第三章 交换机与VLAN

内容

- 3.1路由器实验回顾
- 3.2交换机与vlan
- 3.3交换机实验内容

3.1路由器实验回顾

- 路由器实验中的问题：
  - PC机上的路由
    - 默认路由：
    - Ip route 0.0.0.0 0.0.0.0 f0/0
  - Rip协议观察
    - 224.0.0.9　组播地址
  - Ospf协议观察
    - Debug ip ospf events
    - Debug ip ospf flood
  - Encapsulation用法

```
Router(config-router)#
02:22:37: OSPF: Interface Serial1/1 going Up
02:22:38: OSPF: Build router LSA for area 0, router ID 2.1.1.1, seq 0x80000002
02:22:41: OSPF: 2 Way Communication to 3.1.1.1 on Serial1/1, state 2WAY
02:22:41: OSPF: Send DBD to 3.1.1.1 on Serial1/1 seq 0x167D opt 0x42 flag 0x7 len 32
02:22:41: OSPF: Rcv DBD from 3.1.1.1 on Serial1/1 seq 0x2411 opt 0x42 flag 0x7 len 32  mtu 1500 state EXSTART
02:22:41: OSPF: NBR Negotiation Done. We are the SLAVE
02:22:41: OSPF: Send DBD to 3.1.1.1 on Serial1/1 seq 0x2411 opt 0x42 flag 0x2 len 52
02:22:41: OSPF: Rcv DBD from 3.1.1.1 on Serial1/1 seq 0x2412 opt 0x42 flag 0x3 len 52  mtu 1500 state EXCHANGE
02:22:41: OSPF: Send DBD to 3.1.1.1 on Serial1/1 seq 0x2412 opt 0x42 flag 0x0 len 32
02:22:41: OSPF: Database request to 3.1.1.1
02:22:41: OSPF: sent LS REQ packet to 1.1.1.2, length 12
02:22:41: OSPF: Rcv DBD from 3.1.1.1 on Serial1/1 seq 0x2413 opt 0x42 flag 0x1 len 32  mtu 1500 state EXCHANGE
02:22:41: OSPF: Exchange Done with 3.1.1.1 on Serial1/1
02:22:41: OSPF: Send DBD to 3.1.1.1 on Serial1/1 seq 0x2413 opt 0x42 flag 0x0 len 32
02:22:41: OSPF: Synchronized with 3.1.1.1 on Serial1/1, state FULL
02:22:41: %OSPF-5-ADJCHG: Process 20, Nbr 3.1.1.1 on Serial1/1 from LOADING to FULL, Loading Done
02:22:44: OSPF: Build router LSA for area 0, router ID 2.1.1.1, seq 0x80000003
Router(config-router)#
02:23:05: OSPF: end of Wait on interface FastEthernet0/0
02:23:05: OSPF: DR/BDR election on FastEthernet0/0
02:23:05: OSPF: Elect BDR 2.1.1.1
02:23:05: OSPF: Elect DR 2.1.1.1
02:23:05: OSPF: Elect BDR 0.0.0.0
02:23:05: OSPF: Elect DR 2.1.1.1
02:23:05:        DR: 2.1.1.1 (Id)   BDR: none
02:23:06: OSPF: No full nbrs to build Net Lsa for interface FastEthernet0/0
```

- Rip
- Network 1.1.1.0

- Network 1.0.0.0

- wr　保存设置
- .net
  - confreg = 0x2102

- Router>

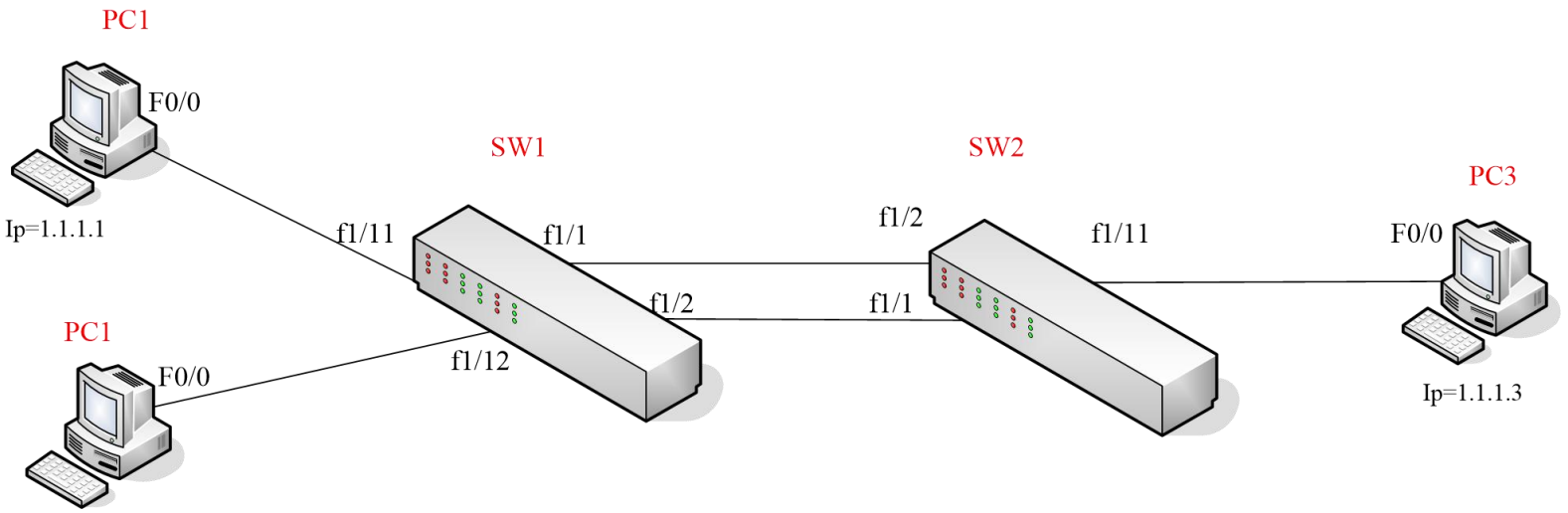
- OSPF
- 改变网络状态
- Debug ip ospf flood

```
Router#debug ip ospf flood
OSPF flooding debugging is on
Router#
00:09:49: OSPF: received update from 2.1.1.1, Serial1/0
00:09:49: OSPF: Rcv Update Type 1, LSID 2.1.1.1, Adv rtr 2.1.1.1, age 1, seq 0x8
0000004
00:09:51: OSPF: Sending delayed ACK on Serial1/0
00:09:51: OSPF: Ack Type 1, LSID 2.1.1.1, Adv rtr 2.1.1.1, age 1, seq 0x80000004
00:11:00: OSPF: received update from 2.1.1.1, Serial1/0
00:11:00: OSPF: Rcv Update Type 1, LSID 2.1.1.1, Adv rtr 2.1.1.1, age 1, seq 0x8
```

```
Router(config-router)#network 3.0.0.0 255.0.0.0 a
Router(config-router)#network 3.0.0.0 255.0.0.0 area 0
Router(config-router)#
00:13:29: Inc retrans unit nbr count index 1 (0/1) to 1/1
00:13:29: Set Nbr 2.1.1.1 1 first flood info from 0 (0) to 623820F8 (1)
00:13:29: Init Nbr 2.1.1.1 1 next flood info to 623820F8
00:13:29: OSPF: Add Type 1 LSA ID 3.1.1.1 Adv rtr 3.1.1.1 Seq 80000003 to Serial
1/0 2.1.1.1 retransmission list
00:13:29: OSPF: Start Serial1/0 2.1.1.1 retrans timer
00:13:29: Set idb next flood info from 0 (0) to 623820F8 (1)
00:13:29: OSPF: Add Type 1 LSA ID 3.1.1.1 Adv rtr 3.1.1.1 Seq 80000003 to Serial
1/0 flood list
00:13:29: OSPF: Start Serial1/0 pacing timer
00:13:29: OSPF: Build router LSA for area 0, router ID 3.1.1.1, seq 0x80000003
00:13:30: OSPF: Flooding update on Serial1/0 to 224.0.0.5 Area 0
00:13:30: OSPF: Send Type 1, LSID 3.1.1.1, Adv rtr 3.1.1.1, age 1, seq 0x8000000
3 (0)
00:13:30: Create retrans unit 0x6274E9AC/0x62A37144 1 (0/1) 1
00:13:30: OSPF: Set nbr 1 (0/1) retrans to 4516 count to 0
00:13:30: Set idb next flood info from 623820F8 (1) to 0 (0)
00:13:30: OSPF: Remove Type 1 LSA ID 3.1.1.1 Adv rtr 3.1.1.1 Seq 80000003 from S
erial1/0 flood list
00:13:30: OSPF: Stop Serial1/0 flood timer
00:13:32: OSPF: Received ACK from 2.1.1.1 on Serial1/0
00:13:32: OSPF: Rcv Ack Type 1, LSID 3.1.1.1, Adv rtr 3.1.1.1, age 1, seq 0x8000
0003
00:13:32: Dec retrans unit nbr count index 1 (0/1) to 0/0
00:13:32: Free nbr retrans unit 0x6274E9AC/0x62A37144 0 total 0. Also Free nbr r
etrans block
00:13:32: Set Nbr 2.1.1.1 1 first flood info from 623820F8 (1) to 0 (0)
00:13:32: Adjust Nbr 2.1.1.1 1 next flood info to 0
00:13:32: OSPF: Remove Type 1 LSA ID 3.1.1.1 Adv rtr 3.1.1.1 Seq 80000003 from 2
.1.1.1 retransmission list
```

3.2交换机与vlan

- Vlan的工作原理
- 三层交换机


PC1
F0/0
Ip=1.1.1.1
SW1
f1/11
f1/1
f1/2
f1/2
f1/1
f1/11
PC3
F0/0
Ip=1.1.1.3
PC1
F0/0
f1/12

虚拟局域网

虚拟网络的概念

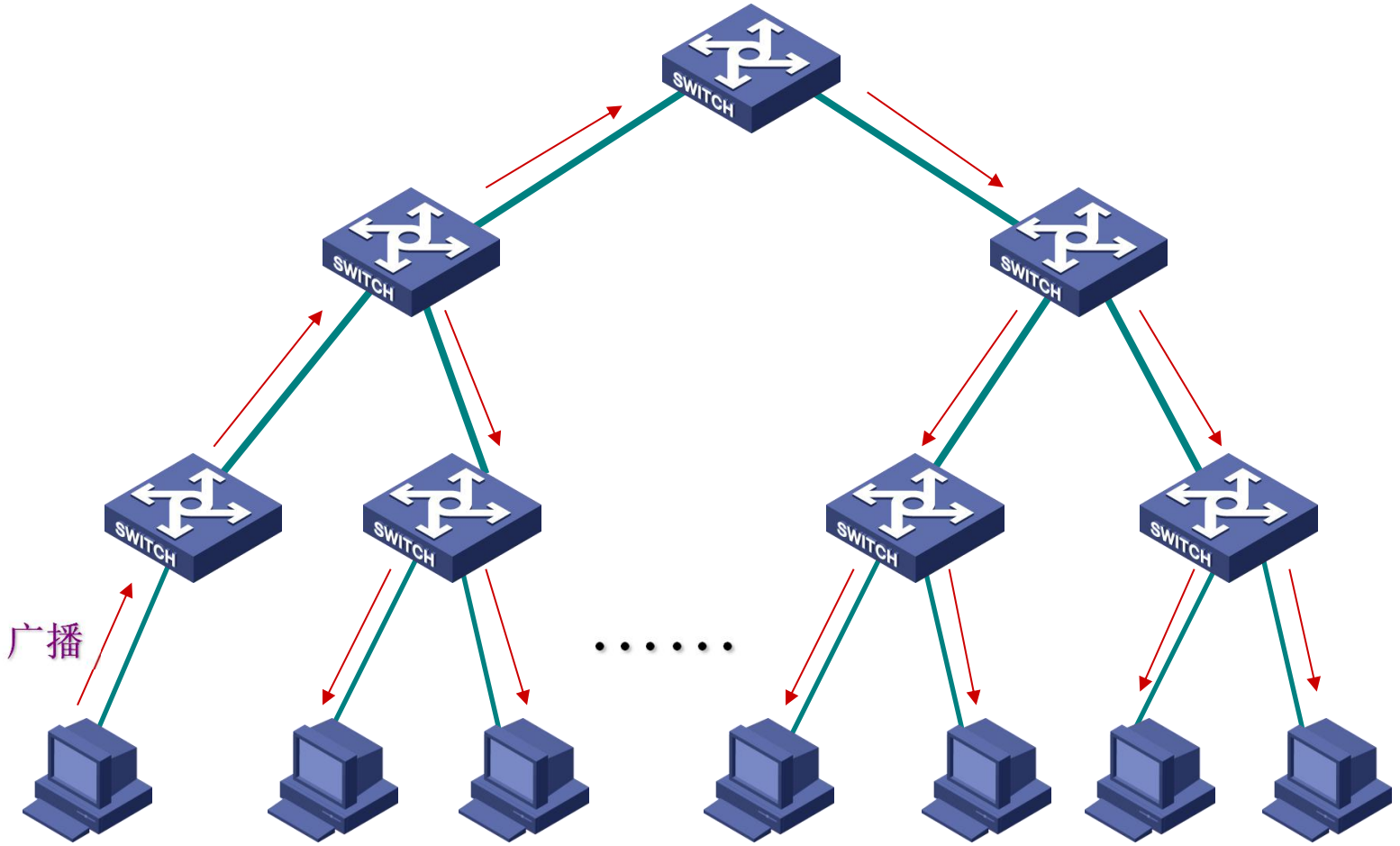
- 虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组。
  - 这些网段具有某些共同的需求。
  - 每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的工作站是属于哪一个 VLAN。
- 虚拟局域网其实只是局域网给用户提供的一种服务，而并不是一种新型局域网。

3.2.1 VLAN的含义

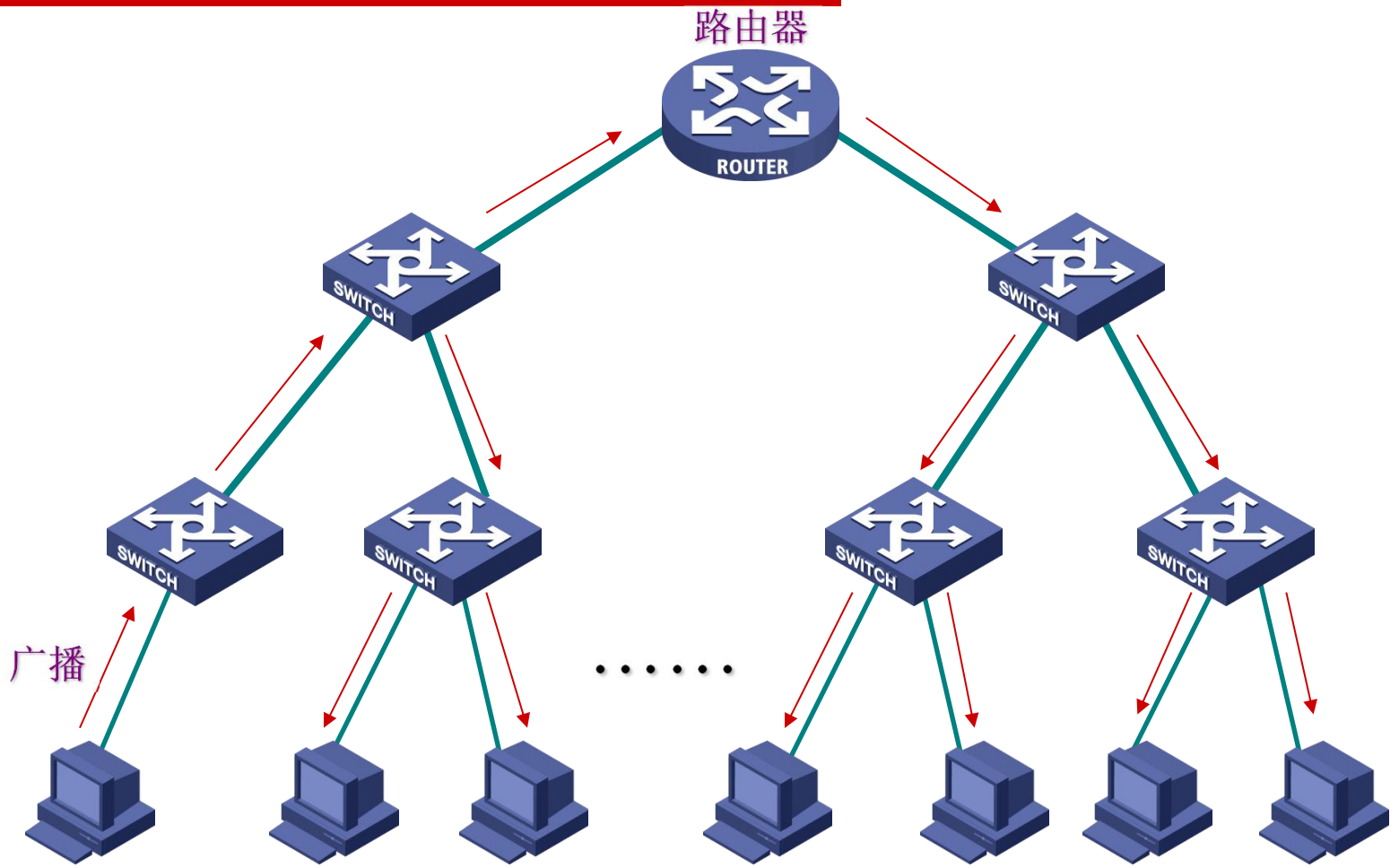
- VLAN，即虚拟局域网（Virtual LAN），它也是一种局域网（LAN）。

- 网桥/交换机分割广播域
  - 通过将网络分割成多个冲突域提供增强的网络服务，然而网桥/交换机仍是一个广播域，一个广播数据包可被网桥/交换机转发至全网。虽然OSI模型的第三层的路由器提供了广播域分段，但交换机也提供了一种称为VLAN的广播域分段方法。
- 一个VLAN＝一个广播域＝逻辑网段
- VLAN的优点：
  - 安全性。一个VLAN里的广播帧不会扩散到其他VLAN中。
  - 网络分段。将物理网段按需要划分成几个逻辑网段
  - 灵活性。可将交换端口和连接用户逻辑的分成利益团体，例如以同一部门的工作人员，项目小组等多种用户组来分段。
- VLAN如何操作：
  - 配置在交换机上的每一个VLAN都能执行地址学习、转发/过滤和消除回路机制，就像一个独立的物理网桥一样。VLAN可能包括几个端口
  - 交换机通过将数据转发到与发起端口同一VLAN的目的端口实现VLAN。
  - 通常一个端口只运载它所属VLAN的通信量。

VLAN的产生原因—广播风暴



通过路由器将网络分段

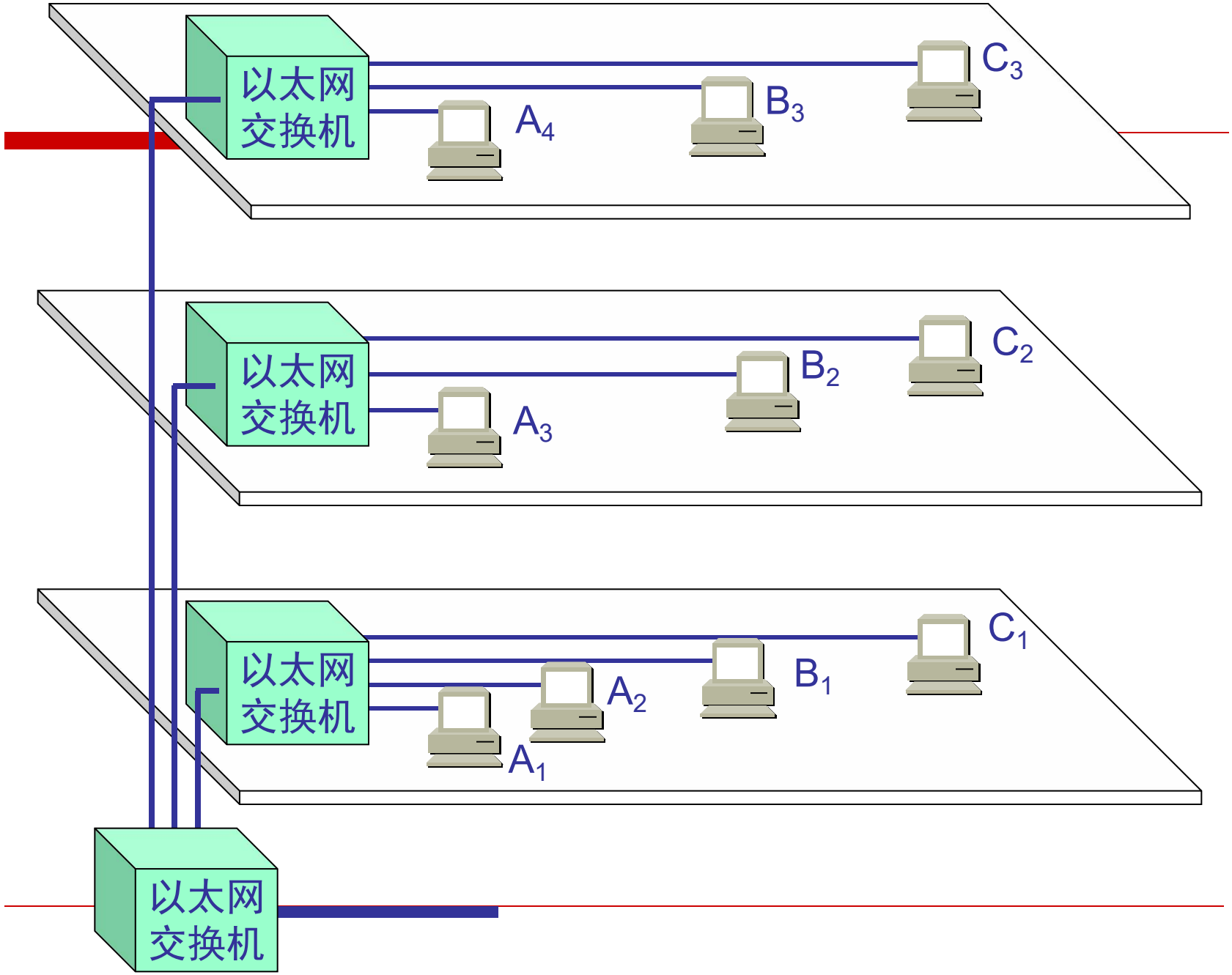


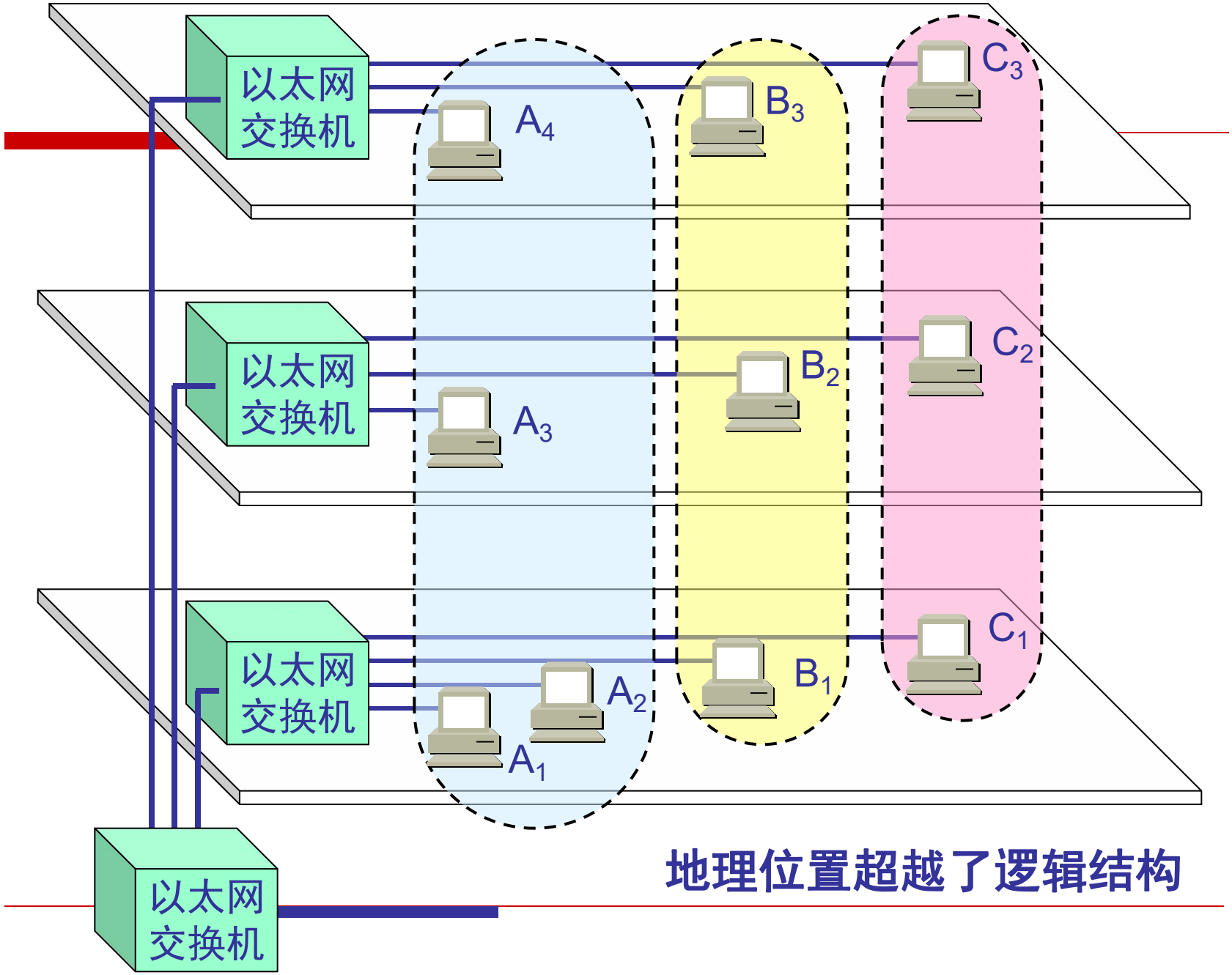
与普通的局域网不同的是：

- （1）VLAN中的工作站一般属于不同的LAN或LAN网段。
- （2）先有LAN，后有VLAN。换句话说，VLAN是建立在LAN之上的。VLAN是通过将LAN中的工作站按一定的方法划分到逻辑组中而形成的。VLAN的形成并没有改变原有网络的拓扑，在用户看来，网络的视图是一致的。

VLAN 主要解决以下2个方面的问题：

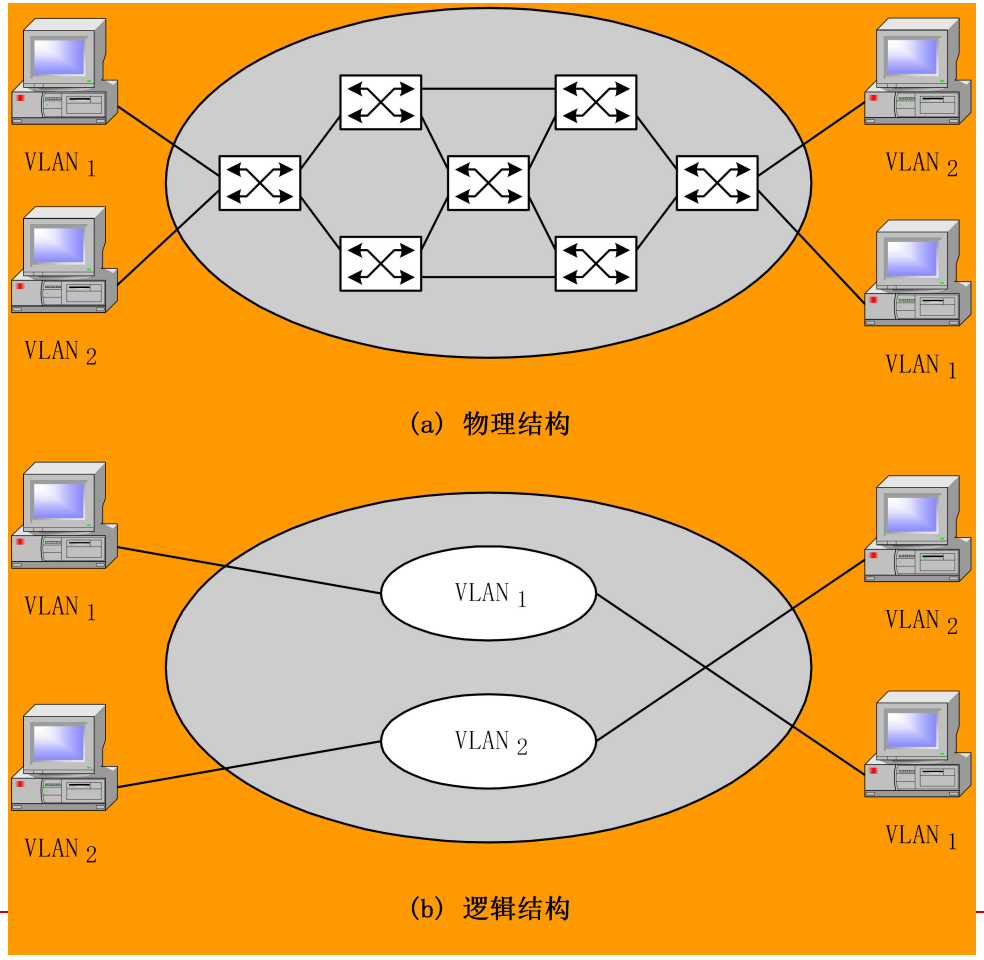
- （1）保持网络的广播通信方式，将对路由器的依赖减少到最小程度。
- （2）减少网络移动和变化的成本。


以太网
交换机
A_4
B_3
C_3
以太网
交换机
A_3
B_2
C_2
以太网
交换机
A_2
A_1
B_1
C_1
以太网
交换机



地理位置超越了逻辑结构

虚拟的网络


VLAN 1
VLAN 2
VLAN 2
VLAN 1
(a) 物理结构
VLAN 1
VLAN 2
VLAN 1
VLAN 2
VLAN 2
VLAN 1
(b) 逻辑结构

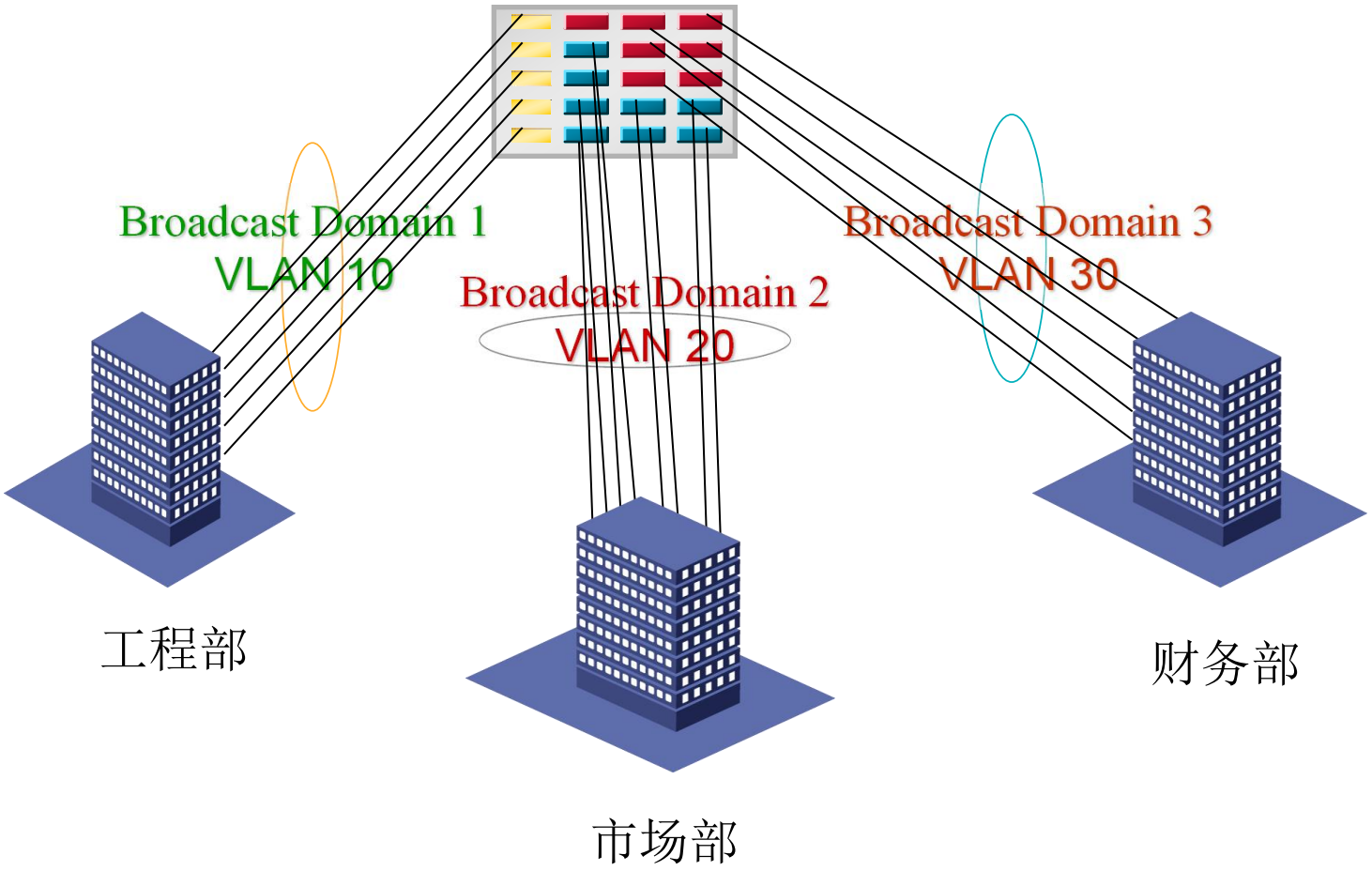
为什么需要VLAN

- 主要因为以下2个原因：
  （1）　　需求驱动。
  （2）　　技术驱动。

1　需求驱动

- VLAN的引入首先是由于用户需求的驱动。
- 需要有一种办法，在尽量不改动网络固有配置的前提下，通过灵活的、标准的、基于软件的做法将具有相同需求的用户放到一起，使之就象在一个LAN中那样工作。

通过VLAN划分广播域



2 技术驱动

- 但是怎样使网络延伸扩展呢？这就需要技术支持，需要更高级的技术，它不但能够在物理上使网络延伸，还能使对网络实施更灵活强大的控制功能成为可能。使VLAN成为可能的技术包括：
  - （1）LAN交换技术
  - （2）生成树算法（IEEE802.1D）
  - （3）过滤服务（IEEE802.1p）
  - （4）帧标签技术（IEEE802.1Q）
  - （5）LAN安全标准（IEEE802.1O）

3.2.3 VLAN的种类

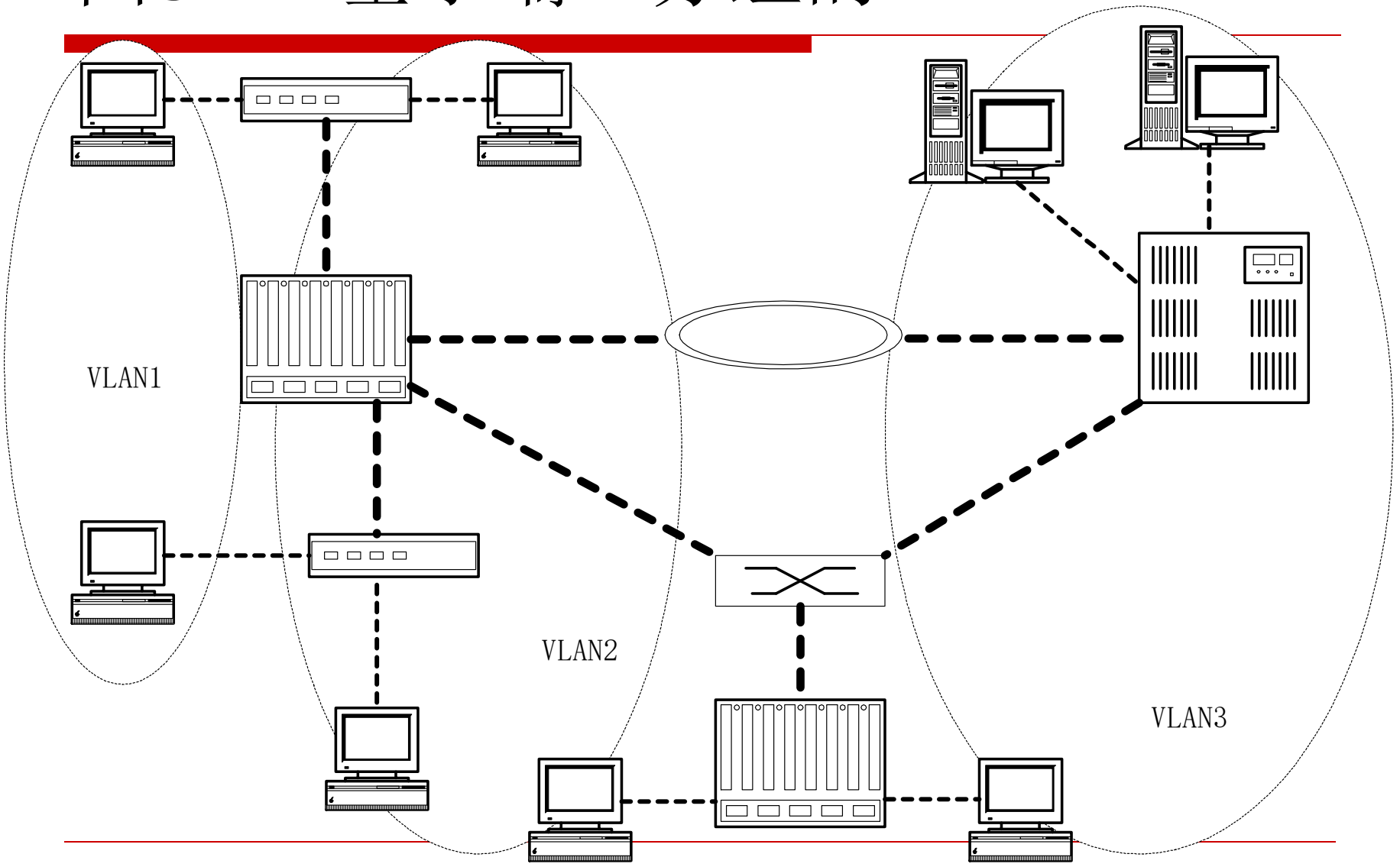
- 从简到繁依次是：
  （1）基于端口的VLAN (Port-Based)
  （2）基于协议的VLAN (Protocol-Based)
  （3）基于MAC层分组的VLAN (MAC-Layer Grouping)
  （4）基于网络层分组的VLAN (Network-Layer Grouping)
  （5）基于IP组播分组的VLAN (IP Multicast Grouping)
  （6）组合的VLAN
  （7）基于策略的VLAN (Policy-Based)

1 基于端口分组的VLAN

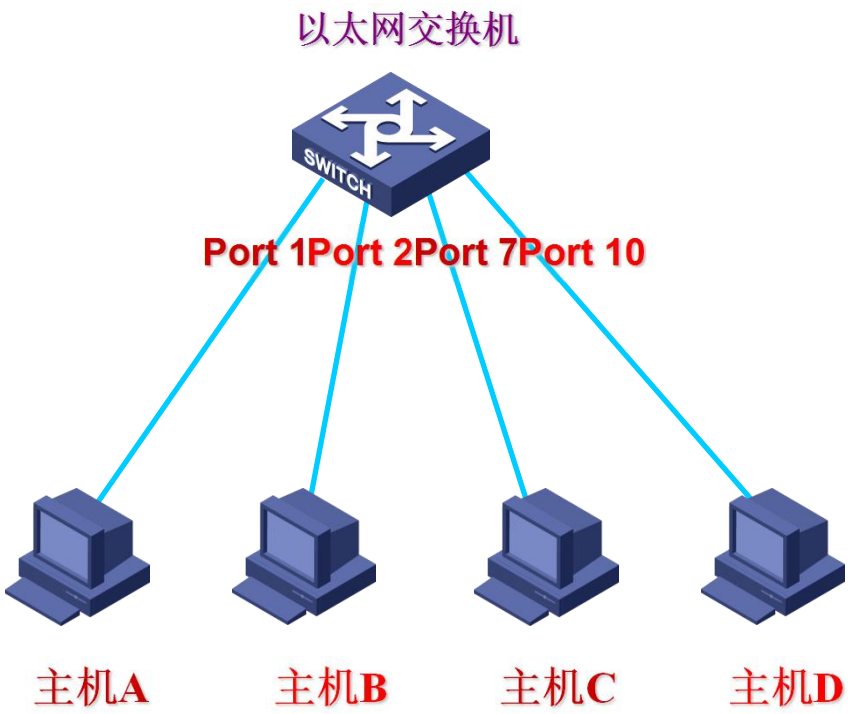
- 按端口分组是早期定义VLAN成员关系的方法。在这种定义方法中，某个交换机上的端口（例如端口1、3、5）构成VLANA，而该交换机上的其他端口构成VLANB。早期基于端口的VLAN成员只能位于一个交换机中。第二代基于端口的VLAN支持多个交换机，例如交换机X上的端口1和端口2与交换机Y上的端口3和端口4构成一个VLAN。

  基于端口VLAN的示意图

图3-1 基于端口分组的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

VLAN成员之间信息通信

- 第2层VLAN成员间的通信
  我们知道第2层LAN成员之间的通信是根据帧中MAC地址寻址的，第2层VLAN成员之间的通信还要使用新增加的VLAN标签中的VLAN标识符（VLAN ID）进行寻址。
  VLAN标签的标准是IEEE802.1Q，我们在3.2.6节介绍。

第2层VLAN寻址包括2个步骤：

- （1）先根据VLAN ID找到目的VLAN。
  （2）再根据MAC地址找到目的主机。

举例

- （1）假设aaa向ddd发送数据。aaa的数据帧Faaa通过端口1被交换机S1接收，S1发现Faaa的目的地址是ddd，S1通过查阅VLAN成员关系数据库（如表3-2所示）得知ddd属于VLAN B，并且ddd位于S2。
  （2）于是S1给Faaa加上VLAN A的标识符（Faaa记为Faaa'）。Faaa'经S1与S2之间的链路发送到S2。S2接收到Faaa'后，通过检查VLAN ID知道此帧来自VLAN A，目的地址是ddd。S2查表5-2（S2中也有该表）判断ddd所属的VALN，发现ddd属于VALN B。
  （3）如果S2允许VALN A到VLAN B的转发（符合过滤规则，由802.1p标准化），则查表3-3确定ddd所在的端口（4），然后将Faaa'去掉标签，通过端口4交给ddd。
- 如图3-6所示

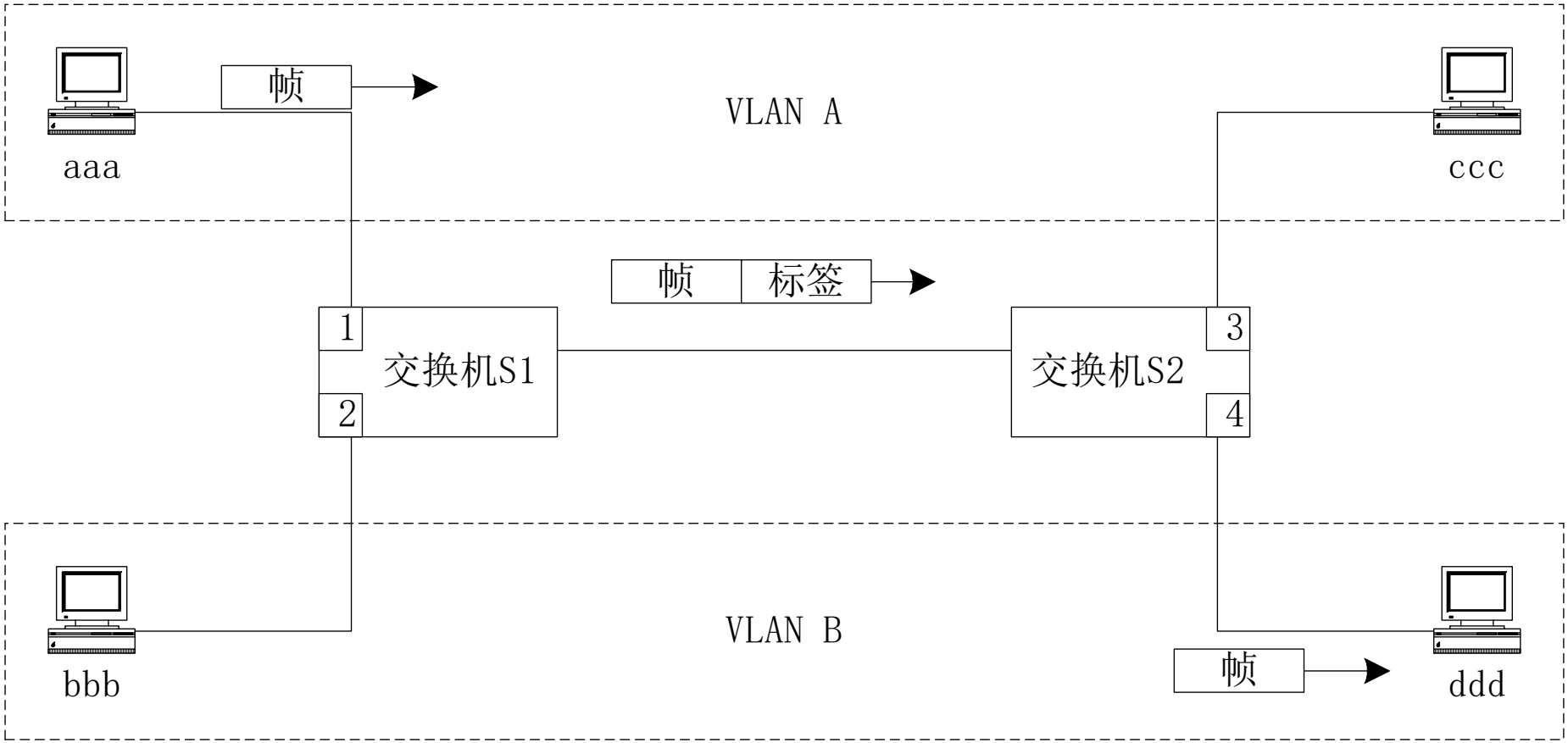
表3-2 VLAN成员关系

MAC地址	VALN ID
Aaa	A
Bbb	B
Ccc	A
Ddd	B

表3-3 S2的交换表

MAC地址	端口ID
ccc	3
ddd	4

图3-6第2层VLAN成员通信



3.2.5 VLAN标准

- （1）IEEE：其制定的标准是IEEE802.1O和802.1Q。
- （2）ATM论坛：其制定的标准是LANE标准。
- （3）IETF：其工作是在IEEE802.1D和802.1p基础上增强过滤控制功能。
- 除了上述标准外，VLAN还涉及以下标准：
  - （1）管理标准：包括简单网络管理协义SNMP和远程监控RMON。该类协议解决交换式网络、ATM网络中通信量管理等问题。
  - （2）安全标准：包括ISAKMP协议、Oakley KDP协议、RADIUS协议。安全标准解决数据完整性、审计、事件监控、报警、计帐等问题。

1 IEEE802.1D

- IEEE802.1D标准通常被称为生成树（spanning tree）标准。生成树算法用于消除网络拓扑中的环路（Loop）。当网络中主机之间存在替代路由时，环路就会出现。环路会导致通信量增加，使网络性能下降。为了深入理解IEEE802.1D，必须了解生成树算法。下面我们介绍生成树算法。

生成树算法

- 生成树算法使用5个参数值来驱动生成树拓扑。它们是：

  （1）组播地址：指明扩展网络中的所有网桥。该参数值与LAN类型有关，由软件自动确定。

  （2）扩展网络中每个网络的唯一的标识符。

  （3）桥/LAN接口端口的唯一标识符。

  （4）端口优先级。

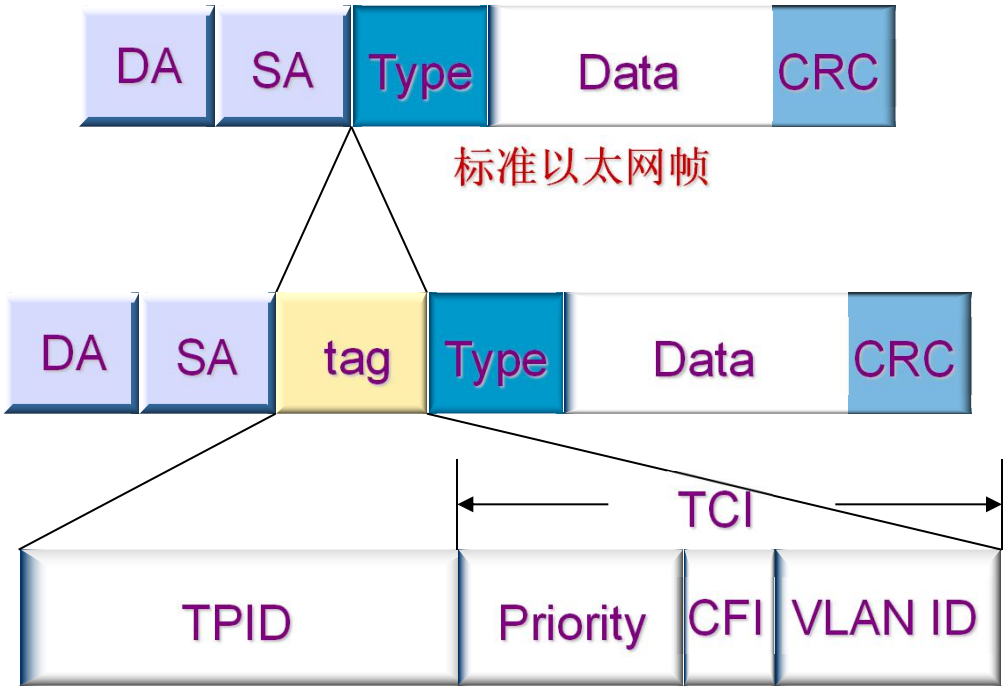
  （5）端口的成本。

  其中后4个参数值由人工分配。

3 IEEE802.1Q

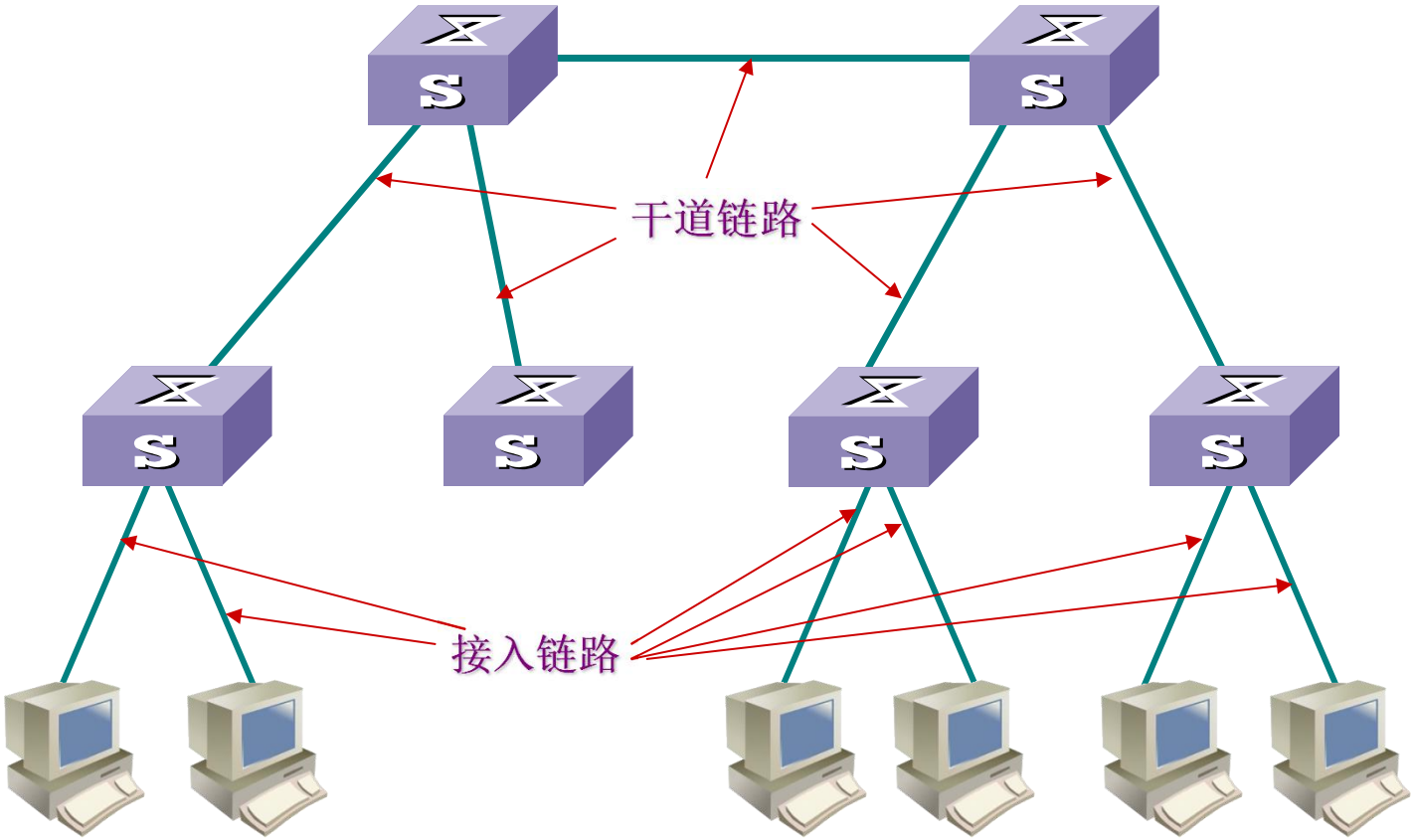
- 1996年3月，IEEE802.1网络互联分会完成了制定VLAN标准的初始阶段的调查工作，并通过了标准方案，该方案包括了3个方面的内容：
  - （1）VLAN的结构化方法。
  - （2）在多个VLAN和多供应商设备环境中支持VLAN成员关系信息通信的帧标签的标准格式。
  - （3）VLAN标准化的未来方向

VLAN的帧格式



TPID = 0x8100

Access Link和Trunk Link



端口对接收报文的处理

收报文：

Acess端口： 1、收到一个报文

2、判断是否有VLAN信息：如果没有则转到第3步，否则转到第4步

3、打上端口的PVID，并进行交换转发

4、直接丢弃（缺省）

trunk端口： 1、收到一个报文

2、判断是否有VLAN信息：如果没有则转到第3步，否则转到第4步

3、打上端口的PVID，并进行交换转发

4、判断该trunk端口是否允许该VLAN的数据进入：如果可以则转发，否则丢弃

hybrid端口： 1、收到一个报文

2、判断是否有VLAN信息：如果没有则转到第3步，否则转到第4步

3、打上端口的PVID，并进行交换转发

4、判断该hybrid端口是否允许该VLAN的数据进入：如果可以则转发，否则丢弃

端口对发送报文的处理

发报文：

Acess端口： 1、将报文的VLAN信息剥离，直接发送出去

trunk端口： 1、比较端口的PVID和将要发送报文的VLAN信息

2、如果两者相等则转到第3步，否则转到第4步

3、剥离VLAN信息，再发送

4、直接发送

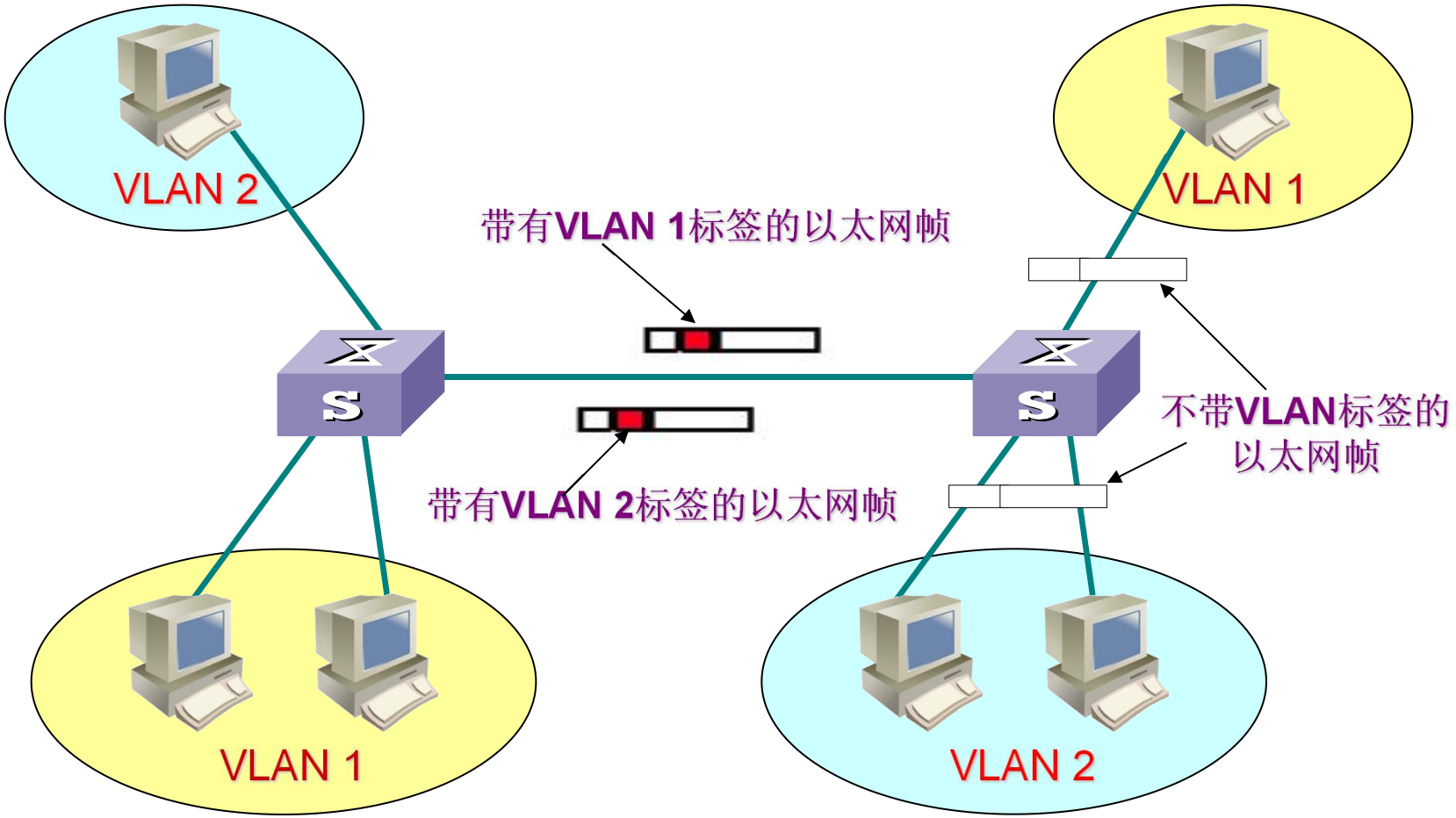
hybrid端口：1、判断该VLAN在本端口的属性（disp interface 即可看到该端口对哪些VLAN是untag，哪些VLAN是tag）

2、如果是untag则转到第3步，如果是tag则转到第4步

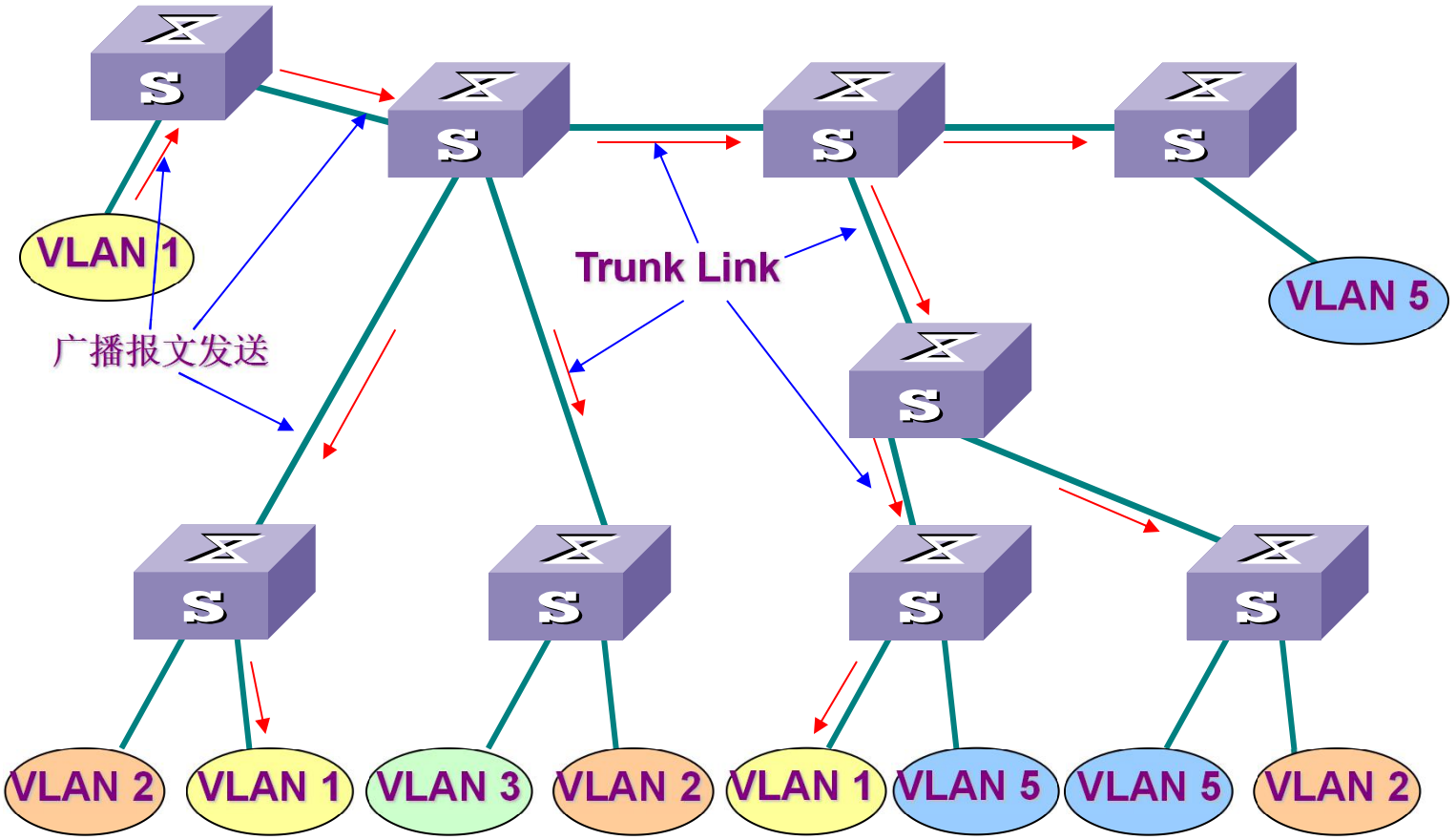
3、剥离VLAN信息，再发送

4、直接发送

帧在网络通信中的变化

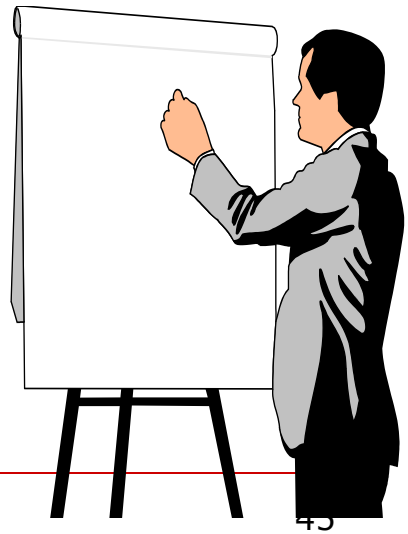

VLAN 2
VLAN 1
带有VLAN 1标签的以太网帧
S
S
不带VLAN标签的
以太网帧
带有VLAN 2标签的以太网帧
VLAN 1
VLAN 2

Trunk link和VLAN



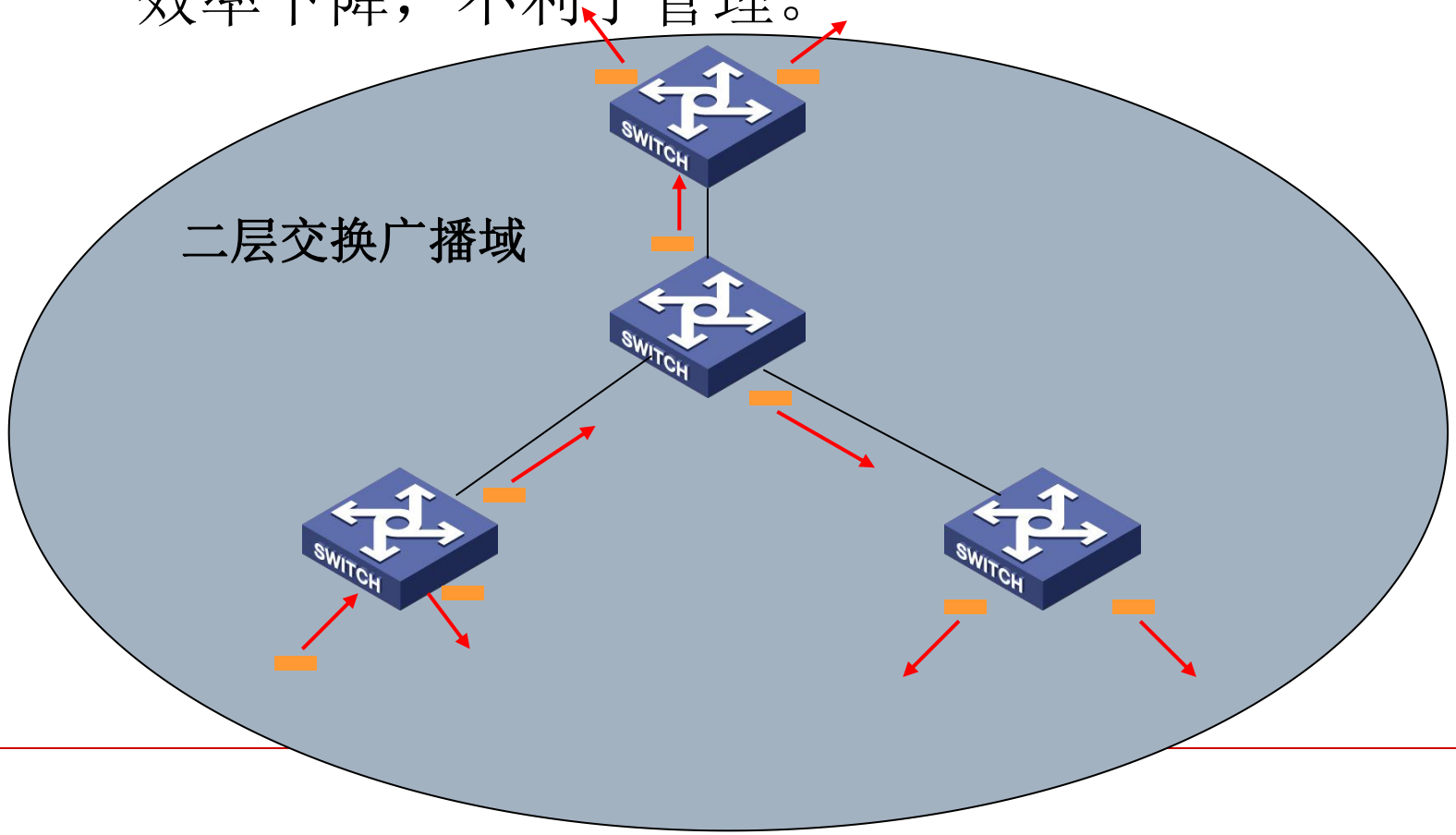
VLAN间路由

- VLAN间路由产生的问题
  - 隔离的广播域
  - 查找路由
  - 承载多个VLAN的流量
- 分布层拓扑结构
- 配置VLAN间路由

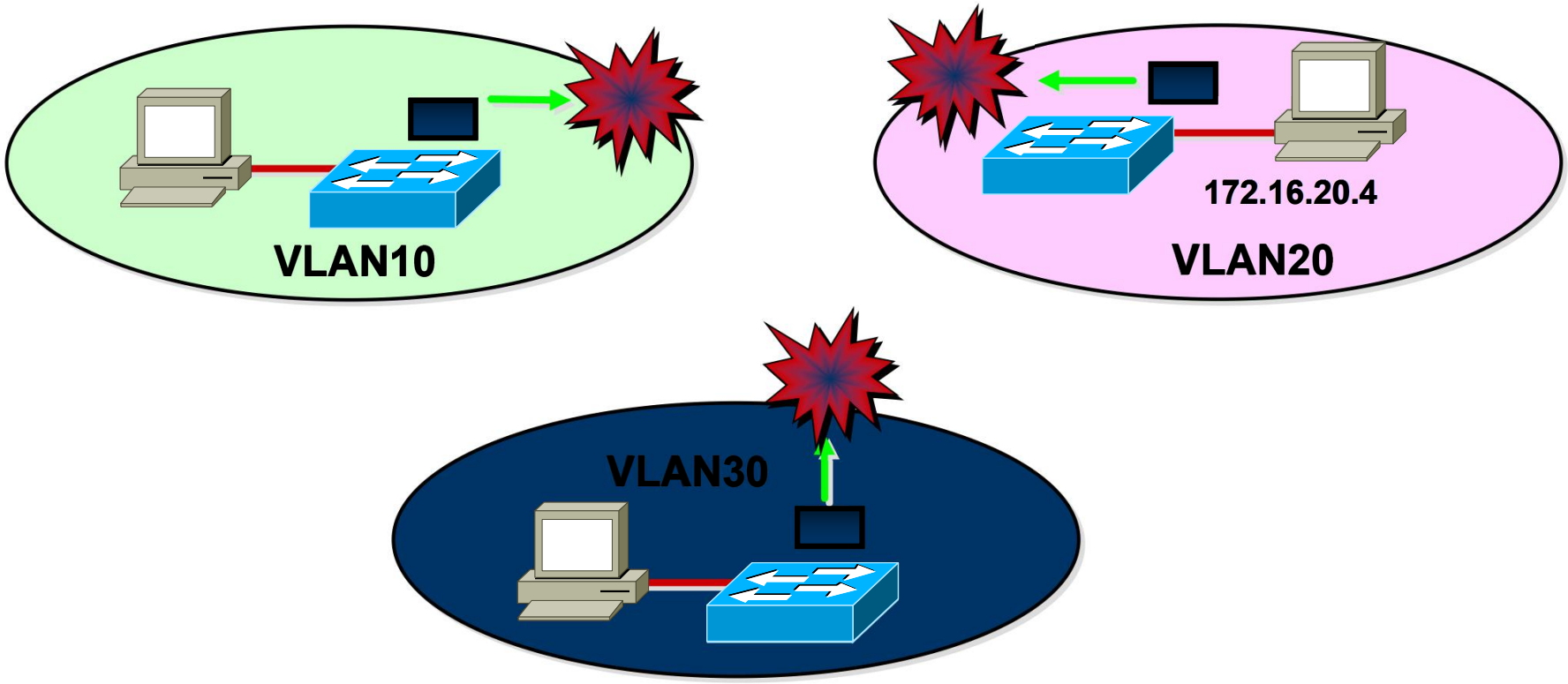


二层交换网络——广播网络

- 传统的二层交换网络，整个网络就是一个广播域，当网络规模增大的时候，网络广播严重，效率下降，不利于管理。

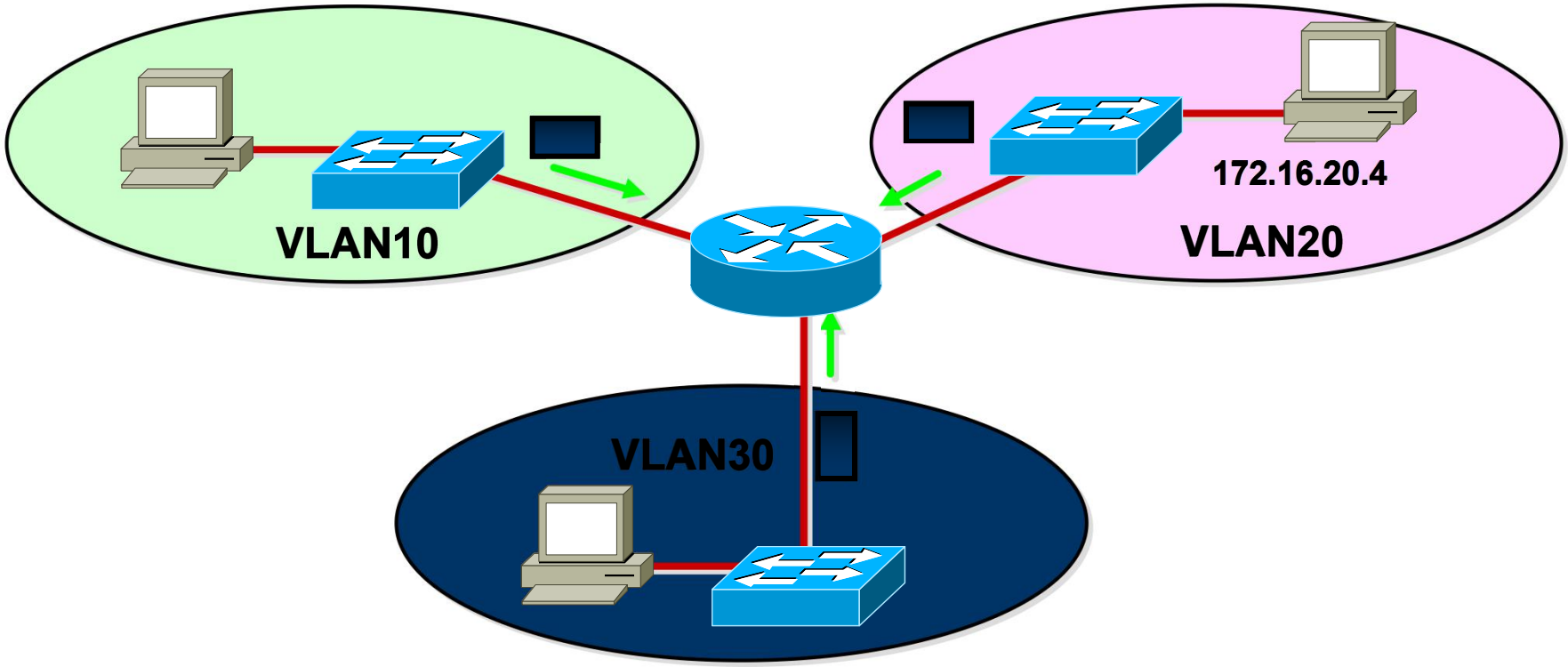


问题：隔离的广播域



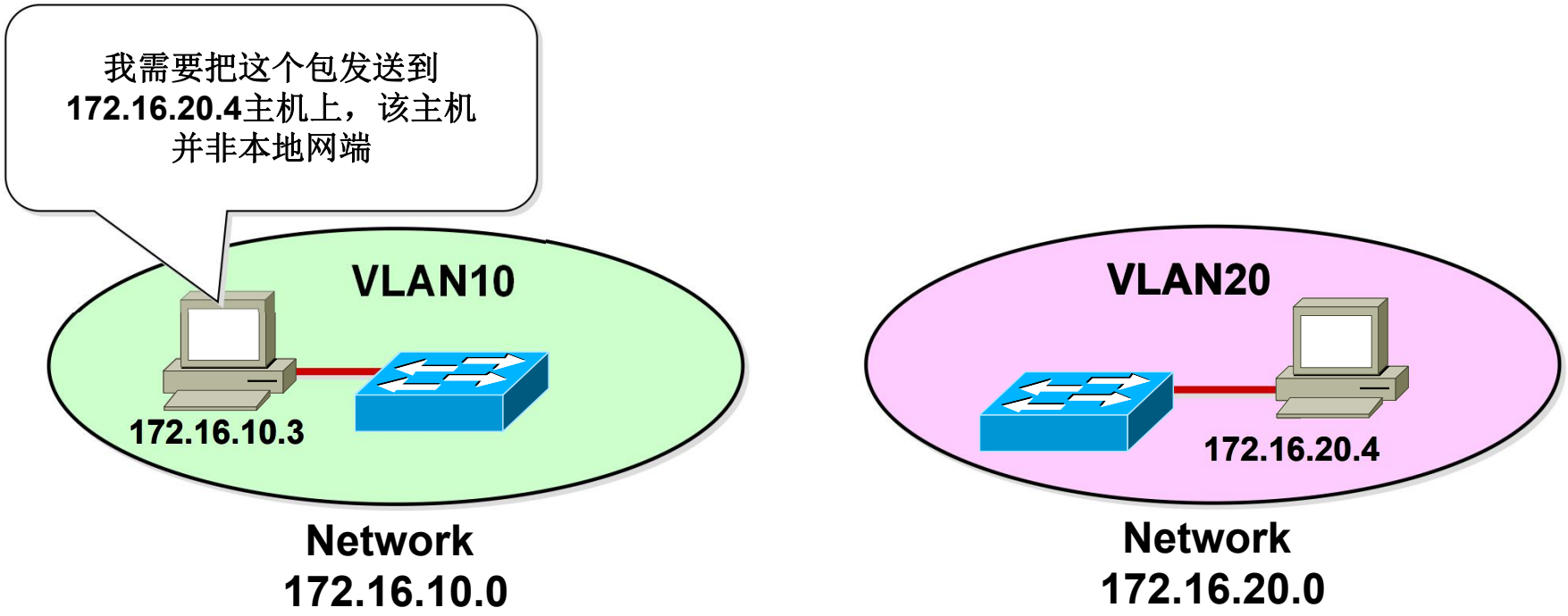
- 因为**VLAN**是设计用来控制广播域大小并将本地数据流保持在本地，所以**VLAN**之间通讯是受限制的

解决方案：在VLAN之间使用路由器



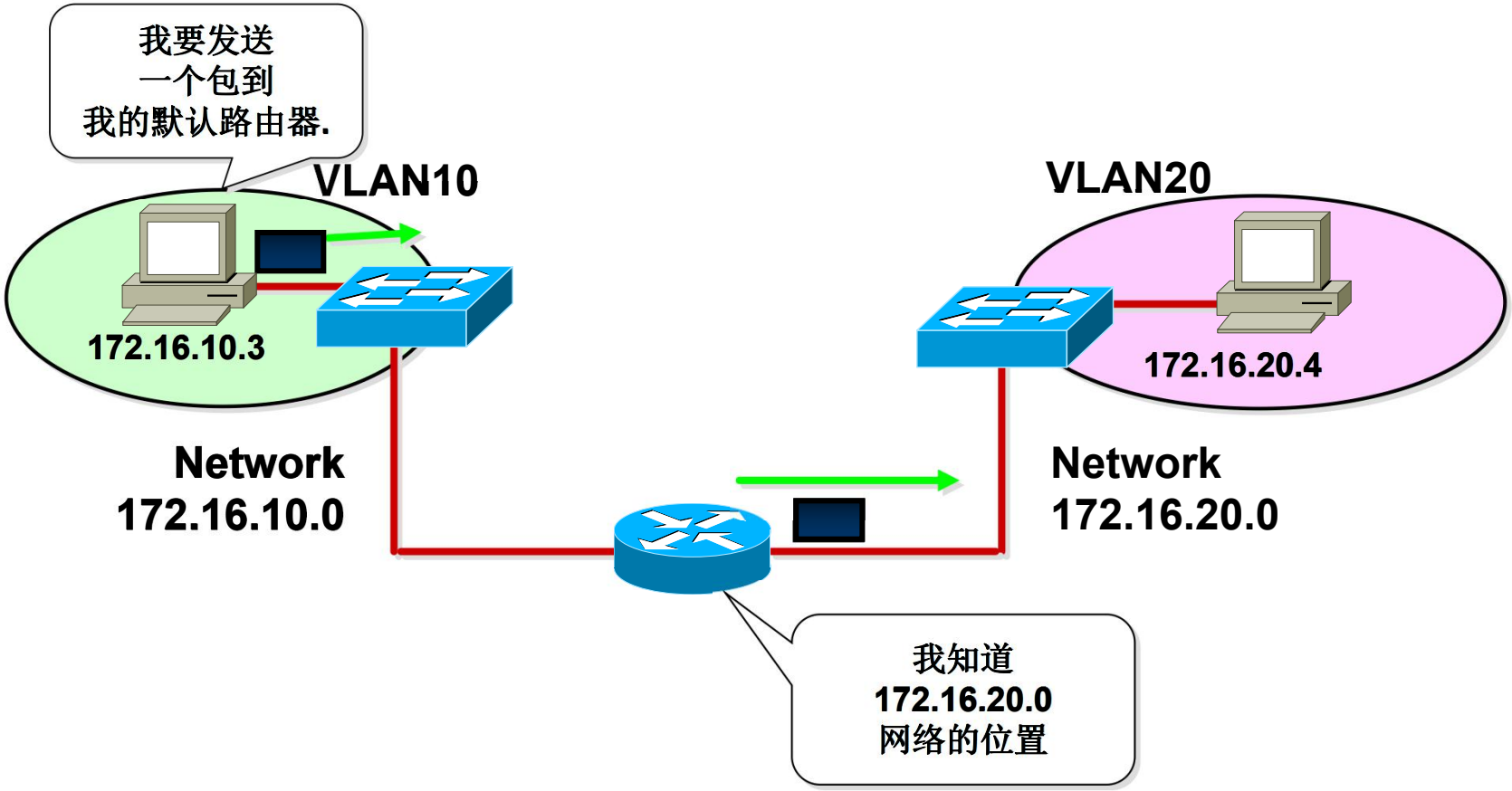
- VLAN之间的通讯需要路由器的处理

问题：查找路由



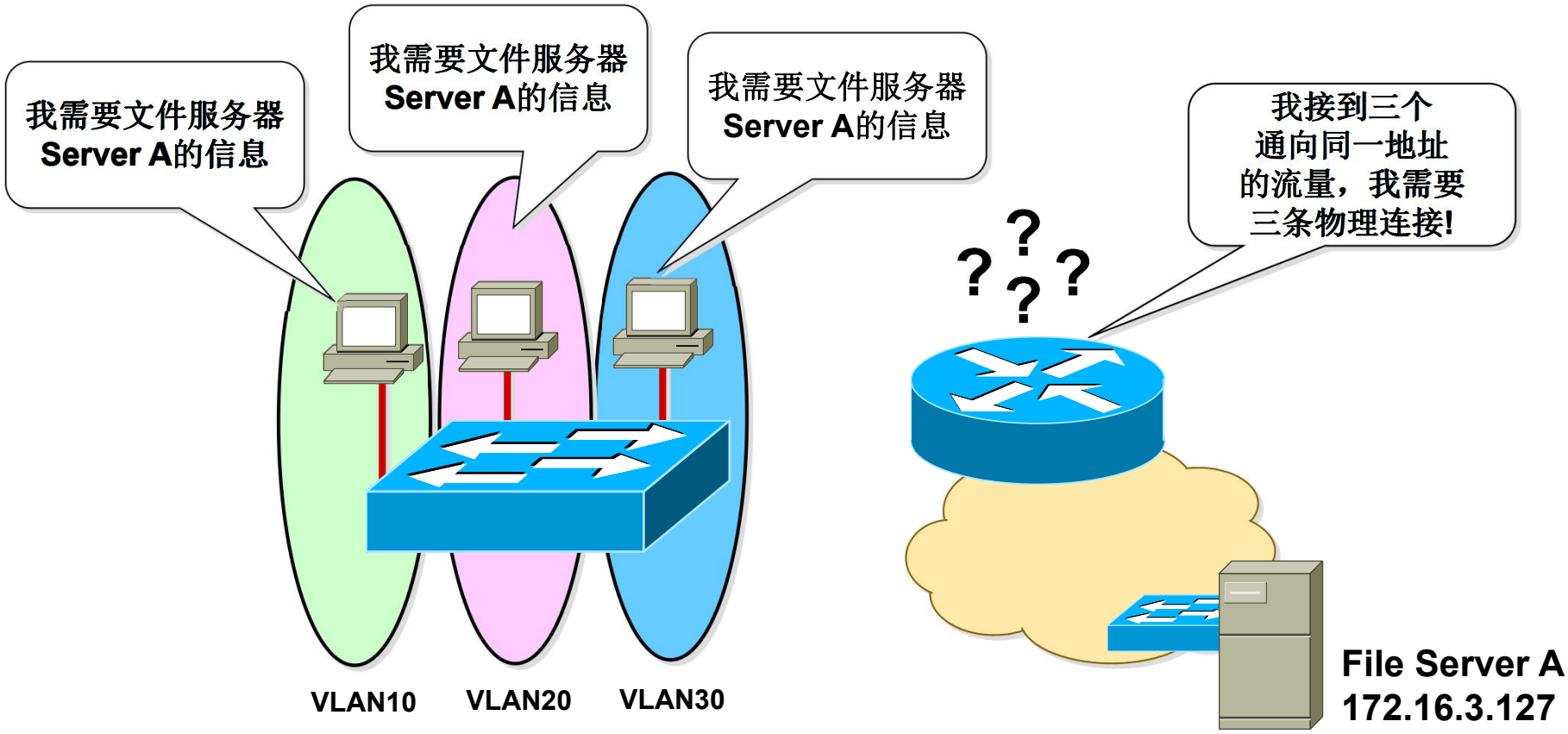
- VLAN之间通讯就引出了终端设备如何能够通过多个局域网段或其他设备进行通讯的问题

解决方案：指定缺省网关



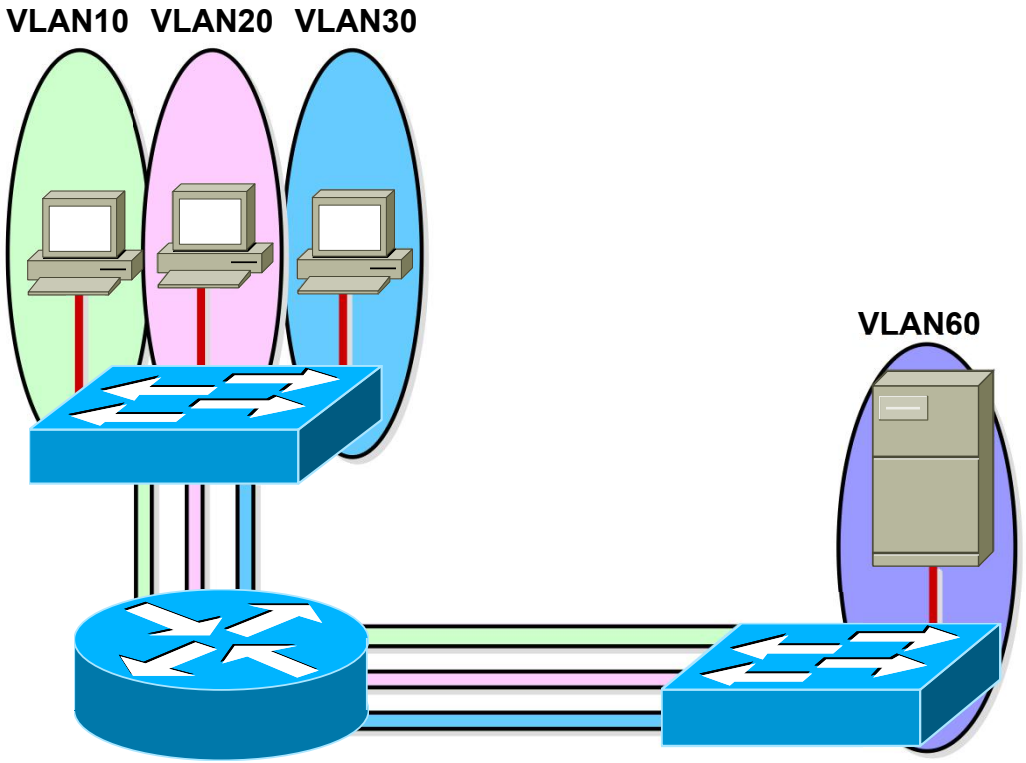
- 终端用户将目标网络为非本地的数据包发送到自己的缺省网关

问题：支持多VLAN数据流



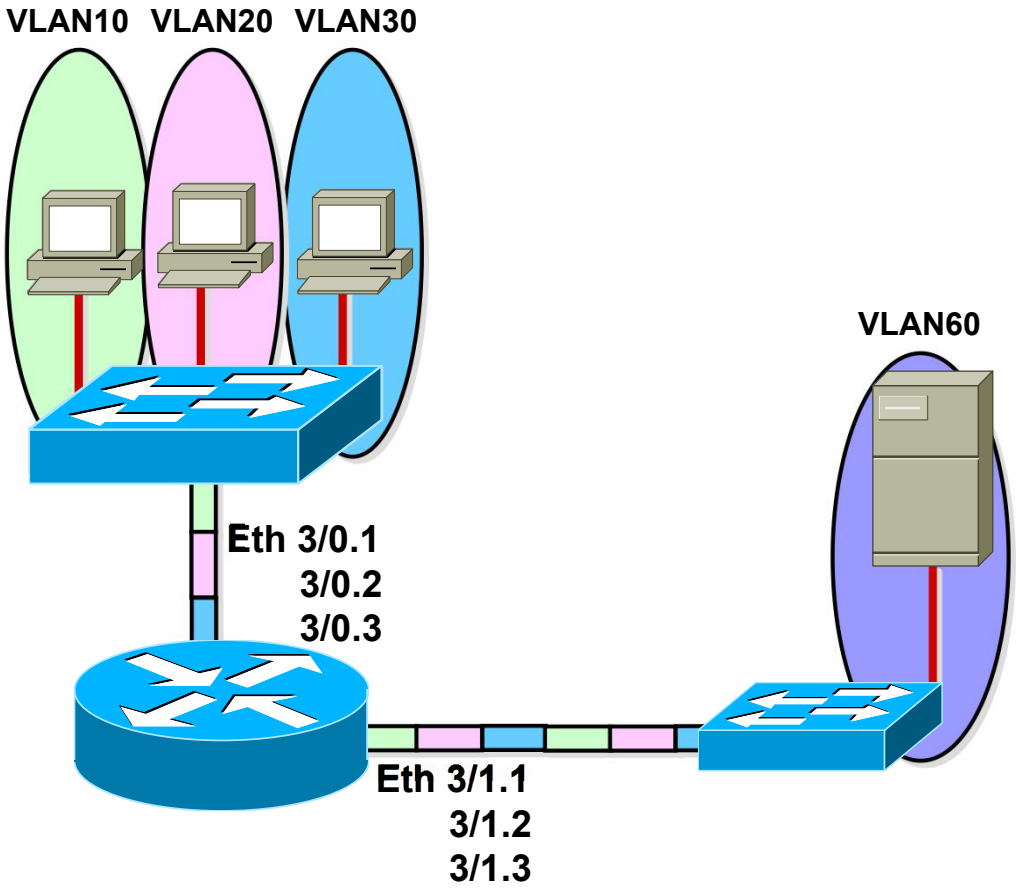
- 多个**VLAN**共用一台外部路由器，就需要到交换机有多条物理连接

解决方案：多链路



- 交换机可以支持为每个**VLAN**提供一个单独的接口

解决方案：一条链路传送多个VLAN的数据流

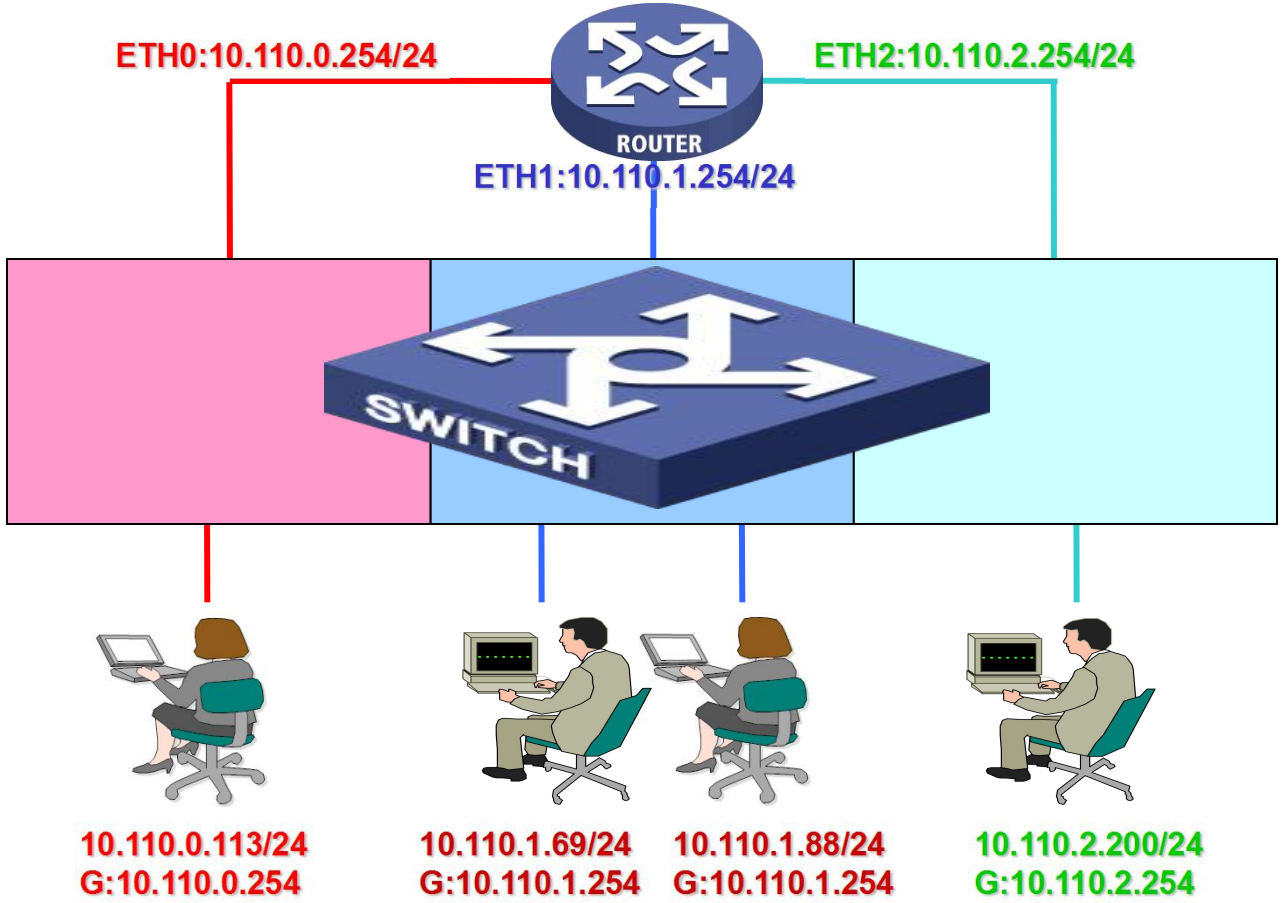


路由器支持为多个VLAN提供一条ISL链路

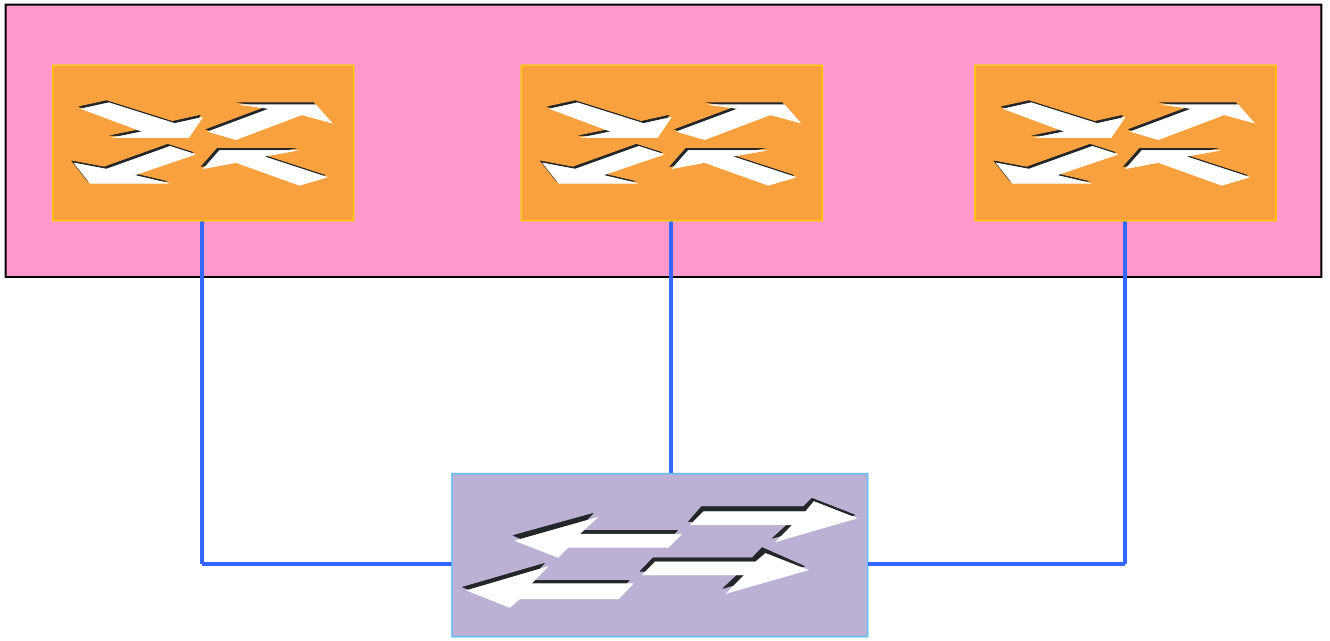
二层交换机工作原理

- 工作方式
  - 交换机根据收到数据帧中的源MAC地址建立该地址同交换机端口的映射，并将其写入MAC地址表中。
  - 交换机将数据帧中的目的MAC地址同已建立的MAC地址表进行比较，以决定由哪个端口进行转发。
  - 如数据帧中的目的MAC地址不在MAC地址表中，则向所有端口转发。这一过程称之为泛洪（flood）。
  - 广播帧和组播帧向所有的端口转发。
- 交换机的三个主要功能：
  - 学习：以太网交换机了解每一端口相连设备的MAC地址，并将地址同相应的端口映射起来存放在交换机缓存中的MAC地址表中。
  - 转发/过滤：当一个数据帧的目的地址在MAC地址表中有映射时，它被转发到连接目的节点的端口而不是所有端口（如该数据帧为广播/组播帧则转发至所有端口）。
  - 消除回路：当交换机包括一个冗余回路时，以太网交换机通过生成树协议避免回路的产生，同时允许存在后备路径。

三层交换机功能模型

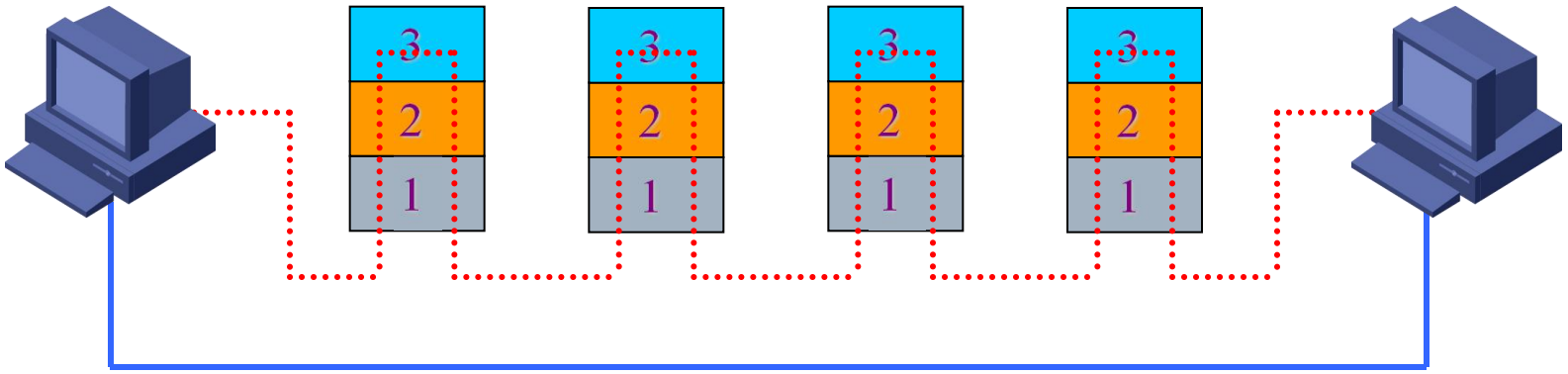

ETH0:10.110.0.254/24
ETH2:10.110.2.254/24
ROUTER
ETH1:10.110.1.254/24
SWITCH
10.110.0.113/24
G:10.110.0.254
10.110.1.69/24
G:10.110.1.254
10.110.1.88/24
G:10.110.1.254
10.110.2.200/24
G:10.110.2.254

三层交换机的路由和二层交换



- 二层交换引擎：实现同一网段内的快速二层转发
- 三层路由引擎：实现跨网段的三层路由转发

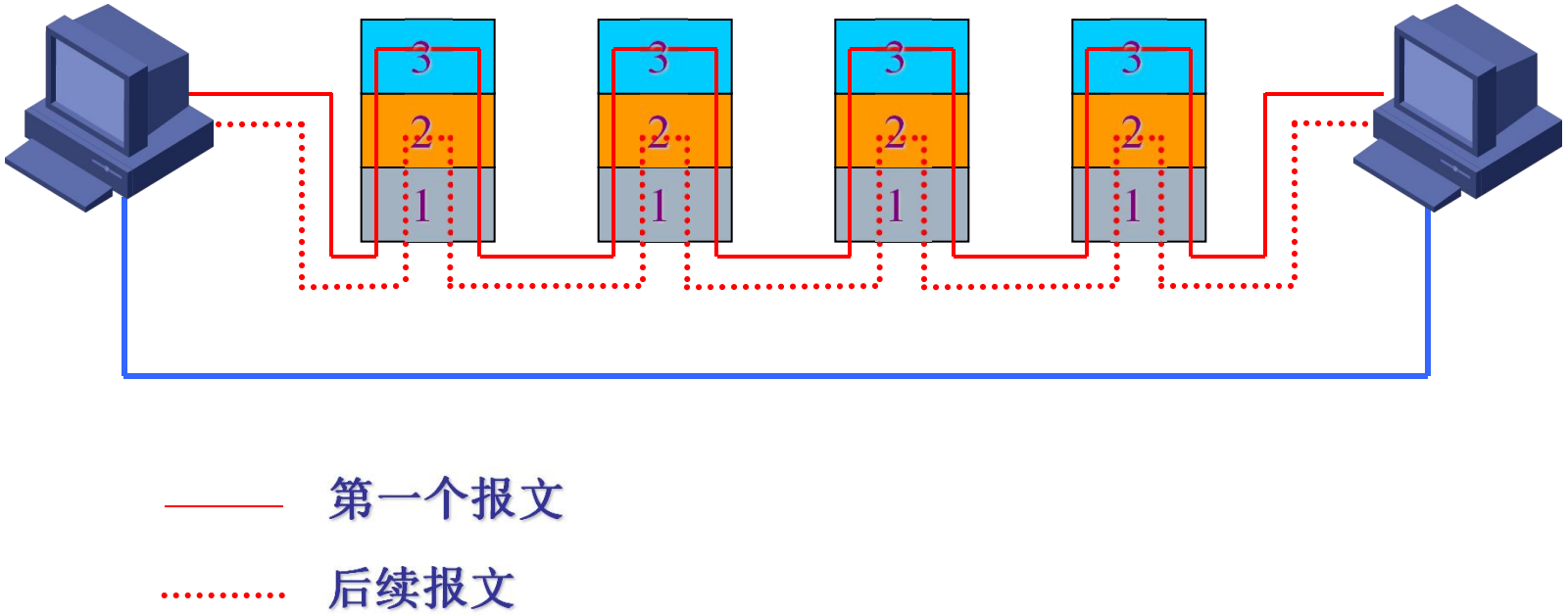
传统的三层路由技术



- 传统三层路由技术对每个报文进行处理，并基于第三层地址信息转发报文。这一方法称为逐包转发。

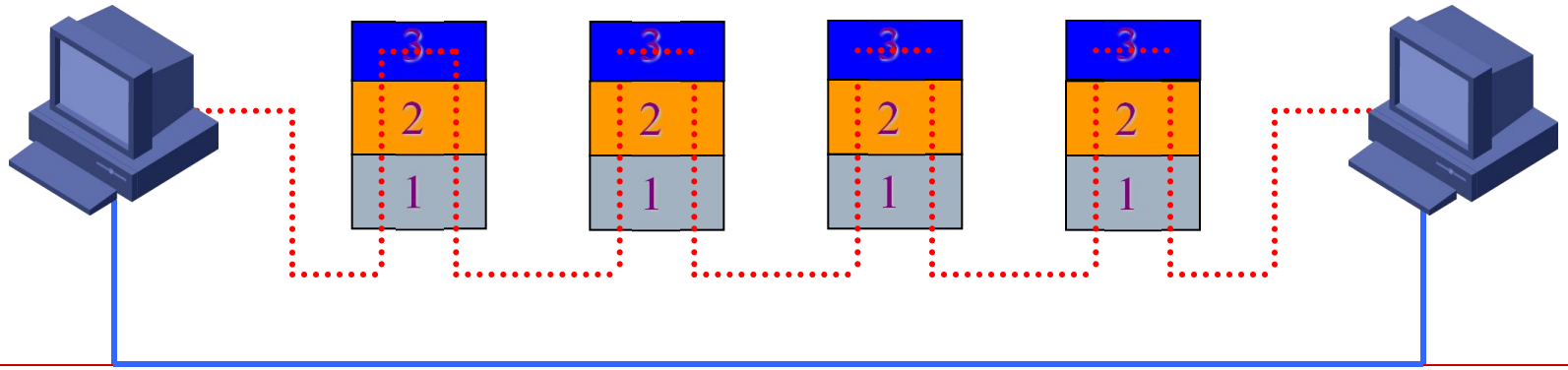
基于流的三层交换技术

- 根据数据流的首报文转发建立新的快速转发路径，同一数据流的后续报文按照此转发路径进行转发的方法称之为流交换（FS）。

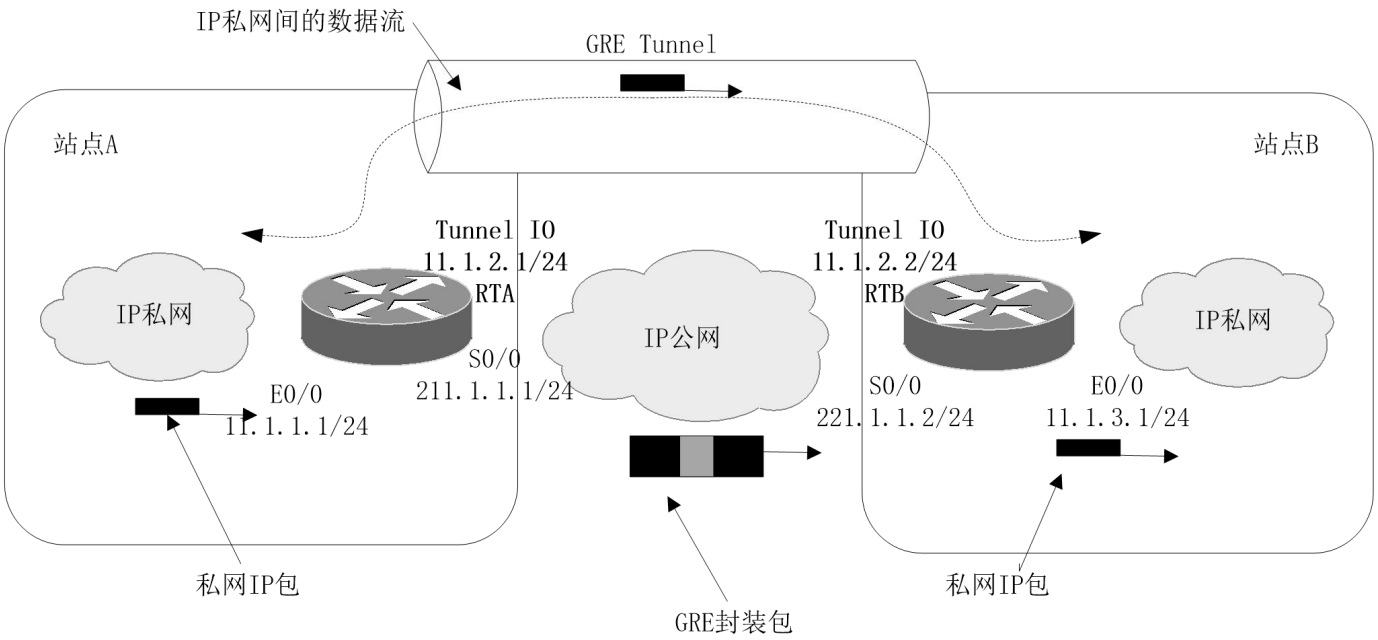


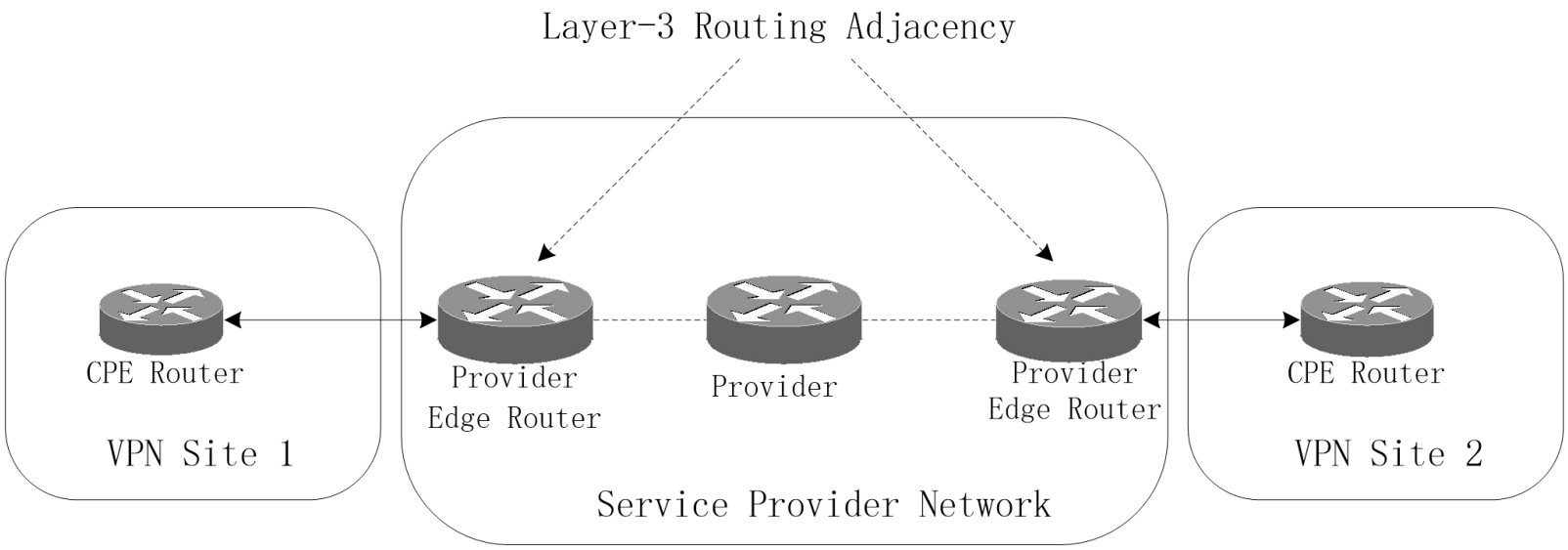
最长匹配的三层交换技术

- 传统的三层路由技术通过软件查找路由表进行逐包转发。
- 流交换通过硬件完成后续报文的快速转发，这个转发过程称为精确匹配，而且首报文转发仍然采用软件查找路由表实现转发。
- 最长匹配的三层交换技术，所有报文的转发都通过硬件的快速匹配完成转发。

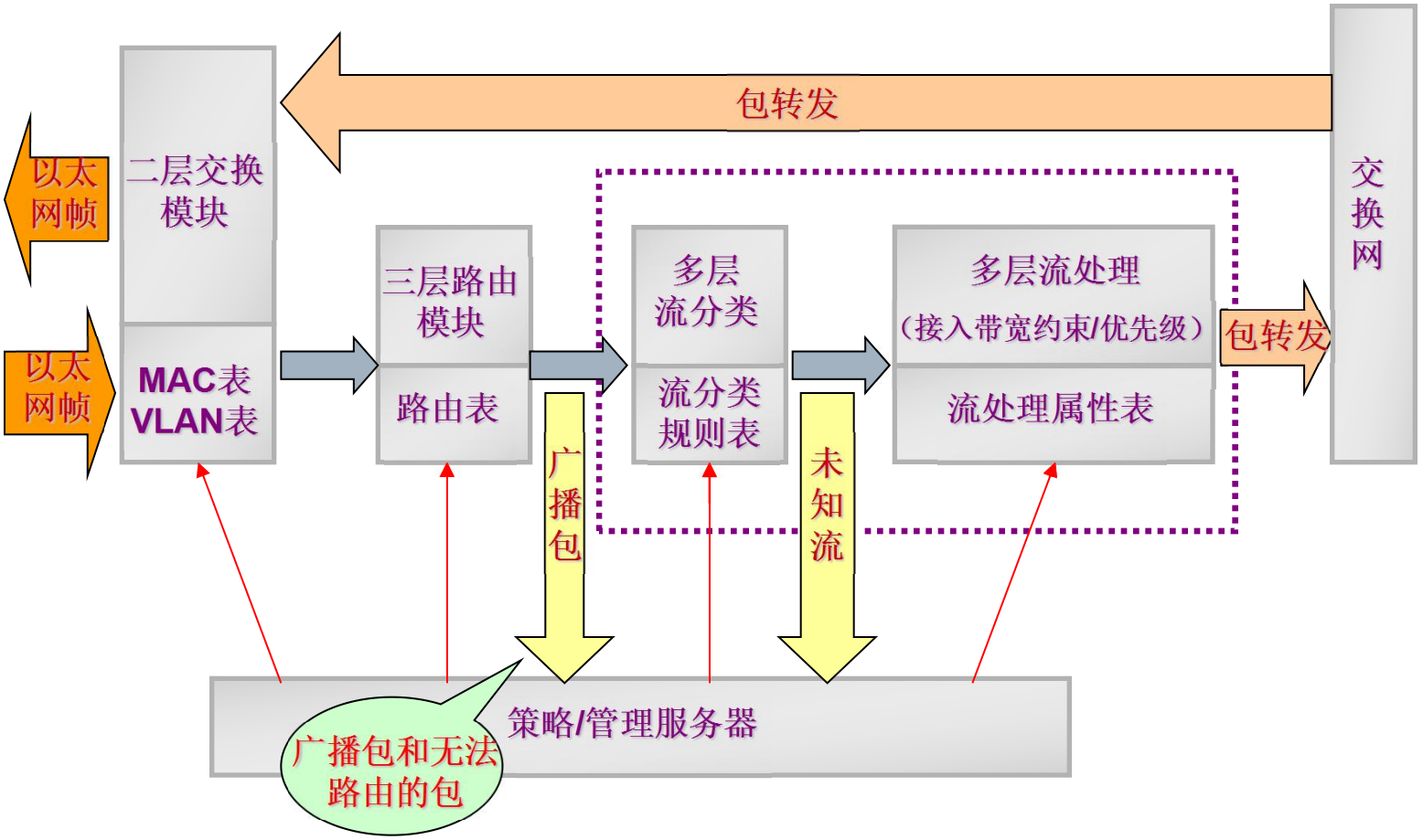


- 三层交换机并非简单地把路由设备的硬件和软件添加到普通的交换机上
  - 三层交换机和路由器的主要功能不同：前者的主要功能是数据交换，后者的主要功能是路由转发（两者同时具备了数据交换和路由转发功能）
  - 三层交换机和路由器的使用场所不同：前者主要用于简单的局域网连接，提供快速数据交换的功能；后者不仅适用于同种协议的局域网间，还适用于不同协议的局域网和广域网间，其优势在于强大的路由转发功能
  - 三层交换机和路由器处理数据的方式不同：前者通过硬件执行数据包交换，后者由基于微处理器的软件路由引擎执行数据包交换

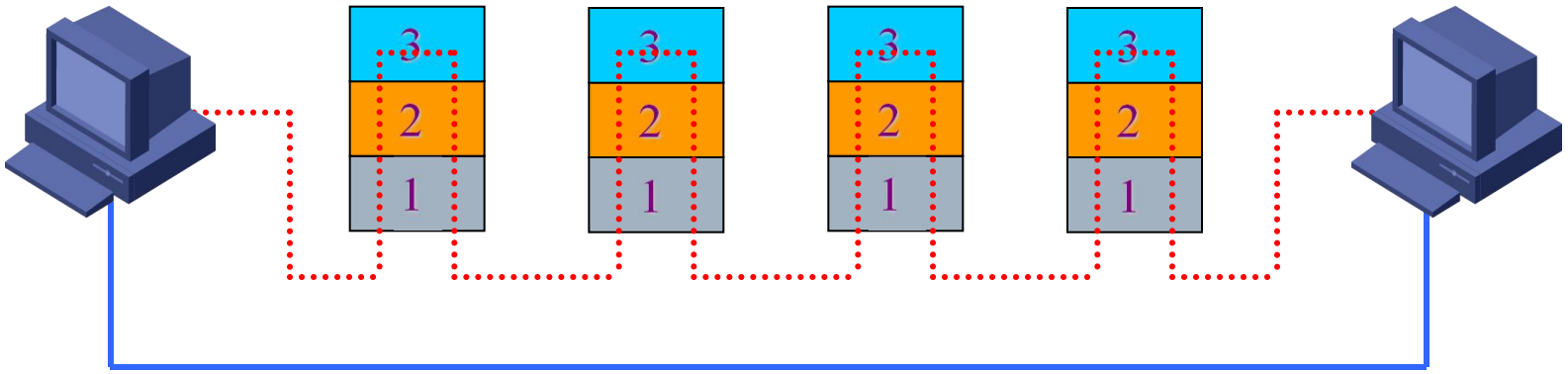

IP私网间的数据流
GRE Tunnel
站点A
站点B
Tunnel IO
11.1.2.1/24
RTA
Tunnel IO
11.1.2.2/24
RTB
IP私网
IP公网
IP私网
S0/0
211.1.1.1/24
S0/0
221.1.1.2/24
E0/0
11.1.1.1/24
E0/0
11.1.3.1/24
私网IP包
GRE封装包
私网IP包


Layer-3 Routing Adjacency
CPE Router
VPN Site 1
Provider
Edge Router
Provider
Provider
Edge Router
Service Provider Network
CPE Router
VPN Site 2

基于流交换的三层交换机的转发流程



传统的三层路由技术



- 传统三层路由技术对每个报文进行处理，并基于第三层地址信息转发报文。这一方法称为逐包转发。