



Chapter 15

连接局域网、主干网和 虚拟局域网

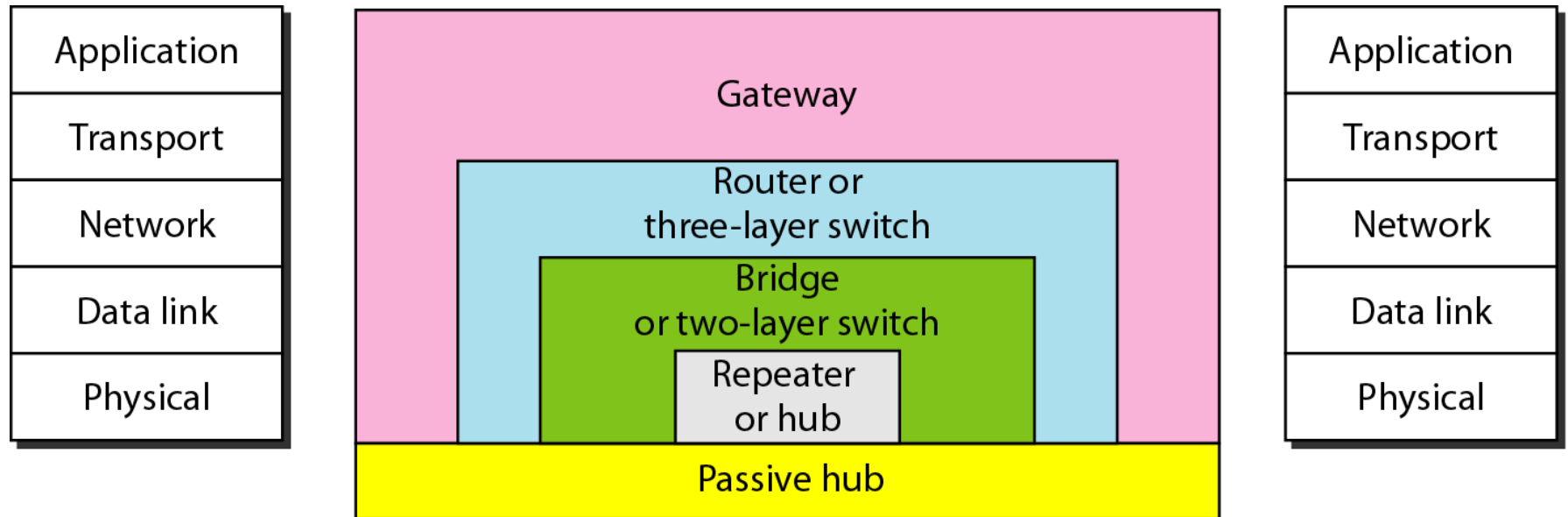
15-1 CONNECTING DEVICES

根据在网络中工作的层可将连接设备分为 5 类

Topics discussed in this section:

- Passive Hubs （无源集线器）
- Active Hubs （有源集线器）
- Bridges （桥）、 Two-Layer Switches （二层交换）
- Routers （路由器）、 Three-Layer Switches （三层交换）
- Gateways （网关）

Figure 15.1 五类连接设备



无源集线器

- 无源集线器只是个连接器，连接来自不同分支的线路。
- 在星型拓扑中，无源集线器只是一个来自不同站点的信号冲突点，集线器是冲突点。
- 无源集线器在物理层以下。

中继器

- 中继器是仅工作在物理层的设备；
- 中继器能够扩展局域网的物理长度；
- 中继器不能连接采用不同协议的两个局域网，它连接的是同一局域网的两个分段；
- 中继器转发每一帧，没有过滤能力；
- 中继器可重新生成原始的位模式，是再生器而不是放大器；
- 常用于星型结构中，可多级连接（级联）。

中继器 Repeater

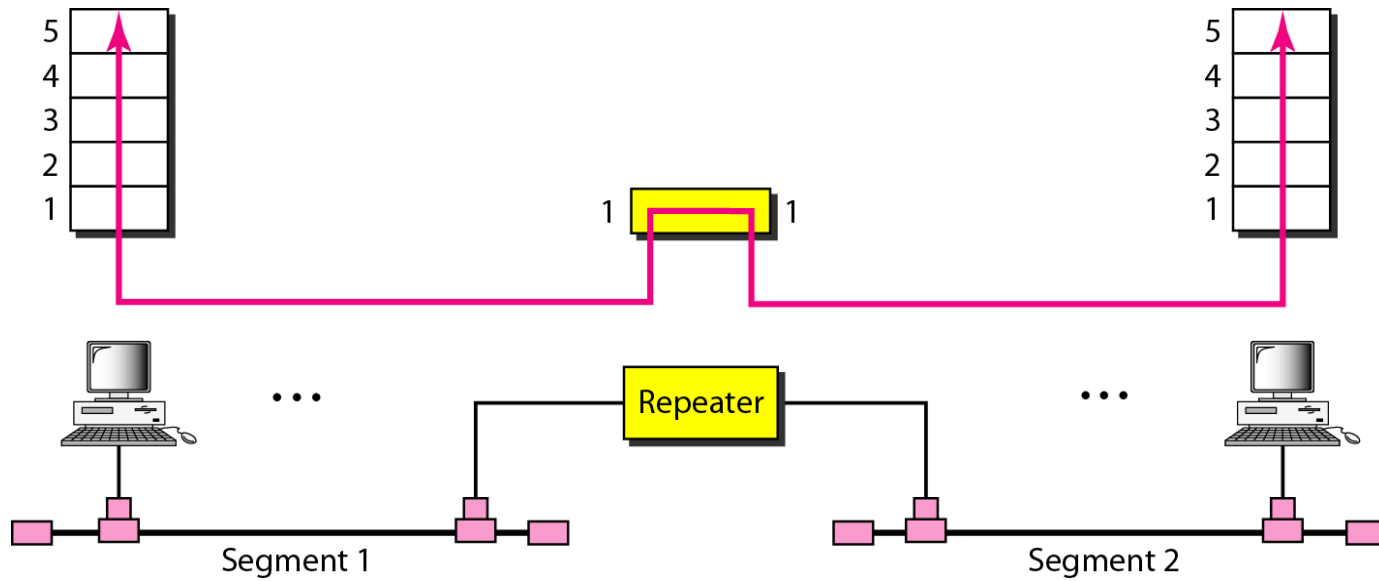
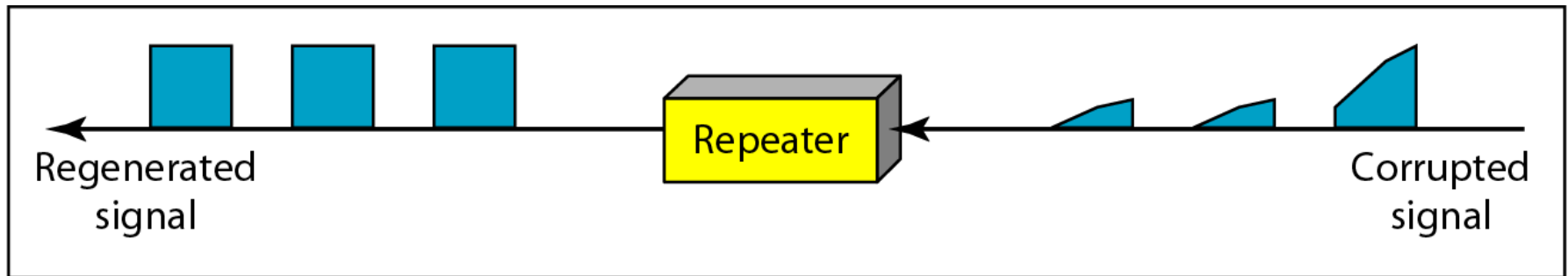
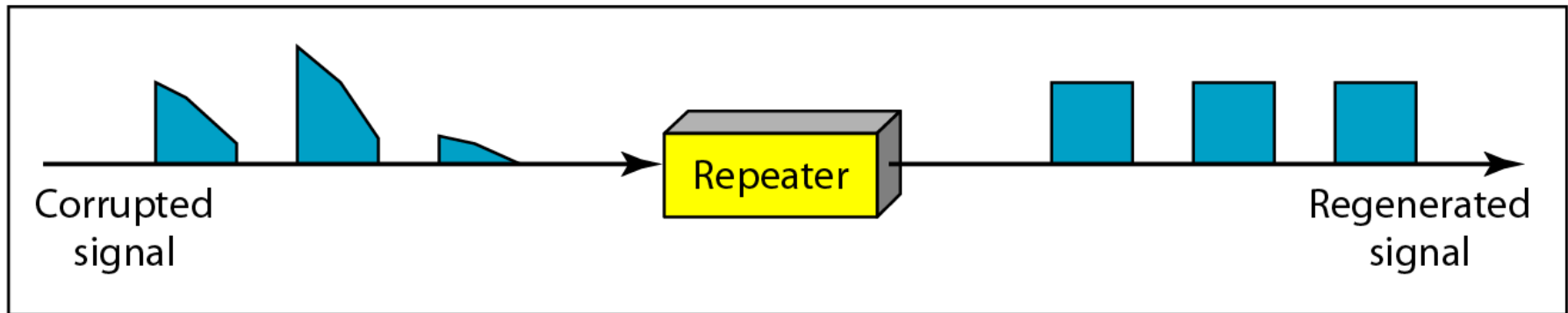


Figure 15.2 中继器

Figure 15.3 中继器的功能



a. Right-to-left transmission.

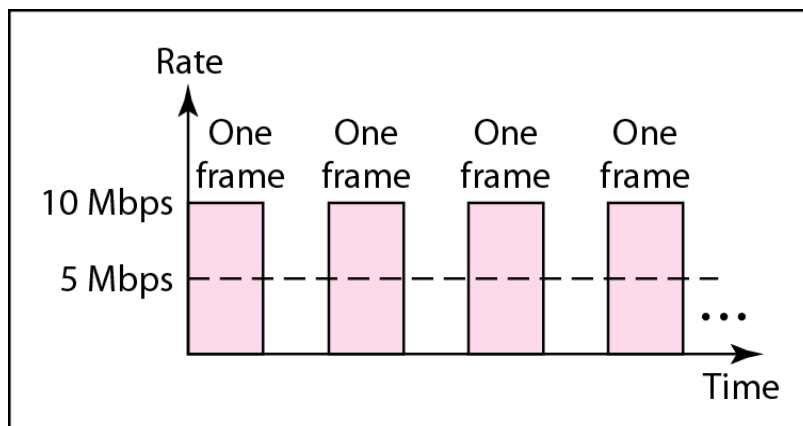


b. Left-to-right transmission.

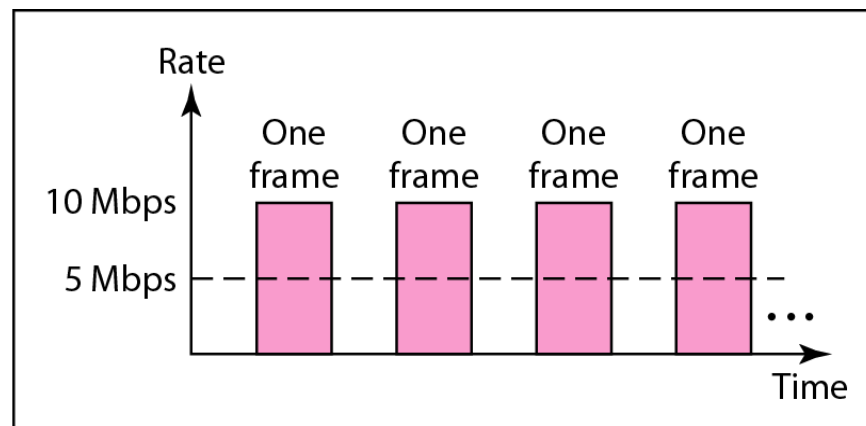
有源集线器

- 集线器和网线一样工作在物理层，功能和网线一样只是将数字信号发送到其它端口，并不能识别哪些数字信号是帧前同步码、帧定界符及网络层首部等；
- 集线器组建的以太网中计算机共享带宽，计算机数量越多，平均带宽就越低；
- 集线器组建的以太网中，无论数据帧的 MAC 地址是否是自己的，都能够捕获，因此以太网具有与生俱来的安全隐患。

带宽共享

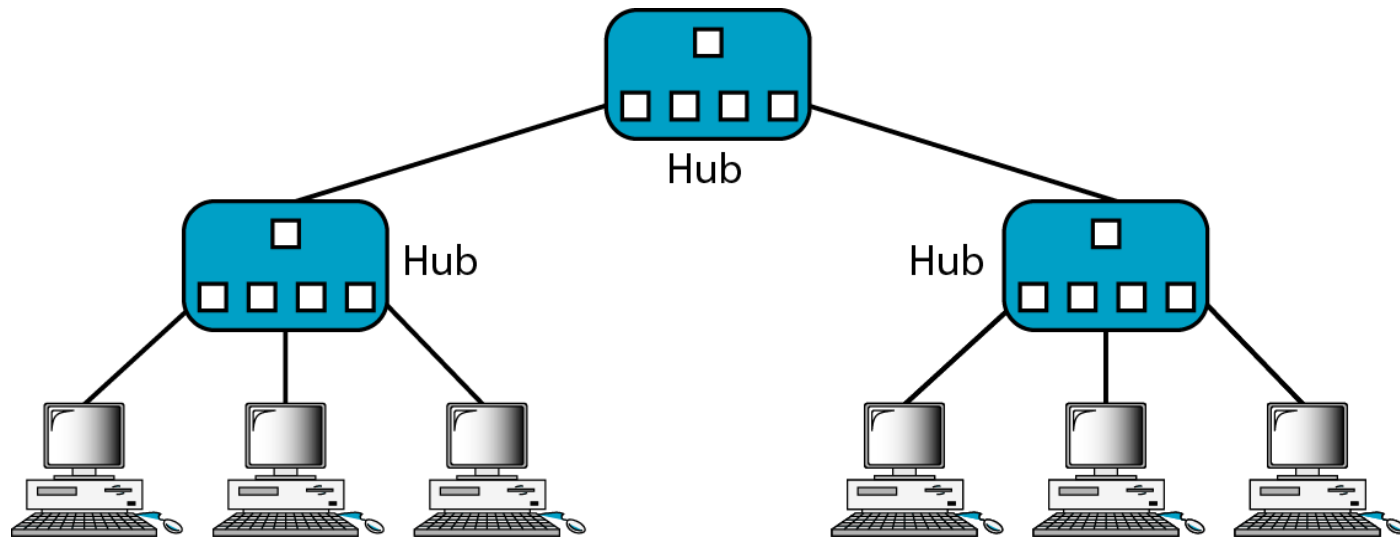


a. First station



b. Second station

Figure 15.4 有源集线器的级联



有源集线器级联的优缺点

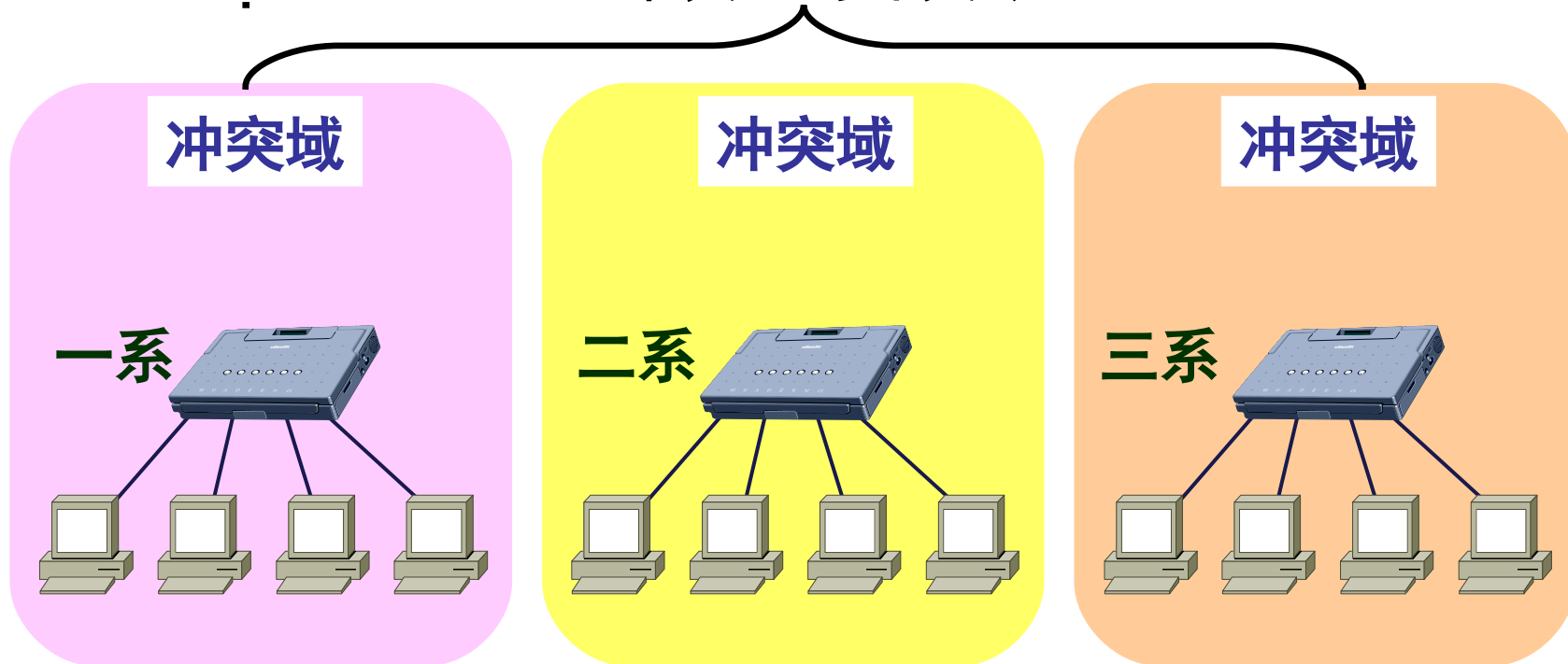
- 有源集线器是一个多端口的中继器；
- 常用于星型拓扑，克服了 10Base-T 标准的 100m 距离限制，因此扩展了以太网覆盖的范围并增加了以太网中计算机的数量；
- 级联后以太网的计算机处于一个冲突域中，增大了冲突的概率，每台计算机分到的带宽也降低了；
- 相连的集线器每个接口带宽要一样。如果速率不一致，则工作在较低的数据速率，因为集线器接口不能缓存帧。

单播与广播、广播域与冲突域

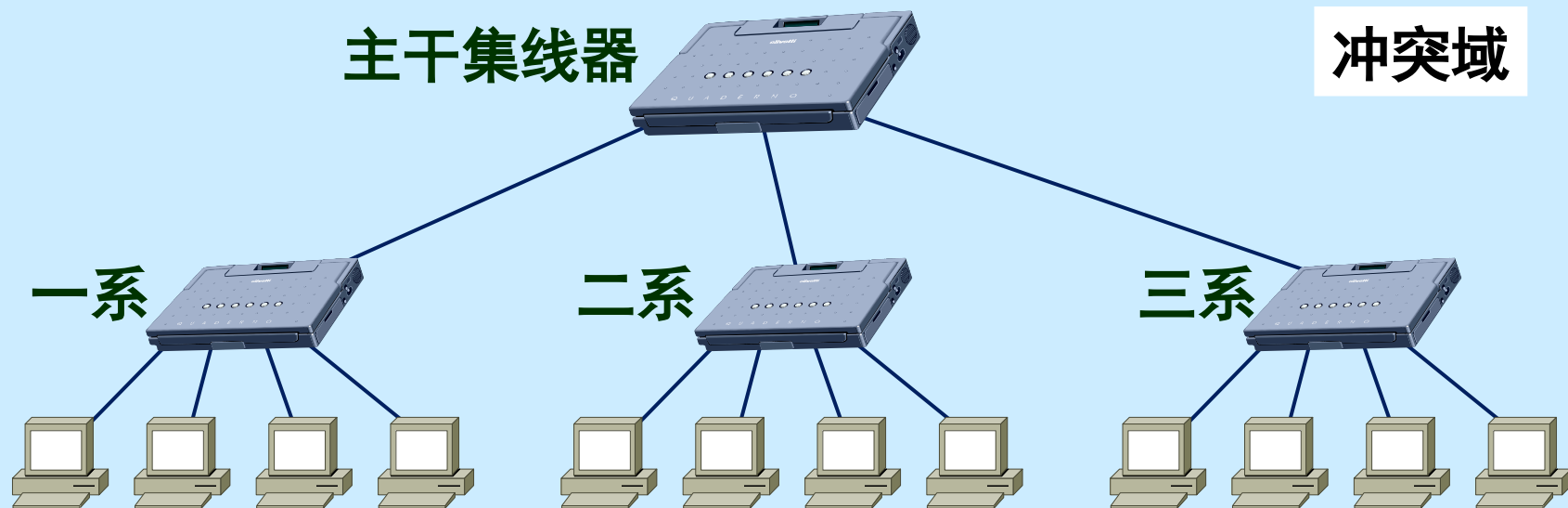
- **单播**（ Unicast ）： 在一个发送者和一个接收者之间通过网络进行的通信。
- **广播**（ Broadcast ）： 主机之间“一对所有”的通信模式，网络对其中每一台主机发出的信号都进行无条件复制并转发，所有主机都可以接收到所有信息（不管是否需要）。数据网络中的广播被限制在二层交换机的局域网范围内，禁止广播数据穿过路由器，防止广播数据影响大面积的主机。
- **广播域**： 彼此能够接收广播帧的所有设备的集合被称为一个广播域。
- **冲突域**： 在同一个网络上两个比特同时进行传输会产生冲突，这样的区域称为冲突域。所有的共享介质环境都是冲突域。

冲突域

三个独立的冲突域

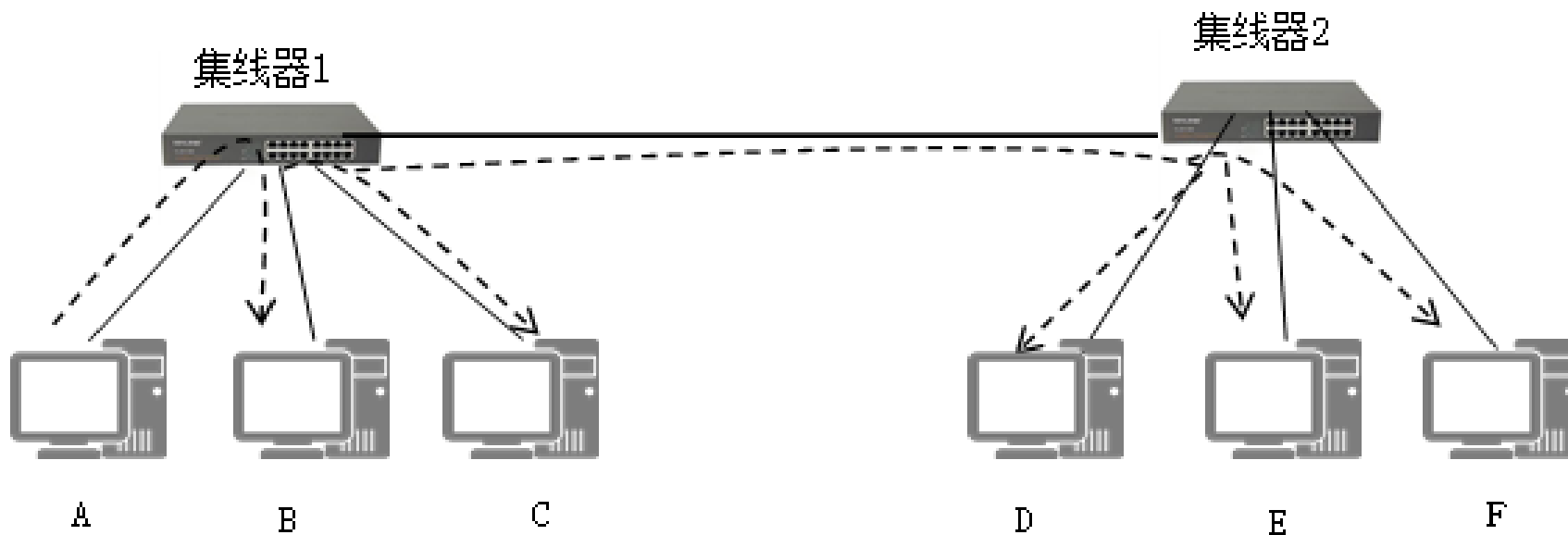


一个更大的冲突域



同一个广播域

多个集线器

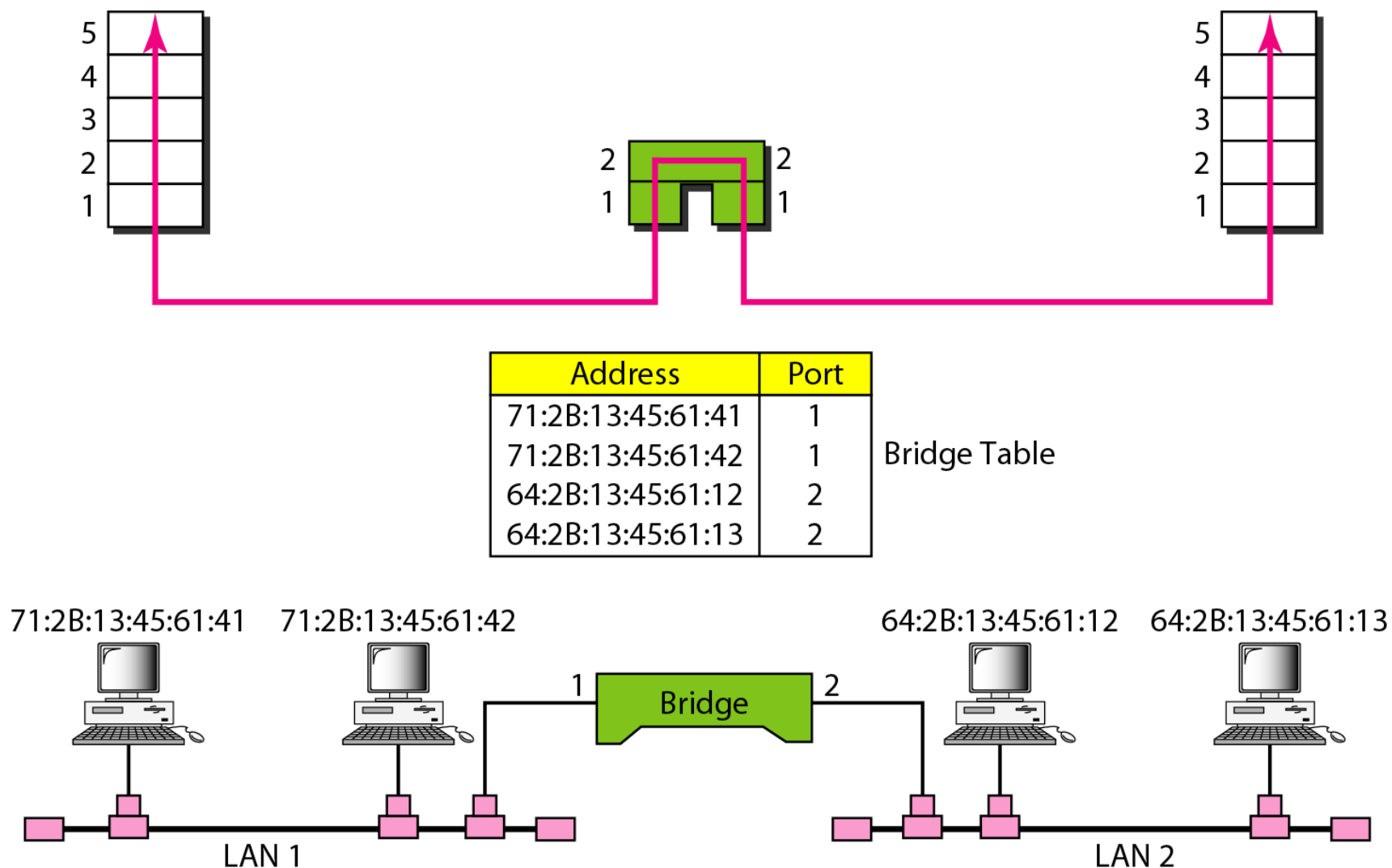


A 向 B 发送帧，数字信号会通过集线器之间的网线发送到集线器 2，导致 D 和 E 不能通信。计算机数量增加后网络利用率大大降低

网桥

- 网桥工作在物理层和数据链路层。
- 作为物理层设备时，重新生成收到的信号。
- 作为数据链路层设备时，可以检查帧所包含的MAC 地址。
- 具有一个用作过滤决策的表，有过滤作用，检查帧的目的地址。

Figure 15.5 网桥连接两个局域网



网桥组网的特点

- 网桥基于 MAC 地址转发帧，转发之前运行 CSMA/CD 算法，工作在数据链路层；
- 一个接口是一个冲突域，冲突域的数量增加，但冲突的概率降低；
- 实现帧的存储转发，增加了时延；
- 网桥的不同接口可以是不同的带宽。

透明网桥（ Transparent Bridge ）

- 网桥不改变帧中的 MAC 地址；
- 透明网桥是指站点完全意识不到桥的存在；
- 802.1d 规范了透明网桥的标准：
 - 帧必须能从一个站点转发到另外一个站点；
 - 学习帧中的地址，自动建立转发表；
 - 避免形成循环（ Loop ）问题。

Figure 15.6 学习型网桥和学习过程

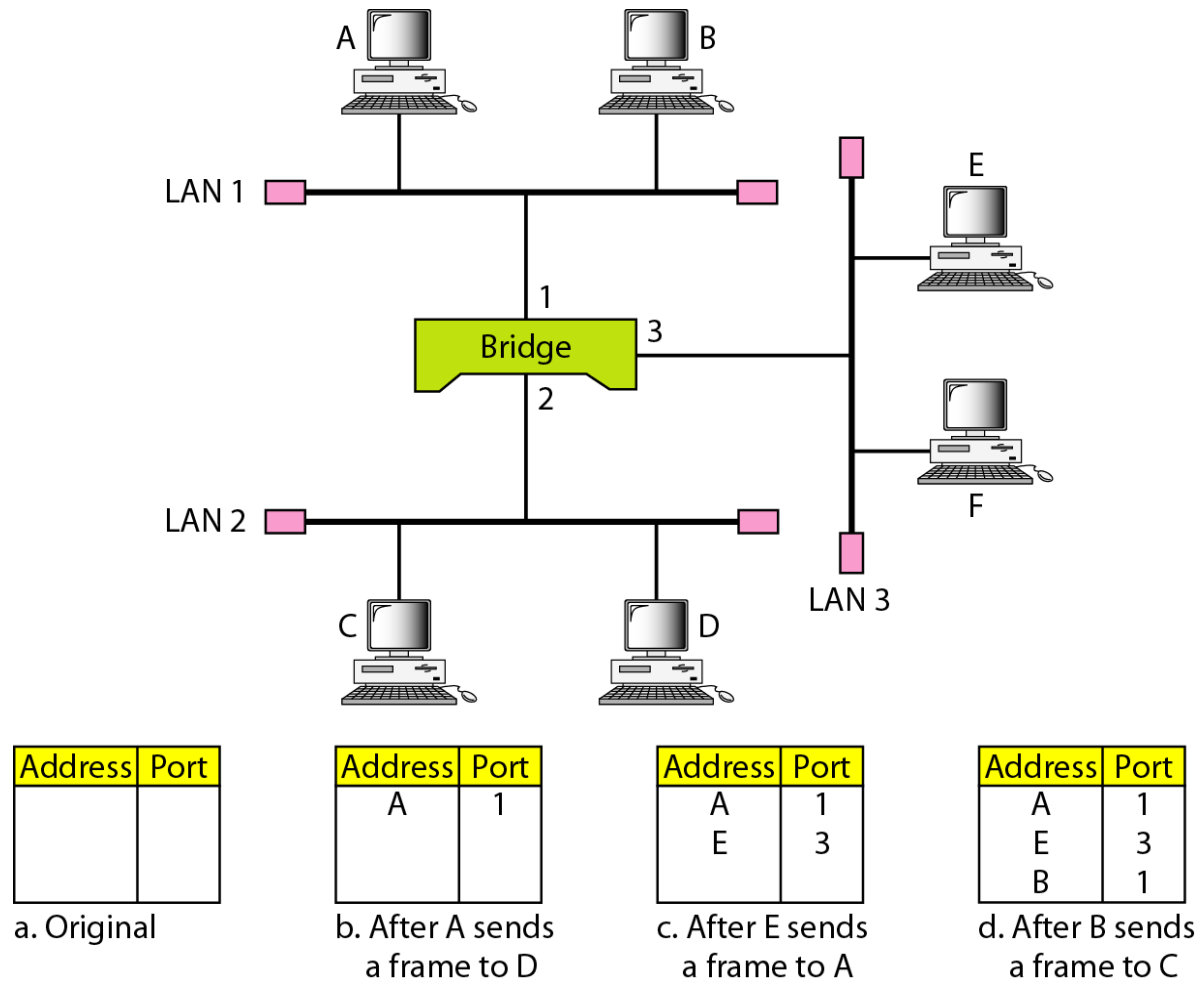
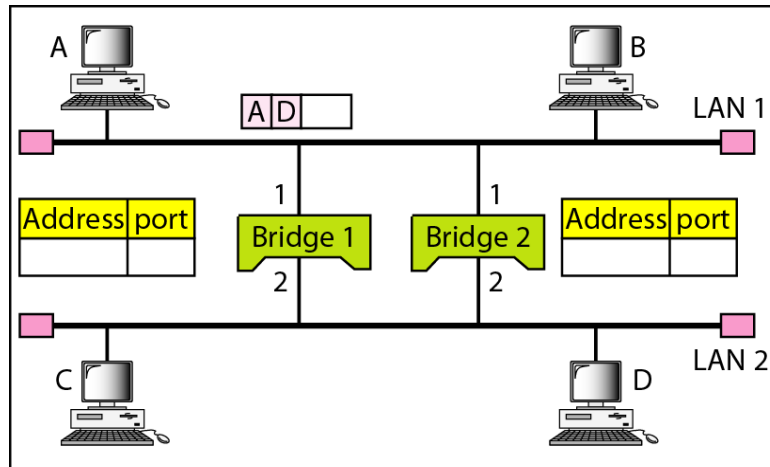
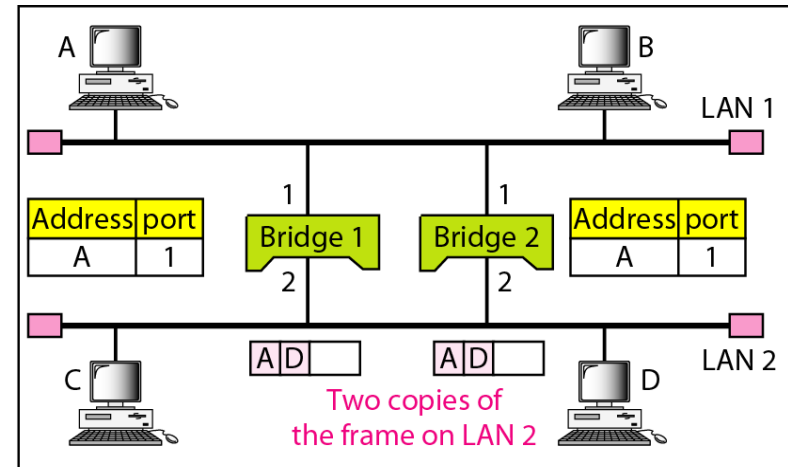


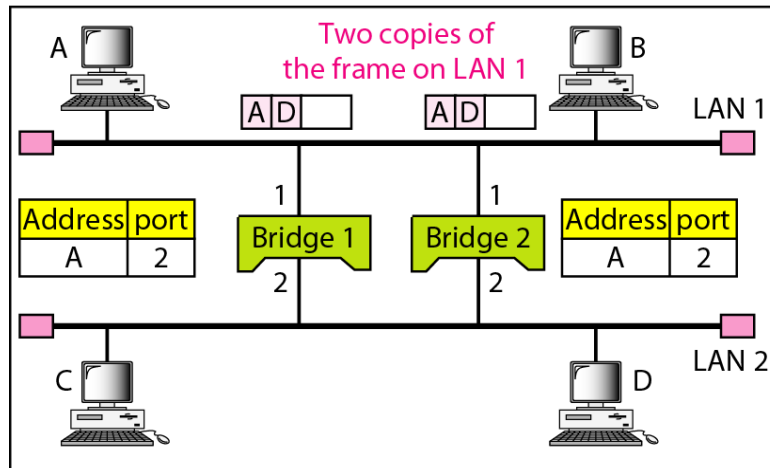
Figure 15.7 环路问题



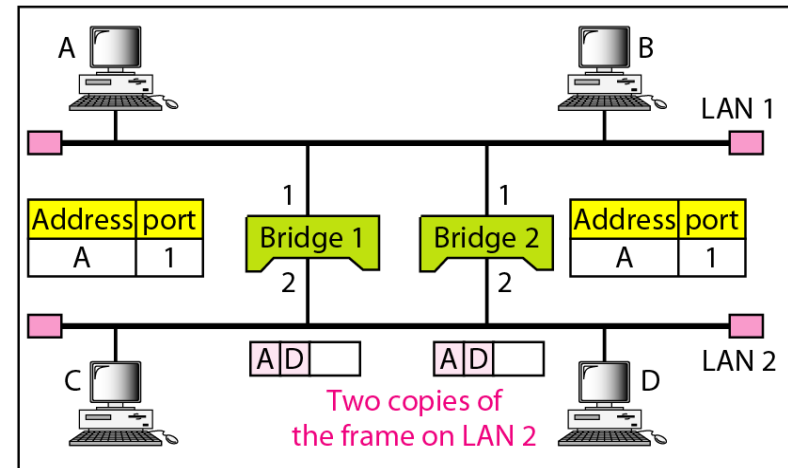
a. Station A sends a frame to station D



b. Both bridges forward the frame



c. Both bridges forward the frame

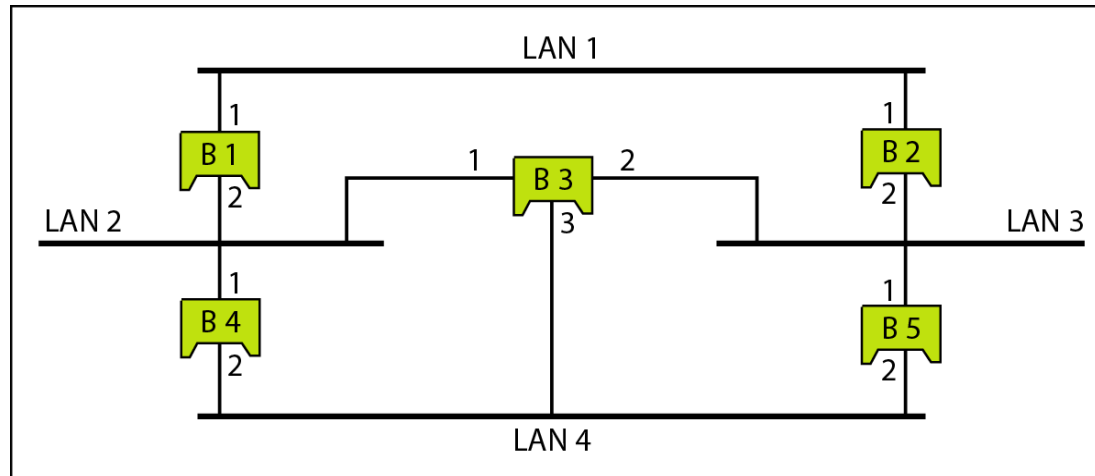


d. Both bridges forward the frame

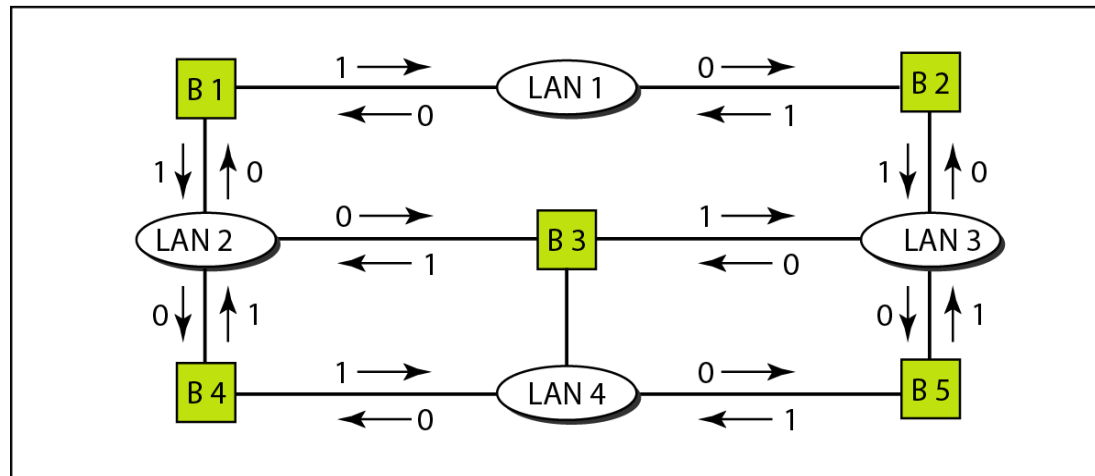
生成树（ Spanning Tree ）

- 生成树是一个没有循环路径的图，用于建立到达其它 LAN 的唯一路径；
- 基于某种度量（最小跳数、最小延迟、最短队列、最大带宽）选择最小代价；
- 假设从网桥到 LAN 跳数为 1，从 LAN 到网桥跳数为 0。

Figure 15.8 连接的 LAN 系统及图示



a. Actual system

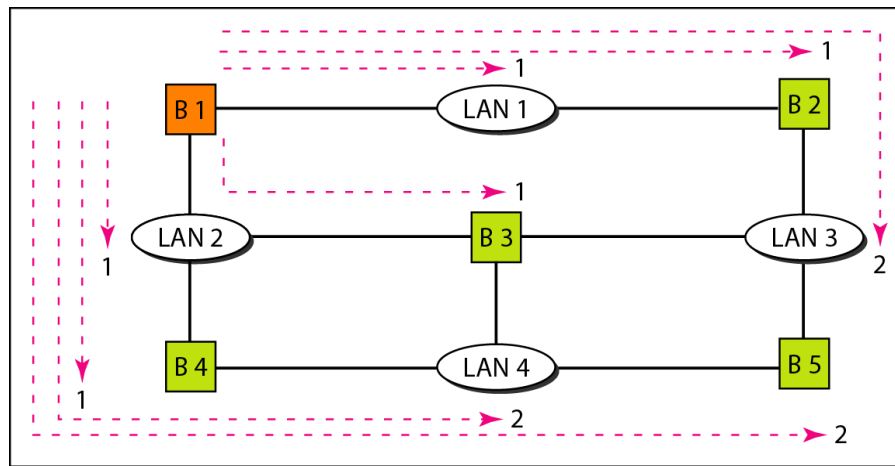


b. Graph representation with cost assigned to each arc

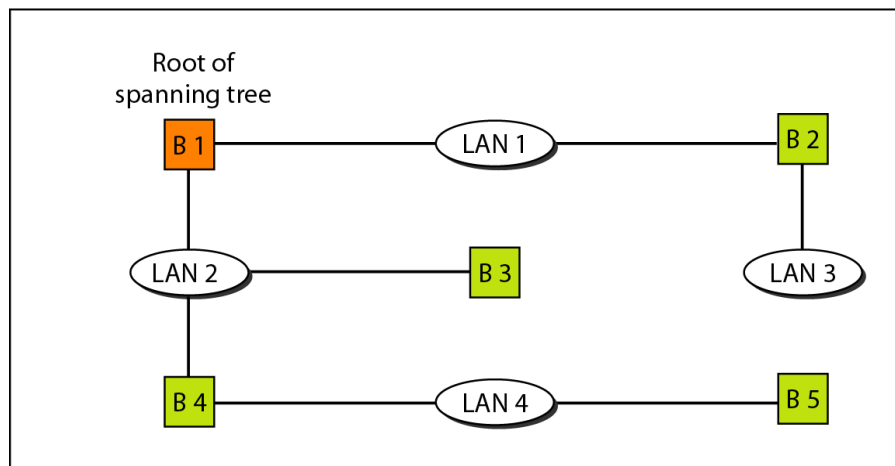
生成树算法

- 每个网桥广播其 ID ， 选择最小 ID 的网桥作为根网桥；
- 找出从根网桥到其它网桥或 LAN 的最短路径；
- 最短路径组合生成最短的树；
- 标记转发端口和阻塞端口。

Figure 15.9 最短路径和生成树

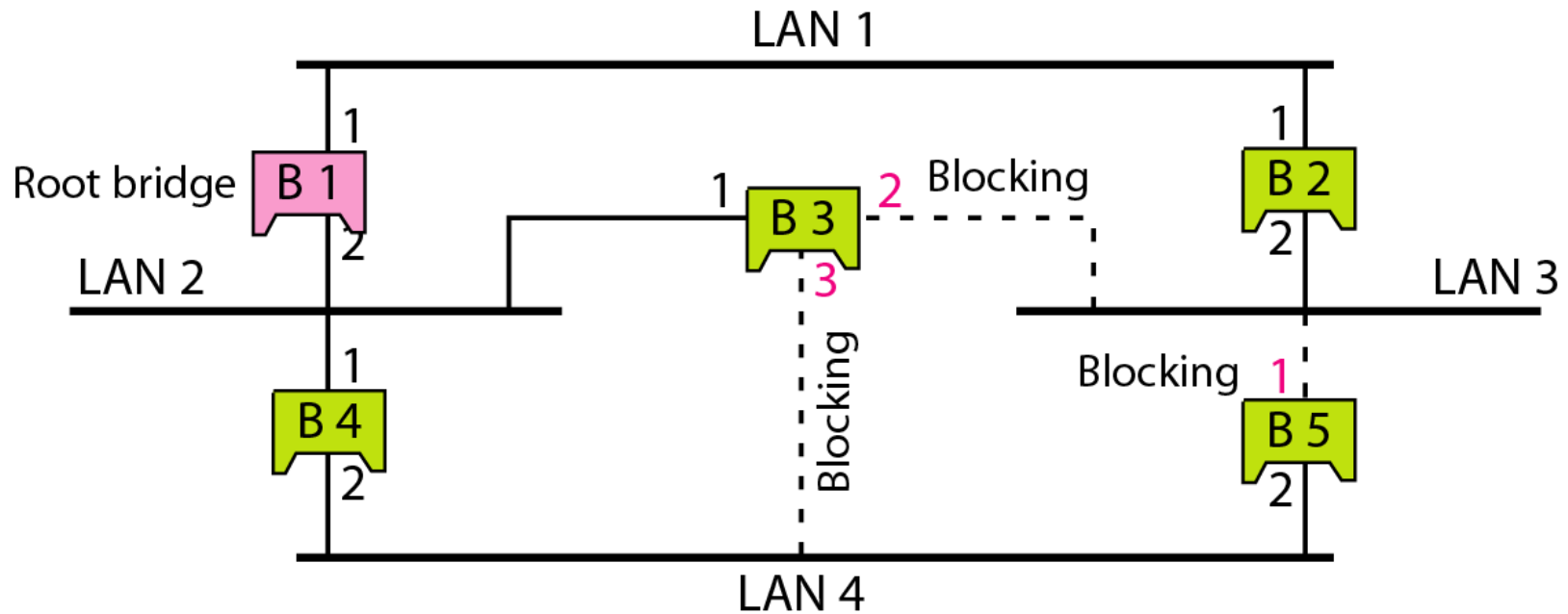


a. Shortest paths



b. Spanning tree

Figure 15.10 使用生成树算法后的转发端口和阻塞端口



Ports 2 and 3 of bridge B3 are blocking ports (no frame is sent out of these ports).
Port 1 of bridge B5 is also a blocking port (no frame is sent out of this port).

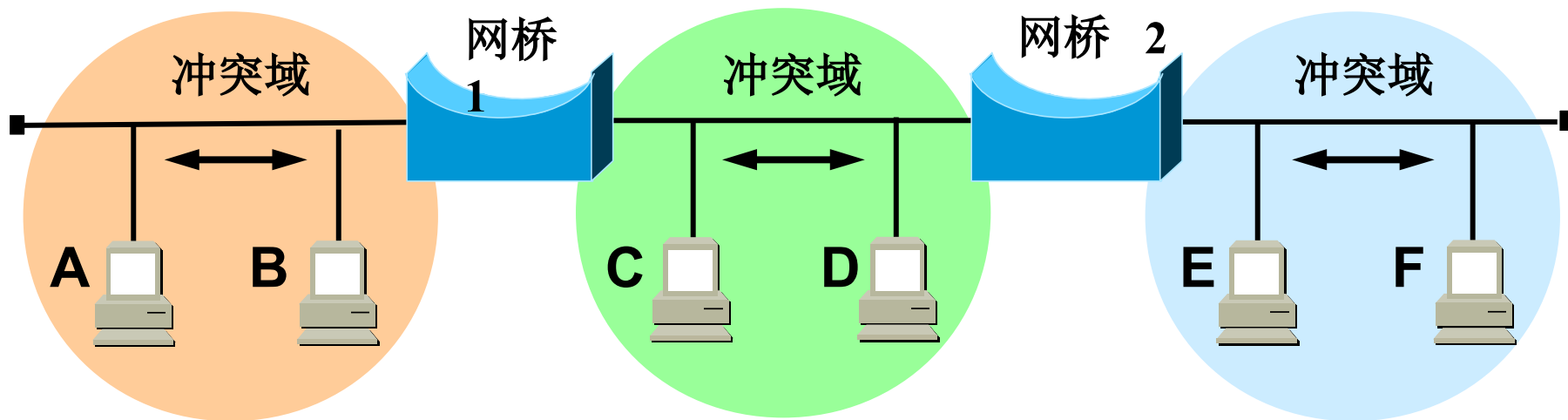
源路由网桥

- 防止环路的另外一种方法；
- 透明网桥的职责（过滤帧、转发和阻塞）由源站点来执行；
- 由源方指定帧必须经过的网桥。发送数据帧之前，源站点和目的站点通过交换特定帧来得到网桥地址；
- 用于令牌环网。

用网桥连接不同的局域网

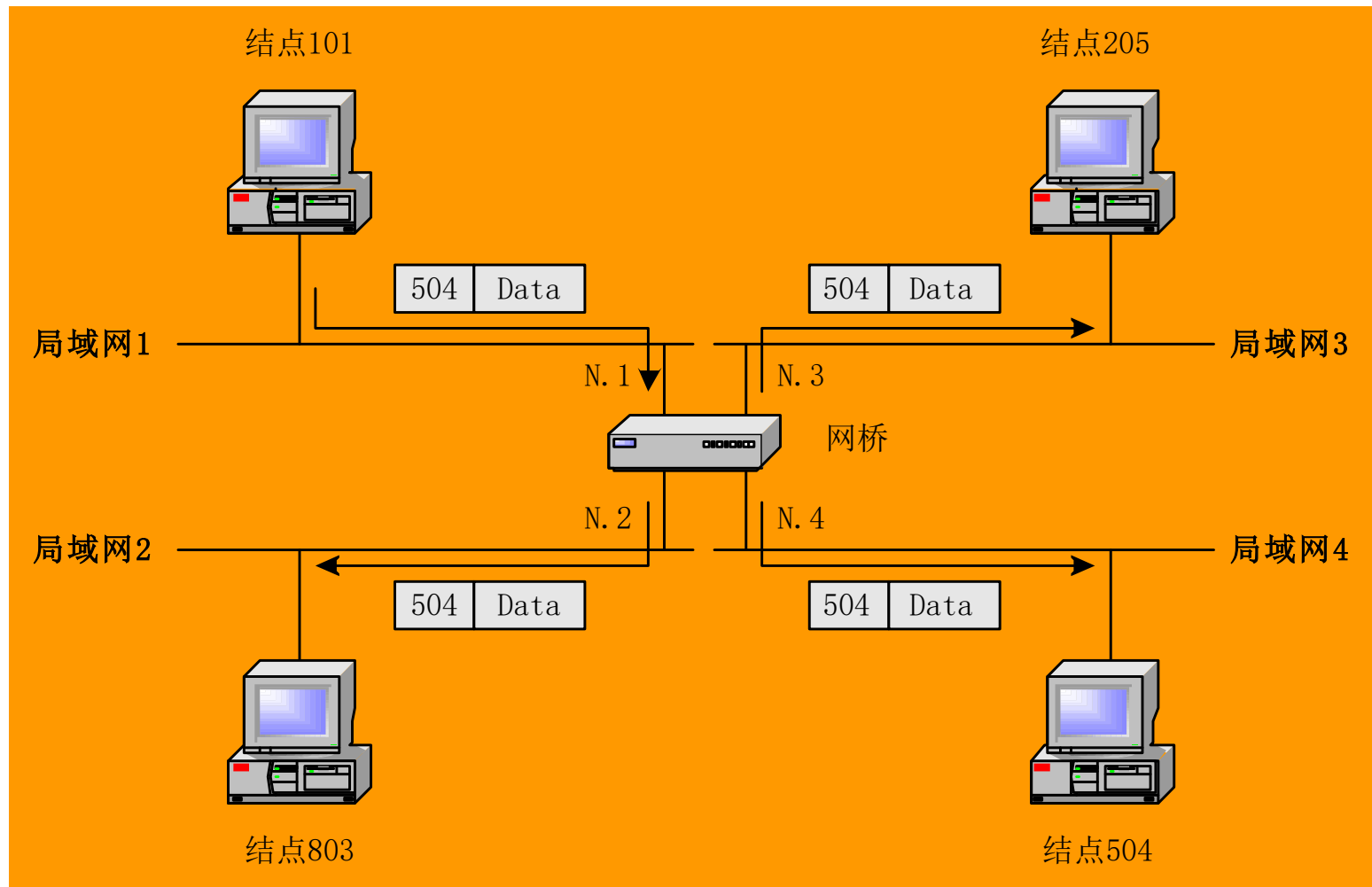
- 帧格式
- 最大数据长度
- 数据速率
- 位顺序（先发送高位还是先发送低位）
- 安全
- 多媒体支持

用网桥连接不同的局域网



网桥将不同端口连接的网络分隔成独立的冲突域，但是网桥在收到一个广播数据帧时，会向所有端口转发这个广播帧，即所有端口处于同一个广播域中。

网桥与广播风暴



交换机——多端口网桥

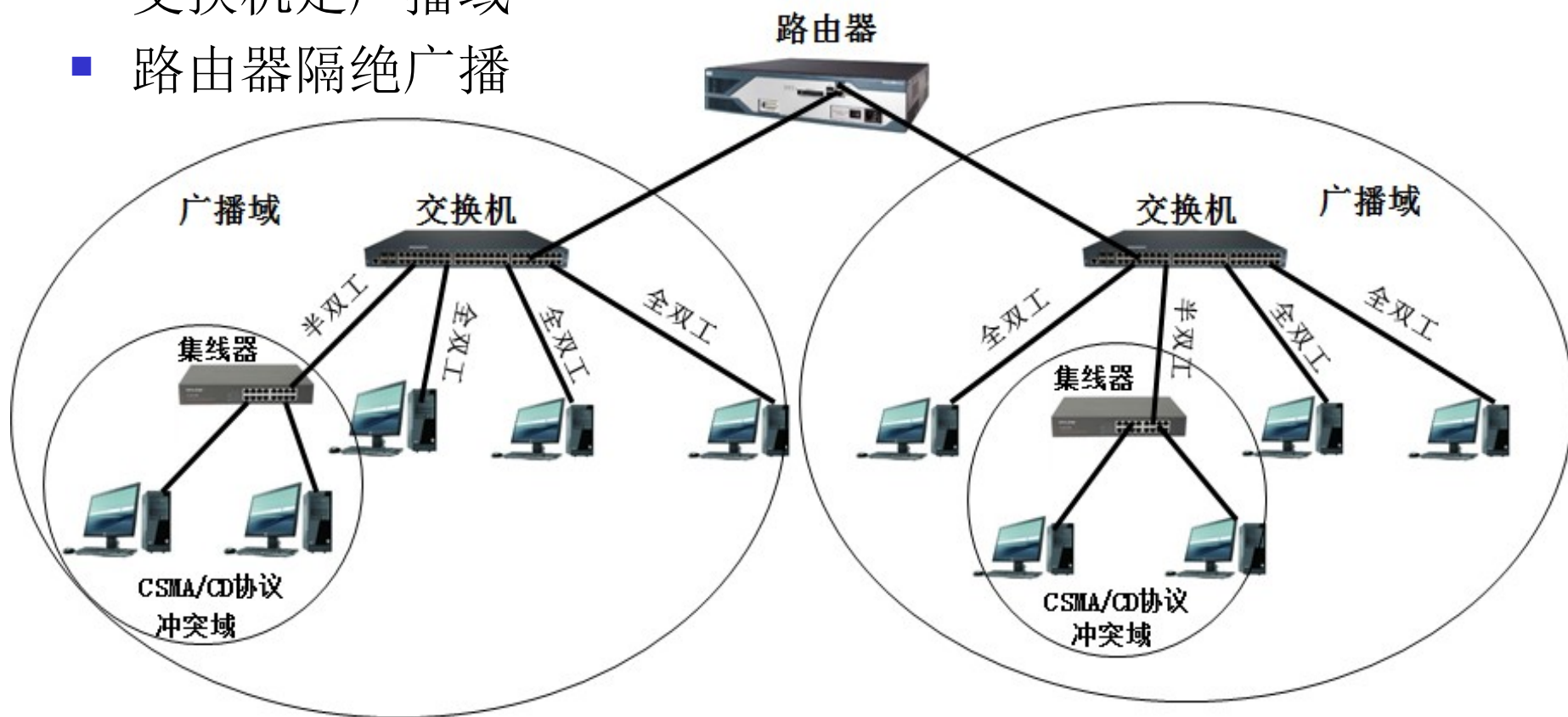
随着技术的发展，网桥接口日益增多，发展成现在的交换机。

使用交换机组网与集线器组网相比具有以下特点：

- 端口独享带宽：集线器是共享带宽；
- 安全：交换机根据 MAC 地址只转发到目标端口；
- 全双工通信；
- 全双工不再使用 CSMA/CD 协议；
- 接口可工作在不同速率：交换机使用存储转发技术；
- 转发广播帧：转发到除了发送端口以外的所有端口。

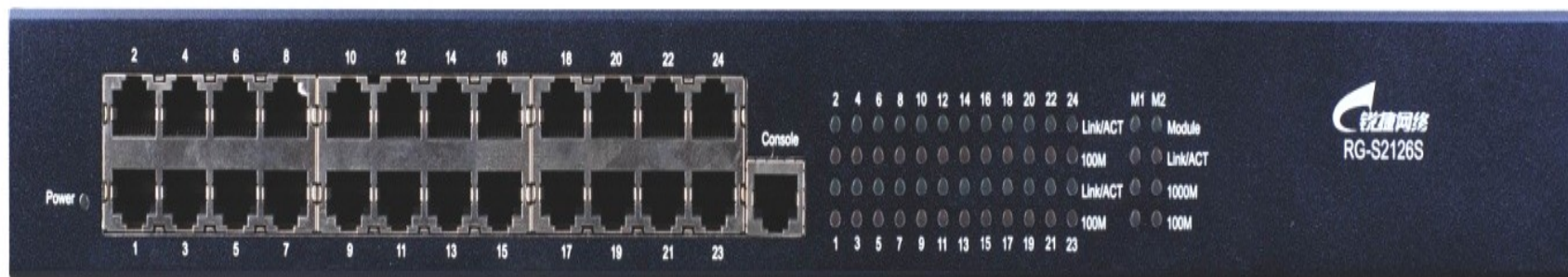
交换机的冲突域和广播域

- 集线器是冲突域
- 交换机是广播域
- 路由器隔绝广播



二层交换（ Two-layer Switch ）

- 交换机包括二层交换机和三层交换机。
- 二层交换机是一个多端口并且有更好性能的网桥，可以像网桥一样，基于收到帧的 MAC 地址做出过滤决策。
- 二层交换机工作过程比网桥更加复杂，它有缓存区来保存帧并进行处理。



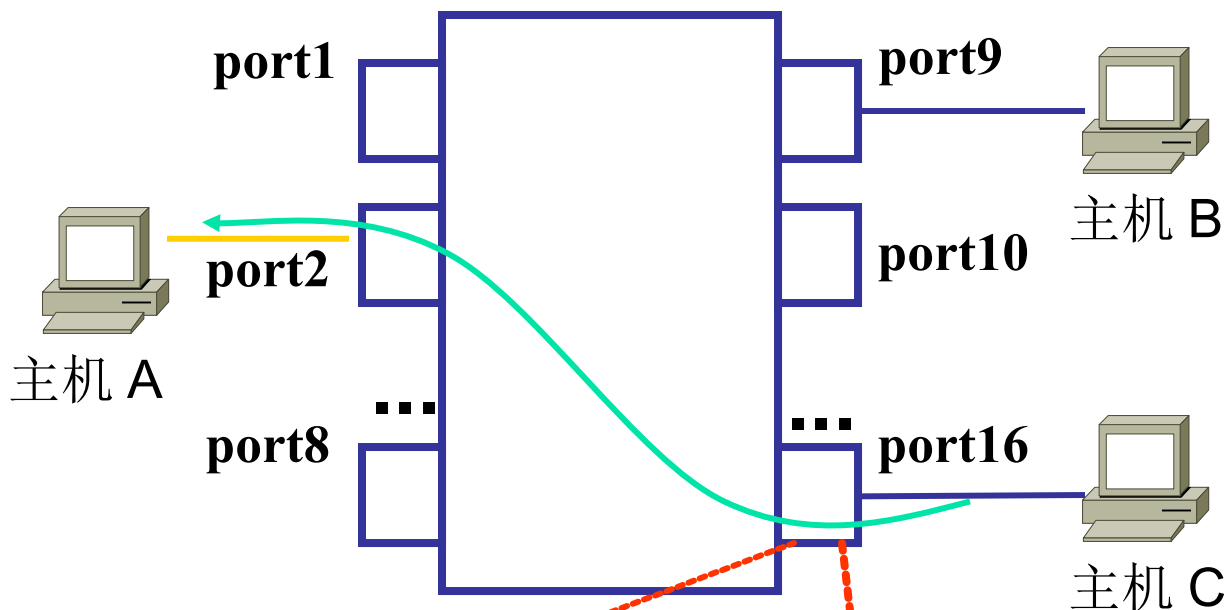
二层交换机的优点

- 从总线型局域网或集线器局域网转变为交换局域网，连接设备在软件或硬件上不需做任何修改。例如原来是以太网，连接设备继续使用以太网媒体接入控制协议来接入局域网。
- 每个连接设备都具有相当于原来整个局域网容量的专用容量，只要二层交换机有足够容量为所有连接设备服务。
- 二层交换机扩容简单。

二层交换机的类型

- 存储转发式（ Store-and-forward ）
 - 从输入线路上接收帧
 - 缓存
 - 通过路由选择将其发到适当的输出线路上
 - 发送方和接收方之间存在延迟
 - 增进了网络的整体一致性
- 直通式（ Cut-through ）
 - 利用了目的地址总是出现在 MAC 帧的最前面的特点
 - 交换机识别出目的地址后就将帧转发到适当的输出线路
 - 能够达到很高的吞吐量
 - 可能传播损坏帧（交换机在重传之前无法做 CRC 检查）

直通模式



端口刚收到帧的目的地址和源地址，还没有收到整个帧就开始交换。

- 速度快，达到线速。
- 没有检查校验码，容易出错，因此用于误码率低的网络。

不等收到整个帧，就开始交换

引导码	目的 MAC 地址	源 MAC 地址	长度	帧内容	校验码
-----	-----------	----------	----	-----	-----

三层交换机

三层交换机具有路由功能，与传统路由器的路由功能总体上一致，但是它们还是存在着相当大的本质区别的。

- 主要功能不同。三层交换机同时具备了数据交换和路由转发两种功能，但其主要功能还是数据交换；而路由器仅具有路由转发这一种主要功能。
- 主要适用的环境不一样。三层交换机的路由功能通常比较简单，在局域网中的主要用途还是提供快速数据交换功能。路由器则更多体现在不同类型网络之间的互联上，如局域网与广域网之间的连接、不同协议的网络之间的连接等，可进行最佳路由选择、负荷分担、链路备份及和其他网络进行路由信息的交换等。
- 性能体现不一样。路由器一般由基于 CPU 的软件路由引擎执行数据包交换，而三层交换机通过硬件执行数据包交换。从整体性能上三层交换机的性能远优于路由器，适用于数据交换频繁的局域网中；路由器虽然路由功能非常强大，但它的数据包转发效率远低于三层交换机，更适合于数据交换不是很频繁的不同类型网络的互联，如局域网与互联网的互联。

路由器（ Router ）

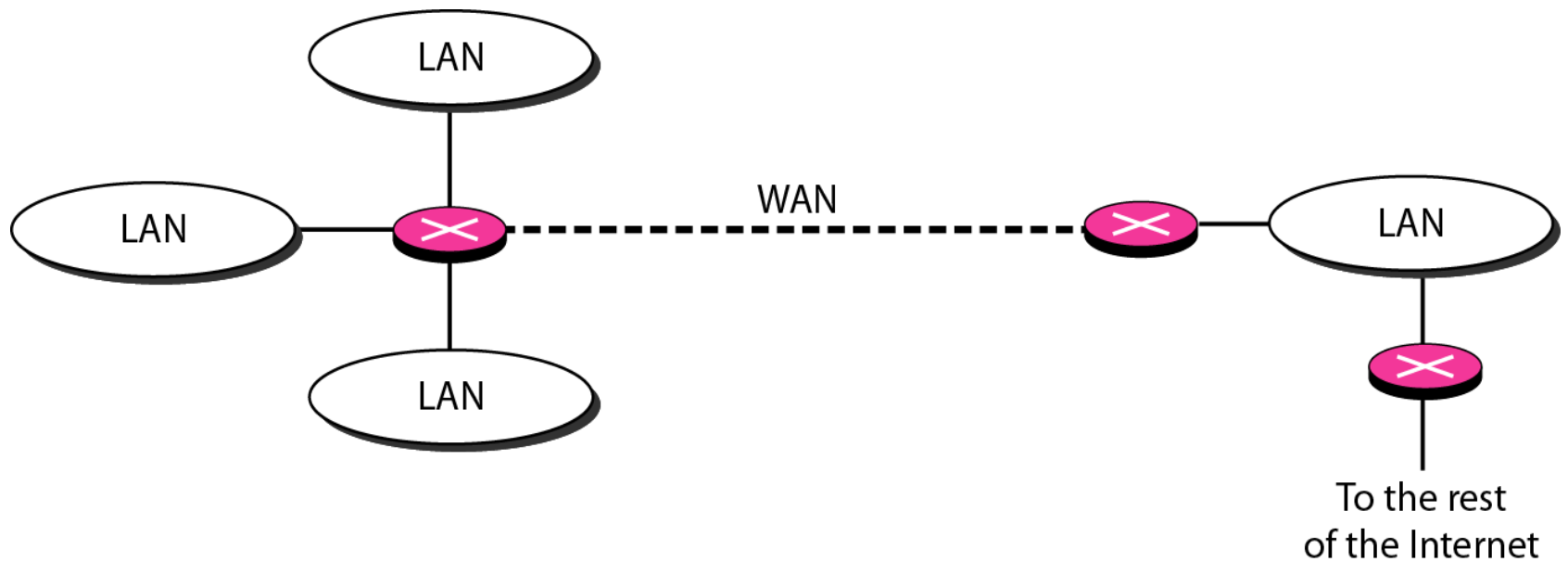
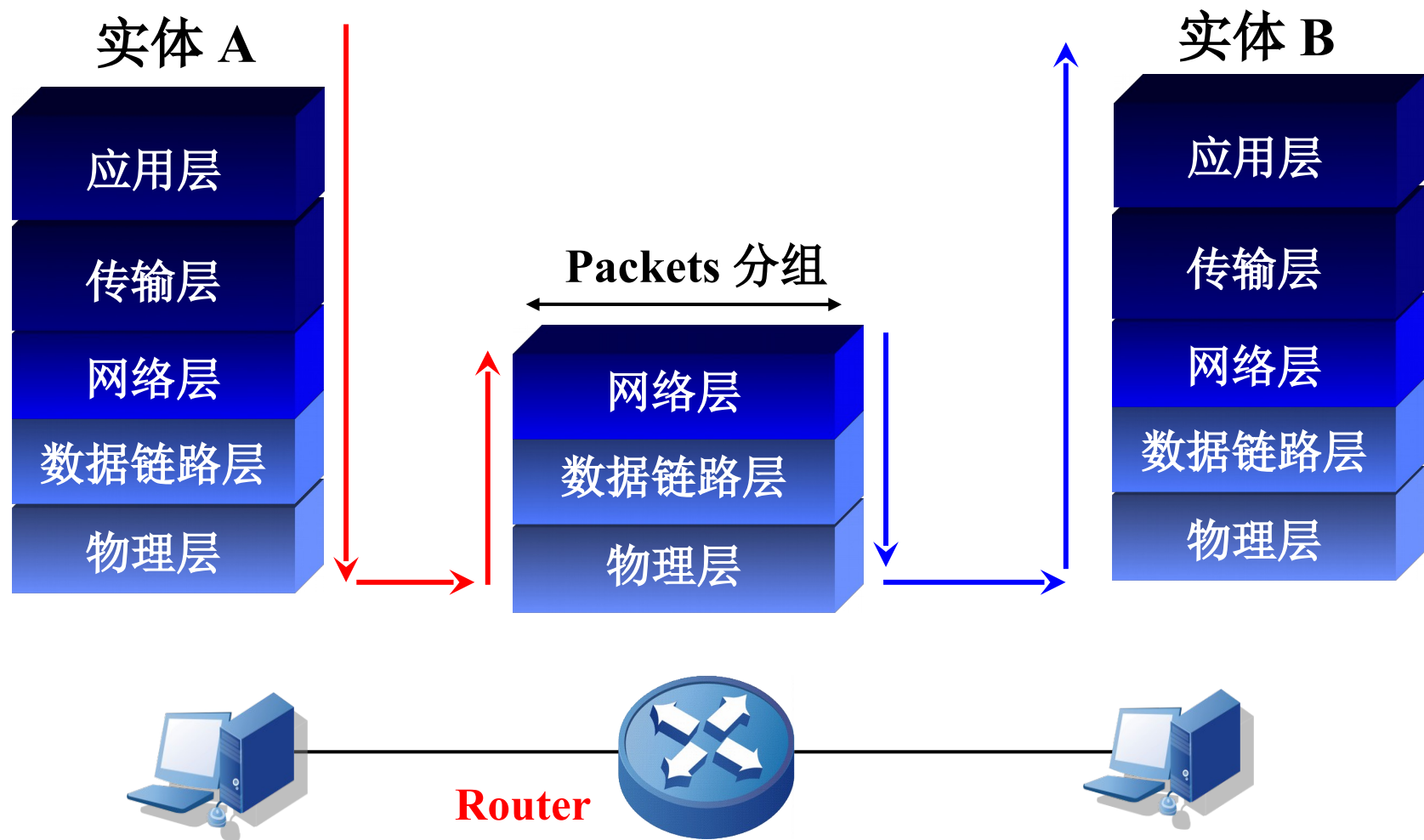
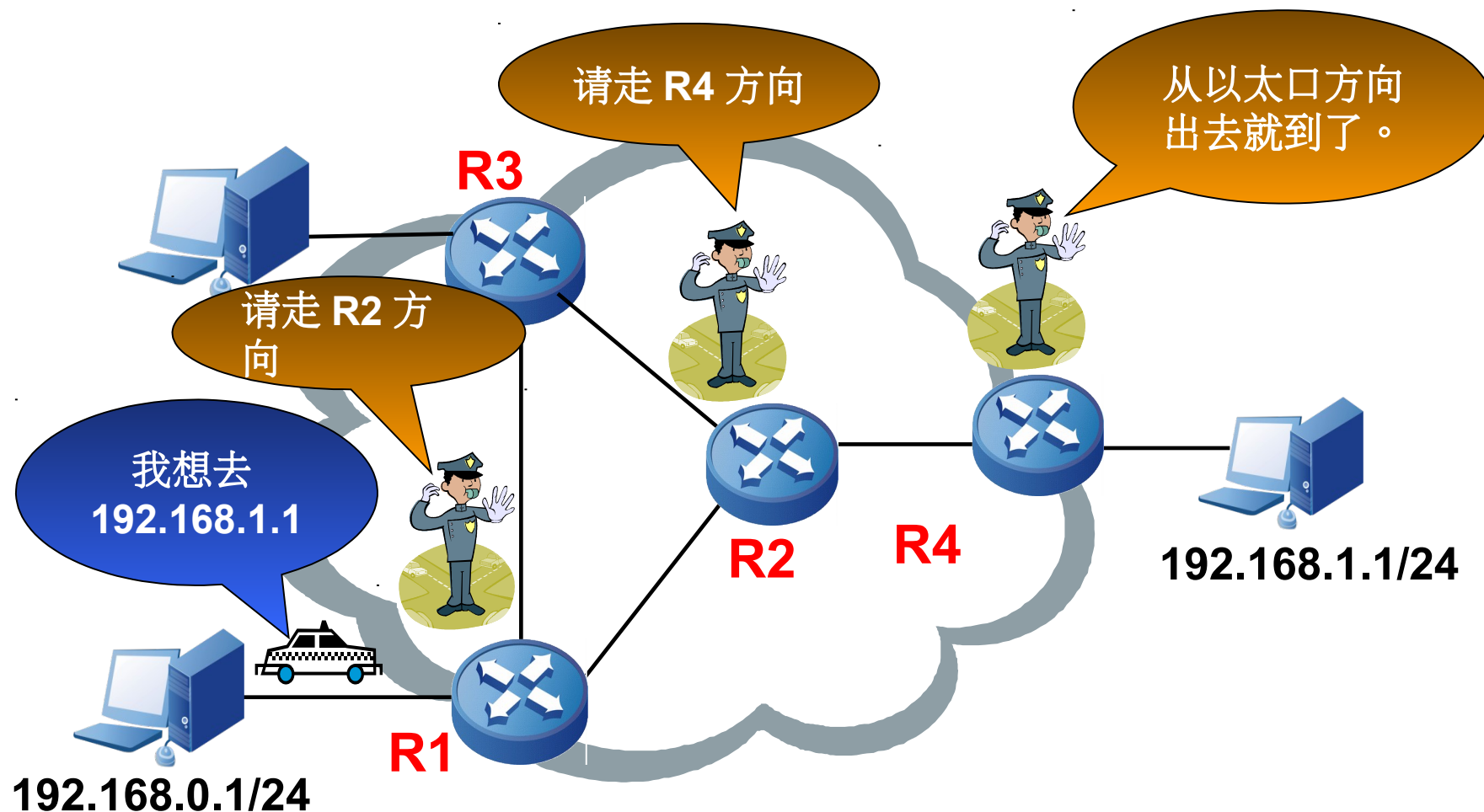


Figure 15.11 路由器连接 LAN 和 WAN

路由器的数据处理



路由器的基本工作原理



路由（Routing）是指导 IP 报文发送的路径信息。

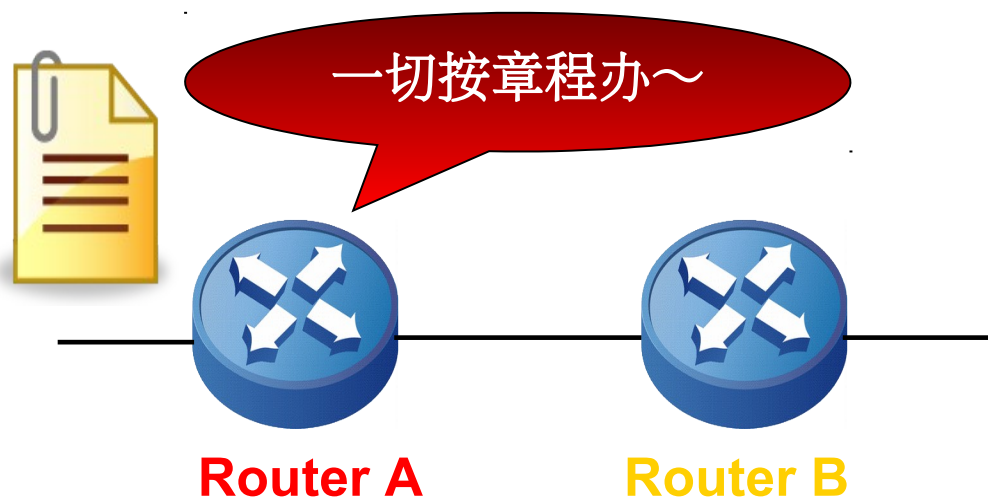
路由表（ routing table ）

- 用于保存各种传输路径的相关数据（路由信息）供数据转发（路由选择）时使用。
- 路由表中包含了下列关键项：
 - 目的地址（ Destination ）：标识 IP 数据报的目的地址或目的网络
 - 网络掩码（ Mask ）：与目的地址一起标识目的主机或路由器所在网段的地址
 - 输出接口（ Interface ）：说明 IP 数据报从路由器哪个接口转发
 - 下一跳 IP 地址（ Next hop ）：说明 IP 数据报所经由的下一个路由器的接口地址

路由的来源

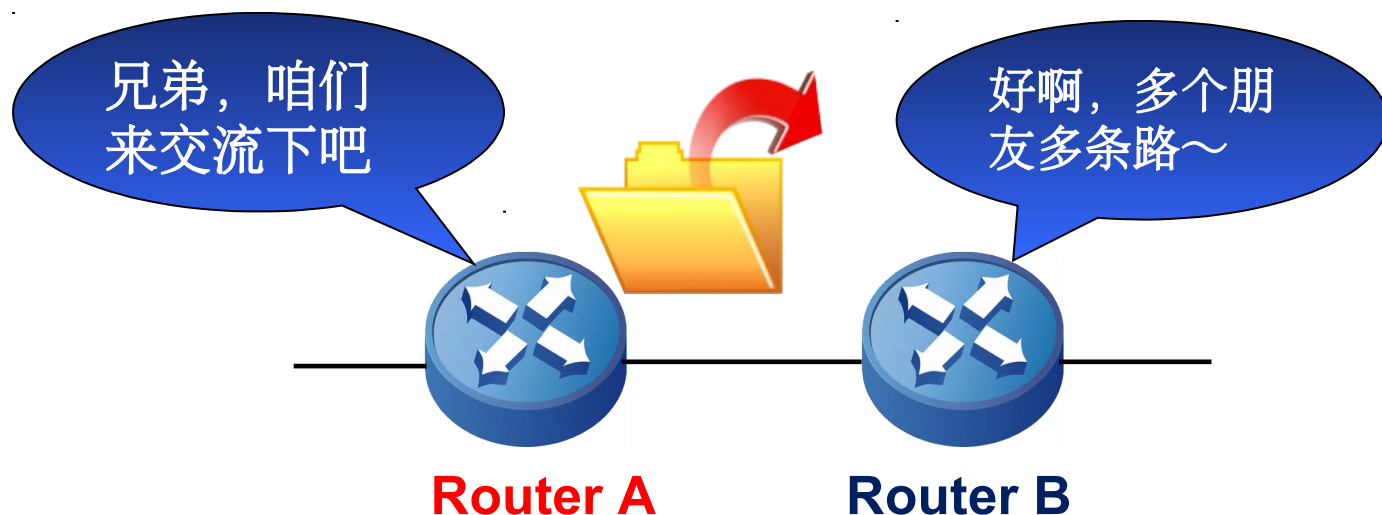
- 链路层协议发现的直连路由
开销小，配置简单，无需人工维护。只能发现本接口所属网段的路由。
- 手工配置静态路由
无开销，配置简单，需人工维护，适合简单拓扑结构的网络。
- 动态路由协议发现的动态路由
开销大，配置复杂，无需人工维护，适合复杂拓扑结构的网络。

静态路由



- **静态路由：** 是网络管理员在路由器中设置的固定的路由表，除非人为干预，否则不会发生变化，一般用于网络规模不大、拓扑结构固定的网络中。
- **优点：** 简单、高效、可靠，优先级最高；
- **缺点：** 配置繁琐，而且无法适应网络环境的变化，配置繁琐。

动态路由



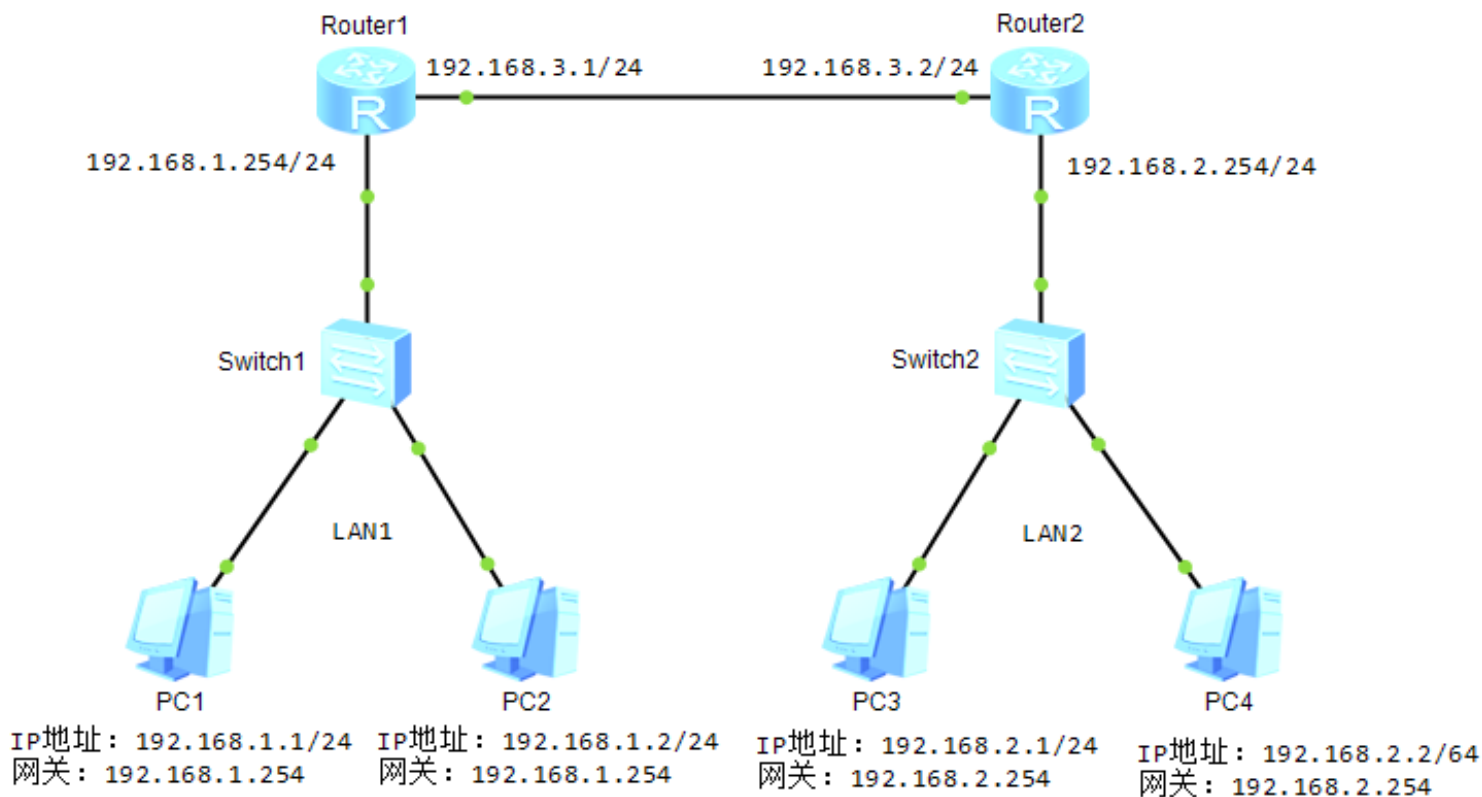
- **动态路由**：网络中的路由器之间运行动态路由协议，相互通信、传递路由信息，利用收到的路由信息更新路由表。一般适用于大型、拓扑经常变动的网络中。
- **优点**：配置简单，能实时地适应网络结构的变化。如果发生了网络变化，就会引起网络中所有路由器重新计算路由。
- **缺点**：各种动态路由协议会不同程度地占用网络带宽和CPU 资源。

网关（ Gateway ）

- 在网络层以上实现网络互连，是复杂的网络互连设备，仅用于两个高层协议不同的网络互连，可用于广域网和局域网。
- 充当转换任务的计算机系统或设备，使用于不同的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间，是一个翻译器。
- 与网桥只是简单地传达信息不同，网关对收到的信息要重新打包，以适应目的系统的需求。
- 由于历史的原因，许多有关 TCP/IP 的文献曾把网络层使用的路由器称为网关，如今很多局域网采用都是路由来接入网络，因此通常指的网关就是路由器的 IP 。

网关（Gateway）

如果 LAN1 中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给 LAN2 的网关，LAN2 的网关再转发给其网络中的某个主机。



15-2 主干网 BACKBONE NETWORKS

- 主干网允许连接多个局域网
- 站点不直接连接到主干上
- 站点是局域网的一部分，有主干连接这些局域网

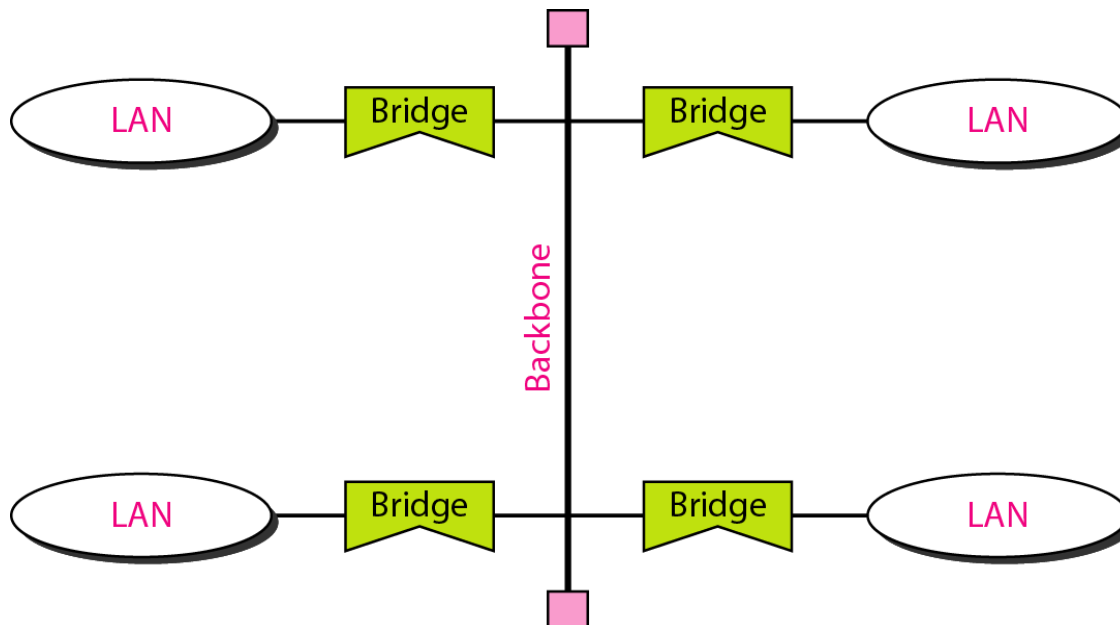
Topics discussed in this section:

Bus Backbone 总线型主干网

Star Backbone 星型主干网

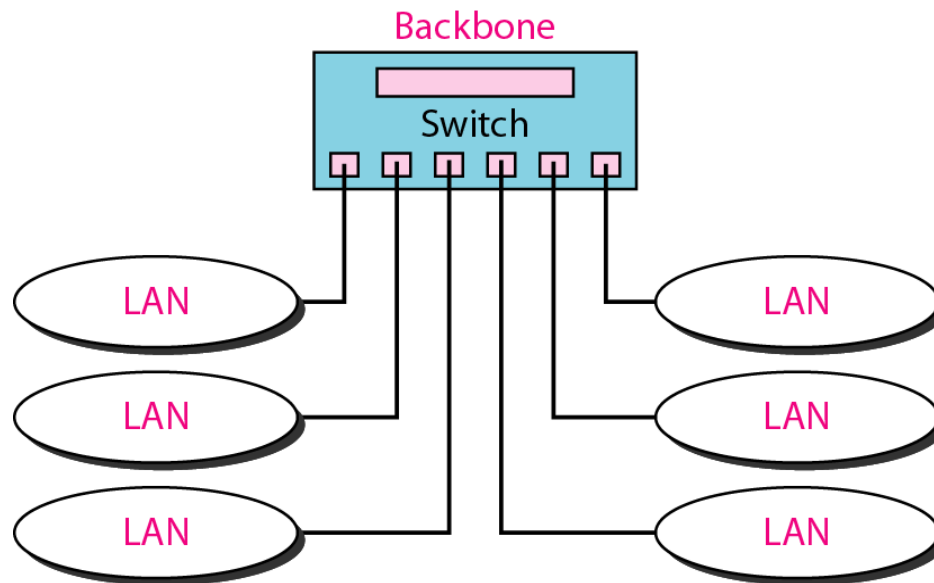
Connecting Remote LANs 连接远程 LAN

Figure 15.12 总线型主干网



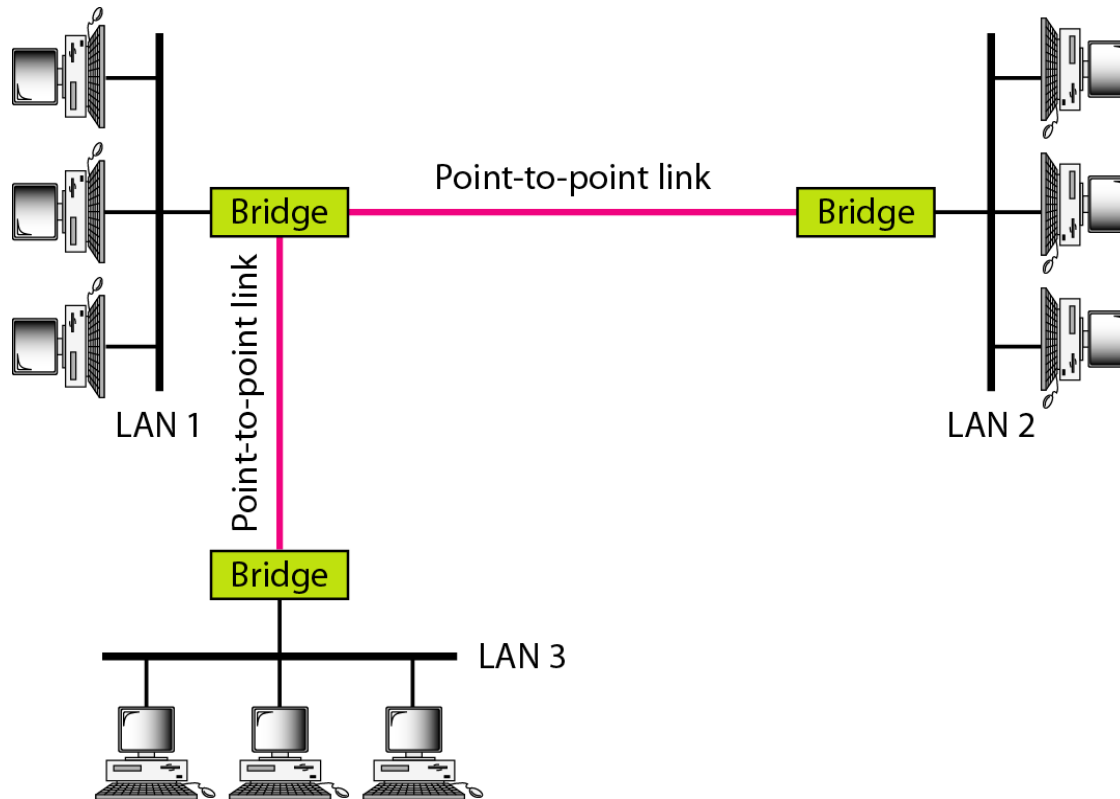
- 如果一个站要向同一 LAN 中的另一个站点发送帧，相应的网桥将阻塞该帧，到达不了主干；
- 如果一个站点要向另外一个 LAN 中的站点发送帧，网桥将传输该帧到主干网，由适当的网桥接收并发送到目的 LAN。

Figure 15.13 星型主干网



- 在星型主干网中，拓扑结构是星型。
- 主干网仅是一台交换机。

Figure 15.14 网桥连接远程 LAN



在远程网桥连接的远程主干网中，点对点链路被认为是一个局域网。

15-3 虚拟局域网 VIRTUAL LAN

通过软件而不是物理线路来配置一个局域网，称为虚拟局域网（VLAN）。

Topics discussed in this section:

Membership 成员

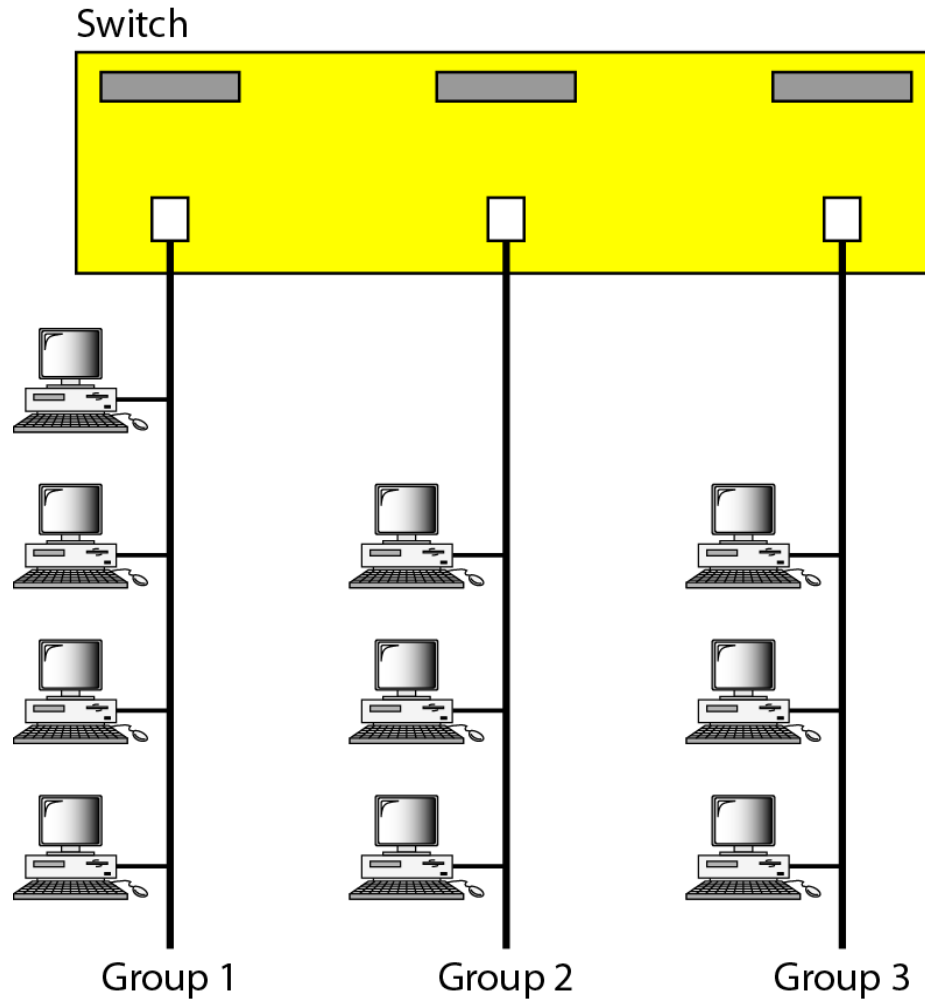
Configuration 配置

Communication between Switches 交换机间的通信

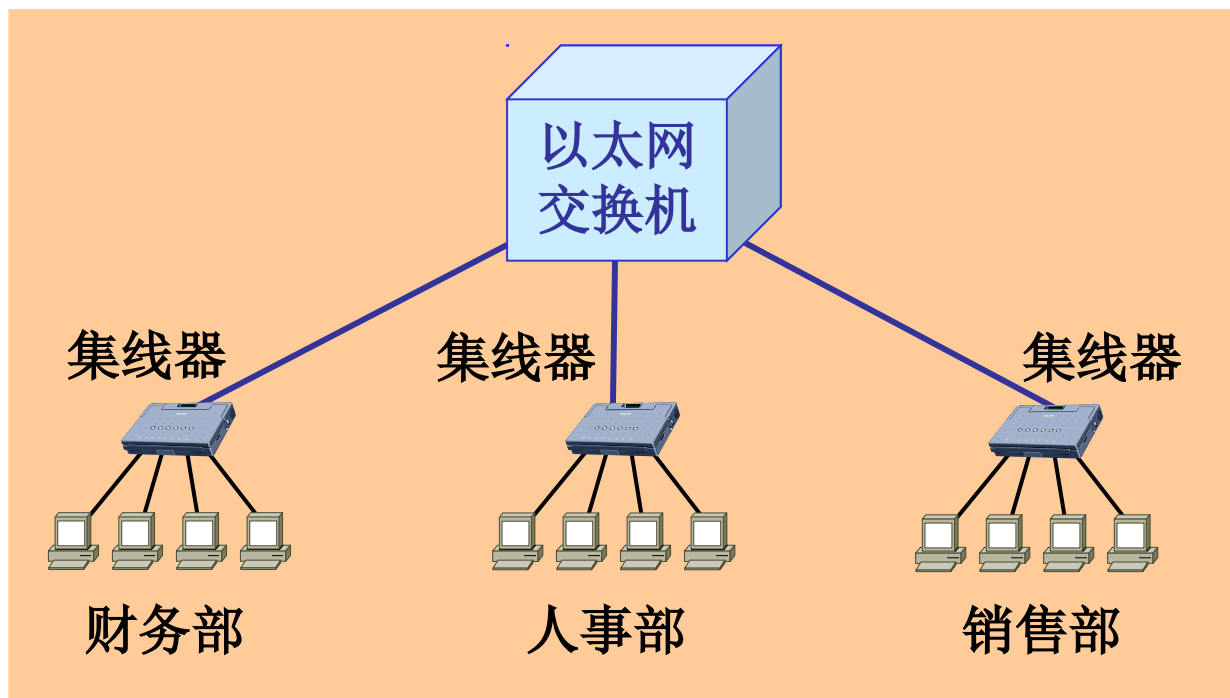
IEEE Standard IEEE 标准

Advantages 优点

Figure 15.15 连接三个 LAN 的交换机



3 个冲突域和 1 个广播域



- 以太网交换机将连接在不同端口的主机分隔成独立的冲突域，但这些网络仍然处在一个共同的广播域中。
- VLAN 以局域网交换技术为基础，通过交换机内部的软件功能，实现将网络中的主机按照功能、应用或部门等因素构成虚拟的工作组或逻辑网段，这些逻辑网段分别拥有独立的冲突域和广播域。

Figure 15.16 使用 VLAN 的交换机

Switch with VLAN software

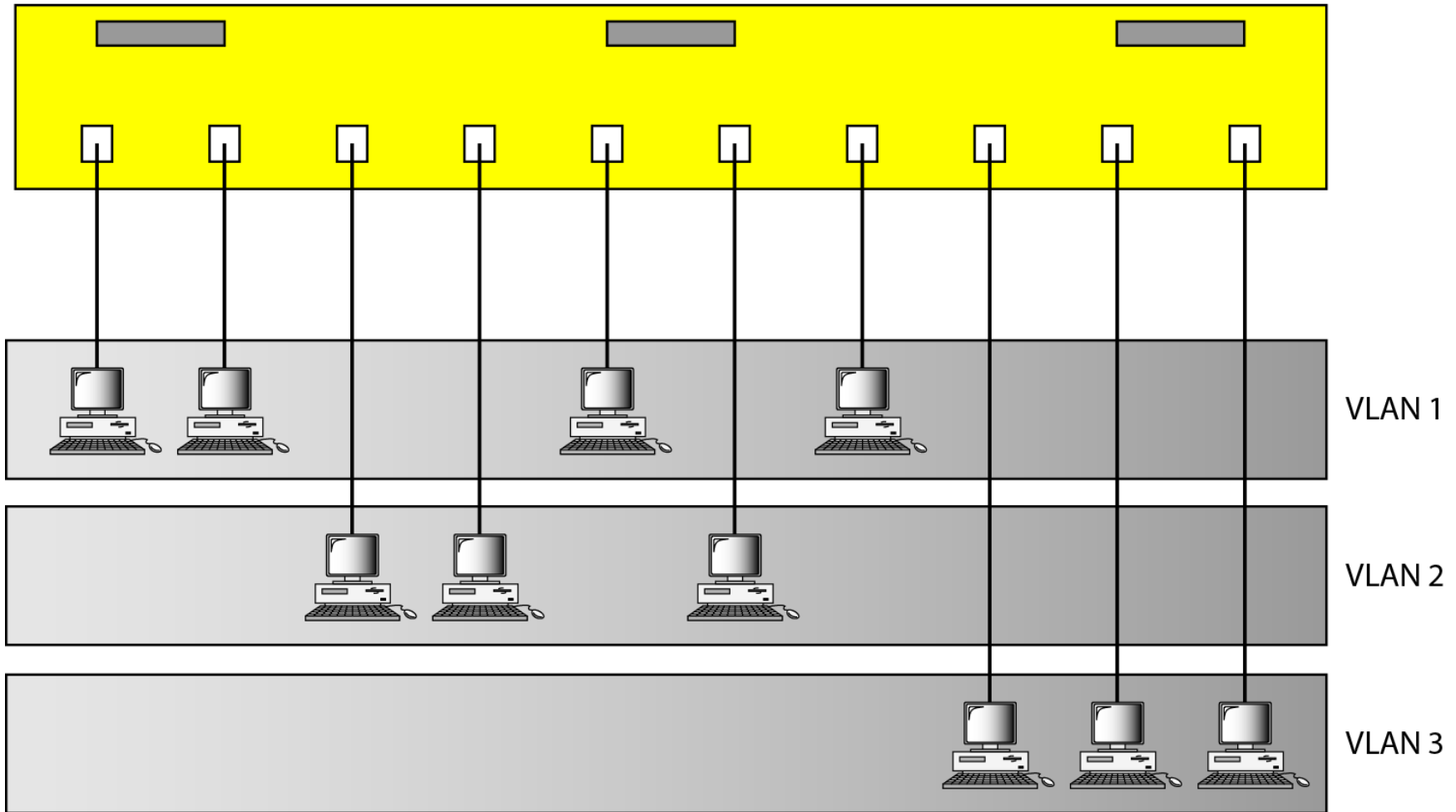
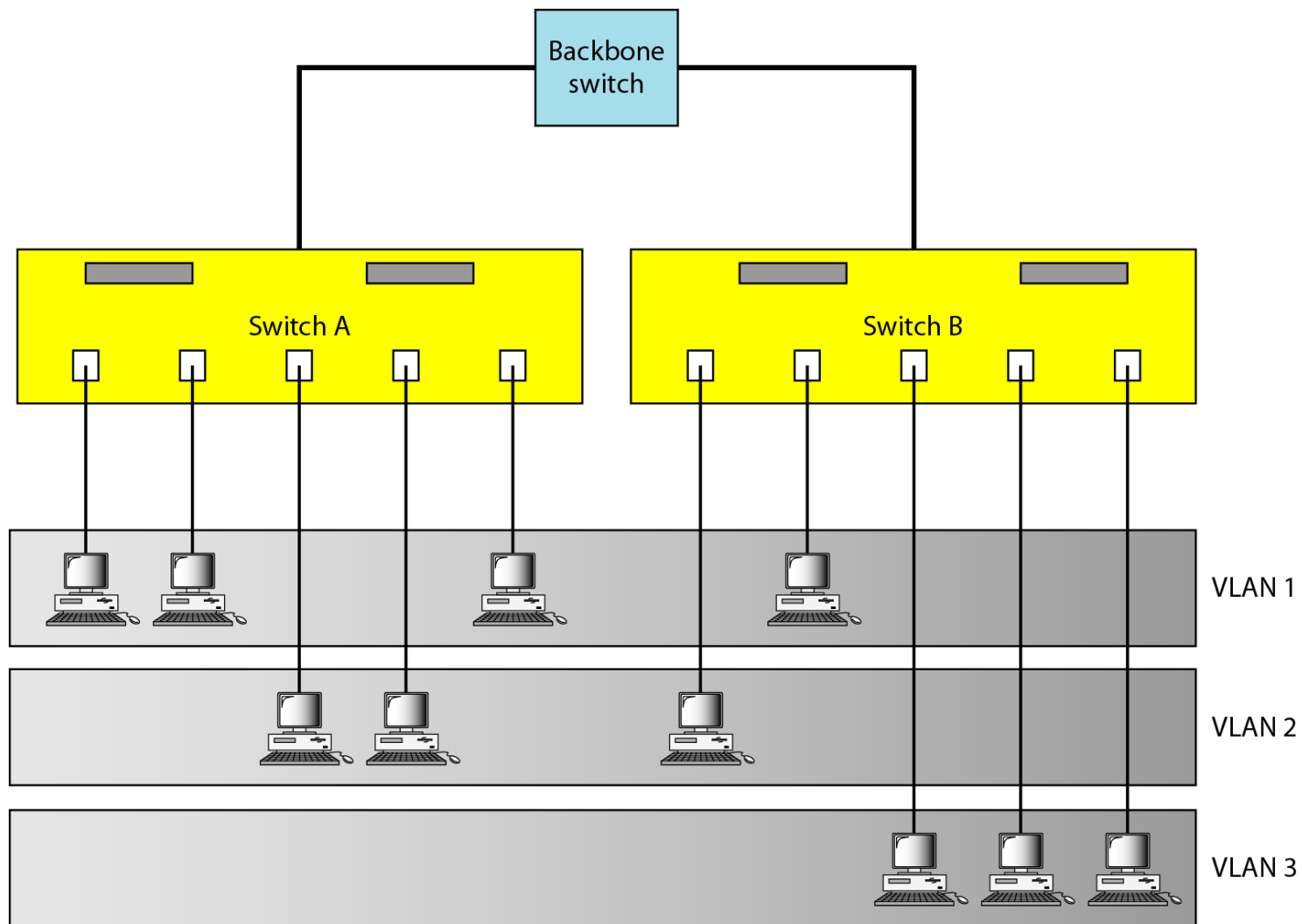


Figure 15.17 主干网中使用 VLAN 的交换机



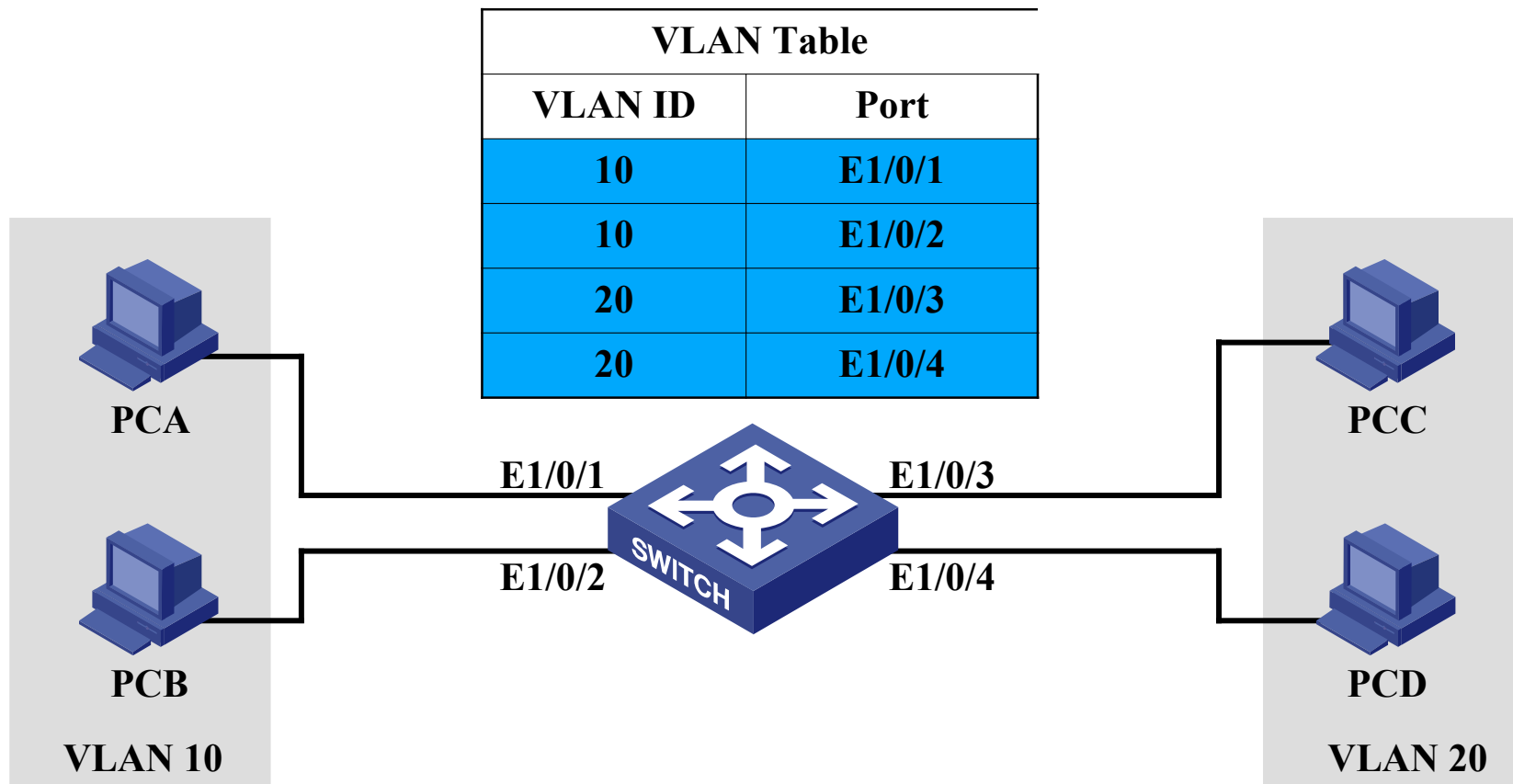
VLAN 的特点

- 将 LAN 划分成逻辑的而不是物理的网段；
- 一个 LAN 可以划分成多个 VLAN，每个 VLAN 是一个工作组；
- 允许连接在不同交换机上的站点组成一个 VLAN；
- VLAN 将属于一个或多个物理 LAN 的站点分组到一个广播域中；
- 同一 VLAN 中的站点通信时就像它们属于一个物理网段一样。

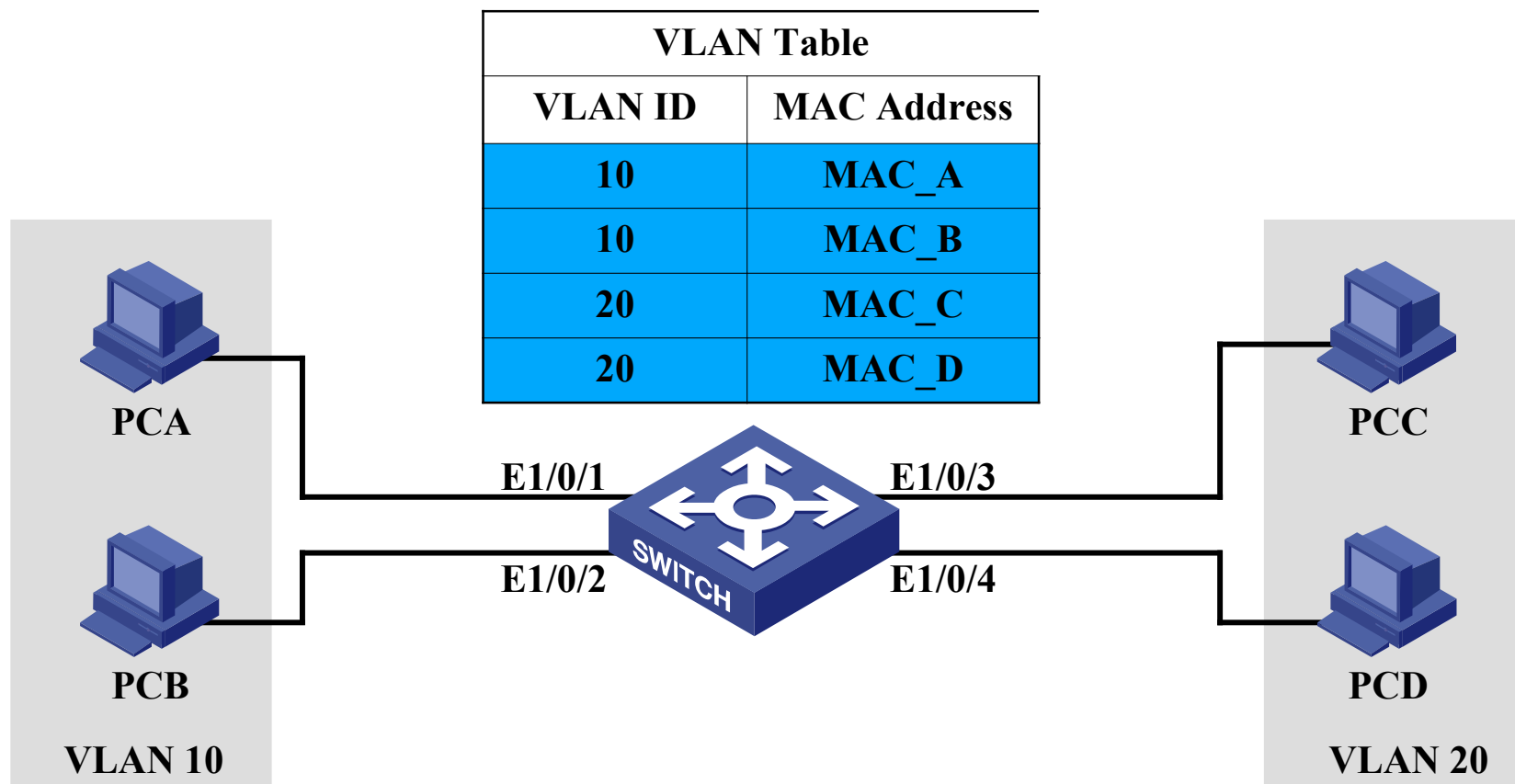
VLAN 的划分方式

- 基于端口：使用交换机的端口号
- 基于 MAC 地址：使用 48 位 MAC 地址
- 基于第三层协议：如使用 IP 地址
- 基于组播组：使用多播 IP 地址

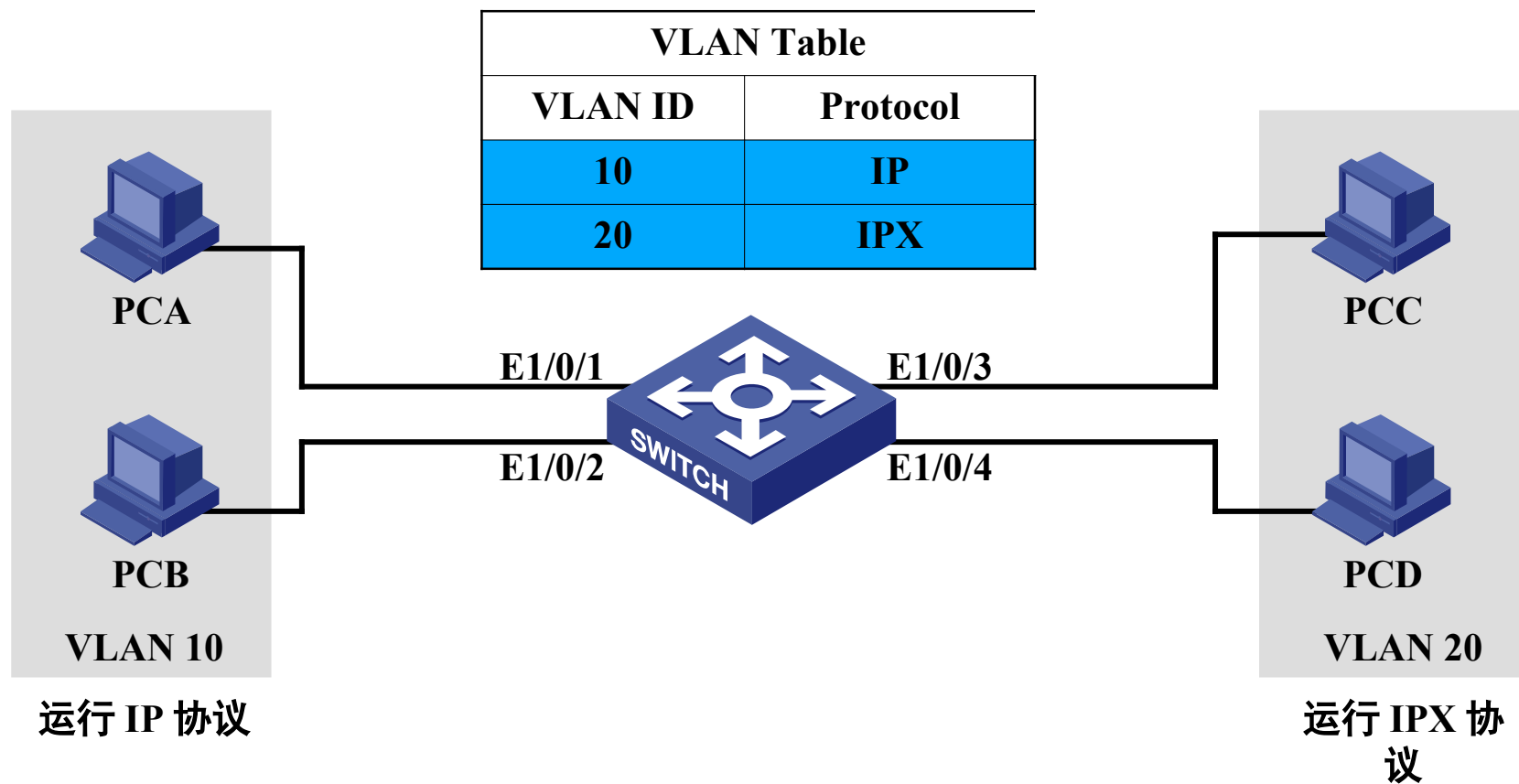
基于端口的 VLAN



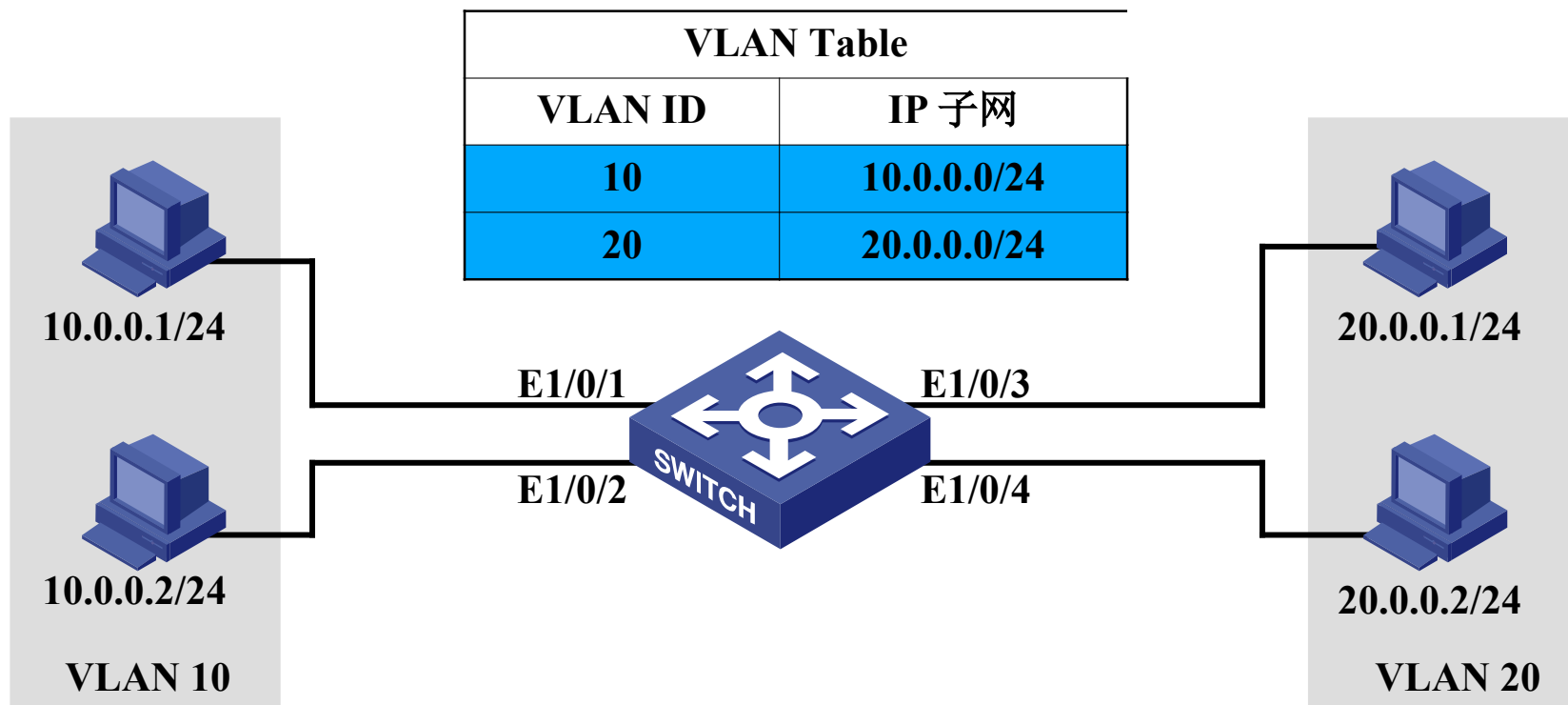
基于 MAC 地址的 VLAN



基于协议的 VLAN



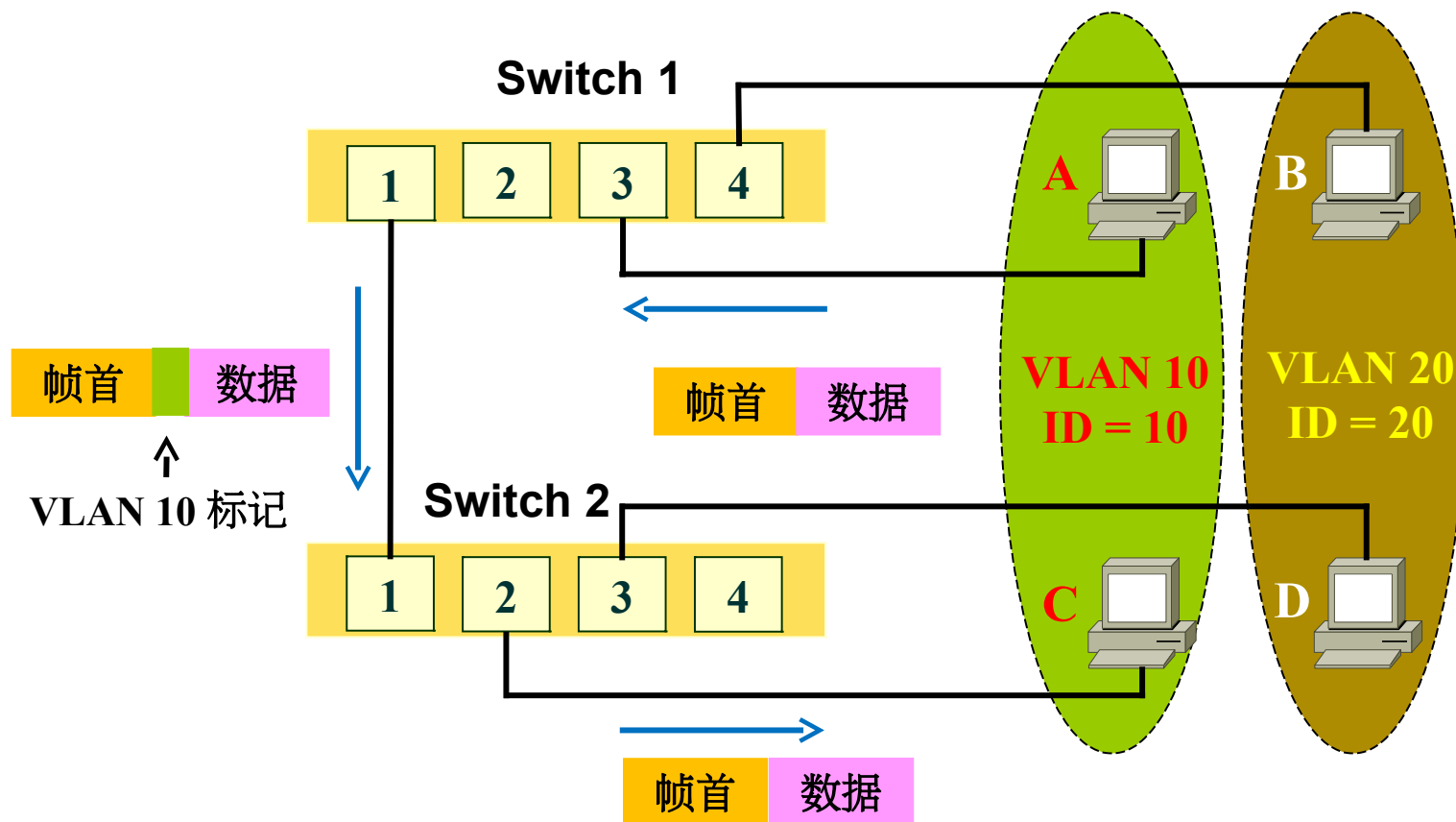
基于子网的 VLAN



默认 VLAN

- 默认 VLAN 是交换机初始就有的 VLAN，通常 ID 为 1，所有接口都处于这个 VLAN 下，这就是设备连接到交换机以后就能互相通信的原因。
 - 。
- VLAN ID 最多总共有 $2^{12} = 4096$ 个（0 - 4095），其中 VLAN 0 和 VLAN 4095 为保留，只在特定的情况下使用。

端口划分 VLAN 数据帧转发过程



有标记帧和无标记帧

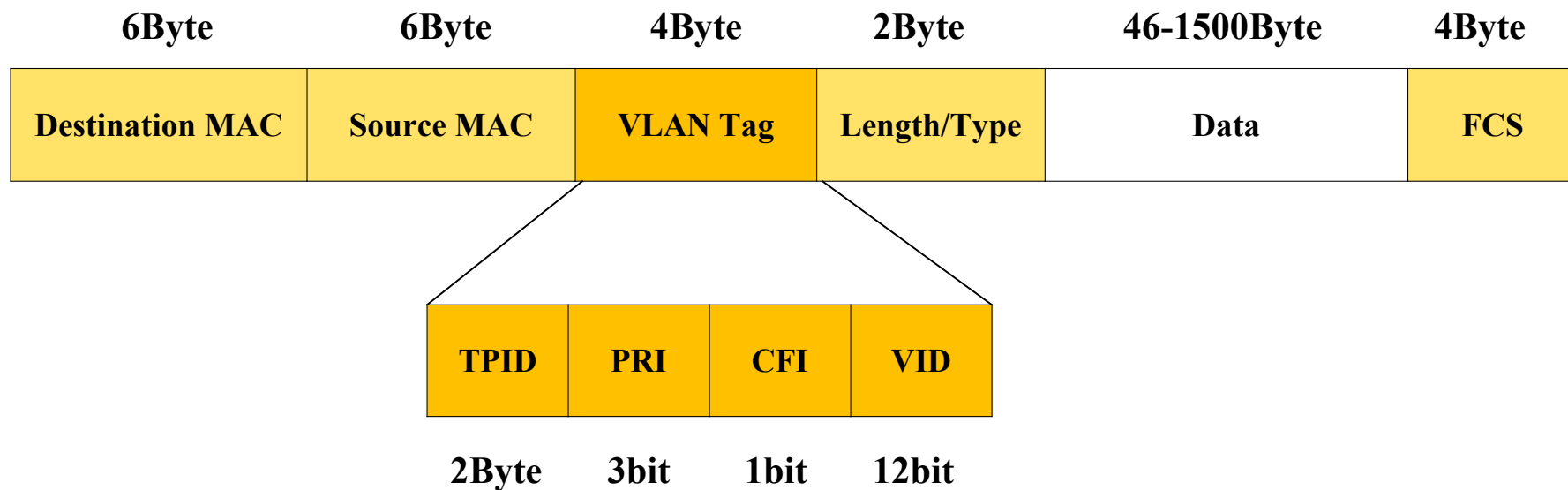
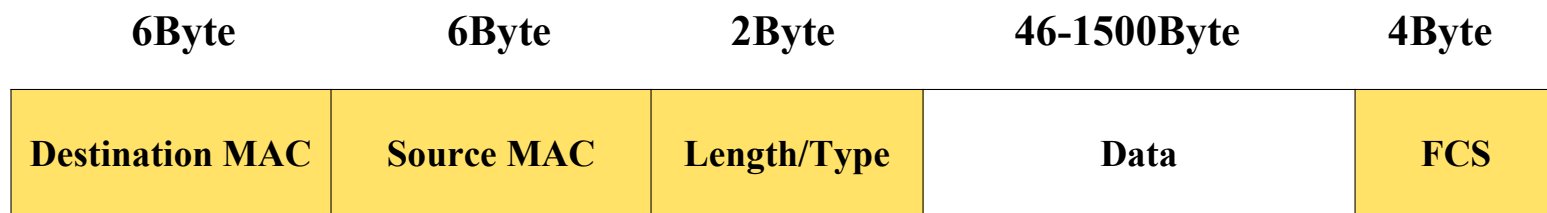
在一个 VLAN 交换网络中，以太网帧主要有以下两种形式：

- 有标记帧（ Tagged ）：加入了 4 字节 VLAN 标签的帧。
- 无标记帧（ Untagged ）：原始的、未加入 4 字节 VLAN 标签的帧。

以太网链路包括接入链路和干道链路：

- 接入链路（ Access Link ）用于连接交换机和用户终端（用户主机、服务器、傻瓜交换机等），只可以承载 1 个 VLAN 的数据帧。在接入链路上传输的帧都是 Untagged 帧。
- 干道链路（ Trunk Link ）用于交换机间互连或连接交换机与路由器，可以承载多个不同 VLAN 的数据帧。在干道链路上传输的数据帧都是 Tagged 帧。

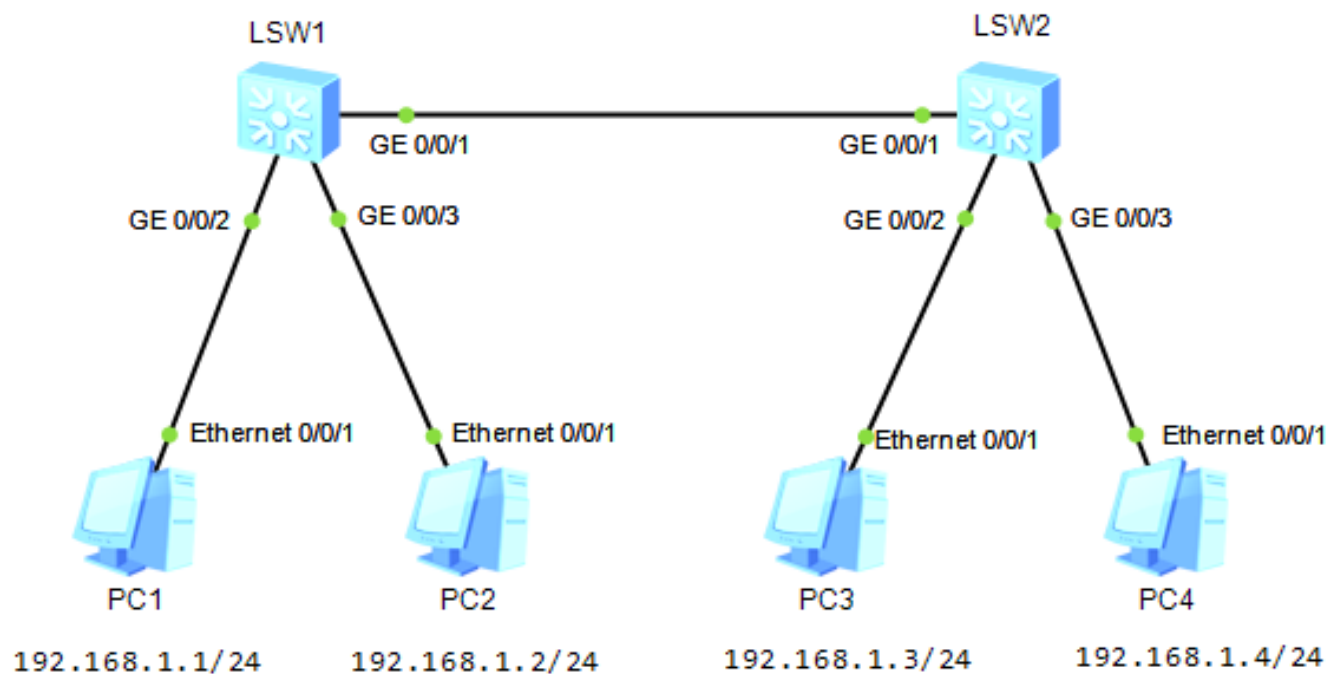
IEEE 802.1Q 协议和帧格式



IEEE 802.1Q 协议和帧格式

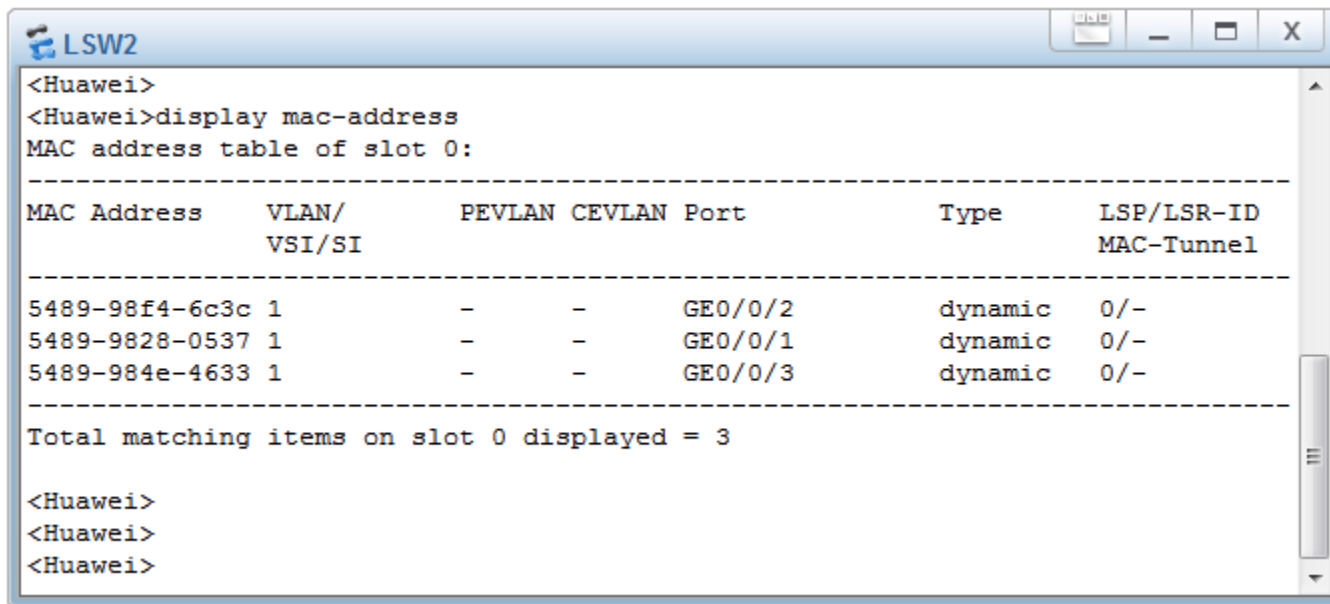
- TPID : Tag Protocol Identifier (标签协议标识符), 表示数据帧的类型。取值为 0x8100 表示该帧是 IEEE 802.1Q 的 VLAN 数据帧。
- PRI : Priority, 表示数据帧的 802.1p 优先级。取值范围为 0-7, 值越大优先级越高, 交换机拥塞时优先发送优先级高的数据帧。
- CFI : Canonical Format Indicator (标准格式指示位), 表示 MAC 地址在不同的传输介质中是否以标准格式封装, 用于兼容以太网和令牌环网。1 表示以非标准格式封装, 在以太网中, CFI 为 0。
- VID : VLAN ID, 数据帧所属的 VLAN 的编号, VLAN ID 取值范围为 0 - 4095。因为 0 和 4095 为协议保留值, 所以 VLAN ID 的有效范围是 1 - 4094。
- PRI、CFI 和 VID 统称为标签控制信息 (Tag Control Information)

实验 1 创建 MAC 地址表



查看 MAC 地址表

用 PC1 分别 ping 另外 3 台 PC，然后查看 LSW2 的 MAC 地址表。

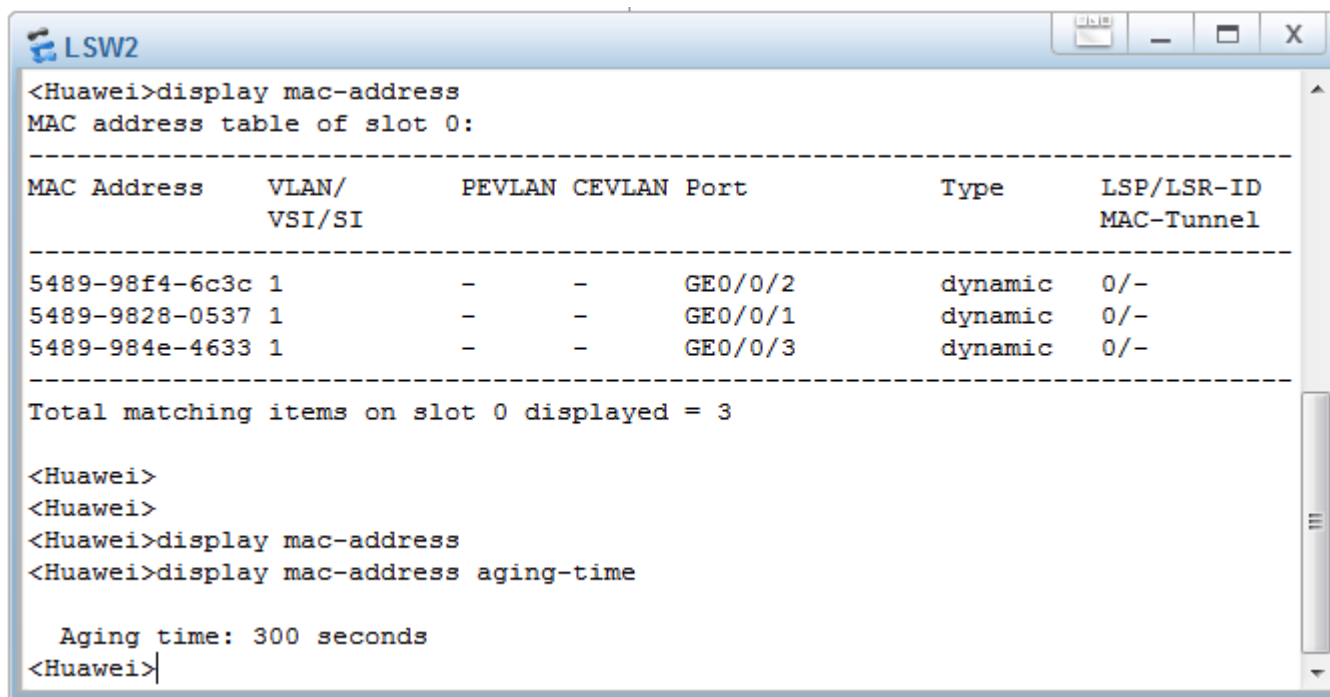


```
<Huawei>
<Huawei>display mac-address
MAC address table of slot 0:
-----
MAC Address      VLAN/      PEVLAN CEVLAN Port      Type      LSP/LSR-ID
                  VSI/SI
-----
5489-98f4-6c3c 1          -      -      GE0/0/2      dynamic   0/-
5489-9828-0537 1          -      -      GE0/0/1      dynamic   0/-
5489-984e-4633 1          -      -      GE0/0/3      dynamic   0/-
-----
Total matching items on slot 0 displayed = 3

<Huawei>
<Huawei>
<Huawei>
```

查看 MAC 地址表的老化时间

查看 LSW2 的 MAC 地址表老化时间，经过 300 秒后 MAC 地址表被删除。这种机制有利于正确反映当前 MAC 地址与端口的映射关系，并减少查找时间。



```
<Huawei>display mac-address
MAC address table of slot 0:

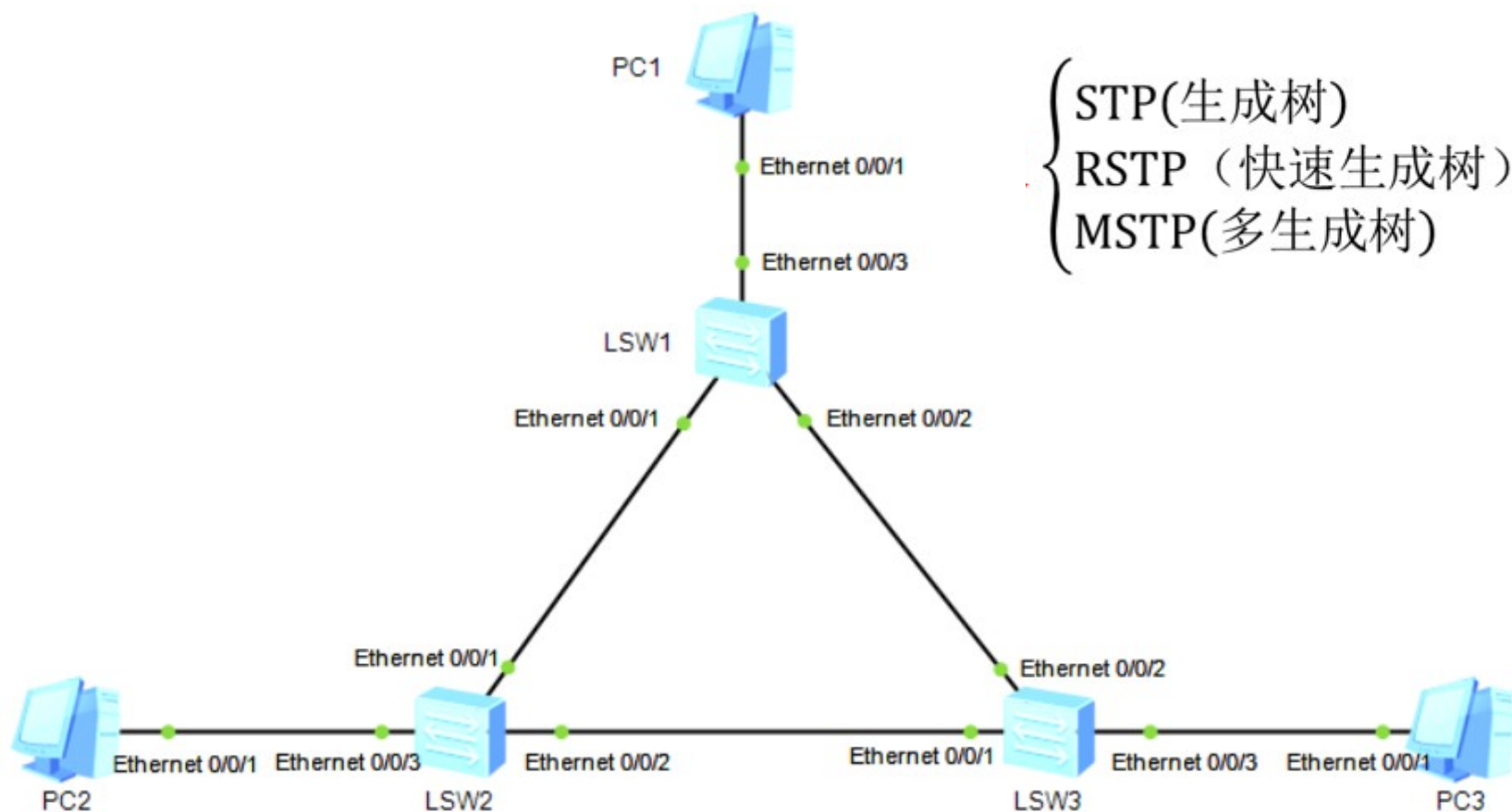
-----
MAC Address      VLAN/      PEVLAN CEVLAN Port      Type      LSP/LSR-ID
                  VSI/SI
-----
5489-98f4-6c3c 1          -      -      GE0/0/2      dynamic   0/-
5489-9828-0537 1          -      -      GE0/0/1      dynamic   0/-
5489-984e-4633 1          -      -      GE0/0/3      dynamic   0/-
-----

Total matching items on slot 0 displayed = 3

<Huawei>
<Huawei>
<Huawei>display mac-address
<Huawei>display mac-address aging-time

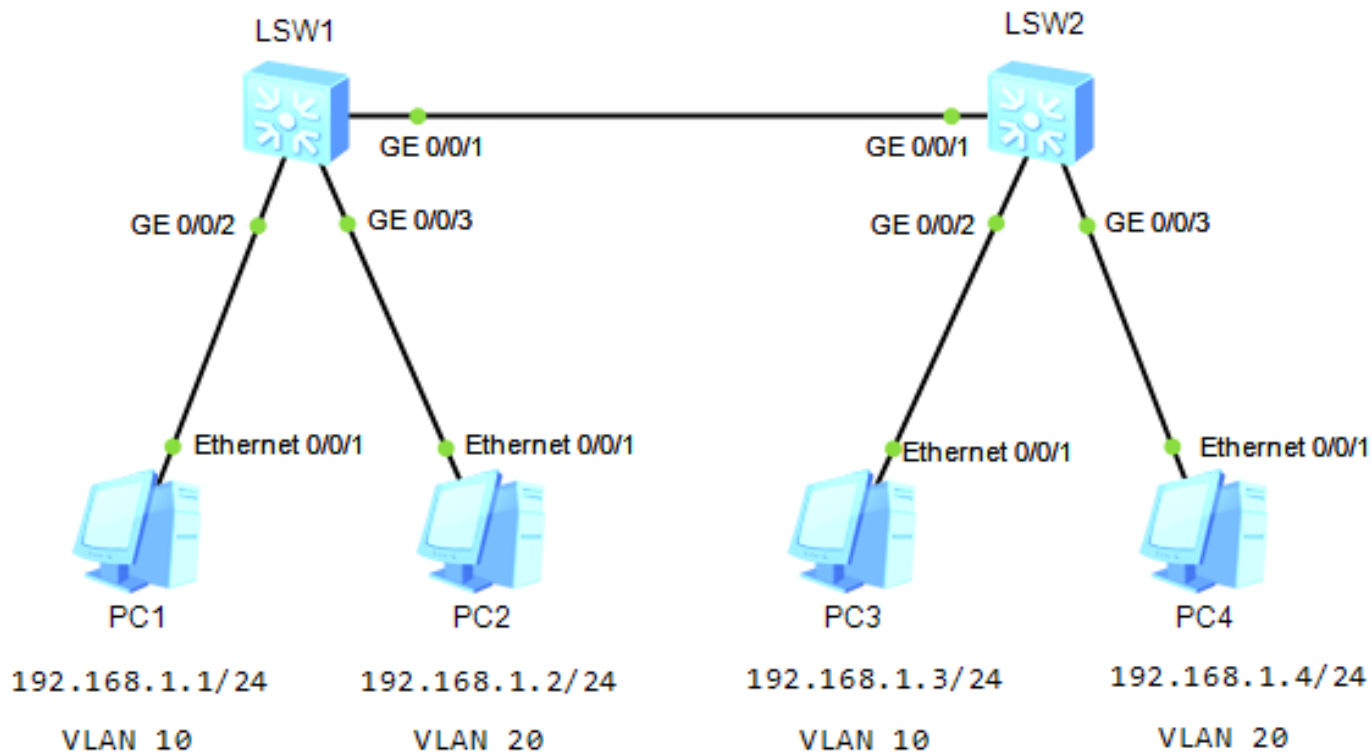
Aging time: 300 seconds
<Huawei>
```

实验 2 生成树实验



用 `dis stp brief` 查看并抓包

实验 3 VLAN 实验



- ◆ 未创建 VLAN 时，4 台 PC 彼此间可以通信。
- ◆ 创建 VLAN 后，只有属于同一 VLAN 的 PC 才能通信。

配置二层交换机

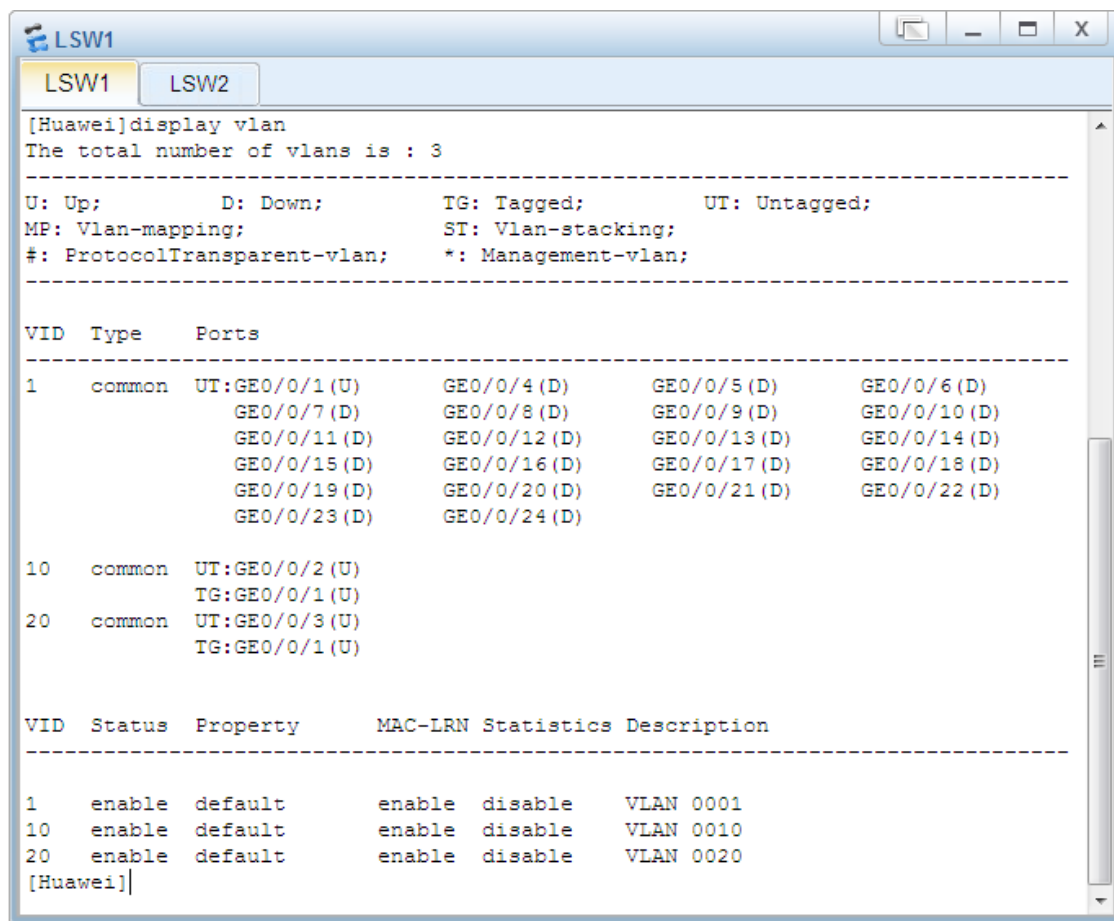
两台交换机进行相同配置：

```
<Huawei>system-view
[Huawei]undo info-center enable
[Huawei]vlan batch 10 20
[Huawei]int g0/0/1
[Huawei-GigabitEthernet0/0/1]port link-type trunk
[Huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
[Huawei-GigabitEthernet0/0/1]quit
[Huawei]int g0/0/2
[Huawei-GigabitEthernet0/0/2]port link-type access
[Huawei-GigabitEthernet0/0/2]port default vlan 10
[Huawei-GigabitEthernet0/0/2]quit
[Huawei]int g0/0/3
[Huawei-GigabitEthernet0/0/3]port link-type access
[Huawei-GigabitEthernet0/0/3]port default vlan 20
[Huawei-GigabitEthernet0/0/3]quit
[Huawei]
```


查看 VLAN

使用命令 `display vlan` 查看已创建的 VLAN，并抓包查看 VLAN 帧

。



```
[Huawei]display vlan
The total number of vlans is : 3

-----
U: Up;           D: Down;           TG: Tagged;       UT: Untagged;
MP: Vlan-mapping; ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
-----

VID  Type    Ports
-----
1    common  UT:GEO/0/1 (U)    GEO/0/4 (D)    GEO/0/5 (D)    GEO/0/6 (D)
                        GEO/0/7 (D)    GEO/0/8 (D)    GEO/0/9 (D)    GEO/0/10 (D)
                        GEO/0/11 (D)   GEO/0/12 (D)   GEO/0/13 (D)   GEO/0/14 (D)
                        GEO/0/15 (D)   GEO/0/16 (D)   GEO/0/17 (D)   GEO/0/18 (D)
                        GEO/0/19 (D)   GEO/0/20 (D)   GEO/0/21 (D)   GEO/0/22 (D)
                        GEO/0/23 (D)   GEO/0/24 (D)
10   common  UT:GEO/0/2 (U)
                        TG:GEO/0/1 (U)
20   common  UT:GEO/0/3 (U)
                        TG:GEO/0/1 (U)

VID  Status  Property      MAC-LRN Statistics  Description
-----
1    enable  default      enable  disable  VLAN 0001
10   enable  default      enable  disable  VLAN 0010
20   enable  default      enable  disable  VLAN 0020
[Huawei]
```

实验 4 交换机实现 VLAN 间通信

