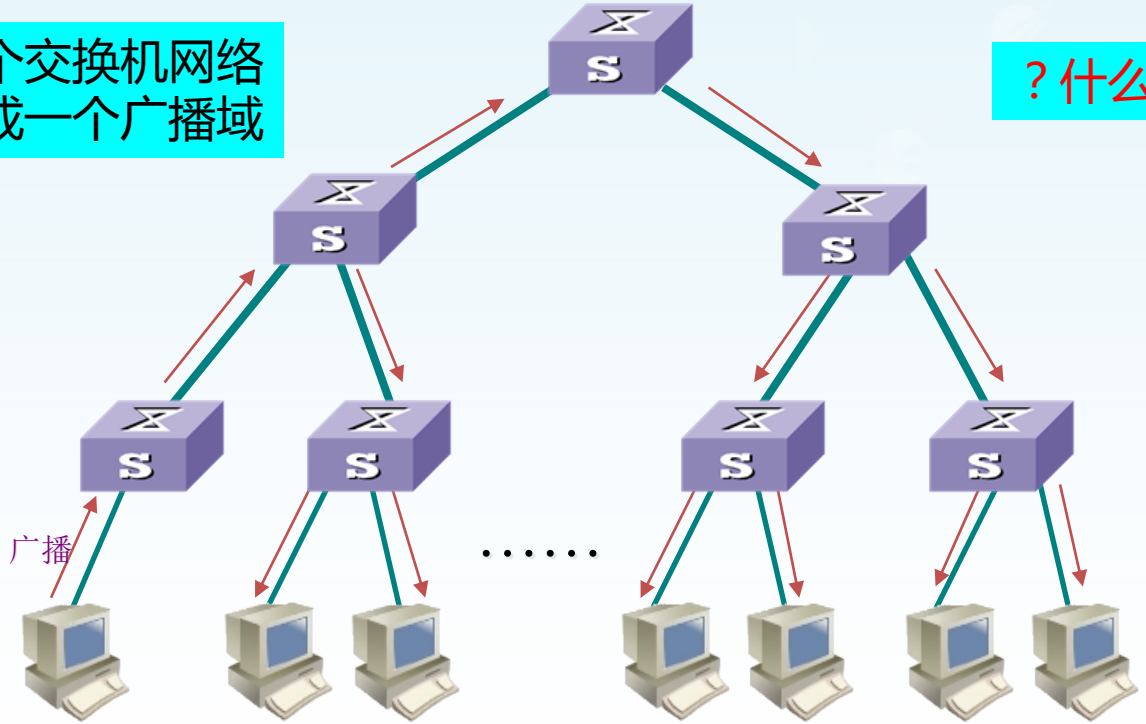
交换机上VLAN的配置

- 使用VLAN的原因
- VLAN的分类
- VLAN标准：IEEE 802.1Q
- VLAN间的路由
- VLAN的基本配置
- VLAN间的路由配置

使用VirtualLAN（VLAN）的原因

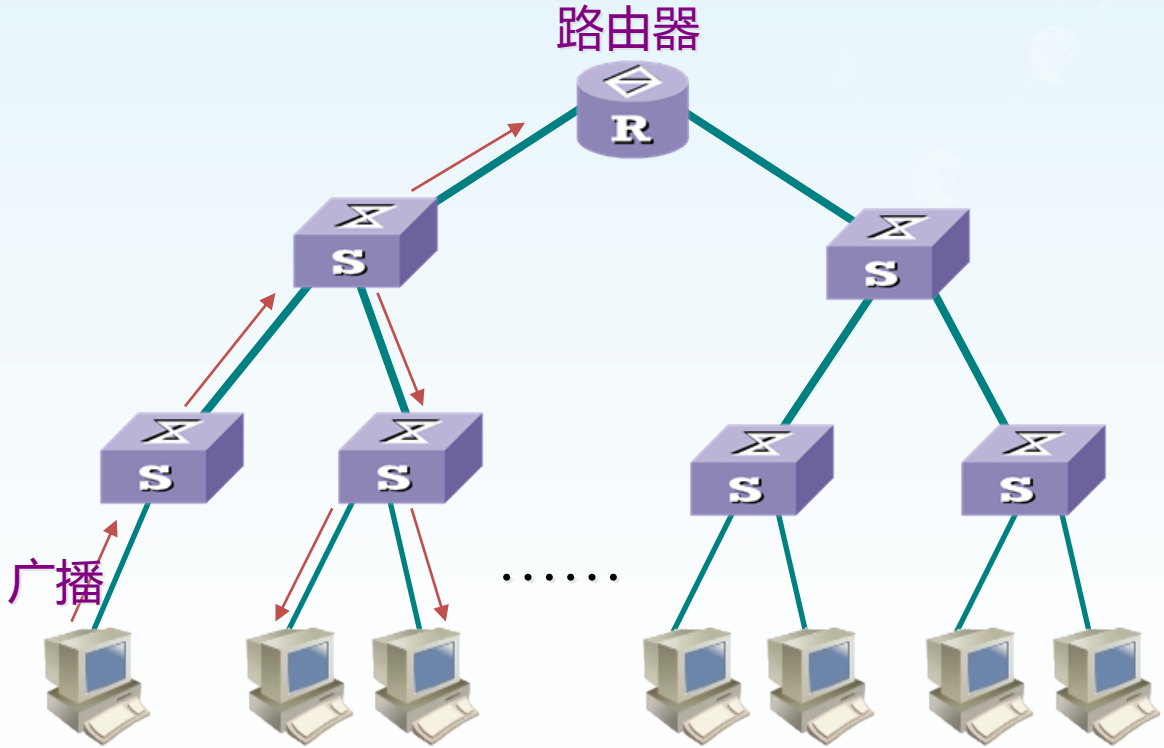
整个交换机网络
构成一个广播域

？什么是广播域



广播域与广播风暴

使用VLAN的原因（续）



使用路由器来隔离广播域代价高

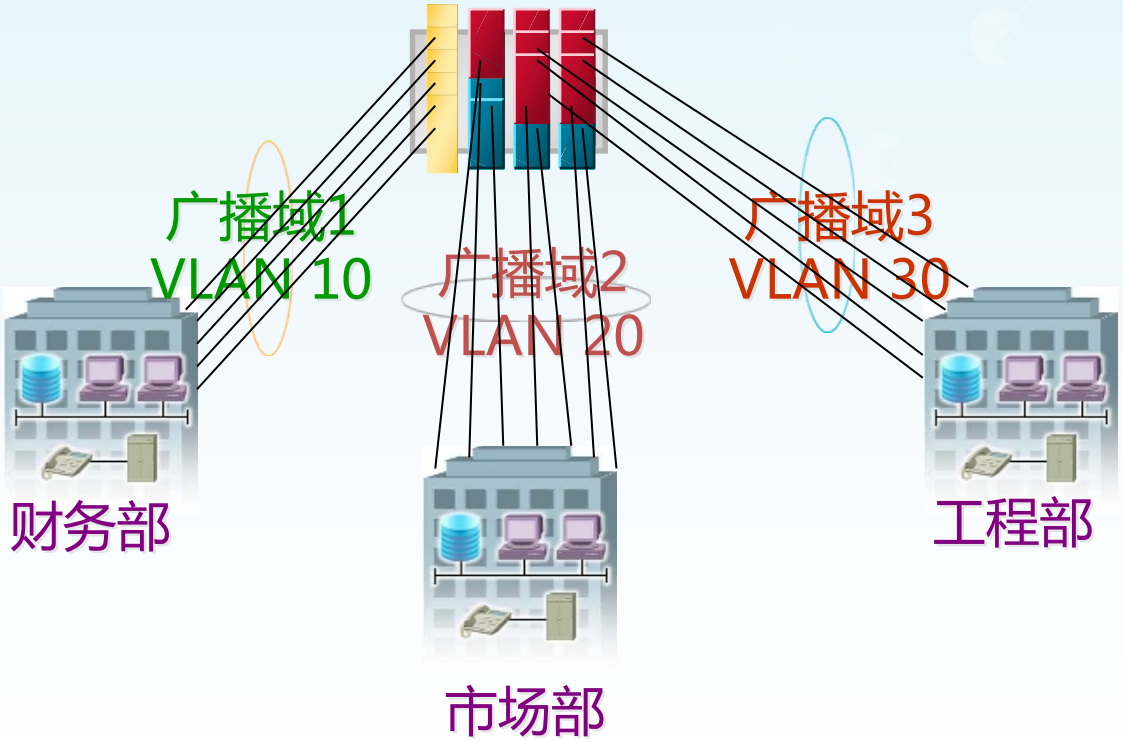
使用VLAN的原因-VLAN概述

- 以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机可实现LAN（Local Area Network）互联，由于交换机采用交换方式将来自入接口的信息转发到指定出接口上，克服了共享介质上的访问冲突问题，有效的解决了冲突严重问题。但是，当来自入接口的信息无法确定指定的出接口时，此信息会通过交换机上其他所有接口转发（除接收该信息的接口），形成了广播域。

- 为了解决广播域问题，可将网络分段，把大的广播域划分为若干个小的广播域，从而限制广播报文的影响范围。通常采用路由器在网络层进行网络隔离，但是存在规划复杂、组网方式不灵活，且成本较高。作为替代的LAN分段方法，VLAN（Virtual Local Area Network，虚拟局域网）技术被引入，用于解决大型的二层网络所面临的广播风暴、安全等问题。

- VLAN是将一个物理的LAN在逻辑上划分成多个广播域（多个VLAN）的通信技术。每一个VLAN都包含一组拥有相同需求的计算机，与物理上形成的LAN具有相同的属性。但是由于VLAN是在逻辑划分而不是在物理上划分，所有同一个VLAN内的各个工作站无需放置在同一个物理空间。即使两台计算机有着同样的网段，如果它们不属于同一个VLAN，它们各自的广播流不会互相转发，从而实现了控制流量、减少设备投资、简化网络管理、提高网络的安全性。

使用VLAN的原因实例（续）



使用VLAN来隔离广播域代价低

使用VLAN的原因实例（续）

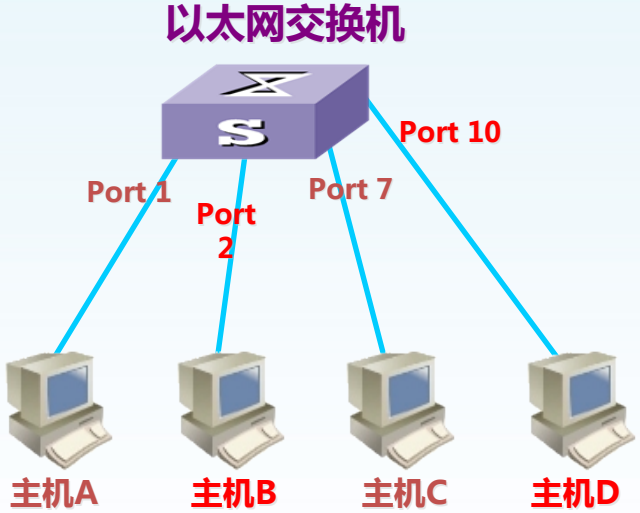
从上页应用实例可以看出VLAN具有以下优势：

- 限制广播域。广播域被限制在一个VLAN内，节省了带宽，提高了网络处理能力。
- 增强局域网的安全性。不同VLAN内的报文在传输时是相互隔离的，即一个VLAN内的用户不能和其它VLAN内的用户直接通信。
- 提高了网络的健壮性。故障被限制在一个VLAN内，本VLAN内的故障不会影响其他VLAN的正常工作。
- 灵活构建虚拟工作组。用VLAN可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，网络构建和维护更方便灵活。

VLAN的分类

- 基于端口的VLAN
- 基于MAC地址的VLAN
- 基于协议的VLAN
- 基于子网的VLAN
- 基于策略的VLAN

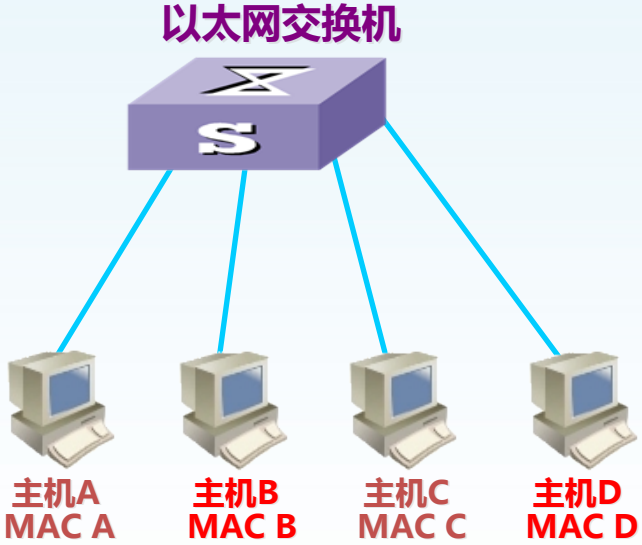
基于端口的VLAN



VLAN表

端口	所属VLAN
Port 1	VLAN 5
Port 2	VLAN 10
……	……
Port 7	VLAN 5
……	……
Port 10	VLAN 10

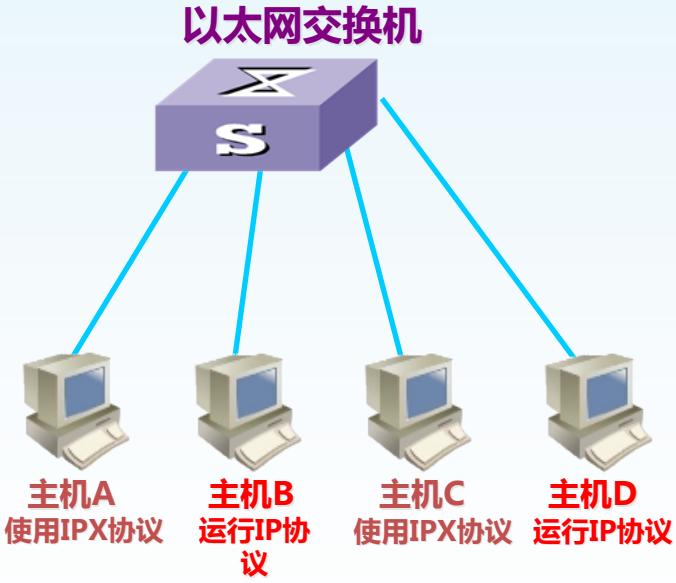
基于MAC地址的VLAN



VLAN表

MAC地址	所属VLAN
MAC A	VLAN 5
MAC B	VLAN 10
MAC C	VLAN 5
MAC D	VLAN 10

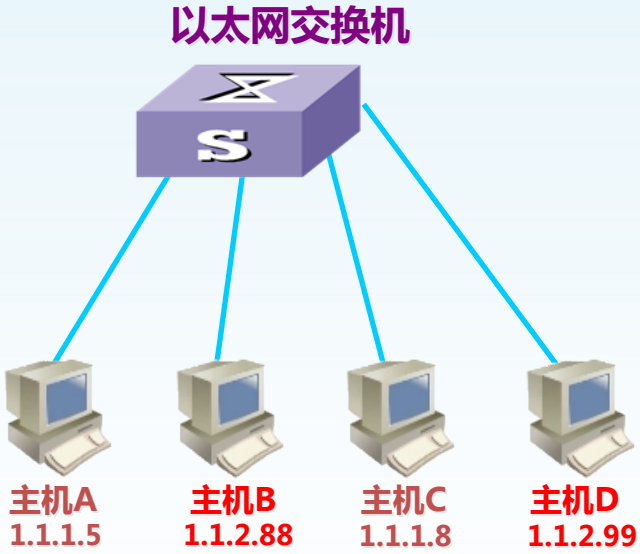
基于协议的VLAN



VLAN表

协议类型	所属VLAN
IPX协议	VLAN 5
IP协议	VLAN 10
……	……

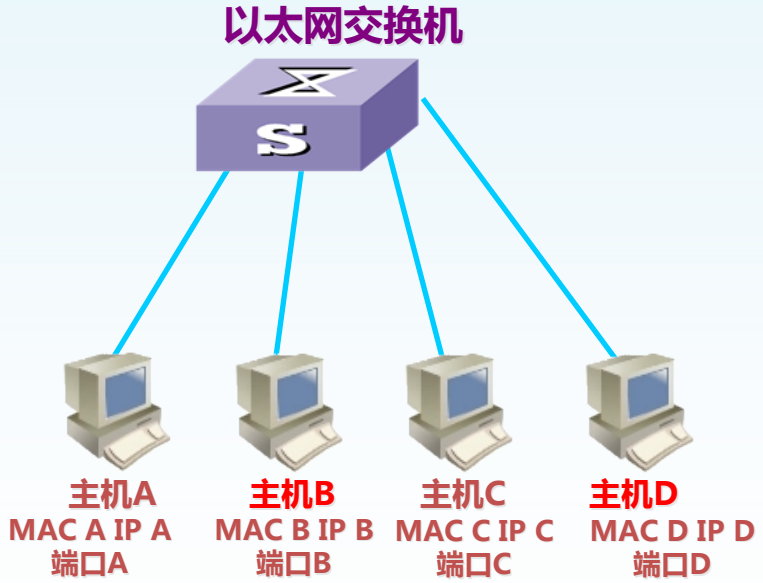
基于子网的VLAN



VLAN表

IP网络	所属VLAN
IP 1.1.1.1/24	VLAN 5
IP 1.1.2.1/24	VLAN 10
……	……

基于策略的VLAN



VLAN表

MAC地址、IP地址、端口	所属VLAN
MAC A IP A 端口A	VLAN 5
MAC B IP B 端口B	VLAN 10
……	……

不同VLAN划分方式对应的应用场景

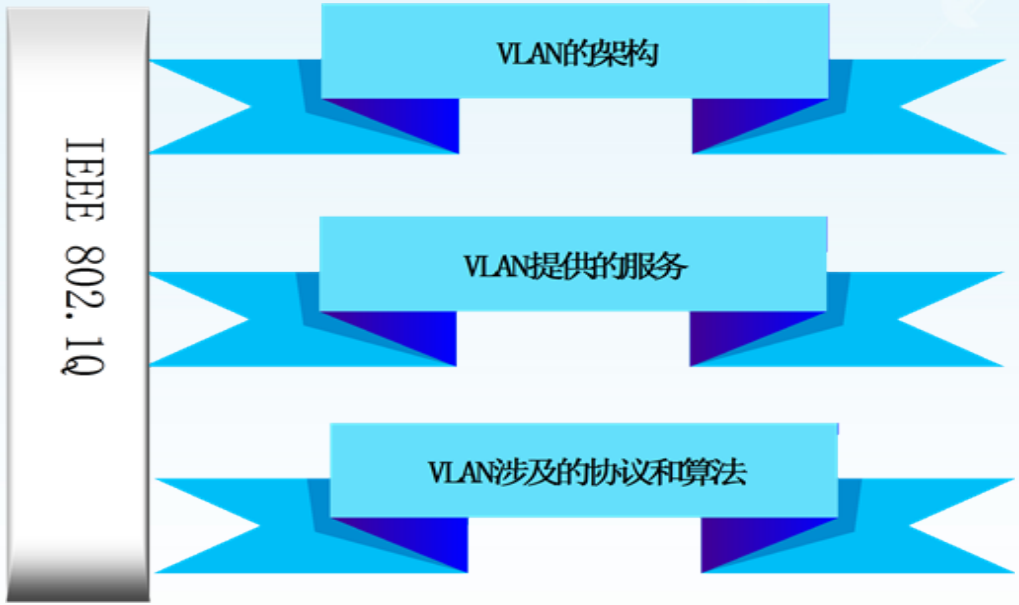
表1 不同VLAN划分方式对应的应用场景

VLAN划分方式	优点	缺点	应用场景
基于端口划分	配置过程简单明了，是最常用的VLAN划分方式。	配置不够灵活，当VLAN中的成员端口移动时需要重新配置VLAN。这对于拥有众多移动用户的网络来说，网络管理者将会花费更多的时间进行维护。	适用于规模大、安全需求不高的场景中。
基于MAC地址划分	用户在变换物理位置时，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。	网络管理者需要事先将归属到指定VLAN的终端MAC地址配置到交换机上。这对拥有大量终端的网络来说，初始配置时，配置工作量较大。	适用于安全和移动性需求较高的场景中。
基于子网划分	基于子网划分VLAN和基于协议划分VLAN统称为基于网络层划分VLAN。 基于网络层划分VLAN，不但大大减少了人工配置VLAN的工作量，同时保证了用户自由地增加、移动和修改。	交换机需要解析源IP地址并进行相应转换，导致交换机响应速度慢。	适用于对安全需求不高，对移动性和简易管理需求较高的场景中。
基于协议划分		交换机需要分析各种协议的地址格式并进行相应转换，导致交换机响应速度慢。	目前支持at、ipv4、ipv6、ipx、llc协议划分VLAN。
基于策略划分VLAN	安全性非常高，基于MAC地址+IP地址、MAC地址+IP地址+接口成功划分VLAN后，禁止用户改变IP地址或MAC地址。 相较于其他VLAN划分方式，基于策略划分VLAN是优先级最高的VLAN划分方式。	针对每一条策略都需要手工配置。	适用于规模小，且对安全和移动性需求非常高的场景中。

VLAN标准：IEEE 802.1Q

- 概述
- VLAN的帧格式
- VLAN的链路类型
- VLAN的帧转发算法

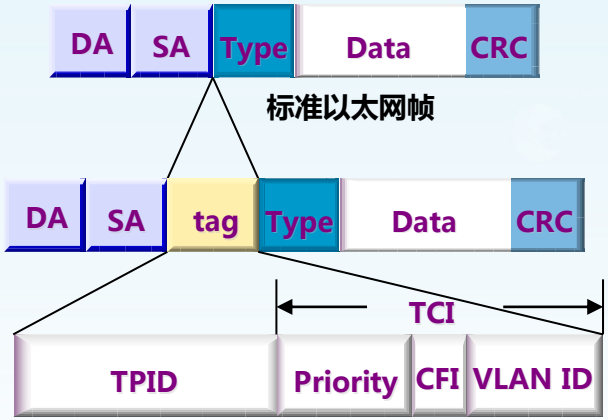
IEEE 802.1Q 概述



IEEE 802.1Q可以在www.ieee802.org免费下载

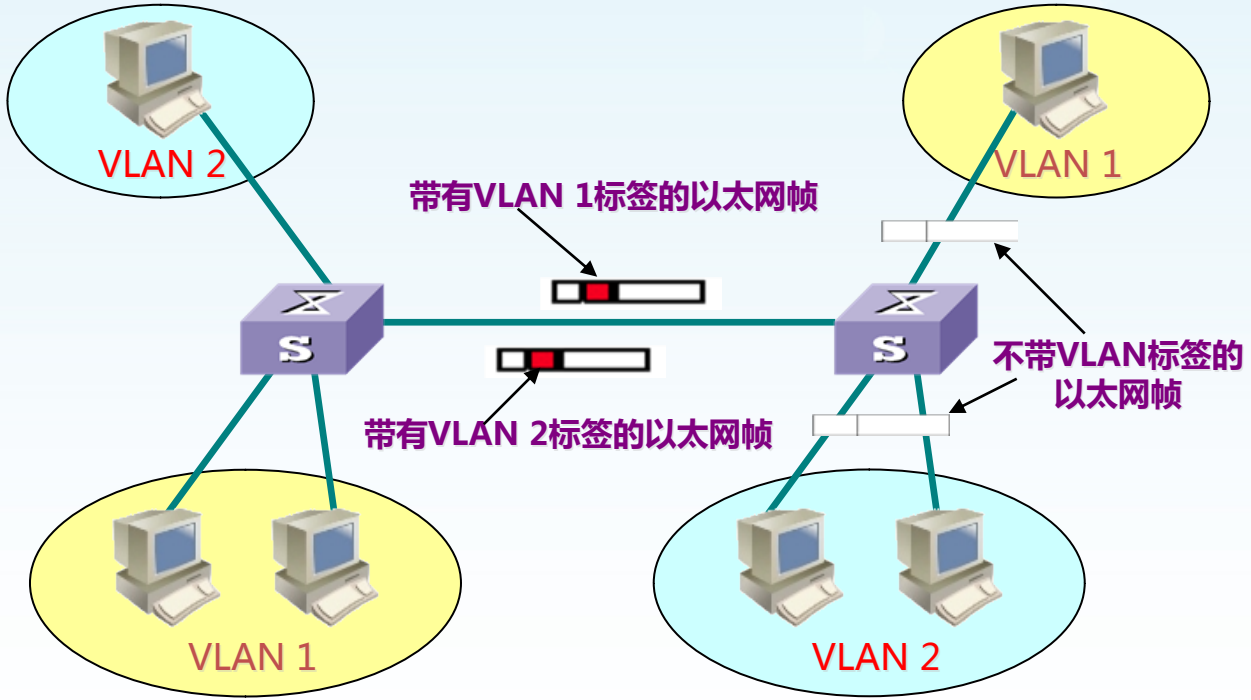
VLAN的帧格式

带有IEEE802.1Q标签的以太网帧：



- TPID: Tag Protocol Identifier, 2字节，标识协议的类型
- TCI: Tag Control Information，2字节
  - Priority：标识帧的优先级，3比特
  - CFI：Canonical Format Indicator，1比特
  - VLAN ID：标识一个VLAN，12比特

PC机和交换机对帧的传输



帧在VLAN间的传输时发生的变化

VLAN的链路类型

- 接入链路（Access Link）
  - 运载不带有VLAN标签的帧（untagged frames）
- 骨干链路（Trunk Link）
  - 运载带有VLAN标签的帧（tagged frames），但VLAN ID与Trunk Link的缺省VLAN ID相同的帧除外
- 混合链路（Hybrid Link）
  - 既可以运载带有VLAN标签的帧，也可以运载不带有VLAN标签的帧
  - 不常用（例如用于Hub等共享介质链路）

VLAN的链路类型（续）

相应的，人们也把交换机上与前面三种链路相连的端口分别称为Access Port，Trunk Port和Hybrid Port：

- 接入端口（Access Port）
  - 发送/接收不带有VLAN标签的帧（untagged frames）
  - 只能属于一个VLAN（也就意味只能允许所属VLAN的帧通过）
- 骨干端口（Trunk Port）
  - 发送/接收带有VLAN标签的帧（tagged frames），但VLAN ID与Trunk Link的缺省VLAN ID相同的帧除外
  - 可以允许多个VLAN的帧通过
- 混合端口（Hybrid Port）
  - 既可以发送/接收带有VLAN标签的帧，也可以发送/接收不带有VLAN标签的帧
  - 可以允许多个VLAN的帧通过

VLAN中的帧转发算法

若从Access端口收到一个帧：

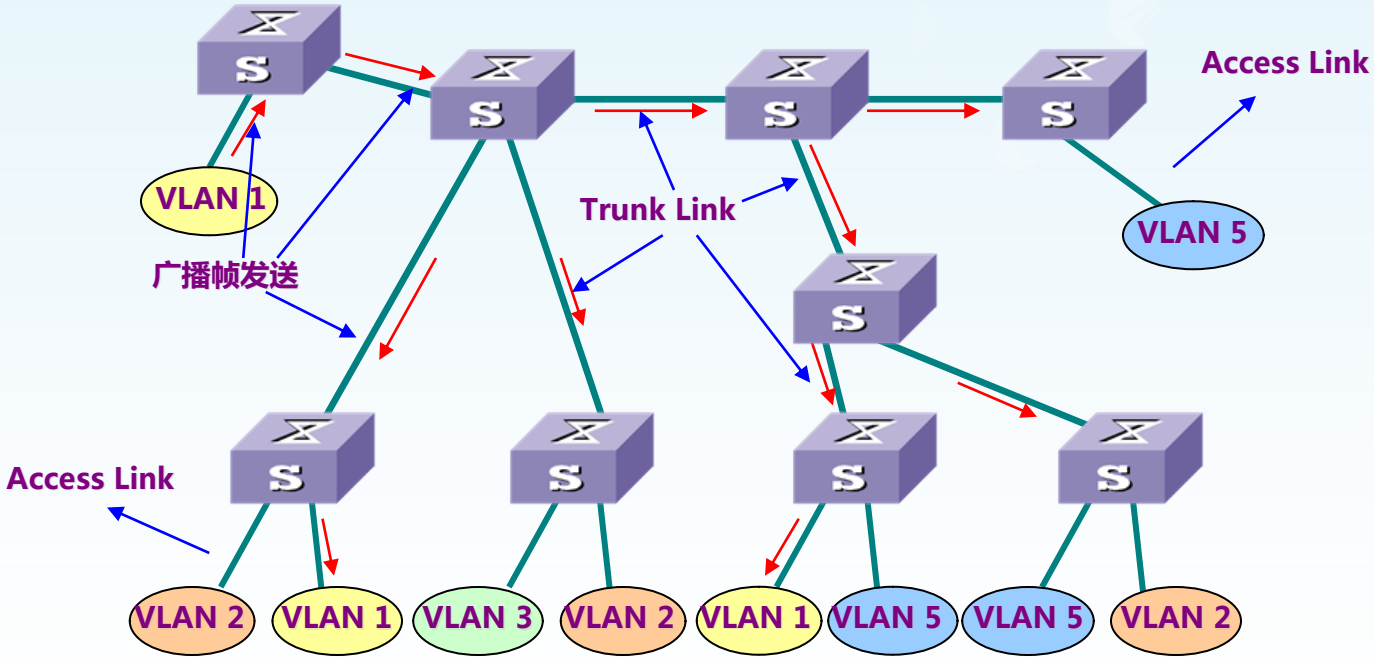
- 根据该端口的VLAN ID为该帧插入标签
- 查该VLAN的MAC地址表，做出转发决定
- 若从Trunk端口转发，则携带标签发出（例外：当该帧的VLAN ID与Trunk端口的缺省VLAN ID相同时，去掉标签后再发出）
- 若从Access端口转发，则去掉标签后再发出

VLAN中的帧转发算法（续）

若从Trunk端口收到一个帧：

- 若该帧不携带标签，则根据该端口的缺省VLAN ID为该帧插入标签
- 查该帧所属VLAN的MAC地址表，做出转发决定
- 若从Trunk端口转发，则携带标签发出（例外：当该帧的VLAN ID与Trunk端口的缺省VLAN ID相同时，去掉标签后再发出）
- 若从Access端口转发，则去掉标签后再发出

举例：广播域的隔离（广播帧的传输）

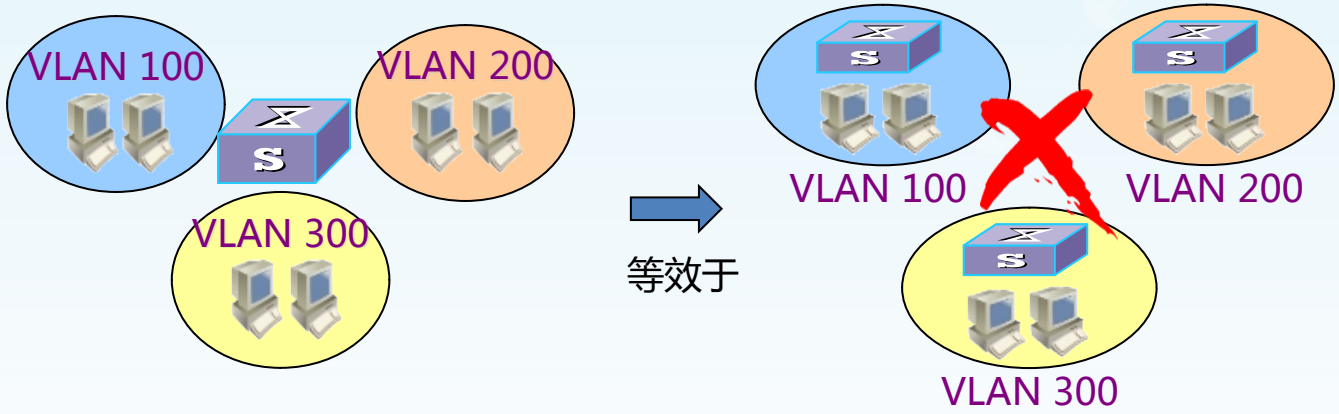


在Trunk Link上全部转发

VLAN间的路由

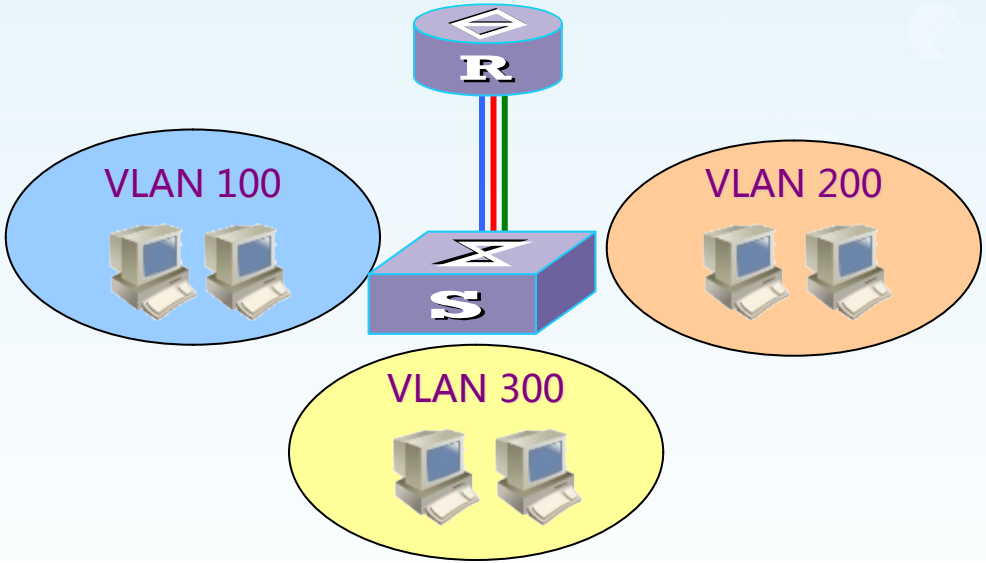
- 使用路由的原因
- 用路由器来做路由
- 用三层交换机来做路由

使用路由的原因



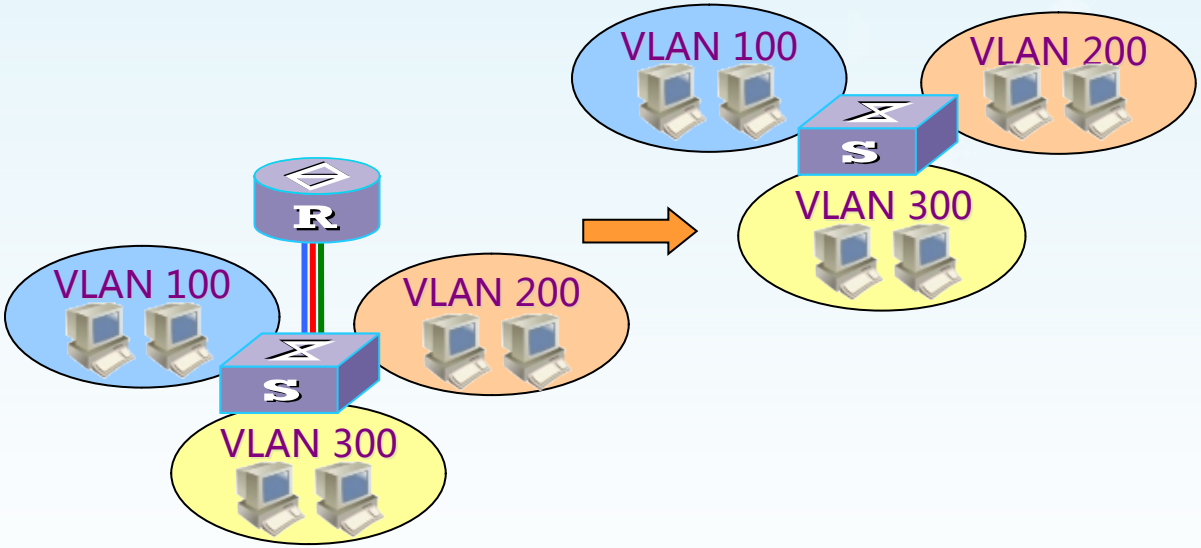
- VLAN隔离了广播域，也就严格地隔离了各个VLAN之间的在第二层上的互相转发
- 只有借助第三层的功能（即路由），才能使各VLAN之间互相通信。

使用路由器来做路由



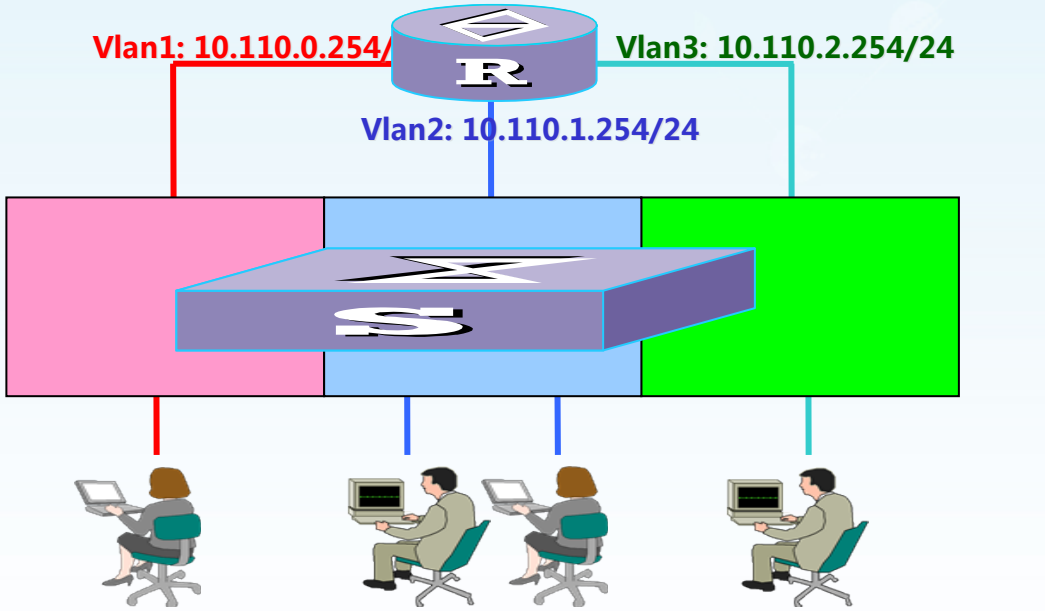
- 将每个VLAN都连接到路由器
- 缺点：路由器的造价高

使用三层交换机来做路由



- 二层交换机和路由器在功能上的集成构成了三层交换机
- 三层交换机一般都实现了VLAN的划分、VLAN内部的二层交换和VLAN间路由的功能。

使用三层交换机来做路由（续）



三层交换机功能模型

使用三层交换机来做路由（续）

划分VLAN后，同一VLAN内的用户可以互相通信，但是属于不同VLAN间的用户不能直接互相通信。为了实现VLAN间通信，可通过下表所示的方案实现

三层交换机实现VLAN间通信方案

VLAN间通信方案	优点	缺点	应用场景
VLAN接口	属于不同VLAN且位于不同网段的用户，只要在路由可达的前提下，随时可以互相通信。	如果网络中存在多个用户属于不同VLAN，那么需要为每一个VLAN创建对应的VLAN接口，并分配IP地址，增加了配置工作量且占用大量IP地址资源。	适用于规模小、IP地址固定的网络，且用户属于不同网段。如果VLAN配置比较多，既要进行二层转发，又要进行三层转发，选择使用VLAN接口。

VLAN的基本配置

- 创建/删除VLAN
- 指定VLAN中的端口（Access端口）
  - 给VLAN指定端口
  - 给端口指定VLAN
- 设定端口的链路类型
- 设置Trunk端口允许通过的VLAN
- 设置Trunk端口的缺省VLAN ID
- 其它常用命令
- VLAN组网配置举例

创建/删除VLAN

- 创建VLAN并进入VLAN视图

  [H3C] vlan *vlan_id*

  注：执行后提示符变为“[H3C-vlan*id*]”；若该VLAN已存在，则仅进入VLAN视图
- 删除VLAN

  [H3C] undo vlan *vlan_id*
- 参数说明：

  vlan-id：VLAN接口的ID，取值范围为1～4094
- 举例：

  [H3C] vlan 1

给VLAN指定端口

- 向VLAN中添加交换机端口
  [H3C-vlan1] port port_num [to port_num] & < 1-10 >
- 从VLAN中删除交换机端口
  [H3C-vlan1] undo port port_num [to port_num] & <1-10>
- 参数说明：
  port_num：由Interface类型和端口序号组成；端口序号由槽号和端口号的二元组组成,或由设备单元号、槽号和端口号的三元组组成。
- 举例：
  [H3C-vlan1] port G1/ 0/1 to G1/ 0/12(G或E为简写)

给端口指定VLAN

- 将端口添加到VLAN:
  [H3C-GigabitEthernet1/0/1] port access vlan *vlan-id*

- 将端口从VLAN中删除
  [H3C-GigabitEthernet1/0/1] undo port access vlan *vlan-id*

- 举例：
  [H3C-GigabitEthernet1/0/1] port access vlan 3

设置端口的链路类型

- 设置命令：
  [H3C-GigabitEthernet1/0/1] port link-type { access | trunk | hybrid }

- 恢复为缺省值命令：
  [H3C-GigabitEthernet1/0/1] undo port link-type

- 举例：
  [H3C-GigabitEthernet1/0/1]port link-type trunk

设置Trunk端口允许通过的VLAN

- 允许某些VLAN的帧通过当前Trunk端口：
  [H3C-GigabitEthernet1/0/1] port trunk permit vlan
  { vlan_id_list | all }
  vlan_id_list: vlan_id1 [to vlan_id2] & <1-10>
- 将当前Trunk端口从某些VLAN中删除：
  [H3C-GigabitEthernet1/0/1] [undo] port trunk permit
  vlan { vlan_id_list | all }
- 举例：
  [H3C-GigabitEthernet1/0/1] port trunk permit vlan 2 6
  to 10 25
  [H3C-GigabitEthernet1/0/1] port trunk permit vlan all

汇聚情况下设置trunk链路（备注）

- [H3C]interface bridge-aggregation 1
- [H3C-bridge-aggregation1]port link-type trunk
- [H3C-bridge-aggregation1]port trunk permit vlan 2 to 3

不需要在实际物理端口视图下分别设置trunk属性

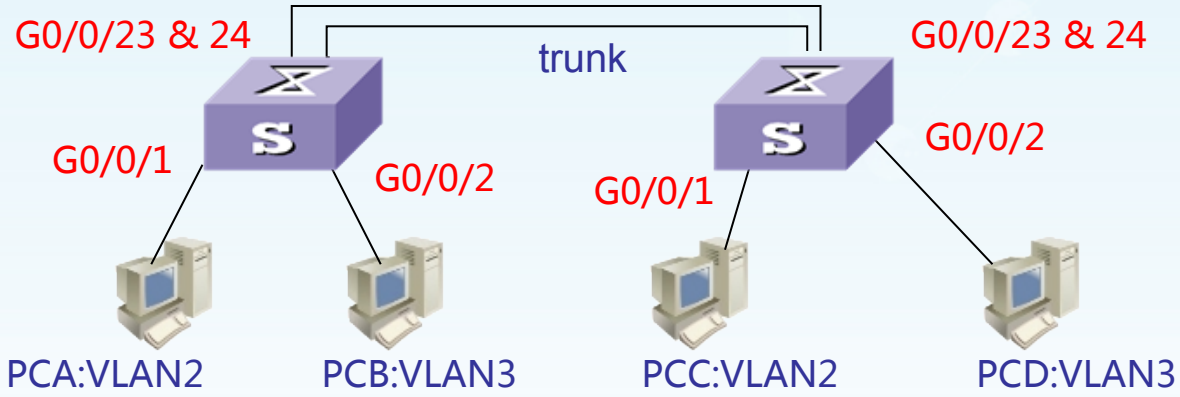
设置Trunk端口的缺省VLAN ID

- 设置端口的缺省VLAN ID（pvid, Port Vlan ID）：
  [H3C-GigabitEthernet1/0/1] port trunk pvid vlan *vlan_id*
- 恢复端口的缺省VLAN ID：
  [H3C-GigabitEthernet1/0/1] undo port trunk pvid
  注：vlan_id的缺省值为1
- 举例：
  [H3C-GigabitEthernet1/0/1] port trunk pvid vlan 3

其他常用命令

- 指定/删除VLAN描述字符：
  [H3C-vlan1] description *string*
  [H3C-vlan1] undo description
  例：[H3C-vlan1] description Floor 1 and 2
- 查看VLAN设置：
  [任意视图] display vlan [*vlan_id*]
- 开启/关闭VLAN接口：
  [H3C-vlan-interface1] shutdown
  [H3C-vlan-interface1] undo shutdown

VLAN组网配置举例



目标：

- PCA和PCC同属于一个VLAN 2且能相互通信。
- PCB和PCD同属于另一个VLAN 3且能相互通信。
- 两台交换机用两根1000M网线通过Trunk链路互连，并使用端口聚合功能增加链路带宽

VLAN组网配置举例（续）

- 配置VLAN：
  - [SwitchA] vlan 2
  - [SwitchA-vlan2] port g1/ 0/1
  - [SwitchA-vlan2] vlan 3
  - [SwitchA-vlan3] port g1/ 0/2
- 配置端口聚合
  - [SwitchA] interface bridge-aggregation 1
  - [interface bridge-aggregation 1] int g1/0/23
  - [SWA-GigabitEthernet1/0/23] port link-aggregation group 1
  - [SWA-GigabitEthernet1/0/23] int g1/0/24
  - [SWA-GigabitEthernet1/0/24] port link-aggregation group 1
  - [SWA-GigabitEthernet1/0/24] interface bridge-aggregation 1
  - [interface bridge-aggregation 1]port link-type trunk
  - [interface bridge-aggregation 1]prot trunk permit vlan 2 to 3

注：SwitchB做类似配置

VLAN间路由的配置

- IP地址的配置
- 静态路由的配置
- 路由配置举例
- 学院校园网剖析

IP地址的配置

- 设定IP地址
  [H3C-vlan-inferface1] ip address *ip-addr netmask*
- 取消IP地址
  [H3C-vlan-inferface1] undo ip address
- 举例
  [H3C-vlan-inferface1] ip address 210.30.103.254 255.255.255.0
- 检查IP地址配置是否正确
  [任意视图] display interface vlan-interface [*vlan_id*]

静态路由的配置

- 添加一条静态路由表项

  [H3C] ip route-static *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *gateway-address* }
- 删除一条静态路由表项

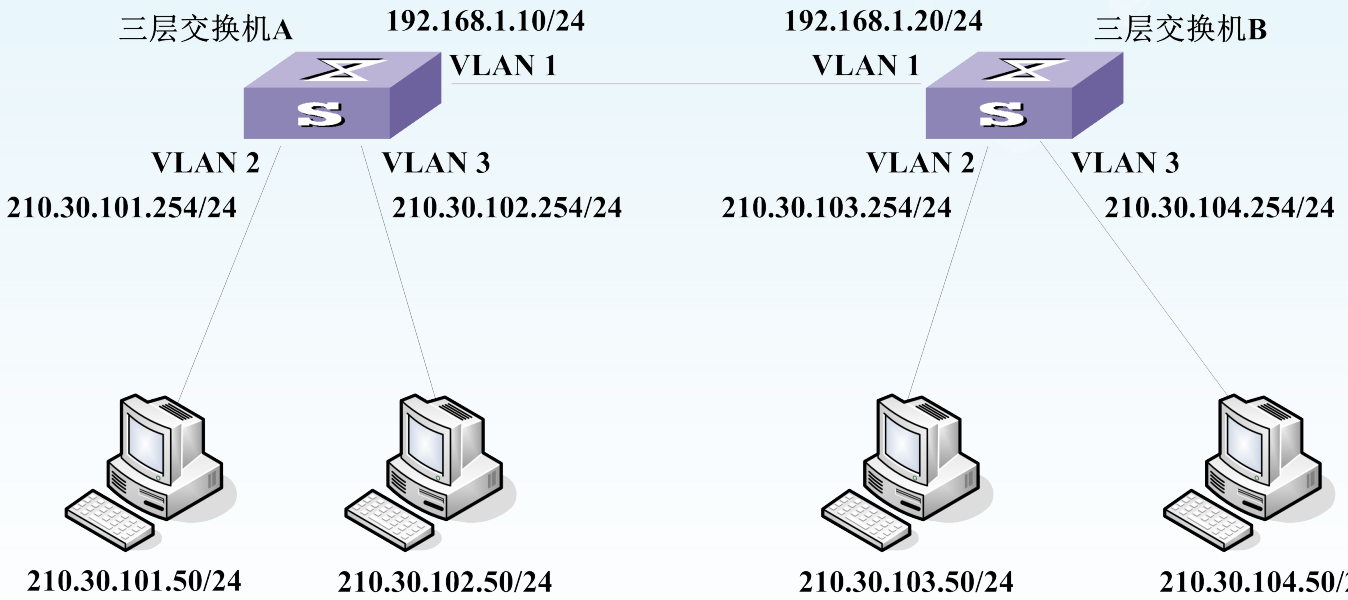
  [H3C] undo ip route-static *ip-address* { *mask* | *mask-length* }
- 举例

  [H3C] ip route-static 210.30.104.0 24 210.30.104.254

  [H3C] ip route-static 0.0.0.0 0 192.168.1.1 //缺省路由
- 检查静态路由配置是否正确

  [任意视图] display ip routing-table

VLAN路由配置举例



要求：使上述PC机之间能够互通

VLAN路由配置举例（续）

- 使用下面命令设置交换机A的三个VLAN接口的IP地址：

  [SwitchA-vlan-interface1] ip address 192.168.1.10 255.255.255.0

  [SwitchA-vlan-interface2] ip address 210.30.101.254 255.255.255.0

  [SwitchA-vlan-interface3] ip address 210.30.102.254 255.255.255.0

- 使用下面命令设置交换机A上的静态路由表：

  [SwitchA] ip route-static 210.30.103.0 255.255.255.0 192.168.1.20

  [SwitchA] ip route-static 210.30.104.0 255.255.255.0 192.168.1.20

- 配置四台PC机上的缺省网关

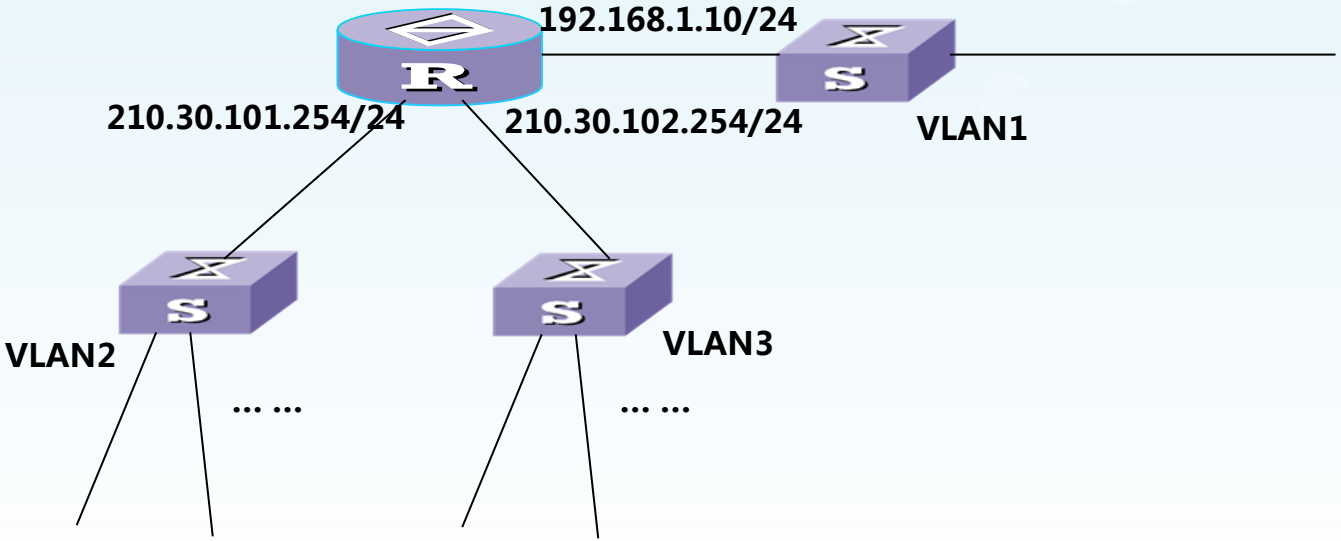
注：

（1）同一交换机上不同VLAN间的路由表项可以由交换机自动生成；

（2）因不存在跨交换机的VLAN，故不需配置Trunk链路；

（3）交换机B上的配置类似。

VLAN路由配置举例



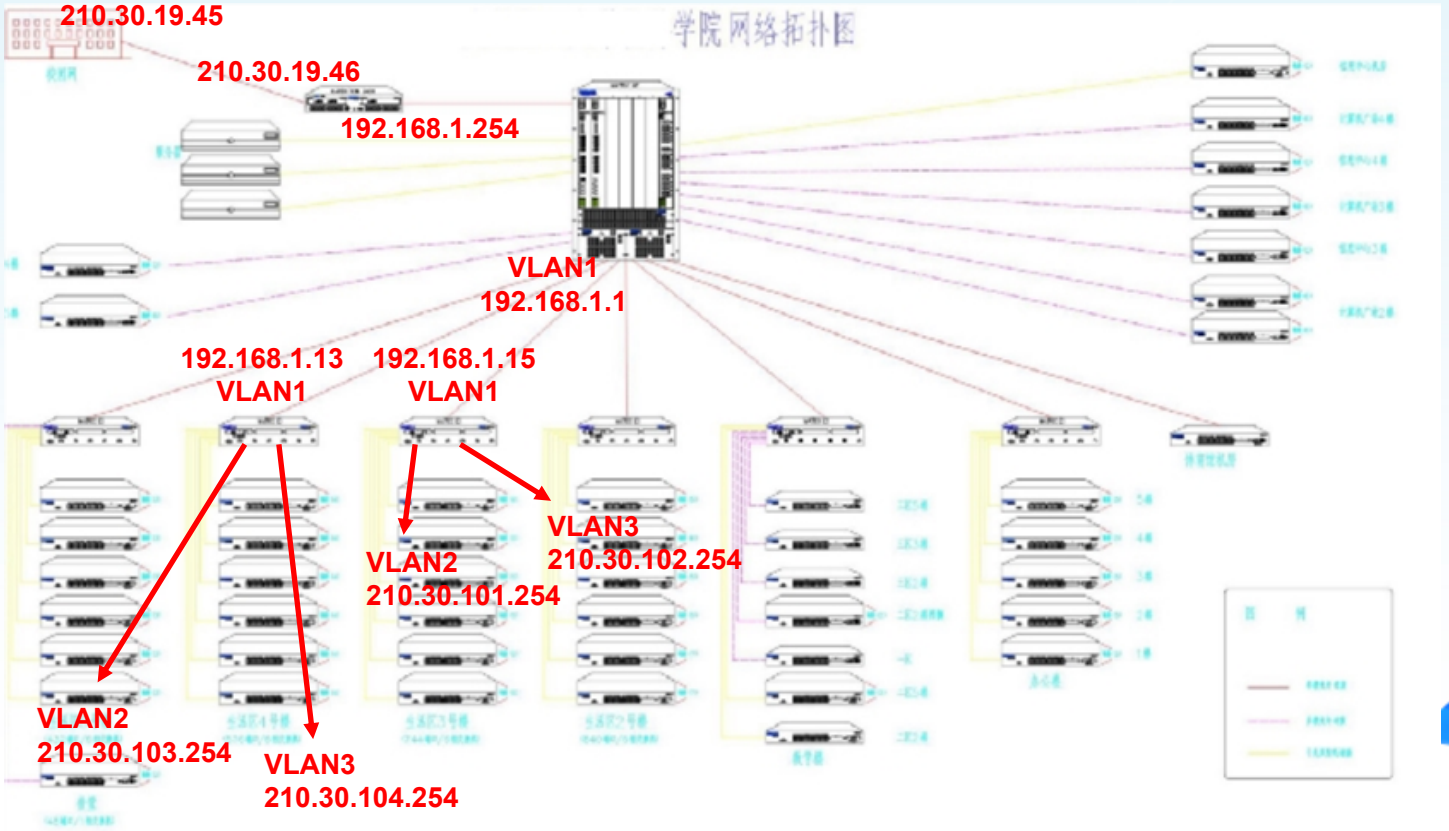
三层交换机A的等价图：三个VLAN把一个交换机分割成了三个交换机，它们之间通过一个路由器相联

理解路由表

[SwitchA] display ip routing-table
Routing Tables:

Destination/Mask	Proto	Pref	Metric	Nexthop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	LoopBack0
127.0.0.1/32	Direct	0	0	127.0.0.1	LoopBack0
192.168.1.0/24	Direct	0	1	192.0.0.2	vlan1
210.30.101.0/24	Direct	0	1	127.0.0.1	LoopBack0
210.30.102.0/24	Direct	0	1	127.0.0.1	LoopBack0
210.30.103.0/24	Static	60	2	192.168.1.20	vlan1
210.30.104.0/24	Static	60	2	192.168.1.20	vlan1

某校园网剖析


学院网络拓扑图
210.30.19.45
210.30.19.46
192.168.1.254
VLAN1
192.168.1.1
192.168.1.13
VLAN1
192.168.1.15
VLAN1
VLAN3
210.30.102.254
VLAN2
210.30.101.254
VLAN2
210.30.103.254
VLAN3
210.30.104.254