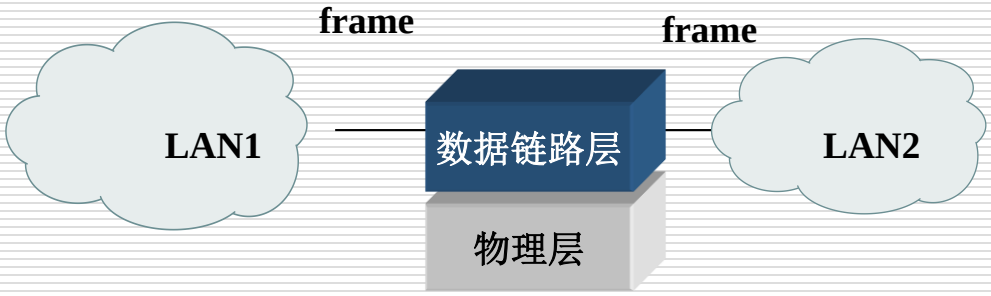
第四章 介质访问控制子层（三）

袁华，hyuan@scut.edu.cn
华南理工大学计算机科学与工程学院
广东省计算机网路重点实验室

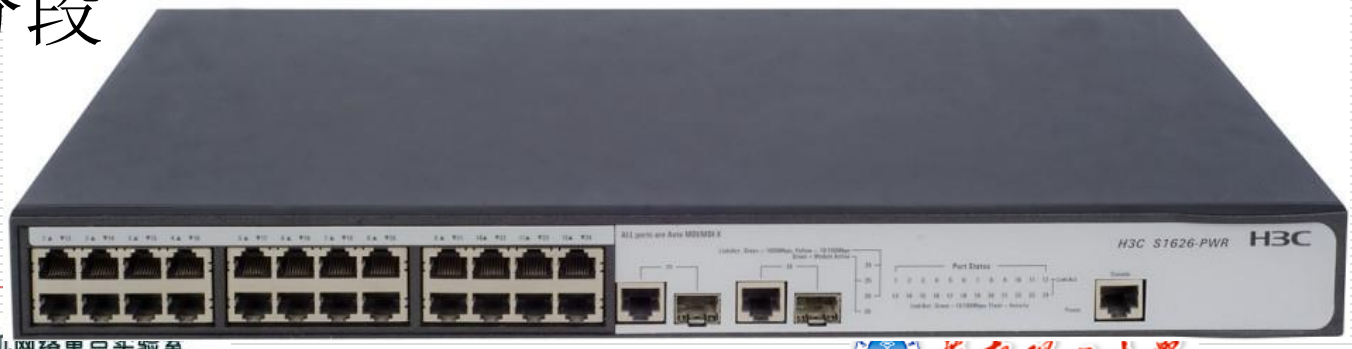
数据链路层网络互连的基本概念

- 广播式网络的最大传输距离和可容纳最大站点数量决定了网络要分段。
- 用同一传输介质连接起来的站点的集合称为一个网段。
- 局域网间数据帧交换称为L2交换。
- L2交换设备是网桥/交换机。



本节主要内容

- 了解数据链路层交换特点
- 了解二层设备及桥接、交换技术
- 掌握网桥/交换机的工作原理
- 理解交换机的三种交换方法及特点
- 了解微分段



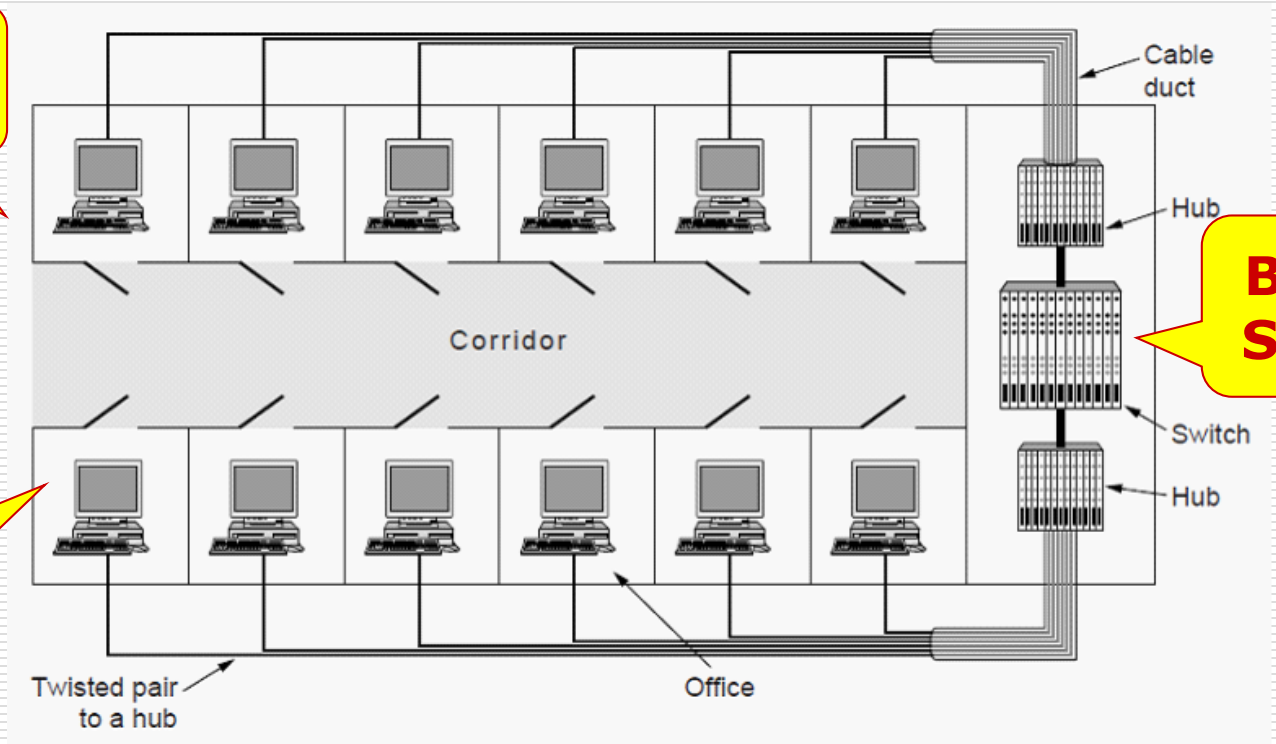
为什么有多个LAN？ P257~258

- 各个部门的目标不一样，建设的LAN网络也可能不一样
- 一个组织可能分布在几栋大楼，这些大楼之间有一定的地理距离，每个楼可能有一个独立的LAN
- 为了适应网络的负载，有可能将一个LAN分割成若干个LAN
- 同个LAN中的最远工作站之间的物理距离可能太远（如，以太网2500米）
- 为了提升网络的性能
- 网桥能够提供一定的安全性能

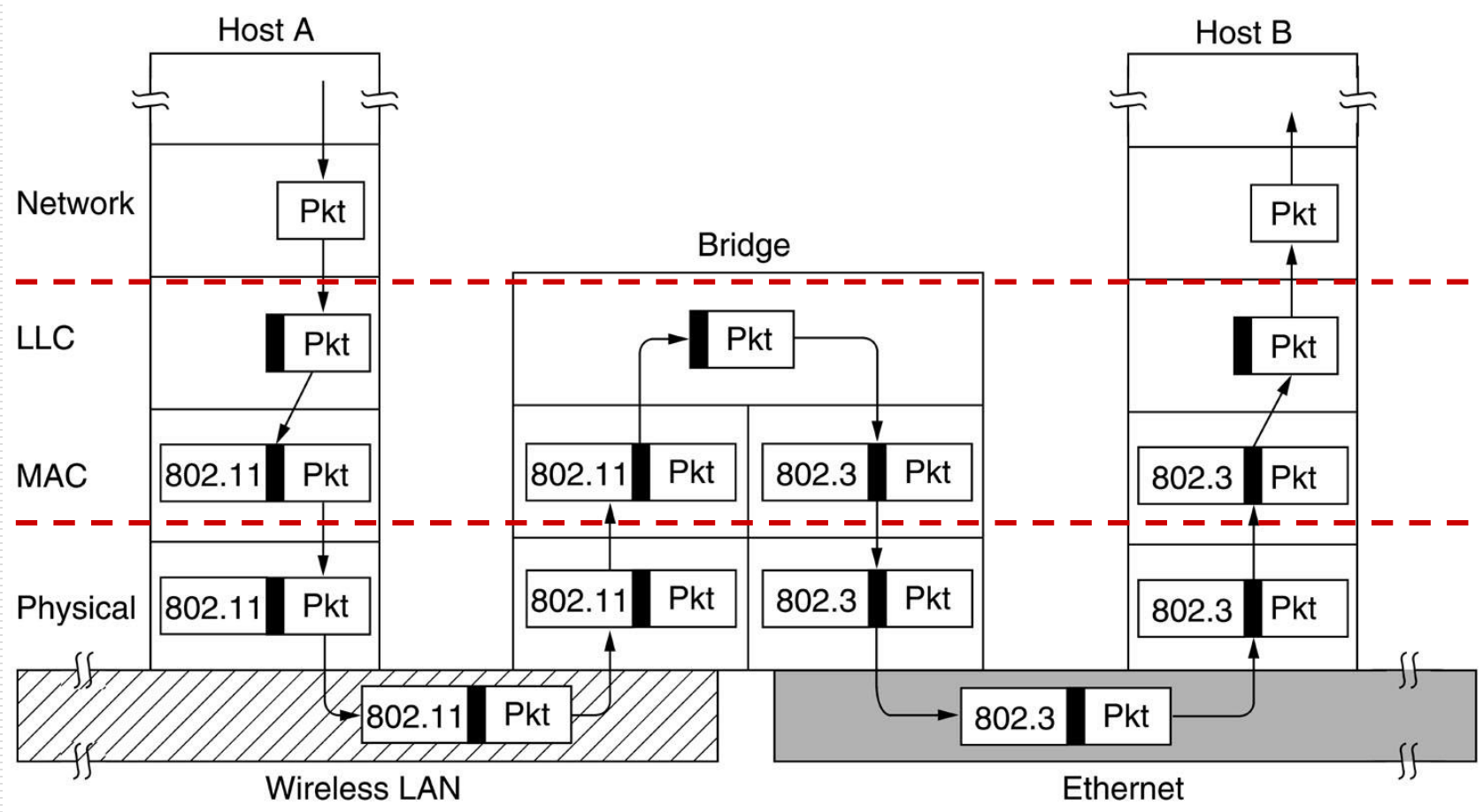
数据链路层交换P256

- 有很多LAN，如何将它们连接起来？
  - 可用网桥（bridges ）将它们连接起来。
- 网桥工作在DLL层，通过检查MAC地址做出转发帧的决策
  - 不会检查网络层，所以，IPv4, IPv6, AppleTalk, ATM, IPX, and OSI 分组均可穿越网桥。
- 路由器和网桥不同
  - 检查逻辑地址（如IP地址）作出分组转发的决策

网桥链接LAN网段


LAN1
LAN2
Cable duct
Hub
Bridges/ Switches
Corridor
Switch
Hub
Twisted pair to a hub
Office

从 802.11 到 802.3 的网桥操作



从 802.X 到 802.Y的网桥

- 遇到的问题：
  - 不同的帧格式 – 重新封装
  - 不同的数据传输速率 - Buffering.
  - 不同的802LAN有不同的最大帧长度 （如， 802.3 1526 字节, 802.11 2346 字节）
  - 安全： 802.11 和 802.16 支持数据链路层的加密，但 802.3 不支持
  - 服务质量：802.11 和 802.16 提供了服务质量，但 802.3 没有

透明的网桥 P257

- 通过透明网桥（transparent bridges ）将多个LAN连接起来，硬件和软件不需要做任何的变化
- 透明网桥工作在混杂模式（promiscuous mode ），它接收所有跟它相联的LAN的帧
- 当一个帧到达网桥时，它必须作出丢弃（discard）还是转发（ forward ）的决策，如果是转发，它还要知道向哪个LAN转发
- 决策是通过在网桥内部的一张地址表（hash table）中查找目的MAC地址而作出的

怎样透明？

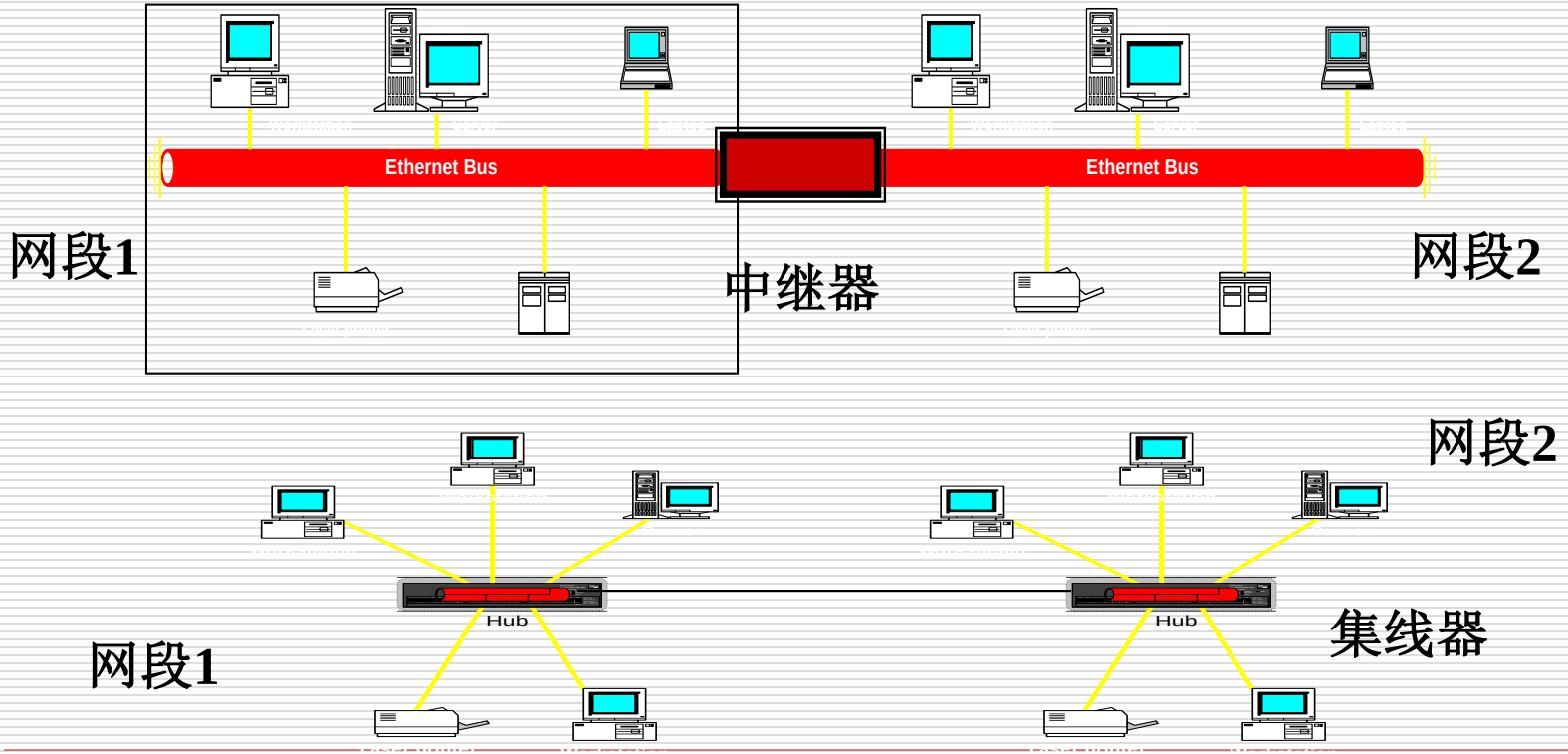
- 网桥如何维护它的内部转发表？
- 初始时，这张表是空的
- 扩散算法（泛洪算法，flooding algorithm）
  - 当网桥不知道目的地址时（表中查不到），它会将这帧从除来的LAN外的所有LAN转发出去
- 逆向学习（backward learning）
  - 网桥从到达帧的源地址认识到源地址对应的那台机是在帧来的那个LAN上，所以，把它写入MAC地址表
- 但是拓扑是变化的，网桥怎样适应这种变化？
  - 无论何时，凡往表中加入记录，也必须同时打下时戳
  - 到达帧的源地址在表中已有记录，将时戳更新为当前时间
  - 网桥周期性地扫描表，将那些超时的记录从表中删除

网桥工作原理

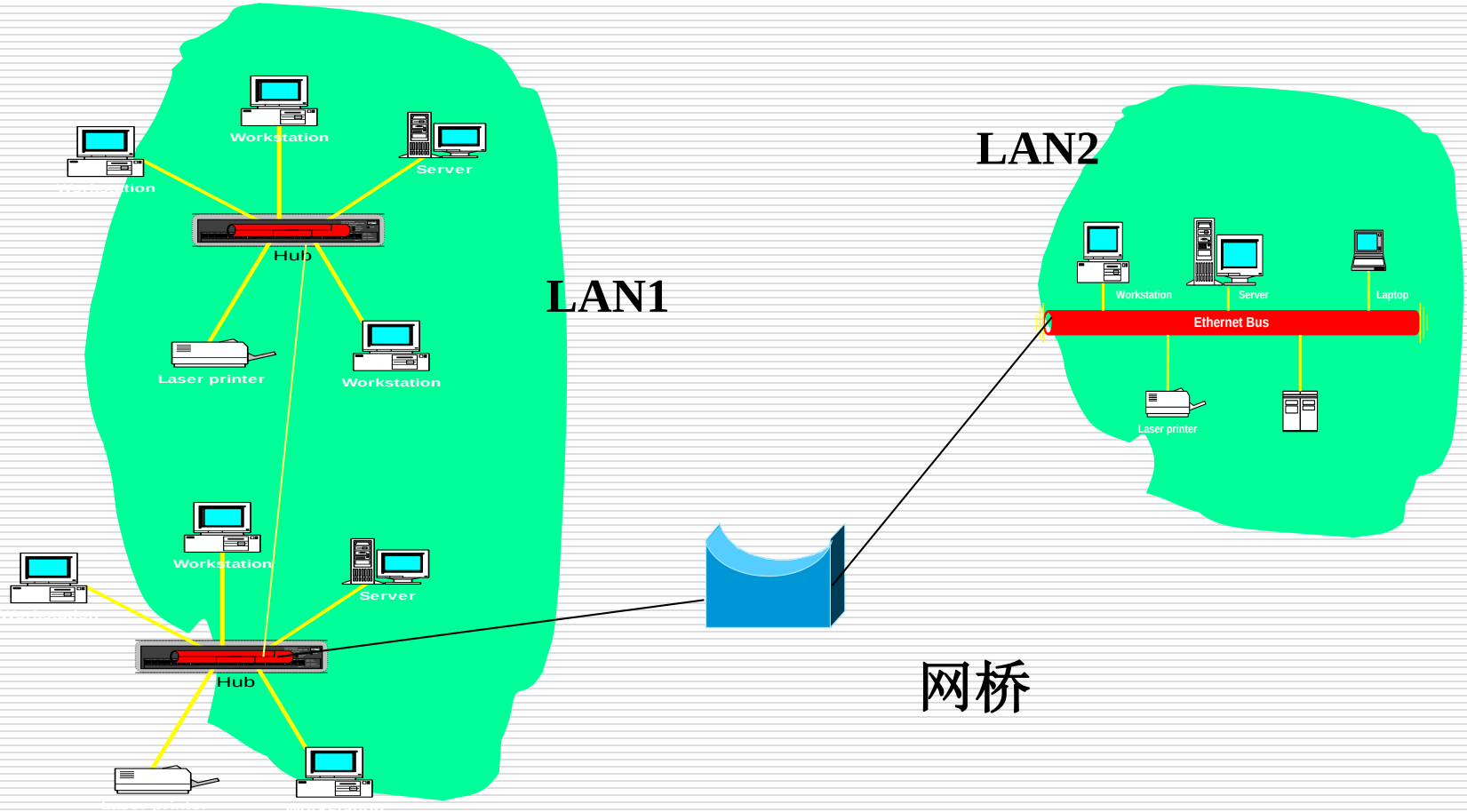
- 当一帧到达时，网桥启动如下算法：P259
  - 如果源LAN和目的LAN相同，则丢弃该帧；
  - 如果源LAN和目的LAN不同，则转发该帧；
  - 如果目的LAN未知，则广播该帧。
- 每当一帧到达，上述算法都将执行一遍
- 有些专用的 VLSI 芯片可以在几微秒内完成查找和更新表项的动作

冲突域的概念

一个网段，或用中继器/集线器连接的多网段，称为冲突域。



二层设备可以隔离冲突域

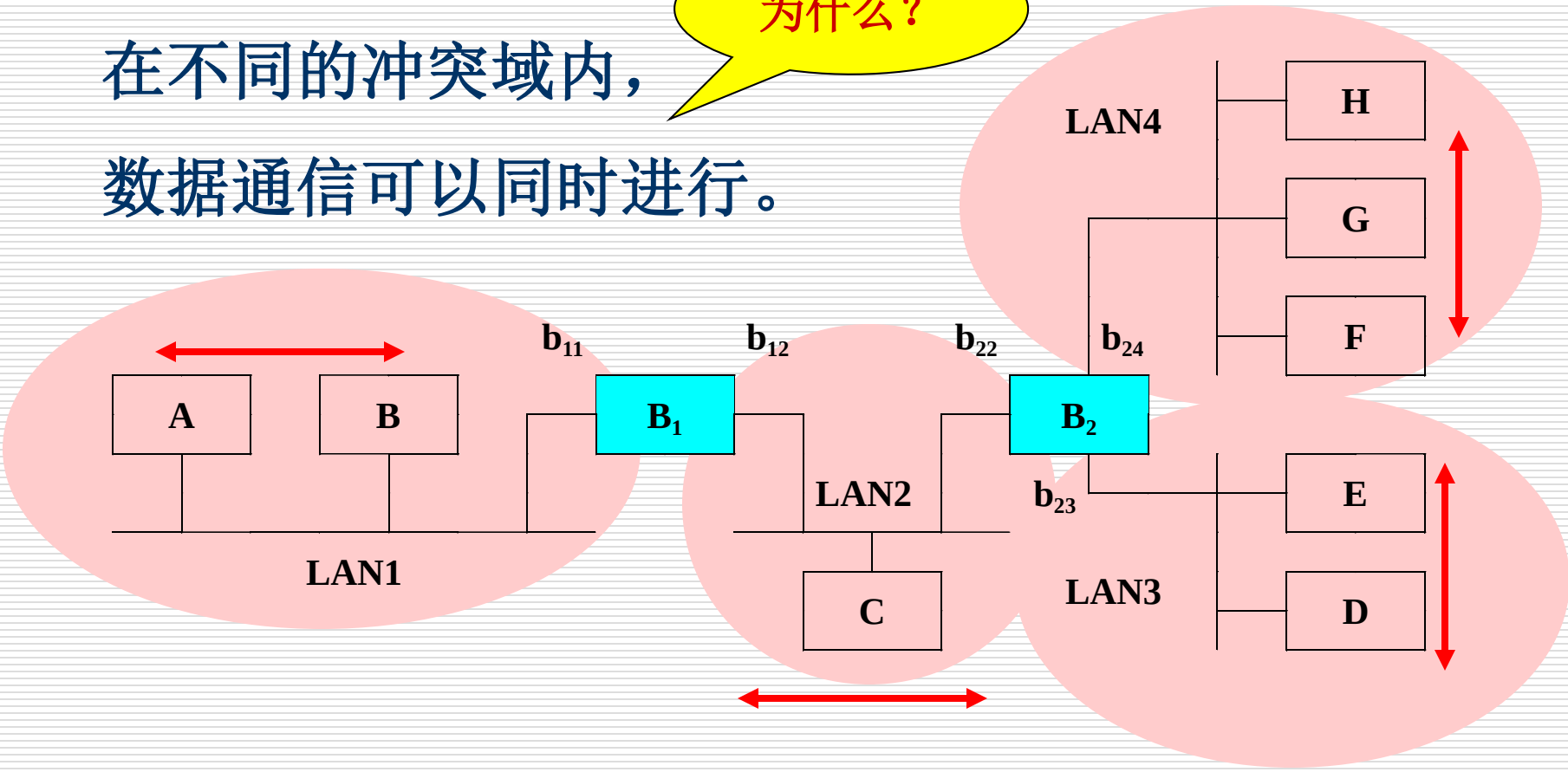


透明网桥举例

为什么？

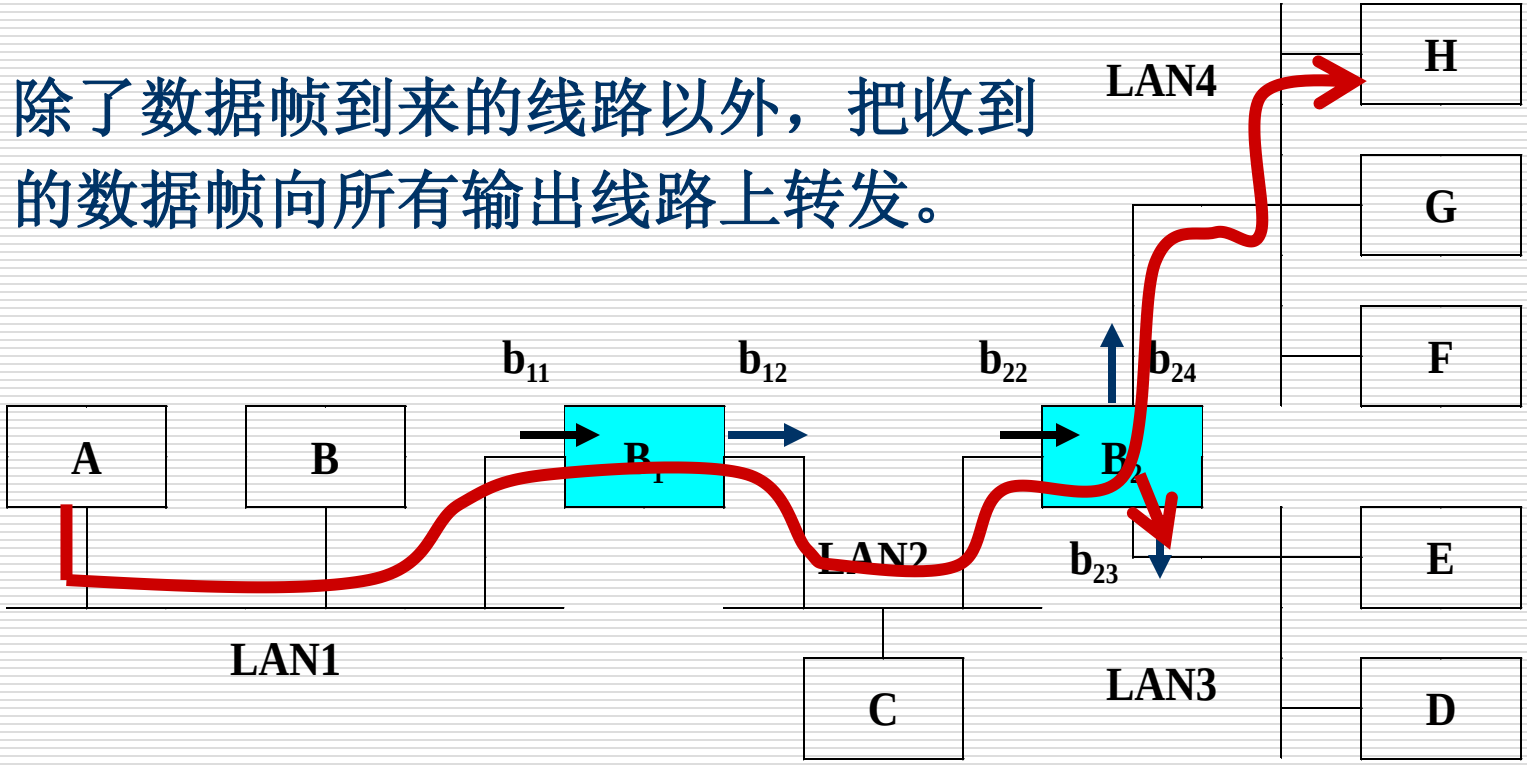
在不同的冲突域内，

数据通信可以同时进行。



帧跨网络传输：扩散（Flooding）

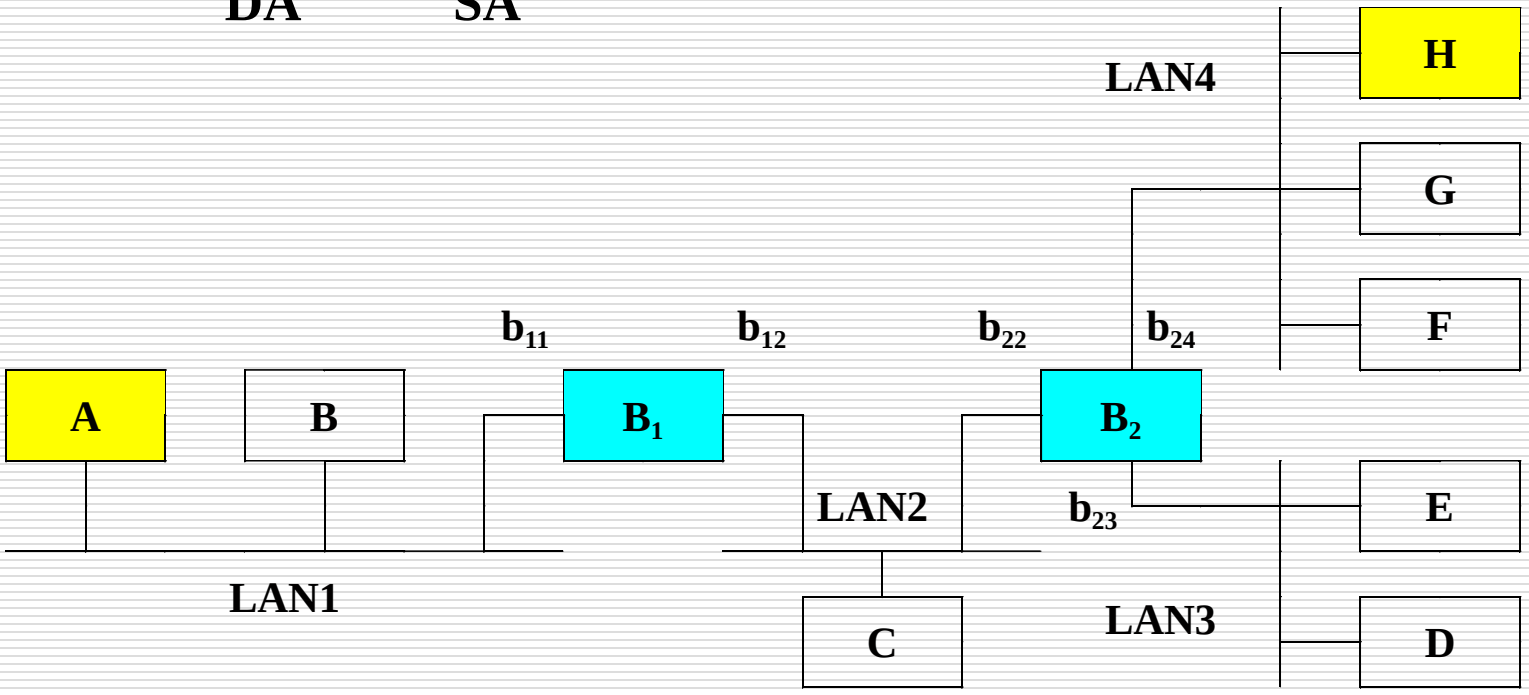
除了数据帧到来的线路以外，把收到的数据帧向所有输出线路上转发。



步骤1： A向H发送数据帧Fa

先导	11	H	A	类型	数据	校验和
		DA	SA			

帧Fa

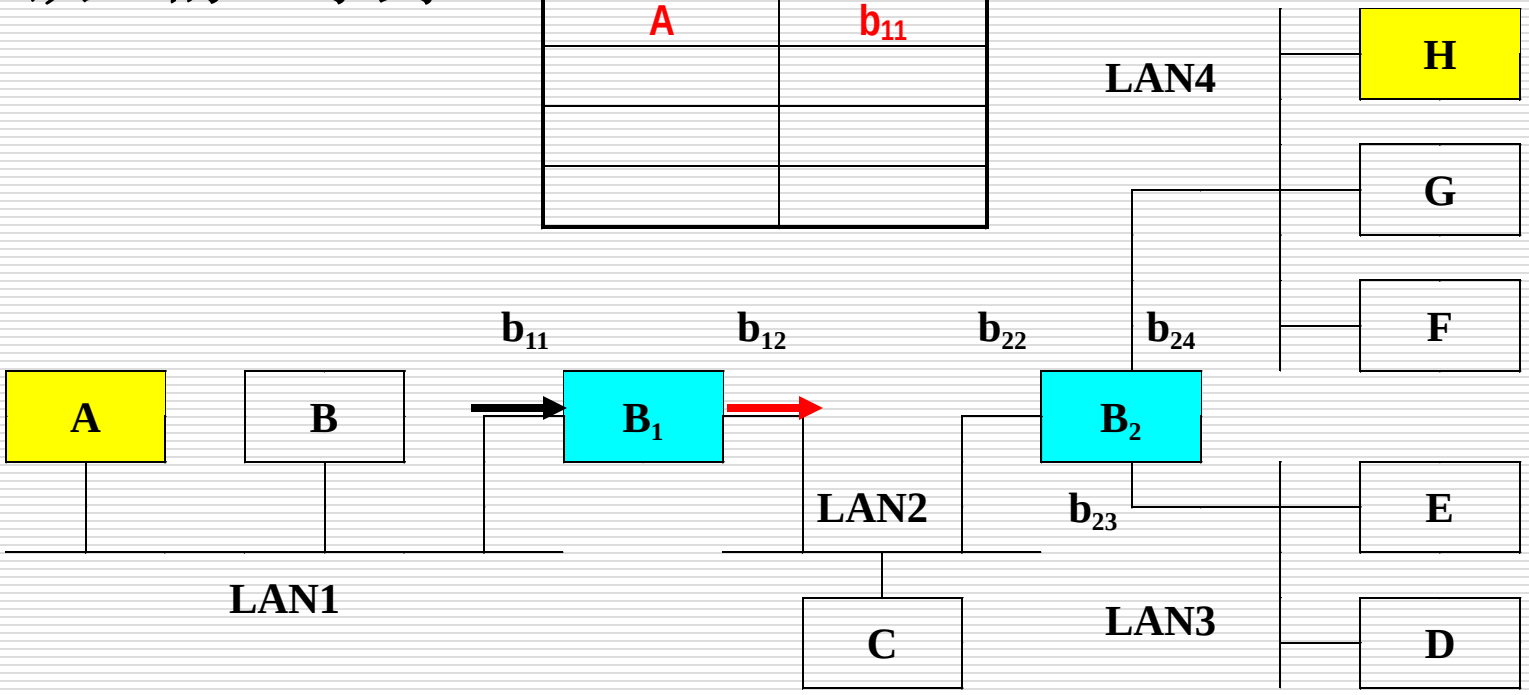


步骤2：网桥B1扩散帧Fa

- B1从b11接收帧Fa，从b12向LAN2扩散帧Fa

- **B1从Fa的SA学到A**

MAC	Port #
A	b_{11}



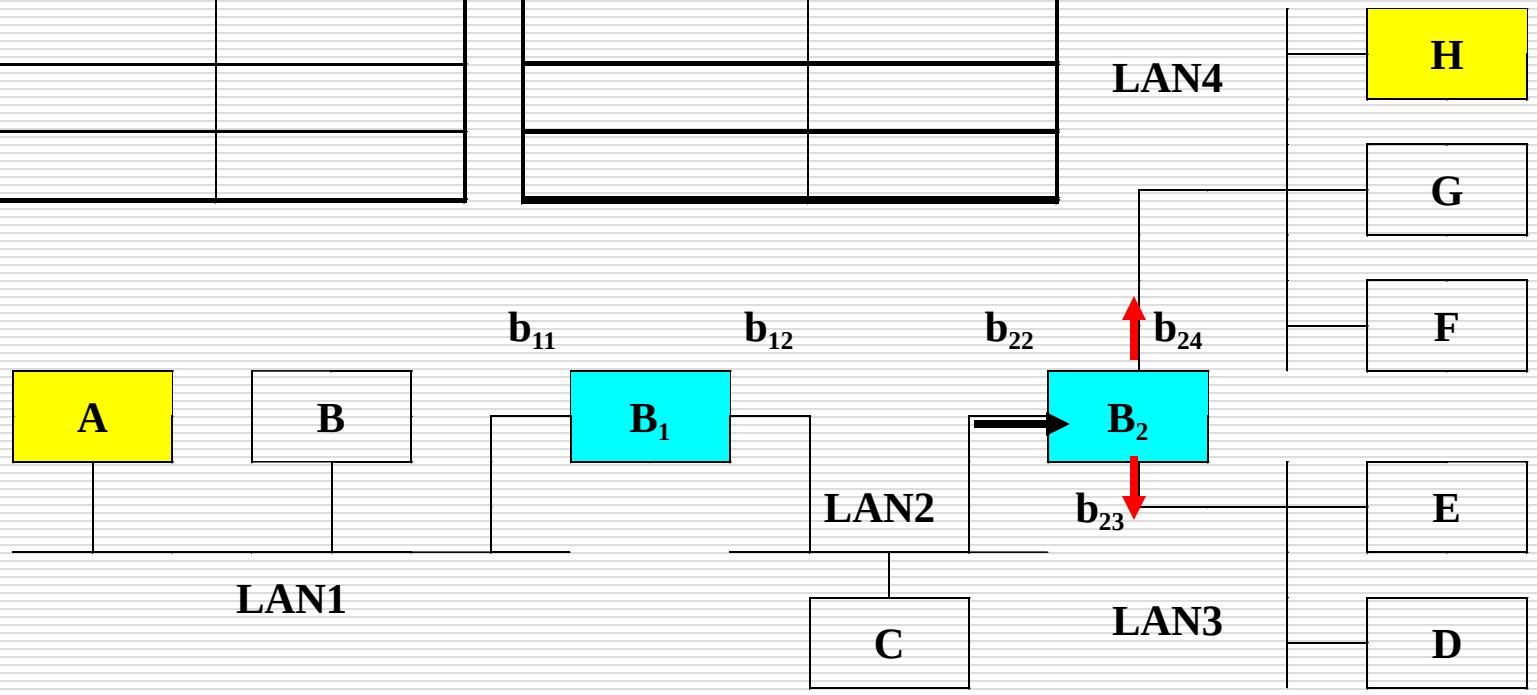
步骤3：网桥B2扩散帧Fa

B_1

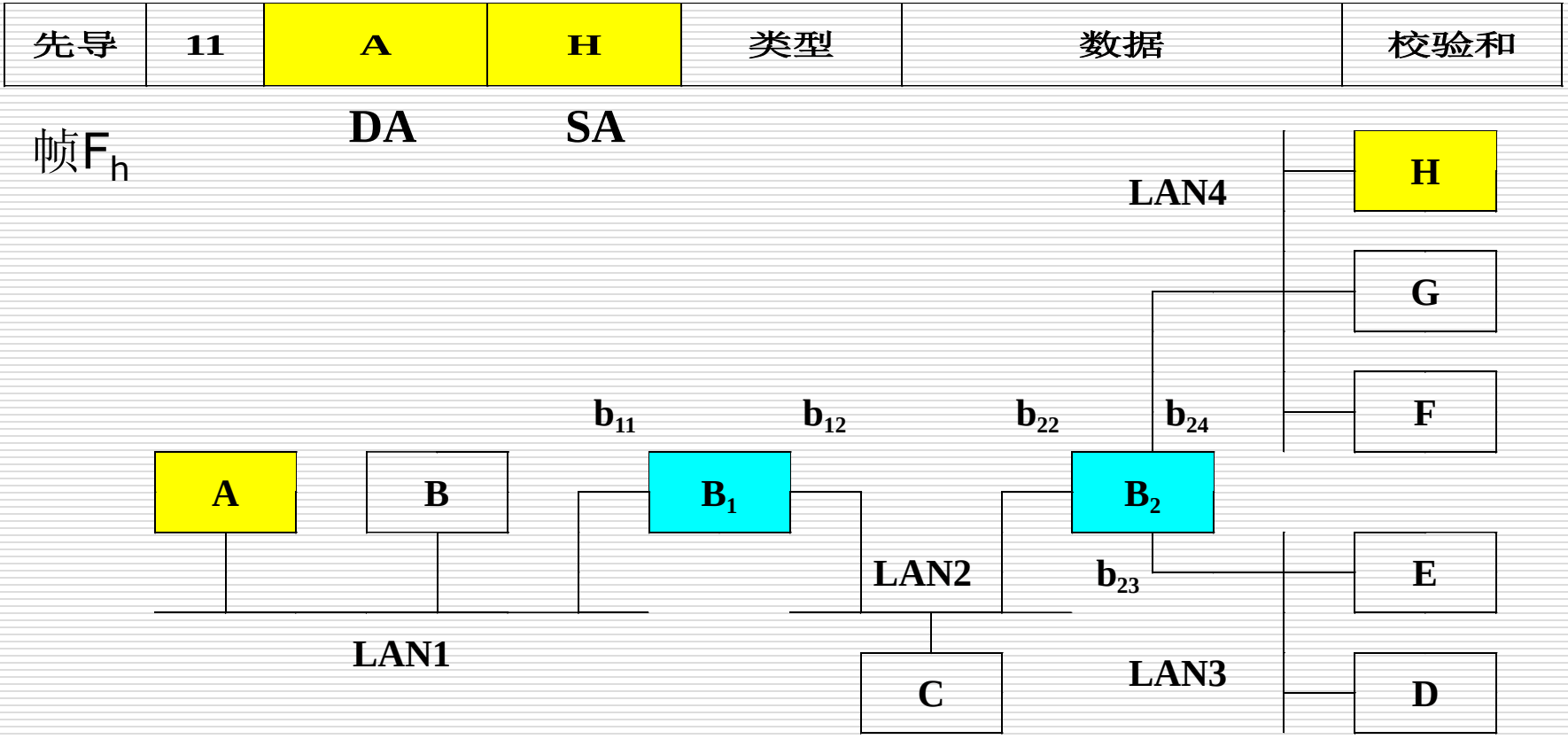
MAC	Port #
A	b_{11}

B_2

MAC	Port #
A	b_{22}



步骤4： H向A回送数据帧F_h



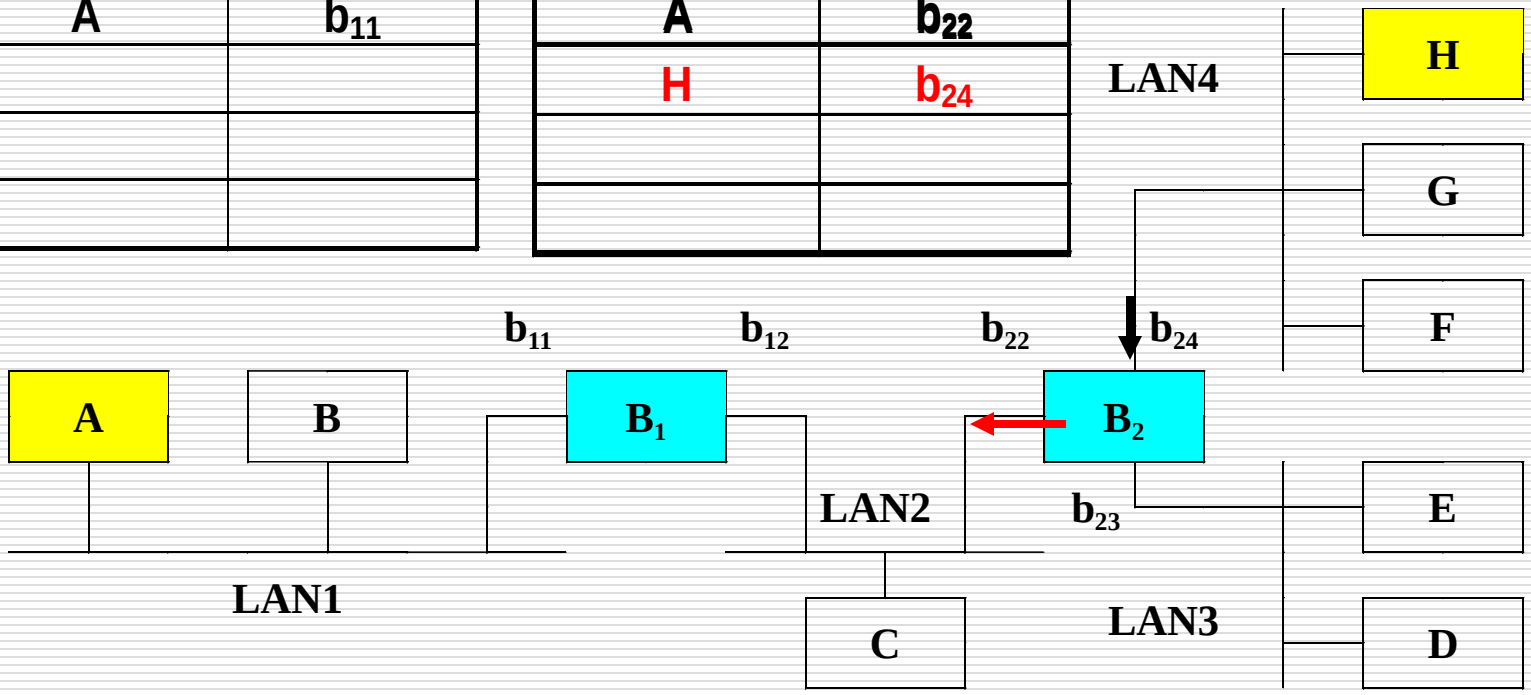
步骤5：网桥B2 转发 帧F_h

B_1

MAC	Port #
A	b_{11}

B_2

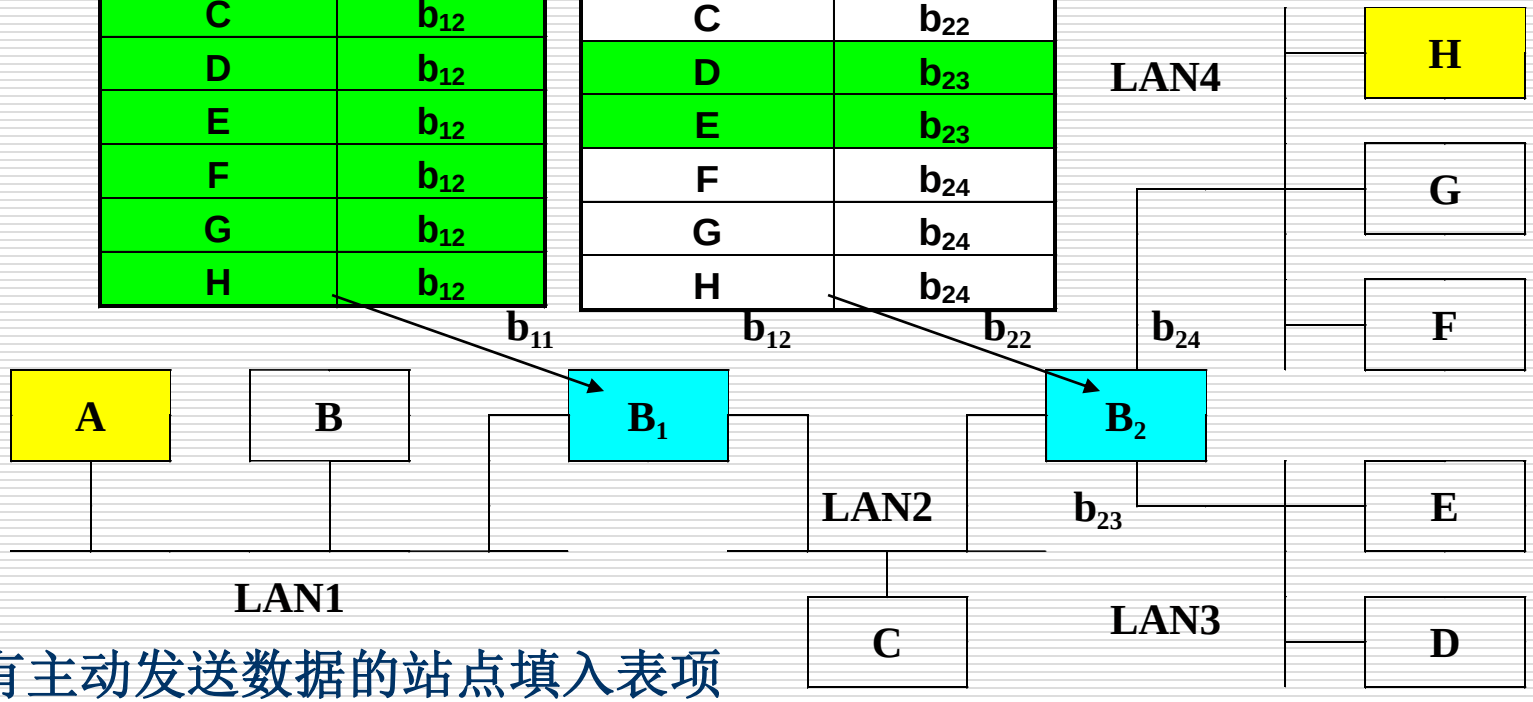
MAC	Port #
A	b_{22}
H	b_{24}



所有站点都工作的地址表

MAC	Port #
A	b_{11}
B	b_{11}
C	b_{12}
D	b_{12}
E	b_{12}
F	b_{12}
G	b_{12}
H	b_{12}

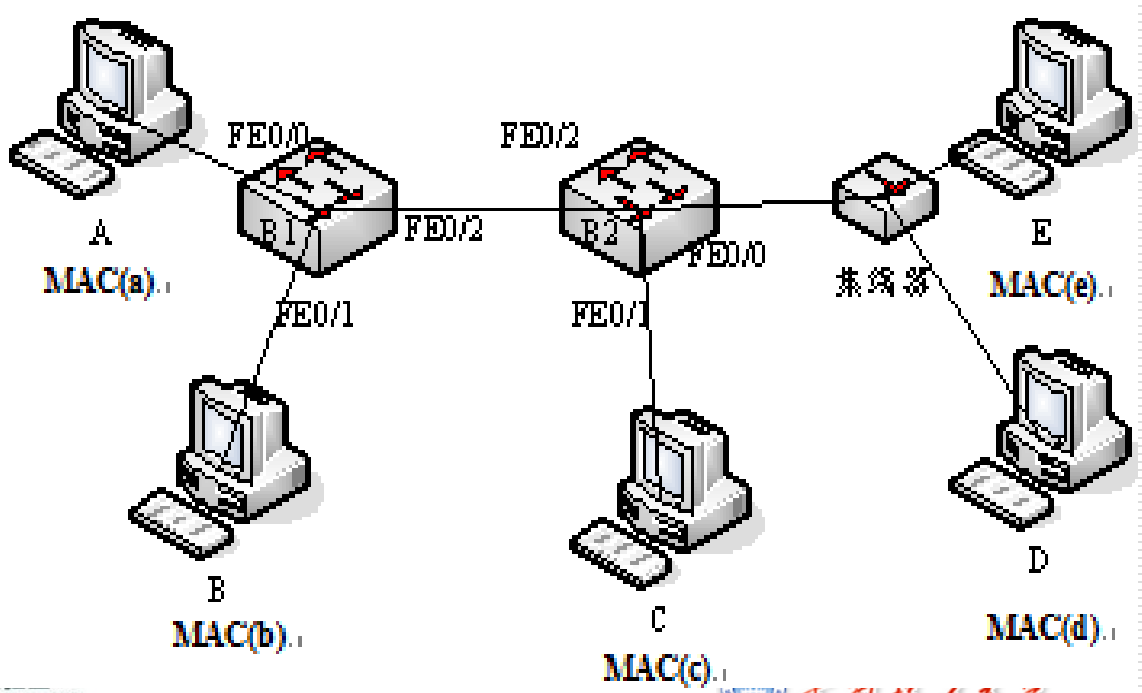
MAC	Port #
A	b_{22}
B	b_{22}
C	b_{22}
D	b_{23}
E	b_{23}
F	b_{24}
G	b_{24}
H	b_{24}

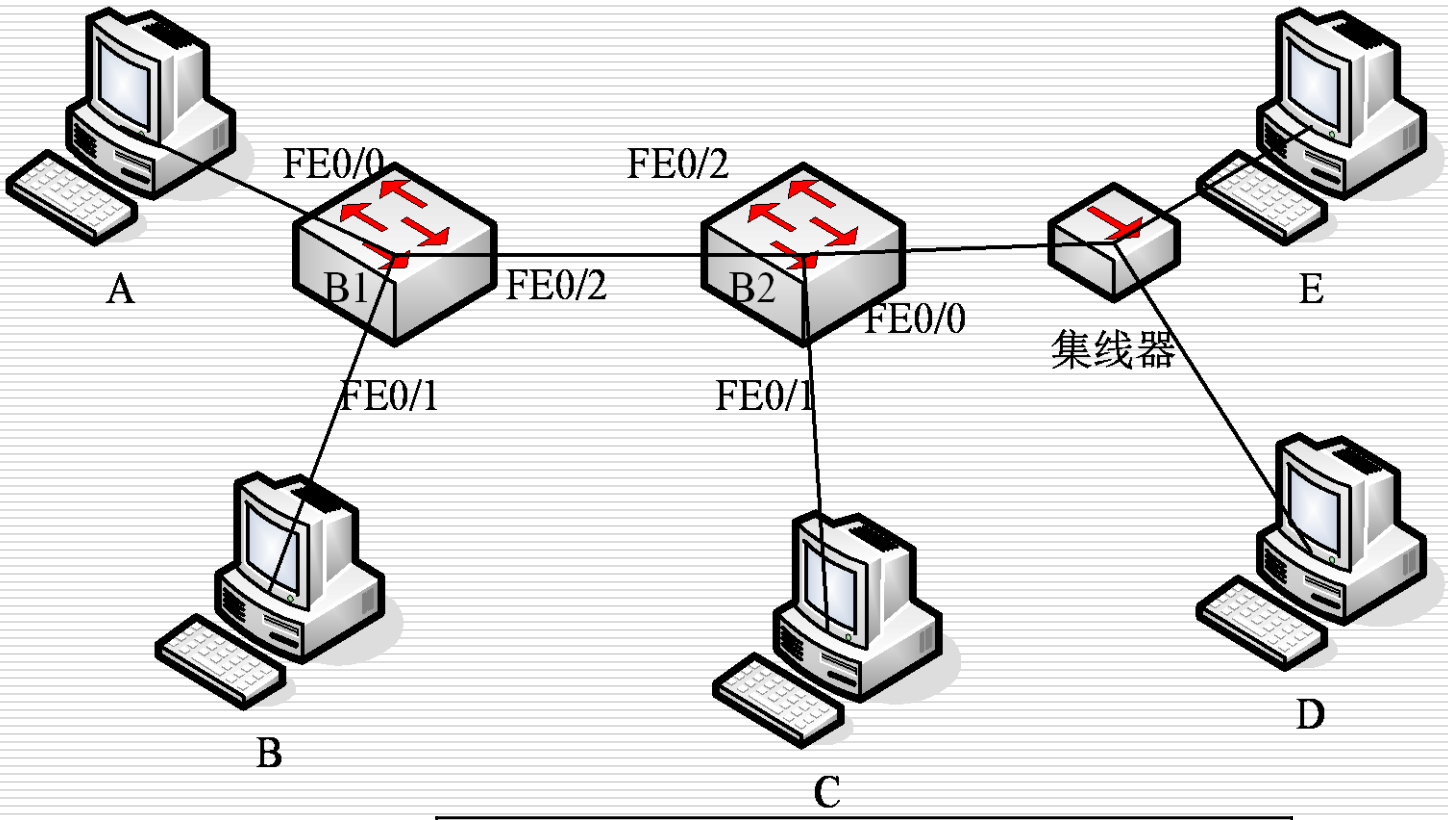


- 只有主动发送数据的站点填入表项
- 定时刷新表项，删除不活动的站点

课堂练习1

- 请写出下列数据帧正常收发之后，两个交换机内部的MAC地址表。
  - **A向D传送一个帧**
  - **E向A传送一**
  - **D向E发送一**





A → D

E → A

D → E

B1/2的MAC地址表（自学习表）	
MAC地址	端口

参考答案

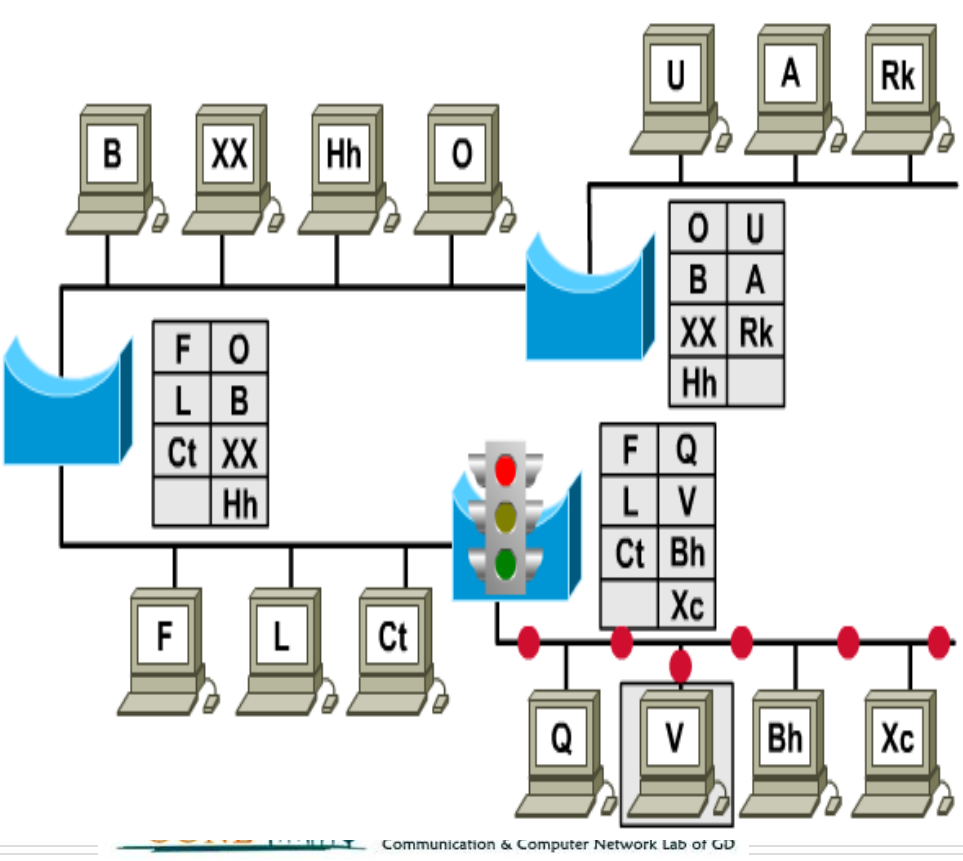
B2的MAC地址表（自学习表）	
MAC地址	端口
Mac(a)	FE0/0
Mac(e)	FE0/2

B2的MAC地址表（自学习表）	
MAC地址	端口
Mac(a)	FE0/2
Mac(e)	FE0/0
Mac(d)	FE0/0

课堂练习2：网桥如何工作?

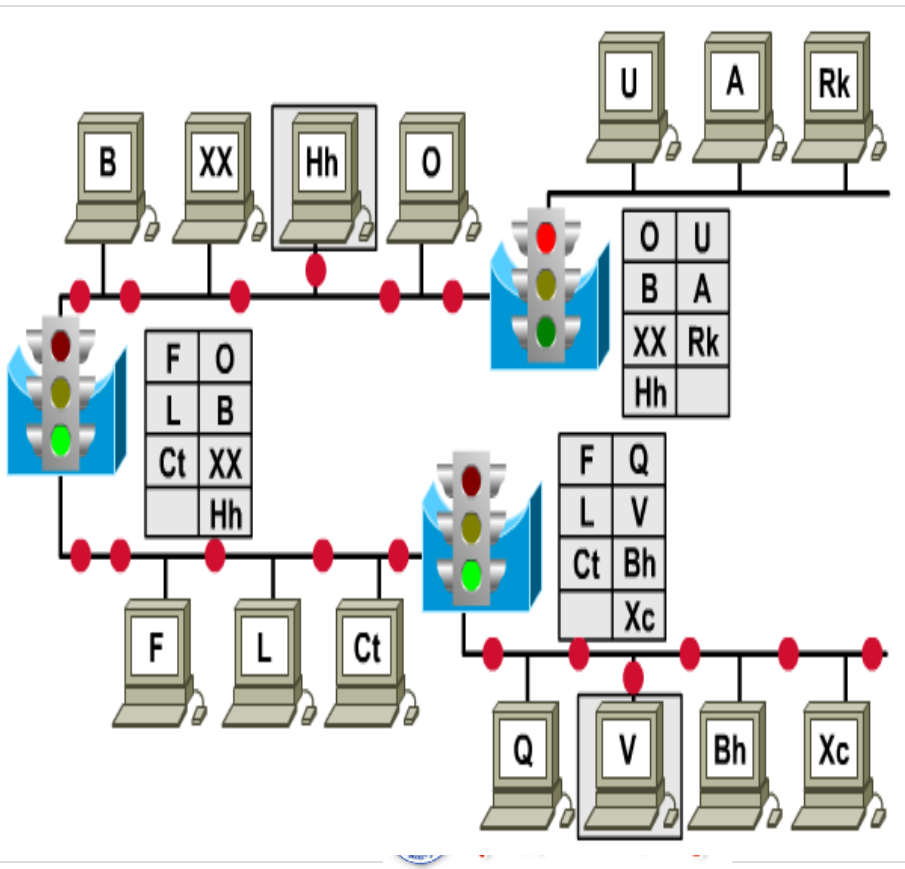
Filter

V ⇨ Xc



Forward

V ⇨ Hh



网桥和中继器的比较

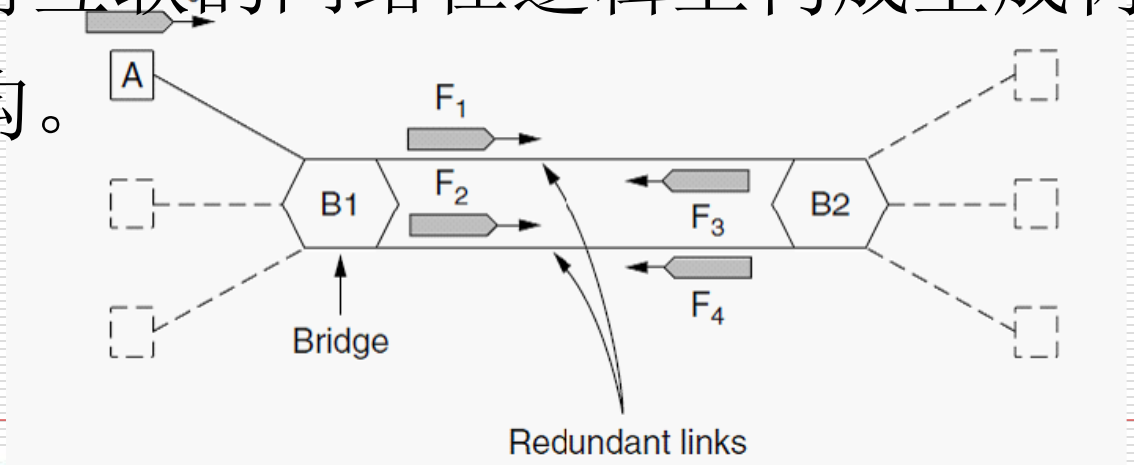
功能	网桥	中继器
再生信号	Yes	Yes
连接采用不同MAC协议的网段	Yes	No
隔离冲突域	Yes	No
根据帧头的物理地址转发帧	Yes	No
丢弃损坏帧	Yes	No

4、8、12、16、24、32

8、12、16、24、48

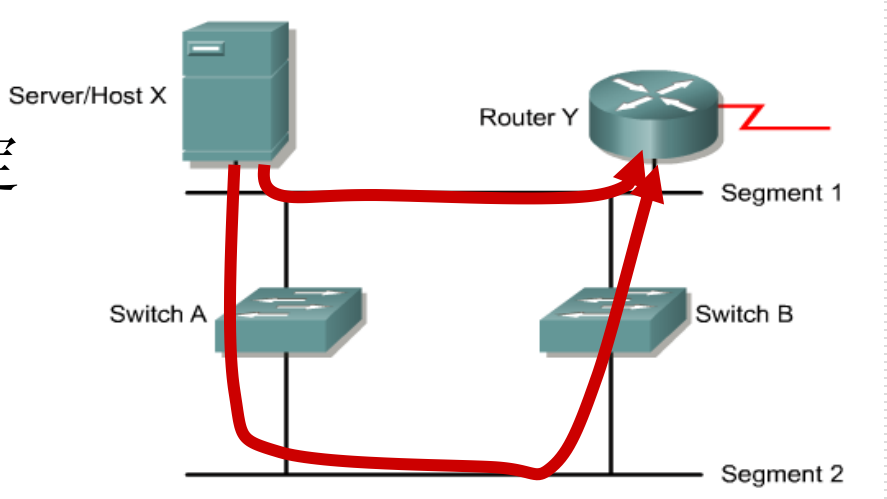
生成树网桥P261

- Spanning Tree Bridge
- 为了可靠，冗余结构，但是
- 透明网桥会产生无休止循环的问题，解决的办法就是将互联的网络在逻辑上构成生成树的拓扑结构。

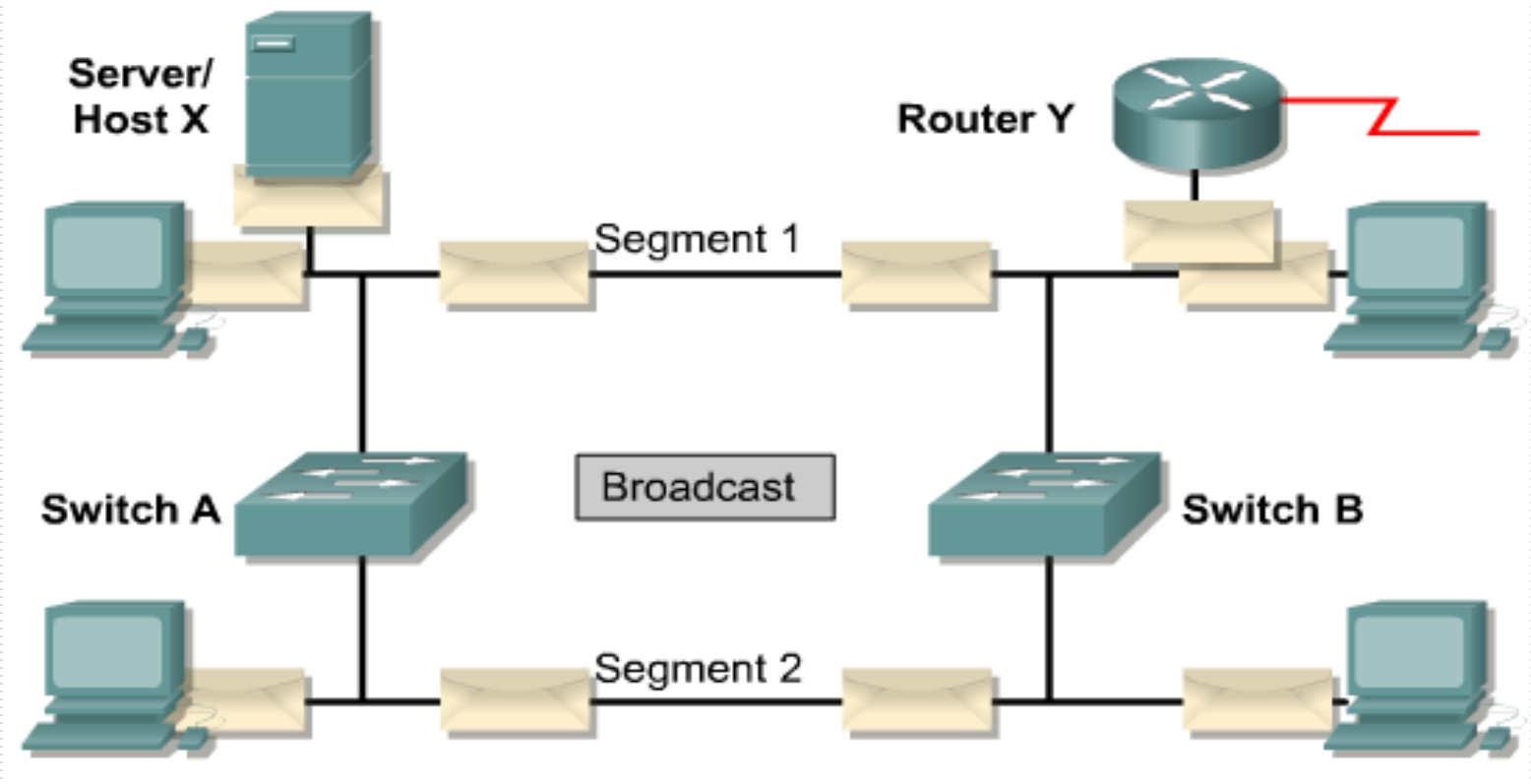


冗余交换拓扑

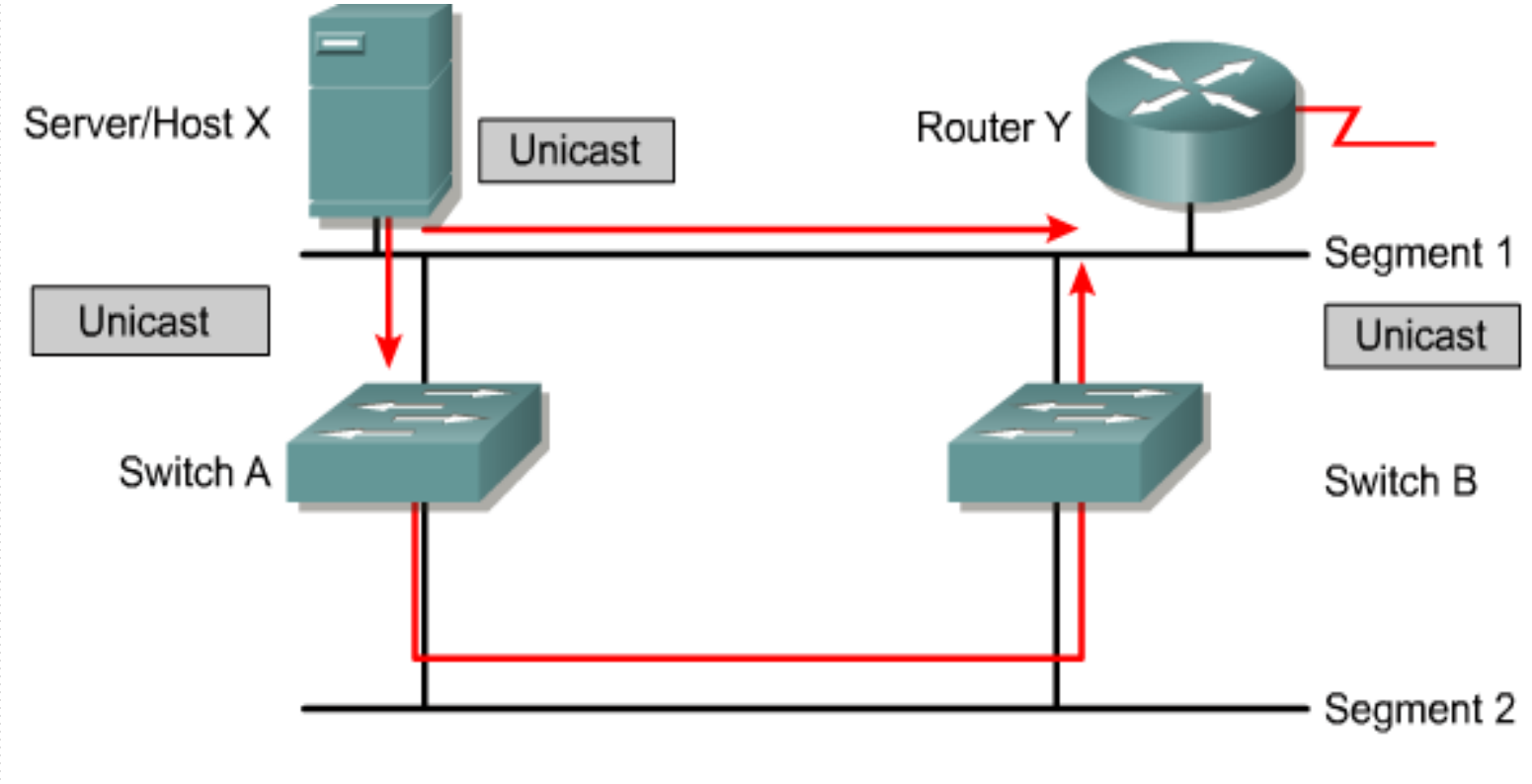
- 为了可靠，采用冗余拓扑
- 可能带来的问题
  - 广播风暴
  - 多帧传送
  - MAC地址库不稳定



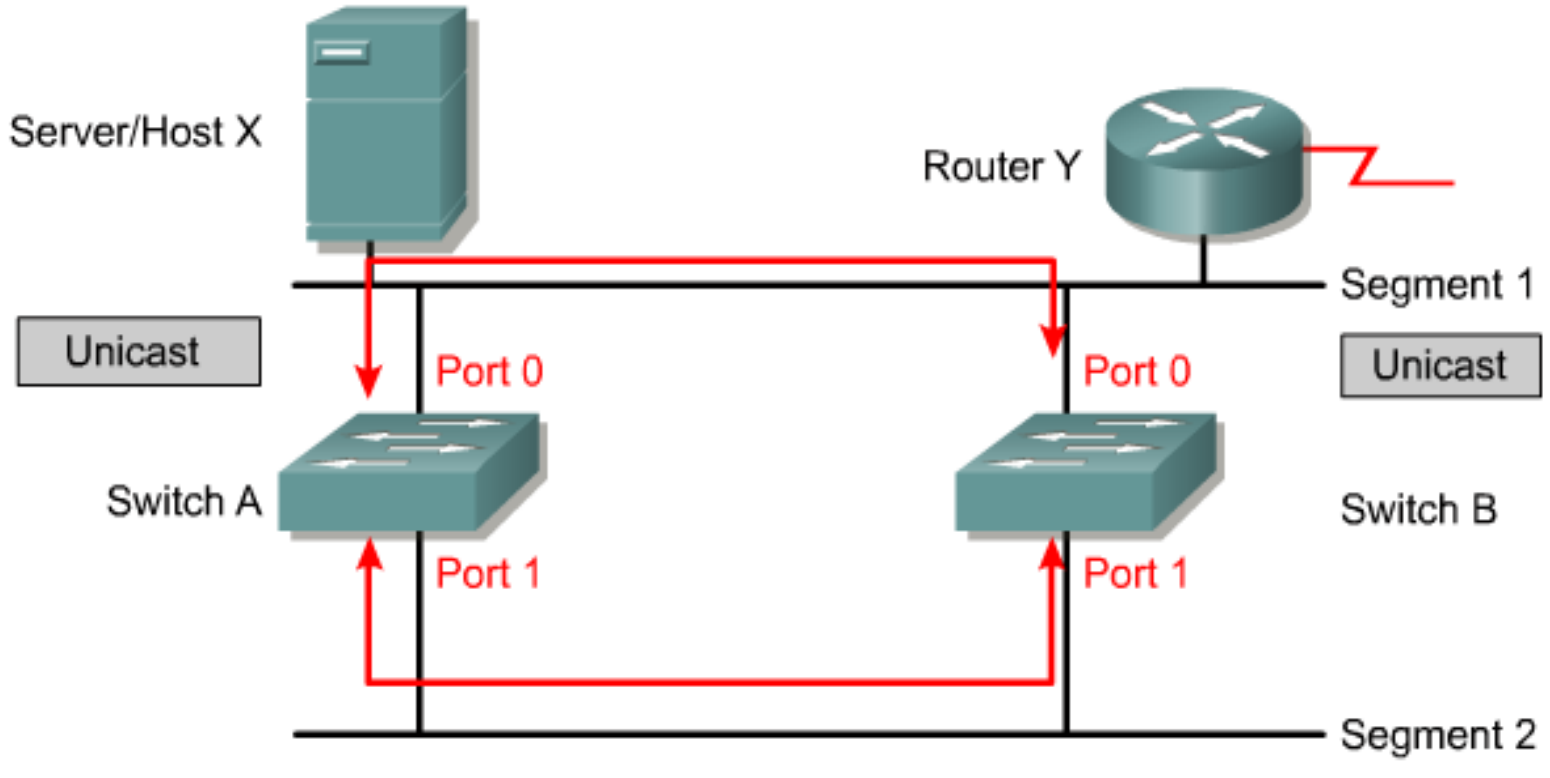
广播风暴


Server/
Host X
Router Y
Segment 1
Broadcast
Switch A
Switch B
Segment 2

多帧传送


Server/Host X
Unicast
Router Y
Segment 1
Unicast
Unicast
Switch A
Switch B
Segment 2

mac地址库的不稳定


Server/Host X
Router Y
Segment 1
Unicast
Port 0
Port 0
Unicast
Switch A
Switch B
Port 1
Port 1
Segment 2

生成树协议概述

- STP:spanning tree protocol
- 为了维护一个无环路的网络拓扑
- 新标准：RSTP

Radia Perlman P262

我想我永远也不会看到

像一棵树那么优美的图画

树那至关紧要的特性

是无回路的连通

树需要无限的扩展

包才能到达每一个L A N

首先，需要选好树根

指定I D即可选定

从树根开始，计算最小代价的路径

这些路径，就是这棵树的枝条

网络出自我等愚人之手

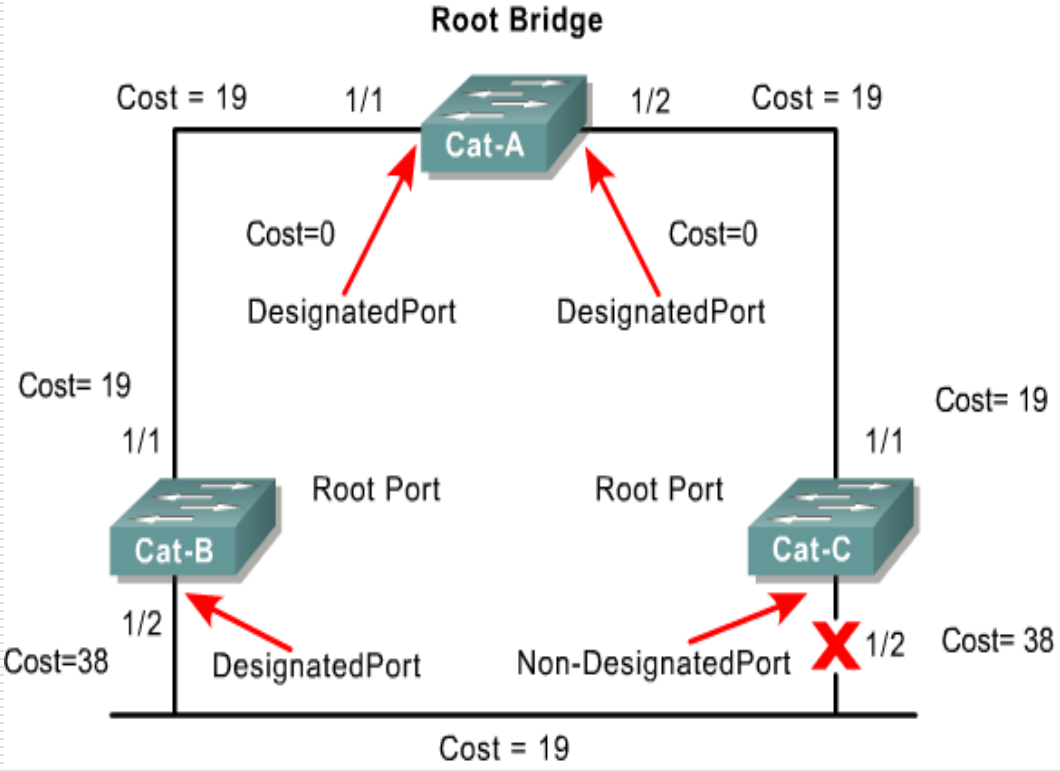
而桥则发现了一棵生成树

Radia perlman简介

- 1951-
- 毕业于MIT，BS、MS、PhD
- 现供职于Intel
- 拥有50个专利
- 代表作：
  - A Protocol for Distributed Computation of a Spanning Tree in an Extended LAN, Ninth Data Communications Symposium, Vancouver, 1985

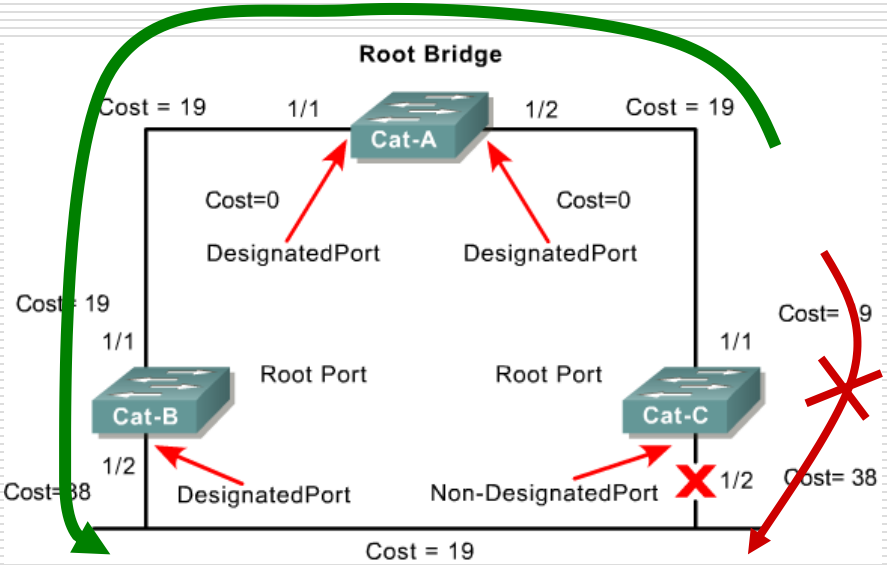
STP的运作

- 每个网络一个根网桥
- 每个网桥一个根端口
- 每网段一个指定端口
- 非指定端口不被使用

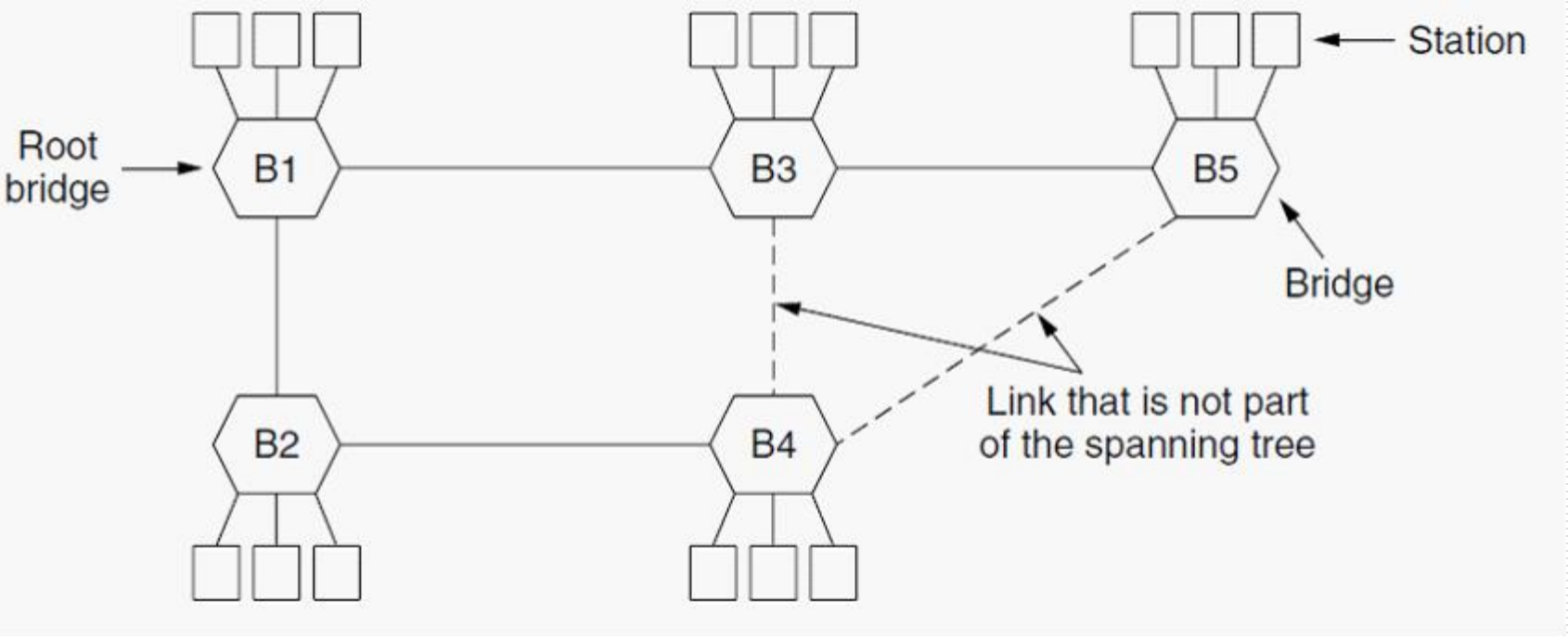


注意

- 生成树算法，生成在逻辑上无回路的树，即生成树
- 生成树算法能在有物理回路的网络中，生成一棵没有逻辑回路的生成树，但并不能保证其中的路径是最优的



一个例子P261

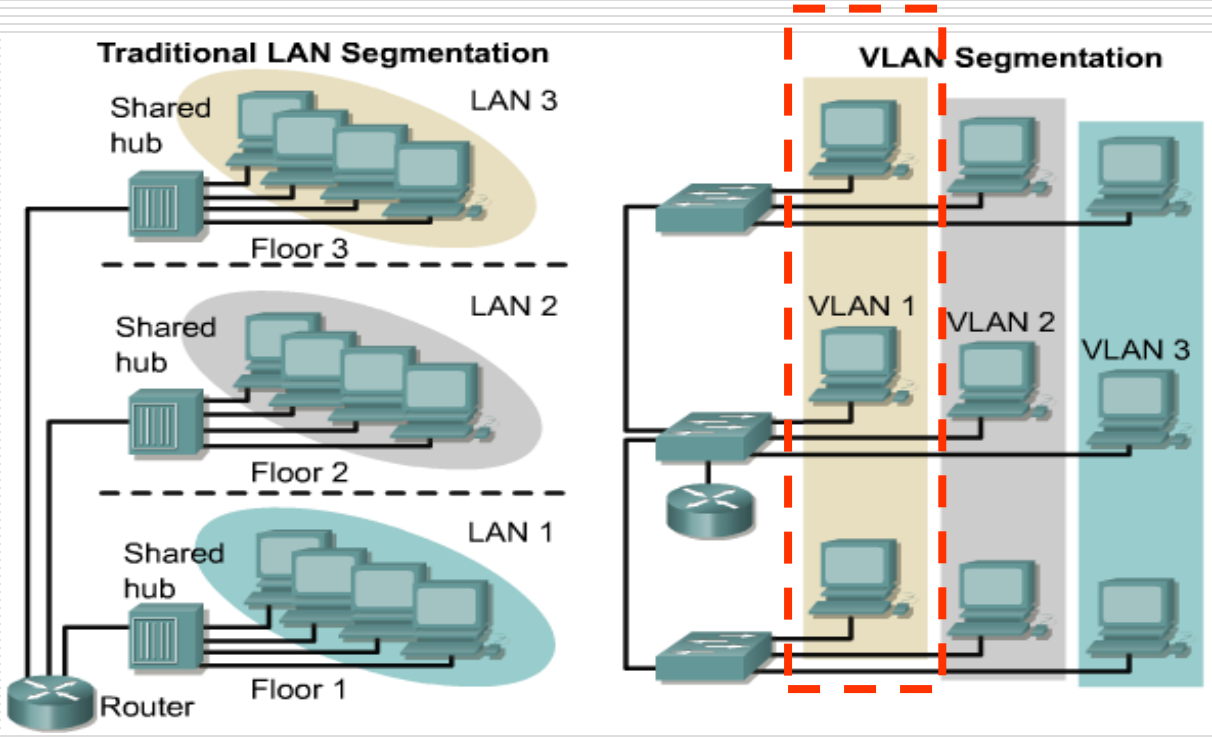

Root
bridge
B1
B2
B3
B4
B5
Station
Bridge
Link that is not part
of the spanning tree

小结SPT

- 为了打断物理环路
- 形成的是逻辑上的无环路
- SPT可能产生非最优路径（付出的代价）
- 运行过程，非指定端口也在收消息，如果需要，重新启用，生成新的生成树，提供冗余可靠性

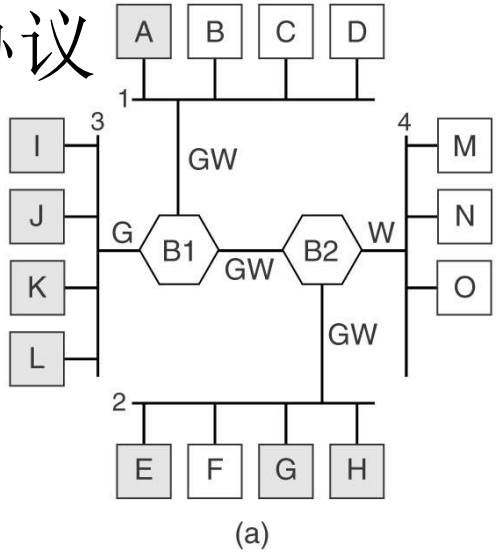
虚拟局域网（VLAN）

- VLAN：一组逻辑上的设备或用户。

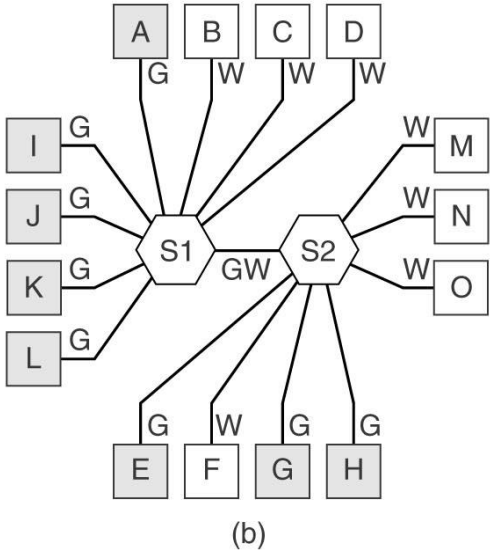


VLAN的实现

- 基于端口
- 基于MAC地址
- 基于三层协议



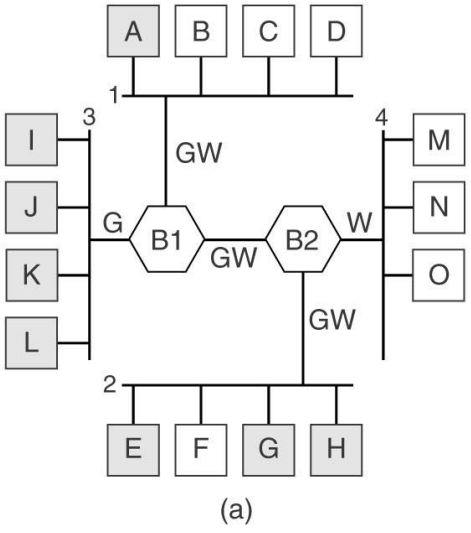
(a)



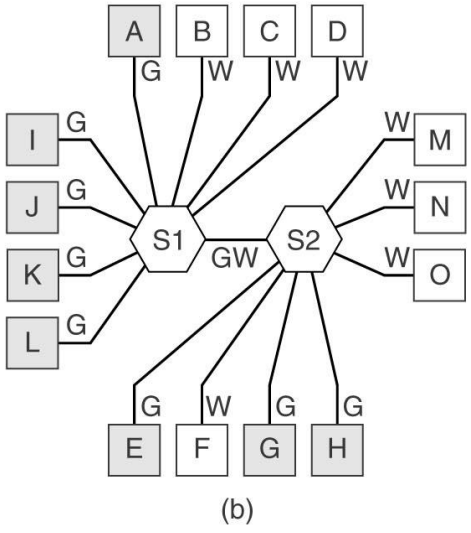
(b)

IEEE 802.1Q 标准 P267

- 1998年颁布
- 一种帧标记方法：VLAN ID
- 通过trunk的时候使用

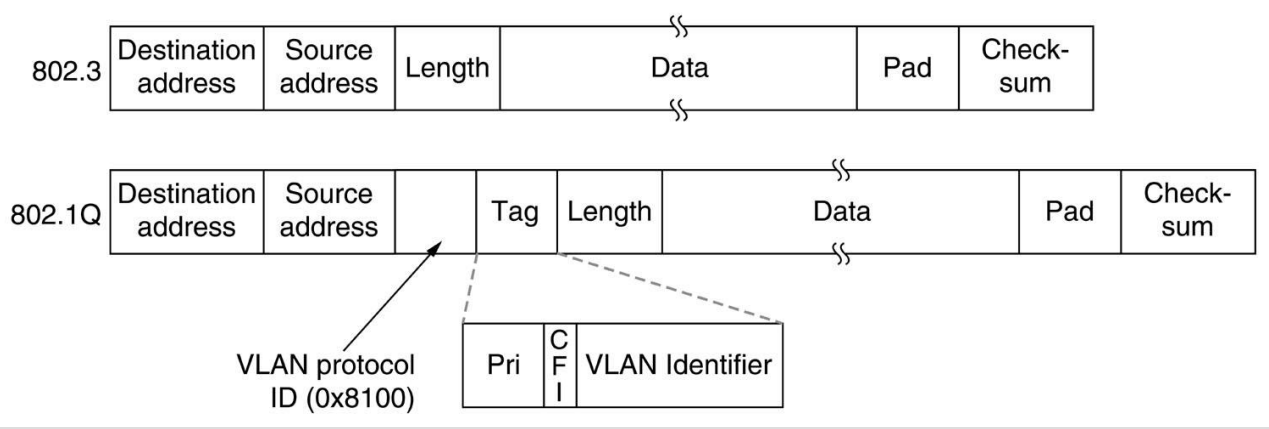


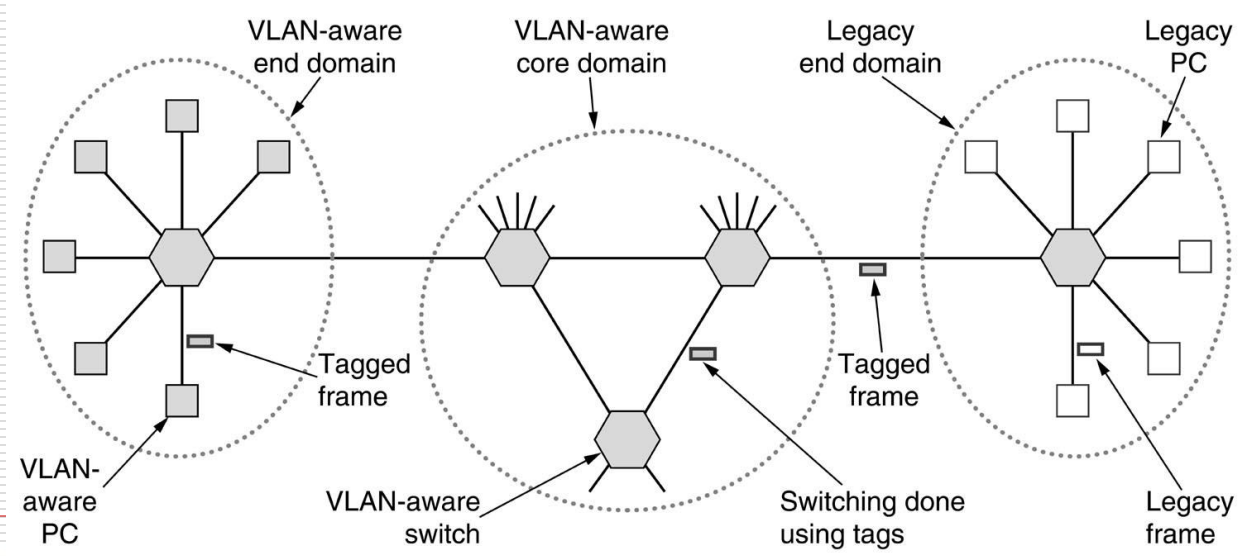
(a)



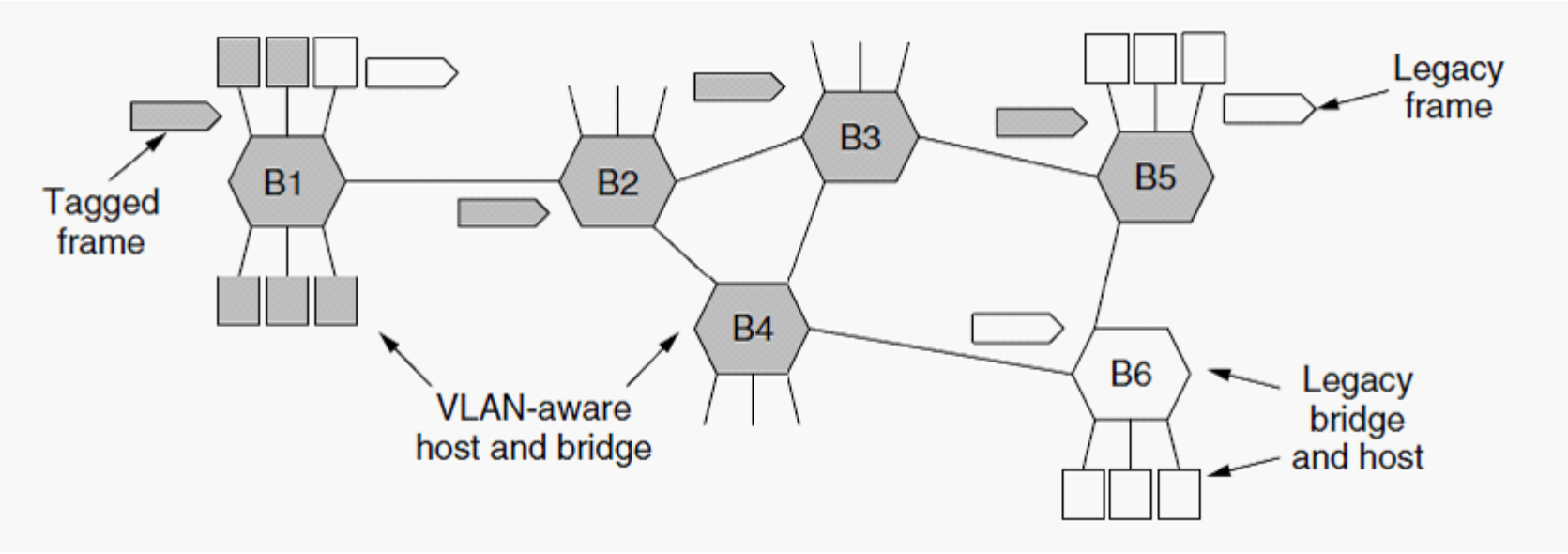
(b)

IEEE 802.1Q 标准 (cont'd)





IEEE802.1Q的一个例子

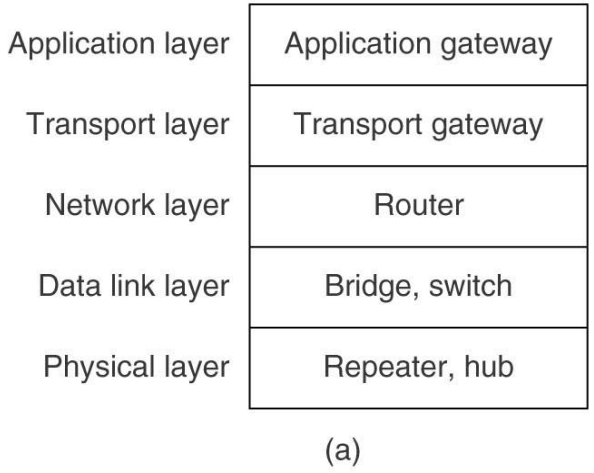


小结VLAN

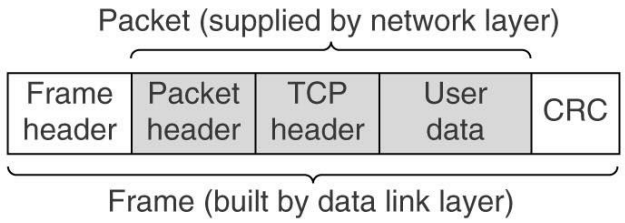
- 一个VLAN对应一个广播域
- 有了VLAN，可使用二层交换机实现广播域的分割
- 当一个VLAN跨越几个交换机的时候，使用802.1Q穿越连接交换机的干线

网络设备（P263~264）

- 中继器
- 集线器
- 网桥
- 交换机
- 路由器（第五章）
- 网关



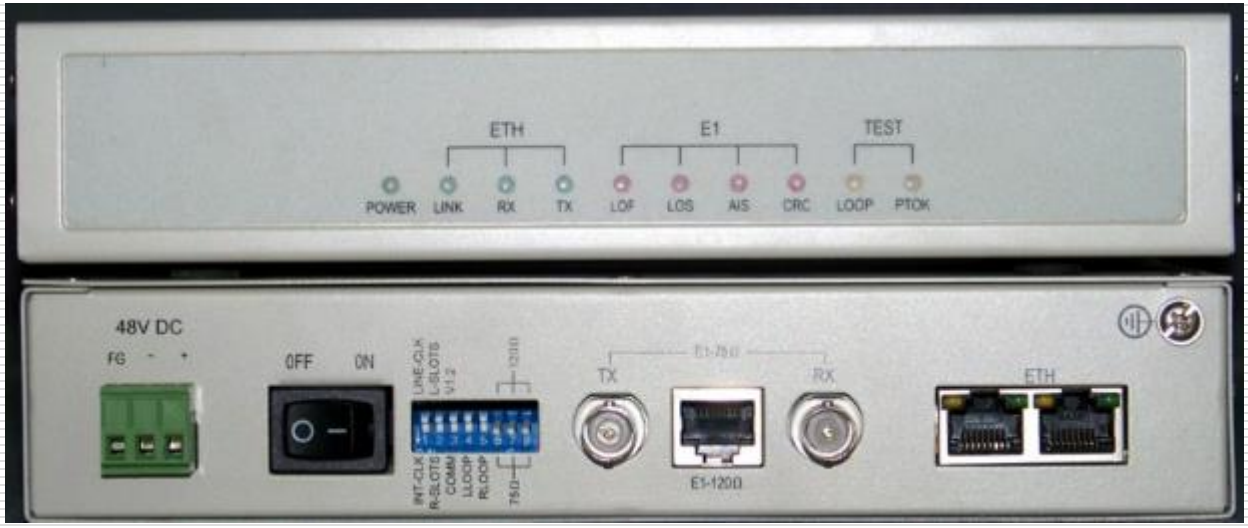
(a)



(b)

二层（数据链路层）设备

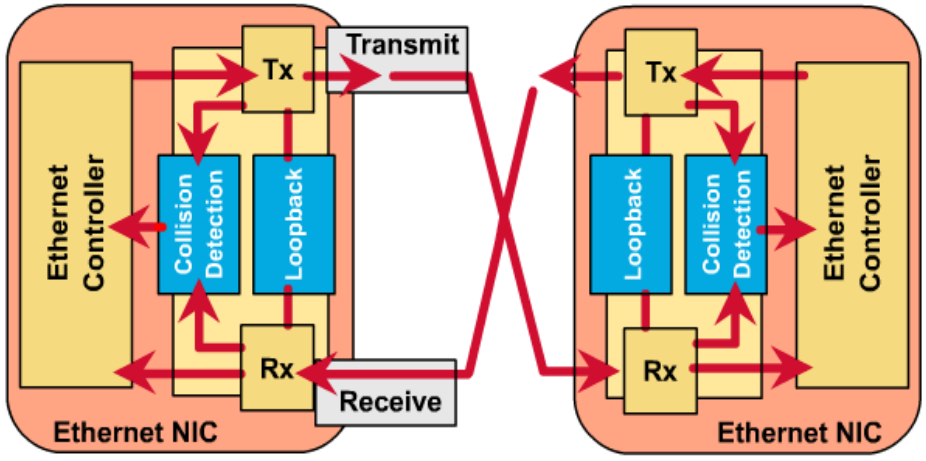
- 网卡
- 网桥
- 交换机



FE1双以太网网桥

1. NIC 网卡

- Nework Interface Card
- 为主机提供介质的访问。
- MAC地址烧在网卡的 ROM中



1. NIC 网卡

- Logical link control (LLC): 和上层通信
- Naming: 提供一个独特的 MAC 地址标识符
- Framing: 封装过程的一部分，为传输比特流打包
- Media Access Control (MAC): 为访问共享介质提供访问策略
- Signaling:创建信号和与介质的接口

NIC 运作

- 第一层和第二层设备
- 主要是第二层的设备
  - 在计算机中与上层通信
    - Logical Link Control (LLC)
  - 烧入芯片的MAC 地址
  - 封装数据城帧
  - 提供介质访问
- 也是第一层设备
  - 创建信号和与介质的接口
  - 内建转发器（ transceiver）

NIC 网卡分类

- Ethernet NIC
  - TOKEN Ring NIC
  - FDDI NIC
- ISA NIC
  - PCI NIC
- 标准以太网卡
  - PCMCIA网卡
- Coxial NIC
  - TP NIC
  - Fiber-Optical NIC
- 10Mbps NIC
  - 100Mbps NIC

网卡选择

- 计算机类型
- 网络类型**Type of network**
  - Ethernet, Token Ring, FDDI
- 介质类型**Type of media**
  - Twisted pair, coax, fiber
- 系统总线类型**Type of system bus**
  - PCI, ISA

2. 网桥 Bridge

网桥的功能特点：

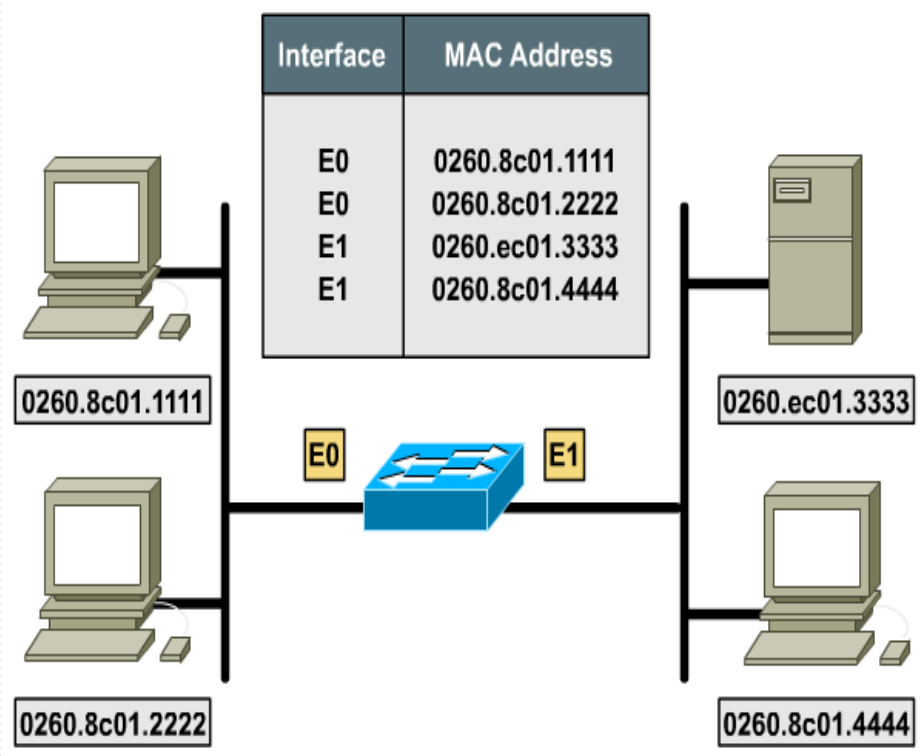
- 连接不同的LAN网段。
- 通过过滤部分交通流量，减少冲突的机会，改善网络性能。
- 以网段分流交通，基于 MAC 地址过滤流量

本章前面已经讲过很多网桥的基本知识，这里不再重复

3. 交换机 Switch

- LAN 交换机是多端口网桥，
- 连接 LAN 网段。
- 使用一张 MAC 表，来决定一帧转发的端口
- 交换机常被用来替换集线器（hub），以改善现有网络性能。
- 增加带宽。
- 比网桥更高的交换速度。
- 支持新的功能，如VLAN。

3. 交换机 Switch


Interface
MAC Address
E0
0260.8c01.1111
E0
0260.8c01.2222
E1
0260.ec01.3333
E1
0260.8c01.4444
0260.8c01.1111
E0
E1
0260.ec01.3333
0260.8c01.2222
0260.8c01.4444


Cisco Systems
RPS

LAN交换机中地址表的维护

1. 动态更新

直接读取数据包中的源地址信息，存入CAM，如在CAM中没有找到所需的地址，添加到CAM中。

2. 删除过时的地址记录：时间标记

1） 每增加一条记录，为它打上时间标记；

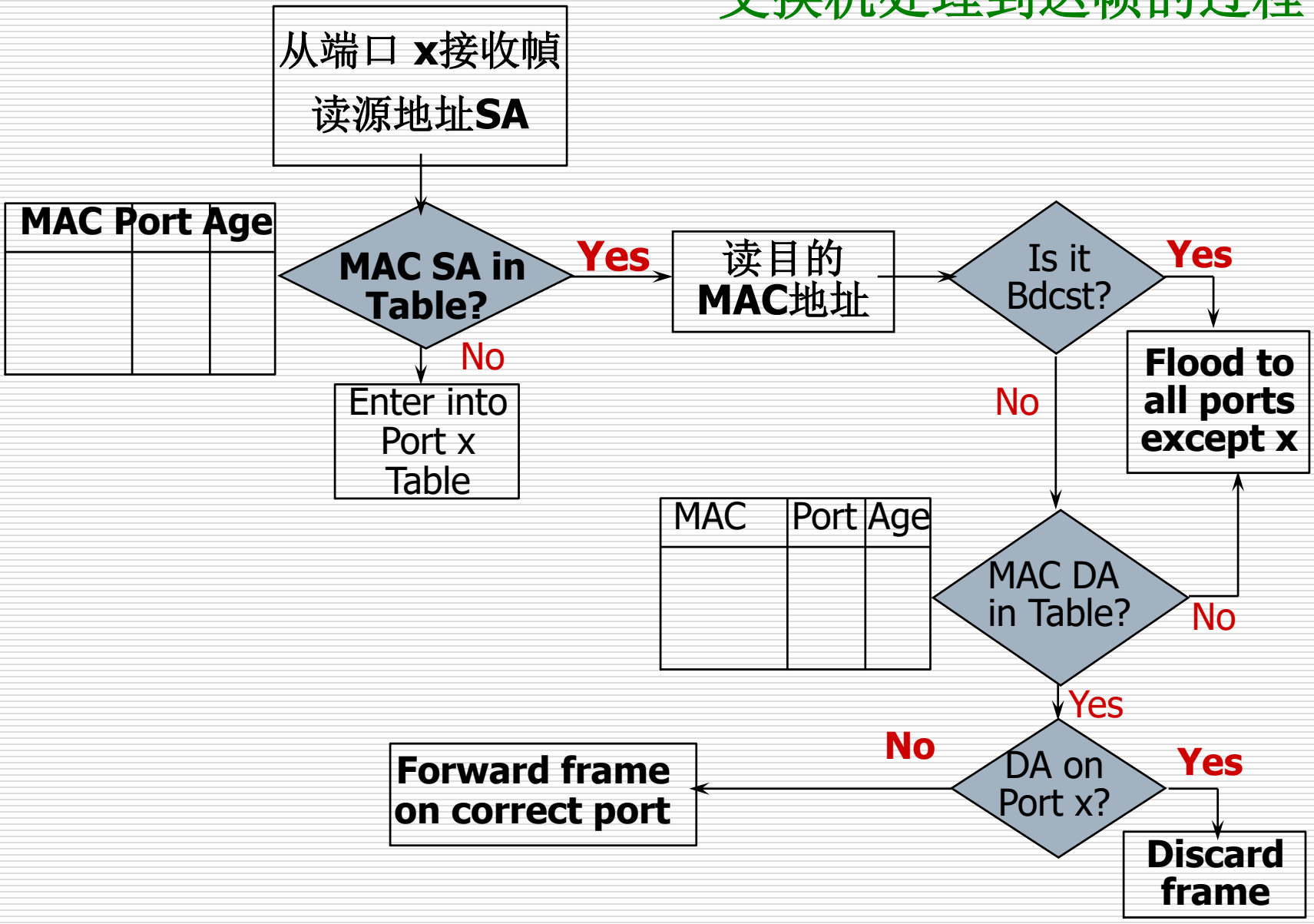
2） 每引用或找到某条记录，为它打上新的时间标记。

3） 当某条地址记录超过一定时间没被引用，则删除它。

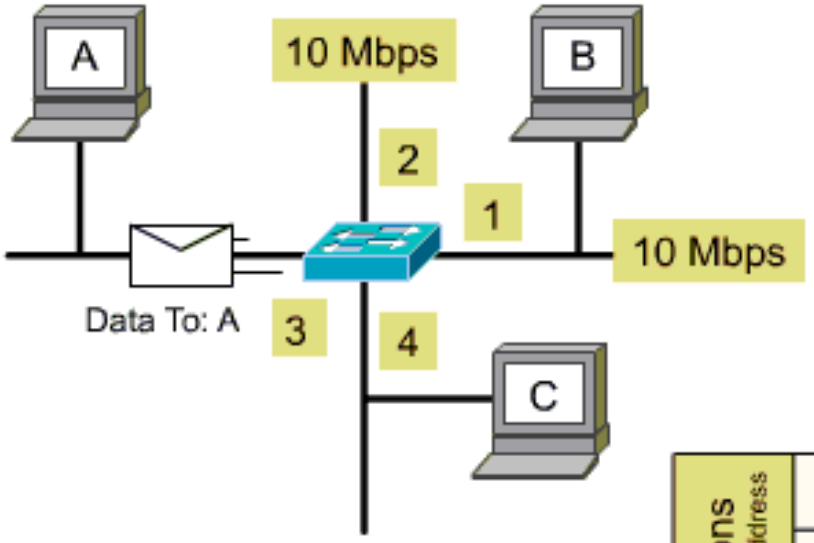
交换机的工作原理

- flooding --当目的地址未知或为广播地址时，桥发送帧到除源端口之外的每个端口
- learning --通过读取每个帧的源地址和对应源端口来学习连在网段上的每个设备的地址
- forwarding --对于已学到的目的地址，桥将直接发送帧到对应的目的设备所在端口
- filtering --如果目的地址和源地址在同一端口，桥将丢掉帧

交换机处理到达帧的过程



How a LAN Switch Learns Addresses



Stations (Layer 2 Address)	Interface 1	2	3	4
A			✓	
B	✓			
C				✓

- Learns a station's location by examining the source address
- Sends out all ports (except the port that the frame entered from) when the destination address is a broadcast, multicast, or an unknown address
- Forwards when the destination is located on a different interface
- Filters when the destination is located on the same interface

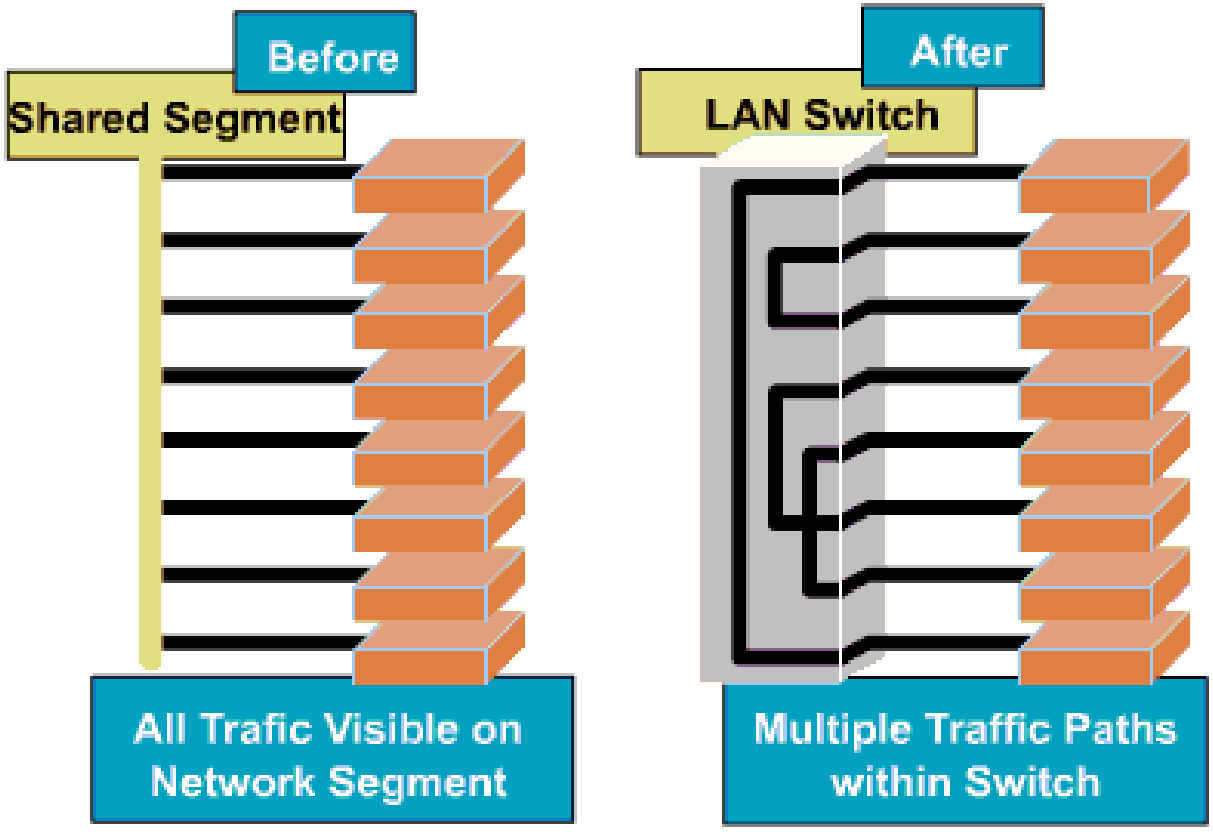
交换机的作用

- 使网络段处于无冲突环境
- LAN交换机利用现有硬件设备
- 使配置和管理更加灵活方便

无冲突域

- 微分段：LAN被交换机分隔开的网段，在一个大的冲突域中产生无冲突域。
- 虚拟线路：在交换机内部把段连接成一个虚拟网络的电路，只在需要时才成立

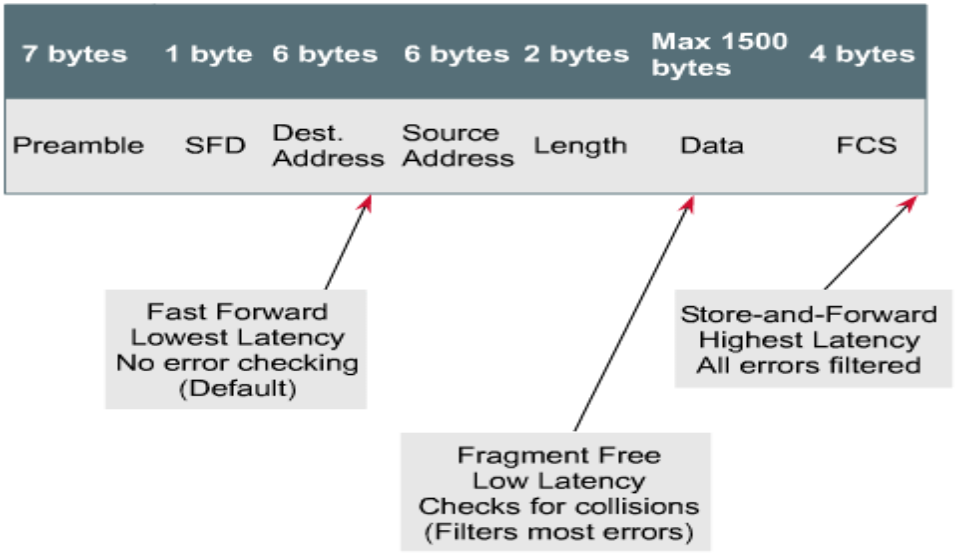
Microsegmentation of the Network



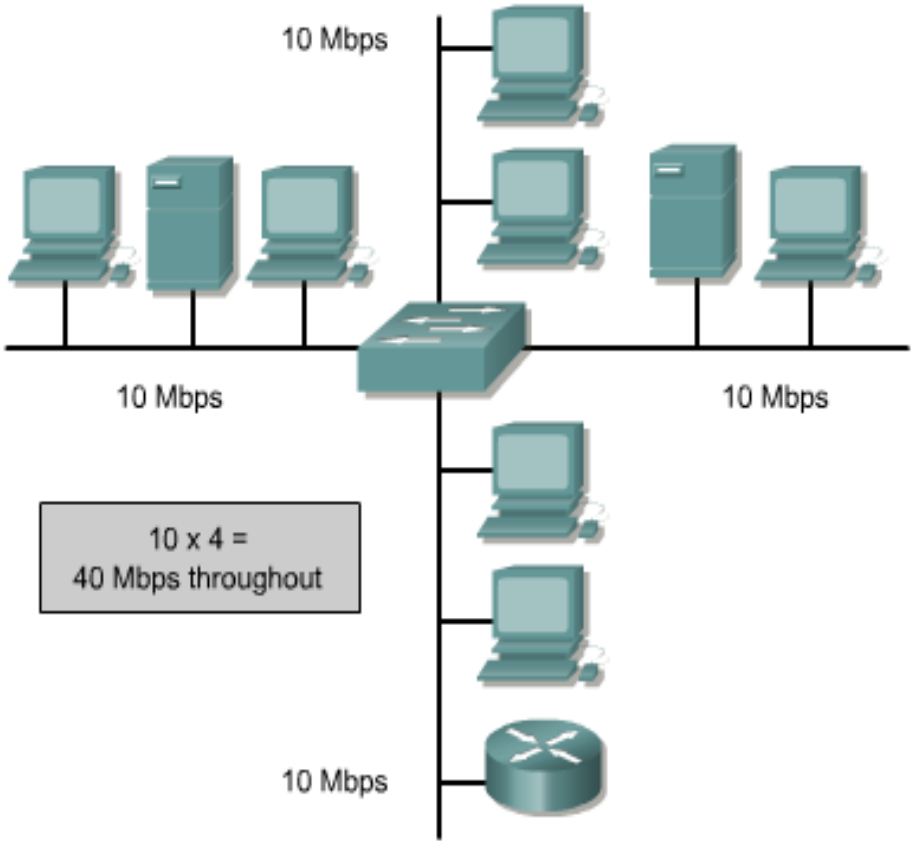
- Dedicated paths between sender and receiver hosts.

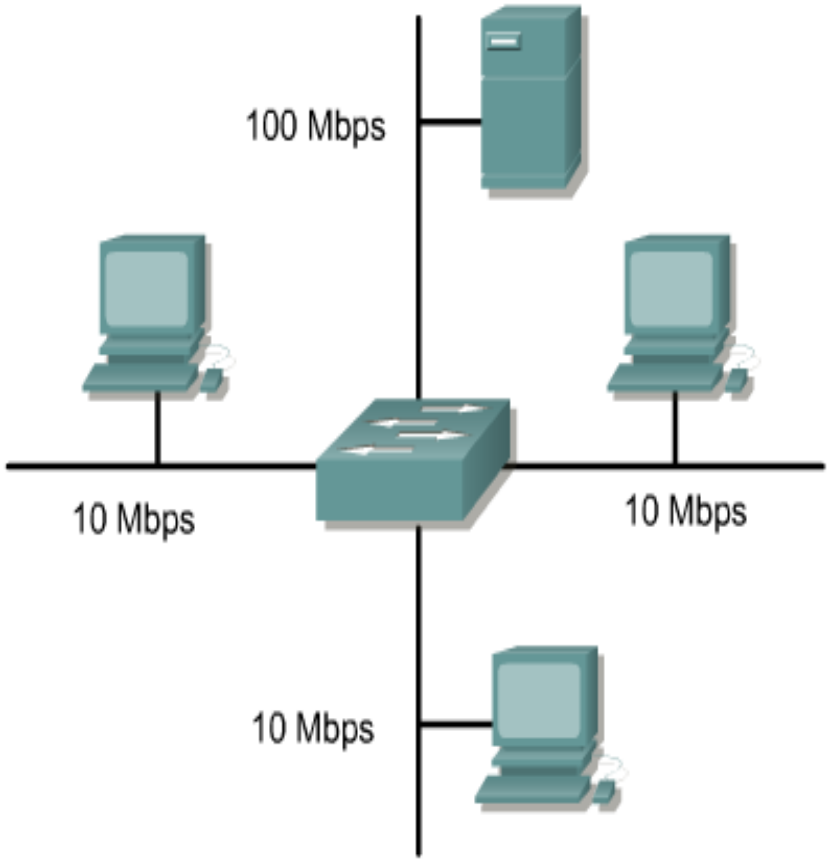
交换模式 P260

- 存储转发
- 直通交换（贯穿）
- 无分片交换



对称交换和非对称交换


10 Mbps
10 Mbps
10 Mbps
10 x 4 =
40 Mbps throughout
10 Mbps


100 Mbps
10 Mbps
10 Mbps
10 Mbps

补充：交换机相关的安全问题

常见安全攻击

- MAC地址泛洪攻击
  - 伪造源地址
  - 伪造目的地址
- DHCP欺骗攻击
  - 伪装成DHCP服务器应答
  - 伪造源地址，向DHCP服务器请求
- Telnet攻击
  - 暴力密码破解
  - 使Telnet服务不可用

应对安全策略

- 使用各种安全工具
  - SSL、服务识别、报文截获
- 配置端口安全性
  - 配置端口安全的策略：如数量、MAC地址
  - 违规（违反策略）后的行动
    - **保护**：丢弃违规包，或移除超出MAC地址
    - **限制**：超出规定源MAC数量后，丢包，直到回到安全范围之类，并发出SNMP陷阱、计入日志、违规计数器
    - **关闭**：立刻关闭端口，LED灯灭，同时发送。。。。

配置命令P72

- 基本命令跟路由器的类似
- 配置策略，以2950为例

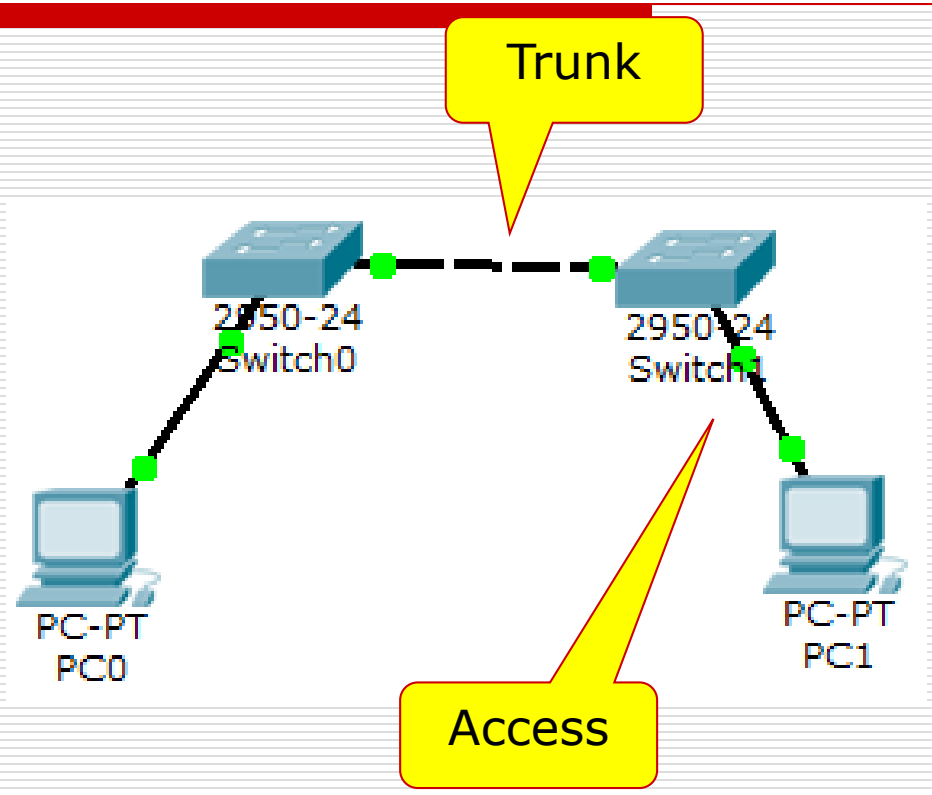
  Switch(config-if)#switchport port-security ?

  mac-address Secure mac address

  maximum Max secure addresses

  violation Security violation mode

- 注意：该命令须在开起了access和trunk模式方可用，在dynamic模式下不可用


Trunk
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
Access

配置命令（继续）

- 配置违规后采取的动作：三种之一

Switch(config-if)#switchport port-Security violation ?

protect Security violation protect mode

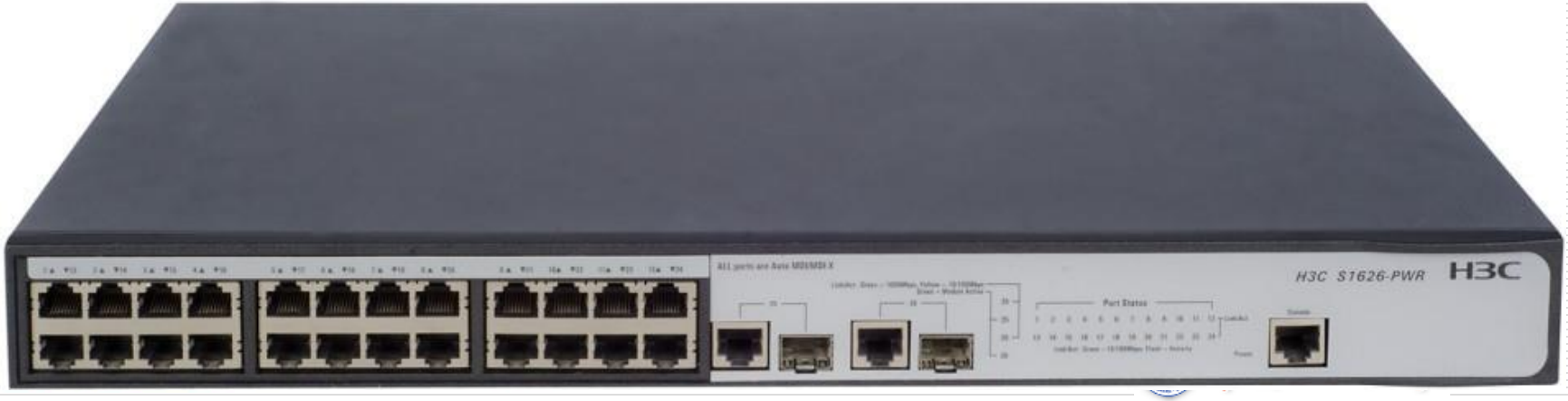
restrict Security violation restrict mode

shutdown Security violation shutdown mode

补充结束

本节小结

- 了解二层设备及桥接、交换技术
- 掌握网桥的工作原理及生成树
- 掌握交换机的工作原理
- 理解交换机的三种交换方法及特点



中英文对照术语

- Pure-ALOHA
- Slotted-ALOHA
- CSAM：多路访问
  - CSMA/CD：带冲突检测的多路访问
- Ethernet：以太网
  - Classical Ethernet：快速以太网
  - Fast Ethernet：经典以太网
  - Switched Ethernet：交换式以太网

中英文对照术语（续）

- KISS：Keep it simple，stupid
- Backward Leraning：逆向地址学习
- L2 Switching：二层交换
- Switch/Bridge：交换机/网桥
  - Store and forward：存储转发
  - Cut through：直通交换
  - Fragment-free：无碎片交换
- Spanning Tree：生成树
- Virtual LAN：虚拟局域网

谢谢！