



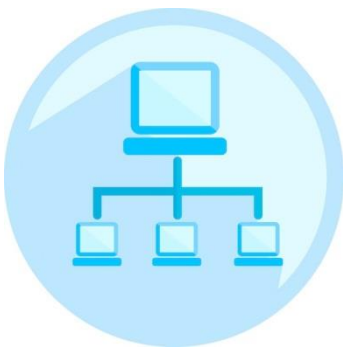
# 计算机网络



顾军

计算机学院

[jgu@cumt.edu.cn](mailto:jgu@cumt.edu.cn)





# 专题3：数据帧怎么到达目的结点

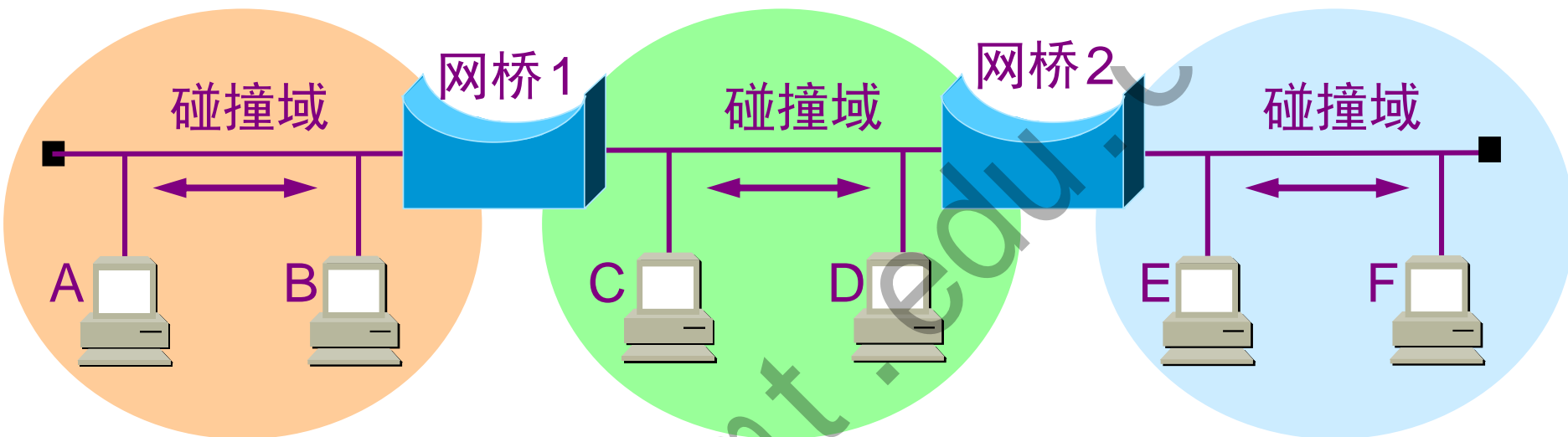


- 应用层(application layer)
- 运输层(transport layer)
- 网络层(network layer)
- 数据链路层(data link layer)
- 物理层(physical layer)





## Q21: 在数据链路层扩展局域网?



- 网桥使各网段成为隔离开的碰撞域。
- 网桥具有过滤帧的功能。当网桥收到一个帧时，并不是向所有的接口转发此帧，而是先检查此帧的目的 MAC 地址，然后再确定将该帧转发到哪一个接口。





存储转发

网桥

站表

接口管理  
软件

网桥协议  
实体

站地址	接口
A	1
B	1
C	1
D	2
E	2
D	2

接口 1

缓存

接口 2

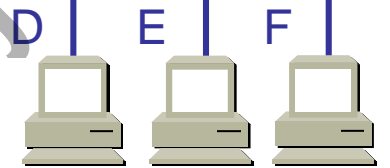
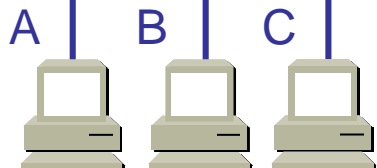
接口 1

接口 2

网桥

接口 1

接口 2



网桥的内部结构

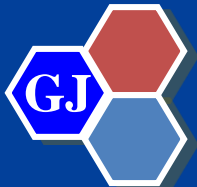




# 网桥和集线器不同

- 网桥的局域网扩展能力更强
  - 过滤通信量。
  - 扩大了物理范围。
  - 提高了可靠性。
  - 可互连不同物理层、不同 MAC 子层和不同速率（如10 Mb/s 和 100 Mb/s 以太网）的局域网。
- 集线器在转发帧时，不对传输媒体进行检测。
- 网桥在转发帧之前必须执行 CSMA/CD 算法。
  - 若在发送过程中出现碰撞，就必须停止发送和进行退避。





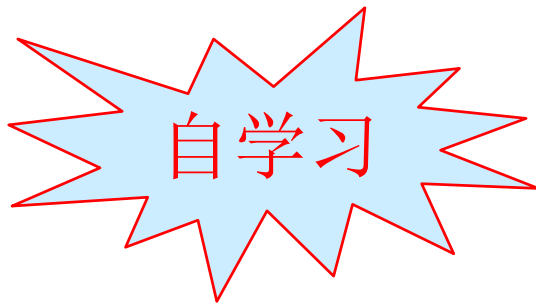
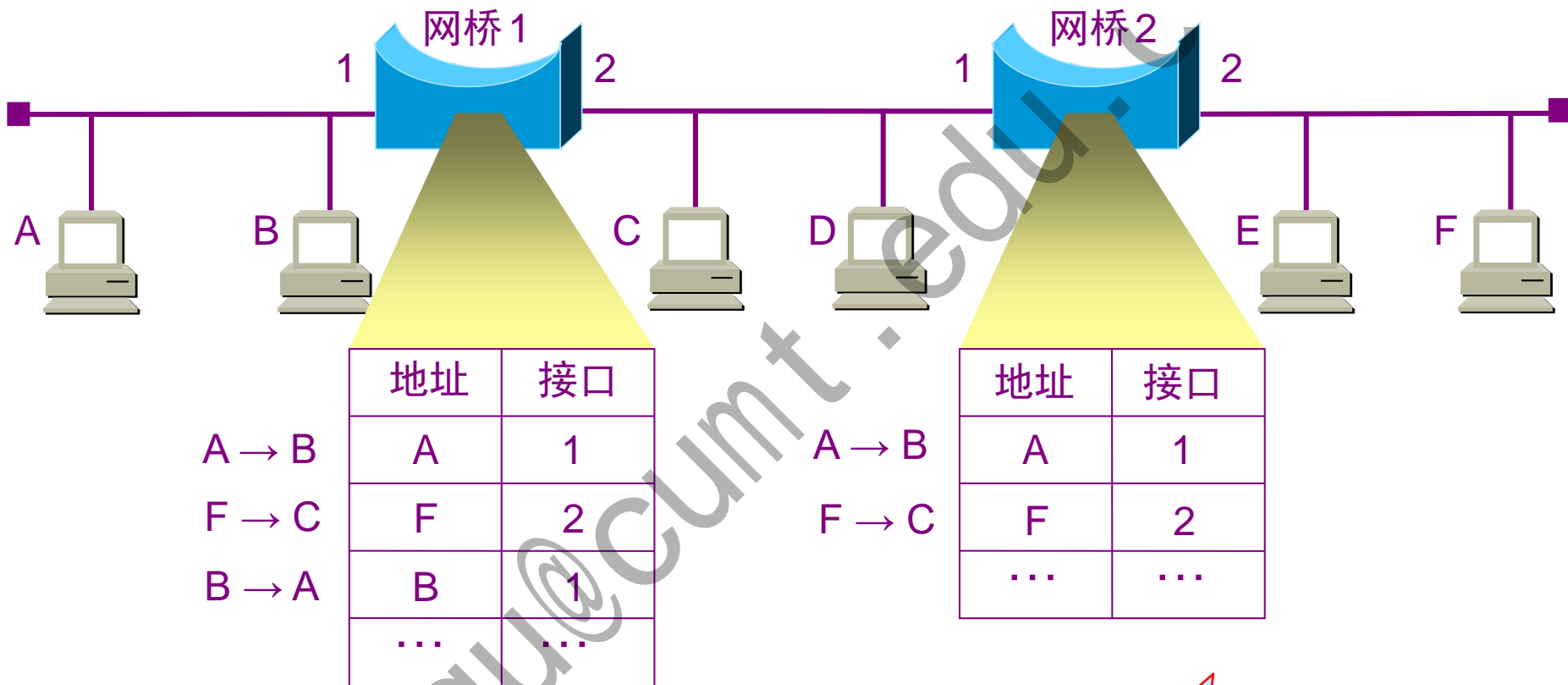
# 透明网桥

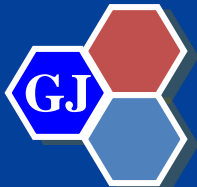
- 目前使用得最多的网桥是透明网桥(transparent bridge)。
  - “透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，因为网桥对各站来说是看不见的。
- 透明网桥是一种即插即用设备，其标准是 IEEE 802.1D。





# 网桥转发表的建立过程举例



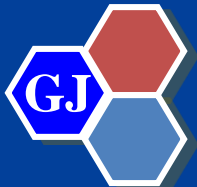


# 网桥按照自学习算法 处理收到的帧和建立转发表

- 若从 A 发出的帧从接口 x 进入了某网桥，那么从这个接口出发沿相反方向一定可把一个帧传送到 A。
- 网桥每收到一个帧，就记下其源地址和进入网桥的接口，作为转发表中的一个项目。
- 在建立转发表时是把帧首部中的源地址写在“地址”这一栏的下面。
- 在转发帧时，则是根据收到的帧首部中的目的地址来转发的。这时就把在“地址”栏下面已经记下的源地址当作目的地址，而把记下的进入接口当作转发接口。







## 网桥在转发表中登记以下三个信息

- 在网桥的转发表中写入的信息除了地址和接口外，还有帧进入该网桥的时间。
  - 这是因为以太网的拓扑可能经常会发生变化，站点也可能会更换适配器（这就改变了站点的地址）。另外，以太网上的工作站并非总是接通电源的。
  - 把每个帧到达网桥的时间登记下来，就可以在转发表中只保留网络拓扑的最新状态信息。这样就使得网桥中的转发表能反映当前网络的最新拓扑状态。





# 网桥的自学习和转发帧的步骤归纳

- 网桥收到一帧后先进行**自学习**。查找转发表中与收到帧的源地址有无相匹配的项目。如没有，就在转发表中增加一个项目（源地址、进入的接口和时间）。如有，则把原有的项目进行更新。
- **转发帧**。查找转发表中与收到帧的目的地址有无相匹配的项目。
  - 如没有，则通过所有其他接口（但进入网桥的接口除外）按进行转发。
  - 如有，则按转发表中给出的接口进行转发。
  - 若转发表中给出的接口就是该帧进入网桥的接口，则应丢弃该帧（因为不需要经过网桥进行转发）。





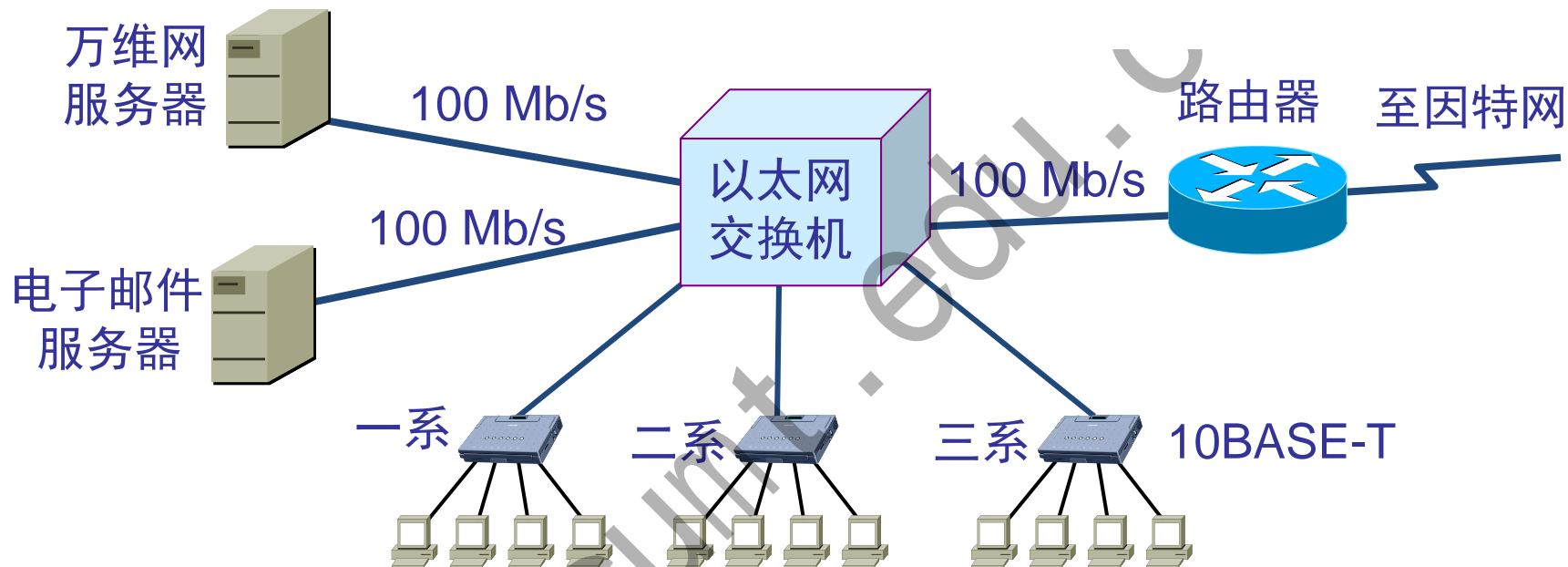
## Q22: 使用交换机扩展以太网?

- 1990 年问世的**交换式集线器**(switching hub), 可明显地提高局域网的性能。
  - ✓ 交换式集线器常称为**以太网交换机**(switch)或**第二层交换机**(L2 switch)。
- 以太网交换机机工作在数据链路层, 实质上就是一个**多接口的网桥**。
  - ✓ 通常都有十几个或者更多接口
- 从共享总线以太网转到交换式以太网时, 所有接入设备的软件和硬件、适配器等都不需要做任何改动。





# 用以太网交换机扩展局域网



**100 BASE - T**

→ **双绞线**

→ **基带**

→ **速率为100 Mbit/s**





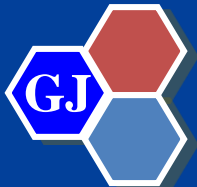
## Q23: 以太网交换机如何自学习?

- 以太网交换机是一种**即插即用**设备，其内部的帧交换表（又称为地址表）是通过**自学习**算法自动地逐渐建立起来并进行后续维护。
- 开始时，以太网交换机里面的交换表是空的。

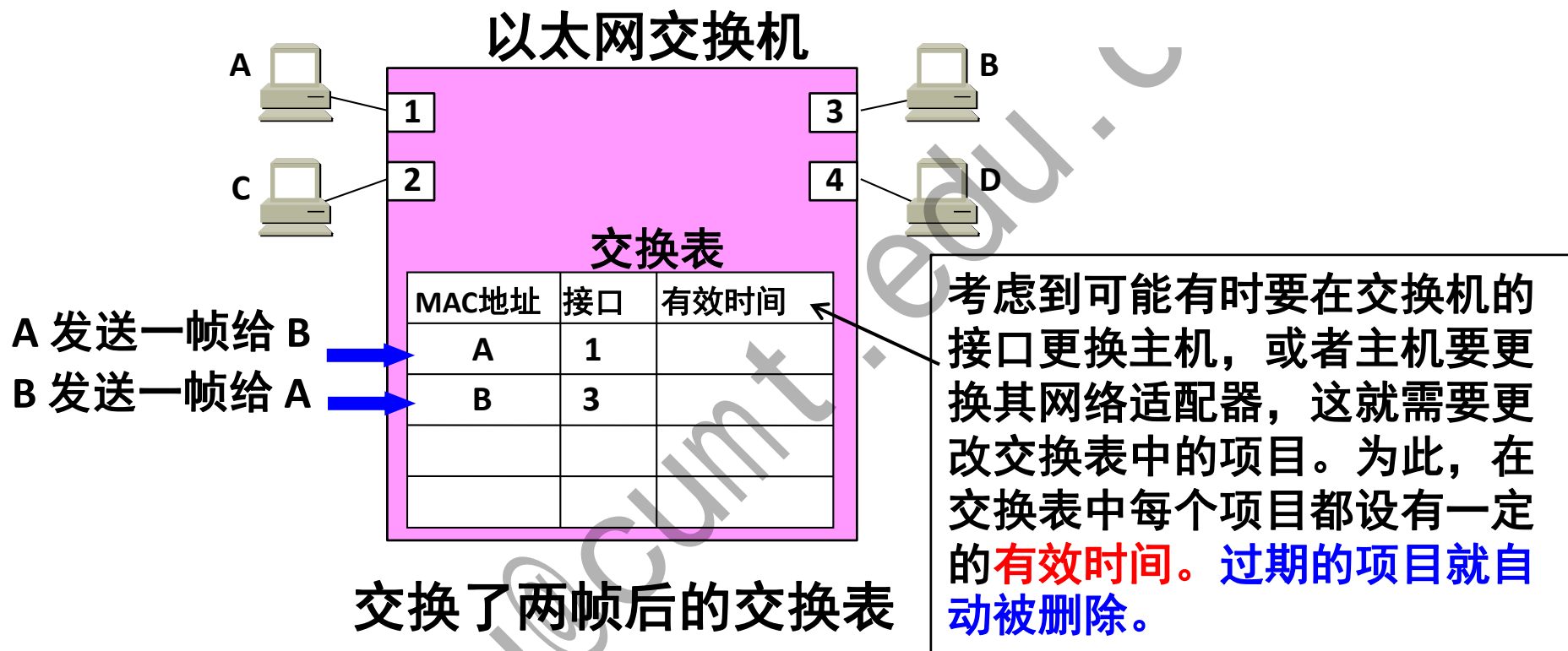


交换表一开始是空的





# 按照以下自学习算法 处理收到的帧和建立交换表



以太网交换机的这种自学习方法使得以太网交换机能够即插即用，不必人工进行配置，因此非常方便。

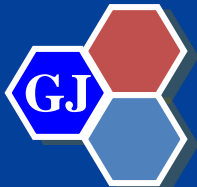




## 按照以下自学习算法 处理收到的帧和建立交换表

- A 先向 B 发送一帧，从接口 1 进入到交换机。
- 交换机收到帧后，先查找交换表，没有查到应从哪个接口转发这个帧。
- 交换机把这个帧的源地址 A 和接口 1 写入交换表中，并向除接口 1 以外的所有的接口广播这个帧。
- C 和 D 将丢弃这个帧，因为目的地址不对。只 B 才收下这个目的地址正确的帧。这也称为过滤。
- 重新写入交换表的项目 (A, 1) 可以看出，以后不管从哪一个接口收到帧，只要其目的地址是 A，就应当把收到的帧从接口 1 转发出去。



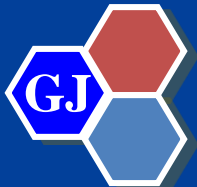


## 按照以下自学习算法 处理收到的帧和建立交换表

- B 通过接口 3 向 A 发送一帧。
- 交换机查找交换表，发现交换表中的 MAC 地址有 A。表明要发送给 A 的帧（即目的地址为 A 的帧）应从接口 1 转发。于是就把这个帧传送到接口 1 转发给 A。显然，现在已经没有必要再广播收到的帧。
- 交换表这时新增加的项目 (B, 3)，表明今后如有发送给 B 的帧，就应当从接口 3 转发出去。
- 经过一段时间后，只要主机 C 和 D 也向其他主机发送帧，以太网交换机中的交换表就会把转发到 C 或 D 应当经过的接口号（2 或 4）写入到交换表中。







# 交换机自学习和转发帧的步骤归纳

- 交换机收到一帧后先进行**自学习**。查找交换表中与收到帧的**源地址有无相匹配**的项目。
  - 如没有，就在交换表中增加一个项目（源地址、进入的接口和有效时间）。
  - 如有，则把原有的项目进行更新（进入的接口或有效时间）。
- **转发帧**。查找交换表中与收到帧的**目的地址有无相匹配**的项目。
  - 如没有，则向所有其他接口（进入的接口除外）转发。
  - 如有，则按交换表中给出的接口进行转发。
  - 若交换表中给出的接口就是该帧进入交换机的接口，则应丢弃这个帧（因为这时不需要经过交换机进行转发）。





## Q24: 以太网交换机如何工作?

- 以太网交换机使用**专用集成电路**(Application Specified Integrated Circuit, **ASIC**)处理数据帧的交换操作, 其转发速率要比使用软件转发的网桥快很多, 在很多机型上都能实现以**缆线速度**(Wired Speed)交换。
- 以太网交换机一般都具有**多种速率的接口**, 方便了各种不同情况的用户。
- 以太网交换机的**接口有存储器**, 能在输出端口繁忙时把到来的帧进行缓存。





# 以太网交换机的转发方式

- 存储转发方式
  - 把整个数据帧先缓存后再进行处理。
- 直通 (cut-through) 方式
  - 接收数据帧的同时就立即按数据帧的目的 MAC 地址决定该帧的转发接口，因而提高了帧的转发速度。
  - 缺点是它不检查差错就直接将帧转发出去，因此有可能也将一些无效帧转发给其他的站。

在某些情况下，仍需要采用基于软件的存储转发方式进行交换，例如，当需要进行线路速率匹配、协议转换或差错检测时。





# 以太网交换机提升了网络总容量

- 以太网交换机的每个接口都直接与一个单台主机或另一个以太网交换机相连，并且一般都工作在全双工方式。
- 以太网交换机具有并行性。
  - 能同时连通许多对的接口，使每一对相互通信的主机都能像独占通信媒体那样，进行无碰撞地传输数据，即多对主机能同时通信。
- 用户独享带宽，增加了总容量。

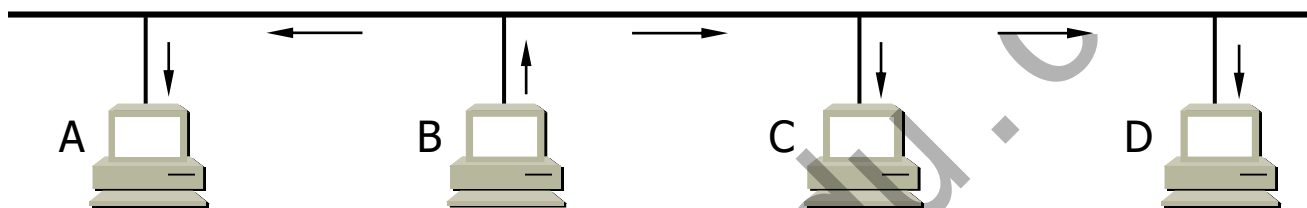




# 三种以太网的比较

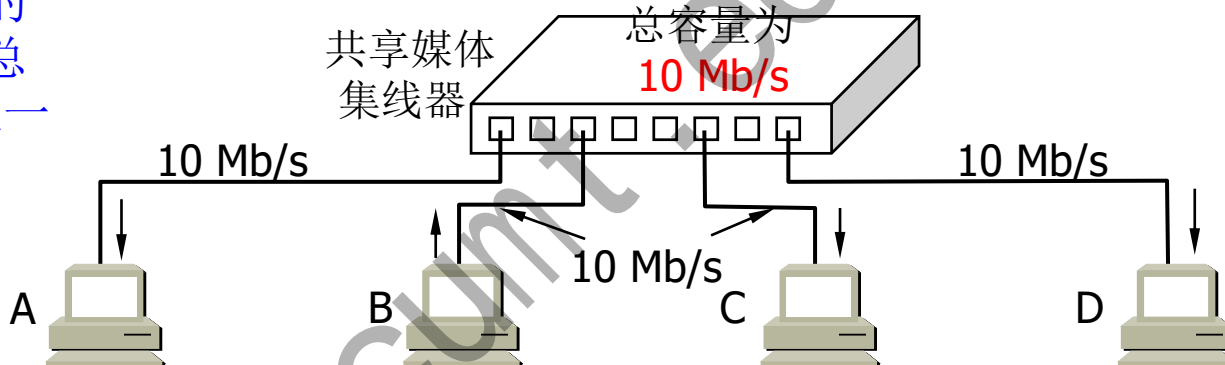
共享总线 10 Mb/s

(a)



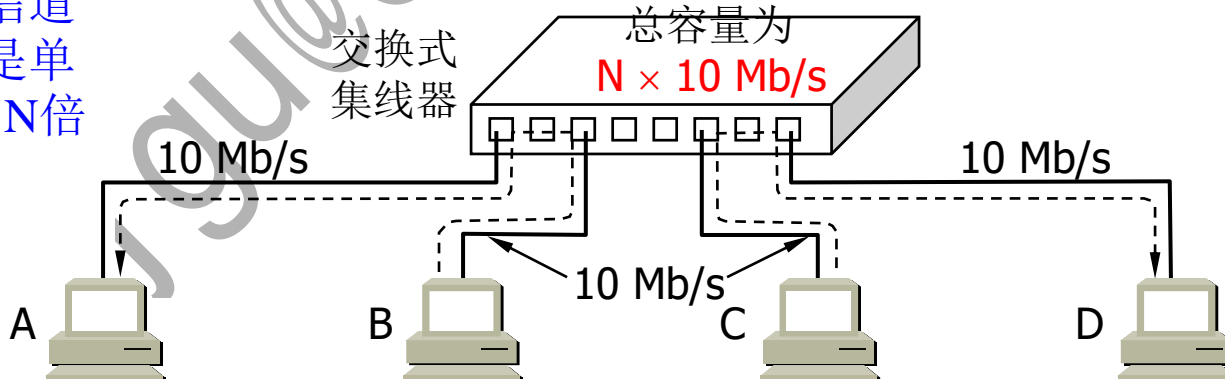
每个用户占有的  
平均带宽只有总  
带宽的  $N$  分之一

(b)



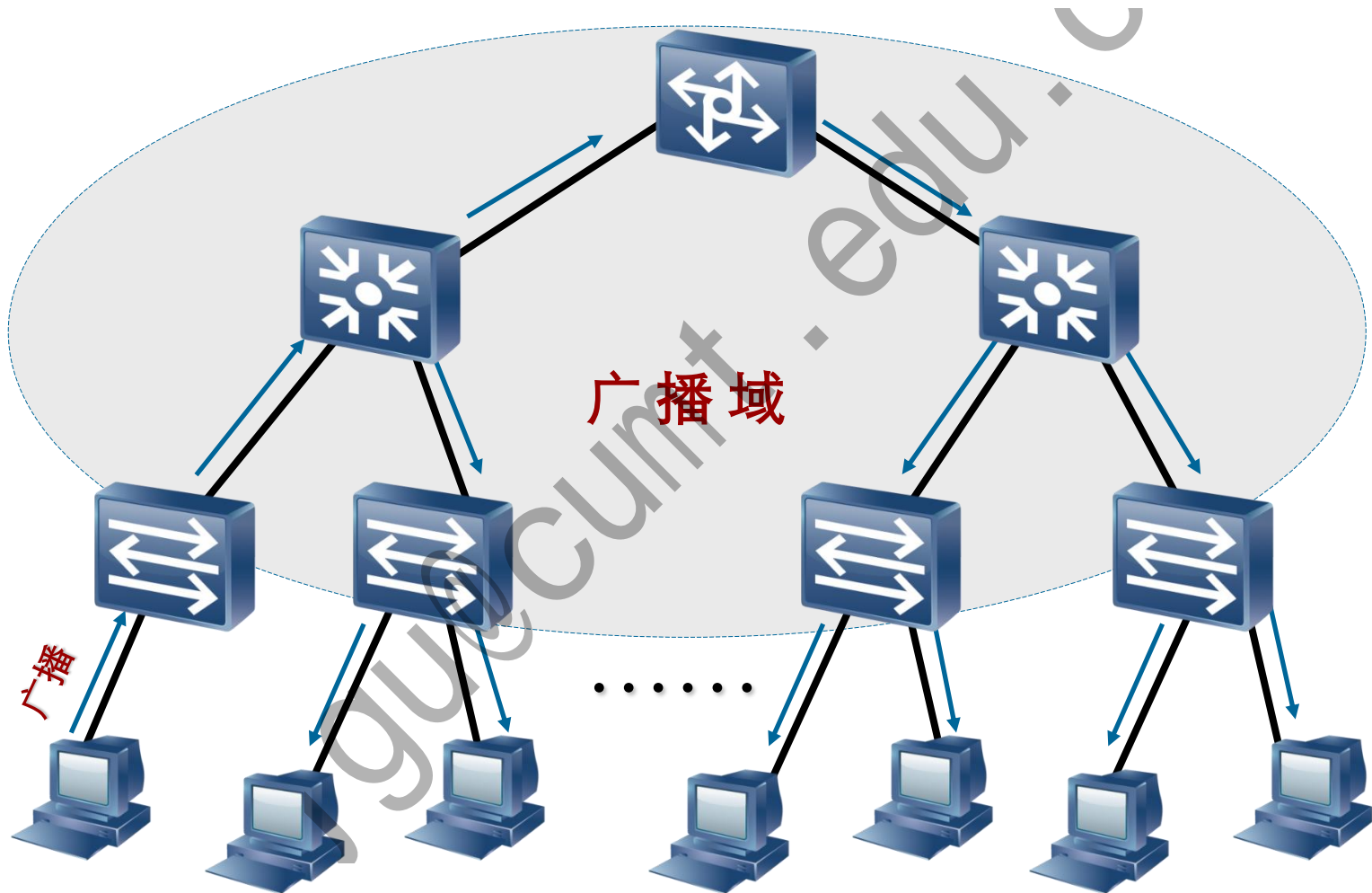
每个用户独占信道  
带宽，总容量是单  
个接口带宽的  $N$  倍

(c)





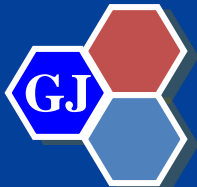
# Q25: 什么是广播域和广播风暴?



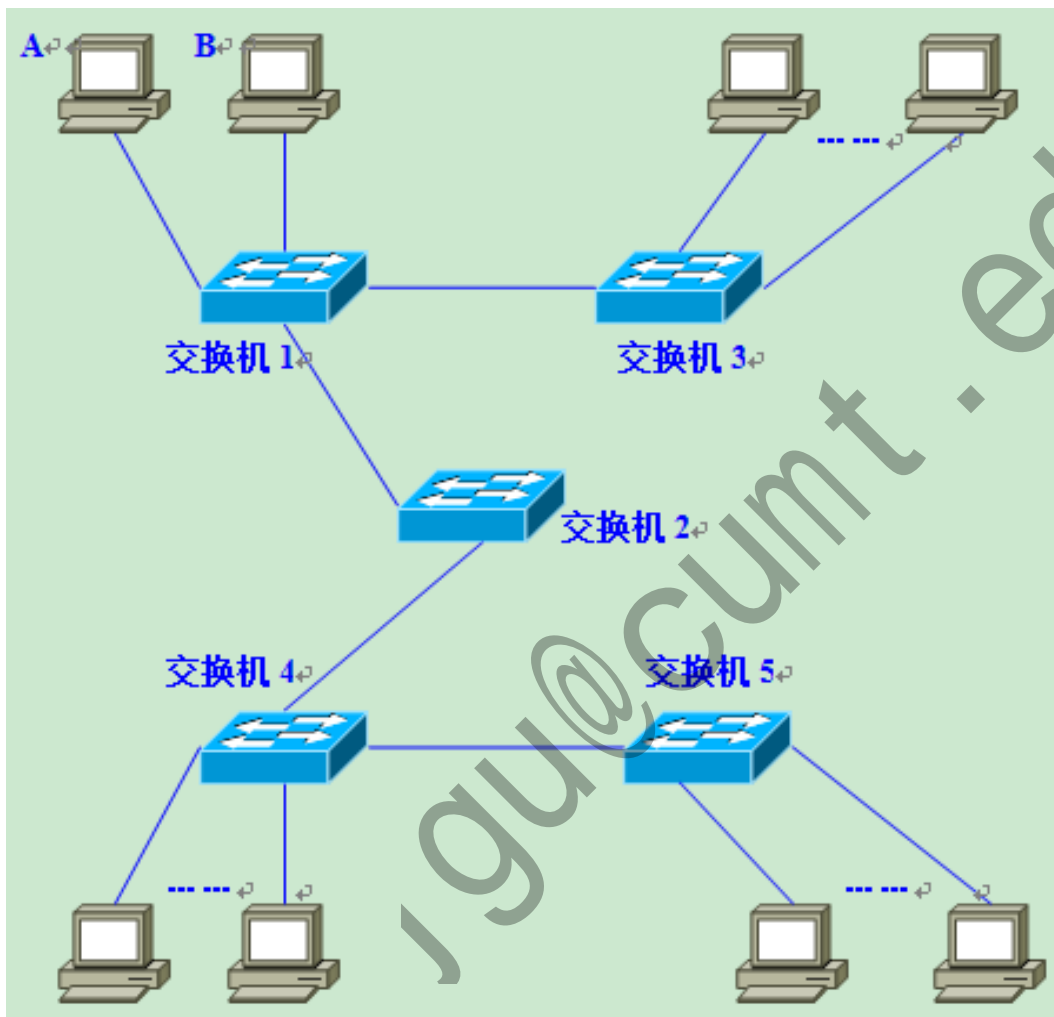


- **广播**，指一个数据帧被传输到本地网段（由广播域定义）上的每个节点就是广播，该帧被称为广播帧(目标MAC地址全部为1)。
- **广播域**，指的是广播帧所能传递到的范围，亦即能够直接通信的范围。
  - 严格地说，并不仅仅是广播帧，多播帧(Multicast Frame)和目标不明的单播帧(Unknown Unicast Frame)也能在同一个广播域中畅行无阻。
- **广播风暴**，由于网络拓扑的设计和连接问题，或其他原因导致广播在网段内大量复制，传播数据帧，导致网络性能下降，甚至网络瘫痪，这就是广播风暴。





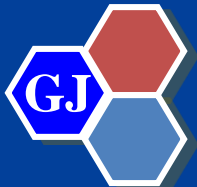
# 交换网络中的广播域问题——以ARP为例



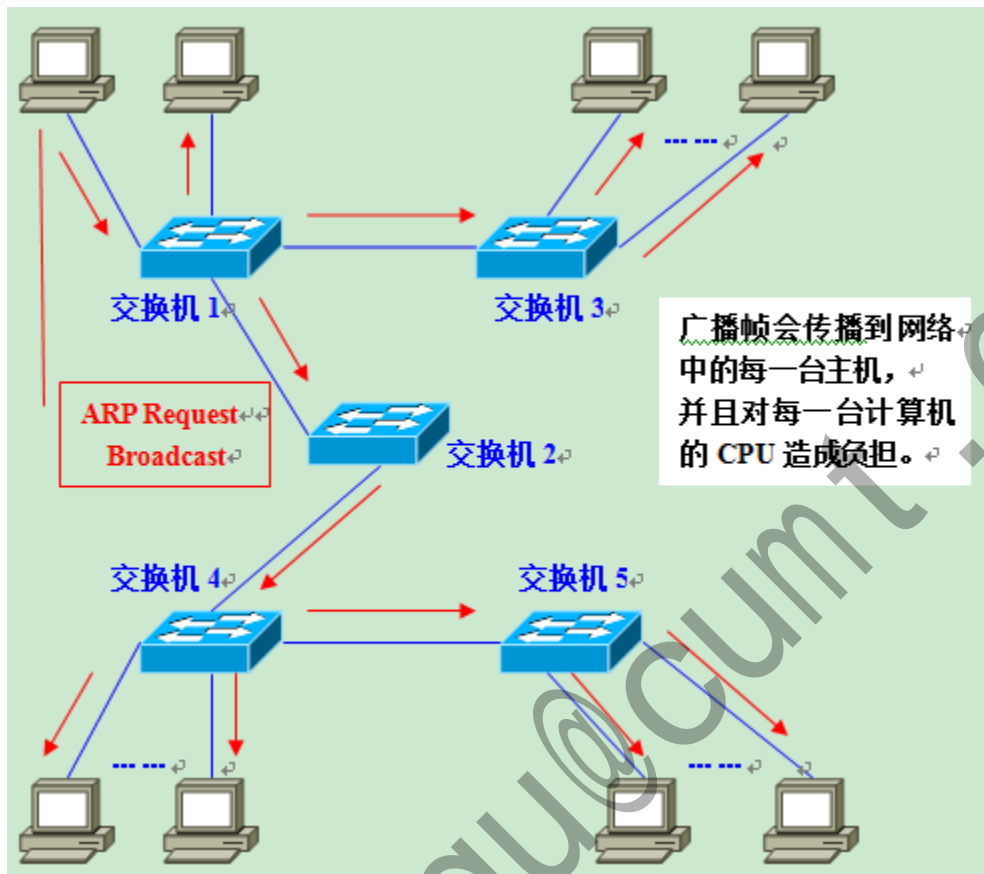
假设，计算机A需要与计算机B通信。在基于以太网的通信中，必须在数据帧中指定目标MAC地址才能正常通信，因此计算机A必须先广播“ARP请求(ARP Request)信息”，来尝试获取计算机B的MAC地址。







# 交换网络中的广播域问题——以ARP为例



交换机1收到广播帧(ARP请求)后，会将其转发给除接收端口外的其他所有端口。接着，交换机2、3、4、5收到广播帧后都会按照同样的方式进行转发。最终ARP请求会被转发到同一网络中的所有客户机上。

由此可见，原本是为了获得B的MAC地址而发出的ARP请求数据帧却传遍整个网络，导致所有的计算机都收到了它。造成整体网络带宽和CPU运算能力的大量无谓消耗。





# 为什么广播帧信息会经常出现？

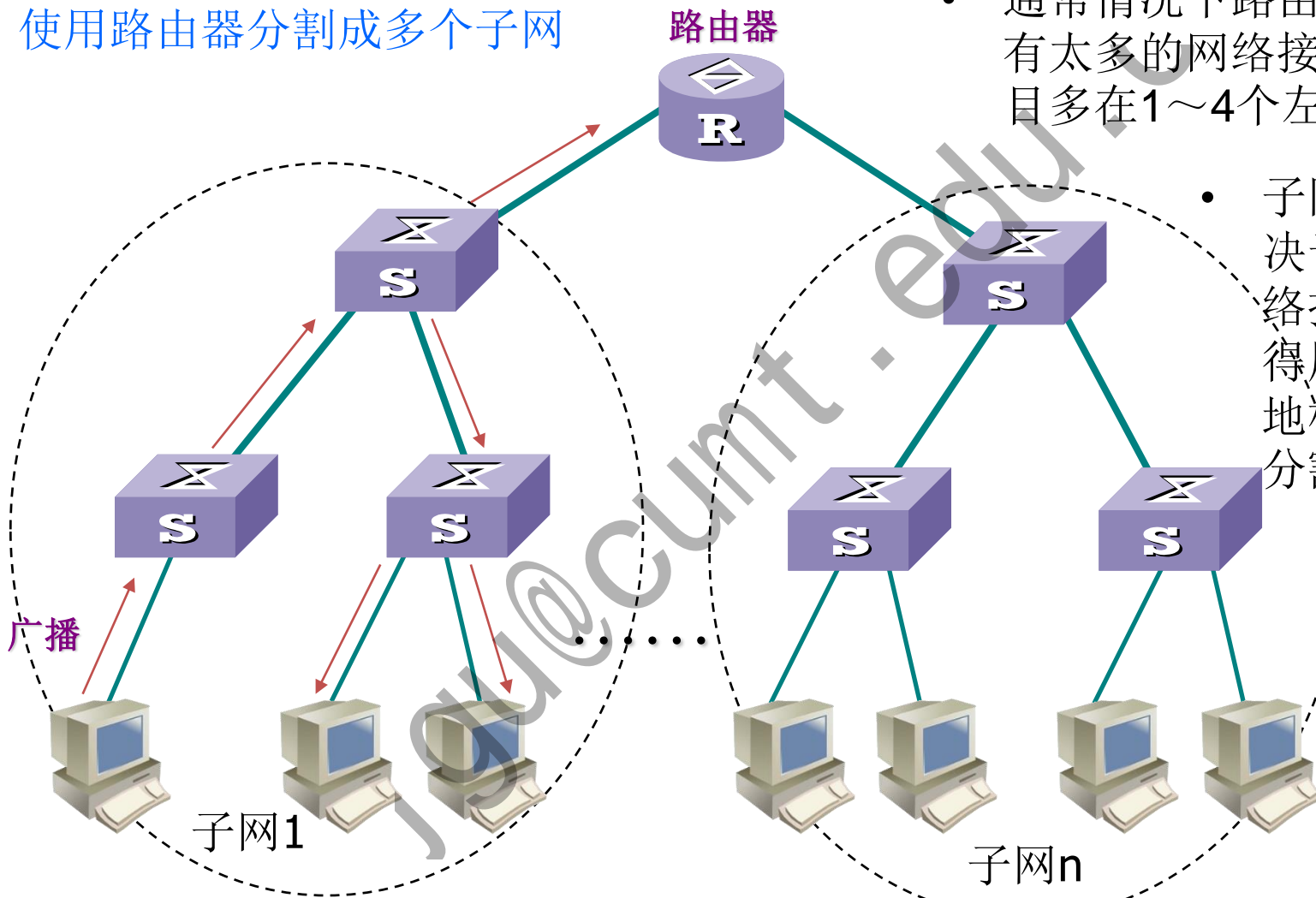
- 利用TCP/IP协议栈通信时，除了前面出现的ARP外，还有可能需要发出DHCP、RIP等很多其他类型的广播信息。
  - ARP广播，是在需要与其他主机通信时发出的。
  - 当客户机请求DHCP服务器分配IP地址时，就必须发出DHCP的广播。
  - 而使用RIP作为路由协议时，每隔30秒路由器都会对邻近的其他路由器广播一次路由信息。
  - RIP以外的其他路由协议使用多播传输路由信息，这也会被交换机转发(Flooding)。
- 解决广播域过大的方法是分割广播域，将一个大范围的广播域变成多个小范围的广播域。





# 通过路由器将网络分段隔离广播风暴

使用路由器分割成多个子网



- 通常情况下路由器上不会有太多的网络接口，其数目多在1~4个左右。

- 子网个数完全取决于路由器的网络接口个数，使得用户无法自由地根据实际需要分割广播域。

引入VLAN解决广播报文的泛滥问题

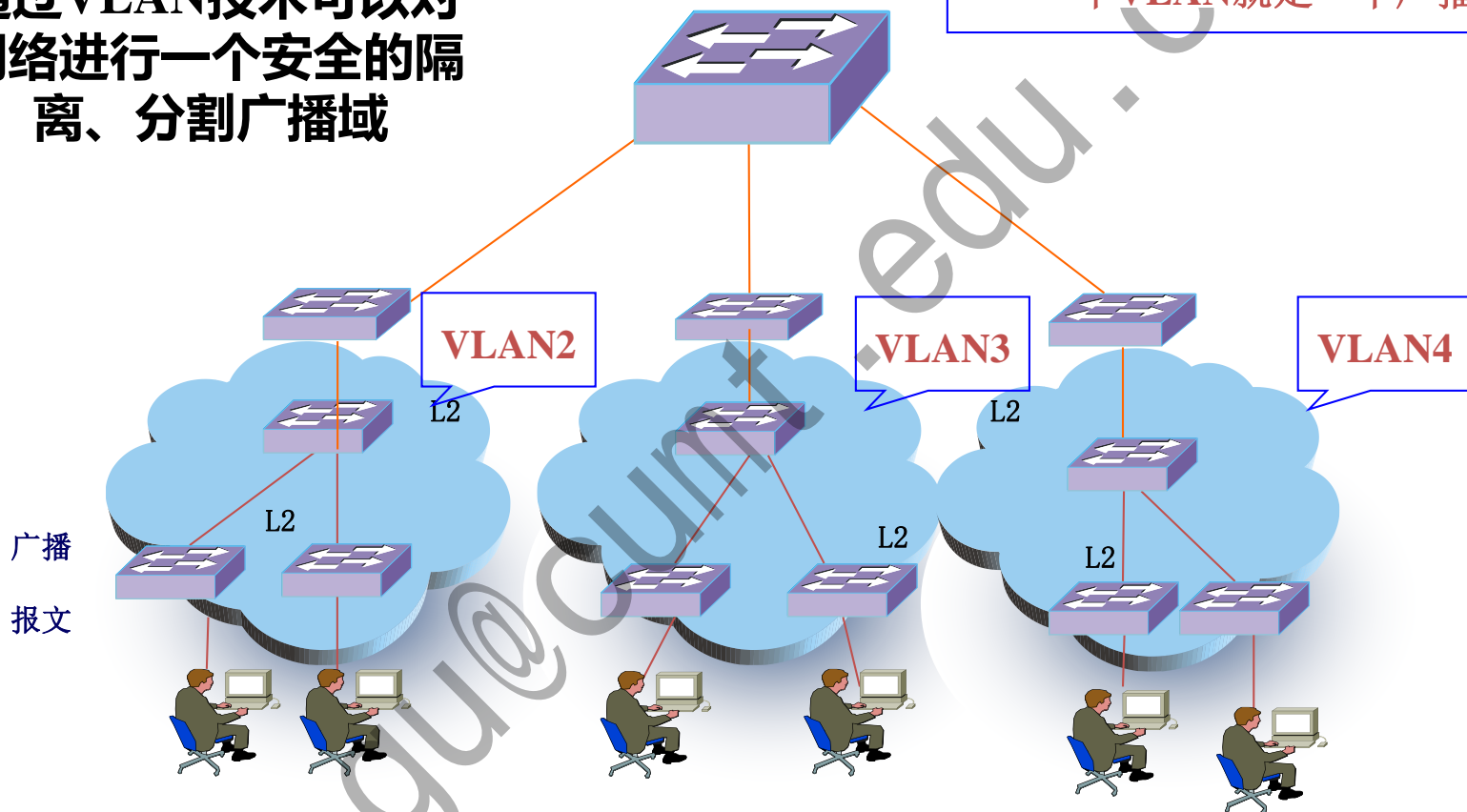




# Q26: 什么是虚拟局域网?

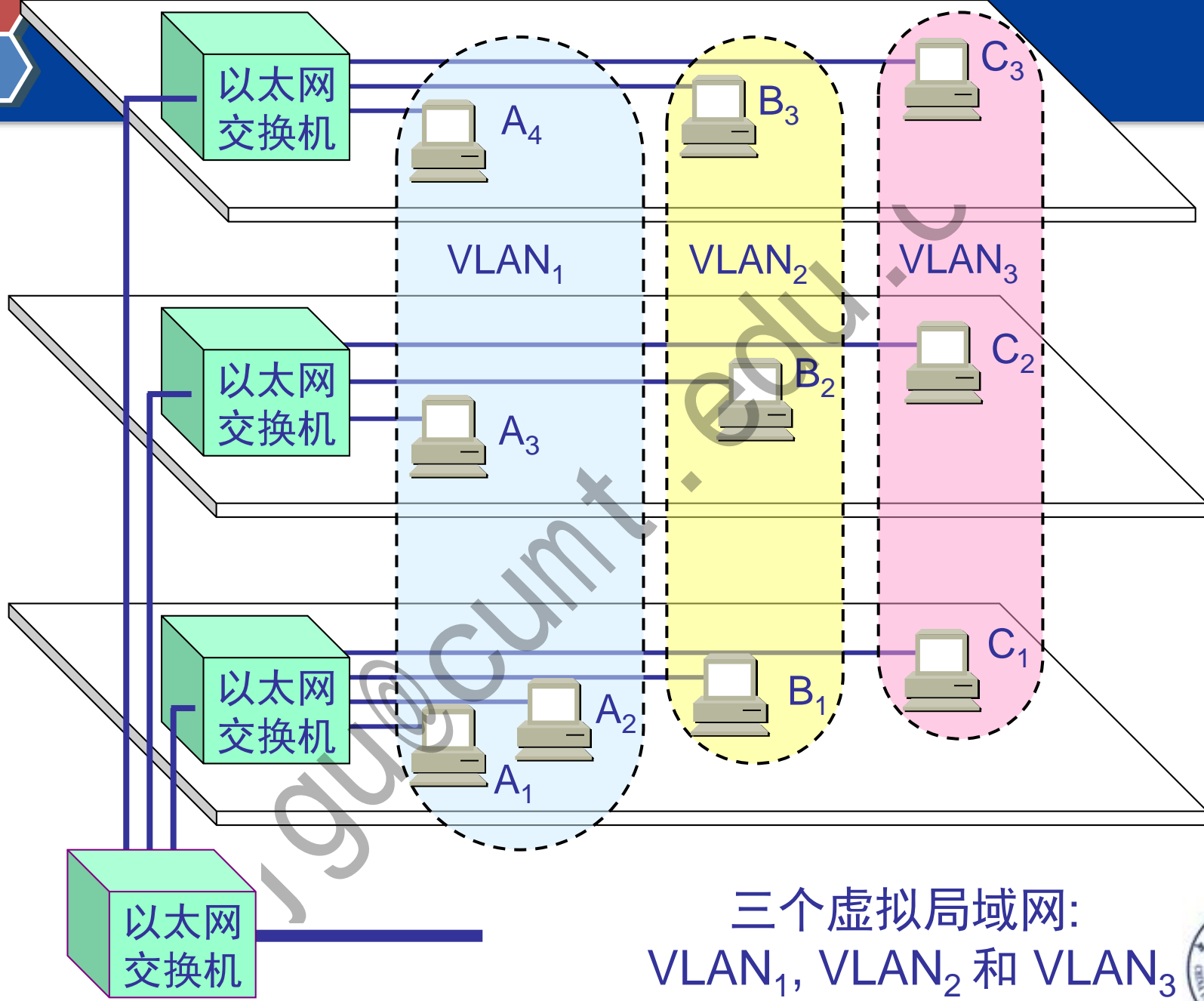
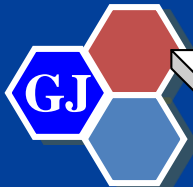
通过VLAN技术可以对网络进行一个安全的隔离、分割广播域

一个VLAN就是一个广播域



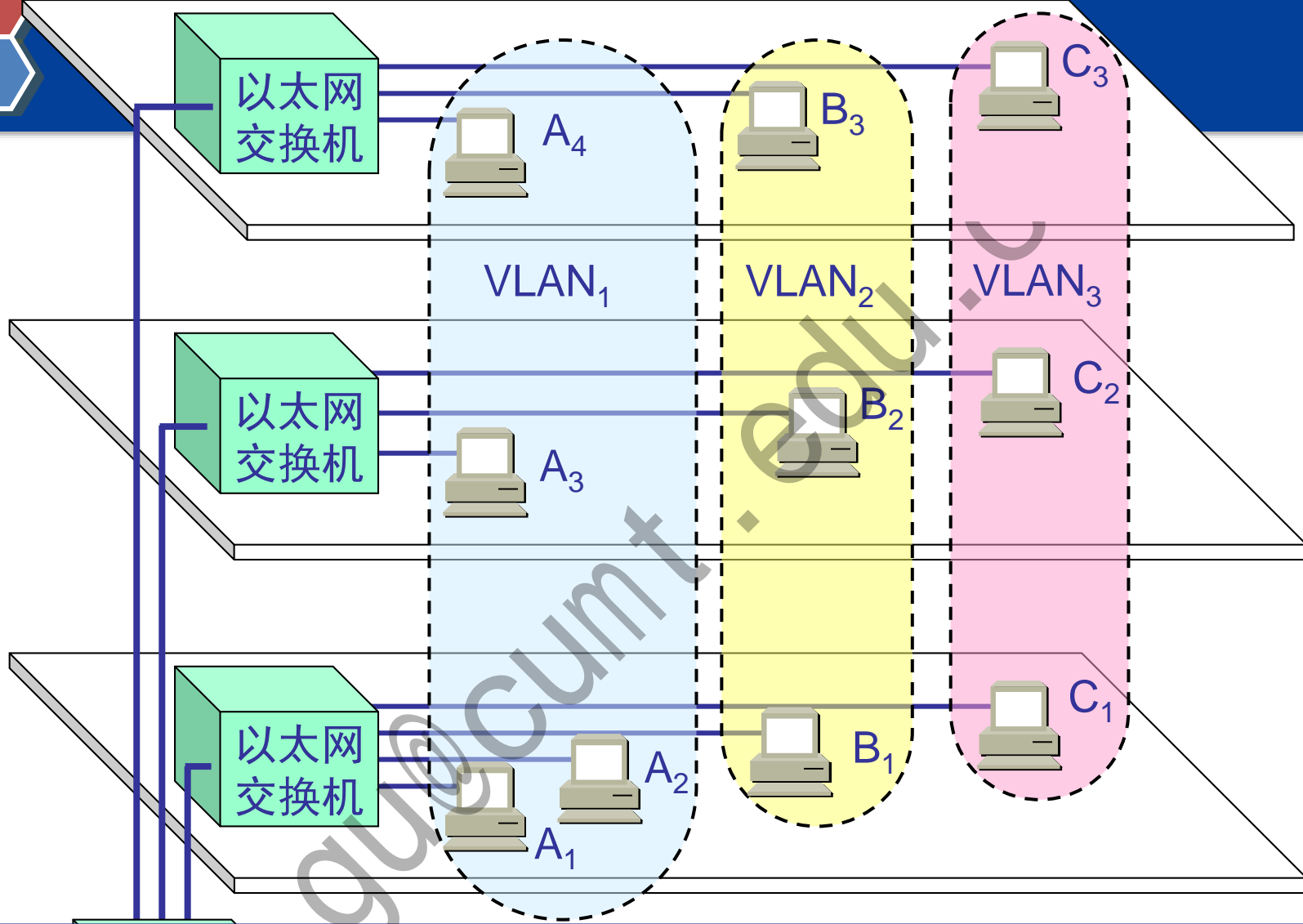
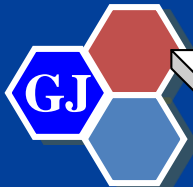
与路由器相比，二层交换机一般带有多个网络接口，用来分割广播域可以大大提高运用上的灵活性。





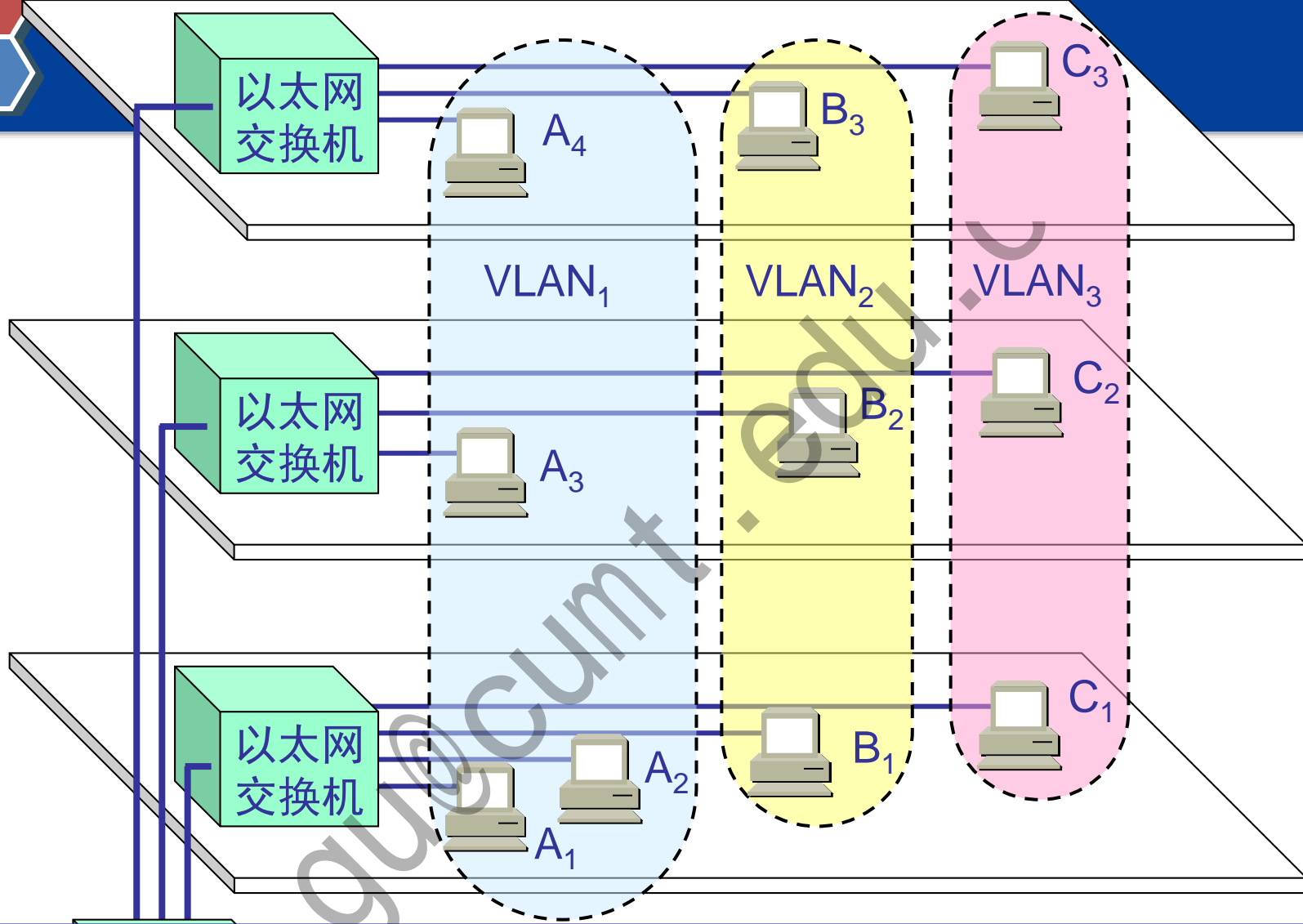
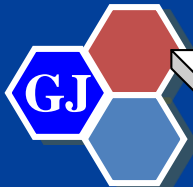
三个虚拟局域网：  
VLAN<sub>1</sub>, VLAN<sub>2</sub> 和 VLAN<sub>3</sub>





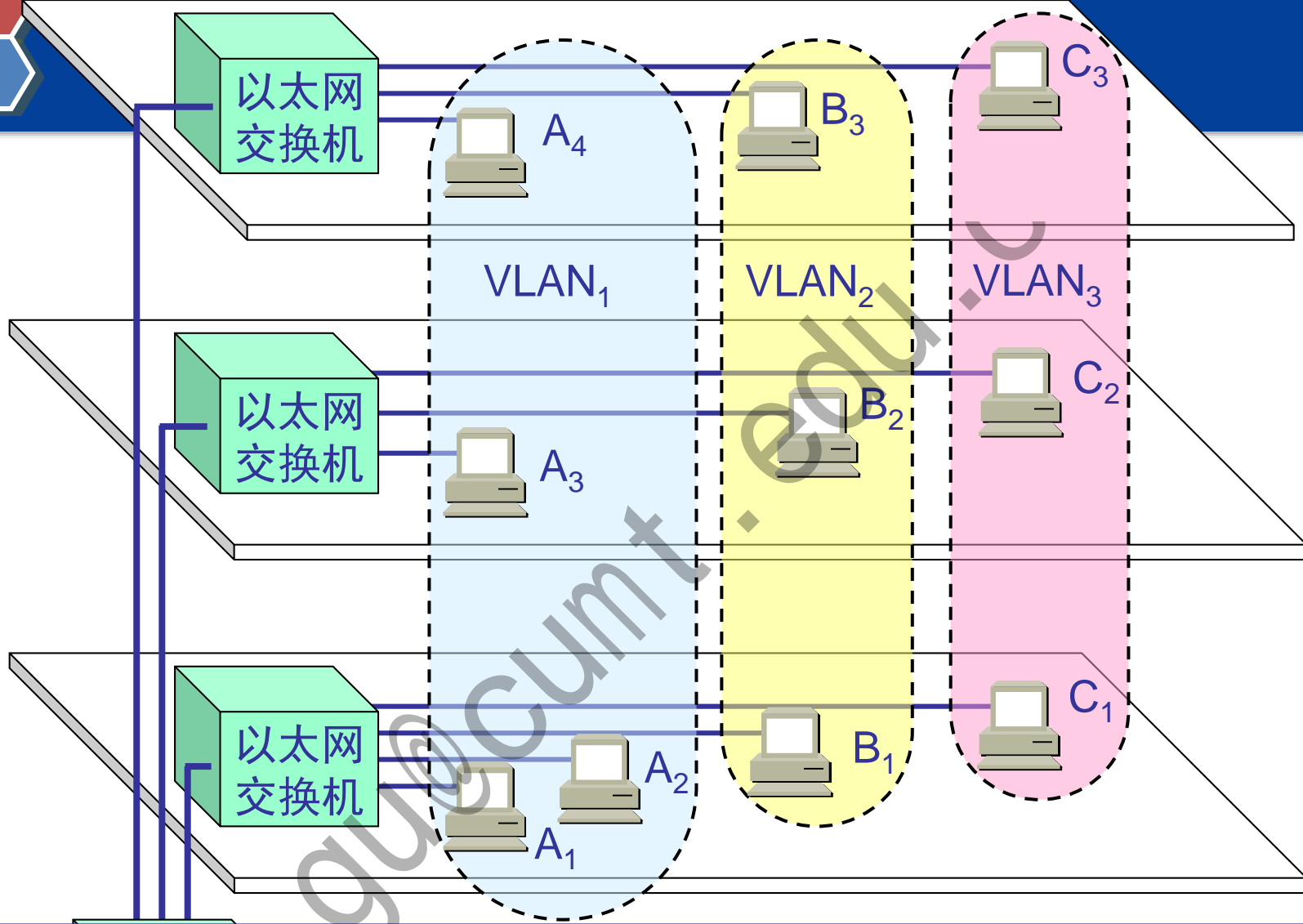
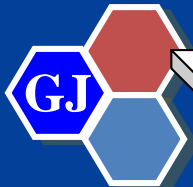
当 B<sub>1</sub> 向 VLAN<sub>2</sub> 工作组内成员发送数据时，  
工作站 B<sub>2</sub> 和 B<sub>3</sub> 将会收到广播的信息。





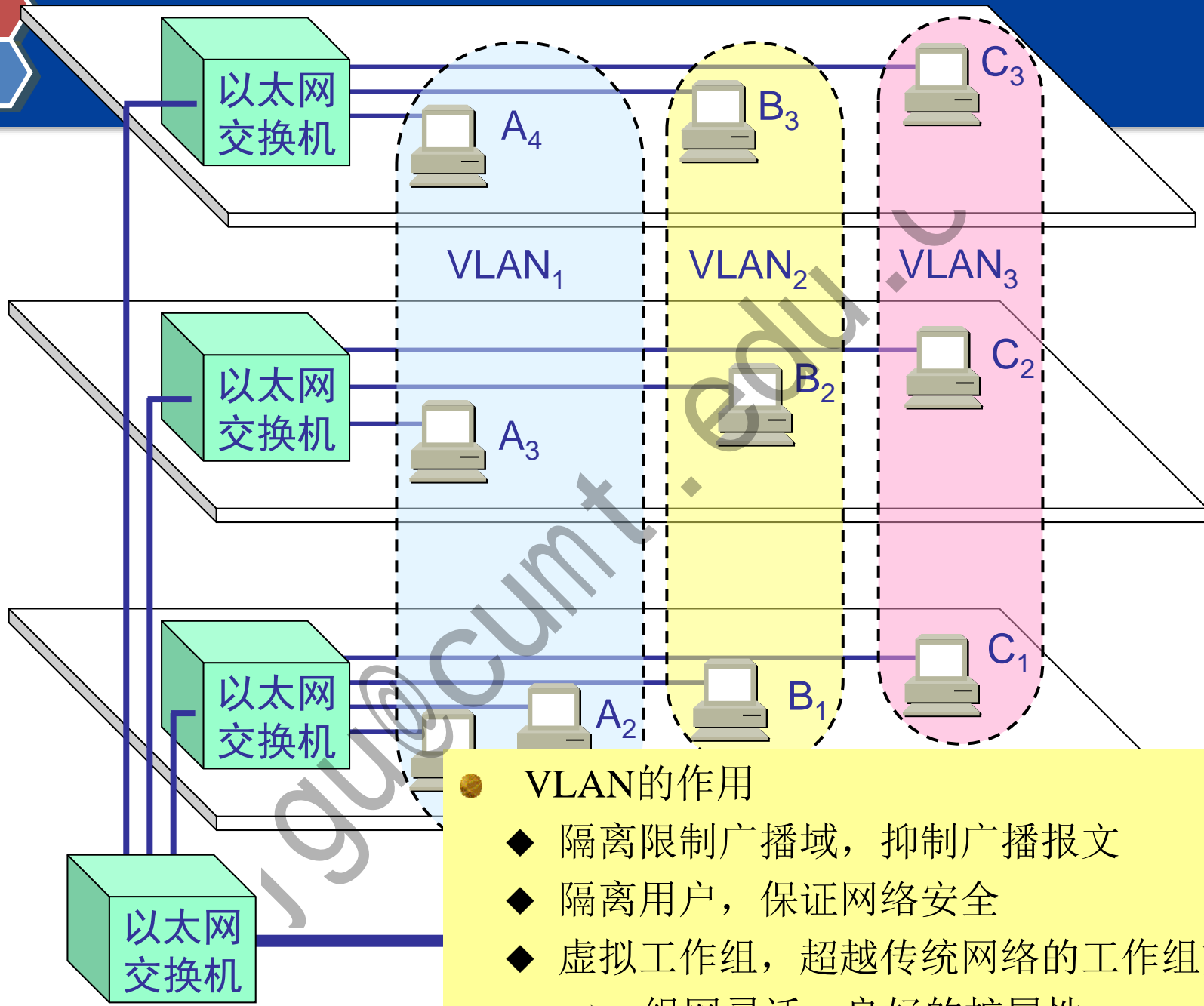
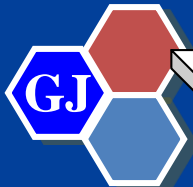
B<sub>1</sub> 发送数据时，工作站 A<sub>1</sub>, A<sub>2</sub> 和 C<sub>1</sub> 都不会收到 B<sub>1</sub> 发出的广播信息。





虚拟局域网限制了接收广播信息的工作站数，使得网络不会因传播过多的广播信息（即“广播风暴”）而引起性能恶化。





### ● VLAN的作用

- ◆ 隔离限制广播域，抑制广播报文
- ◆ 隔离用户，保证网络安全
- ◆ 虚拟工作组，超越传统网络的工作组方式
  - 组网灵活、良好的扩展性



## Q27: VLAN的定义方法?

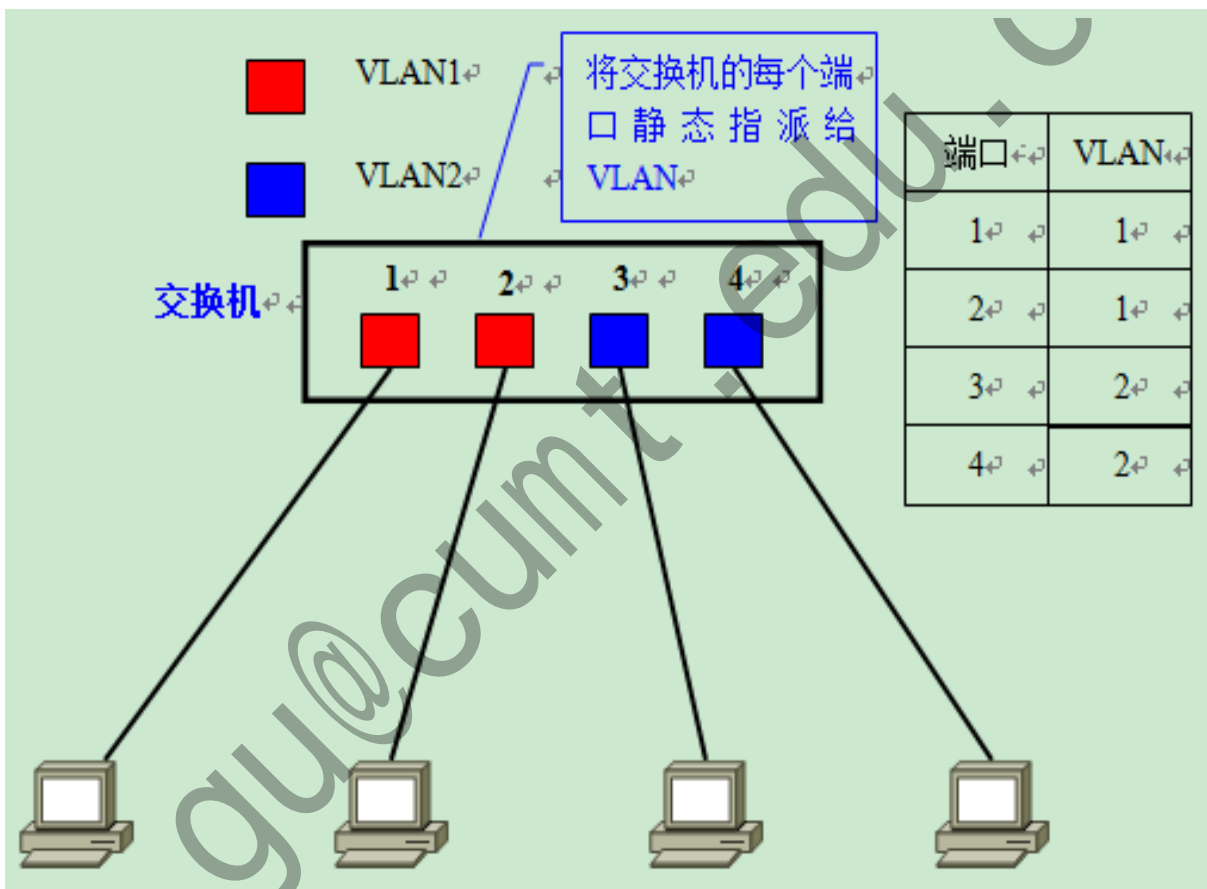
最常用的方法

- 基于端口的VLAN
  - 根据以太网交换机的端口来划分VLAN，管理员只要管理和配置交换端口，而不管交换端口连接什么设备
- 基于MAC地址的VLAN
  - 根据每个主机网卡的MAC地址来划分VLAN，当设备移动时，VLAN能够自动识别，而无需重新配置，当网络规模很大时，会给管理带来难度
- 基于IP地址的VLAN
  - 根据每个主机的IP地址划分VLAN，只要用户的IP地址不变，VLAN号也不变
- 基于策略的VLAN
  - 根据MAC、IP、以太网协议类型、上层应用等来进行灵活的划分



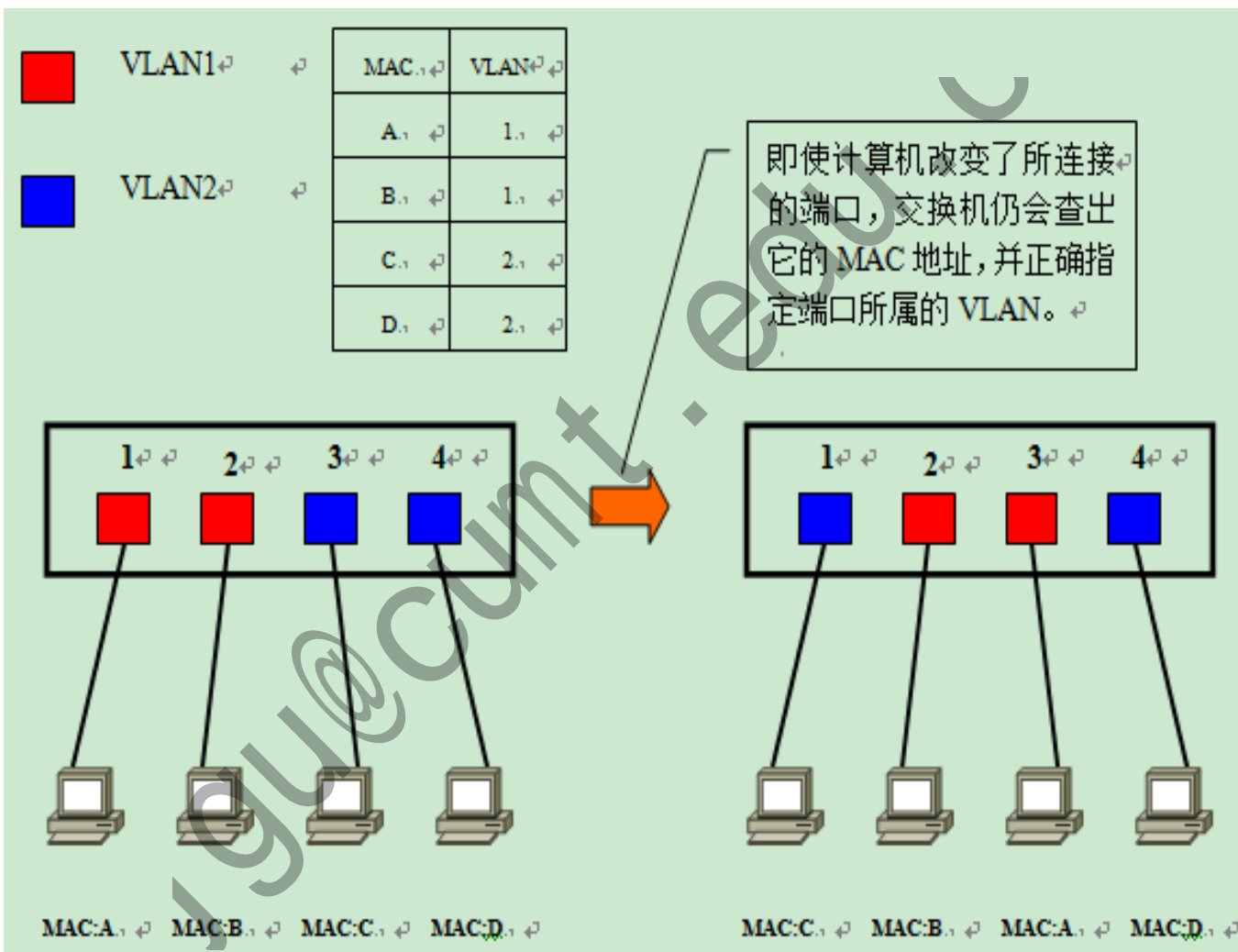


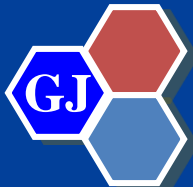
# 静态VLAN——基于端口



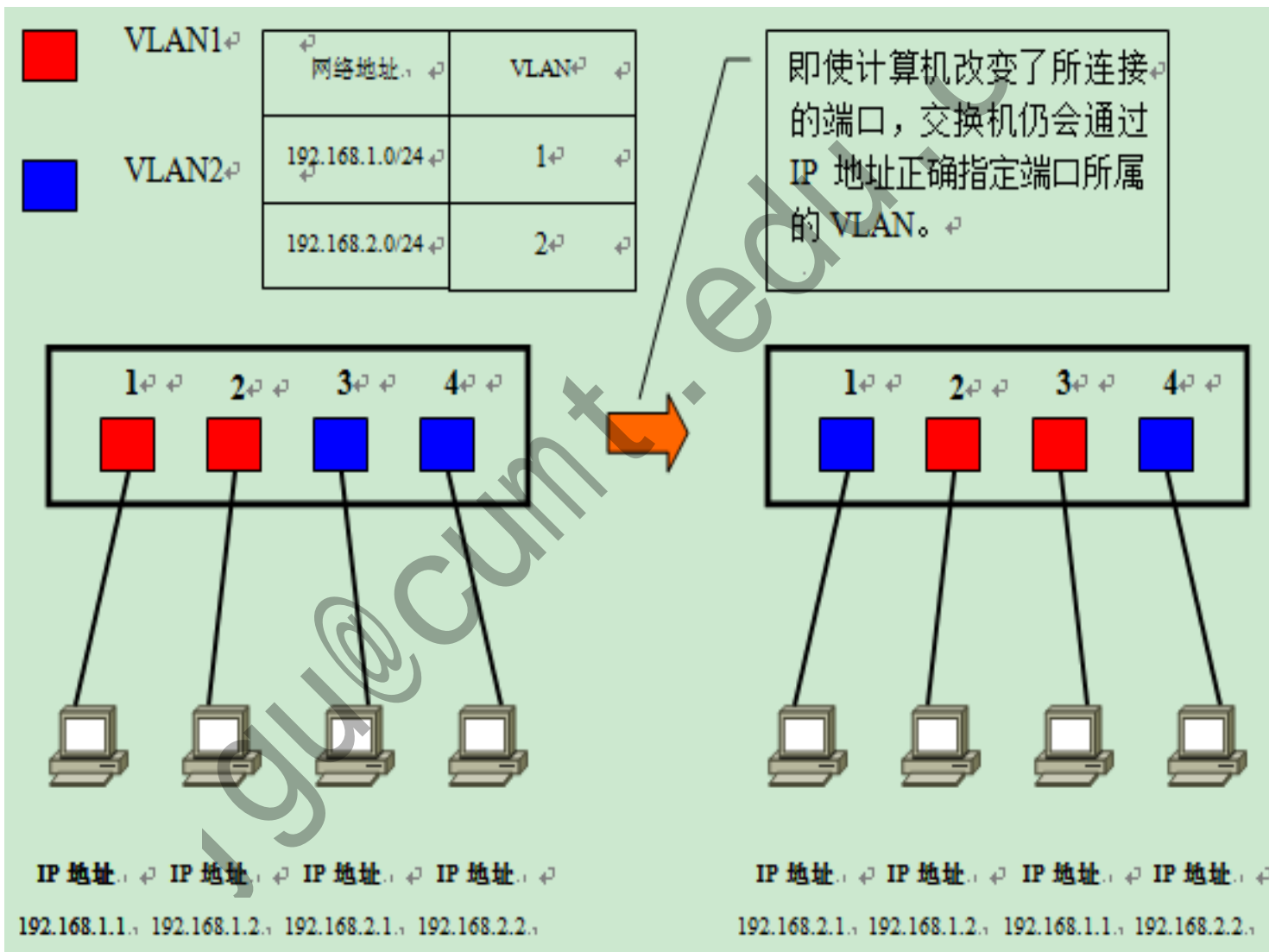


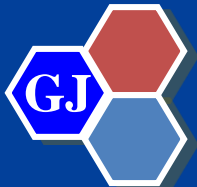
# 动态VLAN——基于MAC地址





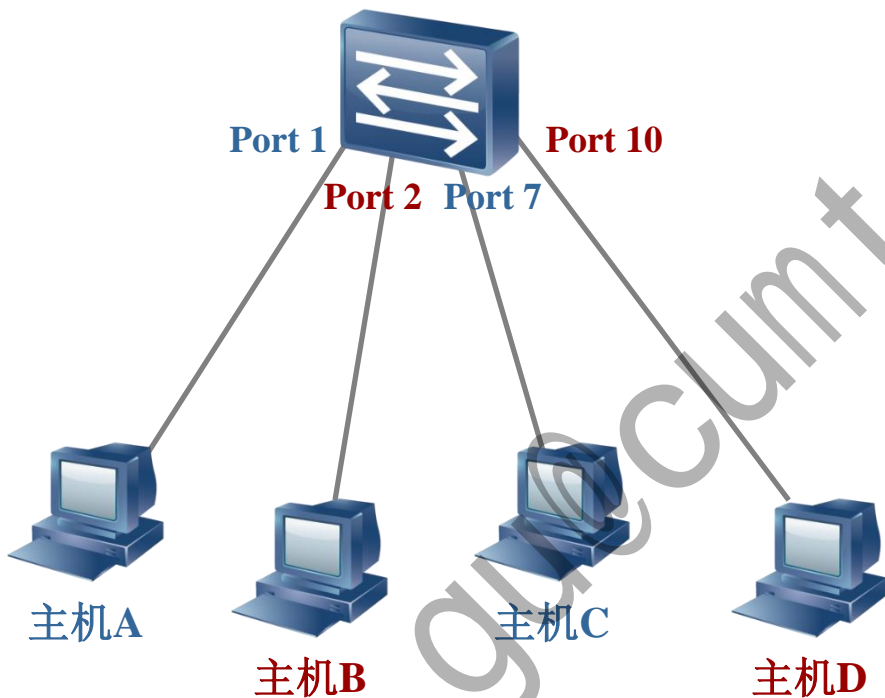
# 动态VLAN——基于IP地址





# Q28: 基于端口的VLAN划分技术?

## 单交换机中基于端口的VLAN划分



VLAN表

端口	所属VLAN
Port1	VLAN5
Port2	VLAN10
.....	.....
Port7	VLAN5
.....	.....
Port10	VLAN10

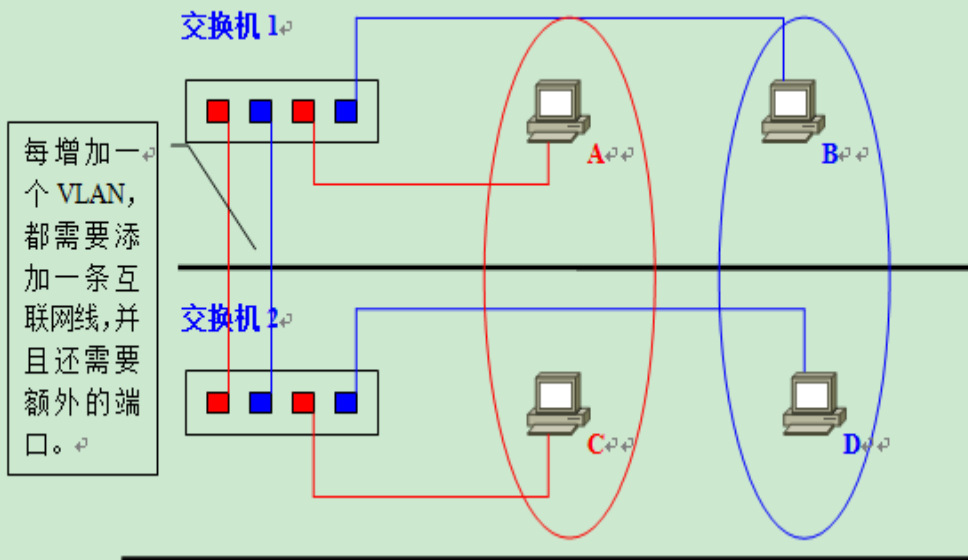


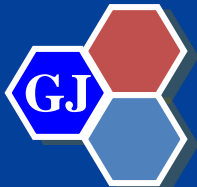


# 横跨多台交换机的VLAN构建

关键是“交换机1和交换机2该如何连接才好呢？”

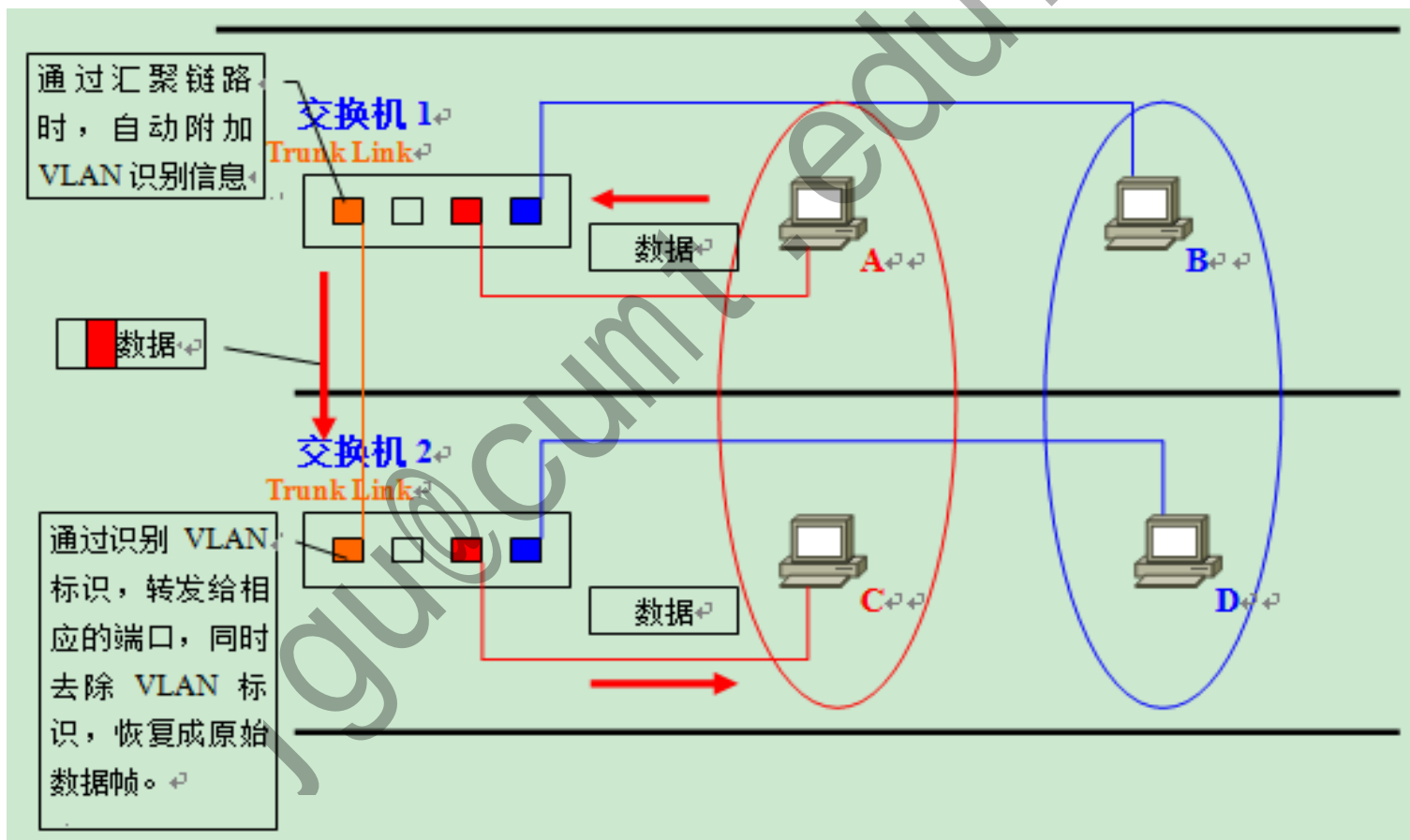
最简单的方法，自然是在交换机1和交换机2上各设一个红、蓝VLAN专用的接口并互联。  
从扩展性和管理效率来看都不好。





# 汇聚链接(Trunk Link)

- ◆ 汇聚链接(Trunk Link)指的是能够转发多个不同VLAN的通信的端口。



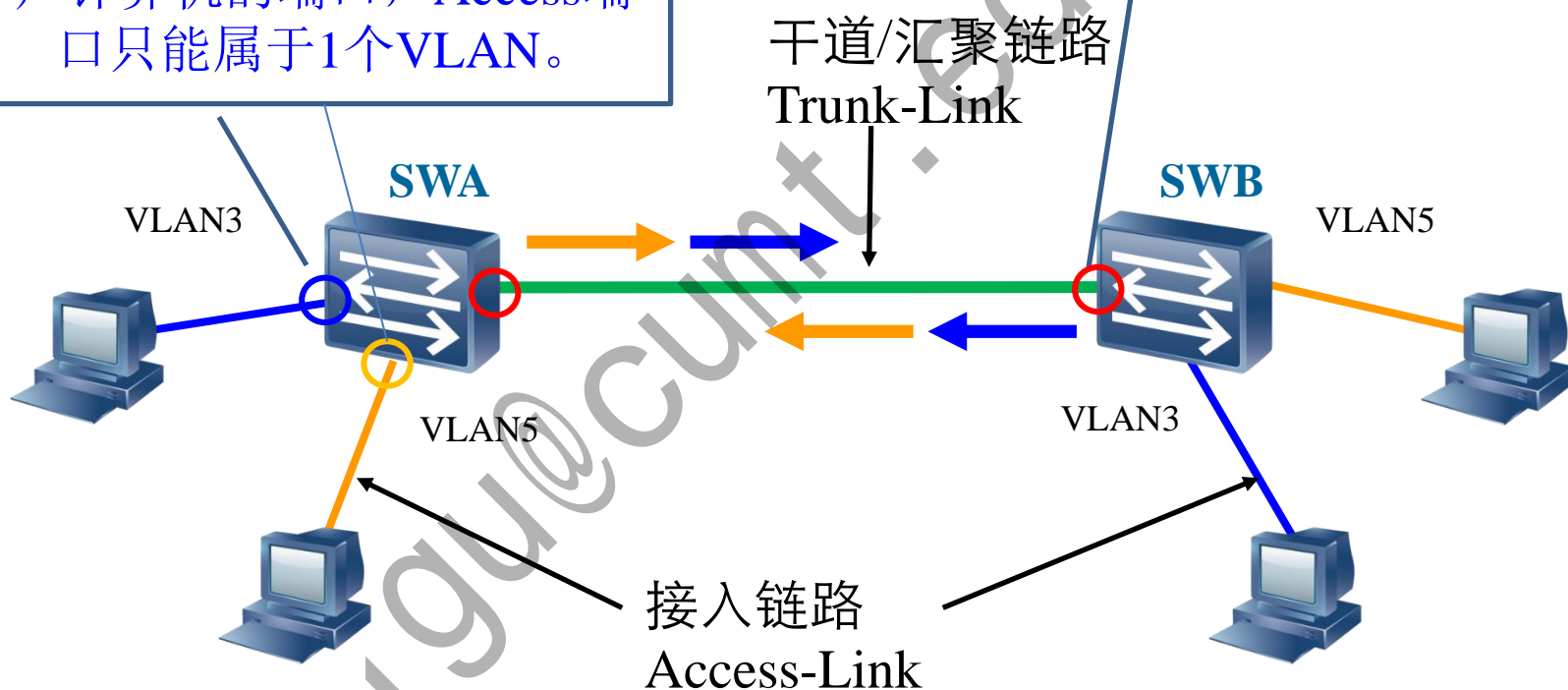




# 新的链路和端口类型

**Access端口：**一般用于接用户计算机的端口，Access端口只能属于1个VLAN。

**Trunk端口：**一般用于交换机之间连接的端口（交换机均具备Vlan协议功能），Trunk端口可以属于多个VLAN，可以接收和发送多个VLAN的报文。



**VLAN数据通过Trunk链路跨越多台交换机转发**

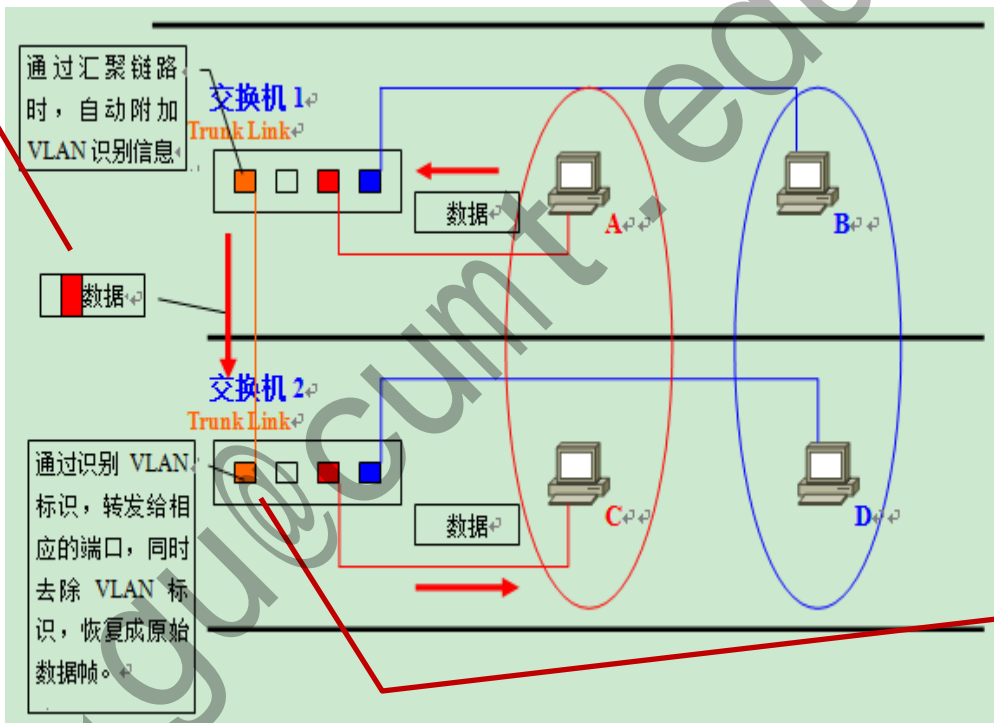




# VLAN数据的跨交换机转发

- ◆ 汇聚链路上流通的数据帧，都被附加了用于识别分属于哪个VLAN的**特殊信息**。

A发送的数据帧从交换机1经过汇聚链路到达交换机2时，在数据帧上附加了表示属于红色VLAN的标记。



交换机2收到数据帧后，经过检查VLAN标识发现这个数据帧是属于红色VLAN的，因此去除标记后根据需要将复原的数据帧只转发给其他属于红色VLAN的端口。

如何标识不同VLAN的数据帧？





# 802.1Q协议

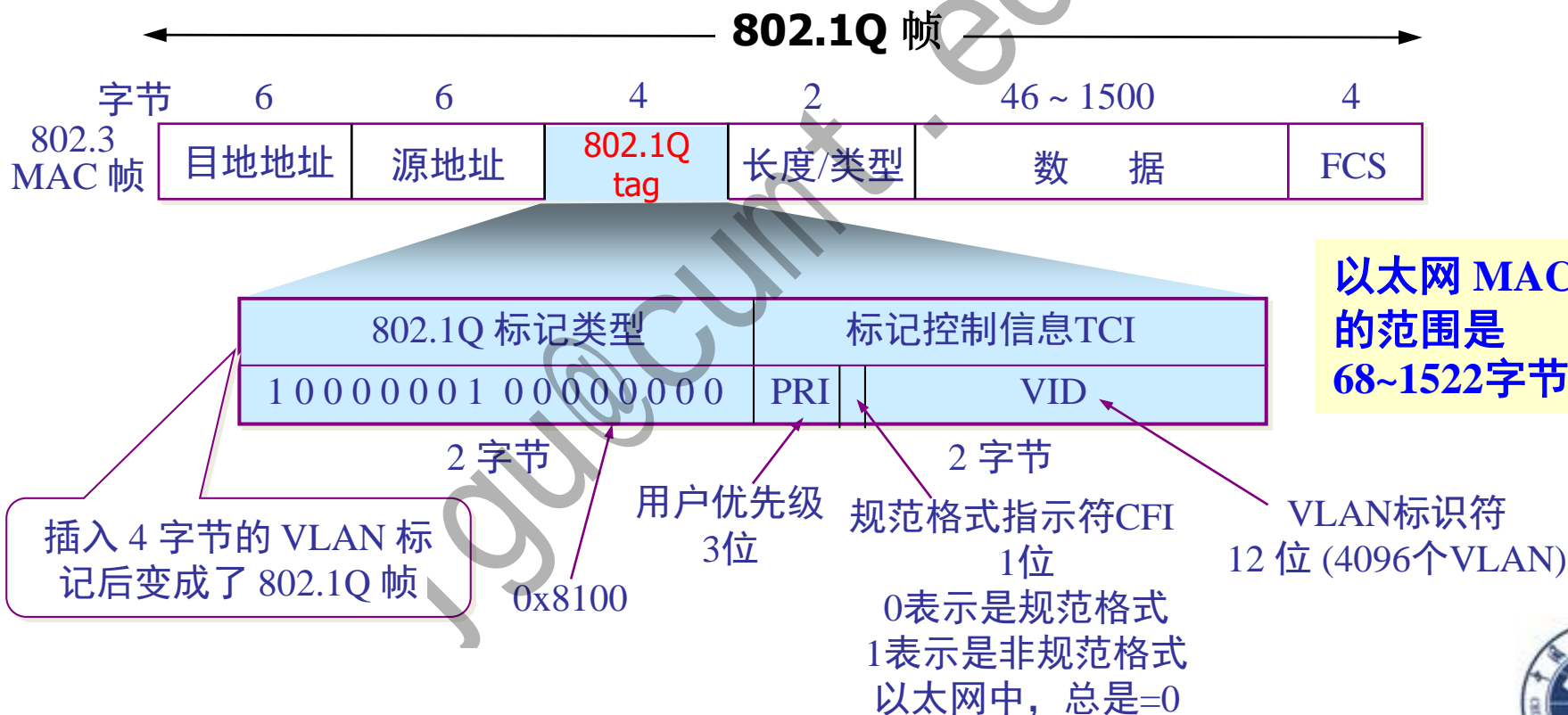
- 802.1Q是IEEE组织批准的一套VLAN协议，它定义了基于端口的VLAN模型，为标识带有VLAN成员信息的以太网帧建立了一种标准方法，是一种使用得最多最广泛的成熟协议。
- 802.1Q协议主要用来解决如何将大型网络划分为多个小网络，这样广播和组播流量就不会占据更多的带宽。此外还提供更高的网络段间安全性。
- 基本原理：
  - 802.1Q给每个需要转发的帧都添加一个“标签”，其中包含了vlan的编号，交换机在进行帧转发的时候，同时判断这些“标签”是否匹配，从而确定其互通性。
  - 同时，不支持802.1Q的主机会因为无法“读懂”标签而丢弃该帧。





# 802.1Q 帧格式

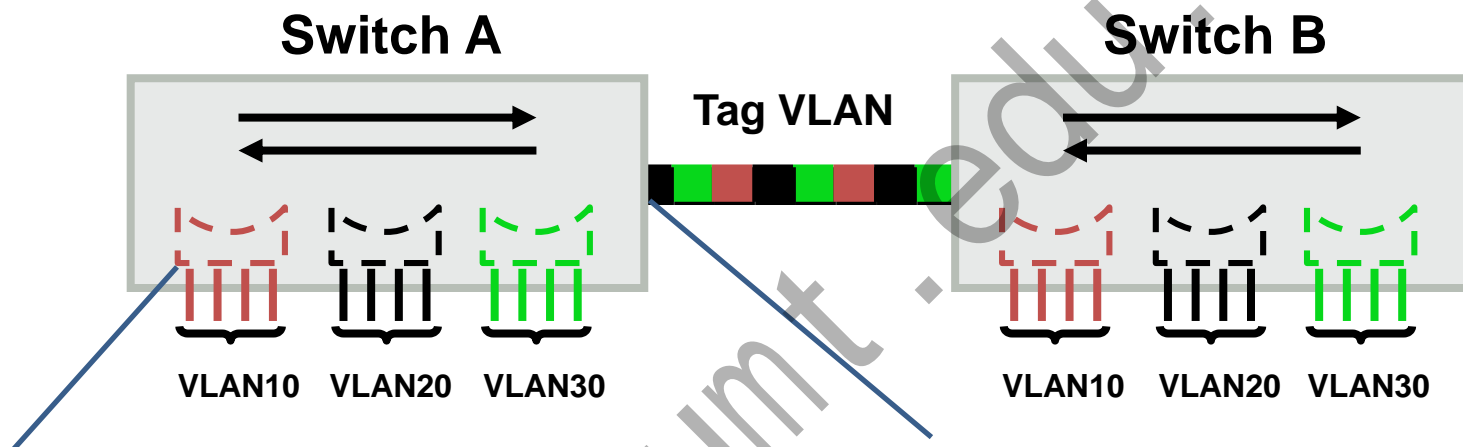
- 虚拟局域网协议允许在以太网的帧格式中插入一个 4 字节的标识符，称为 VLAN 标记(tag)，用来指明发送该帧的工作站属于哪一个虚拟局域网。





# Tag VLAN的处理过程

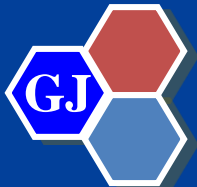
- Tag VLAN特点：传输多个VLAN的信息，实现同一VLAN跨越不同的交换机，要求Trunk至少要100M



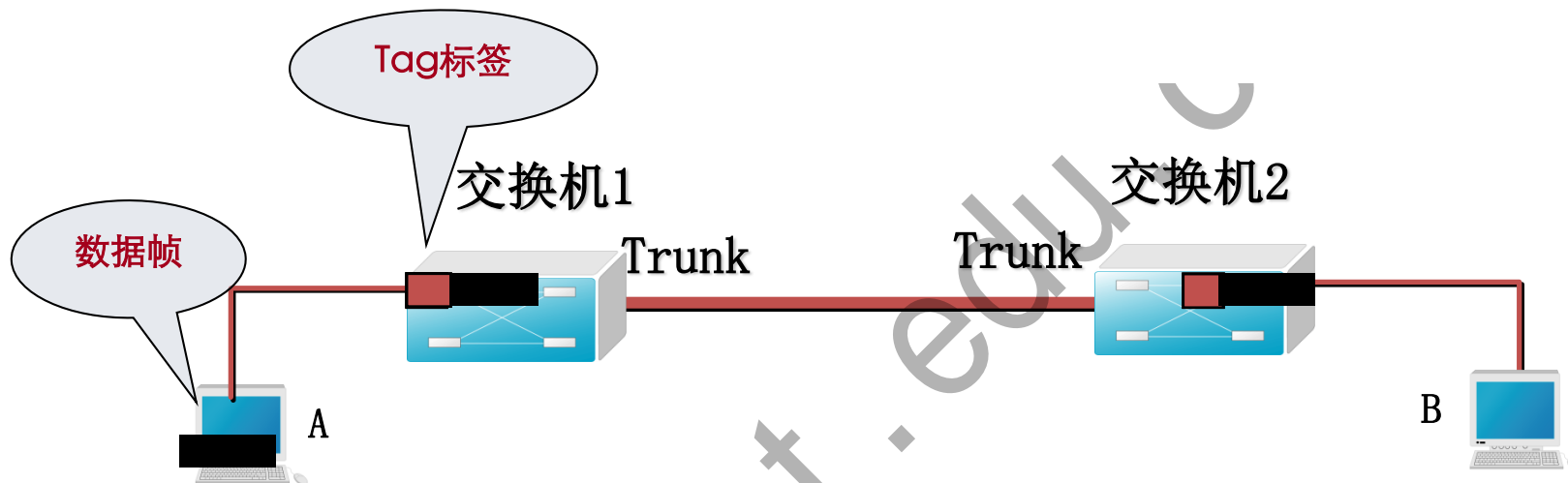
从ACCESS端口进来的数据帧都不包含TAG标记。但进入之后，会被加上标识该端口所属VLAN的TAG标记。如果有数据需要从这种接口发送出去，数据帧中的TAG标记将被删除。这种端口一般用于连接用户主机或路由器。

从Trunk端口发送出去的数据帧都包含有TAG标记（缺省VLAN ID的数据帧除外）；接收到的报文，如果已经有TAG标记，则直接转发；如果没有TAG标记，则加上带有缺省VLAN ID的TAG标记。这种端口一般用于连接交换机或路由器。





# 802.1Q工作原理



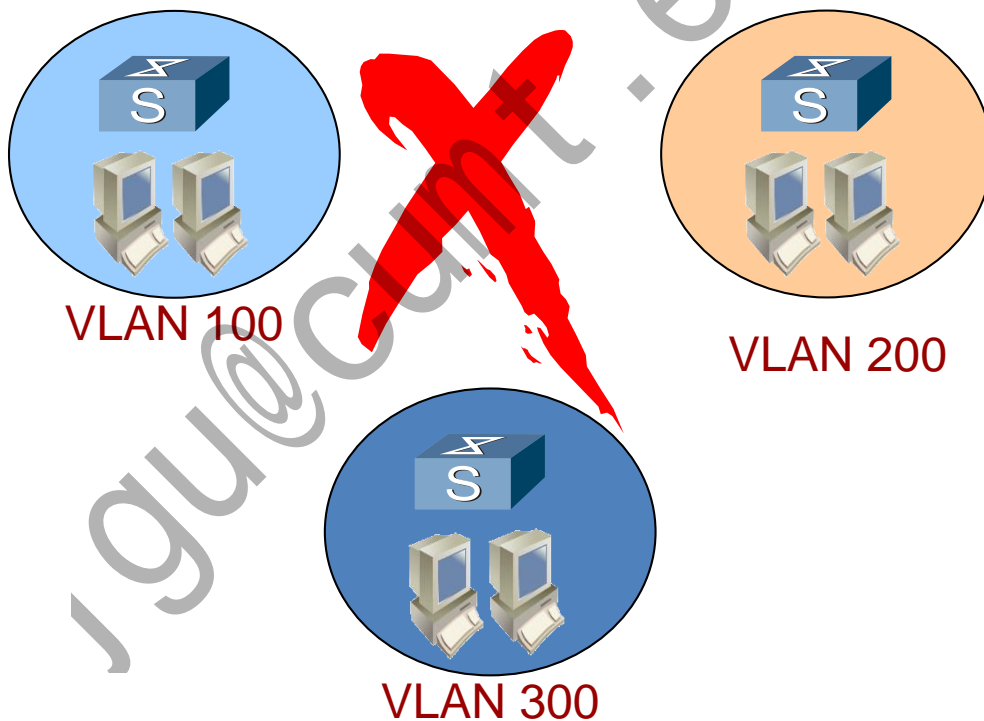
- 802.1Q工作特点：
  - › 802.1Q数据帧传输对于用户是完全透明的。
  - › Trunk上默认会转发交换机上存在的所有VLAN的数据。
  - › 交换机在从Trunk口转发数据前会在数据打上个Tag标签，在到达另一交换机后，再剥去此标签。

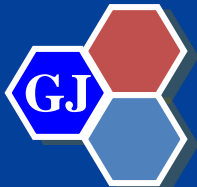




## Q29: 怎么跨VLAN转发数据?

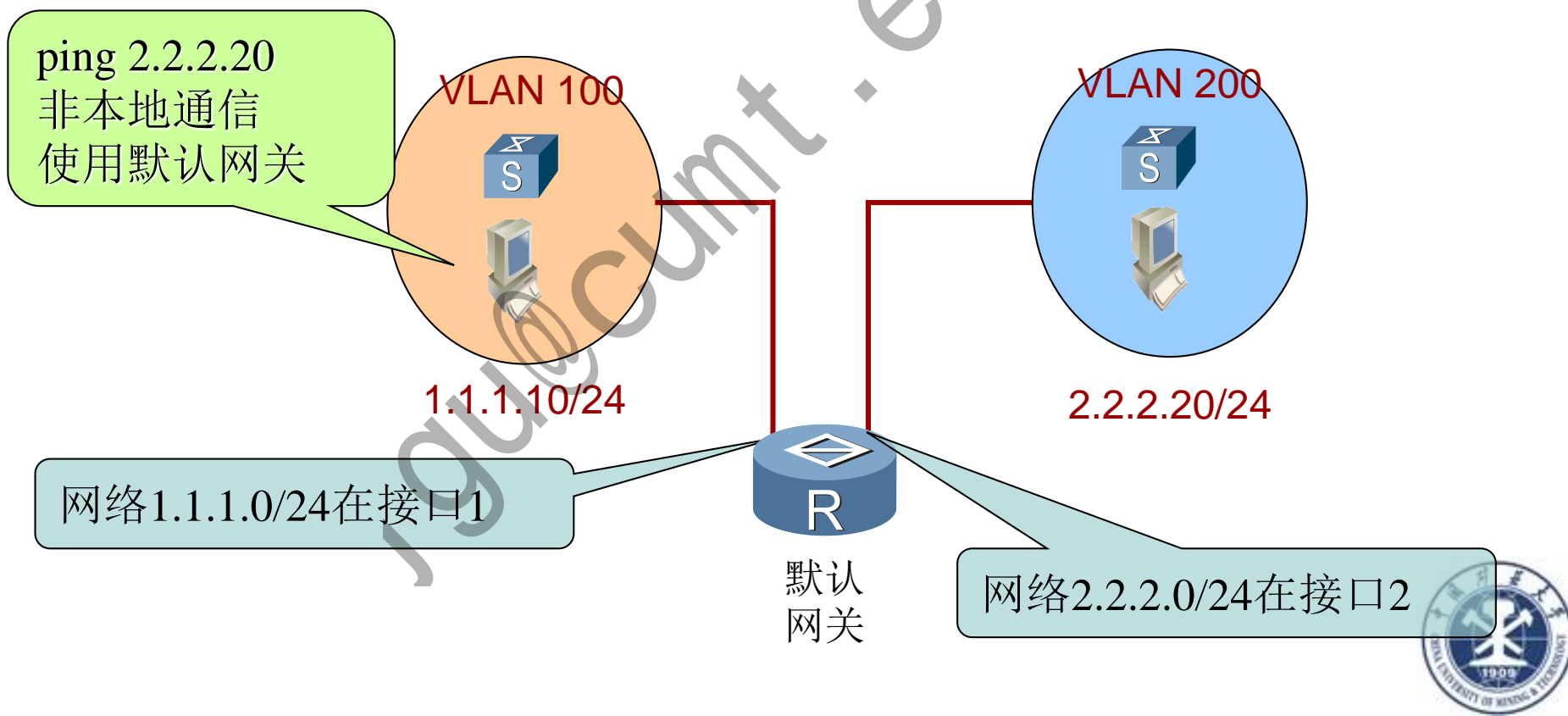
- VLAN在隔离广播的同时也限制了各个VLAN之间的数据流，分属不同VLAN的用户不能通过二层交换机实现通信。



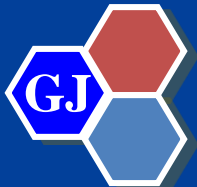


# 不同VLAN之间的互通——三层路由

- 为每个VLAN配置一个IP地址
- 在主机上配置默认网关
- 对于非本地的通信，主机会自动寻找默认网关，并把报文交给默认网关转发而不是直接发给目的主机

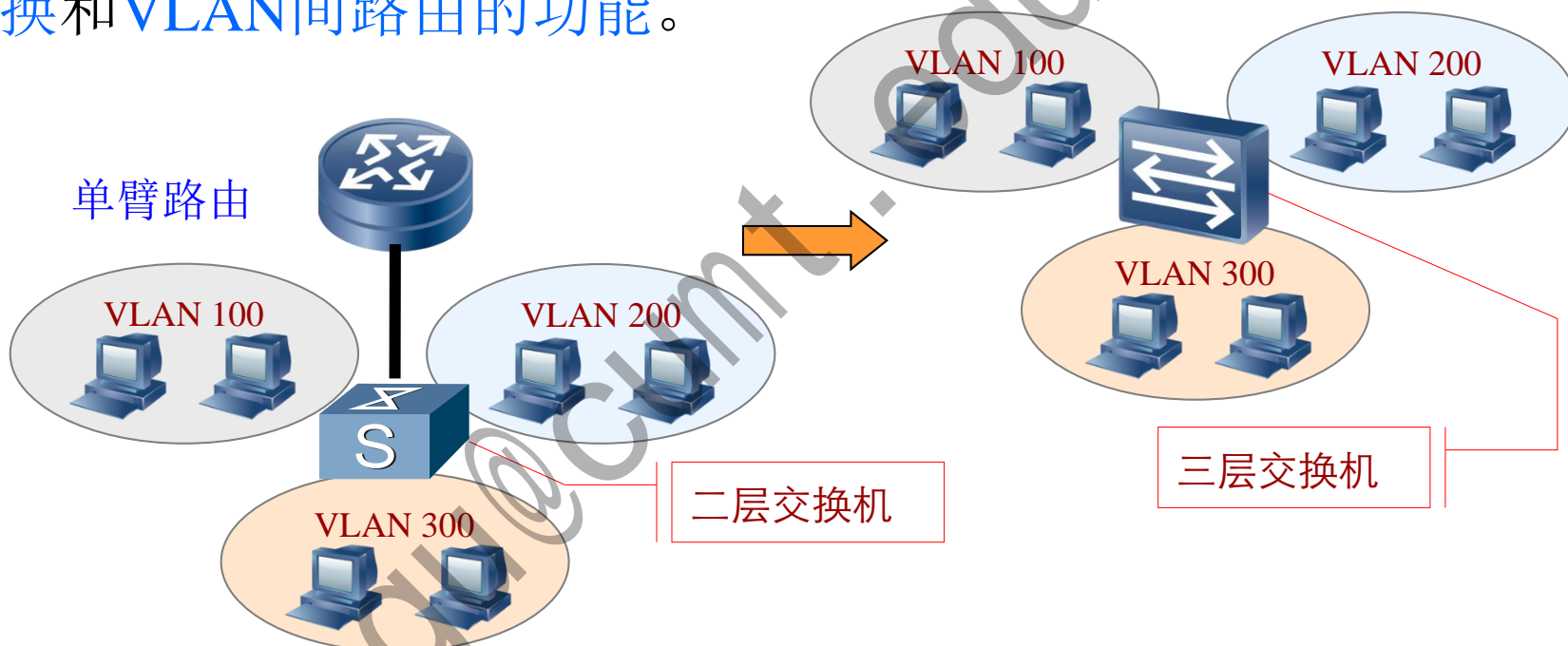






# 不同VLAN之间的互通——三层交换机

- 三层交换机是二层交换机和路由器在功能上的集成，三层交换机在功能上实现了VLAN的划分、VLAN内部的二层交换和VLAN间路由的功能。



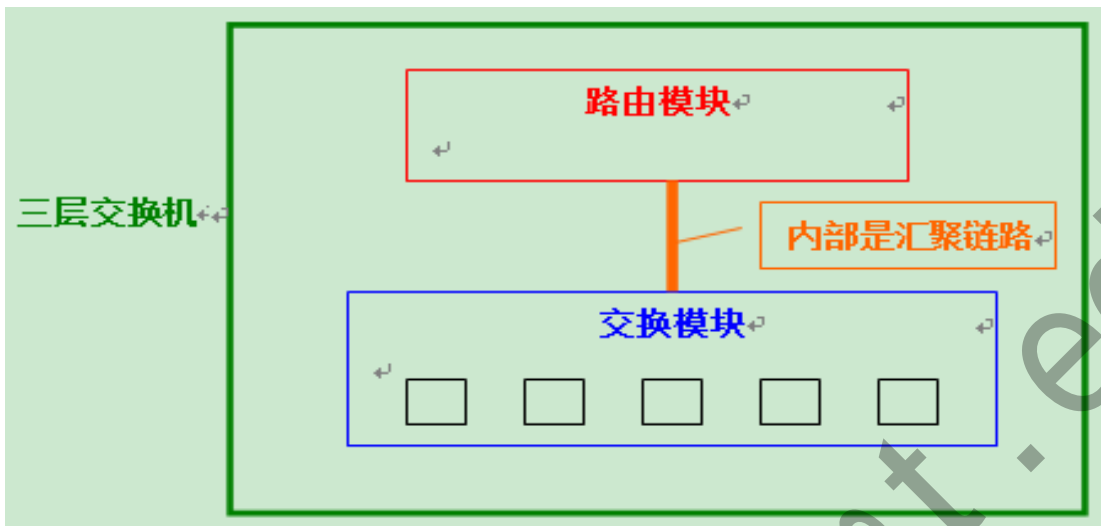
- 二层交换引擎：实现同一网段内的快速二层转发
- 三层路由引擎：实现跨网段的三层路由转发





# 三层交换机

一次路由  
多次交换



内置的路由模块与交换模块相同，使用ASIC硬件处理路由。与传统的路由器相比，可以实现高速路由。并且，路由与交换模块是汇聚链接的，由于是内部连接，可以确保相当大的带宽。

- 二层交换+三层转发技术：

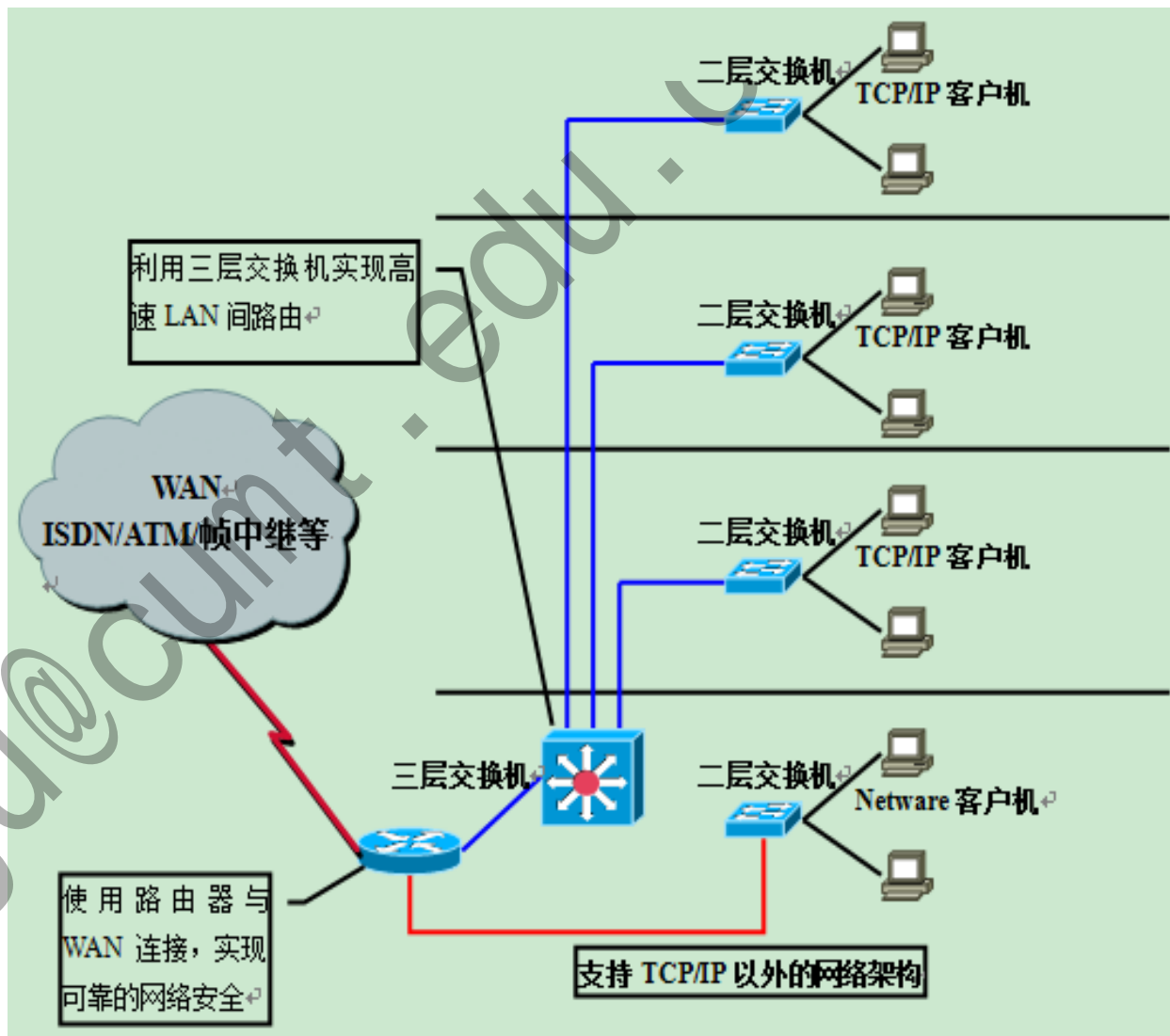
- ▣ 路由模块在以太网上创建出虚拟局域网的三层接口。
- ▣ 这些接口具有三层报文转发的功能，可以将二层不能转发的数据帧进行数据帧头的剥离。
- ▣ 利用三层交换机的路由功能，通过识别数据包的IP地址，查找路由表进行选路转发。
- ▣ 三层交换机会将第一次IP报文转发时源与目的主机的MAC地址及转发端口的对应关系记录进流缓存条目表，以后再进行通信时就直接交由二层交换模块完成。

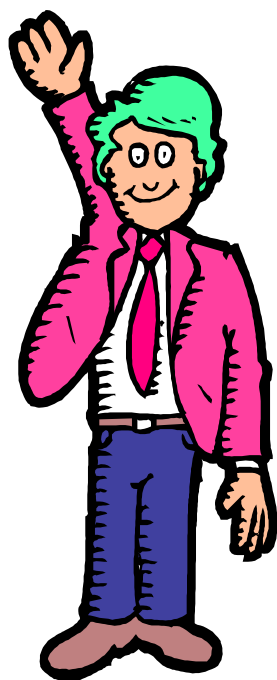




# 路由器和二层/三层交换机配合构建LAN

- ✓ 三层交换机利用直连路由可以实现不同VLAN之间的互相访问。
- ✓ 三层交换机给接口配置IP地址，采用SVI(交换虚拟接口, Switch Virtual Interface)的方式实现VLAN间互连。
- ✓ SVI是三层交换机为各个VLAN配置IP地址的虚拟接口，作为VLAN的网关，用于不同VLAN之间互相访问，实现路由功能。





**THANK  
YOU!**

