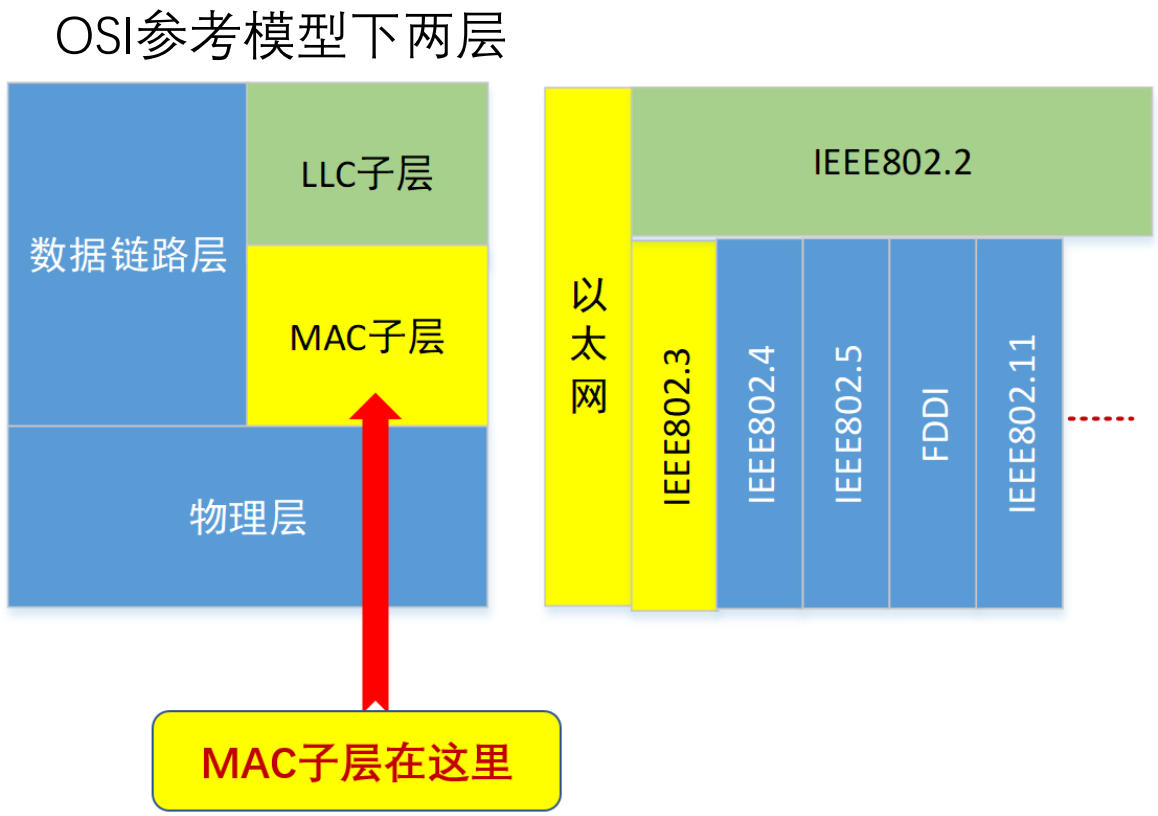
第四章 介质访问控制和局域网

“101计划”
计算机网络

MAC子层在哪里？

- 数据链路层分为两个子层：
  - MAC子层：介质访问
  - LLC子层：承上启下（弱层）
- 以太网和IEEE802.3
  - 覆盖的层数不同（1.5层 vs 2层）
  - 帧的结构有细微不同
  - 以太网：事实上的标准，而802.3系列让接入有了无限的延展性
- 局域网：以太网、无线局域网……



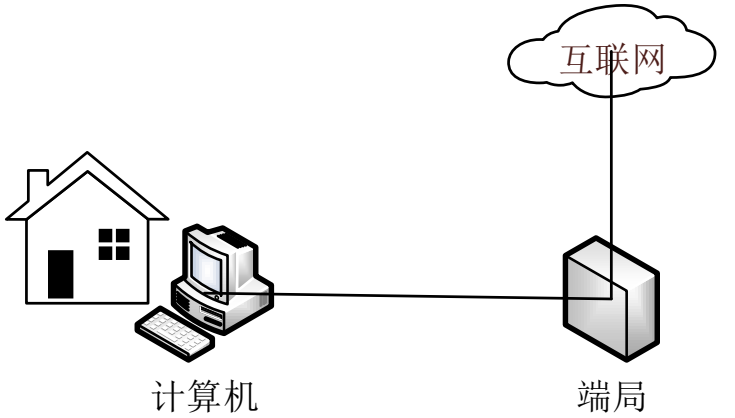
本章内容

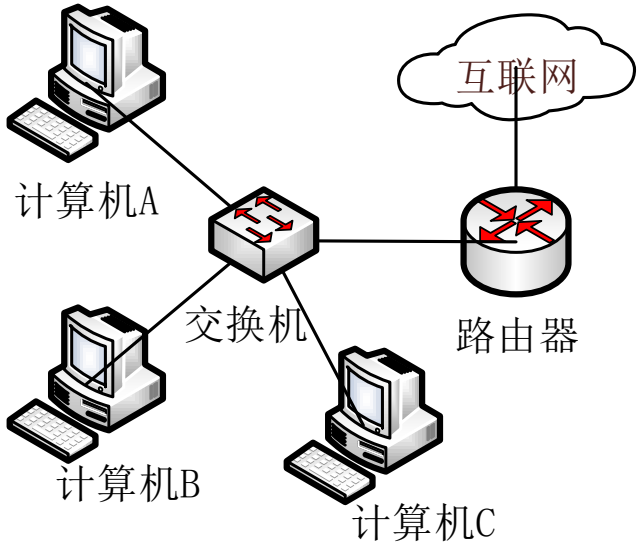
- 4.1 信道分配问题
- 4.2 多路访问协议
- 4.3 IEEE802.3协议和以太网
- 4.4 IEEE802.11协议和无线局域网
- 4.5 网桥技术和交换机

1. 局域网信道
2. 静态分配
3. 动态分配

常见的接入情形

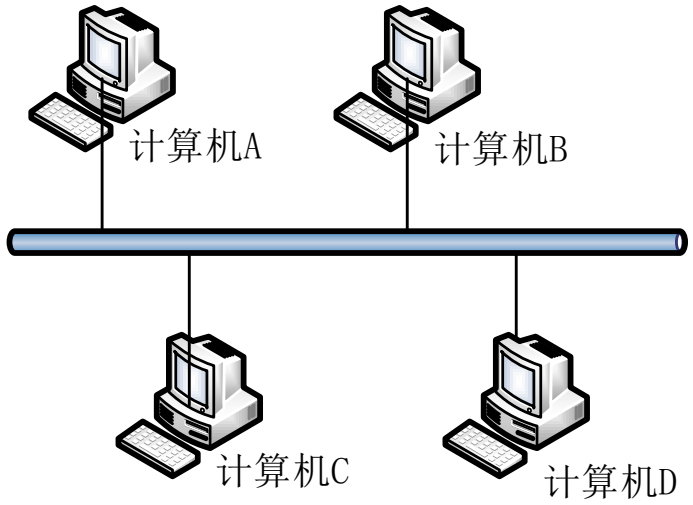
- 信道：信号的通道
  - 比如：双绞线、铜缆、光纤、卫星、空气等
- 点到点信道：信道直接连接两个端点
  - 比如：家中计算机通过modem连接到电信公司端局
- 多点访问信道： 多用户共享一根信道
  - 比如：右图是以太网的典型拓扑，早期星型拓扑是集线器，现在几乎都是交换机，当使用集线器或交换机工作在半双工模式的时候，它的逻辑拓扑是总线式的，信道是共享的

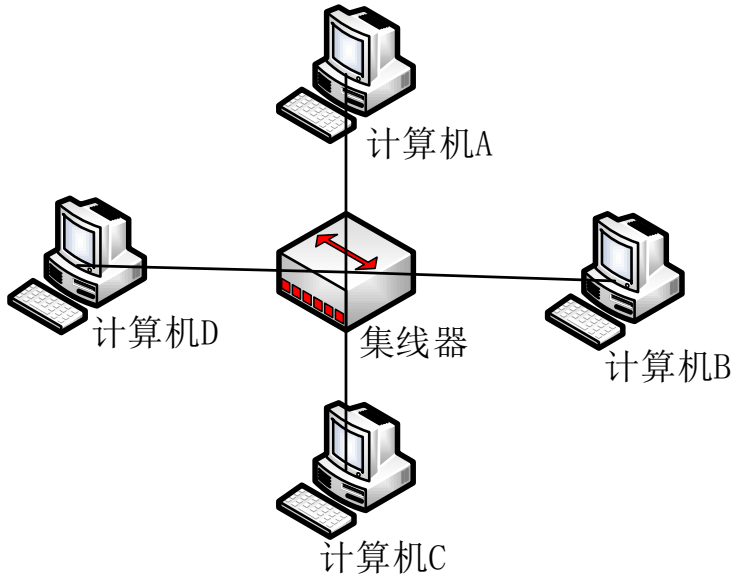


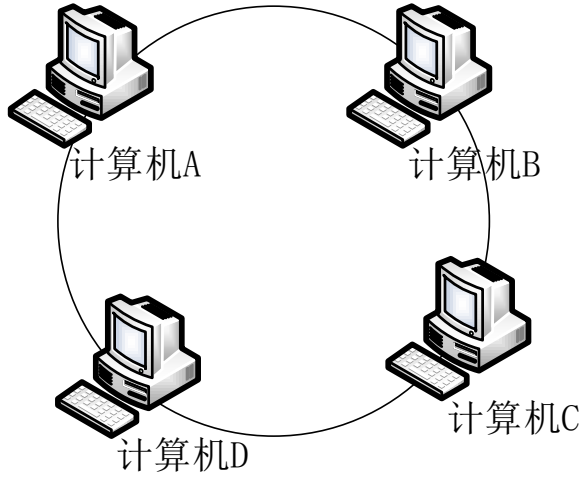


常见的局域网拓扑

- 总线拓扑、星型拓扑、环型拓扑
- 共同点：共享一根信道（别称：广播信道、多路访问信道、随机访问信道）

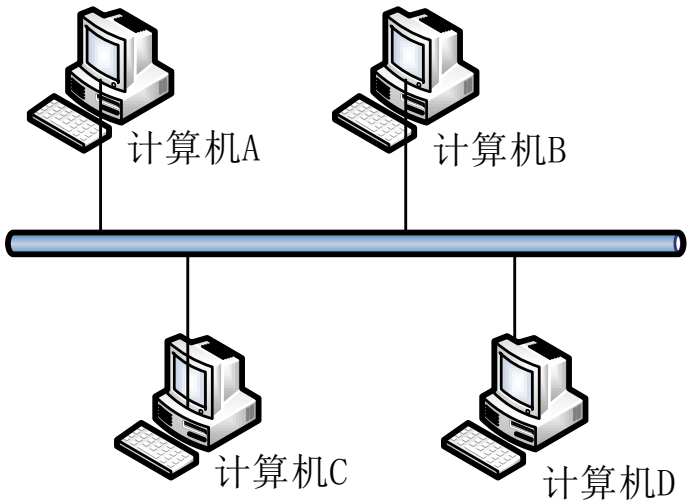






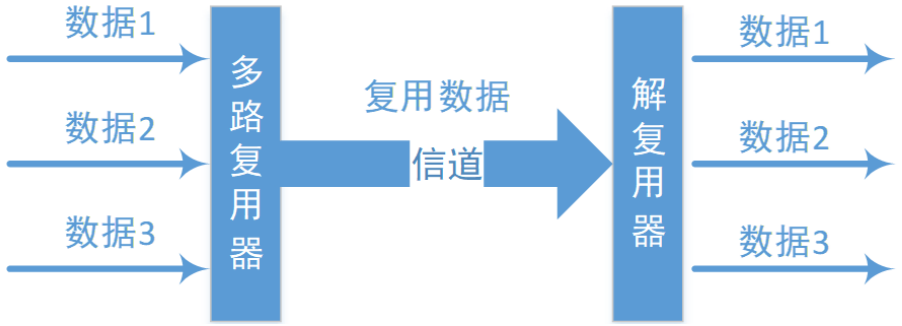
某时由谁来访问共享信道呢？

- 广播信道面临的问题
  - 可能两个（或更多）站点同时请求占用信道
- 解决办法：介质的多路访问控制
  - 在多路访问信道上确定下一个使用者（信道分配）
- 怎么介质访问控制（分配信道）？
  - 静态分配
  - 动态分配



静态分配的性能分析

- 静态分配方法：TDM、FDM
- 静态分配的排队论分析（ M/M/1排队系统模型）
  - M（顾客到达时间间隔分布）
    - 帧到达时间间隔服从指数分布
    - 平均到达率（输入率）：λ 帧/秒
  - M（服务时间分布）
    - 帧长度服从指数分布，平均长度$1/\mu$ 位/帧
    - 信道容量为C位/秒，则信道服务率为μC帧/秒
  - 1（并列服务台个数）



子信道的平均延迟

- 根据排队理论，可证明：单信道平均延迟时间T（顾客在服务系统中的逗留时间）为：

$$T = 1/(\mu C - \lambda)$$

假设：

信道容量：C bps

平均到达帧率：λ帧/秒

平均帧长：1/μ 位/帧

- 信道N等分后每个子信道的平均延迟时间

M —平均输入率： λ/N ；

M —平均服务率： $\mu C/N$

$$T_{FDM} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT$$

静态分配的特点

- 问题
  - 资源分配不合理，不满足用户对资源占用的不同需求
  - 有资源浪费，效率低
  - 延迟时间增大N倍
- 适用情况
  - 适于用户数量少且用户数目固定的情况
  - 适于通信量大且流量稳定的情况
  - 不适用于突发性业务的情况
- 设计动态分配的方法
  - 目的1：更好地满足需求
  - 目的2：提高信道利用率

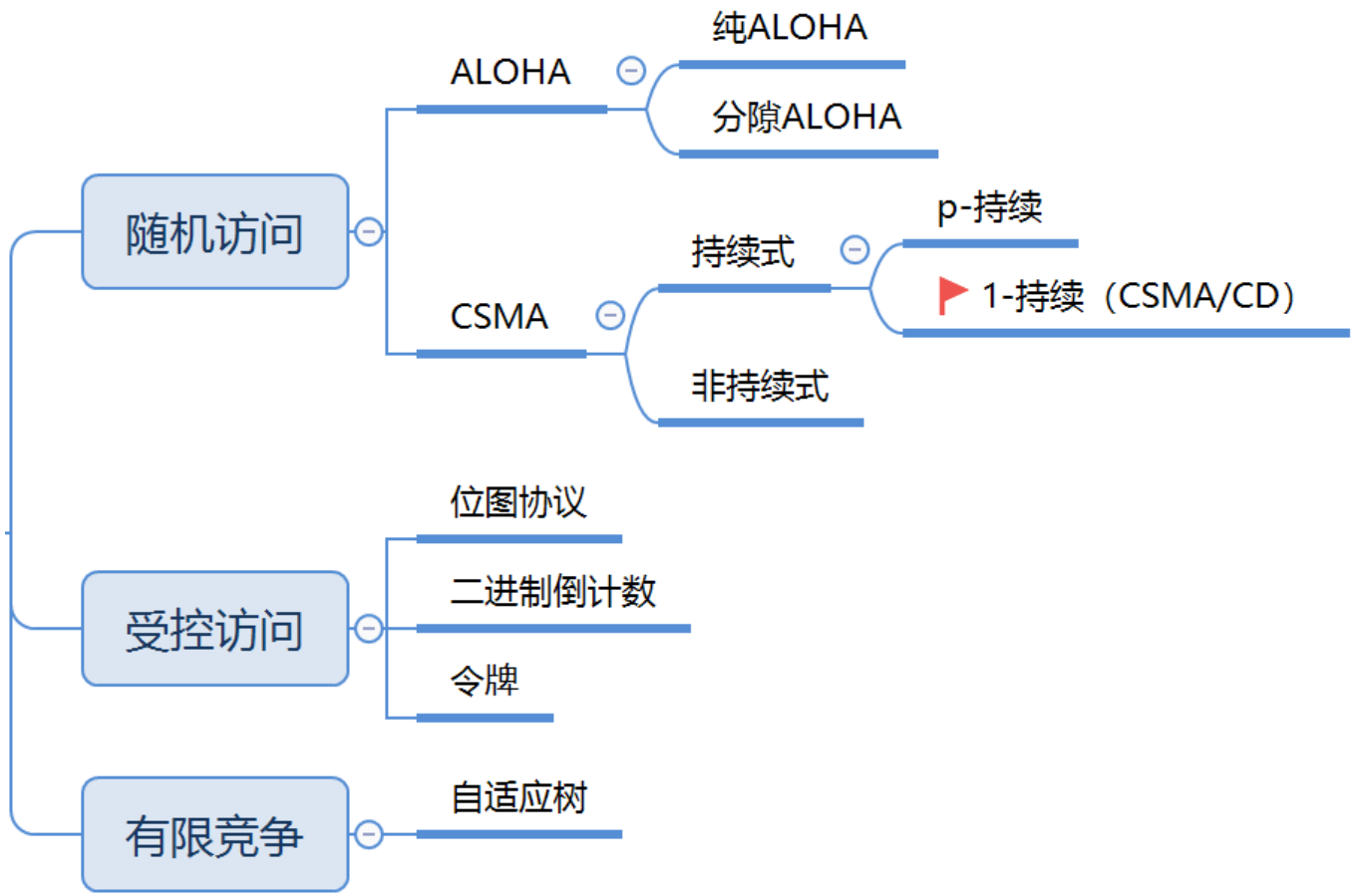
本章内容

- 4.1 信道分配问题
- 4.2 多路访问协议
- 4.3 IEEE802.3协议和以太网
- 4.4 IEEE802.11协议和无线局域网
- 4.5 网桥技术和交换机

1. 多路访问协议
2. 受控访问协议
3. 有限竞争协议

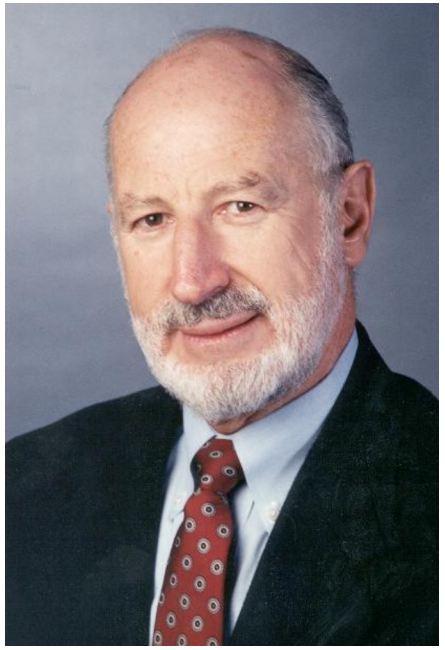
三大类多路访问协议及小分类

- 4.2.1 随机访问协议
  - 特点：冲突不可避免
- 4.2.2 受控访问协议
  - 特点：克服了冲突
- 4.2.3 有限竞争协议
  - 利用上述二者的优势



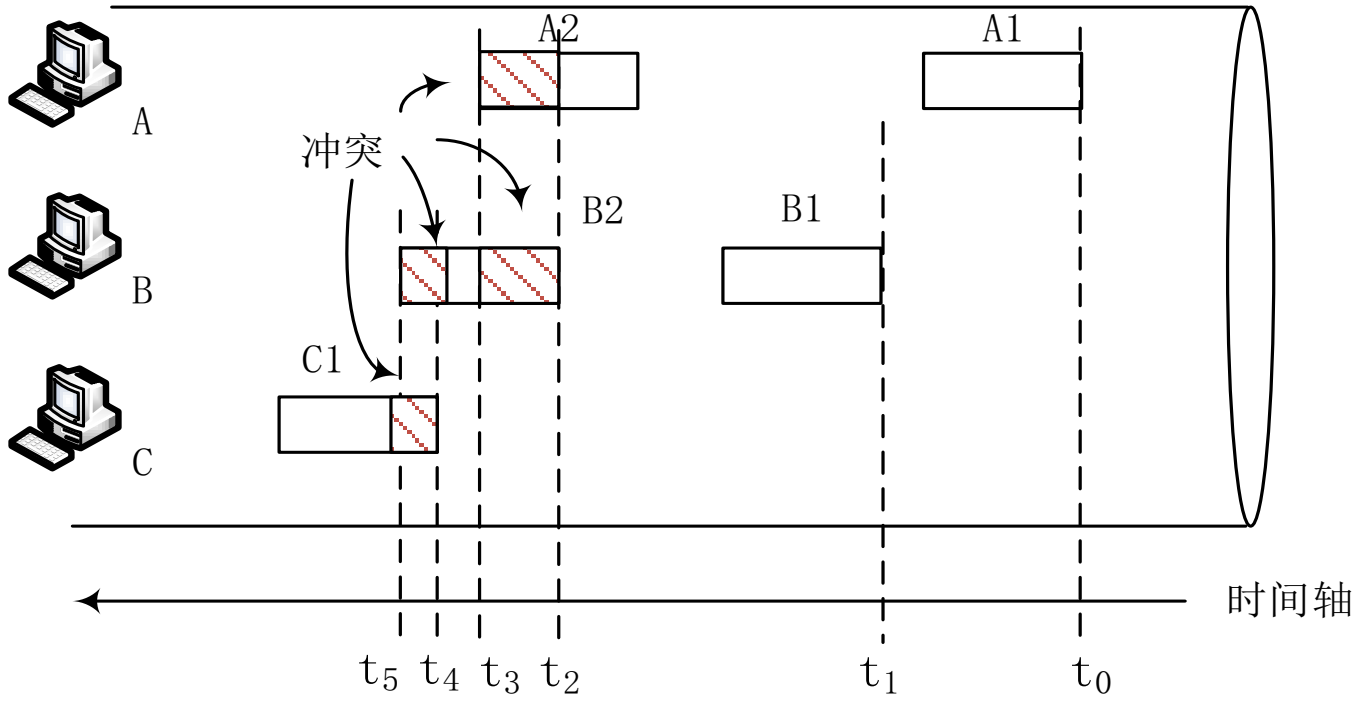
ALOHA协议的由来

- 夏威夷大学Norman Abramson及他的同事设计
- ALOHANet：连接檀香山和其它岛屿
- 两个版本
  - 纯ALOHA协议
  - 分隙ALOHA协议



纯ALOHA协议工作原理：任性！

- 原理：想发就发！
- 特点
  - 冲突：两个或以上的帧
  - 随时可能冲突
  - 冲突的帧完全破坏
  - 破坏了的帧要重传



纯ALOHA协议的数学描述

- 定义
  - 帧时：发送一个标准长的帧所需的时间
- 服从泊松分布
  - 一个帧时内用户产生新帧：均值N个
  - 一个帧时内信道中产生的帧（包括重传）：均值G个
- 分析：
  - 0< N < 1，轻载N接近0，重载N接近1
  - G >= N，轻载G=N（无冲突），重载G>N（冲突/重传）
- 概率

  $Pr[k] = G^k e^{-G} / k!$ (一个帧时内信道中产生k个帧，泊松分布)

  $Pr[k=0] = e^{-G}$ （一个帧时内信道中产生0个帧）

性能分析

- 吞吐量(Throughout) S
  - 在发送时间T内发送成功的平均帧数。

    显然，0<S<1
  - S = 1时分组一个接一个地发送出去，帧之间没有空隙。一般用S接近于1的程度来衡量信道的利用率

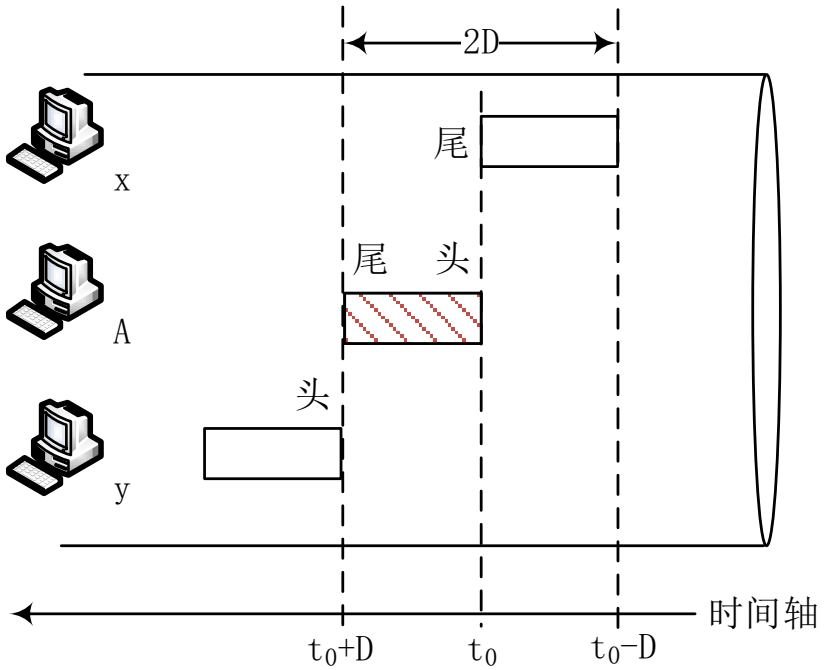
性能分析（续）

- 运载负载(Carried load) G，又称网络负载
  - 时间T内所有通信站总共发送的帧平均值(包括原发和重发的分组)。
  - 显然，G≧S，只有在不发生冲突时G才等于S。当重负载(G>>1) 时，冲突频繁
- P_0：P_0是一帧发送成功(即未发生冲突)的概率。就是发送成功的分组在已发送分组的总数中所占的比例

$$S = G \times P_0$$

如何计算传输成功的概率P_0？

- 单向传播延迟Delay：D
- 冲突危险期：2D（为什么？）
  - 生成帧均值：2G
  - 不遭受冲突的概率：$P_0=e^{-2G}$



冲突危险期：2D

传输成功的概率P_0的计算

- P_0的含义是在连续两个T的时间内都没有其它帧生成的概率，即连续两个T的时间内都生成0帧的概率(P[0])之乘积
- 生成0帧的概率(即不生成帧的概率)，即是将k=0代入上式，得：

  $P[0] = e^{-G}$

  - 注意：P_0与P[0]是两个完全不同的概念。
- 所以：$P_0 = P[0]P[0] = (e^{-G})^2 = e^{-2G}$

纯ALOHA协议的性能

- 将$P_0 = e^{-2G}$代入$S = GP_0$得：

  $S = Ge^{-2G}$

- 求吞吐率S的极大值：

  $S' = e^{-2G} - 2Ge^{-2G} = 0$

- 当G = 0.5 时，S ≈0.184

- 即纯ALOHA信道的利用率最高为18.4%

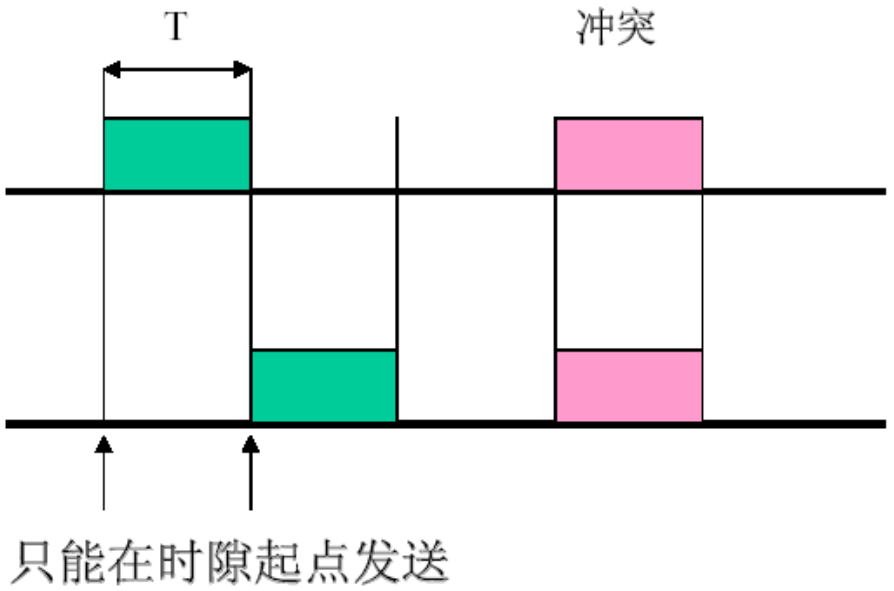
S：吞吐量

G：网络负载

P_0：成功传输概率

分隙ALOHA (Slotted ALOHA)工作原理

- 分隙ALOHA是把时间分成时隙（时槽）
- 时隙的长度对应一帧的传输时间。
- 帧的发送必须在时隙的起点。
- 冲突只发生在时隙的起点



冲突危险期：D

分隙ALOHA的性能分析

- $P[0] = e^{-G}$
  - $P_0 = P[0] = e^{-G}$（为什么？P14）
  - $S = Ge^{-G}$
- 在$G = 1$时得到最大吞吐率：
- $S_{max} = 1/e \cong 0.368$
- 该值是纯ALOHA S值的两倍

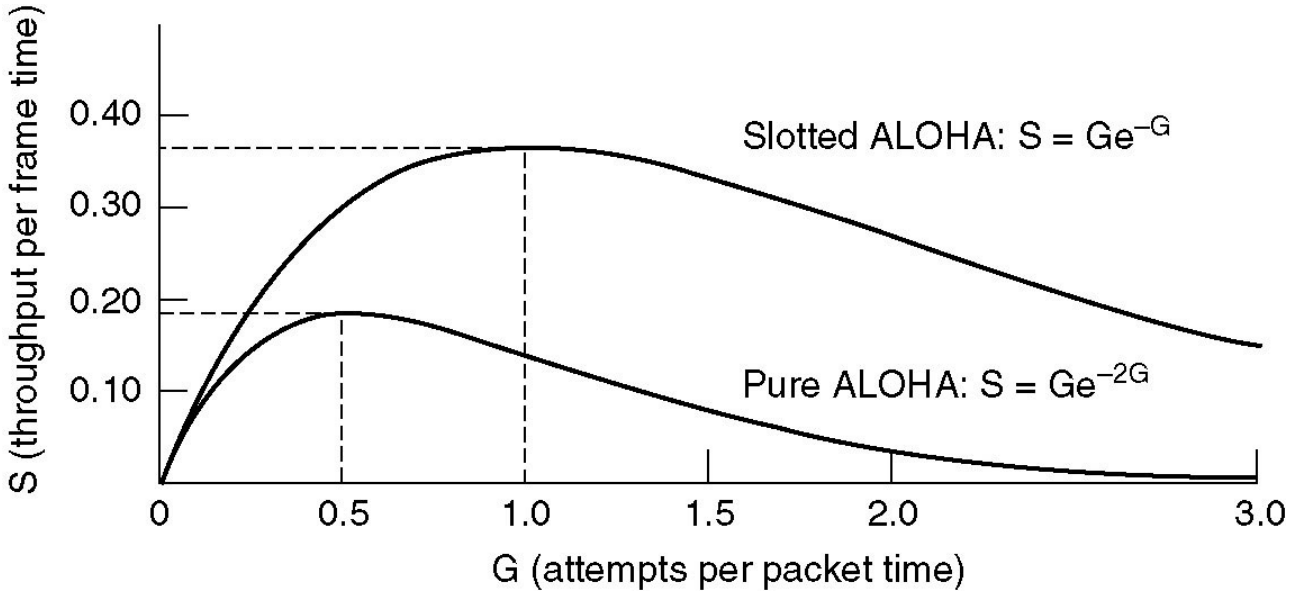
S：吞吐量

G：网络负载

P_0：成功传输概率

小结两种ALOHA协议

- ALOHA
  - 冲突危险期：2D
  - 生成帧均值：2G
  - 吞吐量：$S = G\,P_0 = G\,e^{-2G}$
- 分隙ALOHA
  - 以帧时t为离散间隔
  - 冲突危险期减半：D
  - 吞吐量：$S = G\,P_0 = G\,e^{-G}$

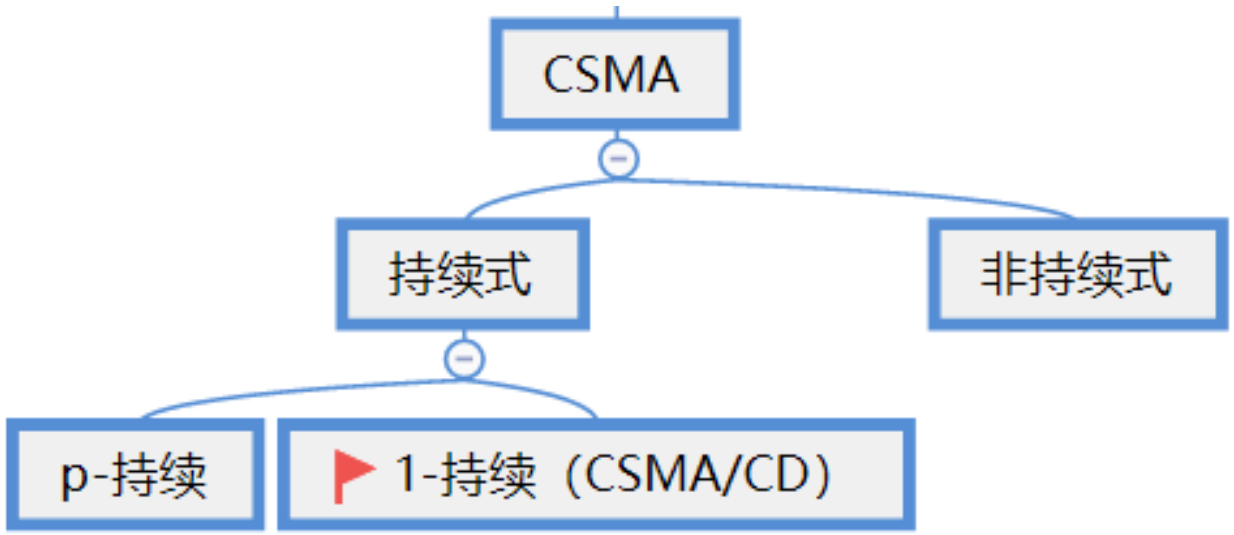


为什么还要学？

怎么改进？

载波侦听多路访问协议

- CSMA：Carrier Sense Multiple Access
- 特点：“先听后发”
  - 改进ALOHA的侦听/发送策略分类



不再任性！
变得礼貌了！

非持续式CSMA

- 特点
  - ①经侦听，如果介质空闲，开始发送
  - ②如果介质忙，则等待一个随机分布的时间，然后重复步骤①
- 好处
  - 等待一个随机时间可以减少再次碰撞冲突的可能性
- 缺点
  - 等待时间内介质上如果没有数据传送，这段时间是浪费的

持续式(指1-持续式)CSMA

- 特点
  - ①经侦听，如介质空闲，则发送
  - ②如介质忙，持续侦听，一旦空闲立即发送
  - ③如果发生冲突，等待一个随机分布的时间再重复步骤①
- 好处：持续式的延迟时间要少于非持续式
- 主要问题：如果两个以上的站等待发送，一旦介质空闲就一定会发生冲突

p-持续式CSMA

➢特点

- ①经侦听，如介质空闲，那么以p的概率发送，以(1–p)的概率延迟一个时间单元发送
- ②如介质忙，持续侦听，一旦空闲重复①
- ③如果发送已推迟一个时间单元，再重复步骤①

➢注意

- 1-持续式是p-持续式的特例

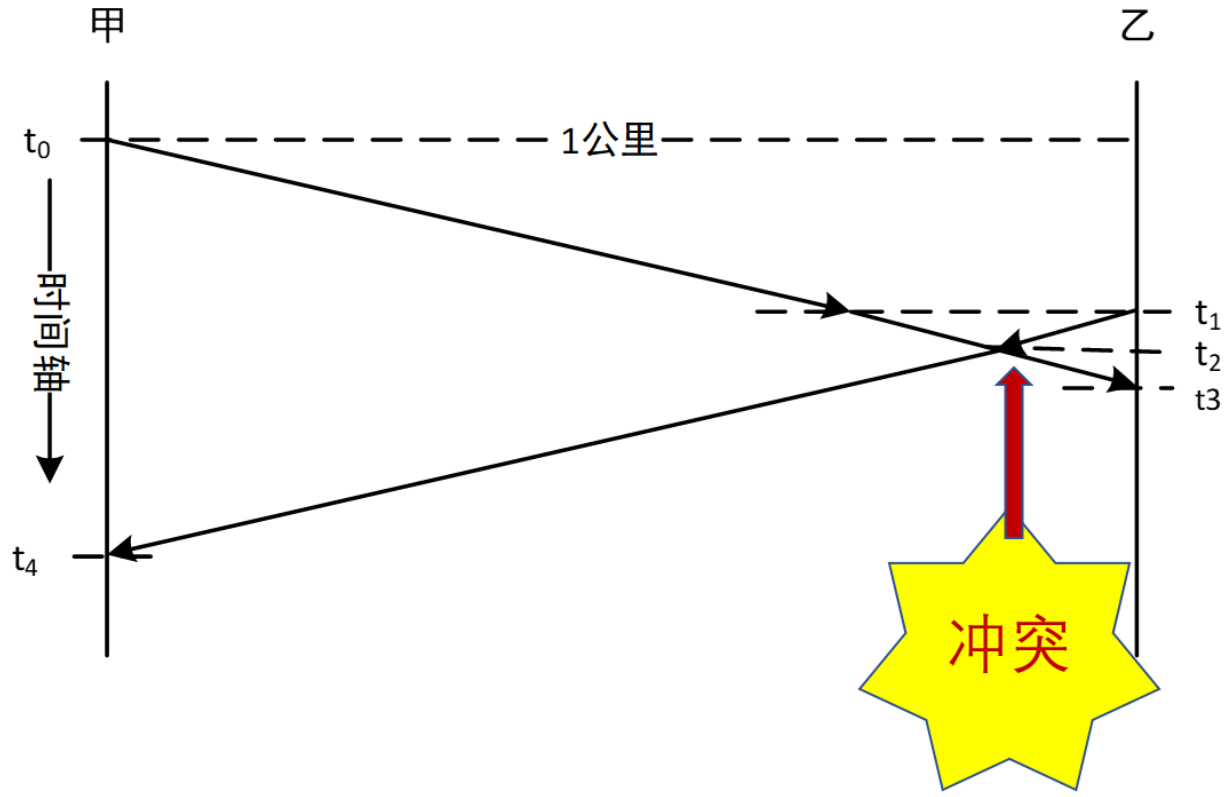
问题：先听再发，避免了冲突吗？

- CSMA：如侦听到介质上无数据发送才发送，发送后还会发生冲突吗？
- 肯定会！
- 两种情形
  - （1）同时传送；（2）传播延迟时间

不再任性了的CSMA还会发生冲突吗？

传播延迟对载波侦听的影响

- 信号传输速度：0.65C
- t_0时刻：甲侦听后发送，到达乙约需5微妙
- t_1时刻：乙侦听后发送
- t_2时刻：冲突
- t_3时刻：乙检测到冲突
- t_4时刻：甲检测到冲突



冲突窗口

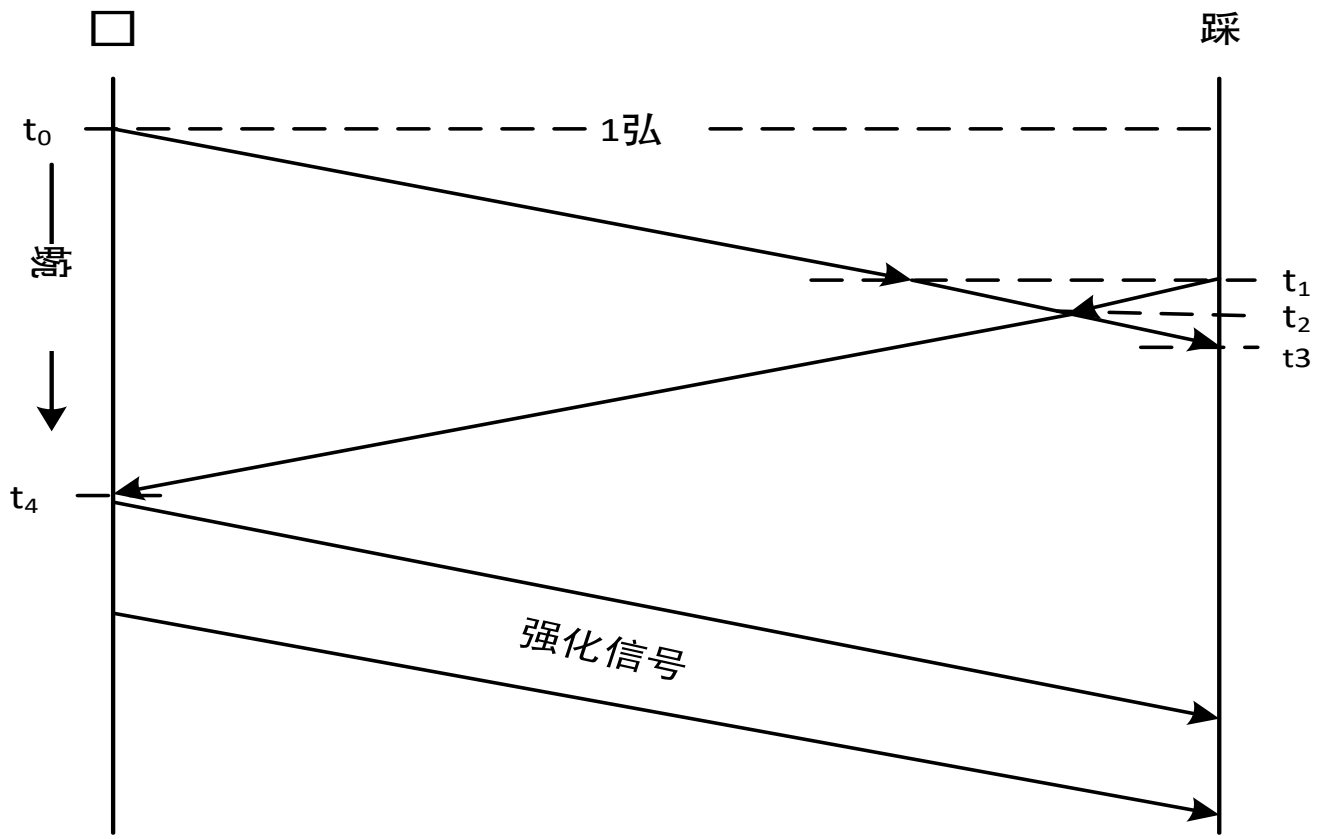
- 即发送站发出帧后能检测到冲突（碰撞）的最长时间。
- 是一个时间区间
  - 可能侦听到发出的帧遭到冲突（碰撞）
- 数值上：等于最远两站传播时间的两倍，即2D（D是单边延迟）
  - 2D相当于1个来回传播延迟RTT：Round Trip Time）

CSMA/CD （1-持续）

- CSMA with Collision Detection
- 原理：“先听后发、边发边听”
- 过程
  - ①经侦听，如介质空闲，则发送。
  - ②如介质忙，持续侦听，一旦空闲立即发送。
  - ③如果发生冲突，等待一个随机分布的时间再重复步骤①

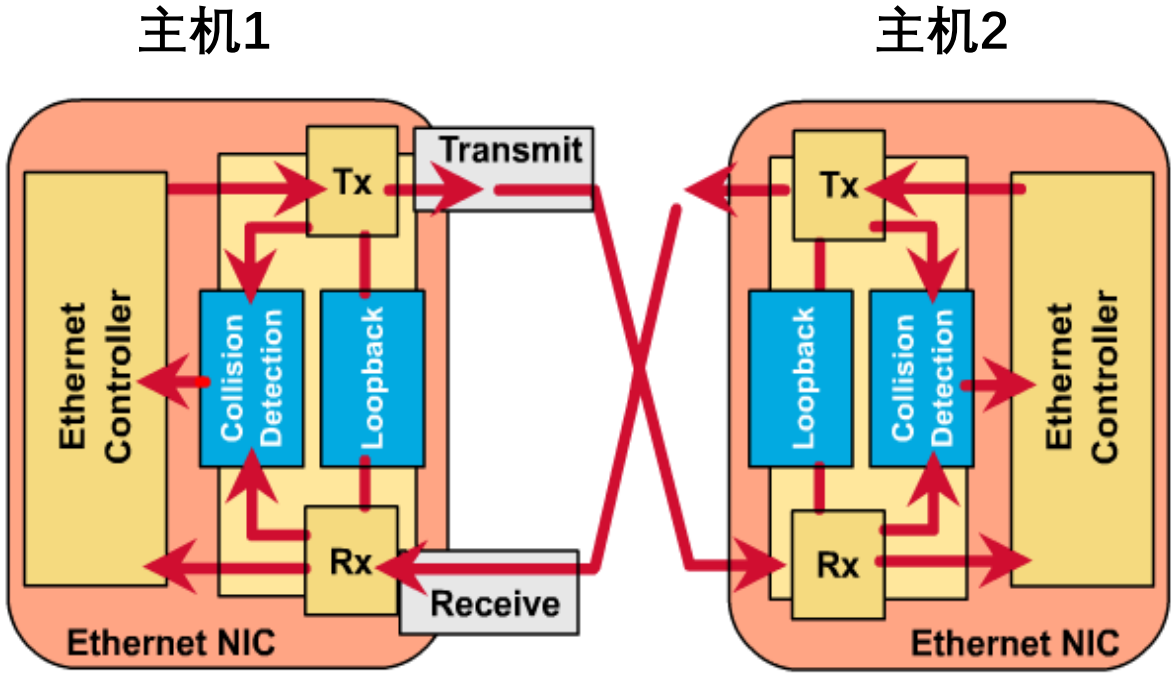
CSMA/CD（续）

- 边发边听：是否发生了冲突？
- 一旦冲突，发送Jam（强化）信号
  - t_4时刻：甲检测到冲突，发送Jam
  - t_3时刻：乙检测到冲突，是否发送？



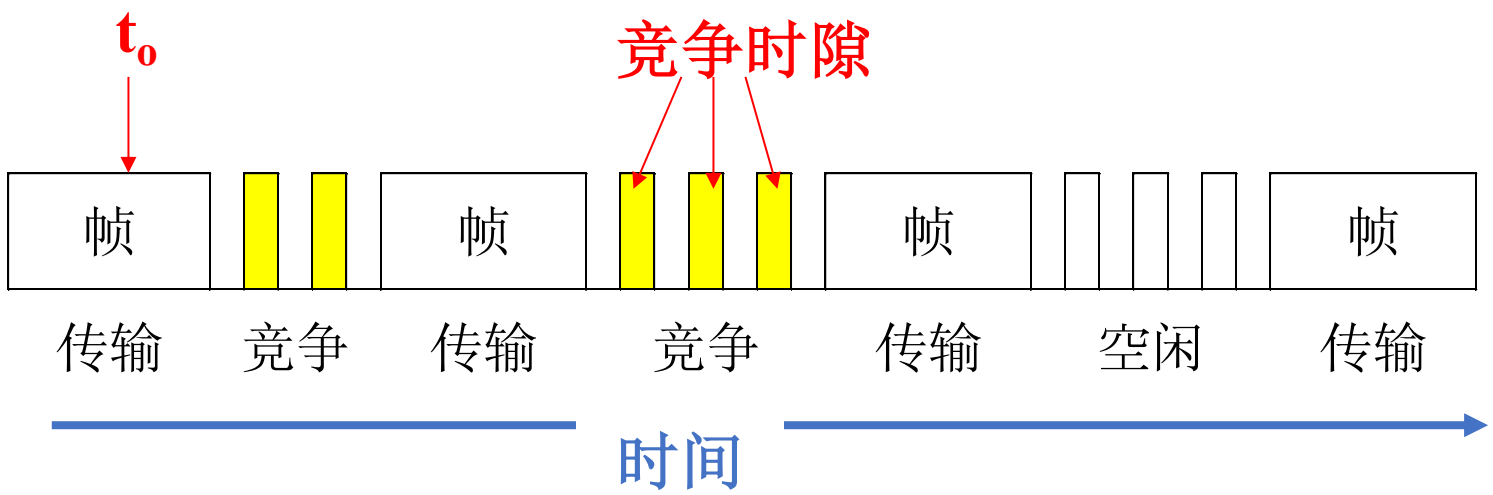
怎么能侦听到冲突？

- Tx：发出信号，分叉
- Rx：收到两路信号
  - 比较，不同则有冲突
- 所以，自然要求
  - 发送帧的时间不能太短
  - 至少一个冲突窗口的时间：2D



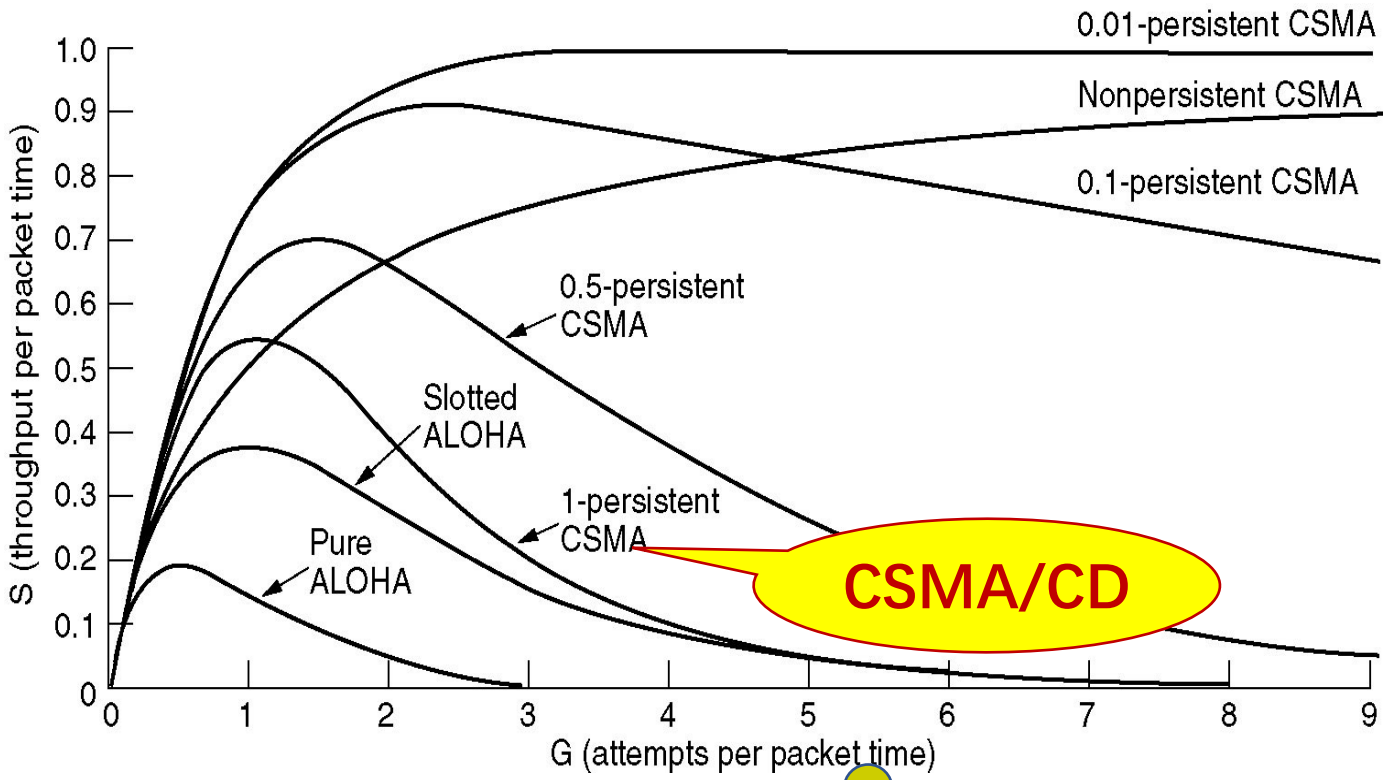
CSMA/CD概念模型

- 传输周期：一个站点使用信道，其他站点禁止使用
- 竞争周期：所有站点都有权尝试使用信道，争用时间槽
- 空闲周期：所有站点都不使用信道



各种CSMA的性能比较

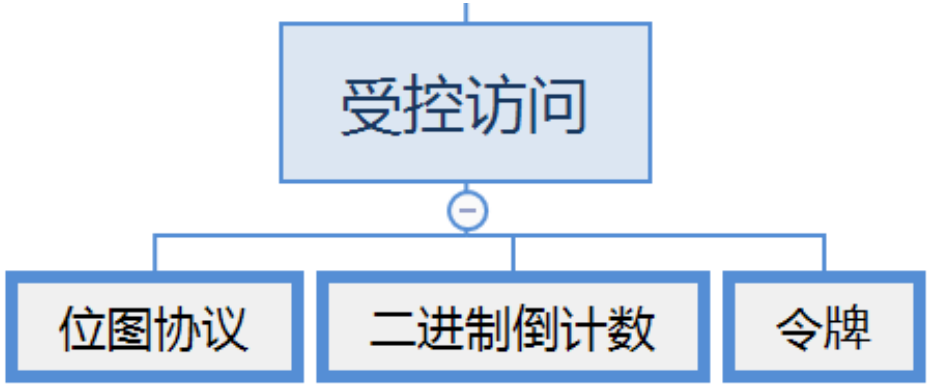
- CSMA/CD：1-持续CSMA
- 以太网采用了CSMA/CD
  - 吞吐量：比ALOHA高，比P-持续式CSMA低
  - 冲突：比ALOHA少，比P-持续式高
  - P-持续式付出了高延迟的代价



先听后发，边发边听；
一旦冲突，立刻停发；
等待时机，然后再听。

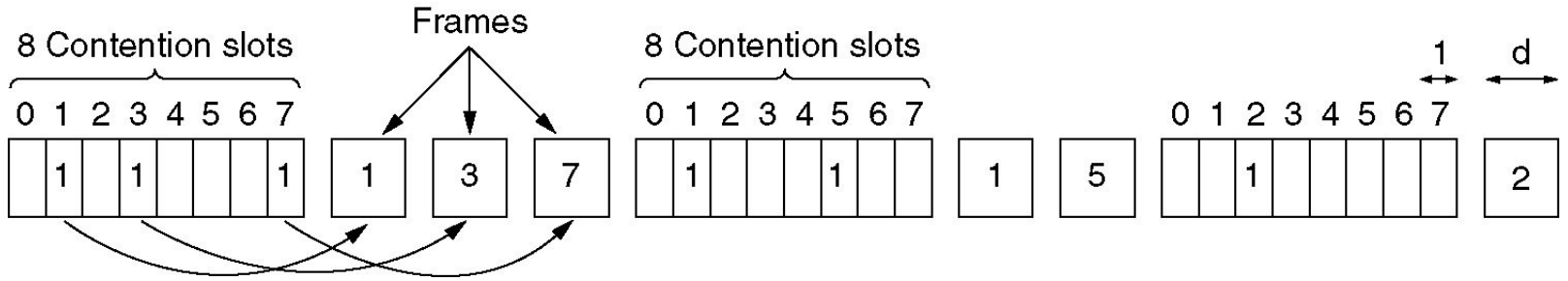
受控访问协议

- 4.2.2 受控访问（无冲突）协议
  - 4.2.2.1 位图协议（预留协议）
  - 4.2.2.2 令牌
  - 4.2.2.3 二进制倒计数协议



位图协议（预留协议）图示

- 竞争期：在自己的时槽内发送竞争比特
  - 举手示意
  - 资源预留
- 传输期：按序发送
  - 明确的使用权，避免了冲突

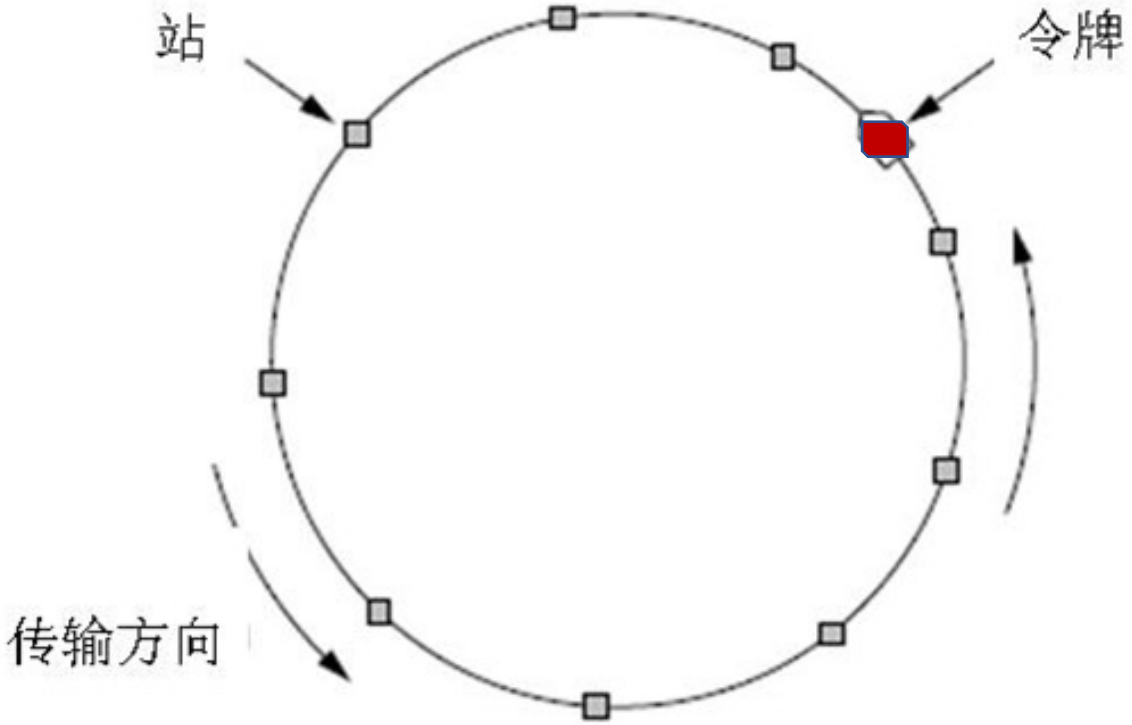


位图协议的信道利用率分析

- 假设
  - 有N个用户，需N个时隙，每帧d比特
- 信道利用率
  - 在低负荷条件下：d/(d+N)　　（N越大，站点越多，利用率越低）
  - 在高负荷条件下：d/(d+1)，接近100%
- 缺点
  - 位图协议无法考虑优先级

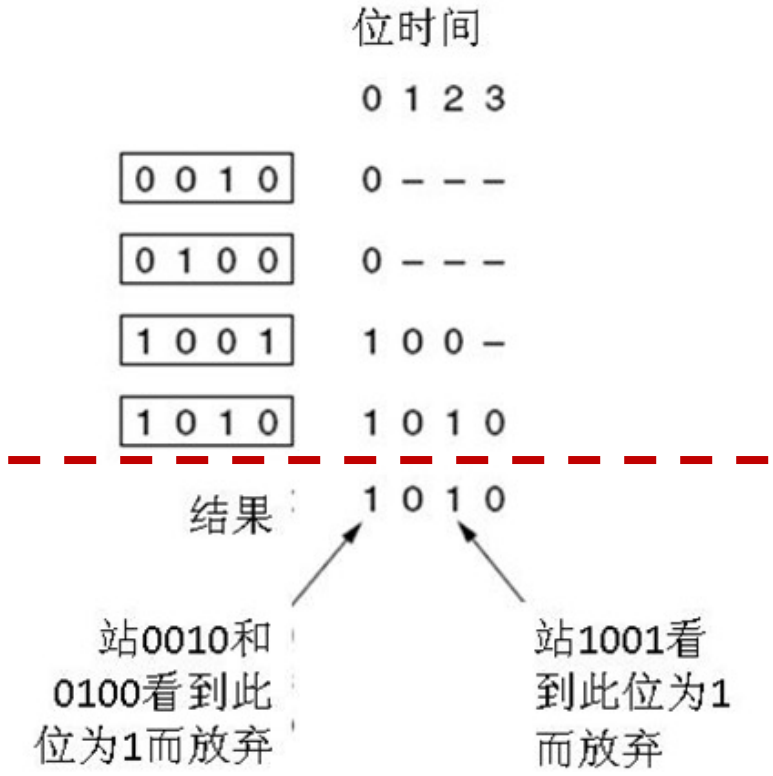
令牌传递

- 令牌：发送权限
- 令牌的运行：发送工作站去抓取，获得发送权
  - 除了环，令牌也可以运行在其它拓扑上，如令牌总线
- 发送的帧需要目的站或发送站将其从共享信道上去除；防止无限循环
- 缺点：令牌的维护代价



二进制倒计数协议

- 站点：编序号，序号长度相同
- 竞争期：有数据发送的站点从高序号到低序号排队，高者得到发送权
- 特点：高序号站点优先
  - 好事还是坏事？



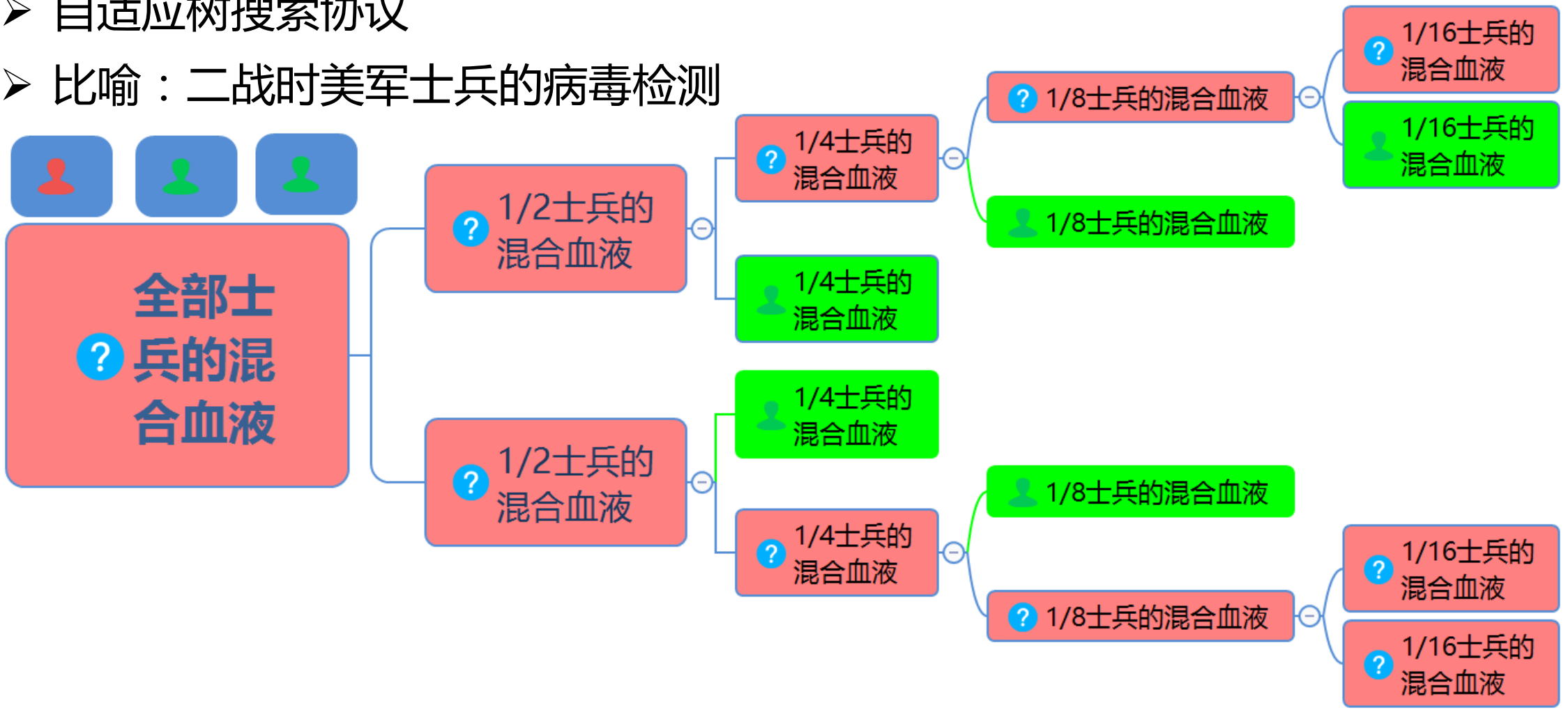
防止低序号站点一直抢不到发送权，可以怎样办？

二进制倒计数协议的信道效率分析

- N个站的二进制编码所需位数是$\log_2 N$位
- 信道的利用率为：$d/(d+\log_2 N)$
- 如果规定每个帧的帧头为发送地址，即竞争的同时也在发送。则效率为100%

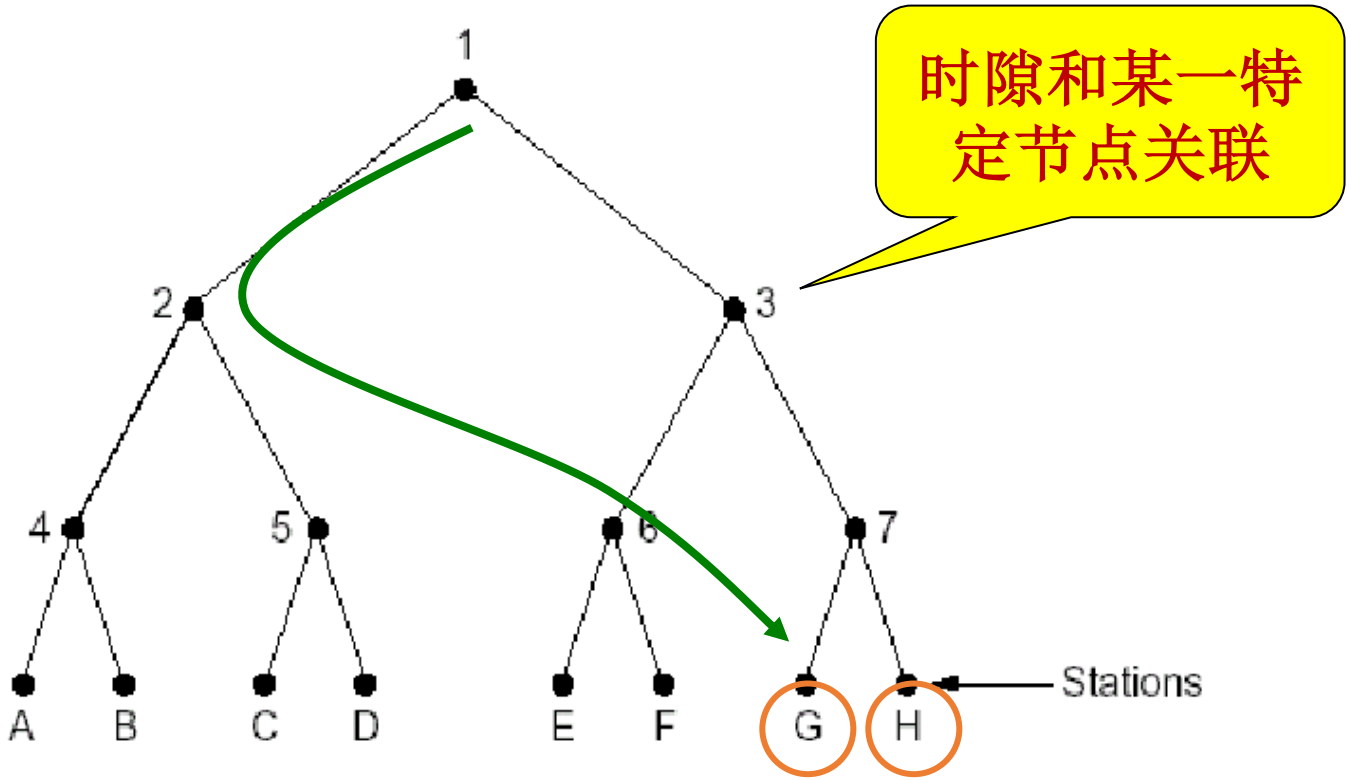
有限竞争协议

- 自适应树搜索协议
- 比喻：二战时美军士兵的病毒检测



自适应树搜索协议（Adaptive Tree Walk Protocol）

- 在一次成功传输后的第一个竞争时隙，所有站点同时竞争。
- 如果只有一个站点申请，则获得信道。
- 否则在下一竞争时隙，有一半站点参与竞争（递归），下一时隙由另一半站点参与竞争
- 即所有站点构成一棵完全二叉树。

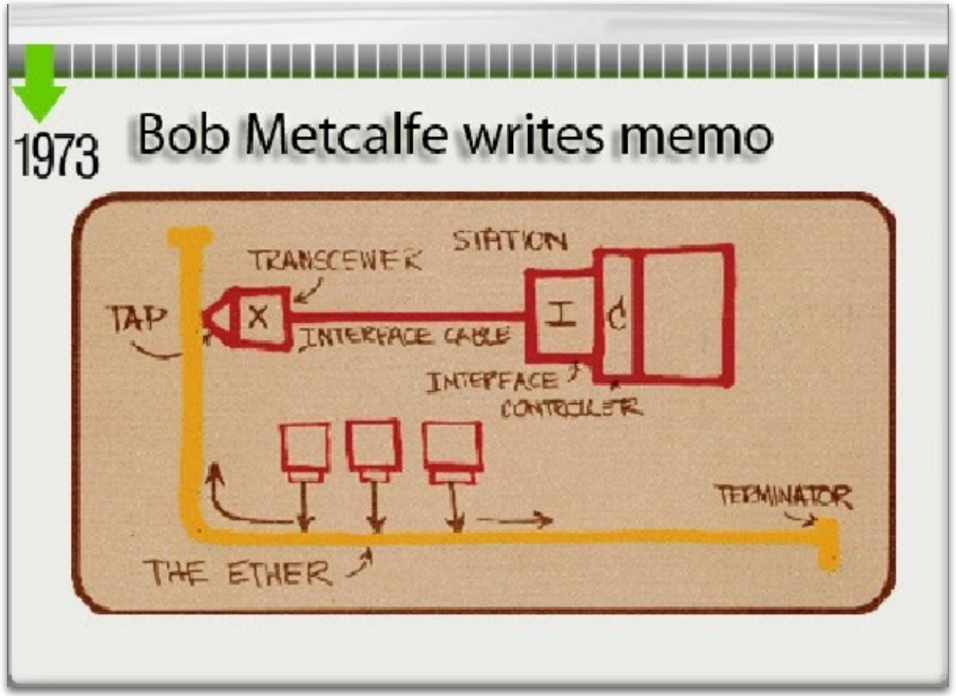


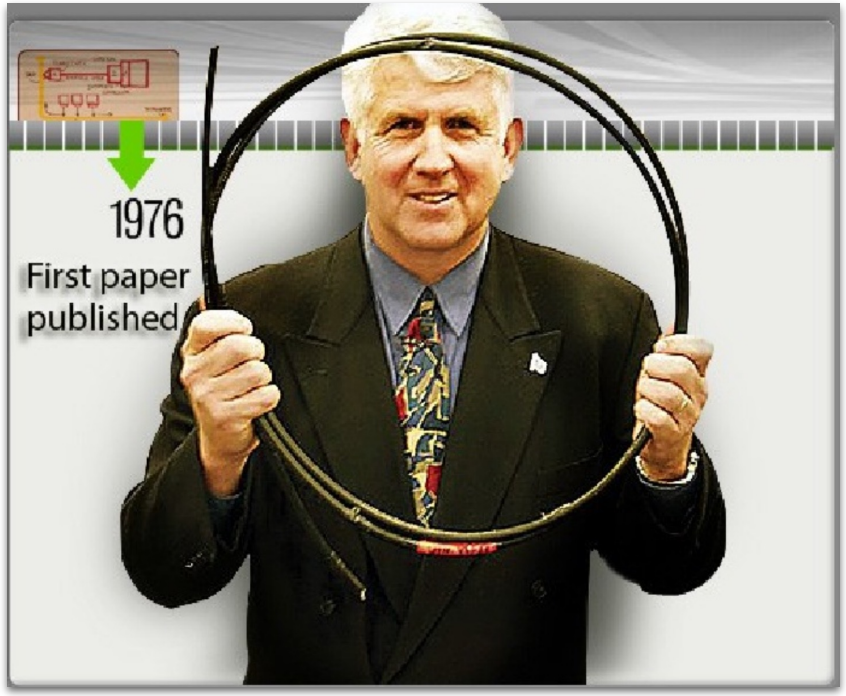
本章内容

- 4.1 信道分配问题
- 4.2 多路访问协议
- 4.3 IEEE802.3协议和以太网
- 4.4 IEEE802.11协议和无线局域网
- 4.5 网桥技术和交换机

1. 以太网的前世今生
2. 经典以太网
3. 以太网的性能
4. 交换式以太网
5. 快速以太网
6. 千兆以太网
7. 万兆以太网
8. 40G与100G以太网
9. 以太网的未来

以太网的前世今生



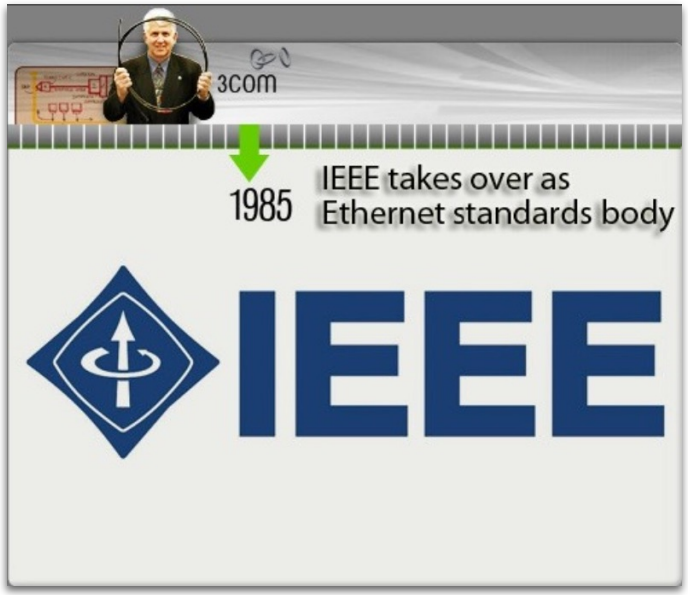


- Bob Metcalfe设计的在同轴电缆上实现3Mbps以太网连接方案的备忘录
- Metcalfe和David Boggs发表了题为《以太网：本地计算机网络的分布式包交换方式》的论文

图片来源 https://www.slideshare.net/citizenearth/bridge-to-tera-bit-ethernet

以太网的前世今生

- Metcalfe离开施乐创办3Com。第二年，他又发表了10Mbps以太网的标准，也就是DIX标准

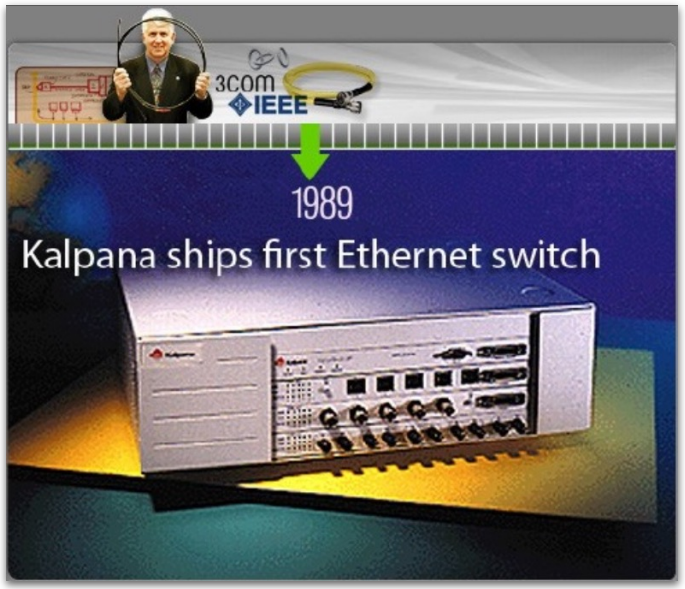


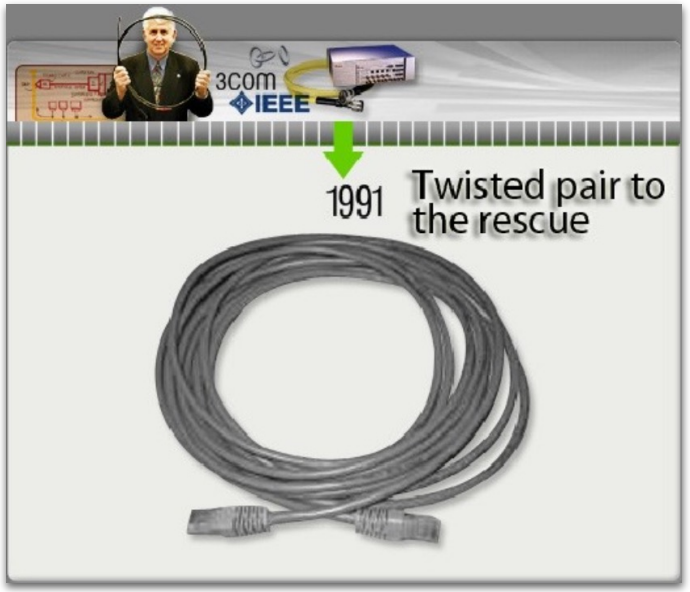
- IEEE成为以太网的官方标准化组织。开放的标准帮助以太网成了占绝对支配地位的LAN技术

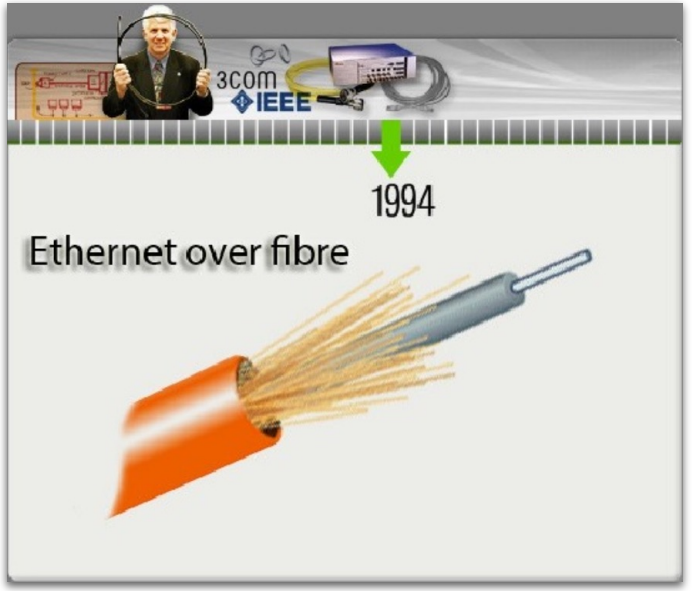
- IEEE发表了10Base5以太网标准，也称粗以太网

图片来源 https://www.slideshare.net/citizenearth/bridge-to-tera-bit-ethernet

以太网的前世今生



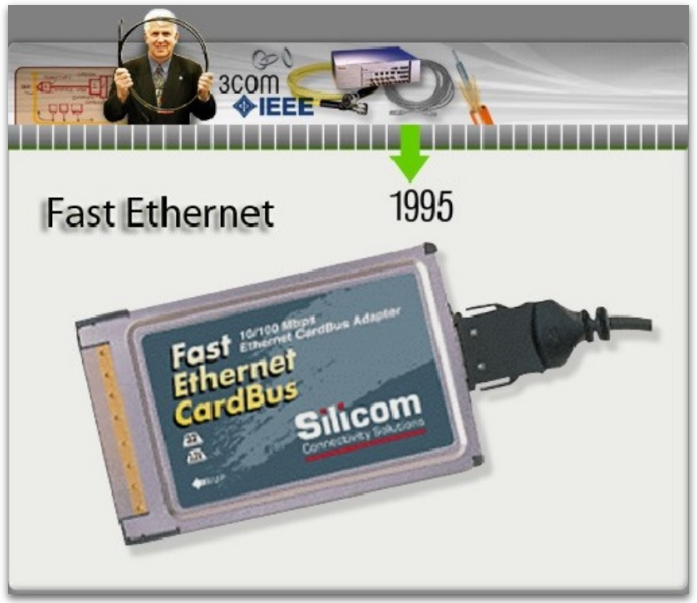


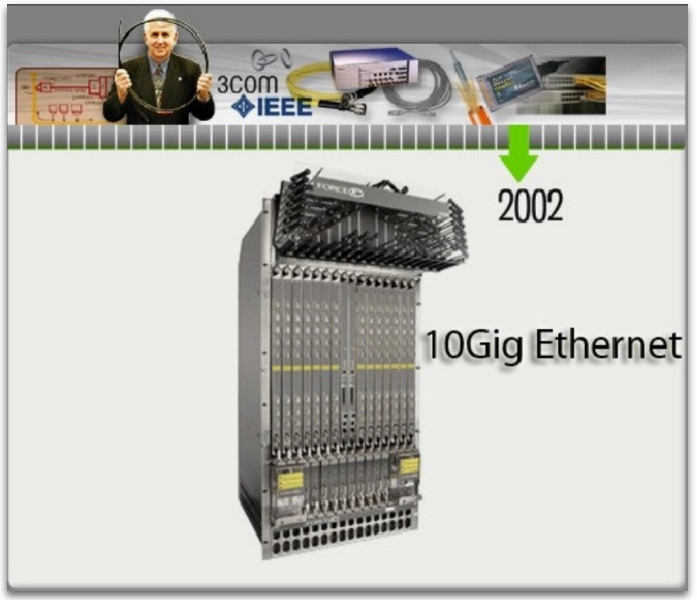


- Kalpana推出了第一台以太网交换机，最终取代了网桥和集线器
- IEEE批准了Cat-3双绞线10Base-T以太网，很快成为LAN部署的标准配置
- IEEE批准10BaseF标准，即数据中心所用的光纤以太网标准

图片来源 https://www.slideshare.net/citizenearth/bridge-to-tera-bit-ethernet

以太网的前世今生



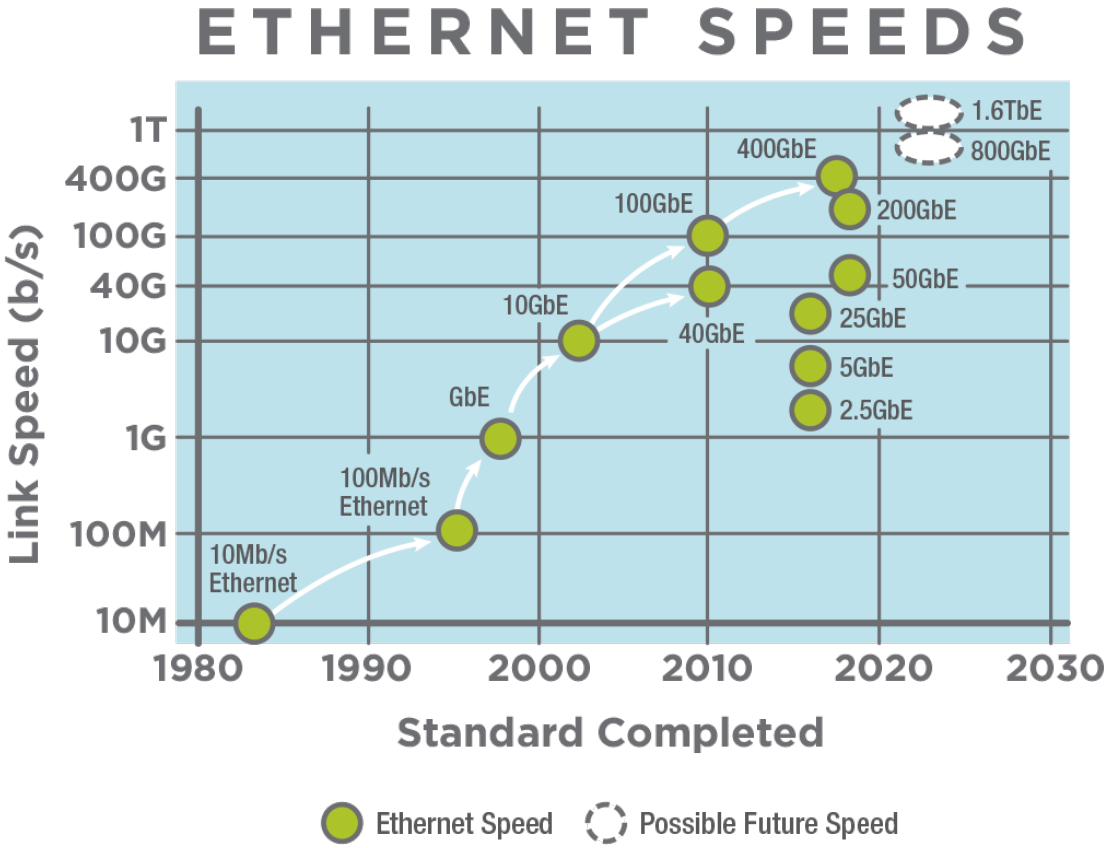


- IEEE批准了100Mbps以太网标准。后被称为快速以太网（Fast Ethernet）
- 千兆以太网标准1000Base-T获得通过
- 2001年，万兆以太网的标准前产品开始问世，正式标准在2002年获得通过

图片来源 https://www.slideshare.net/citizenearth/bridge-to-tera-bit-ethernet

以太网的前世今生

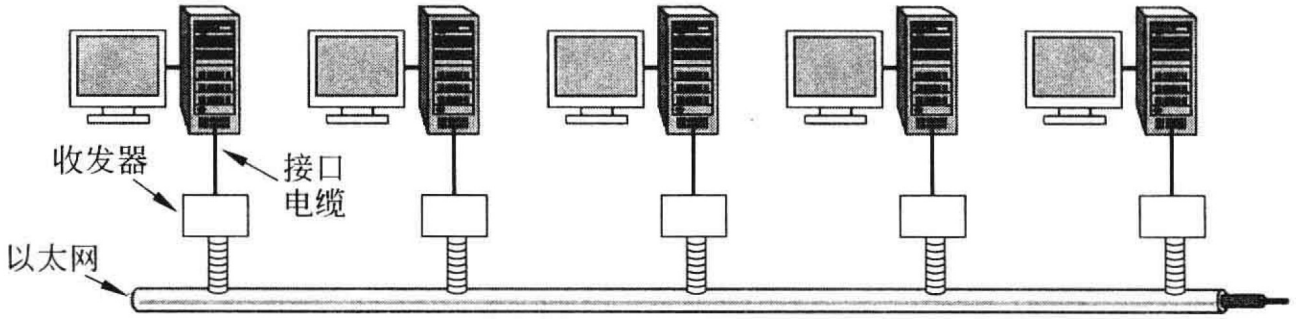
- 40G/100G 以太网标准在2010年中制定完成，当前使用附加标准IEEE 802.3ba用以说明
- 2014年，成立200 Gb/s和400 Gb/s以太网标准工作组IEEE P802.3bs



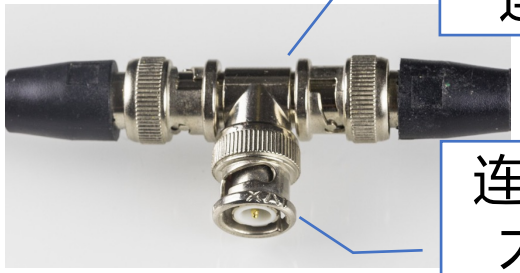
图片来源 https://ethernetalliance.org/technology/2020-roadmap/

经典以太网 - 经典以太网的物理层

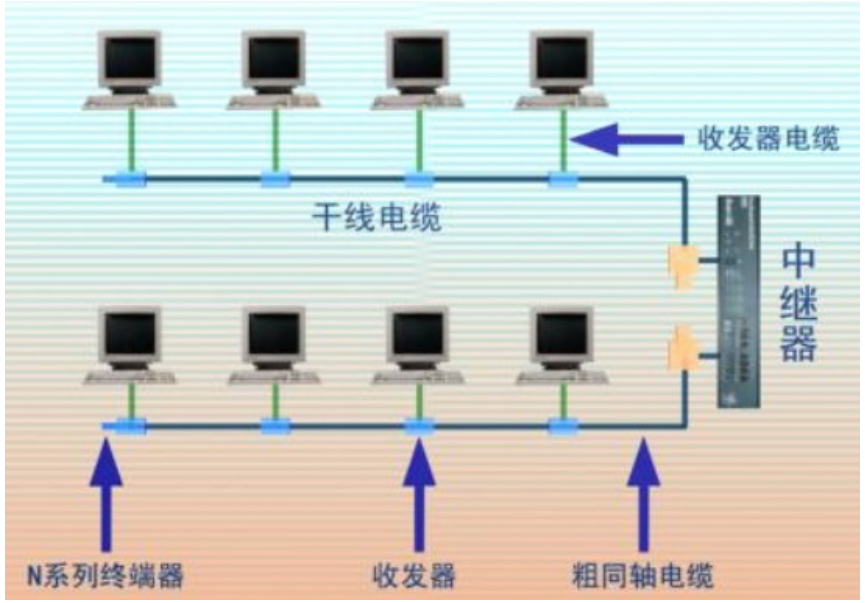
- 最高速率10Mbps
- 使用曼彻斯特编码
- 使用同轴电缆和中继器连接



粗以太网（thick Ethernet）



细以太网（thin Ethernet）



中继器（repeater）

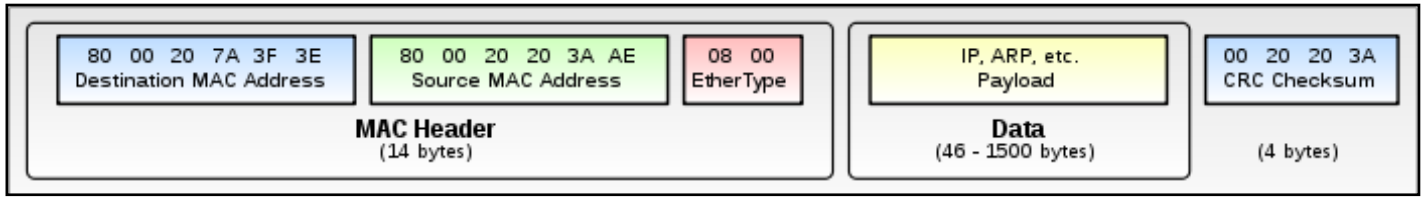
5-4-3-2-1原则

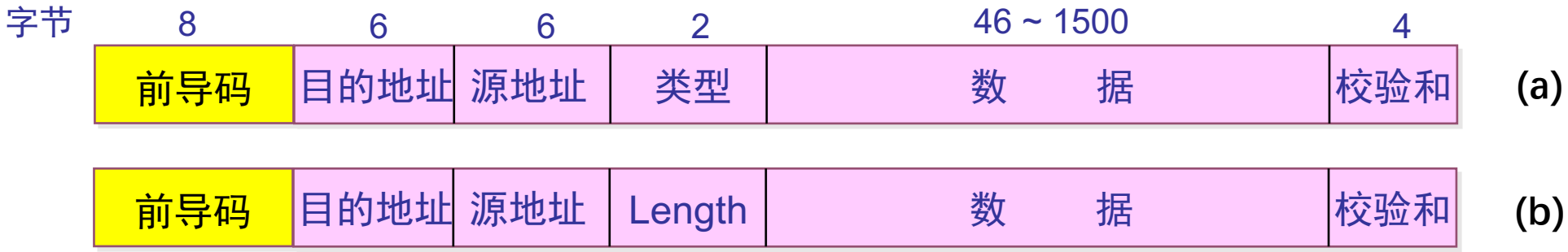
任意两个收发器之间距离不得超过2.5km
且任意两个收发器之间经过的中继器不能超过4个
以保证MAC协议正常工作

图片来源　Andrew S.Tanenbaum, 潘爱民. 计算机网络[M]. 清华大学出版社, 2012.

经典以太网 - MAC子层协议

- 主机运行CSMA/CD协议
- 常用的以太网MAC帧格式有两种标准 ：
  - DIX Ethernet V2 标准（最常用的）
  - IEEE 的 802.3 标准

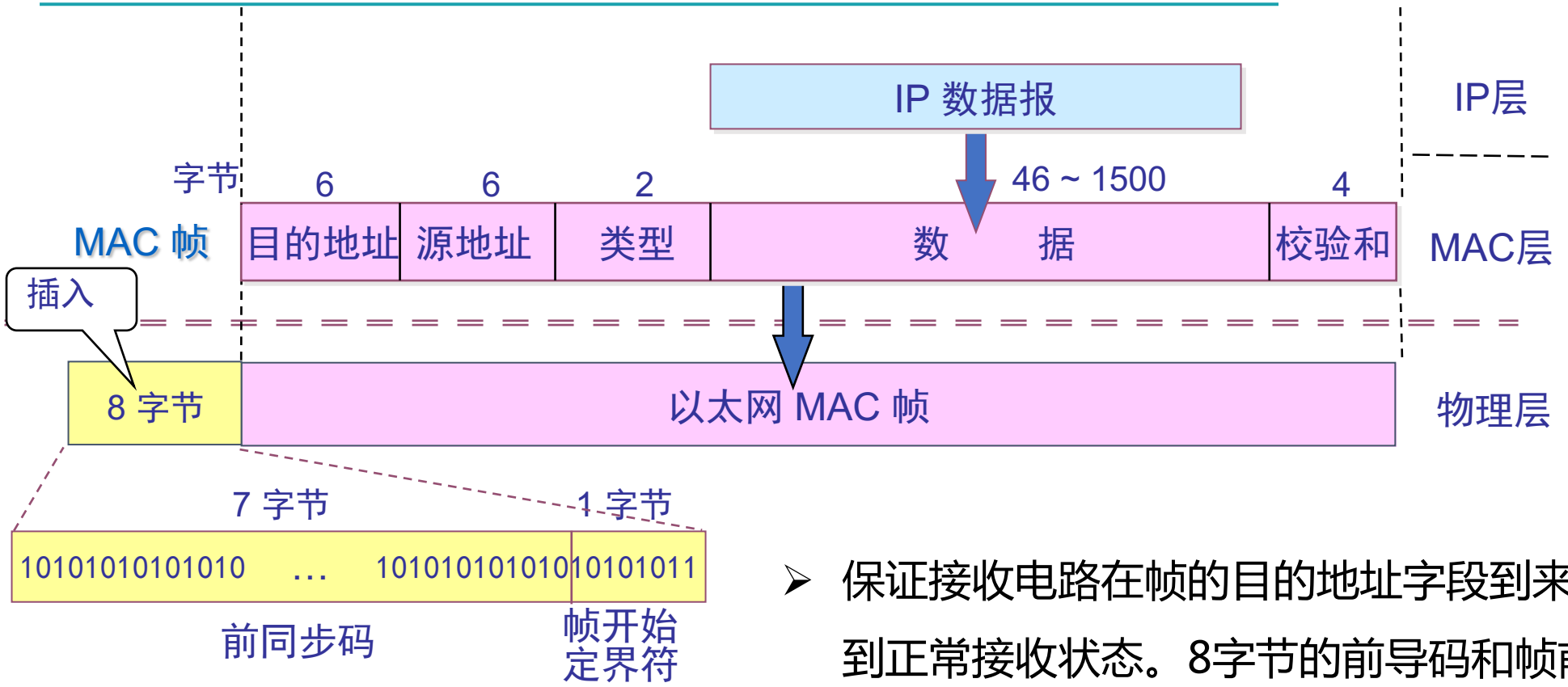




MAC帧格式
(a) DIX Ethernet V2 (b) IEEE 802.3

图片来源 https://en.wikipedia.org/wiki/Ethernet_frame

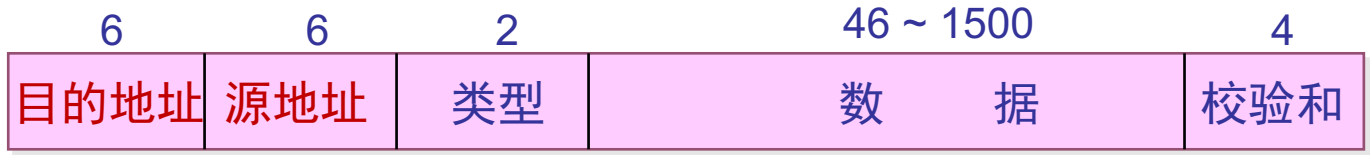
经典以太网 - MAC子层协议

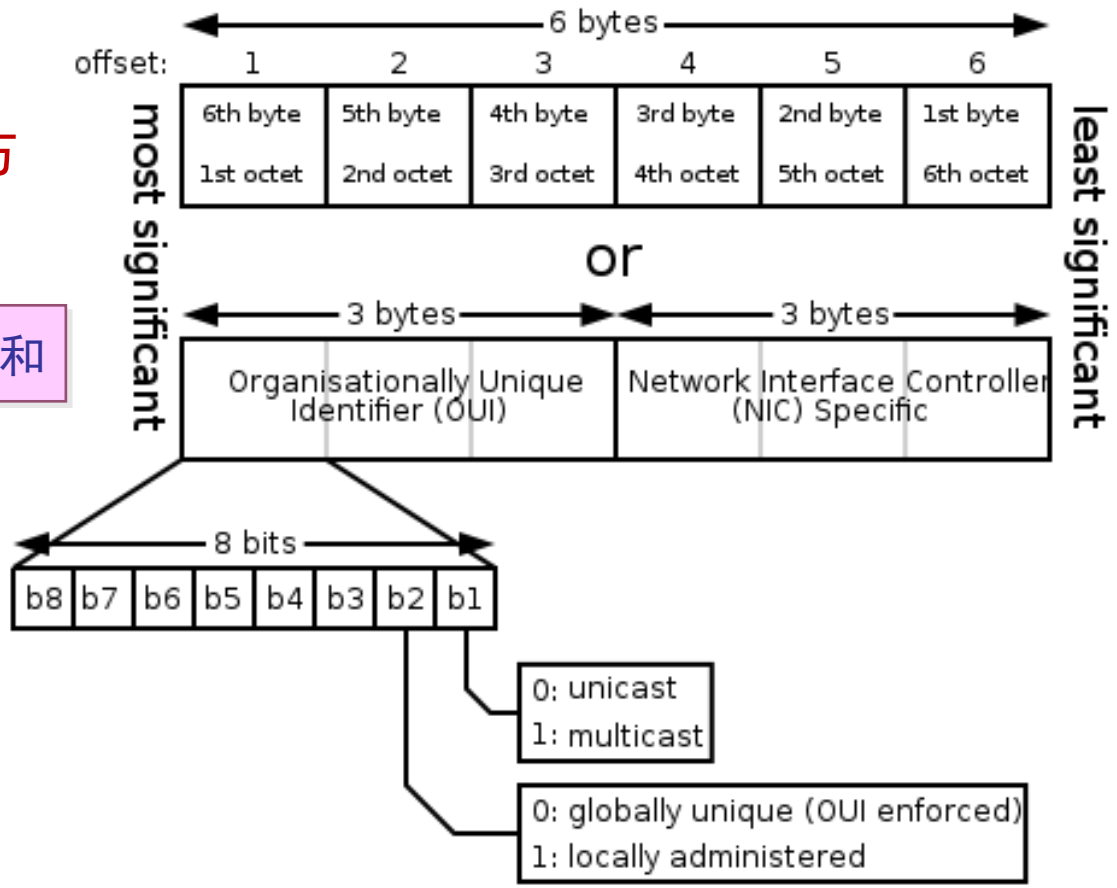


- 保证接收电路在帧的目的地址字段到来之前达到正常接收状态。8字节的前导码和帧前定界符不需要保留，也不计入帧头长度。

经典以太网 - MAC子层协议

- 硬件地址又称为物理地址，或 MAC 地址
- MAC帧中的源地址和目的地址长度均为6字节





MAC地址举例

单播（unicast）：　5C-26-0A-7E-4E-4C

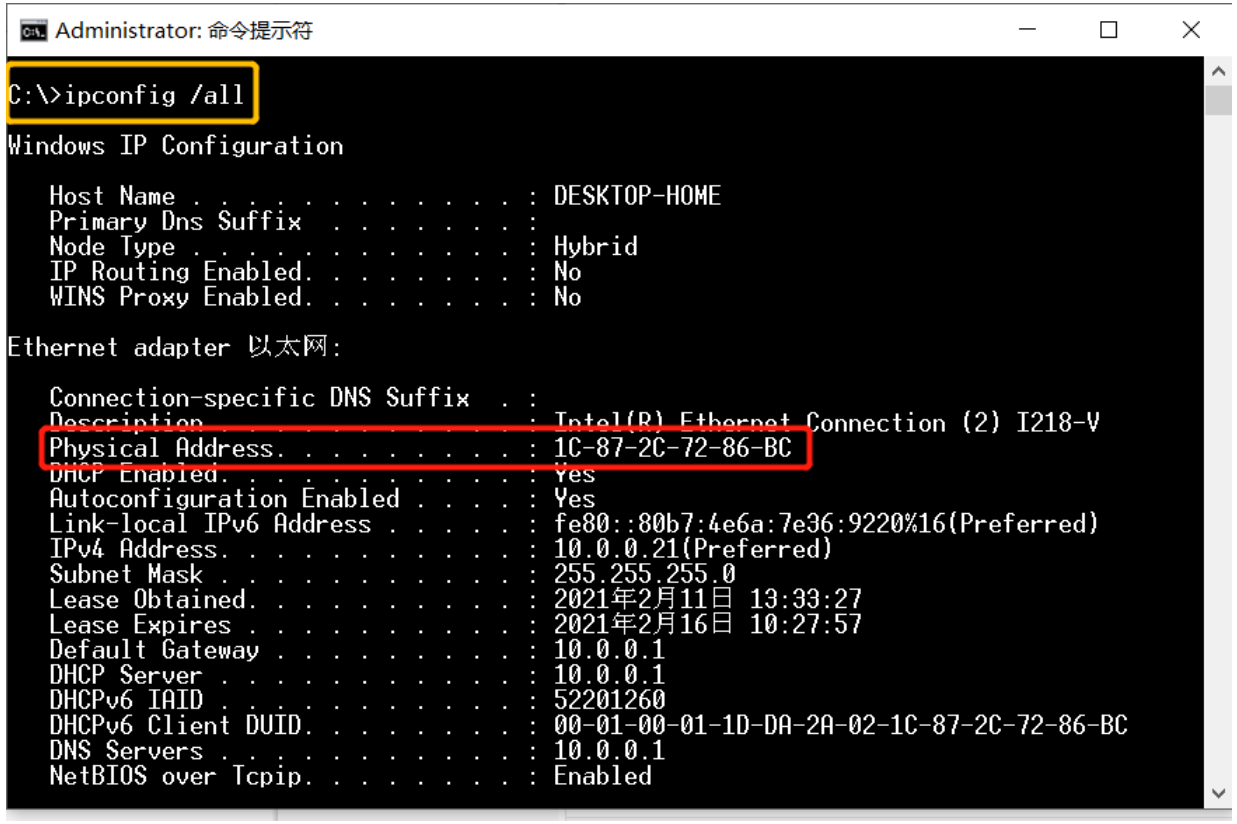
广播（broadcast）：FF-FF-FF-FF-FF-FF

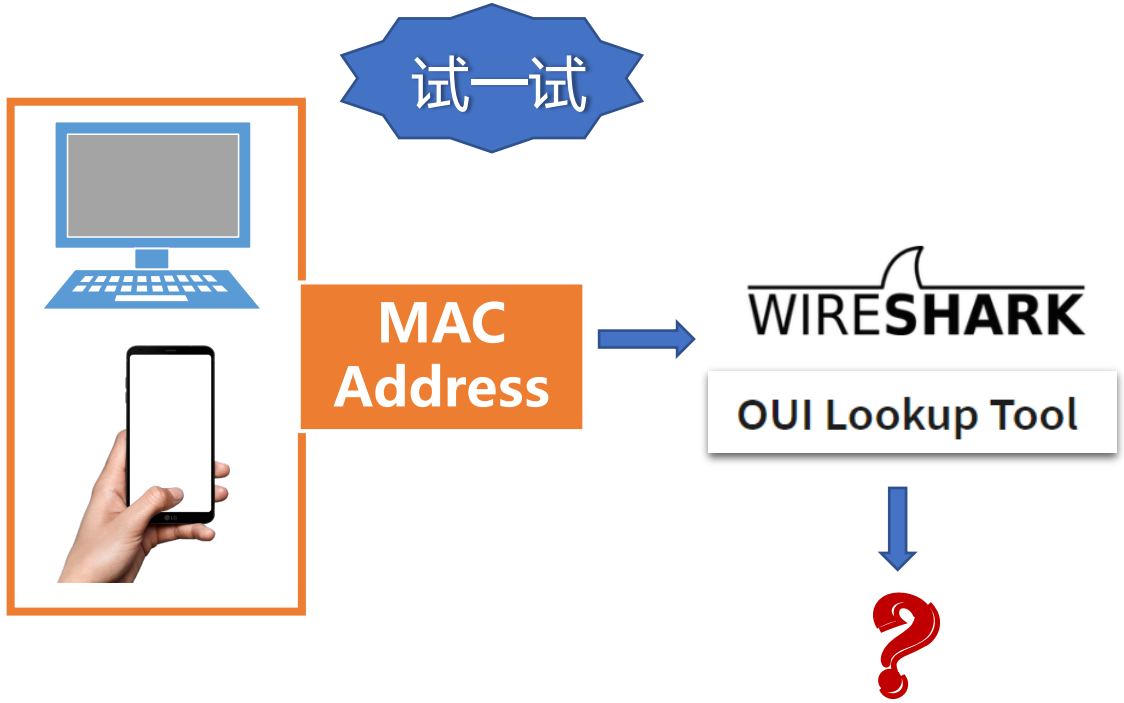
组播（multicast）：01-00-5E-00-00-00

图片来源　https://en.wikipedia.org/wiki/MAC_address

经典以太网 - MAC子层协议

- OUI(Organizationally Unique Identifier)
  - IEEE Registration Authority是负责注册和管理组织唯一标识符（OUI）的管理机构
- 在Windows上使用ipconfig /all命令查看MAC地址

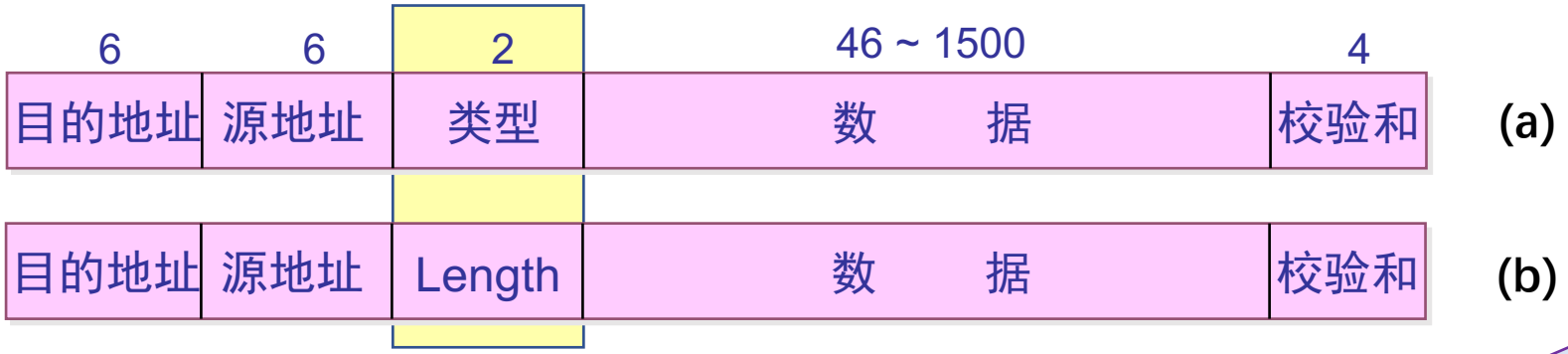




经典以太网 - MAC子层协议

- 源地址后面的两个字节，Ethernet V2将其视为上一层的协议类型，IEEE802.3将其视为数据长度。
- 可在这里查询协议类型（Ether Types）的值

IPv4: 0x0800
ARP: 0x0806
PPPoE: 0x8864
…



MAC帧格式
(a) DIX Ethernet V2 (b) IEEE 802.3

大家来找茬，两种格式哪里不同？

思考：网卡收到帧如何判断是Ethernet V2帧还是IEEE802.3帧呢？

经典以太网 - MAC子层协议

- 数据字段
  - 46 ~ 1500字节
  - 最小帧长 = 46+18 = 64B
  - 最大帧长 = 1500+18 = 1518B （MTU：1500B）

- 数据字段不足46字节，需要填充整数字节（Padding）至46字节，以保证以太网MAC帧不小于64字节。

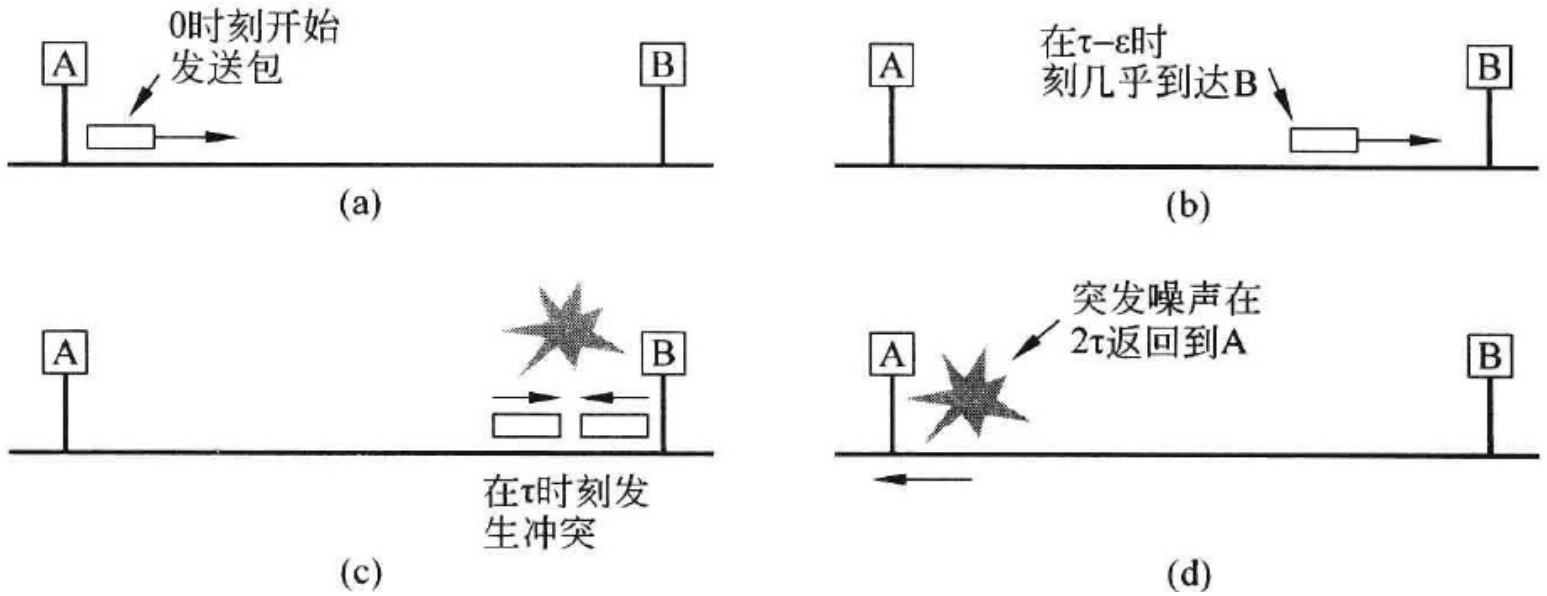
```
> Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: b0:7f:b9:ff:70:aa, Dst: 1c:87:2c:72:86:bc
  > Destination: 1c:87:2c:72:86:bc
  > Source: b0:7f:b9:ff:70:aa
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
> Address Resolution Protocol (reply)
```

```
0000  1c 87 2c 72 86 bc b0 7f  b9 ff 70 aa 08 06 00 01   ..,r.... ..p.....
0010  08 00 06 04 00 02 b0 7f  b9 ff 70 aa 0a 00 00 01   ........ ..p.....
0020  1c 87 2c 72 86 bc 0a 00  00 16 00 00 00 00 00 00   ..,r.... ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

经典以太网 - MAC子层协议

- 以太网规定最短有效帧长为 64 字节，凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧。
  - 如果发生冲突，就一定是在发送的前 64 字节之内
  - 由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 64 字节
  - So，why 64B ？

802.3规范中的10Mbps以太网，最大长度为2500米，具有4个中继器，在最差情况下往返一次时间大约是50微秒，在这个时间内能发送500bit，加上安全余量增加至51bit，即64Bytes。



图片来源　Andrew S.Tanenbaum, 潘爱民. 计算机网络[M]. 清华大学出版社, 2012.

经典以太网 - MAC子层协议

- 校验和
  - FCS, Frame Check Sequence
  - 使用CRC32计算除了校验和以外的其他字段
- 对于检查出的无效 MAC 帧就简单地丢弃。以太网不负责重传丢弃的帧。

- 数据字段的长度与长度字段的值不一致；
- 帧的长度不是整数个字节；
- 用收到的帧检验序列 FCS 查出有差错；
- 数据字段的长度不在 46 ~ 1500 字节之间。

图片来源　https://ethernetalliance.org/technology/2020-roadmap/

经典以太网 - MAC子层协议

怎么确定？

- 使用CSMA/CD的经典以太网检测到冲突后，会立即中止传输，并发出一个短冲突加强信号，在等待一段随机时间后重发。
- 二进制指数后退(Binary exponential backoff)的CSMA/CD
  - 确定基本退避时间槽，其长度为以太介质上往返传播时间(2τ) ，以太网中设为512比特时间
  - 定义重传次数 k ，$k \le 10$，即

    k = min[重传次数 , 10]
  - 从整数集合[0,1,…, $(2^k - 1)$]中随机地取出一个数，记为 r ；
  - 重传所需的时延就是 r 倍的时间槽2τ；
  - 当重传达 16 次仍不能成功时即丢弃该帧，并向高层报告。

图片来源 https://ethernetalliance.org/technology/2020-roadmap/

以太网性能

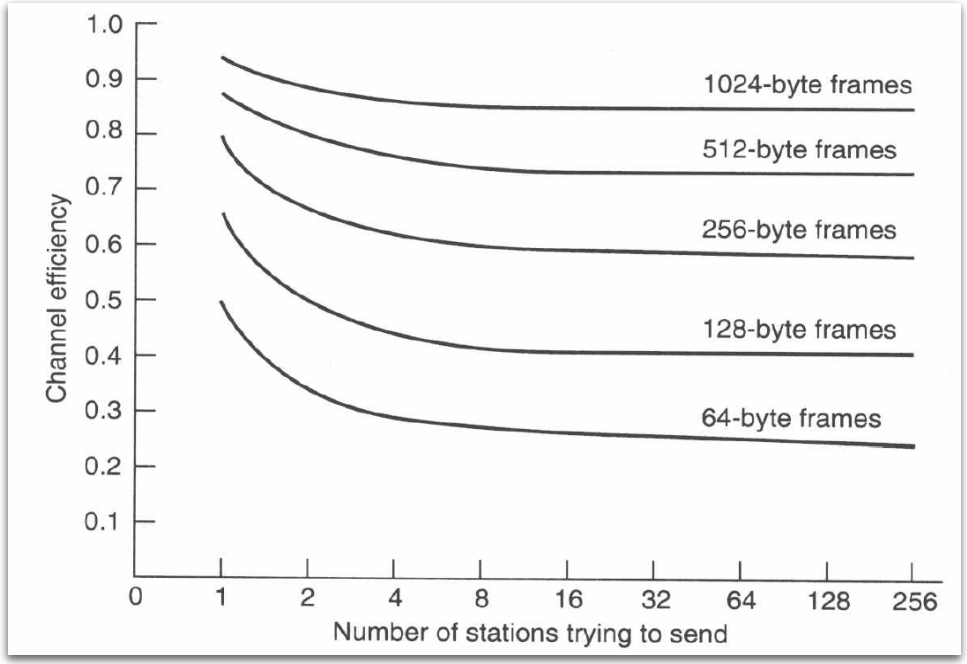
- 使用二进制指数后退算法的CSMA/CD方法，以太网的性能？

$$\text{信道效率} = \frac{P}{P + 2\tau/A}$$

P=F/B，F为帧长，B为带宽；
L为电缆长度，c为信号传播速度；
假设每帧e个竞争时间槽

$$\text{信道效率} = \frac{1}{1 + 2BLe/cF}$$

- 传送一帧平均需要P秒，某个站获得信道的概率为A，2τ为时间槽。
- 电缆越长，τ越大，任何两个站之间的最大电缆距离会影响性能。



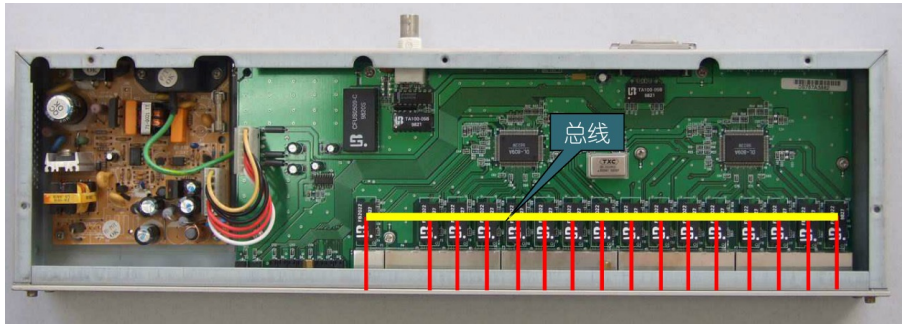
具有512bit时间槽的10Mbps以太网效率

- 在给定帧长的情况下，增加带宽或距离会降低网络效率。
- 然而网络发展的目标总是在长距离上拥有高带宽！

图片来源　Andrew S.Tanenbaum, 潘爱民. 计算机网络[M]. 清华大学出版社, 2012.

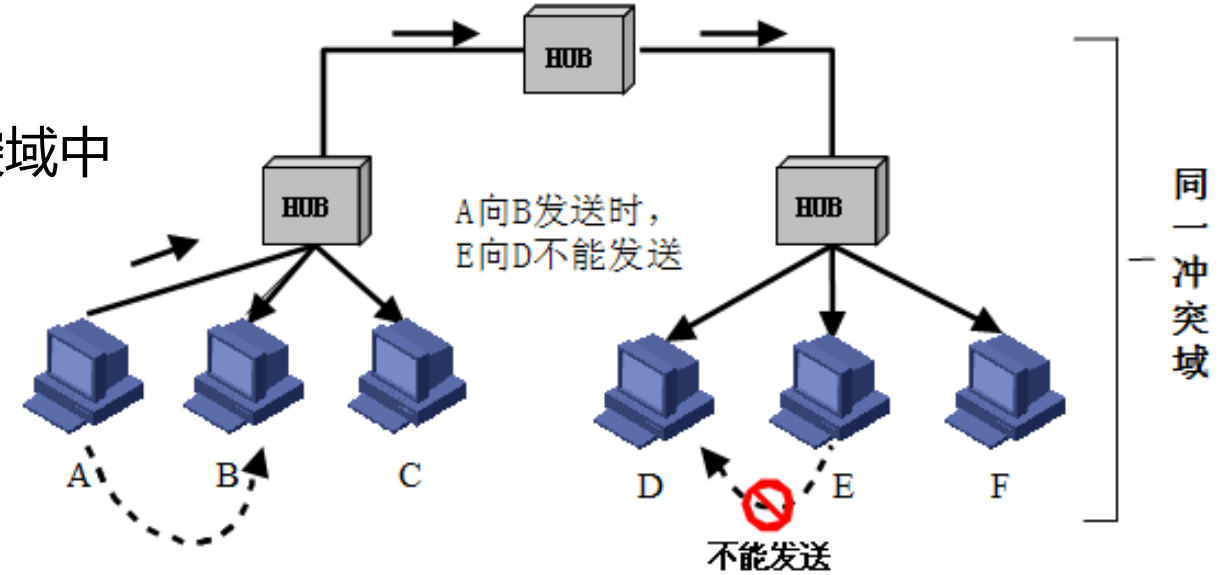
交换式以太网

- 使用集线器（HUB）组建以太网
  - Hub所有端口内部都是连通的
  - 使同一根总线
  - 和Repeater一样，也是物理层设备



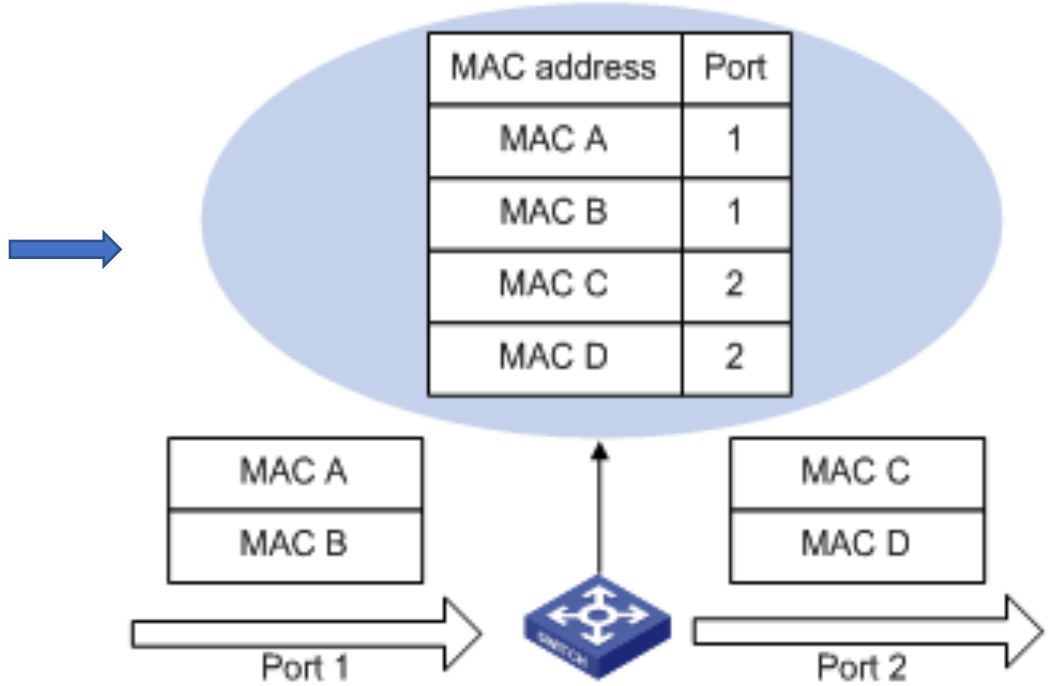
- 使用Hub扩展以太网
  - 集线器不能增加容量
  - 用集线器组成更大的局域网都在一个冲突域中
  - Hub级连：限制了网络的可扩展性

Switched Ethernet
to the rescue!



交换式以太网

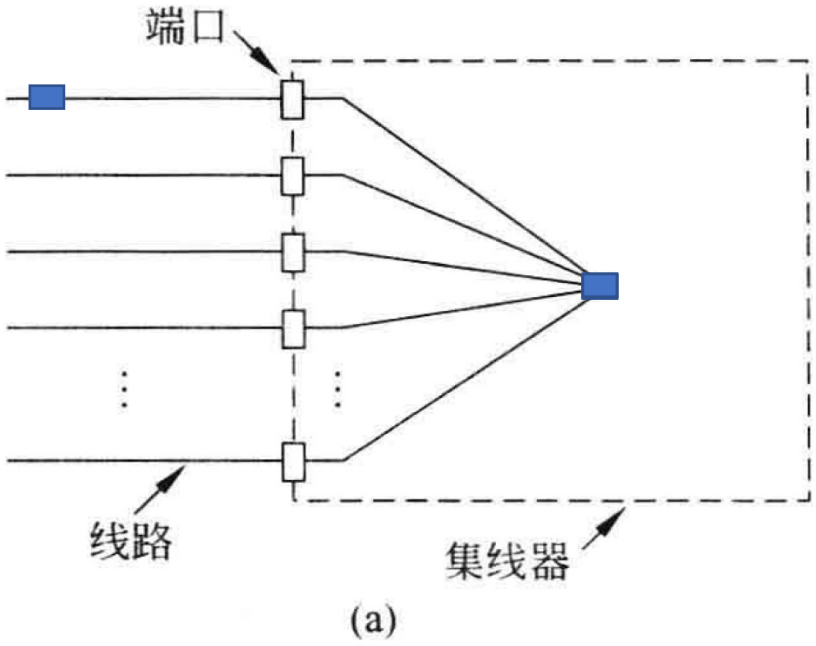
- 交换式以太网的核心是交换机（Switch）
  - 工作在数据链路层，检查MAC 帧的目的地址对收到的帧进行转发
  - 交换机通过高速背板把帧传送到目标端口



  - 混杂模式（promiscuous mode）
    - Hacker
    - 网络分析

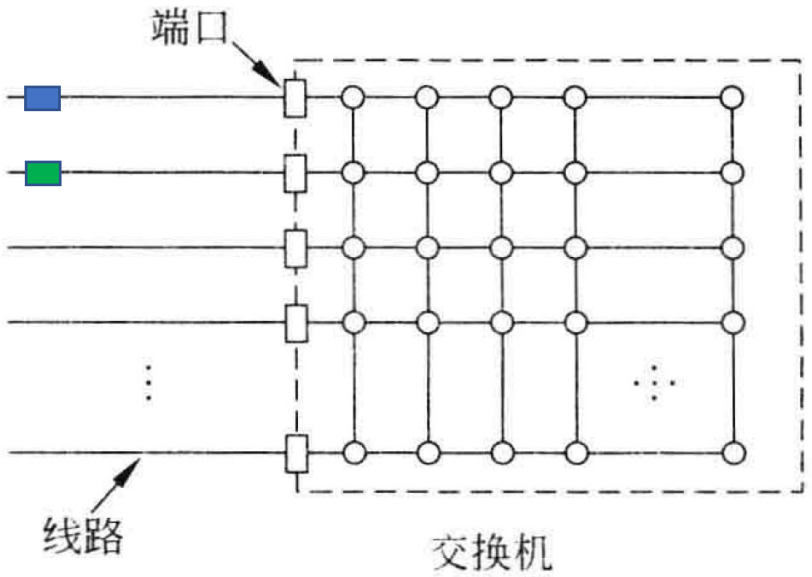
交换式以太网

Hub vs Switch



(a)

- 内部连接所有线缆，逻辑上等同于单根总线的经典以太网
- 所有站都位于同一个冲突域，必须使用CSMA/CD协议



(b)

- 内部通过高速背板连接所有端口
- 每个端口都有独立的冲突域，在全双工模式下端口可以同时收发，则不需要CSMA/CD
- 可以实现并行传输

图片来源　Andrew S.Tanenbaum, 潘爱民. 计算机网络[M]. 清华大学出版社, 2012.

快速以太网

- fast Ethernet(IEEE 802.3u, 1995)
  - 带宽 10Mbps → 100Mbps
  - 比特时间 100ns → 10ns
  - 保留原来的工作方式（帧格式、接口、过程规则）
  - 自动协商（autonegotiation）
  - 线缆类型

与之前10Mbps版本的以太网相比，10倍的速度非常快。千兆以太网诞生后，100Mbps就不再是最快的以太网了，但人们仍习惯于称100Mbps以太网为“快速以太网”。

电缆的最大长度降低到十分之一

名称	线缆	最大长度	编码方式	优点
100Base-T4	双绞线	100米	8B6T	可用3类UTP
100Base-TX	双绞线	100米	4b/5b	全双工速率100Mbps(5类UTP)
100Base-FX	光纤	2000米	4b/5b	全双工速率100Mbps，距离长

千兆以太网

- gigabit Ethernet(IEEE 802.3ab, 1998)
  - 100Mbps → 1000Mbps(1Gbps)
  - 保留原来的工作方式（帧格式、接口、过程规则）
  - 全双工和半双工两种方式工作。
    - 在半双工方式下使用 CSMA/CD （为了向后兼容），增加载波扩充和帧突发
    - 全双工方式不需要使用CSMA/CD（缺省方式）
  - 流量控制和巨型帧（Jumbo frame）
  - 线缆类型

为保证CSMA/CD继续工作，电缆的最大长度再降低到快速以太网的十分之一？

名称	线缆	最大长度	编码方式	优点
1000Base-SX	光纤	550米	8b/10b	多模光纤（50、62.5微米）
1000Base-LX	光纤	5000米	8b/10b	单模光纤（10微米） 或多模光纤（50、62.5微米）
1000Base-CX	2对STP	25米	8b/10b	屏蔽双绞线
1000Base-T	2对UTP	100米	4D-PAM5	标准5类UTP

万兆以太网

- 10-Gigabit Ethernet(IEEE 802.3ae, 2002)
  - 1Gbps → 10Gbps
  - 常记为10GE, 10GbE 或 10 GigE
  - 只支持全双工，不再使用CSMA/CD
  - 保持兼容性
  - 重点是超高速的物理层

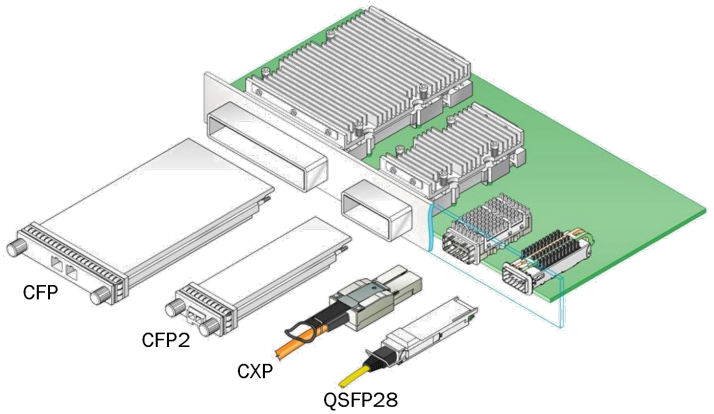
10GBASE-SR SFP +收发器

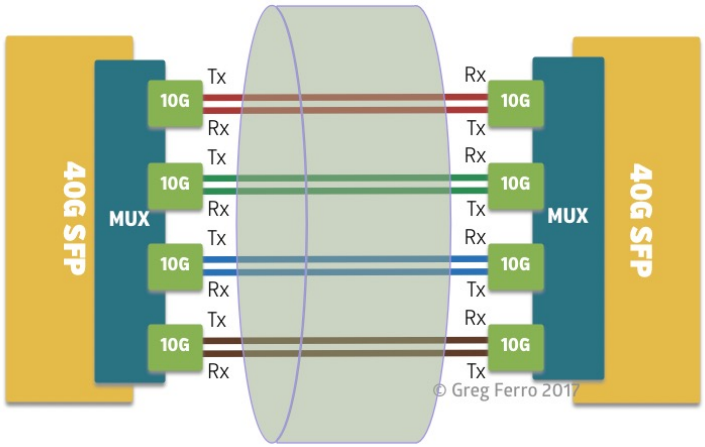
名称	线缆	最大长度	编码方式	优点
10GBase-SR	光纤	最多300米	64b/66b	多模光纤（0.85微米）
10GBase-LR	光纤	10千米	64b/66b	单模光纤（1.3微米）
10GBase-ER	光纤	40千米	64b/66b	单模光纤（1.5微米）
10GBase-CX4	4对双轴	15米	8b/10b	双轴铜缆
10GBase-T	4对UTP	100米	64b/65b	6a类UTP

图片来源 https://en.wikipedia.org/wiki/10_Gigabit_Ethernet

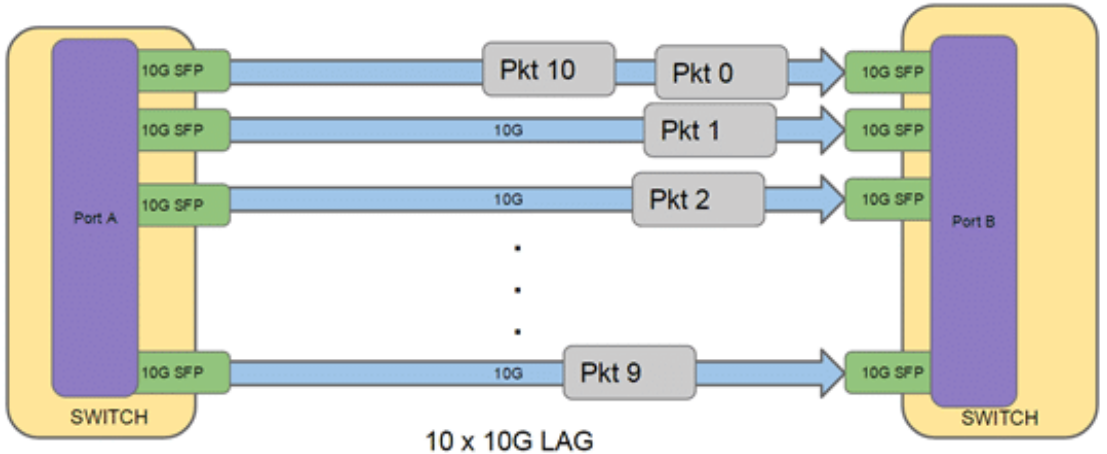
40G-100G以太网

- 40 Gigabit Ethernet (40GbE) and 100 Gigabit Ethernet (100GbE), 2010
  - 10Gbps → 40Gbps & 100Gbps
  - 只支持全双工
  - 保留以太网帧格式和MAC方法
  - 保留当前802.3标准的最小帧和最大帧大小
  - 联网设备可以通过可插拔模块支持不同的物理层类型





4 x 10G lanes



10 x 10G LAG

10 x 10G lanes

图片来源 https://fmad.io/blog-100g-ethernet.html
https://packetpushers.net/buy-40g-ethernet-obsolete/
https://www.optcore.net/understanding-100g-ethernet

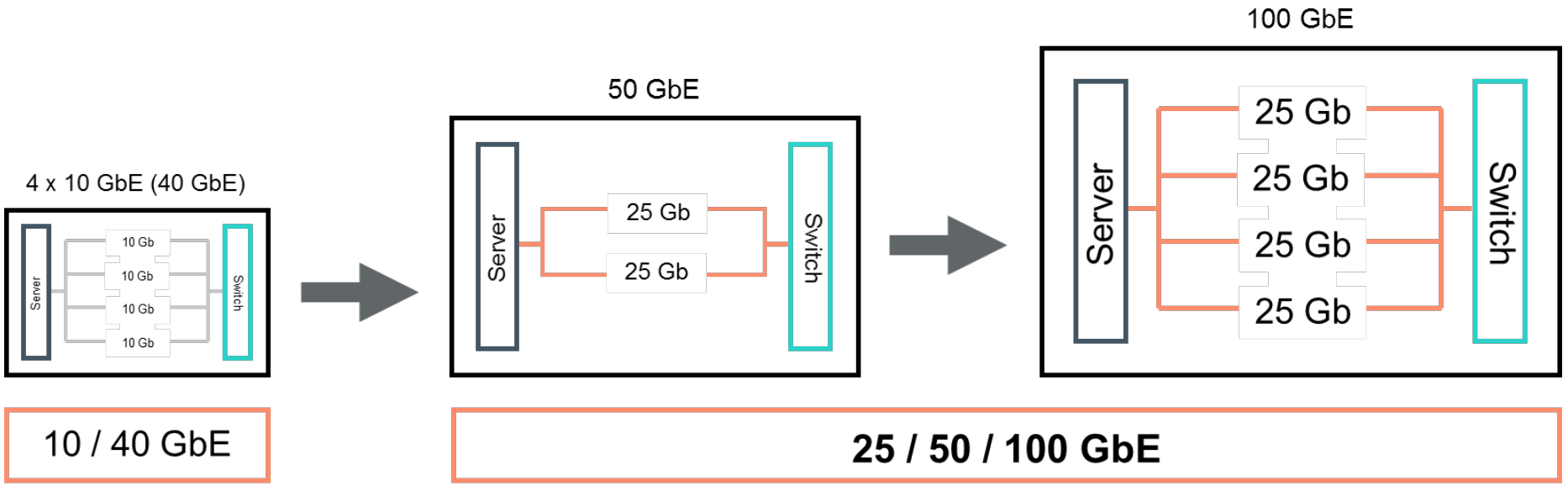
40G-100G以太网

- 40 Gigabit Ethernet (40GbE) 与 100 Gigabit Ethernet (100GbE)
  - 40/100 GbE提供物多种物理层规范（PHY），定义了许多端口类型，具有不同的光学和电气接口，以便在单模光纤、多模光纤、双芯铜缆、双绞线和网络设备背板上运行。

名称	最大长度	40G以太网	100G以太网
改进的背板	1米	40GBASE-KR4	100GBASE-KR4 100GBASE-KR2
双芯铜缆	7米	40GBASE-CR4	100GBASE-CR10 100GBASE-CR4 100GBASE-CR2
8类双绞线	30米	40GBASE-T	-
多模光纤	100米/OM3, 125米/OM4	40GBASE-SR4	100GBASE-SR10 100GBASE-SR4 100GBASE-SR2
单模光纤	500米	-	100GBASE-DR
单模光纤	2千米	40GBASE-FR	100GBASE-FR1
单模光纤	10千米	40GBASE-LR4	100GBASE-LR4 100GBASE-LR1
单模光纤	40千米	40GBASE-ER4	100GBASE-ER4
单模光纤	80千米	-	100GBASE-ZR

以太网的未来

- 25/50G和第二代100G以太网
  - 25G以太网标准（IEEE 802.3by）是由IEEE和IEEE-SA于2014年发布，该标准弥补了10G以太网的低带宽和40G以太网的高成本缺陷。25G以太网采用了25Gb/s单通道物理层技术，可基于4个25Gbps光纤通道实现100G传输。



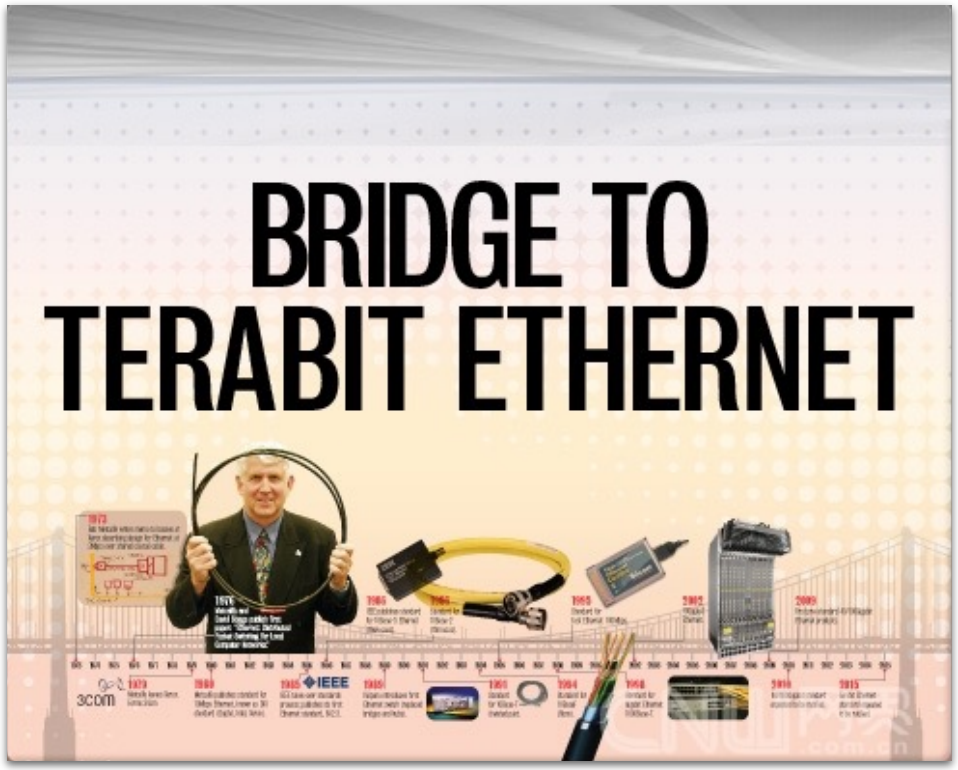
图片来源 https://blogs.arubanetworks.com/solutions/accelerate-network-performance-and-lower-costs-with-hpe-25-100gbe/

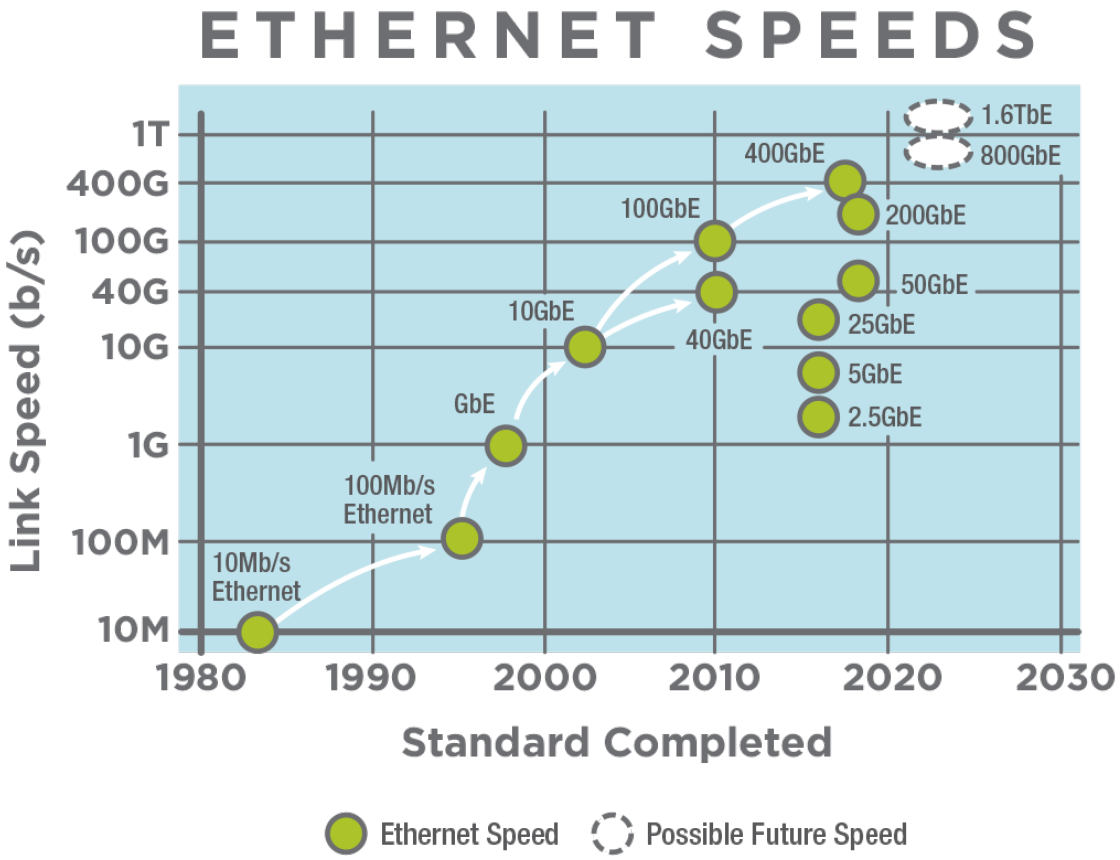
以太网的未来

- 2017年，由IEEE P802.3bs工作组使用与100GbE大致相似的技术开发的400GbE和200GbE标准获得批准。
  - 保留以太网帧格式
  - 保留以太网最小帧长和最大帧长
- 2020年，以太网技术联盟（Ethernet Technology Consortium）宣布开发800G以太网规范，以满足数据中心网络不断增长的性能需求。

以太网的未来

- 以太网联盟的2020技术路线图预计2020年-2030年之间，800Gbps和1.6Tbps的速度将成为IEEE标准。

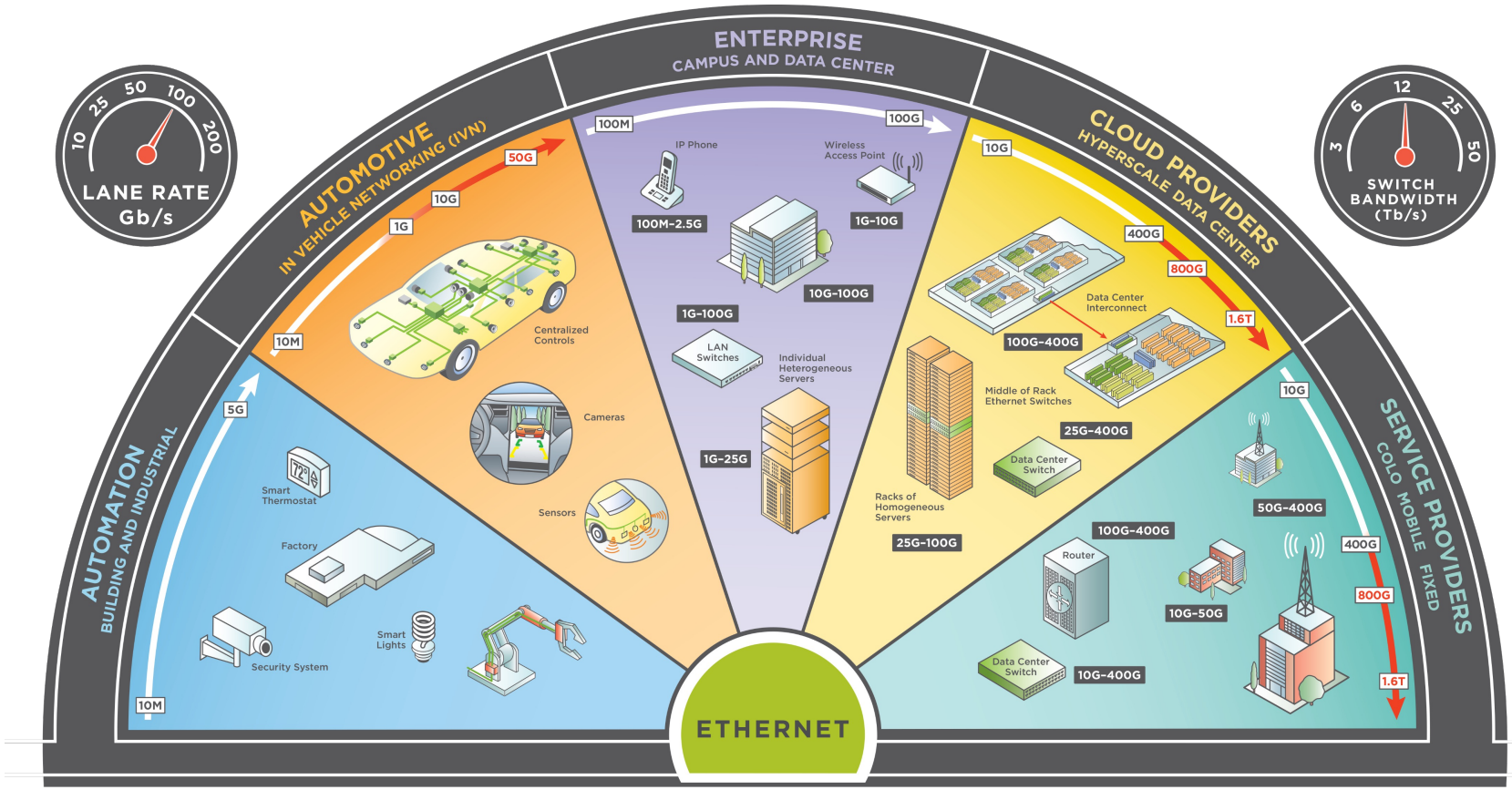




图片来源 https://www.slideshare.net/citizenearth/bridge-to-tera-bit-ethernet
https://ethernetalliance.org/technology/2020-roadmap/

以太网的未来

- 为什么以太网能够持续发展30多年，独占鳌头屹立不倒？
- 不断增长的以太网生态系统



灵活性

简单性

兼容性

廉价

易维护

可靠性

易扩展

图片来源 https://ethernetalliance.org/technology/2020-roadmap/

本章内容

- 4.1 信道分配问题
- 4.2 多路访问协议
- 4.3 IEEE802.3协议和以太网
- 4.4 IEEE802.11协议和无线局域网
- 4.5 网桥技术和交换机

1. 无线局域网概述
2. 无线局域网组网模式
3. 无线局域网体系结构
4. 802.11物理层
5. 802.11介质访问控制
6. 802.11帧结构
7. 无线局域网的构建

无线局域网概述

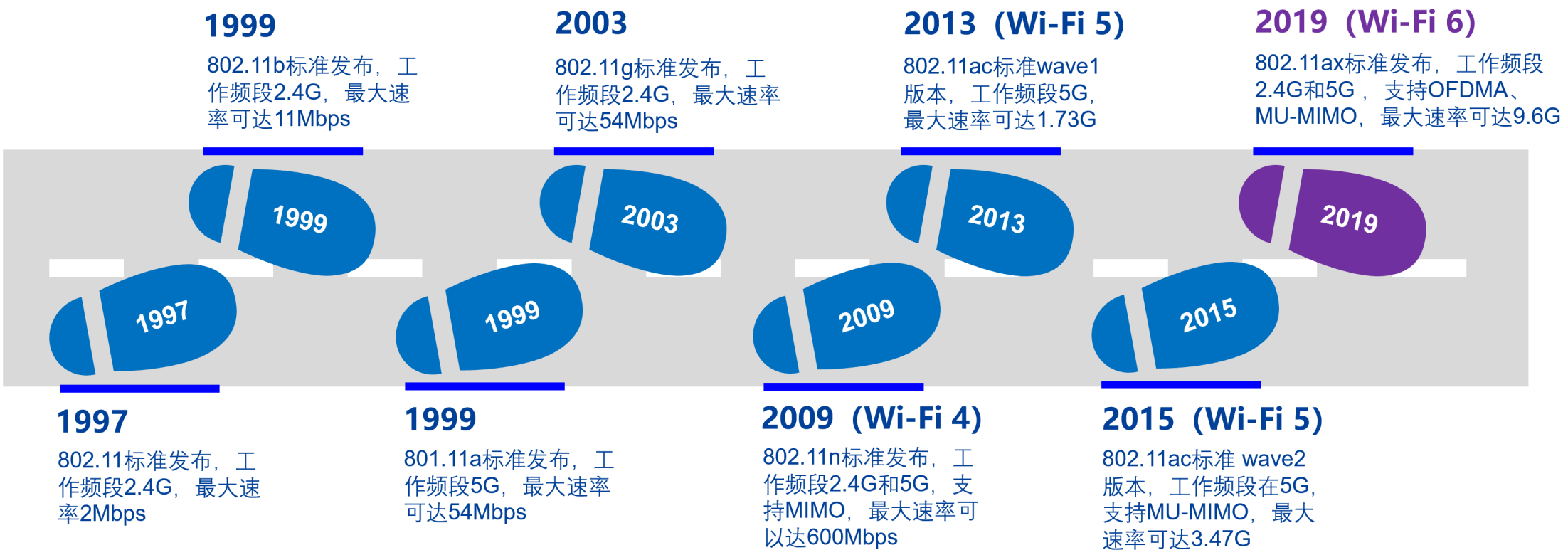
无线局域网（Wireless Local Area Network，WLAN)：指以无线信道作为传输介质的计算机局域网

- 设计目标
  - 针对小的覆盖范围（受限的发射功率）
  - 使用无需授权的频谱（ISM频段)
  - 面向高速率应用
  - 能够支持实时和非实时应用

两个重要组织：IEEE 802.11工作组、Wi-Fi联盟（Wi-Fi Alliance，WFA）

无线局域网概述

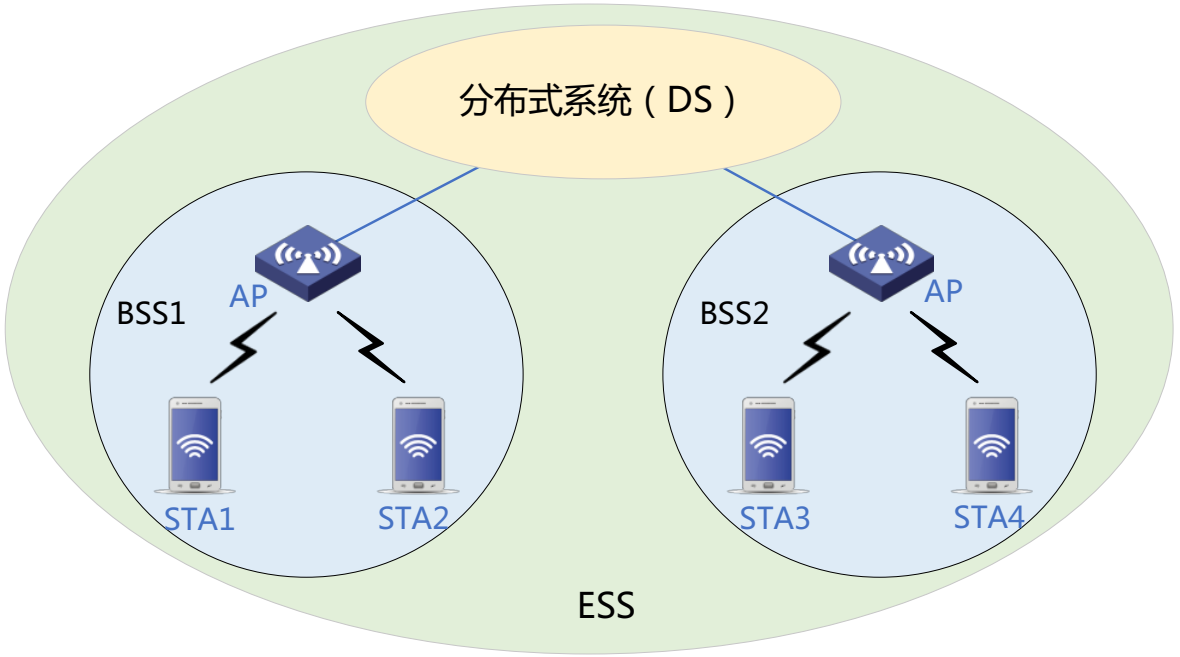
- IEEE 802.11无线局域网发展历程



无线局域网组网模式

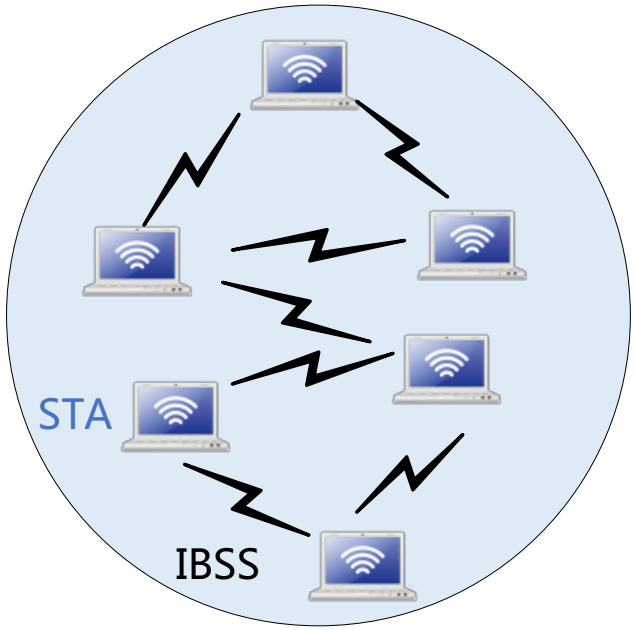
➢ 基础架构模式

- 分布式系统（DS）
- 访问点（AP）
- 站点（STA）
- 基本服务集（BSS）
- 扩展服务集（ESS）
- 站点之间通信通过AP转发



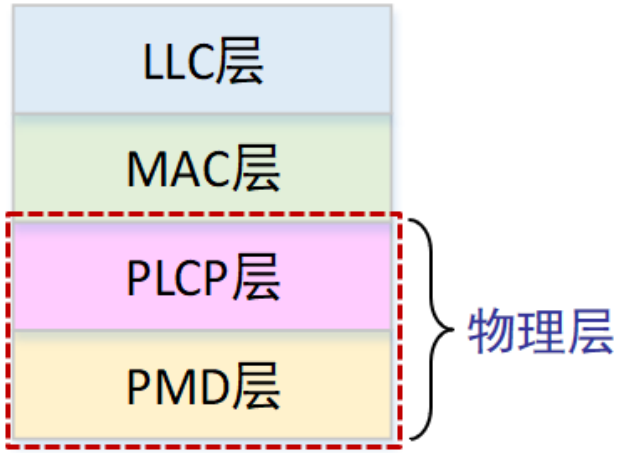
无线局域网组网模式

- 自组织模式（Ad hoc）
  - 站点（STA）
  - 独立基本服务集（IBSS）
  - 站点之间直接通信
  - 共享同一无线信道



无线局域网体系结构

- 物理介质相关子层（PMD层）
  - 调制解调、编码/解码
- 物理层汇聚协议（PLCP层）
  - 向上提供独立于传输技术的物理层访问点
- 介质访问控制层（MAC层）
  - 可靠数据传输
  - 介质访问控制
  - 安全机制
  - ……



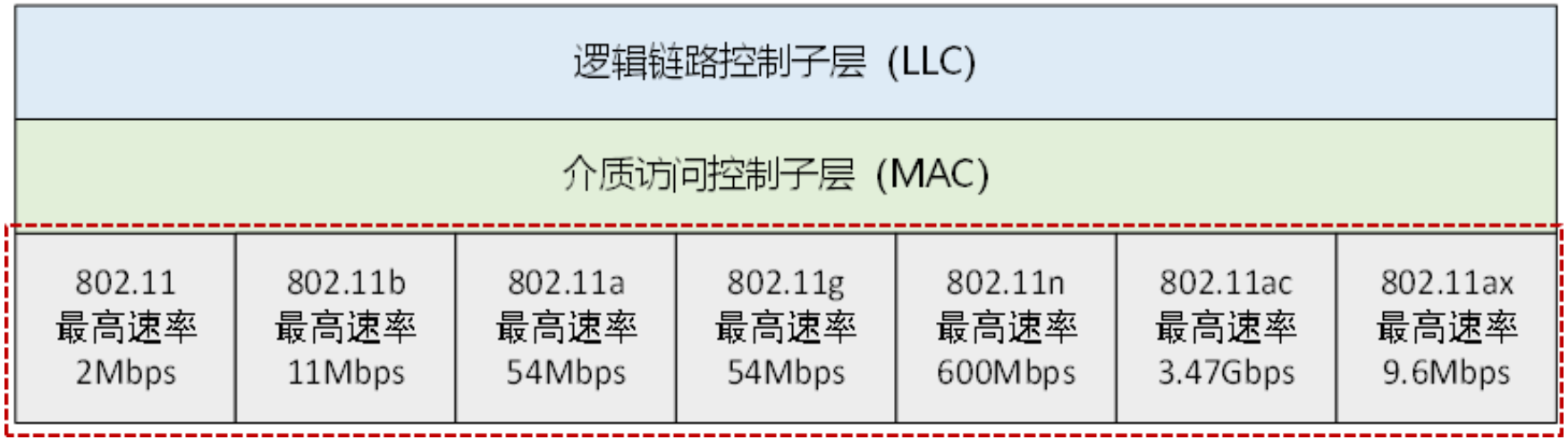
无线局域网体系结构

- 无线局域网需要解决的问题
  - 有限的无线频谱带宽资源
    - 通道划分、空间重用
    - 提高传输速率，解决传输问题
    - 提高抗干扰能力和保密性
  - 共享的无线信道
    - 介质访问控制方法（CSMA/CA）
    - 可靠性传输、安全性
  - 组网模式管理
    - BSS构建、认证、关联
    - 移动性支持（漫游）
    - 睡眠管理（节能模式）

IEEE 802.11物理层

➢ 物理层技术概览

- 频段：2.4GHz、5GHz（ISM频段，无需授权；限制发送功率，例如：≤ 1瓦）
- 调制技术：DPSK → QPSK → CCK → 64-QAM → 256-QAM → 1024-QAM
- 直接序列扩频（DSSS）→ 正交频分多路复用（OFDM）→正交频分多址（OFDMA）
- 单天线 → 单用户多入多出（SU-MIMO）→ 多用户多入多出（MU-MIMO）
- 目标：提升传输速率、增强可靠性、支持高密度接入

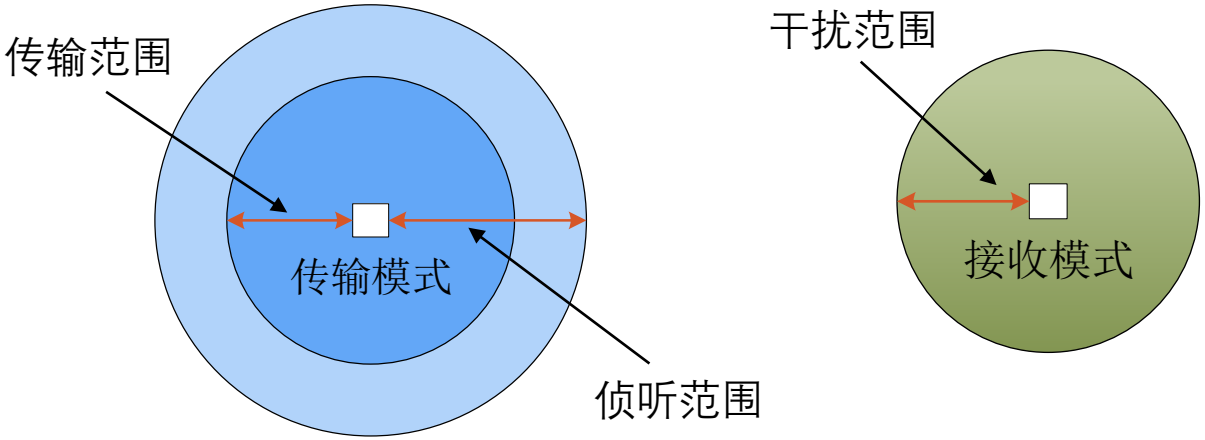


IEEE 802.11介质访问控制

- 直接将CSMA/CD用于无线局域网？
  - 冲突检测困难
    - 在接收端，发送功率和接收功率相差太大
    - 站点在发送时关闭接收功能，无法在发送时同时检测冲突
  - 在同一BSS中，不是所有站点都能互相感知到对方发送的信号
    - 载波侦听失败，但在接收站点处发生冲突
    - 被称为隐藏终端问题
  - 暴露终端问题，降低网络的吞吐量
  - 信号衰落随时间发生变化，使问题变得更加复杂

IEEE 802.11介质访问控制

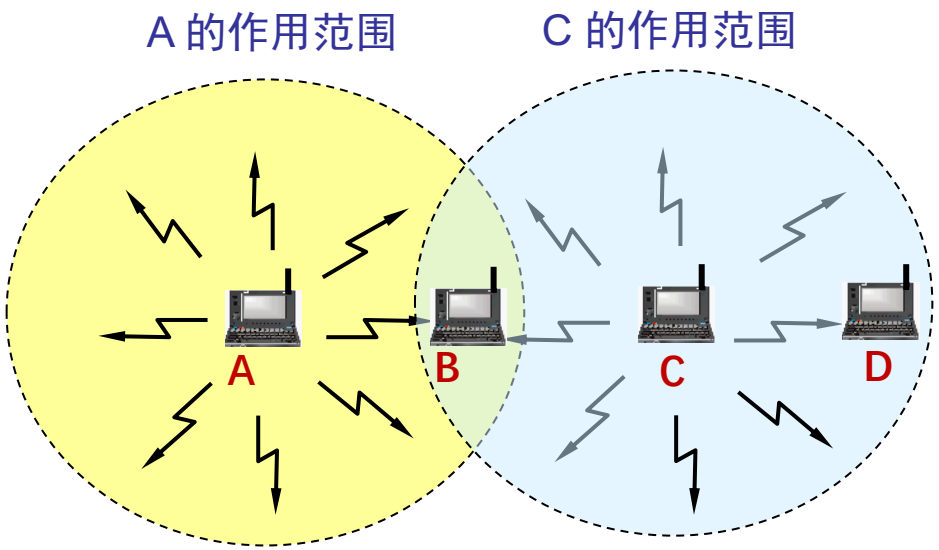
- 无线传输相关的“范围”
  - 传输范围(TX-Range)：成功接收帧的通信范围，取决于发送功率和无线电波传输特性
  - 物理层侦听范围（PCS-Range ）：检测到该传输的范围，取决于接收器的灵敏度和无线电波传输特性
  - 干扰范围（IF-Range ）：在此范围内的节点如果发送不相关的帧，将干扰接收端的接收并导致丢帧

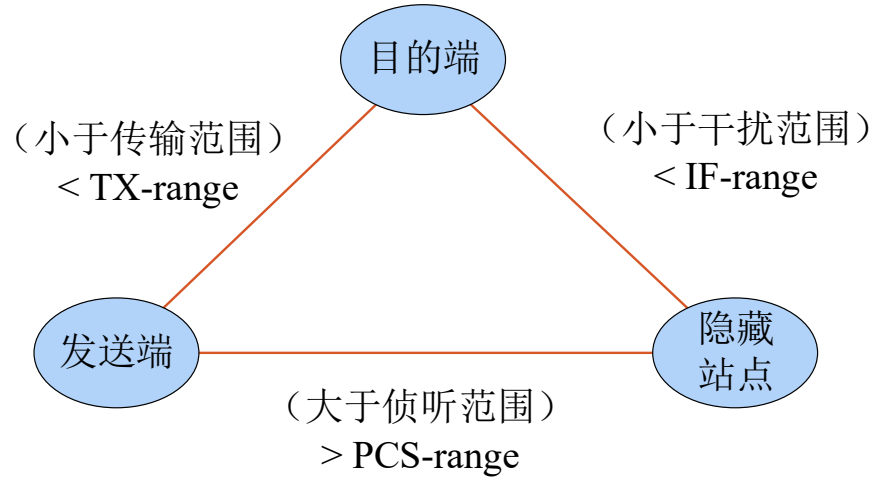


IEEE 802.11介质访问控制

➢ 隐藏终端问题

- 由于距离太远（或障碍物）导致站点无法检测到竞争对手的存在
- 隐藏站点不能侦听到发送端但能干扰接收端
- 假设：A正在向B传输数据，C也要向B发送数据

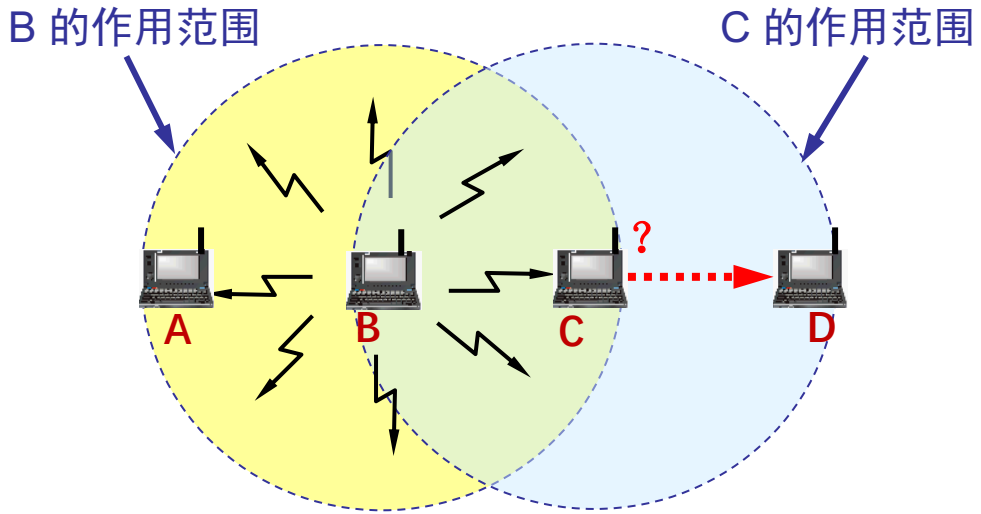


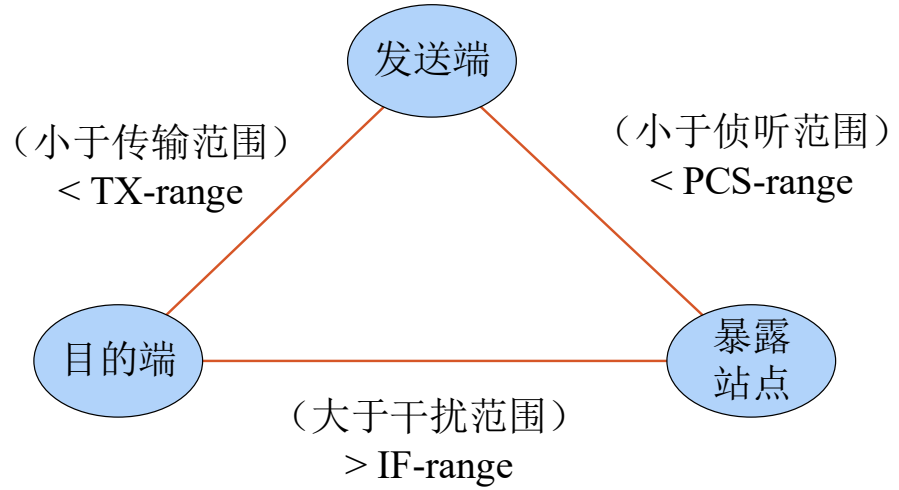


IEEE 802.11介质访问控制

➢ 暴露终端问题

- 由于侦听到其他站点的发送而误以为信道忙导致不能发送
- 暴露站点能侦听到发送端但不会干扰接收端
- 假设：B正在向A传输数据，C要向D发送数据





IEEE 802.11介质访问控制

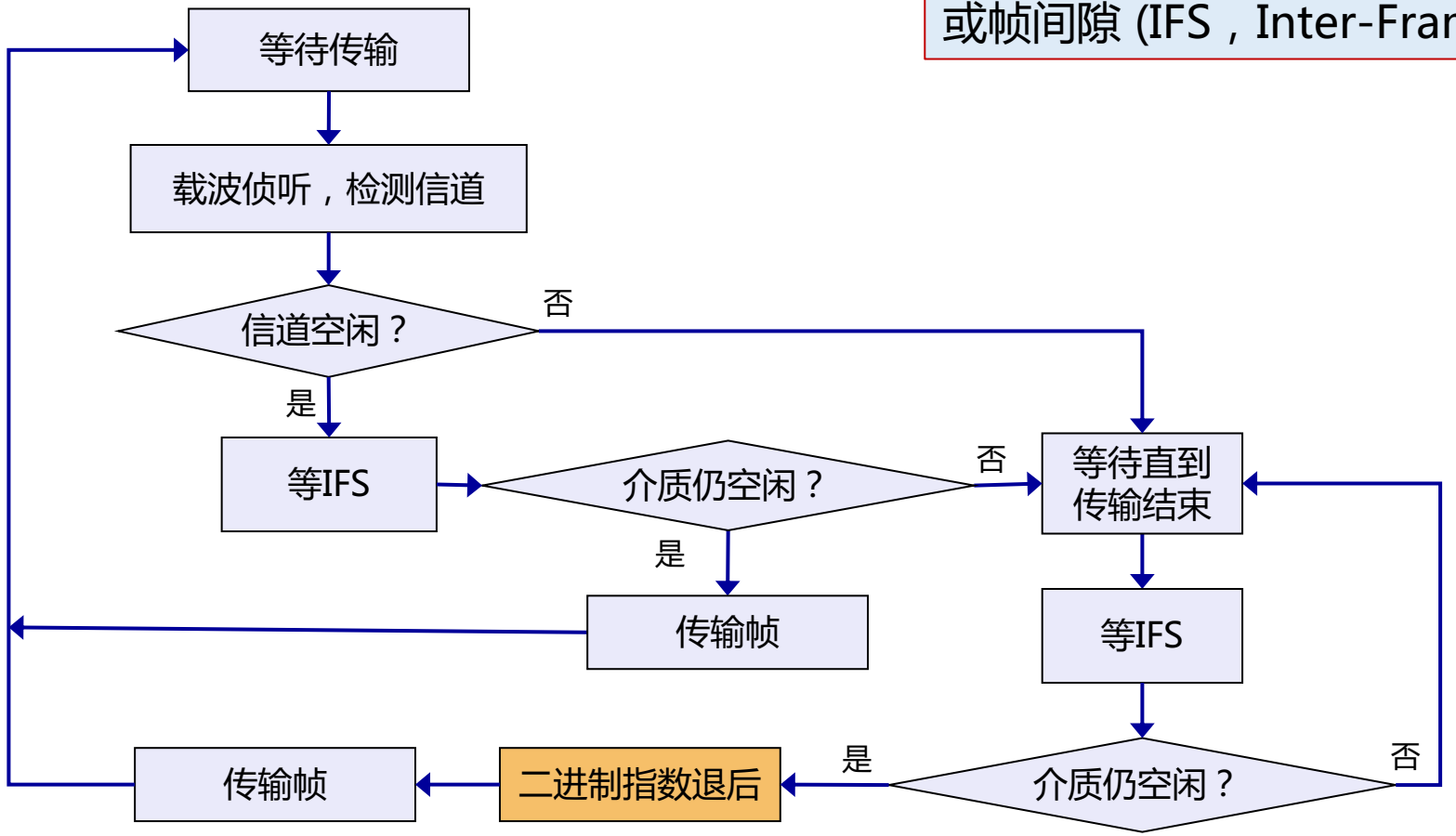
- CSMA/CA（Carrier Sense Multiple Access with Collision Avoid）
  - 当信道空闲时间大于IFS（帧间隙），立即传输
  - 当信道忙时，延迟直到当前传输结束+IFS时间
  - 开始随机退后过程
    - 从（0，CWindow）中选择一个随机数作为退后计数器（backoff counter）
    - 通过侦听确定每个时间槽是否活动
    - 如果没有活动，则减少退后时间
  - 退后过程中如果信道忙，则挂起退后过程（解决站点之间的公平问题）
  - 在当前帧传输结束后恢复退后过程

使用退后过程延迟发送的目的：避免多个站点同时传输引起的冲突

IEEE 802.11介质访问控制

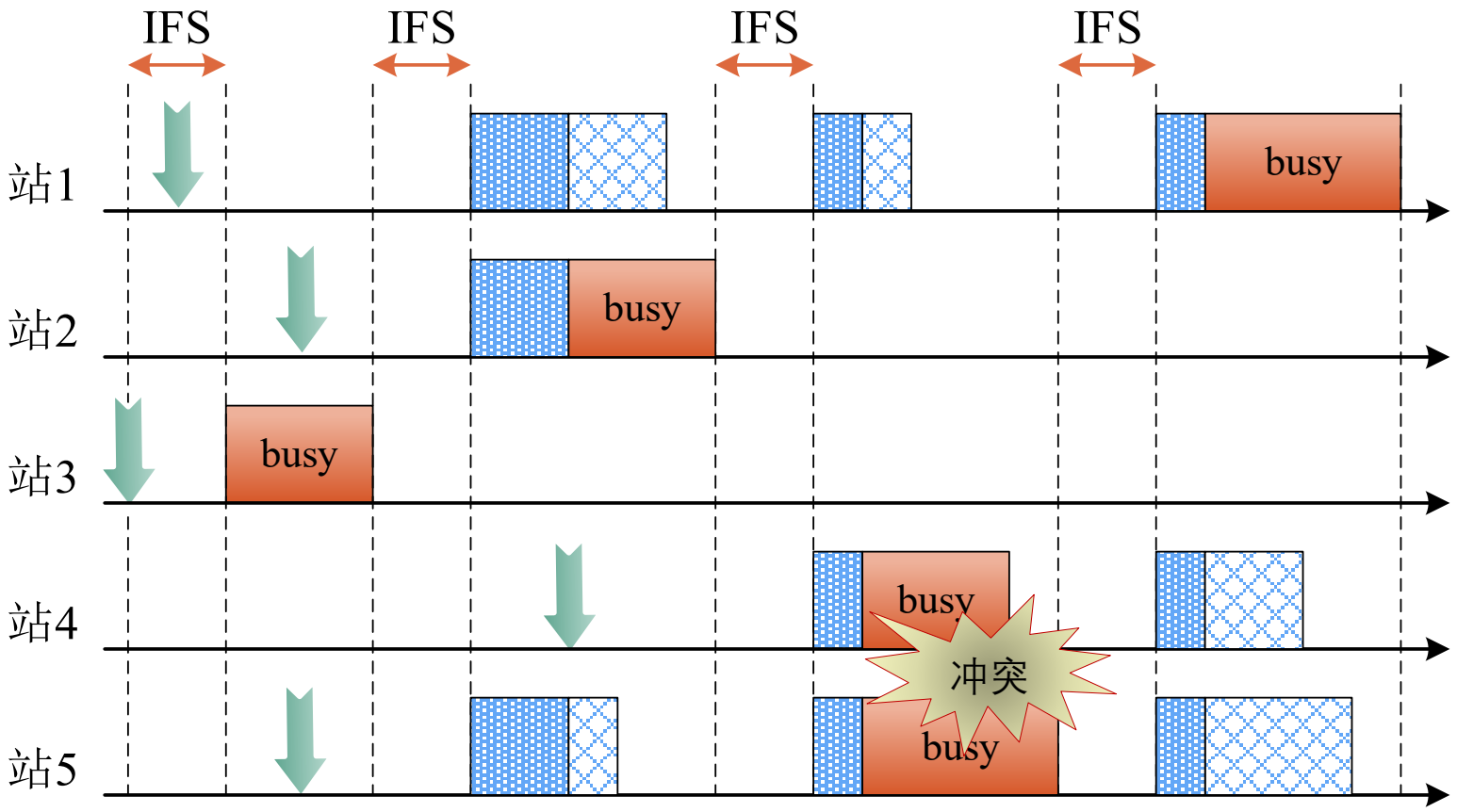
- CSMA/CA发送流程

所有站点完成发送后，必须等待一段很短的时间才能发送下一帧。这段时间通称为帧间间隔或帧间隙 (IFS，Inter-Frame Space)。



IEEE 802.11介质访问控制

- CSMA/CA示例

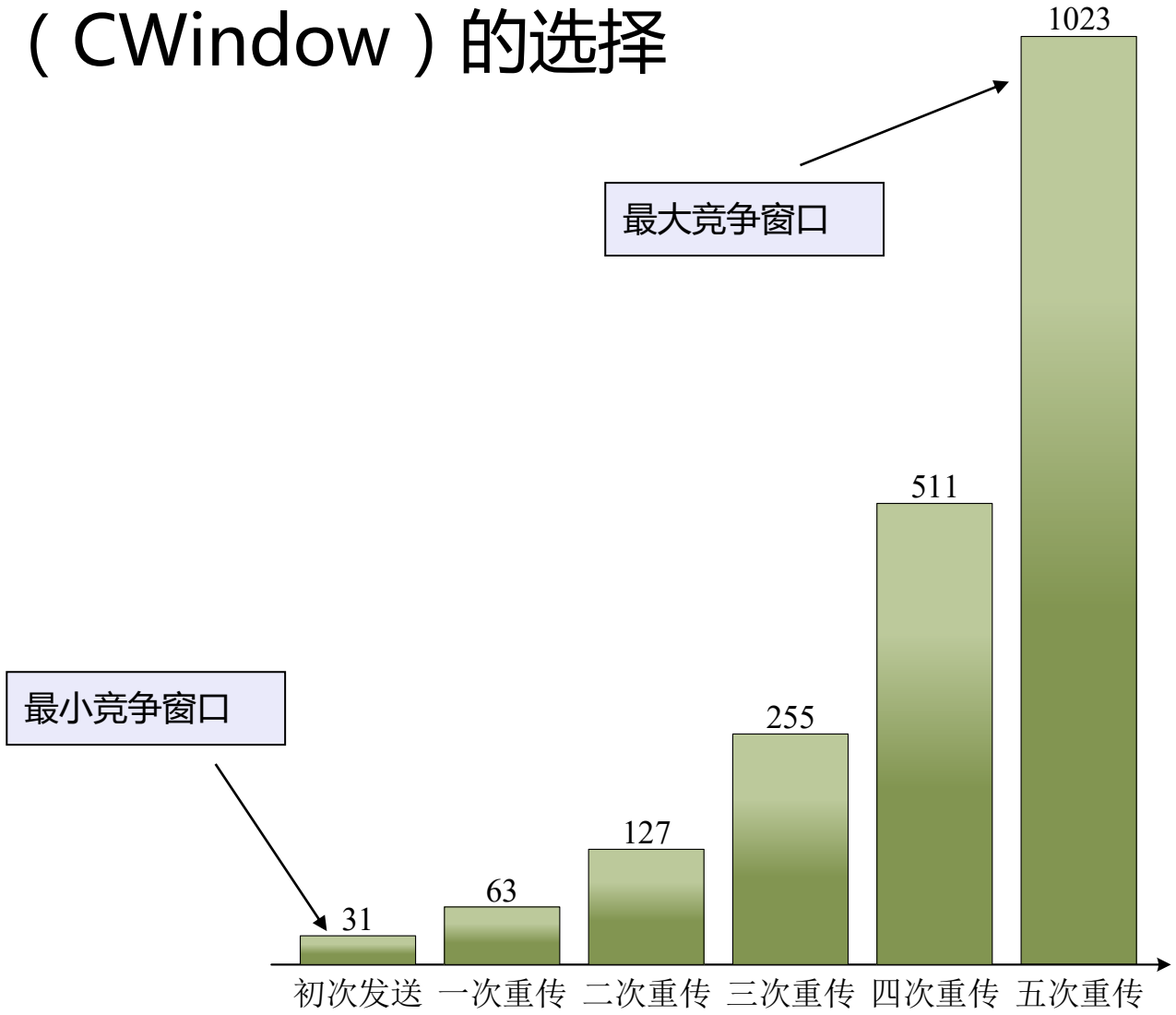


IEEE 802.11介质访问控制

- 竞争窗口（CWindow）的选择
  - 竞争窗口的选择应与网络负载情况相适应
  - 发生冲突的次数能间接反映网络的负载情况
    - 冲突次数越多，表明网络负载越重
  - 二进制指数退后算法
    - 竞争窗口的初始值为某个最小值，发生冲突时加大窗口，直到达到最大值。
  - 二进制指数退后算法对网络负载情况的自适应性
    - 当网络负载轻时，冲突的机率较小，选择较小的竞争窗口，减小站点的等待时间
    - 当网络负载重时，冲突的机率较大，选择较大的竞争窗口，避免站点间选择的随机值过于接近，从而导致太多的冲突

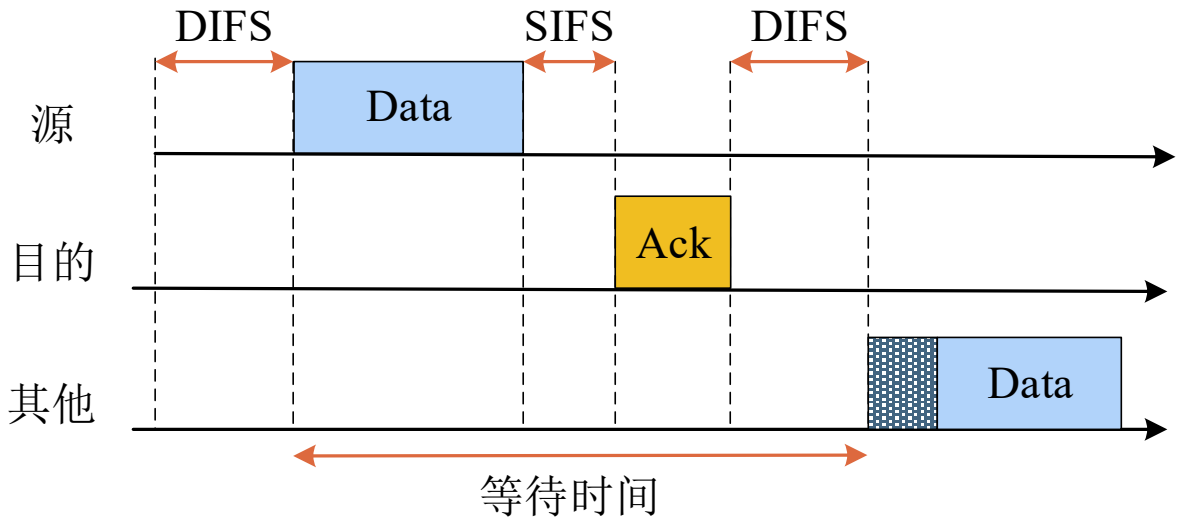
IEEE 802.11介质访问控制

- 竞争窗口（CWindow）的选择



IEEE 802.11介质访问控制

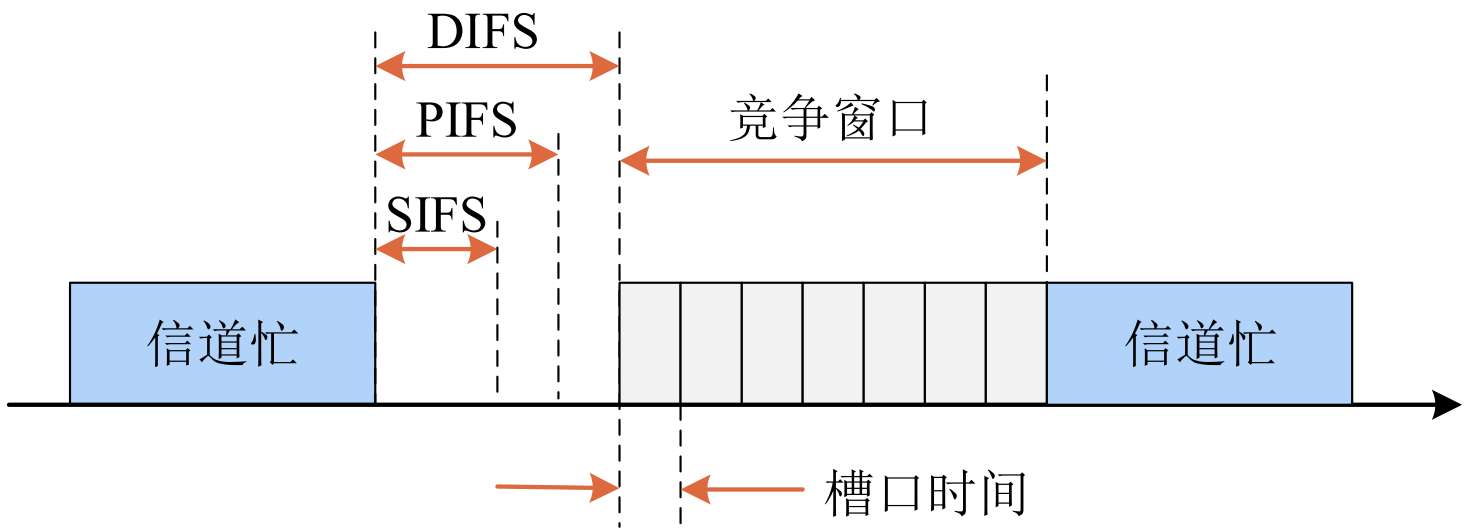
- 差错检测与确认重传
  - 差错检测：32位CRC校验（与以太网相同）
  - 采用停等机制：发送数据，等待确认，超时重传（重传定时器）
  - 如果达到最大重传限制，该帧被丢弃，并告知上层协议



思考：采用停等机制的原因？为什么不采用流水线机制？

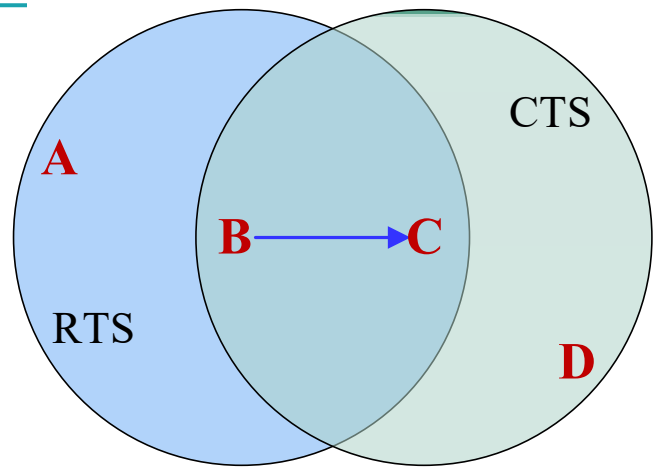
IEEE 802.11介质访问控制

- 不同帧间隙控制优先级
  - SIFS（Short IFS）：最高优先级，用于Ack, CTS, 轮询响应等
  - PIFS（PCF IFS）：中等优先级（SIFS+1槽口时间），轮询服务
  - DIFS（DCF IFS）：最低优先级（ SIFS+2槽口时间），异步数据服务



IEEE 802.11介质访问控制

- RTS-CTS机制（可选机制）
  - 目的：通过信道预约，避免长帧冲突
  - 发送端发送RTS（request to send）
  - 接收端回送CTS（clear to send）
  - RTS和CTS中的持续时间（Duration）中指明传输所需时间（数据+控制）
  - 其他相关站点能够收到RTS或（和）CTS，维护NAV
    - 虚拟载波侦听（Virtual Carrier Sense）
  - RTS和CTS帧很短，即使产生冲突，信道浪费较少

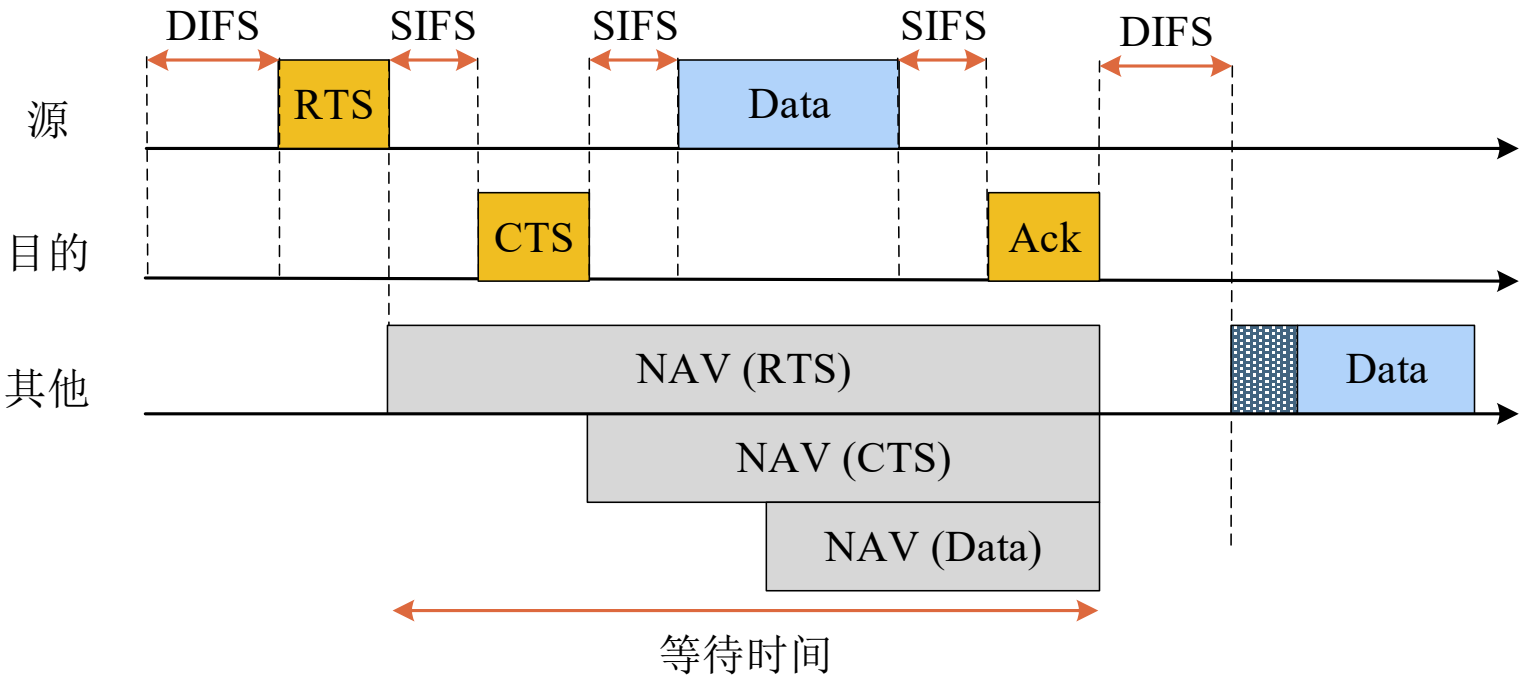


NAV（Network Allocation Vector ）

IEEE 802.11介质访问控制

➢ RTS-CTS机制示例

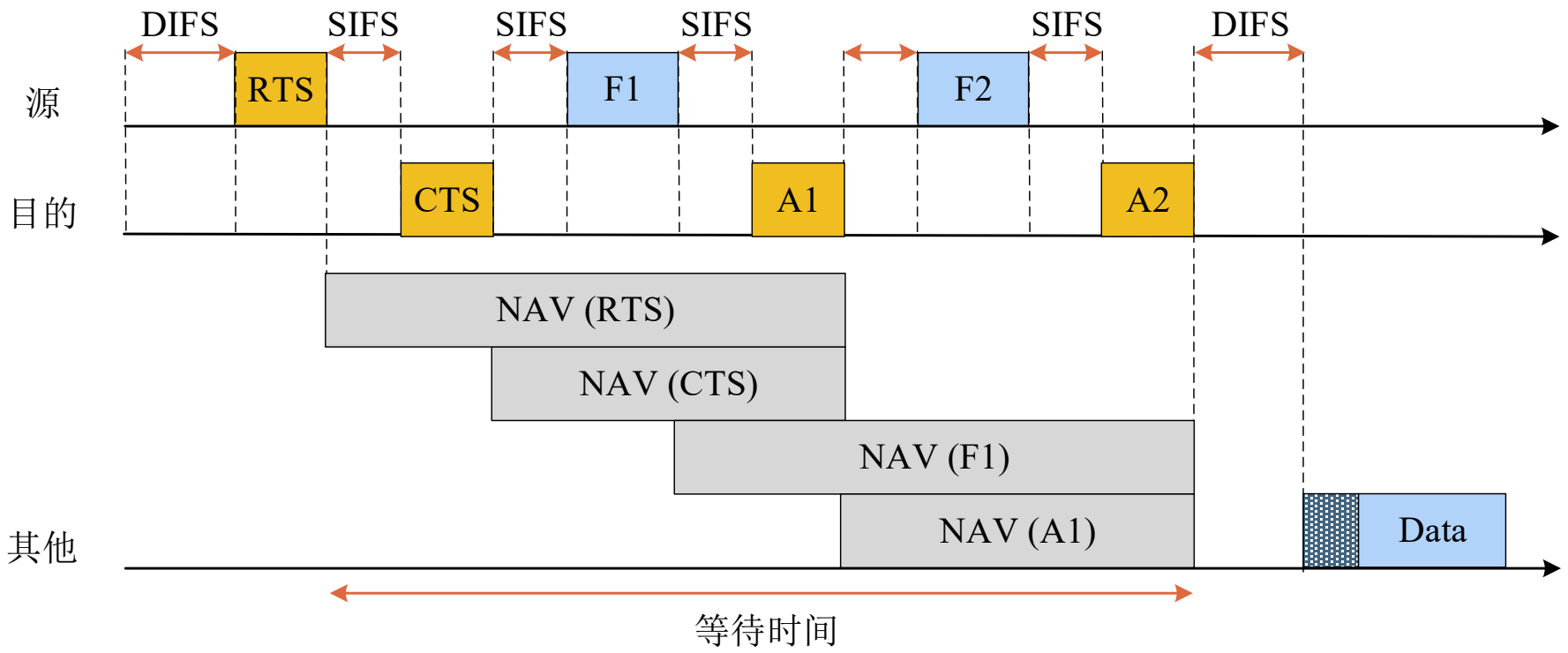
- 源站点的隐藏站点可以接收到目的站点发送的CTS



NAV（Network Allocation Vector ）

IEEE 802.11介质访问控制

- 如何应对无线链路较高的出错率？
  - 解决方法：采用较小的帧（将用户数据帧分段的机制对用户透明）
  - F_i帧中携带F_{i+1}的传输时间



IEEE 802.11介质访问控制

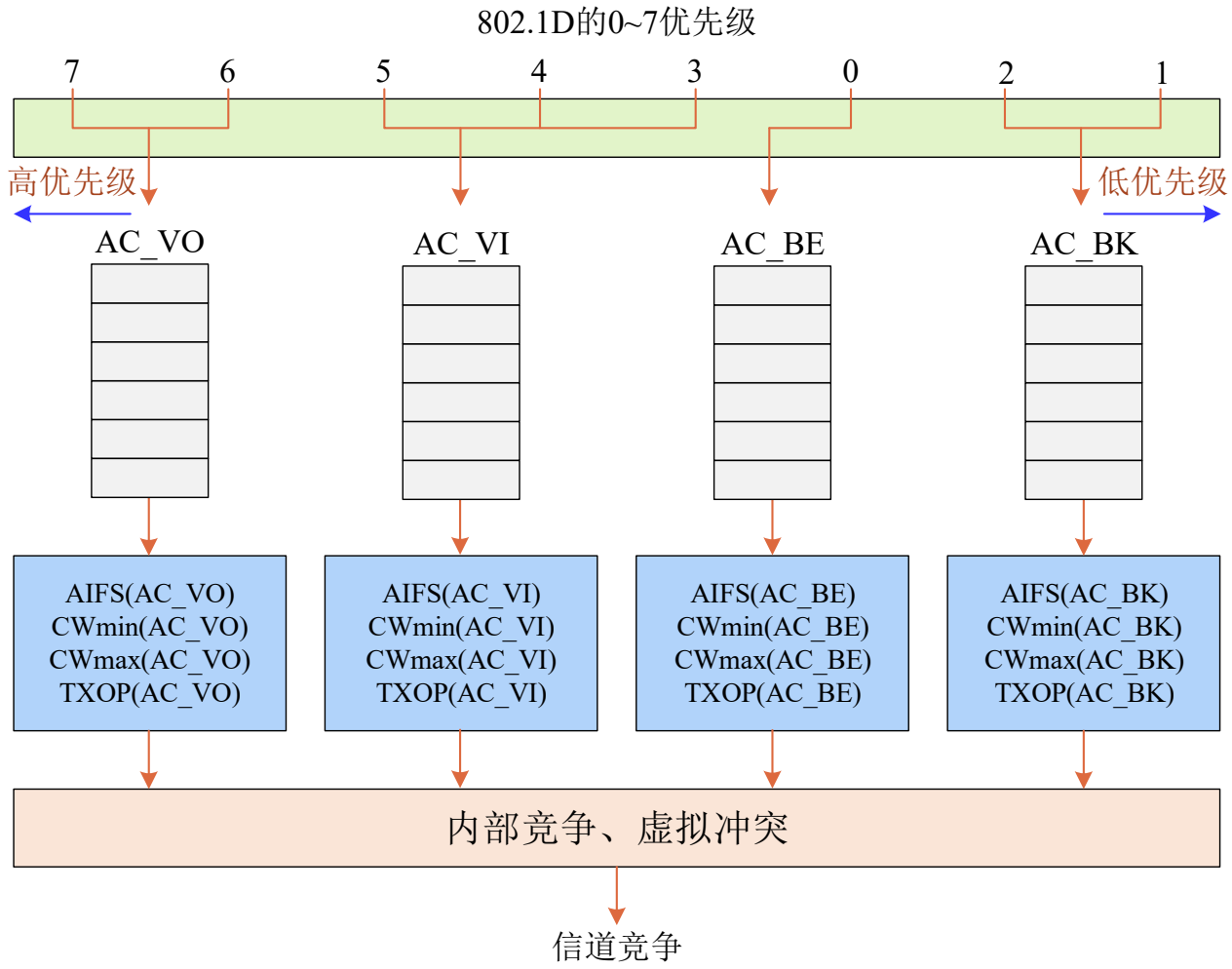
- EDCA（Enhanced Distributed Channel Access）（802.11e）
  - **目标：**针对不同的应用提供不同的优先级，保证QoS
  - 单发送队列 → 多发送队列（AC，Access Category）
    - AC3: 语音（Voice traffic）
    - AC2: 视频（Video traffic）
    - AC1: 尽力而为数据流（Best effort traffic）
    - AC0: 背景流（Background traffic）
  - 每个队列基于下面四种参数独立竞争
    - Cwmin：最小竞争窗口，越小的Cwmin其优先级越高
    - Cwmax：最大竞争窗口，越小的Cwmax其优先级越高
    - TXOP：传输机会，参数值为TXOPlimit，代表占用信道最长时间
    - AIFS：要获得传输机会时，必须等待的信道空闲时间

AIFS：Arbitration Interframe Space
TXOP：Transmission Opportunity

Wi-Fi联盟定义：WMM（Wireless Multimedia Enhancements）

IEEE 802.11介质访问控制

- EDCA多队列机制



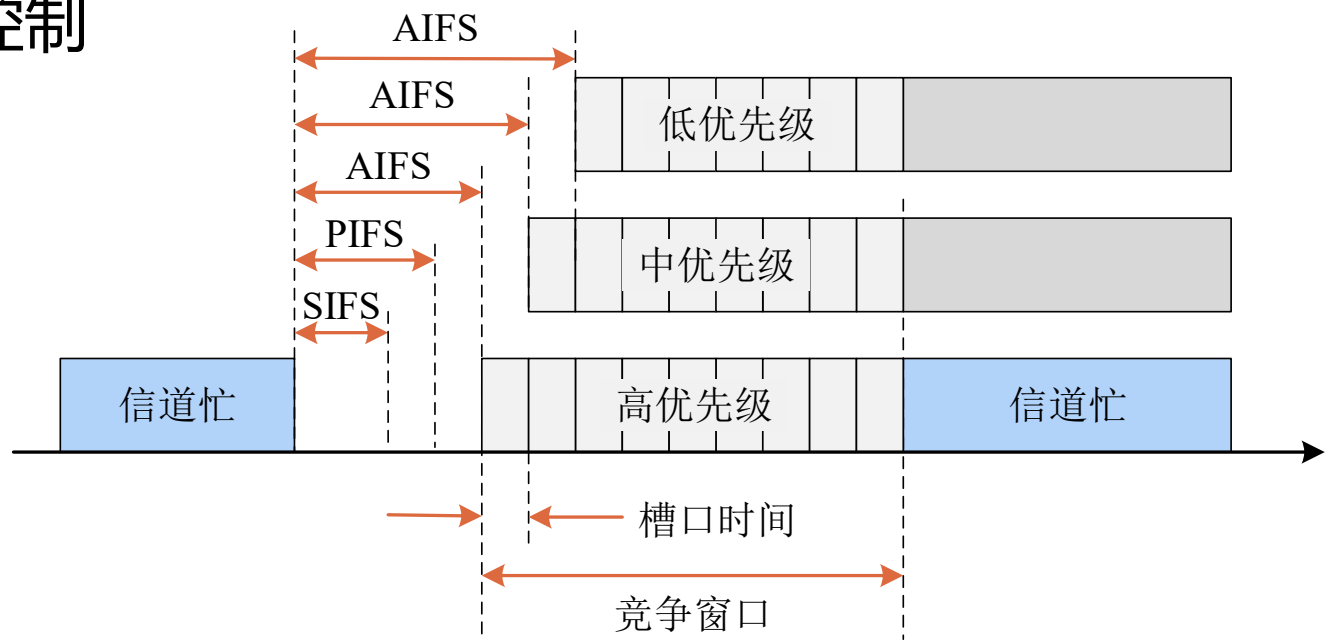
IEEE 802.11介质访问控制

- 队列参数设置（QSTA）
  - 退后随机数选取
    - 从[1, *CW(AC)+1*]中选取一个随机数
  - AIFS计算方法：
    - $AIFS(AC) = AIFSN(AC) \times aSlotTime + SIFS$

AC	CW_{min}	CW_{max}	AIFSN	TXOP Limit（802.11b）	TXOP Limit（802.11a/g）
AC_BK	aCW_{min}	aCW_{max}	7	0	0
AC_BE	aCW_{min}	aCW_{max}	3	0	0
AC_VI	（aCW_{min}+1）/2-1	aCW_{min}	2	6.016ms	3.008ms
AC_VO	（aCW_{min}+1）/4-1	（aCW_{min}+1）/2-1	2	3.264ms	1.504ms

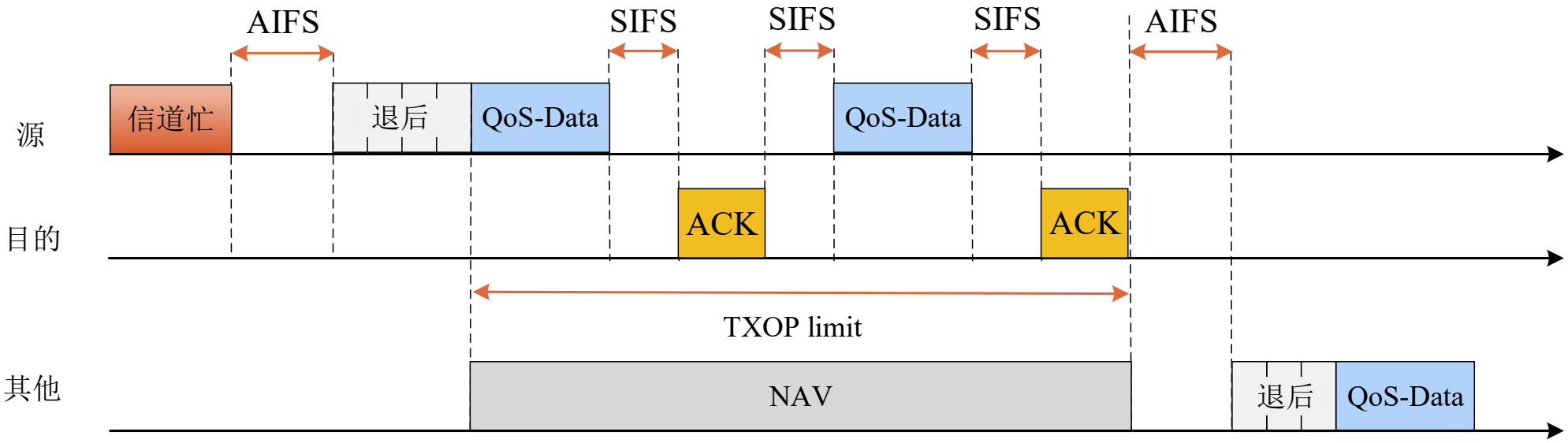
QSTA：支持802.11e的站点

- 队列优先级控制



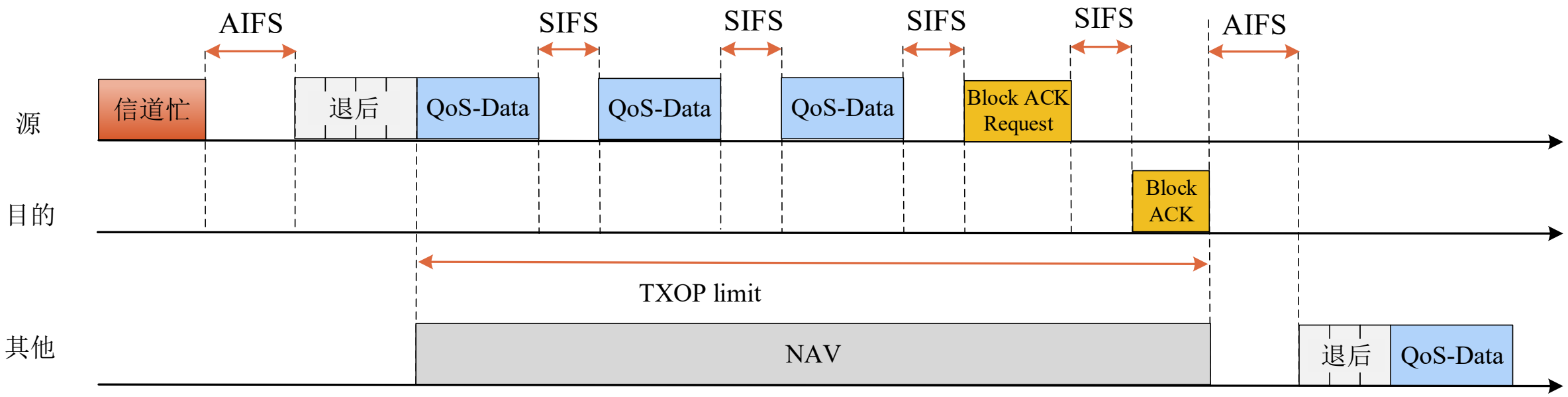
IEEE 802.11介质访问控制

- QoS数据传输（QSTA）
  - QSTA在获得使用权后，在TXOP Limit时间内可以发送多个数据帧
    - AC队列要相同，目的地址可以不同
  - TXOP内首发帧需要预约整个TXOP Limit内帧传输的所有时间，以便其他STA进行虚拟侦听



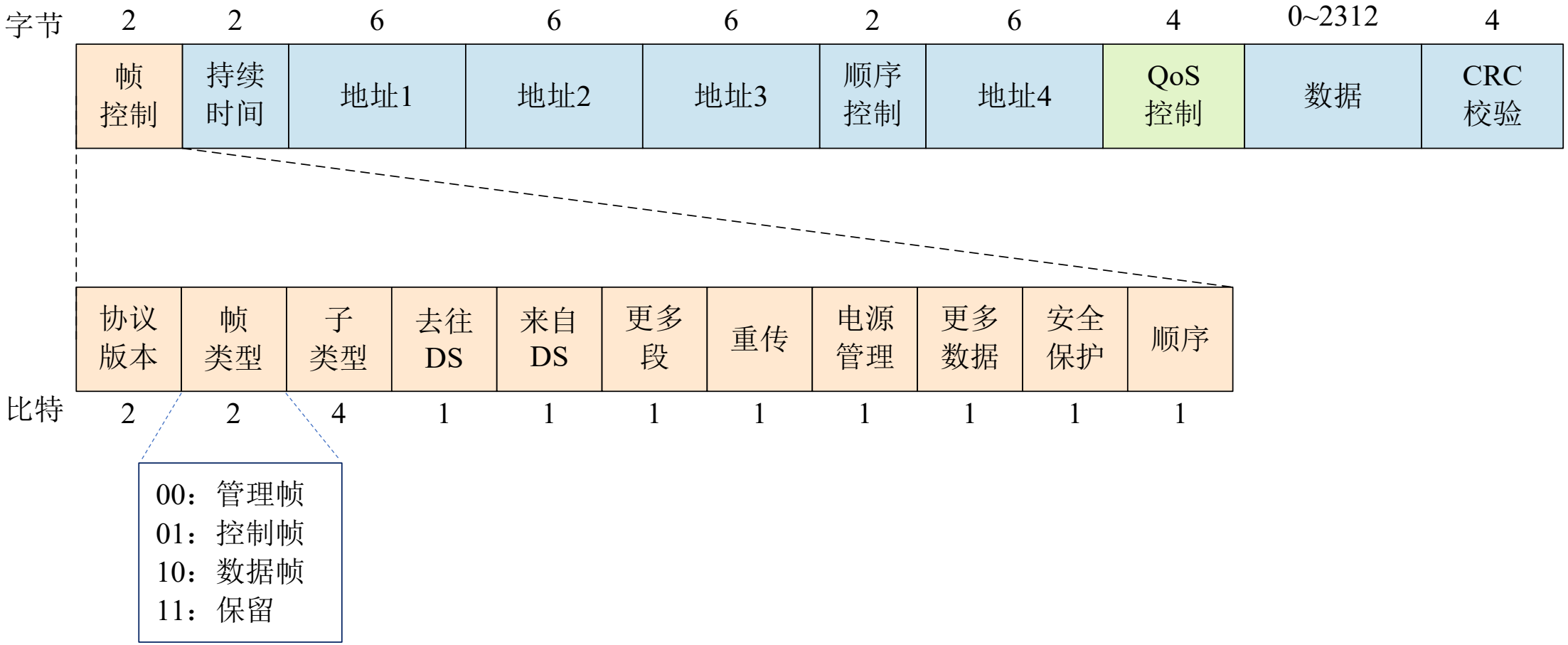
IEEE 802.11介质访问控制

- QoS数据传输（QSTA）
  - 目的相同时，可以使用Block ACK对多帧进行一次确认



IEEE 802.11帧格式

- 802.11帧格式一般结构



IEEE 802.11帧格式

➢ 主要域段解释

- 帧控制：具有多种用途
- 持续时间：下一个要发送帧可能持续的时间（NAV）或关联ID（AID）
- 地址1~地址4：每个地址的含义基于“去往DS”和“来自DS”域段确定
- 顺序控制：过滤掉重复帧，或用于分片组合
- QoS控制域段：存放数据流的QoS信息（802.11e中扩展）
- 数据：包含任意长度的数据（0-2312字节）
- CRC校验：802.11采用4个字节的校验码

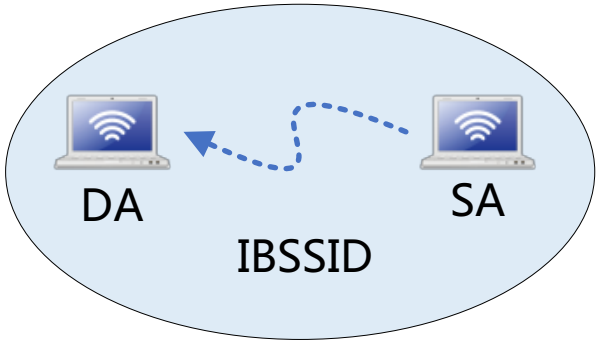
IEEE 802.11帧格式

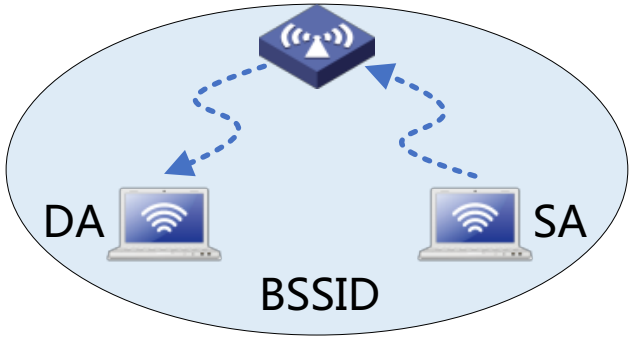
- 帧控制域段解释
  - 协议版本：通常为0
  - 类型和子类型：如果子类型的最后一位设置为1，表示是QoS数据帧
  - 更多段：用于长帧被分段的情况，1表示不是最后一段
  - 重传：表明当前帧是以前帧的重传
  - 电源管理：1表示节能模式；0表示活跃状态
  - 更多数据：指明有更多的数据要发送（缓存）
  - 安全保护：1表明采用802.11标准的安全机制，对数据进行保护
  - 顺序：1指示接收者必须严格按照顺序处理

IEEE 802.11帧格式

- 地址域段的使用

BSSID：基本服务集标识符，为AP的MAC地址





说明	去往DS	来自DS	地址1（物理接收者）	地址2（物理发送者）	地址3（逻辑发送者）	地址4（逻辑接收者）
自组织模式	0	0	DA	SA	IBSSID	—
接收自AP	0	1	DA	BSSID	SA	—
发送至AP	1	0	BSSID	SA	—	
AP到AP	1	1	接收AP	发送AP	SA	DA

IEEE 802.11帧格式

- 主要管理帧

帧控制	持续时间	地址1	地址2	BSSID	顺序控制	数据	CRC校验

类型	子类型	名称
00	0000	关联请求（Association Request）
00	0001	关联响应（Association Response）
00	0010	重新关联请求（Reassociation Request）
00	0011	重新关联响应（Reassociation Response）
00	0100	探测请求（Probe Request）
00	0101	探测响应（Probe Response）
00	1000	信标帧（Beacon）
00	1001	通知传输指示消息（ATIM）
00	1010	解除关联（Disassociation）
00	1011	认证（Authentication）
00	1100	解除认证（Deauthentication）

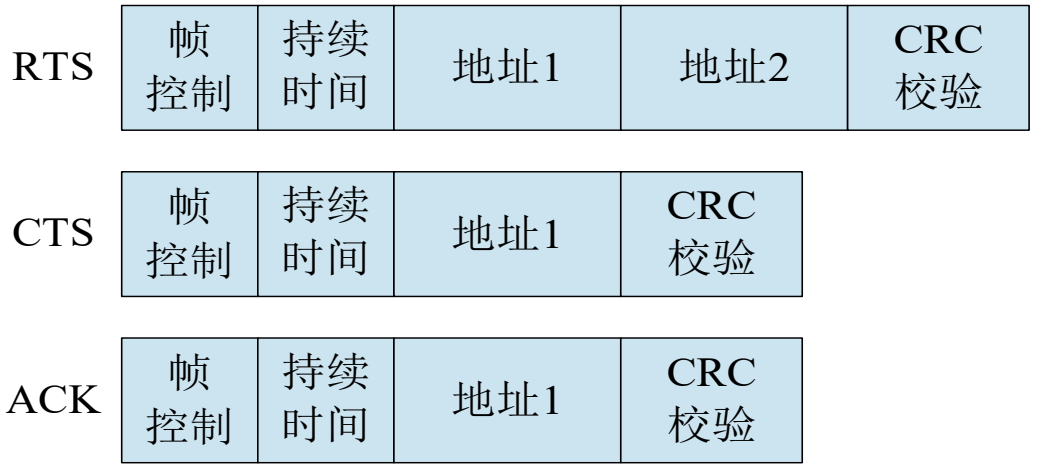
IEEE 802.11帧格式

可以使用Wireshark捕获802.11帧，分析帧结构和包含的内容。例如Beacon帧的结构，包含的BSSID、SSID等

```
▸ Frame 13063: 265 bytes on wire (2120 bits), 265 bytes captured (2120 bits) on interface 0
▸ Radiotap Header v0, Length 54
▸ 802.11 radio information
▾ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  ▾ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: HuaweiTe_1e:8c:70 (d4:94:e8:1e:8c:70)
    Source address: HuaweiTe_1e:8c:70 (d4:94:e8:1e:8c:70)
    BSS Id: HuaweiTe_1e:8c:70 (d4:94:e8:1e:8c:70)
    .... .... .... 0000 = Fragment number: 0
    0011 1101 0101 .... = Sequence number: 981
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 0x0000012dfa87e03b
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x1501
  ▾ Tagged parameters (175 bytes)
    ▸ Tag: SSID parameter set: NKU_WLAN
    ▸ Tag: Supported Rates 12(B), 18, 24(B), 36(B), 48, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 60
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
```

IEEE 802.11帧格式

- 主要控制帧



类型	子类型	名称
01	1010	PS-Poll
01	1011	RTS
01	1100	CTS
01	1101	确认帧（ACK）
01	1000	块确认请求帧（Block ACK Request）
01	1001	块确认帧（Block ACK）

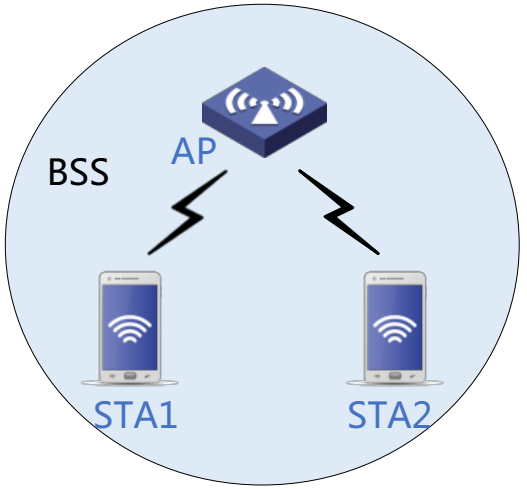
IEEE 802.11帧格式

- 主要数据帧

类型	子类型	名称
10	0000	数据帧（Data）
10	0100	无数据帧（Null）
10	1000	QoS数据帧（QoS-Data）
10	1100	QoS无数据帧（QoS Null）

无线局域网的构建与管理

➢ 基础架构模式



- 通过AP接入有线网络（互联网络）
- 关键：如何关联到AP？
  - BSSID：AP的MAC地址，标识AP管理的基本服务集
  - SSID：32字节网名，标识一个扩展服务集（ESS），包含一个或多个基本服务集
  - 关联到AP的三个阶段
    - 扫描（Scan）、认证（Authentication）、关联（Association）

BSSID: Basic Service Set Identifier
SSID: Service Set Identifier

胖AP: Fat AP，功能全面
瘦AP: Fit AP，配合无线交换机组网

无线局域网的构建与管理

- 被动扫描
  - AP周期性发送Beacon帧，站点在每个可用的通道上扫描Beacon帧
  - Beacon帧提供的AP相关信息包括：
    - Timestamp, Beacon Interval (eg.100ms), Capabilities, SSID, Supported Rates, parameters
    - Traffic Indication Map（TIM）

无线局域网的构建与管理

- 主动扫描
  - 站点依次在每个可用的通道上发出包含SSID的Probe Request 帧，具有被请求SSID的AP返回Probe Response帧
  - Probe Response帧包含AP相关信息：
    - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters

无线局域网的构建与管理

- 认证过程
  - 当站点找到与其有相同 SSID 的 AP，在 SSID 匹配的 AP 中，根据收到的 AP 信号强度，选择一个信号最强的 AP，然后进入认证阶段
  - 主要认证方式包括：
    - 开放系统身份认证 (open-system authentication)
    - 共享密钥认证 (shared-key authentication)
    - WPA PSK认证（pre-shared key）
    - 802.1X EAP认证

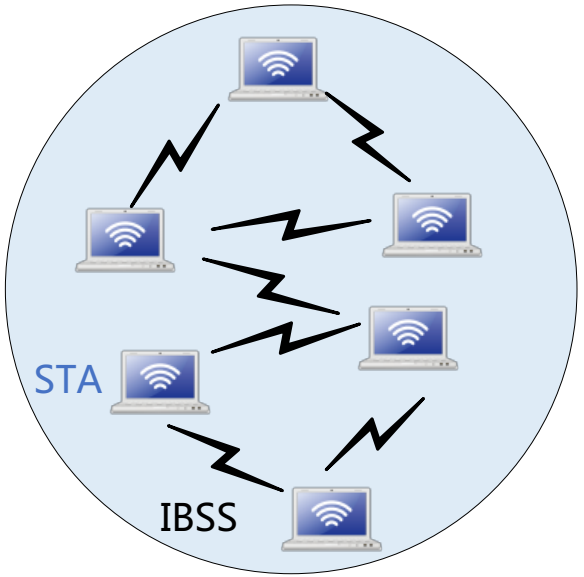
无线局域网的构建与管理

- 关联过程
  - 身份认证获得通过后， 进入关联阶段
  - 站点向 AP 发送关联请求（Association Request）
    - 包含：Capability, Listen Interval, SSID, Supported Rates
  - AP 向站点返回关联响应（Association Response）
    - 包含：Capability, Status Code, Station ID, Supported Rates
  - AP维护站点关联表，并记录站点的能力（如能够支持的速率等）

无线局域网的构建与管理

➢ 自组织模式

- 站点先寻找具有指定SSID的IBSS是否已存在。如果存在，则加入；若不存在，则自己创建一个IBSS，发出Beacon，等其他站来加入
- IBSS中的所有站点参与Beacon发送（保证健壮性），每个站点在Beacon窗口竞争Beacon的产生。对于每个站点：
  - 确定一个随机数k
  - 等待k个时间槽
  - 如果没有其他站点发送Beacon，则开始发送Beacon

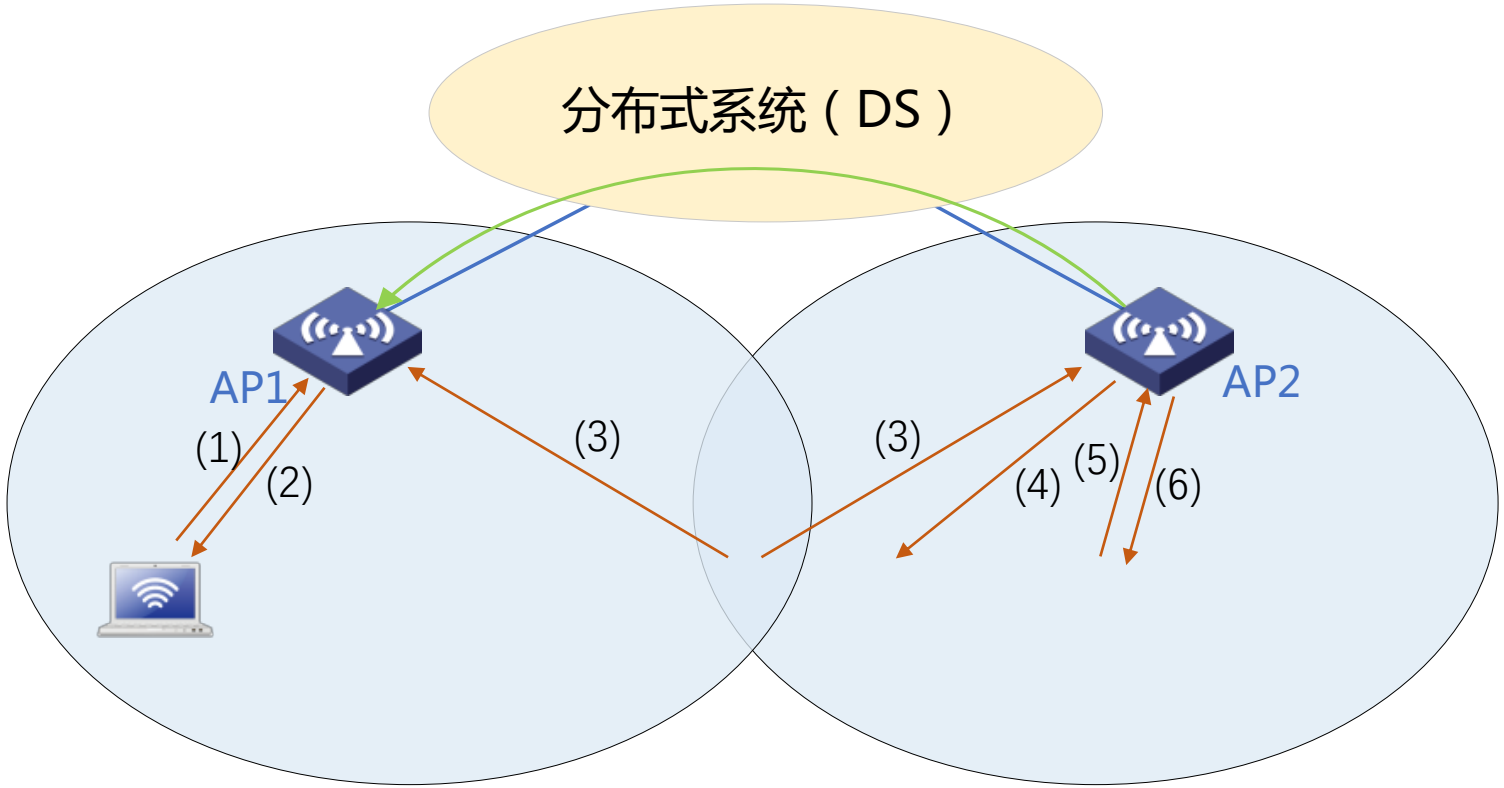


无线局域网的构建与管理

- 站点漫游
  - 当前的AP的通道质量下降时，站点漫游到不同的AP
  - 通过扫描功能发现通道质量更好的AP
    - 被动扫描
    - 主动扫描
  - 站点向新的AP发送重关联请求（Reassociation Request）
  - 如果AP接受重关联请求
    - AP 向站点返回重关联响应（Reassociation Response）
    - 如果重关联成功，则站点漫游到新的AP
    - 新的AP通过分布系统通知之前的AP

无线局域网的构建与管理

- 站点漫游示例



(1) 关联请求
(2) 关联响应
(3) 探测请求
(4) 探测响应
(5) 重关联请求
(6) 重关联响应

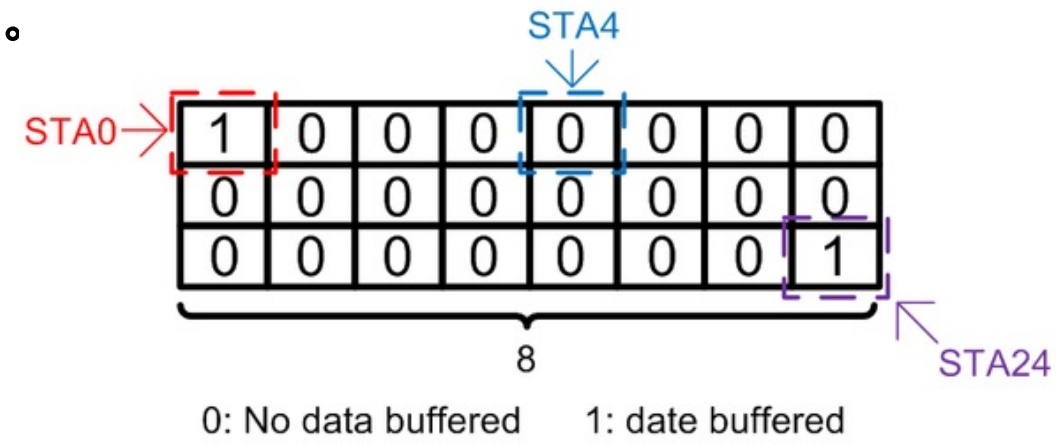
无线局域网的构建与管理

- 站点睡眠管理
  - 目的：延长电池的续航时间
  - 基本思想：
    - 无线网卡的空闲接收状态占电量消耗的主要部分，关闭无线网卡可以减少电量的消耗
    - 关联的AP允许空闲站睡眠，AP跟踪睡眠的站点，并为之缓存数据，保证数据不丢失，保证会话的持续性
    - Beacons 中的TIM（Traffic Indication Map）通知睡眠站点有需要接收的数据
    - 睡眠站点定期唤醒接收数据：如果有数据要接收，发送PS-Poll帧，请求AP发送数据帧

无线局域网的构建与管理

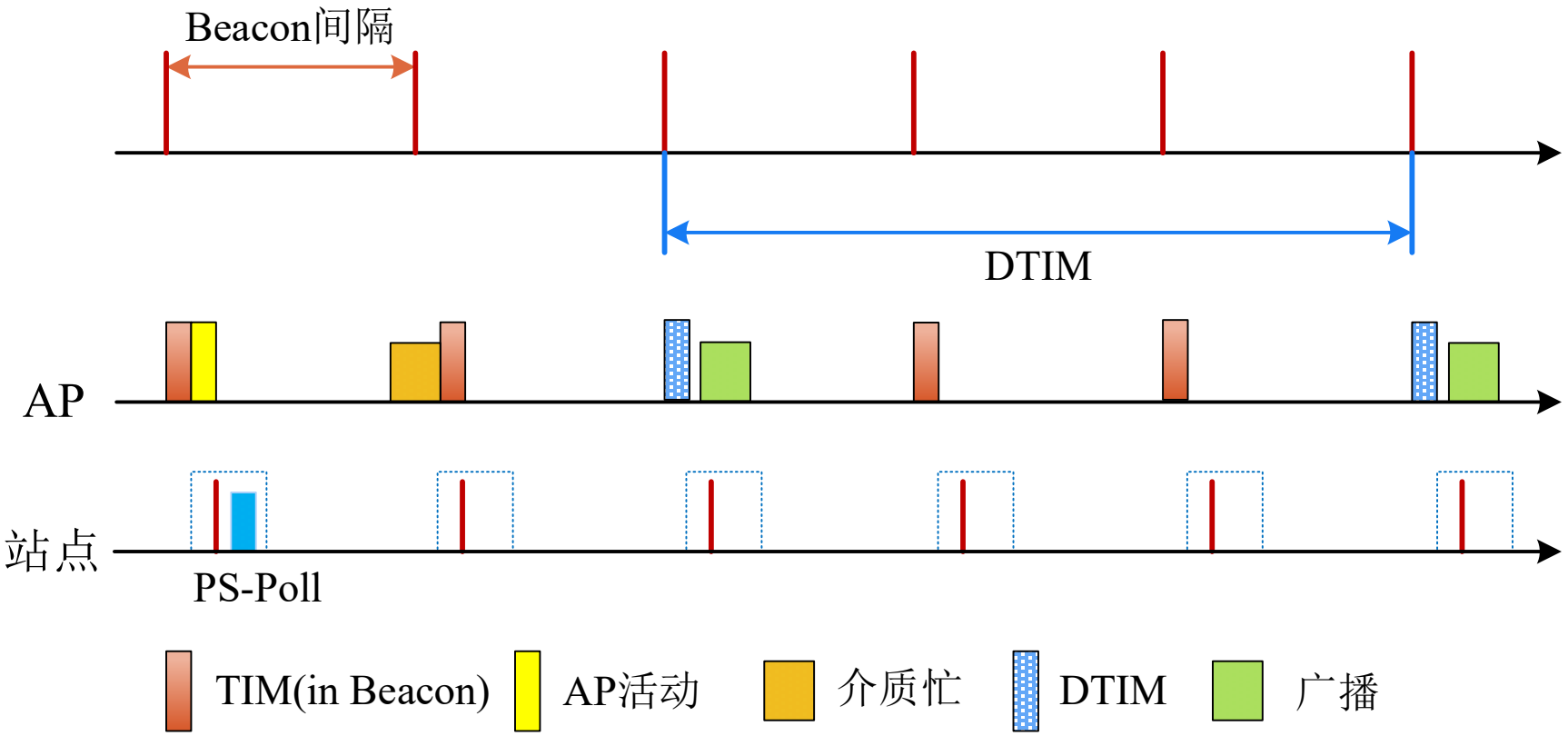
➢ 站点睡眠管理（续）

- 关联ID (Association Identifier，AID)：AP中保留AID表，每个AID与对应的站点MAC地址进行绑定。
- AID的范围为0~2007，每个AP最多可以关联2007个节点。
- AID=0的位置为保留字段，不分配给节点，用以代表所有的组播和广播
- AID的分配：当一个站点向AP发起关联请求后，AP会反馈关联响应帧，AID在这个过程中被分配，并告知站点。



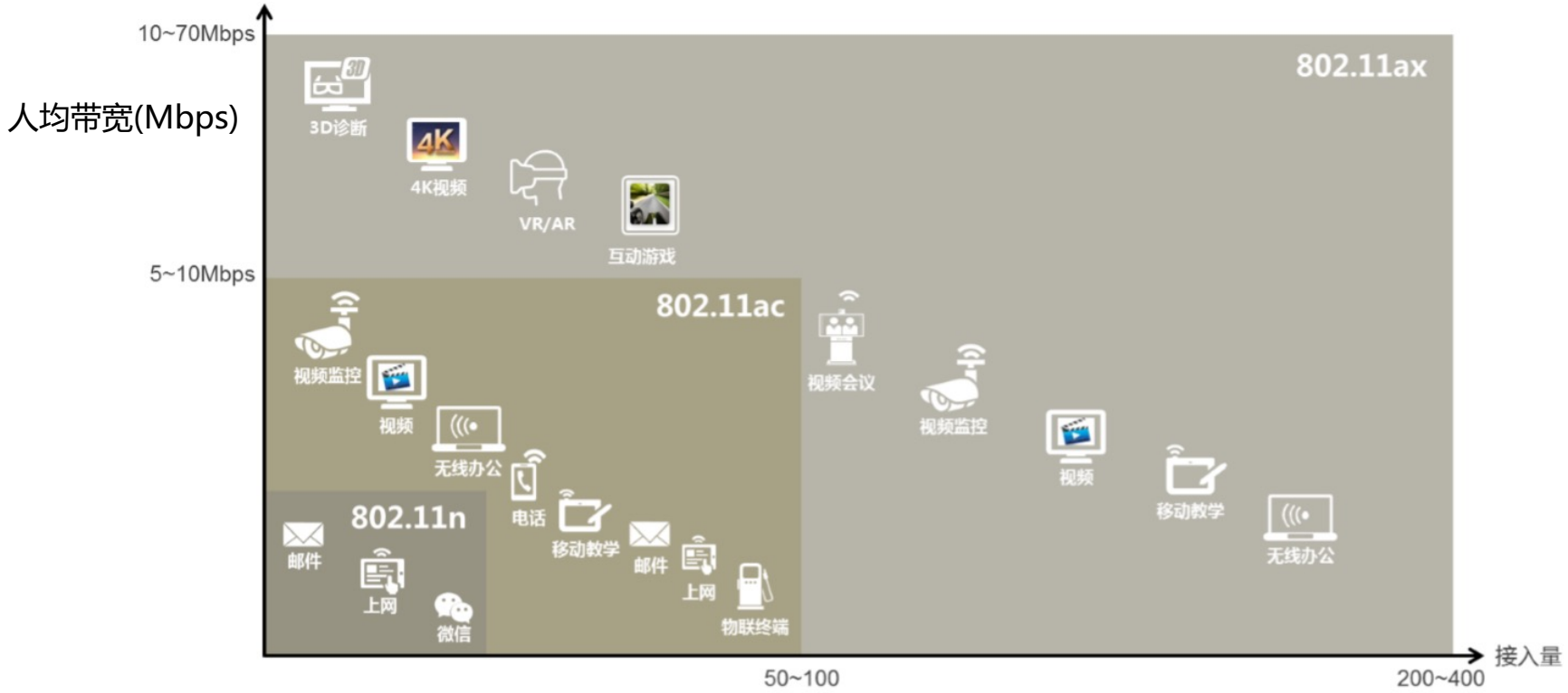
无线局域网的构建与管理

- 站点睡眠管理（示例）



Wi-Fi 6 核心技术概览

- Wi-Fi 6 (802.11ax) 核心目标：解决网络容量和传输效率问题、降低传输时延，相对于 Wi-Fi 5，在高密部署场景中将用户平均吞吐量提升4倍以上，并发用户数提升3倍以上



Wi-Fi 6 核心技术概览

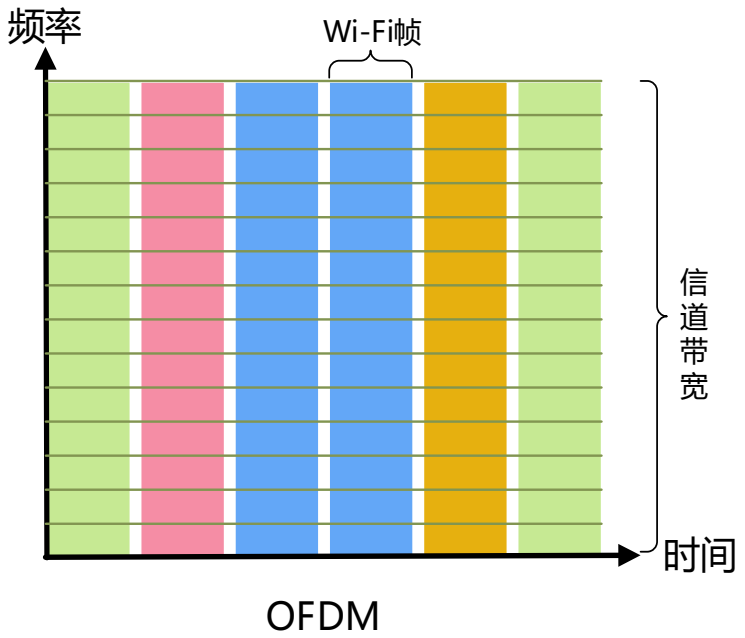
- **Wi-Fi 6核心技术：**相对于Wi-Fi 5， Wi-Fi 6采用了如下新技术
  - OFDMA频分复用技术：实现多站点并行传输，提升效率、降低时延
  - DL/UL MU-MIMO技术：增加系统容量，提升用户的平均吞吐量
  - 高阶调制技术 (1024-QAM)：提高单条空间流的传输速率，相对256-QAM提升25%
  - BSS 着色机制：信道合理划分和利用，提升高密部署环境无线网络的总体容量
  - 扩展覆盖范围：采用Long OFDM symbol发送机制，降低终端丢包率，扩大覆盖范围

Wi-Fi 6 核心技术概览

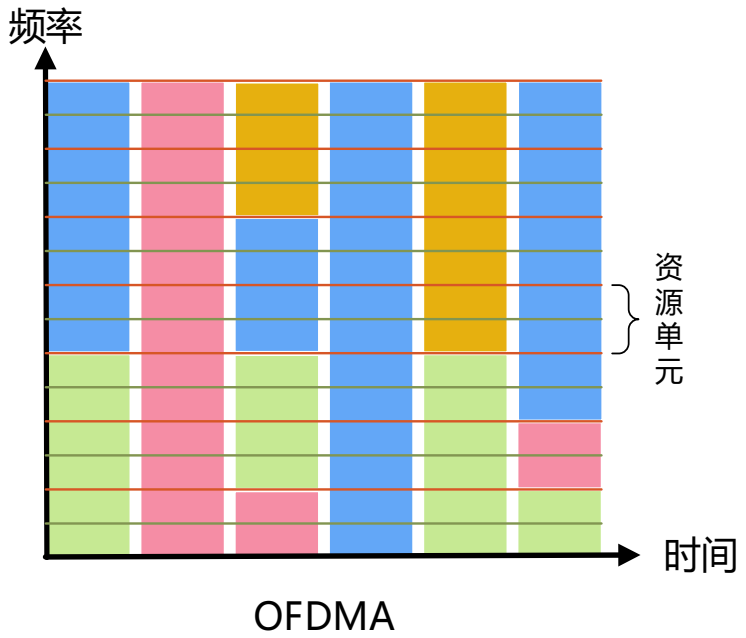
OFDMA: Orthogonal Frequency Division Multiple Access

- OFDMA 频分复用技术
  - OFDM：每个时间片，一个用户占据整个信道的所有子载波，并且发送一个完整的数据包
  - OFDMA：整个信道资源被分成固定大小的时频资源块（Resource Unit, RU)，每个RU至少包含26个子载波，用户的数据承载在RU上。每个时间片上，可以有多个用户同时发送数据

优势：
- 更细的信道资源分配
- 提供更好的QoS
- 更多的用户并发
- 更高的用户带宽



OFDM

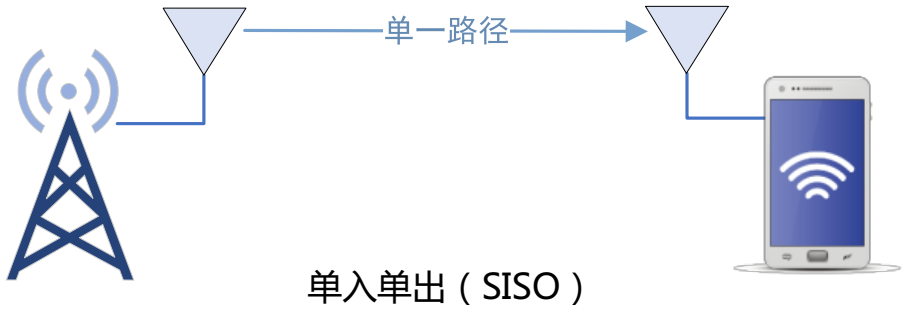


OFDMA

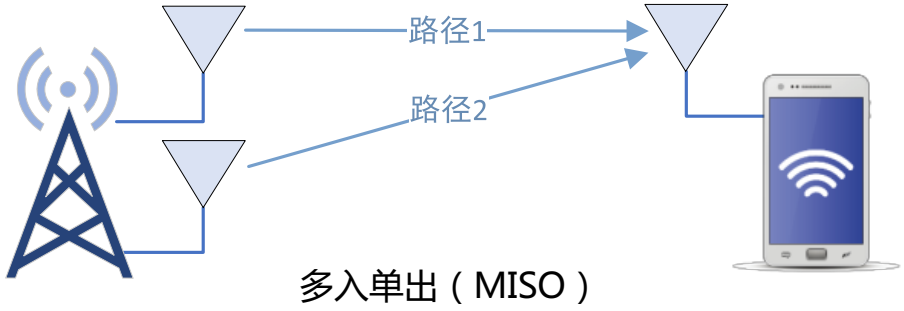
Wi-Fi 6 核心技术概览

➢ DL/UL MU-MIMO技术

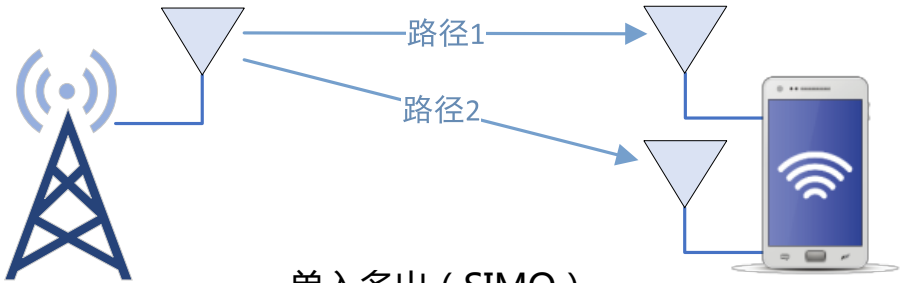
- 理解什么是MIMO



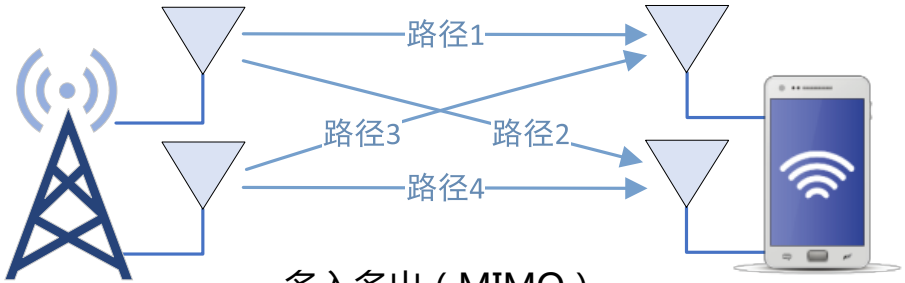
单入单出（SISO）



多入单出（MISO）



单入多出（SIMO）



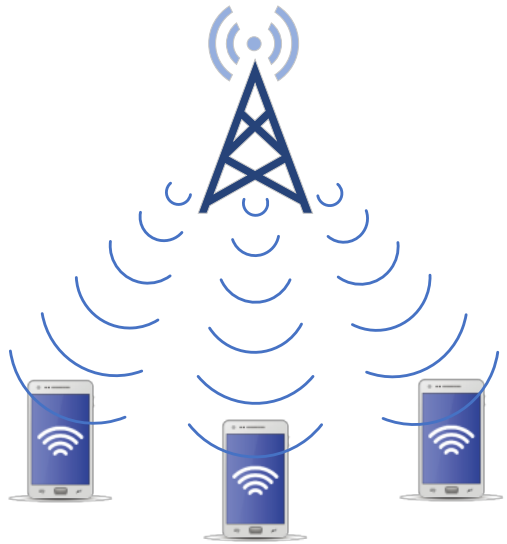
多入多出（MIMO）

多输入多输出（MIMO）：Multi Input Multi Output

Wi-Fi 6 核心技术概览

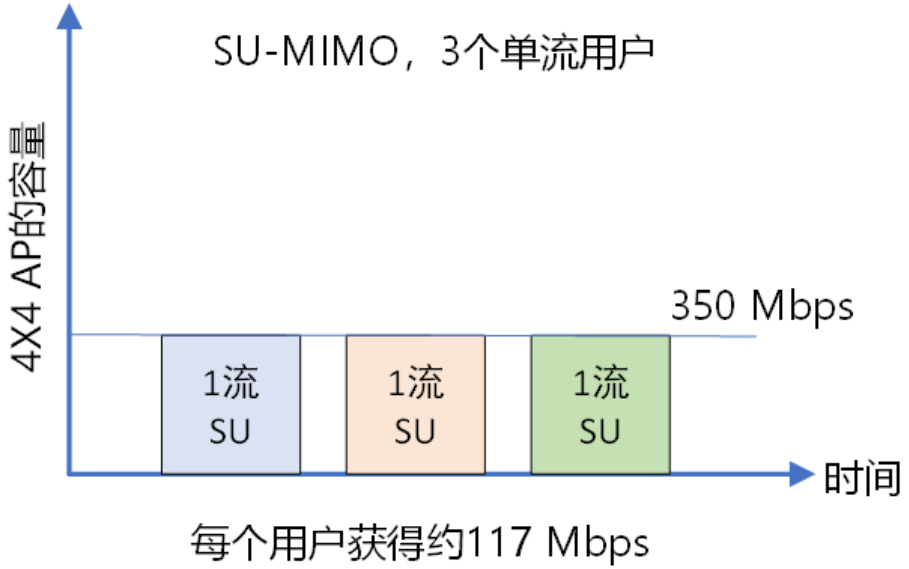
➢ DL/UL MU-MIMO技术

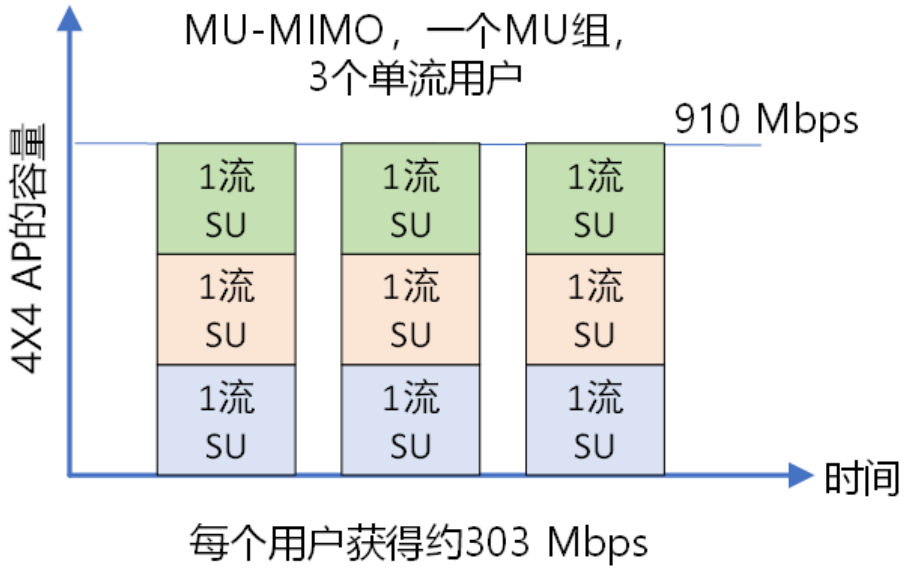
- MIMO可分为SU-MIMO与MU-MIMO，即单用户MIMO和多用户MIMO
- 受限于尺寸，终端通常只有1个或2个空间流 (天线)，比AP的空间流 (天线) 少，在AP 中引入MU-MIMO技术，同一时刻可以实现AP与多个终端之间同时传输数据，增加系统容量，提升用户的平均吞吐量
- Wi-Fi 5 (802.11ac) 支持下行 (DL) 4 x 4 MU-MIMO
- Wi-Fi 6 (802.11ax) 支持下行 (DL) 和上行 (UL) 8 x 8 MU-MIMO



Wi-Fi 6 核心技术概览

- SU-MIMO与MU-MIMO（吞吐量对比）



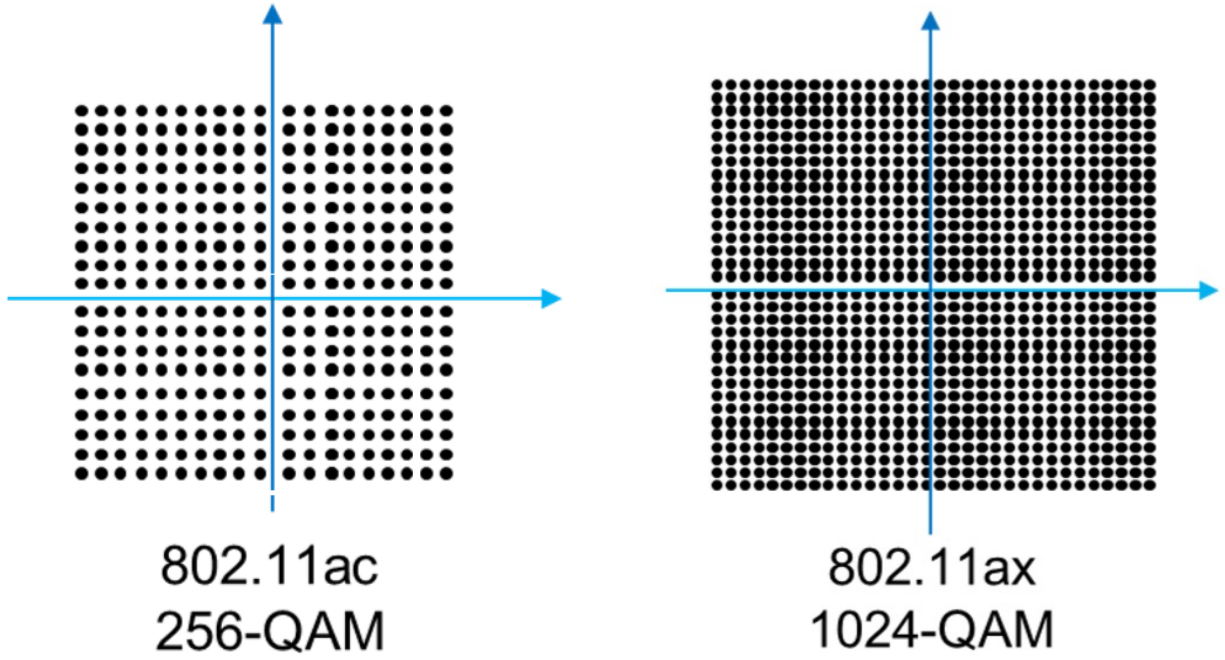


注：MU-MIMO与OFDMA技术结合，可同时进行MU-MIMO传输和分配不同RU进行多用户多址传输，可以增加系统并发接入量，提升多用户并发场景效率，降低应用时延

Wi-Fi 6 核心技术概览

- 高阶调制技术 (1024-QAM)
  - 802.11ac采用的256-QAM正交幅度调制，每个符号传输 8 比特数据（2^8 =256），
  - 802.11ax 采用 1024-QAM正交幅度调制，每个符号位传输10 比特数据（2^{10} =1024)，相对于802.11ac，802.11ax 的单条空间流数据吞吐量提高了25%

星座图



Wi-Fi 6 核心技术概览

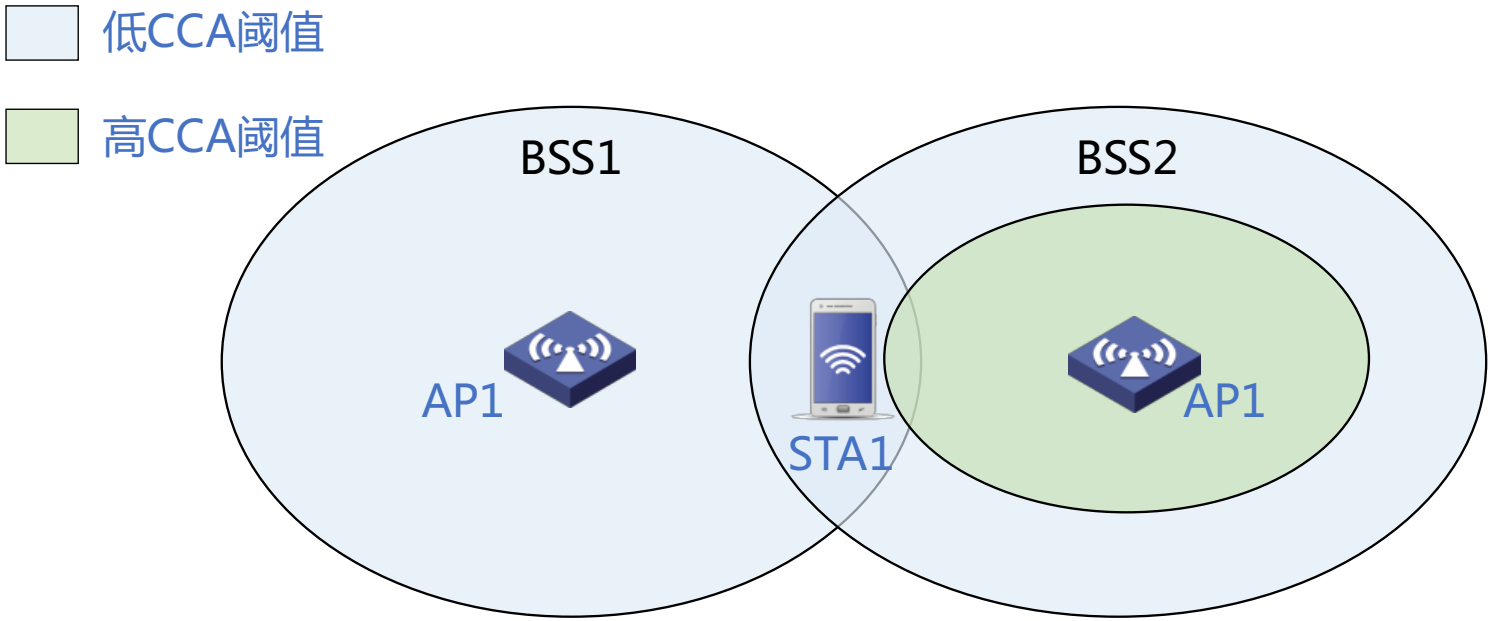
CCA：Clear Channel Assessment

➢ BSS着色机制与动态CCA机制

- 802.11ac 及之前的标准，通过识别同频干扰强度，动态调整CCA阈值，忽略同频弱干扰信号，实现同频并发传输
- 802.11ax中引入了一种新的同频传输识别机制，即 BSS着色 (Coloring) 机制
  - 每个BSS分配一种“颜色”，用前导码中增加6比特标识
  - 每个 STA 在关联时学习自己所属 BSS
  - 具有相同 BSS 颜色的信号使用较低的 CCA 阈值，减少了相同BSS中的冲突
  - 具有不同 BSS 颜色的信号使用较高的 CCA 阈值，允许更多同时传输

Wi-Fi 6 核心技术概览

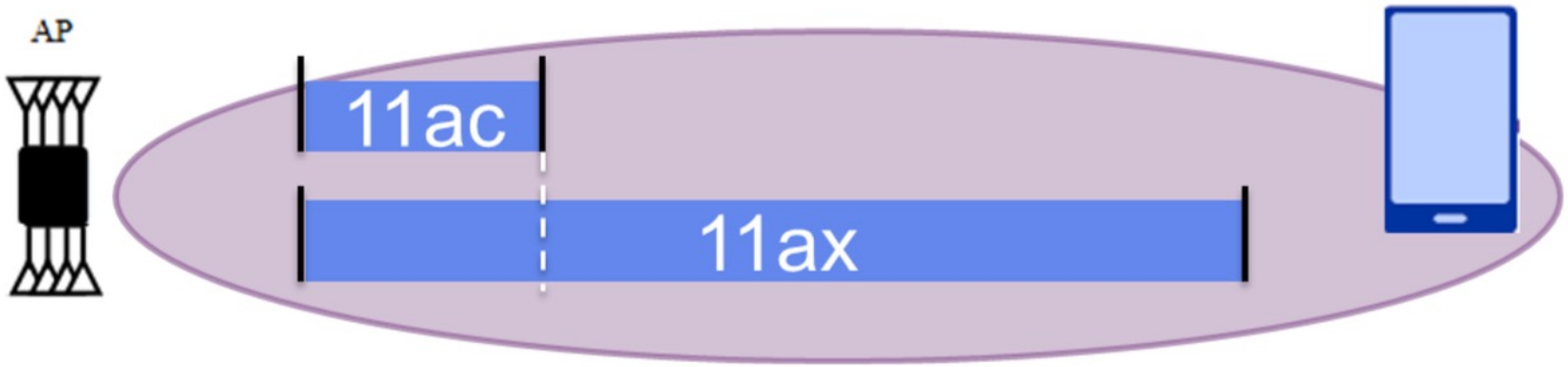
- BSS着色机制与动态CCA机制：示例
  - BSS1和BSS2使用同频信道，STA1关联到AP1，属于BSS1
  - STA1针对BBS1的信号设定低CCA阈值，针对BSS2的信号设定高CCA阈值



注：对统一管理的高密部署环境，该技术会有较好的效果；对于非统一管理的环境，可能会影响传输性能

Wi-Fi 6 核心技术概览

- 扩展覆盖范围
  - 802.11ax 标准采用Long OFDM symbol发送机制，每次数据发送持续时间从原来的 3.2us 提升到 12.8us，更长的发送时间可降低终端丢包率
  - 802.11ax 最小可以仅使用 2MHz 频宽进行窄带传输，有效降低频段噪声干扰，提升了终端接收灵敏度，增加了覆盖距离。



Wi-Fi 6 核心技术概览

- 优化站点睡眠管理
  - Wi-Fi 6引入了目标唤醒时间 TWT，允许设备协商什么时候被唤醒和多久会被唤醒，增加了设备的睡眠时间
  - AP可以将站点分组到不同的TWT周期，以减少唤醒后同时竞争无线介质设备的数量

TWT：Target Wakeup Time

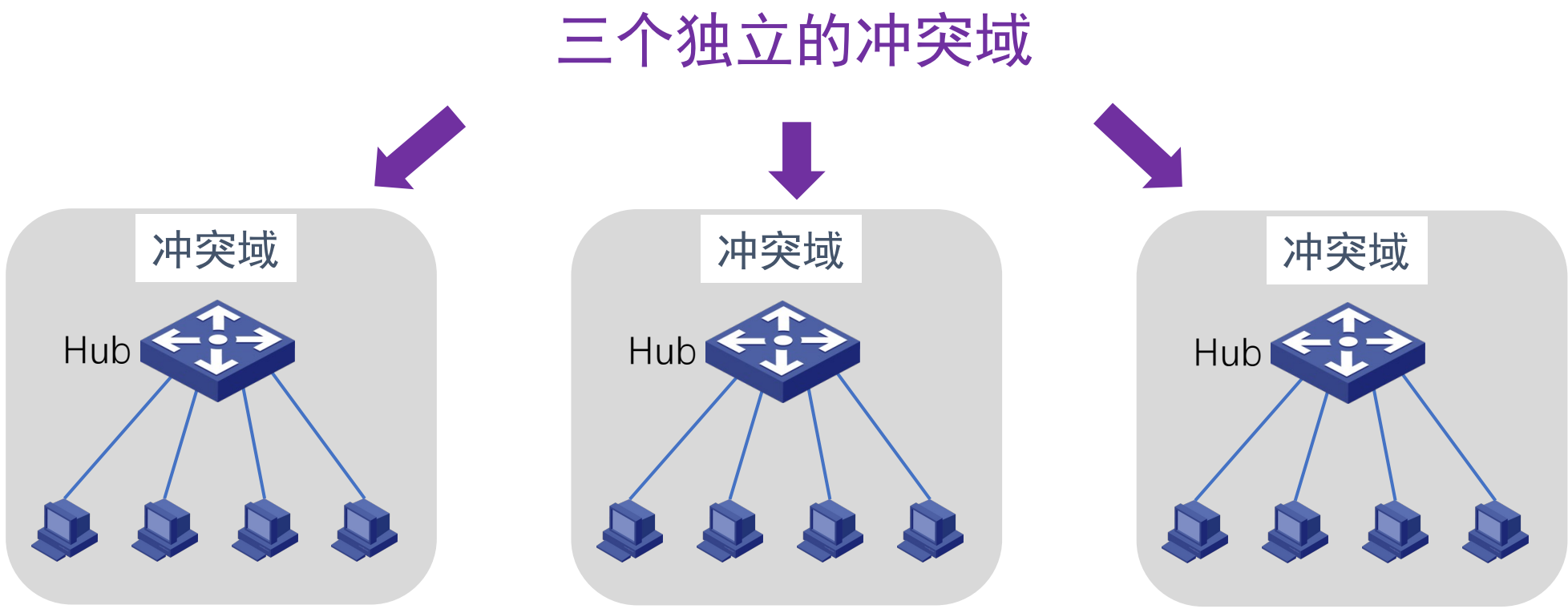
本章内容

- 4.1 信道分配问题
- 4.2 多路访问协议
- 4.3 IEEE802.3协议和以太网
- 4.4 IEEE802.11协议和无线局域网
- 4.5 网桥技术和交换机

1. 数据链路层交换原理
2. 链路层交换机
3. 生成树协议
4. 虚拟局域网

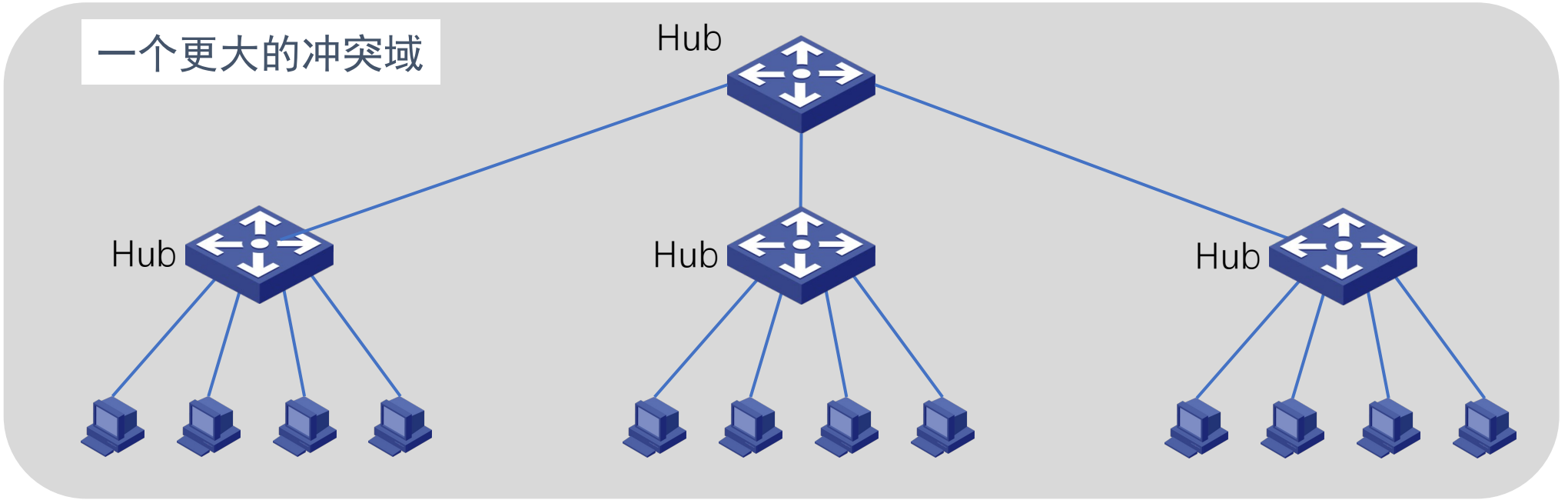
数据链路层交换原理

- 物理层设备扩充网络



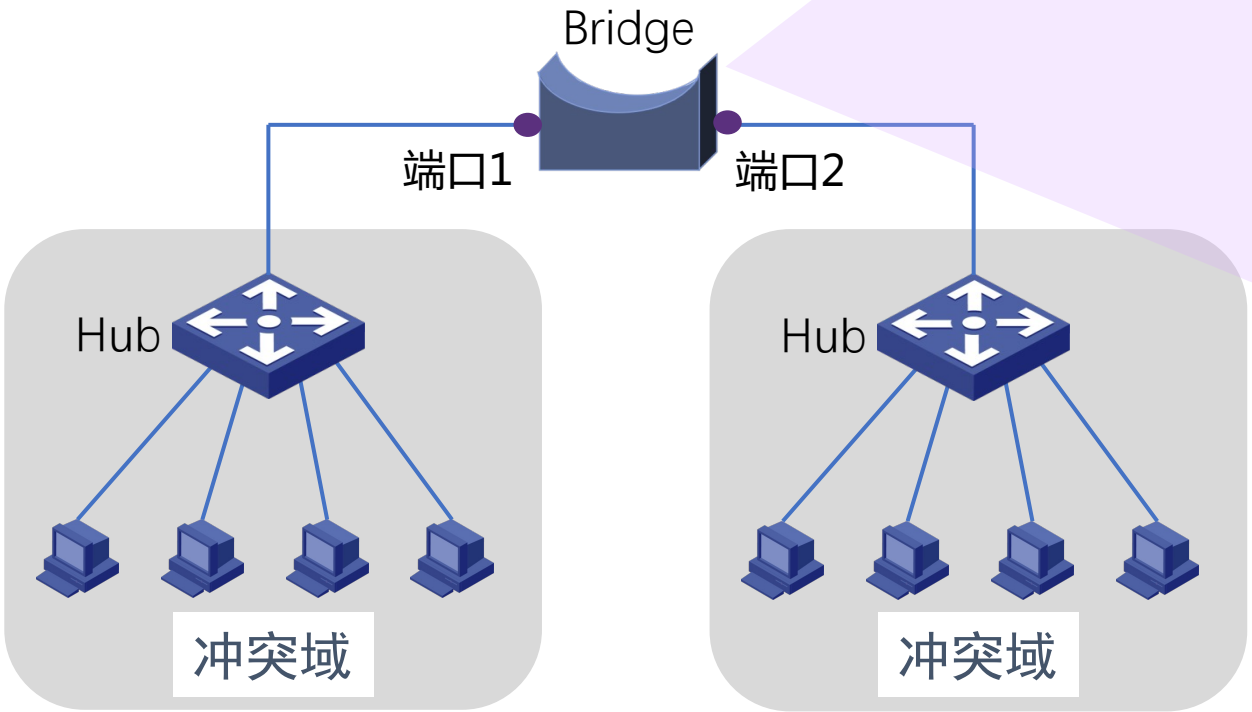
数据链路层交换原理

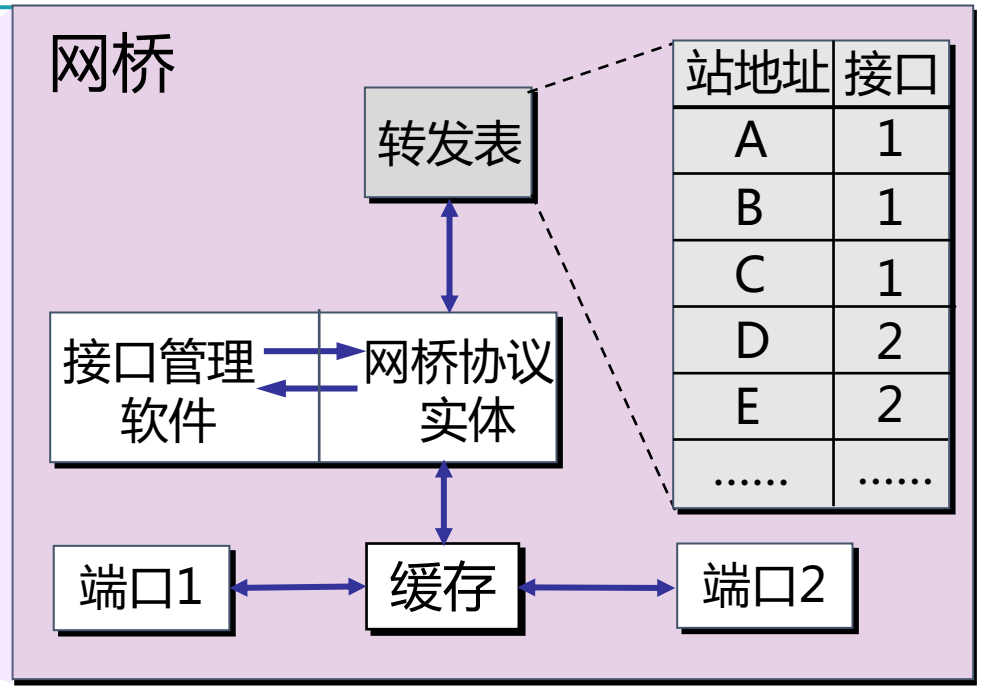
- 物理层设备扩充网络
  - 扩大了冲突域，性能降低，安全隐患



数据链路层交换原理

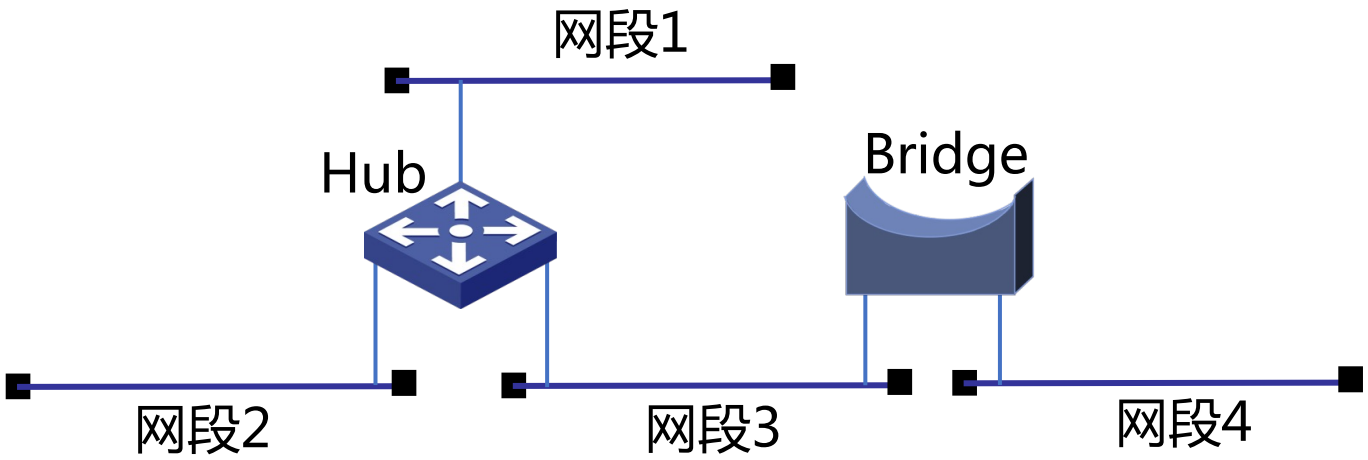
- 数据链路层设备扩充网络
  - 网桥或交换机
  - 分隔了冲突域

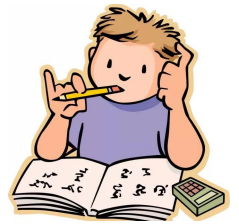




数据链路层交换原理

- 练习：图中有几个冲突域？





数据链路层交换原理

- 理想的网桥是透明的。
  - 即插即用，无需任何配置
  - 网络中的站点无需感知网桥的存在与否

怎么做到透明的？

数据链路层交换原理

- MAC地址表的构建-逆向学习源地址

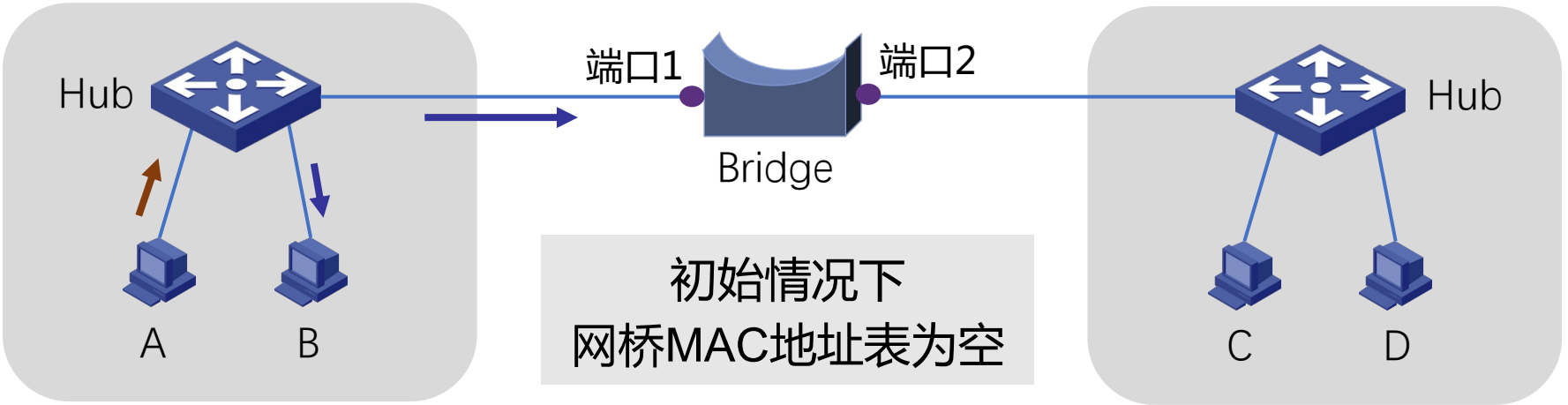
A→B发出数据帧

逆向学习
源地址

MAC地址表	
MAC地址	端口
MAC_A	1

记录帧到达时间
设定老化时间（默认300s）.
当老化时间到期时，该表项会被清除。

Why?



初始情况下
网桥MAC地址表为空

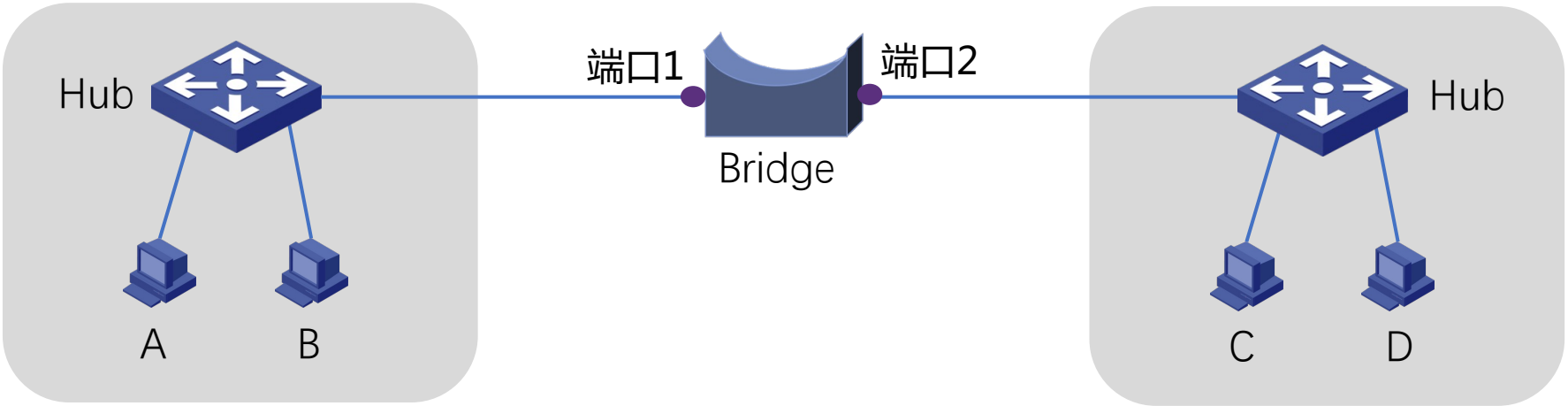
数据链路层交换原理

- 发送帧的站MAC地址被学习

网桥怎样学习到B\C\D的MAC地址？

MAC地址表	
MAC地址	端口
MAC_A	1
MAC_B	1
MAC_C	2
MAC_D	2

主机向外发送数据时其MAC地址就会被学习



数据链路层交换原理

- 网桥构建MAC地址表的过程

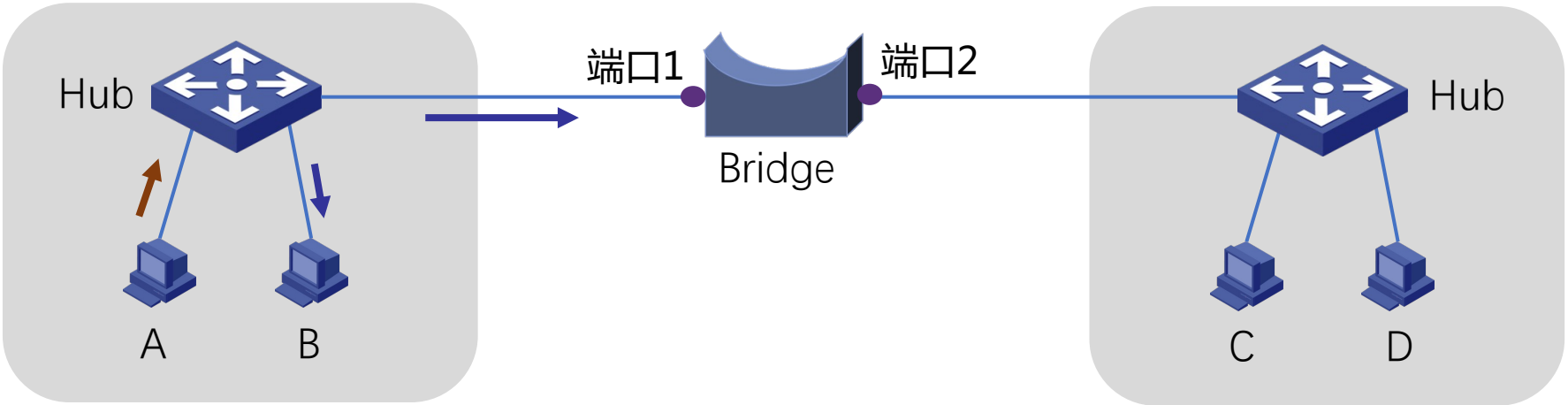
再次：A发出数据帧

逆向学习源地址

MAC地址表	
MAC地址	端口
MAC_A	1
MAC_B	1
MAC_C	2
MAC_D	2

网桥发现MAC_A已在表中！

更新该表项的帧达到时间，重置老化时间



数据链路层交换原理

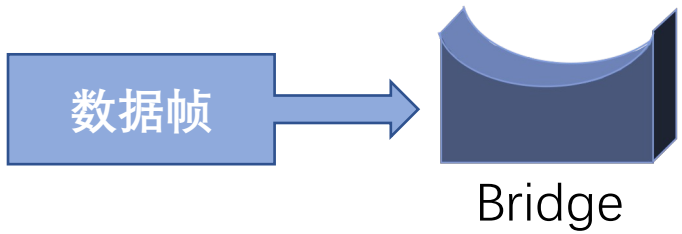
- MAC地址表的构建
  - 增加表项：帧的源地址对应的项不在表中
  - 删除表项：老化时间到期
  - 更新表项：帧的源地址在表中，更新时间戳

MAC地址表会满而溢出吗？是不是存在安全隐患？

数据链路层交换原理

- 网桥通过逆向学习帧的源地址，获知主机所处的位置，
- 网桥通过逆向学习帧的源地址，构建MAC地址表。

网桥如何利用MAC地址表进行数据帧的转发？



网桥对于入境帧的处理过程（forwarding、filtering、flooding）

数据链路层交换原理

- Forwarding（转发）

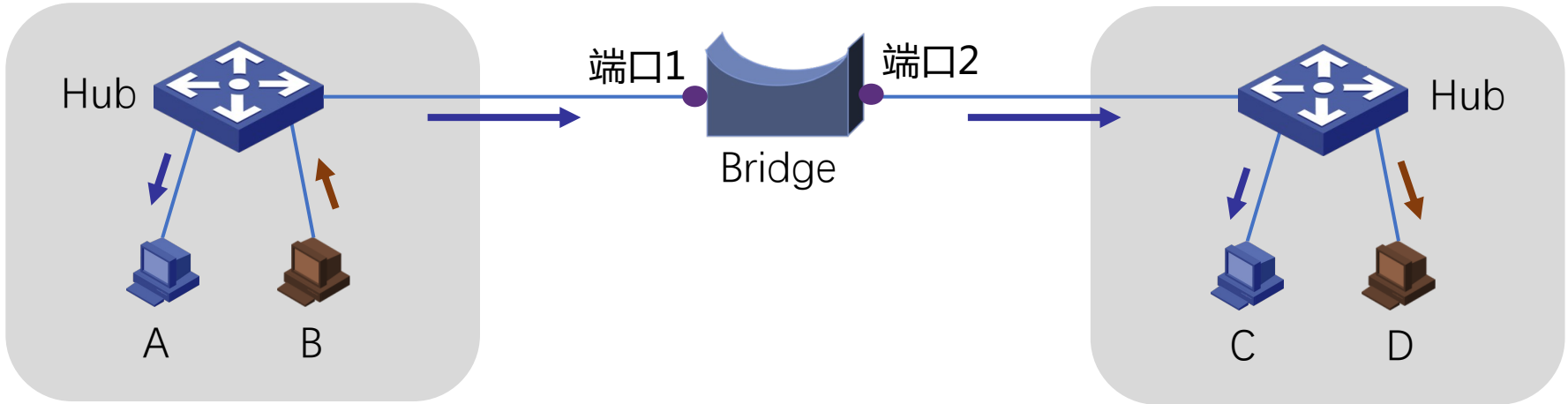
B→D 发出数据帧

逆向学习源地址
并根据**目的地址**
查询MAC地址表

MAC地址表完善时

MAC地址表	
MAC地址	端口
MAC_A	1
MAC_B	1
MAC_C	2
MAC_D	2

找到匹配项！
从对应端口2转发出去



数据链路层交换原理

- Filtering（过滤）

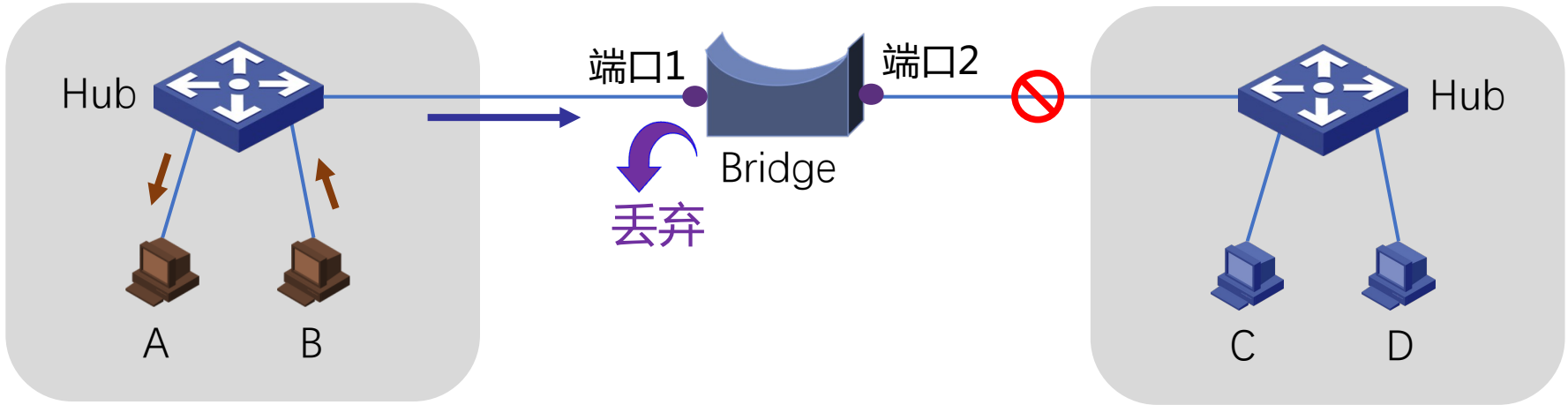
B→A 发出数据帧

逆向学习源地址
并根据**目的地址**
查询MAC地址表

MAC地址表完善时

MAC地址表	
MAC地址	端口
MAC_A	1
MAC_B	1
MAC_C	2
MAC_D	2

找到匹配项！
入境口=出境口，丢弃！



数据链路层交换原理

- Flooding（泛洪）

A→B 发出数据帧

MAC地址表不完善时

MAC地址表	
MAC地址	端口
MAC_A	1

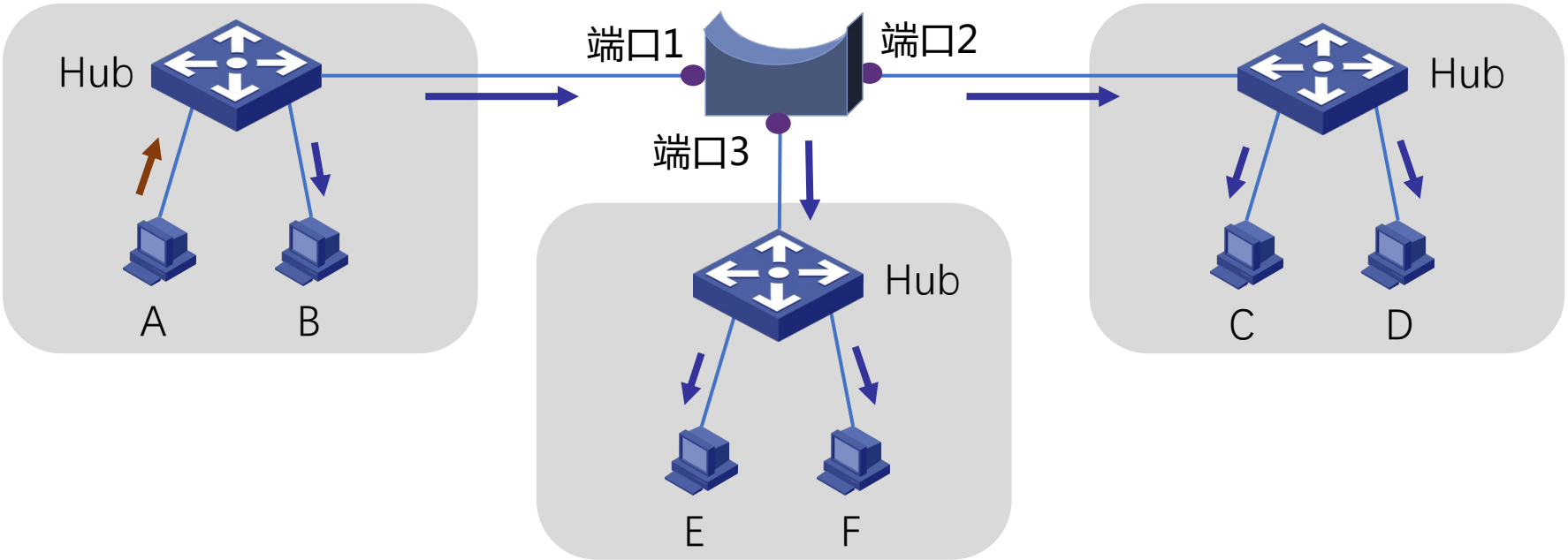
找不到匹配表项！

从所有端口（除了入境口）发送出去

一个网段的数据被发送到无关网段

存在安全隐患

浪费网络资源



数据链路层交换原理

- Flooding（泛洪）
  - 两种目的地址的帧，需要泛洪：
    - 广播帧：目的地址为FF-FF-FF-FF-FF-FF的数据帧
    - 未知单播帧：目的地址不在MAC地址转发表中的单播数据帧

泛洪的两种情形！

数据链路层交换原理

- 透明网桥工作原理（小结）
  - 逆向学习

    根据帧的源地址在MAC地址表查找匹配表项，

    ✓如果没有，则增加一个新表项（源地址、入境端口、帧到达时间），

    ✓如果有，则更新原表项的帧到达时间，重置老化时间。
  - 对入境帧的转发过程（三选一），查帧的目的地址是否在MAC地址表中

    ✓如果有，且入境端口≠出境端口，则从对应的出境端口转发帧；

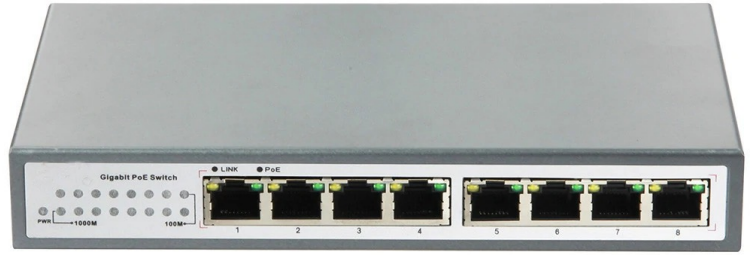
    ✓如果有，且入境端口=出境端口，则丢弃帧（即过滤帧）；

    ✓如果没有，则向除入境端口以外的其它所有端口泛洪帧。

链路层交换机

- 执行数据链路层交换算法
  - 多端口透明网桥，网桥的现代名称
  - 一种即插即用设备

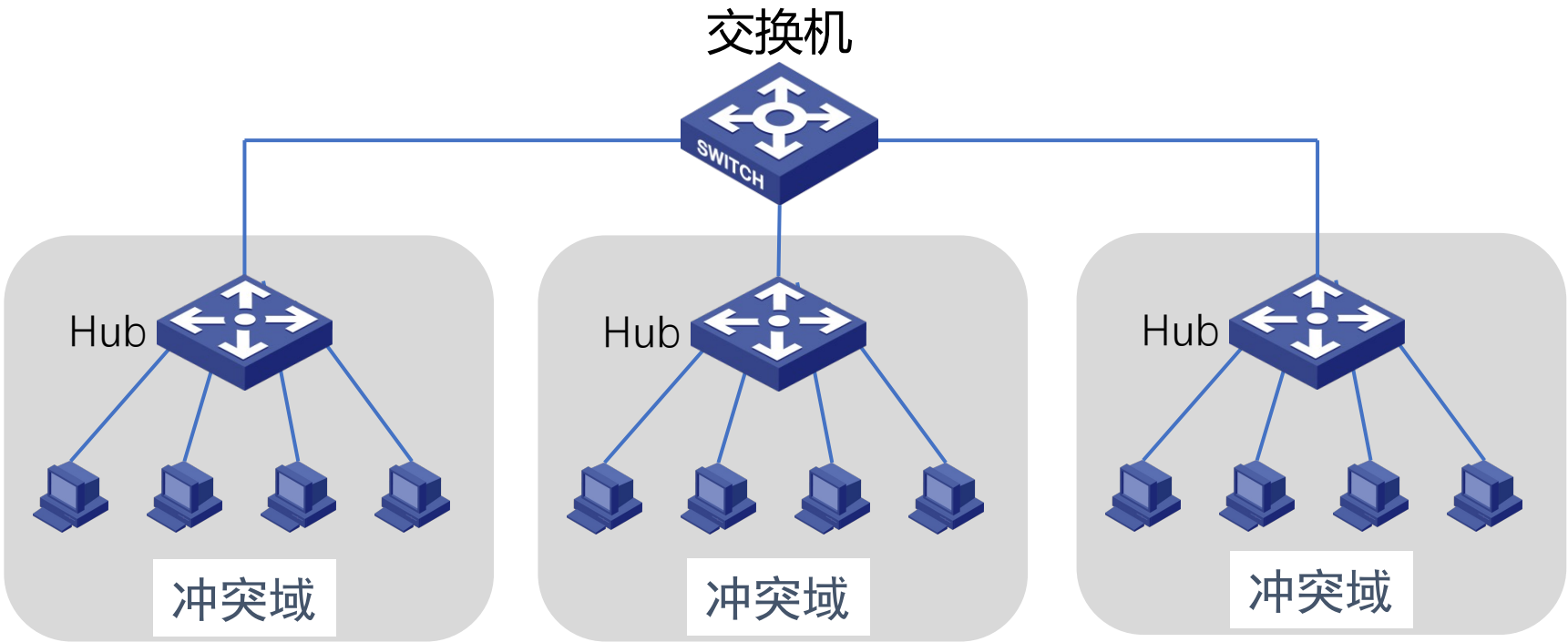
- POE（Power Over Ethernet）交换机
  - 常接：网络摄像机、AP、IP电话等
  - 主要优点：无需电源（受电端）、无需专门布线



为什么PoE交换机并不常见？

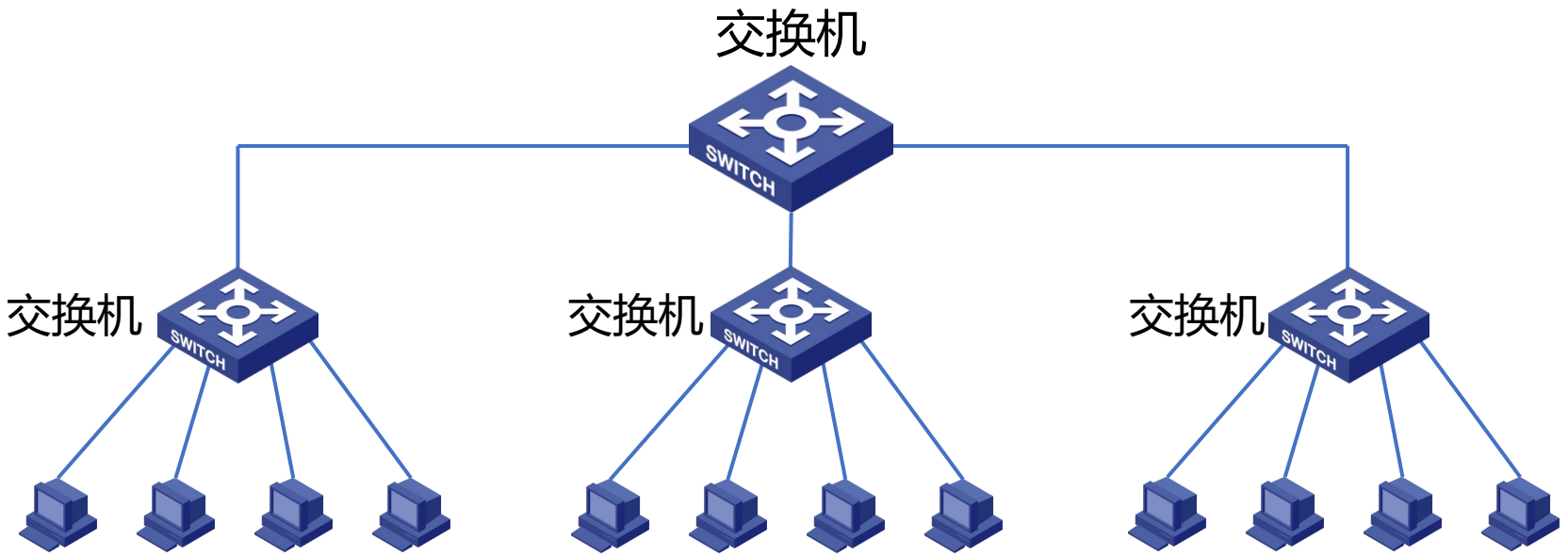
链路层交换机

- 传统LAN分段
  - 交换机端口通常与集线器连接；
  - 使用交换机把LAN分段为更小的冲突域。



链路层交换机

- 现代LAN分段
  - 直连PC，微分段，创建无冲突域

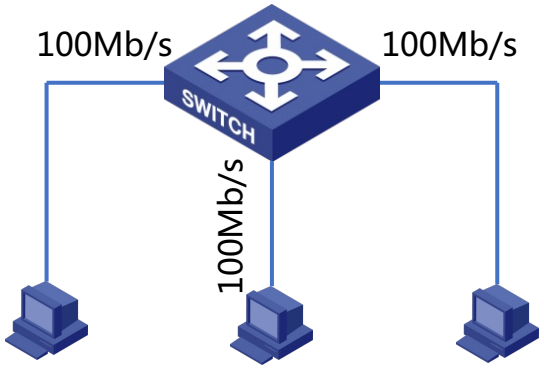


链路层交换机

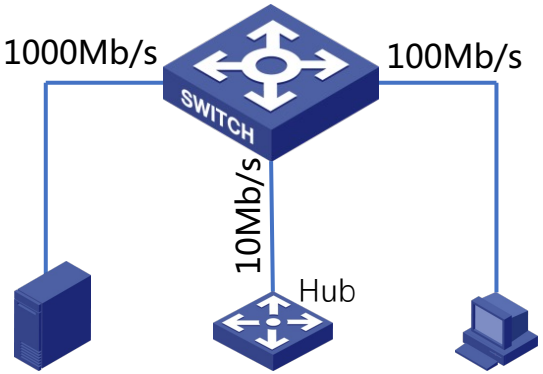
- 交换方式：从带宽的角度
  - 对称交换：出和入的带宽相同

    例如：交换机上全为1000Mb/s速率端口
  - 非对称交换：出和入的带宽不同

    例如：交换机上有100Mb/s、1000Mb/s等多种速率端口



对称交换



非对称交换

链路层交换机

- 交换模式：从转发时机的角度

  1）存储转发模式（Store and Forward）

  2）直通模式（Cut-through）

  3）无碎片模式（Fragment-free）

链路层交换机

- 交换模式1：存储转发
  - 特点：转发前必须接收整个帧、执行CRC校验
  - 缺点：延迟大
  - 优点：不转发出错帧、支持非对称交换

7字节	1字节	6字节	6字节	2字节	46~1500字节	4字节
Preamble	SFD	Destination	Source	Length/ Type	Data and Pad	FCS

存储转发模式
高延迟
过滤所有错误帧

链路层交换机

- 交换模式2：直通交换
  - 特点：一旦接收到帧的目的地址，就开始转发
  - 缺点：可能转发错误帧、不支持非对称交换
  - 优点：延迟非常小，可以边入边出

7字节	1字节	6字节	6字节	2字节	46~1500字节	4字节
Preamble	SFD	Destination	Source	Length/ Type	Data and Pad	FCS

直通模式
低延迟、无错误检查

链路层交换机

- 交换模式3：无碎片交换
  - 特点：接收到帧的前64字节，即开始转发
  - 缺点：仍可能转发错误帧，不支持非对称交换
  - 优点：过滤了冲突碎片，延迟和转发错帧介于存储转发和直通交换之间

7字节	1字节	6字节	6字节	2字节	46~1500字节	4字节
Preamble	SFD	Destination	Source	Length/ Type	Data and Pad	FCS

帧的前64字节

无碎片模式
较低延迟
过滤冲突导致的碎片帧

链路层交换机

➢ 练习

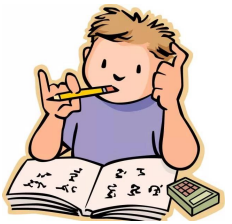
在交换机的三种交换模式中，正常情况下(　　)模式的转发延迟最大。

A、直通

B、存储转发

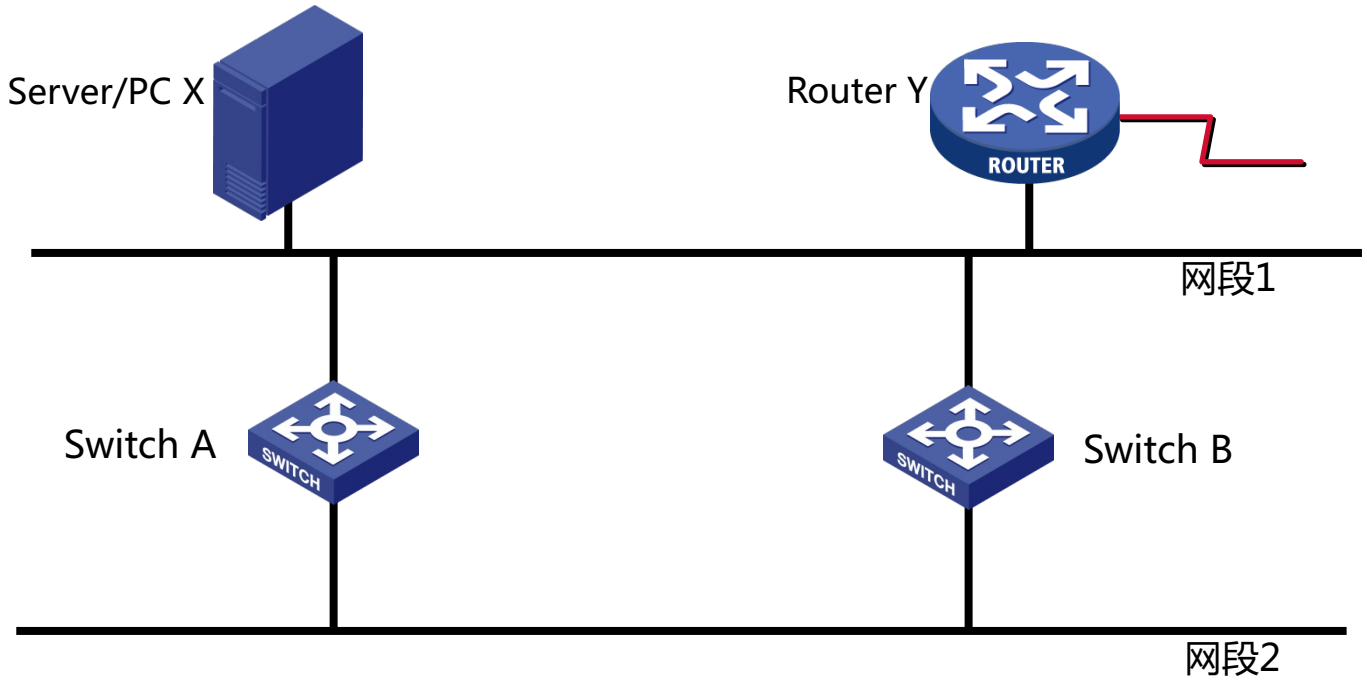
C、无碎片

D、都一样



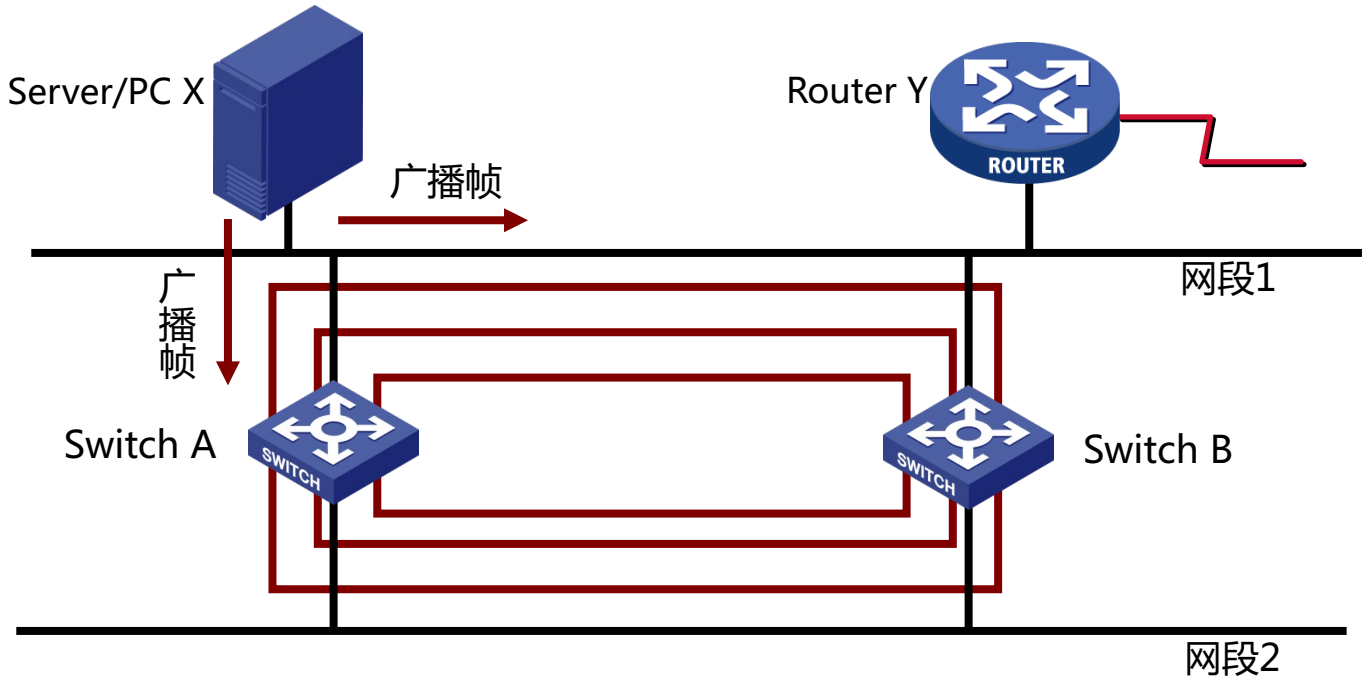
生成树协议

- 可靠传输：冗余拓扑
- 付出的代价：导致物理环路



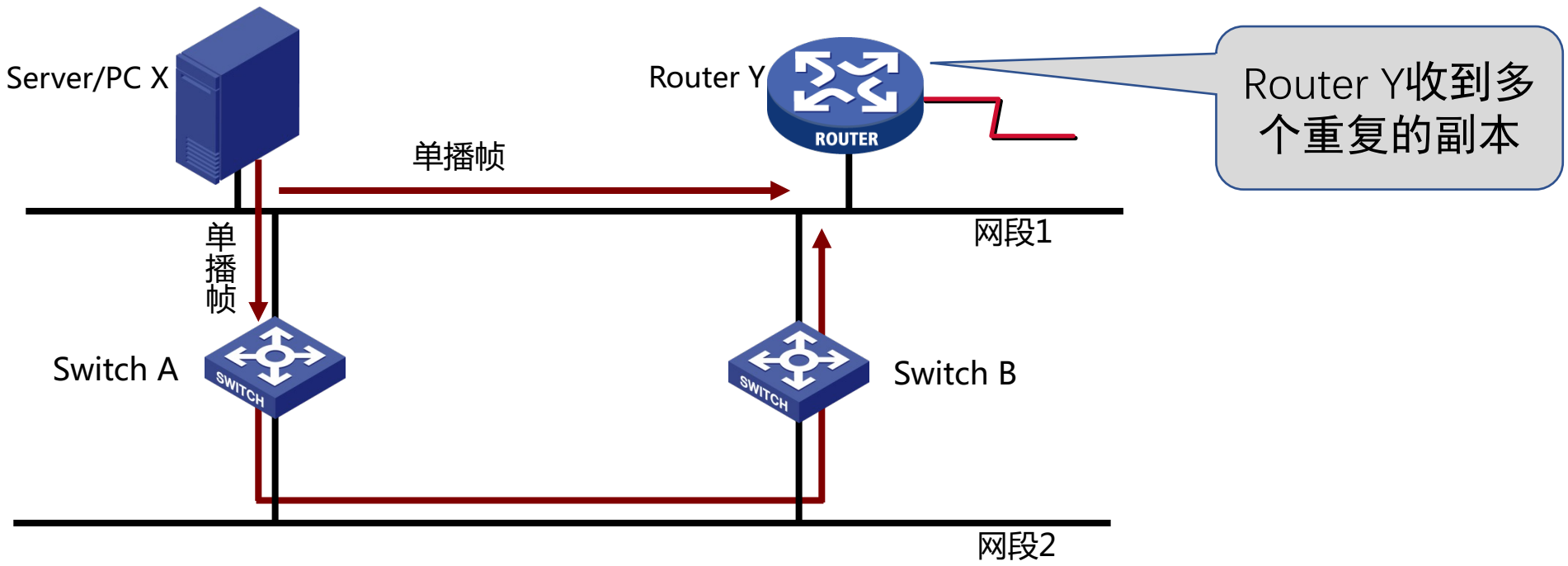
生成树协议

- 物理环路引发的问题1：广播风暴
  - 交换机（网桥）在物理环路上无休止地泛洪广播流量，无限循环，迅速消耗网络资源。



生成树协议

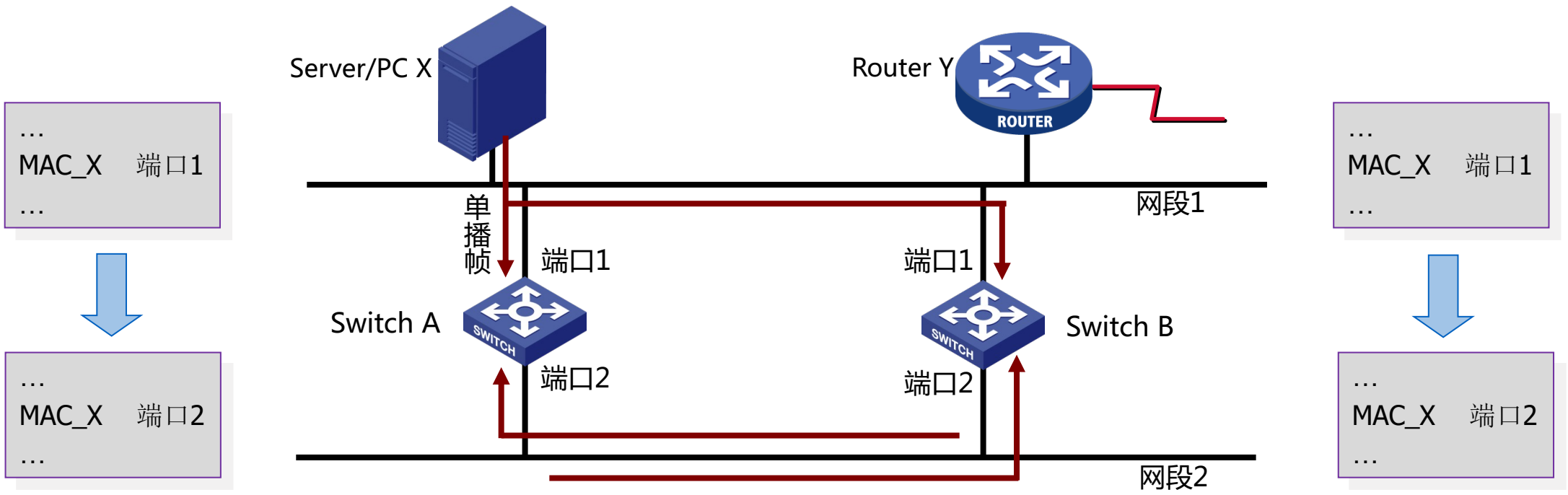
- 物理环路引发的问题2：重复帧
  - X发送到环路的单播帧，造成目的设备Y收到重复的帧。



假设所有交换机的MAC地址表中均没有路由器Y的MAC地址

生成树协议

- 物理环路引发的问题3：MAC地址表不稳定
  - 当一个帧的多个副本到达不同端口时，交换机会不断修改同一MAC地址对应的端口。



生成树协议

- 发明人 Radia Perlman
  - A Protocol for Distributed Computation of a Spanning Tree in an Extended LAN, Ninth Data Communications Symposium, Vancouver, 1985
  - 1983年，发明生成树协议（STP）：打破了物理环，维护一个逻辑无环树

I think that I shall never see

A graph more lovely than a tree.

A tree whose crucial property

Is **loop-free** connectivity.

A tree which must be sure to span.

So packets can reach every LAN.

First the **Root** must be selected

By ID it is elected.

Least cost paths from Root are traced

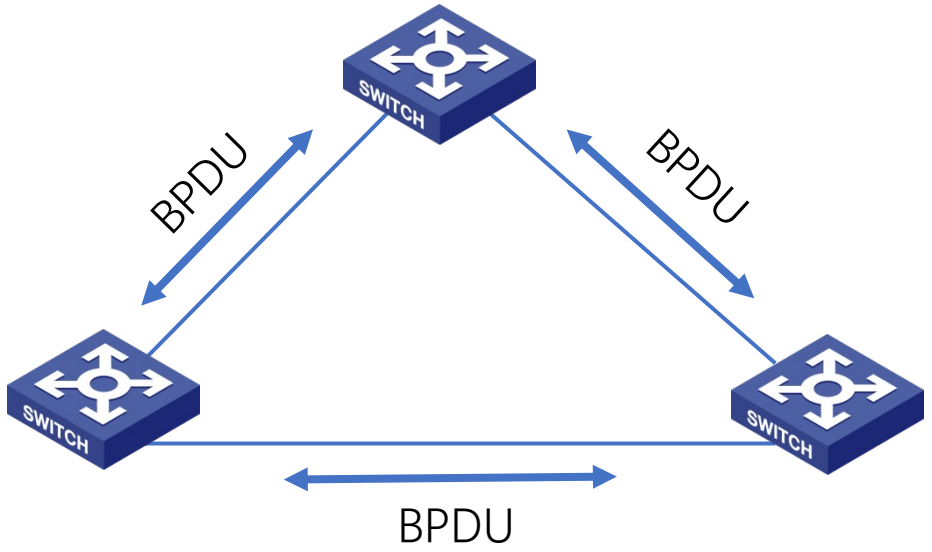
In the tree these paths are placed.

A mesh is made by folks like me

Then bridges find **a spanning tree**.

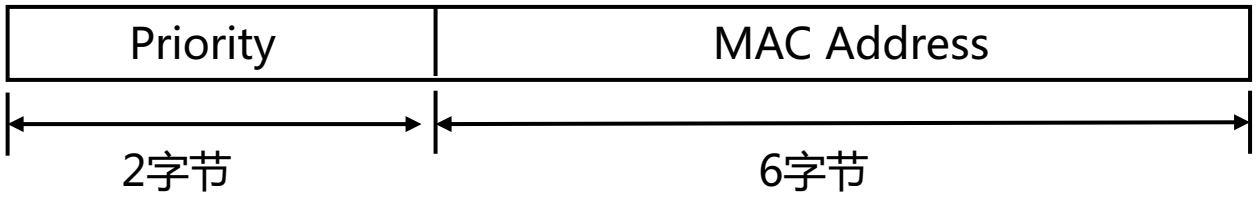
生成树协议

- 怎么得到一棵无环的生成树呢？
  - 参与的交换机（网桥）：收发桥协议数据单元BPDU
  - 选举产生根桥、根端口、指定端口，形成生成树



生成树协议

- 桥协议数据单元BPDU包含的四个关键信息
  - 根桥ID（Root ID）：被选为根的桥ID。
    - 桥ID共8字节，由2字节的优先级和6字节的MAC地址组成的。



  - 根路径开销（Root Path Cost）：到根桥的最小路径开销。
  - 指定桥ID（Designated Bridge ID）：生成和转发BPDU的桥ID
  - 指定端口ID（Designated Port ID）：发送BPDU的端口ID。

生成树协议

- 生成树的三个选举过程

  (1) 选举根桥(Root Bridge)。

  (2) 为每个非根桥选出一个根端口（Root Port）。

  (3) 为每个网段确定一个指定端口（Designated Port）。

生成树协议

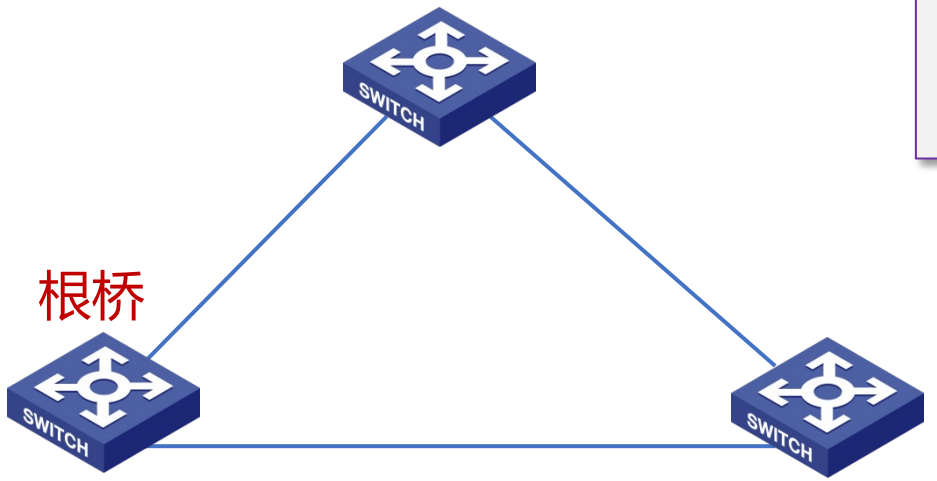
- 生成树的选举过程1：选举根桥
  - 同一广播域中的所有交换机均参与选举；
  - 桥ID最小的交换机（网桥）成为生成树的根；
  - 在给定广播域内只有一个根桥，其它均为非根桥。
  - 根桥的所有端口都处在转发状态。

可以接收和发送数据帧

生成树协议

- 根桥选举实例

Bridge ID
优先级： 32769
MAC地址：00-0A-00-11-11-11



根桥

Bridge ID
优先级： 24577
MAC地址：00-0A-00-33-33-33

Bridge ID
优先级： 32769
MAC地址：00-0A-00-22-22-22

如何比较桥ID大小？

- 首先比较优先级，优先级数值最小的交换机胜出成为根桥。
- 如果优先级数值相等，MAC地址最小的交换机成为根桥。

生成树协议

- 生成树的选举过程2：为每个非根桥选出一个根端口
  - 每个非根桥，通过比较其每个端口到根桥的根路径开销，选出根端口；
  - 具有最小根路径开销的端口被选作根端口；
  - 如果多个端口的根路径开销相同，则端口ID最小的端口被选作根端口；
  - 非根桥只能有一个根端口，根端口处于转发状态。

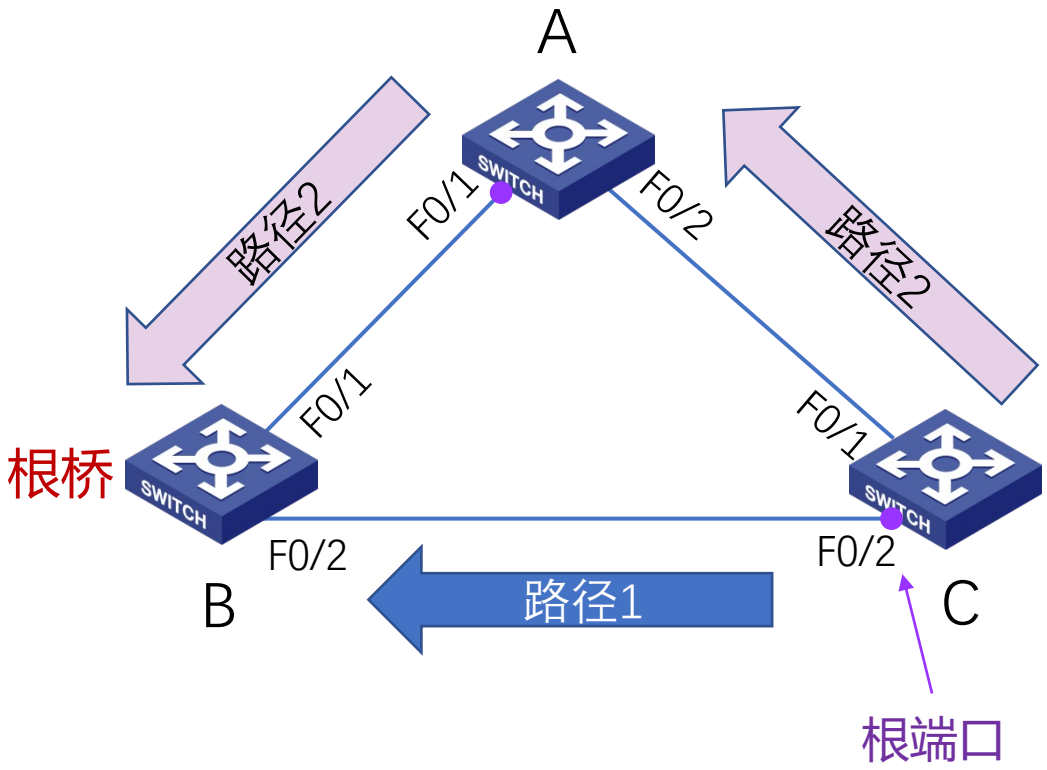
生成树协议

- 什么是根路径开销？
  - 根桥的根路径开销为0；
  - 非根桥的根路径开销为到根桥的路径上所有端口（链路）开销之和。
  - 端口（链路）开销值由IEEE定义（如下表），也可通过手工配置改变。

速率值	开销 （IEEE802.1D-1998）
10Mbps	100
100Mbps	19
1Gbps	4
10Gbps	2
>10Gbps	1

生成树协议

➢ 根端口选举实例



图中交换机端口速率均为100Mb/s

即开销均为19。

C到达根桥有两条路径：

- 路径1开销为19
- 路径2开销为19+19=38

路径1开销较小！

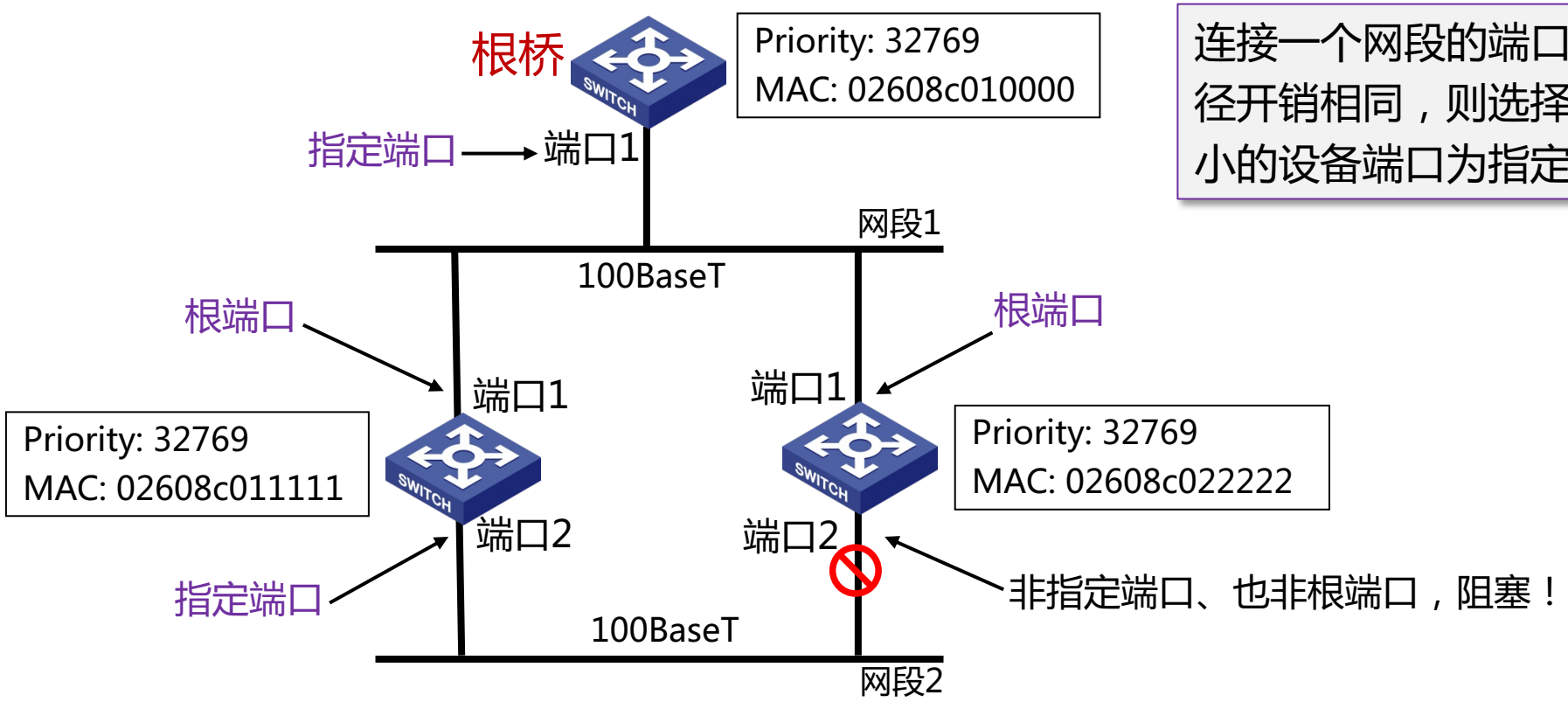
F0/2相比于F0/1到达根桥的根路径开销更小，因此F0/2为C的根端口。

生成树协议

- 生成树的选举过程3：为每个网段确定一个指定端口
  - 对于每一个网段， 在所有连接到它的交换机（网桥）端口中进行选择；
  - 一个具有最小根路径开销的端口，作为该网段的指定端口；
  - 指定端口处于转发状态，负责该网段的数据转发；
  - 连接该网段的其他端口，若既不是指定端口，也不是根端口，则阻塞。

生成树协议

- 指定端口选举实例



连接一个网段的端口的根路径开销相同，则选择桥ID较小的设备端口为指定端口。

生成树协议

- 端口角色与端口状态
  - 经过上述构造生成树的三个过程，端口角色便确定了。

端口角色	英文名称	端口状态
指定端口	Designated port	Forwarding
根端口	Root port	Forwarding
非指定端口/根端口 （通常称为备用端口或冗余端口）	Alternate port	Blocking

练习：根桥的所有连接端口都是指定端口。（判断题）

生成树协议

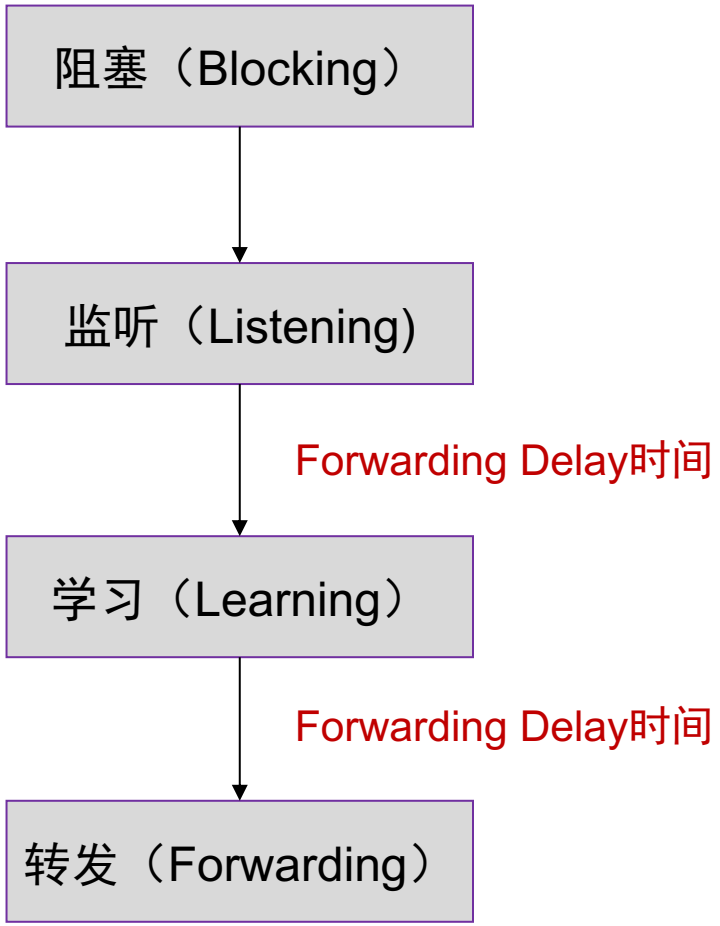
➢ 端口角色与端口状态

- 事实上，802.1D标准给出了五种端口状态。

端口角色	端口状态	端口行为
未启用STP功能的端口	Disabled	不收发BPDU报文，接收或转发数据
非指定端口或根端口	Blocking	接收但不发送BPDU，不接收或转发数据
--	Listening	接收并发送BPDU，不接收或转发数据
--	Learning	接收并发送BPDU，不接收或转发数据
指定端口或根端口	Forwarding	接收并发送BPDU，接收并转发数据

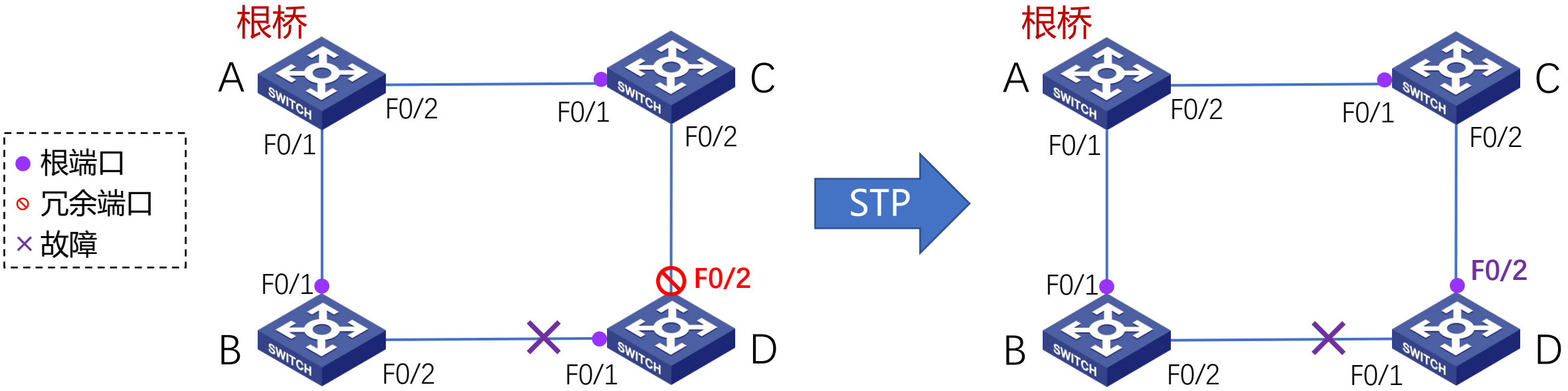
生成树协议

- 端口状态的迁移
  - 端口角色确定为指定端口或根端口后，从Blocking状态经Listening和Learning才能到Forwarding状态；
  - 默认的Forwarding Delay时间是15秒，能保证当网络的拓扑发生改变时，新的配置信息能够传遍整个网络，从而避免由于网络为收敛而造成临时环路。



生成树协议

- 生成树的某“枝”断掉了，怎么办？
  - 当由交换机（网桥）或链路故障导致网络拓扑改变时，重新构造生成树。



交换机D的端口F0/2从Blocking状态到Forwarding状态至少要经过两倍Forwarding Delay时间，导致网络的连通性至少要30秒之后才能恢复。

生成树协议

- 重新构建生成树太慢了，怎么办？
  - 快速生成树协议（Rapid Spanning Tree Protocol, RSTP）
    - RSTP是STP的优化版，在IEEE802.1W中定义；
    - 2004年IEEE将RSTP整合到802.1D中，新规范为IEEE802.1D-2004；
    - RSTP协议能够在拓扑改变时加速重新计算生成树的过程。
    - RSTP能够达到更快的收敛速度，有时甚至只需几百毫秒。

生成树协议

- RSTP的改进

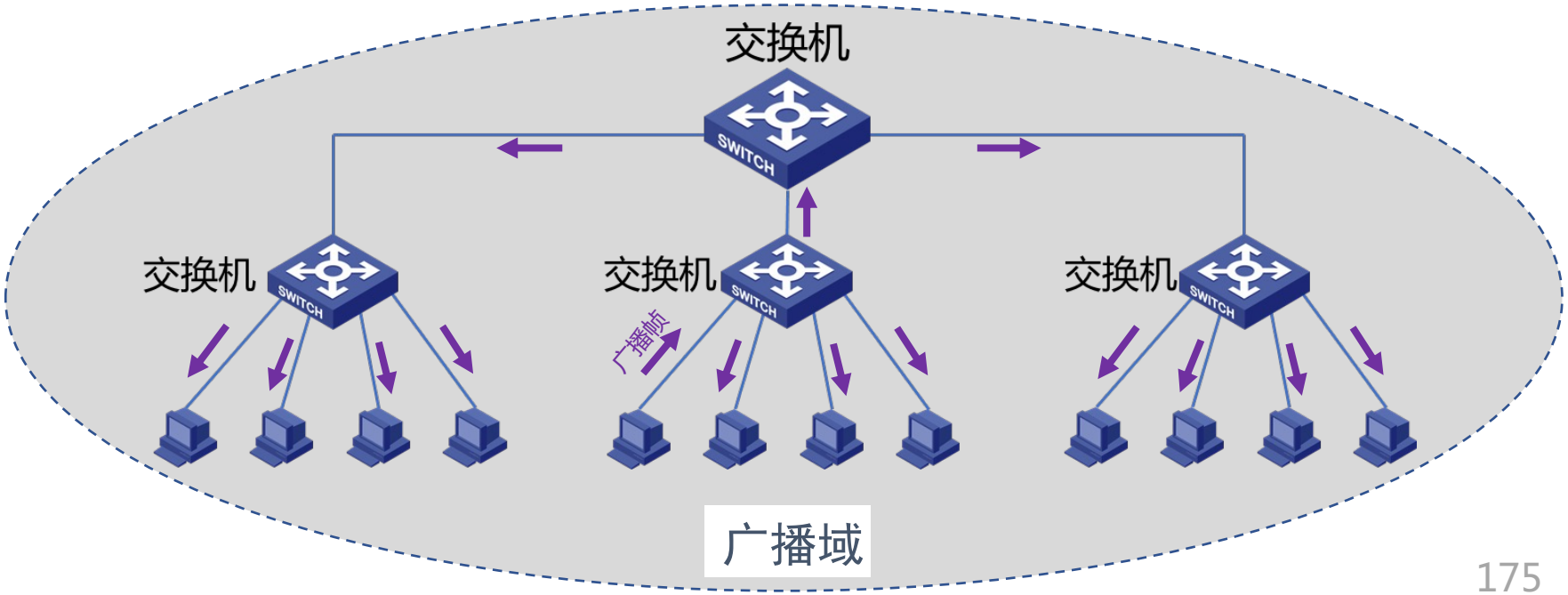
端口角色变化	STP行为	RSTP行为
端口被选为根端口	默认情况下，2倍的Forwarding Delay的时间延迟。	存在阻塞的备份根端口情况下，仅有数毫秒延迟。
端口被选为指定端口	默认情况下，2倍的Forwarding Delay的时间延迟。	在指定端口是非边缘端口的情况下，延迟取决因素较多。
		在指定端口是边缘端口的情况下，指定端口可以直接进入转发状态，没有延迟。

“边缘端口”是指那些直接和终端设备相连，不再连接任何交换机的端口。不能阻塞！

虚拟局域网

- 广播域（Broadcasting Domain）
  - 广播域是广播帧能够到达的范围；
  - 缺省情况下，交换机所有端口同属于一个广播域，无法隔离广播域；
  - 广播帧在广播域中传播，占用资源，降低性能，且具有安全隐患。

图中某个站点
发送了一个广播帧
能够收到该广播帧的设备
同处于一个广播域

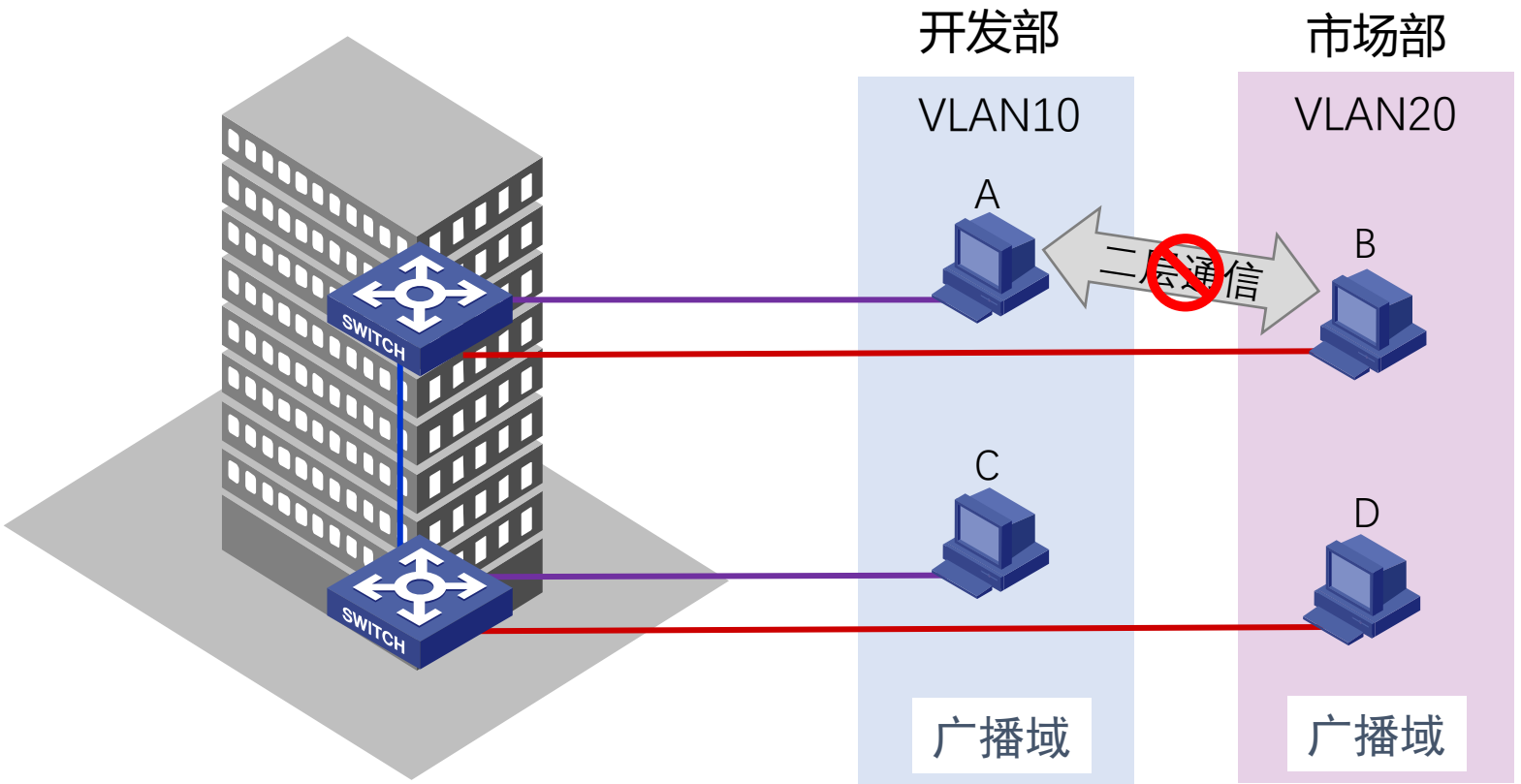


虚拟局域网

- 交换机可以分隔广播域吗？
  - 可以！支持VLAN的交换机；
  - 一个VLAN（Virtual LAN）是一个独立的广播域；
  - 交换机通过划分VLAN，来分隔广播域。

虚拟局域网

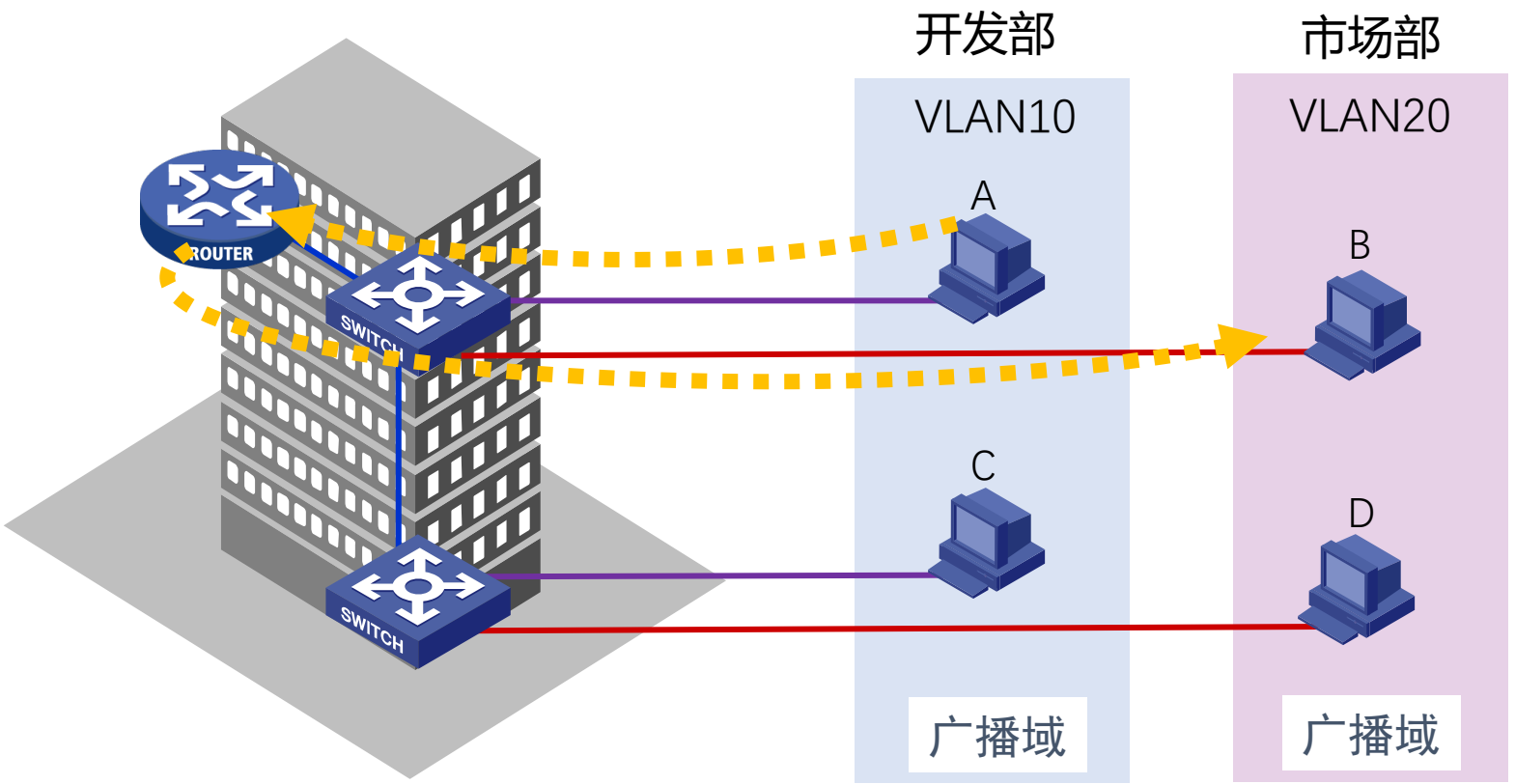
- VLAN是一个在物理网络上根据用途，工作组、应用等来逻辑划分的局域网络，与用户的物理位置没有关系。



不同VLAN的成员
不能直接进行二层通信

虚拟局域网

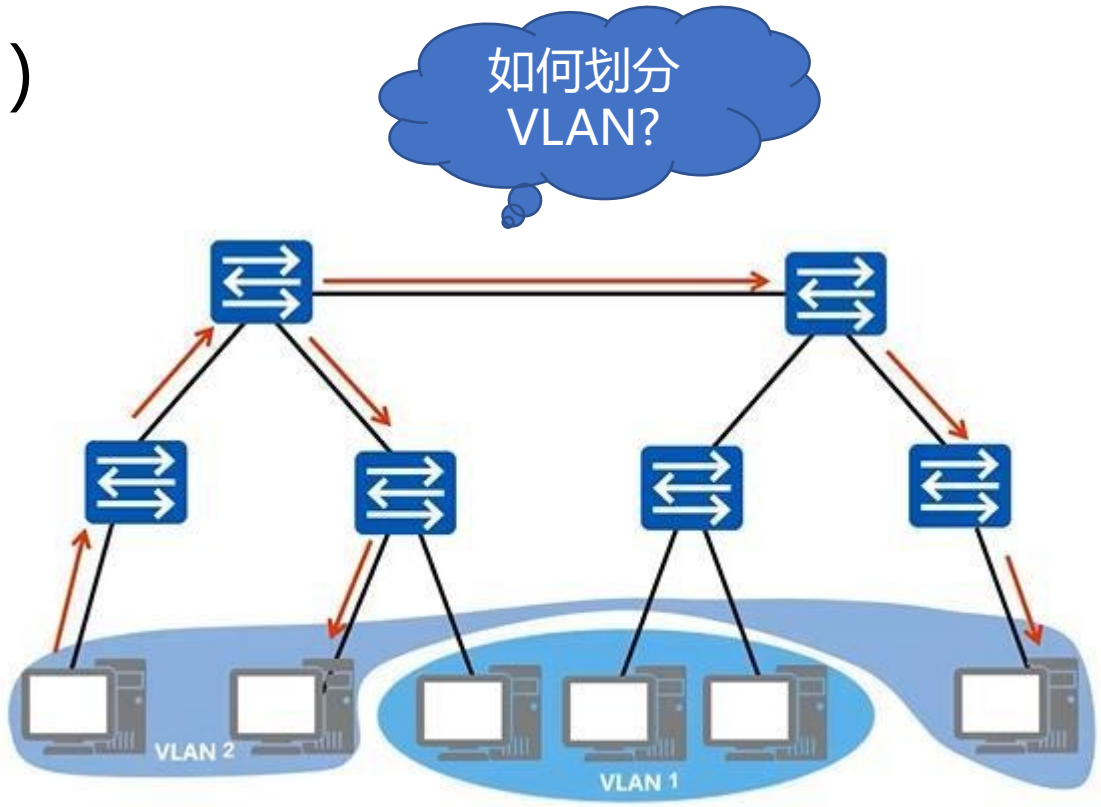
- 通过路由器或三层交换机进行VLAN间路由，实现VLAN间通信。



不同VLAN的成员通信
需要通过三层设备

虚拟局域网

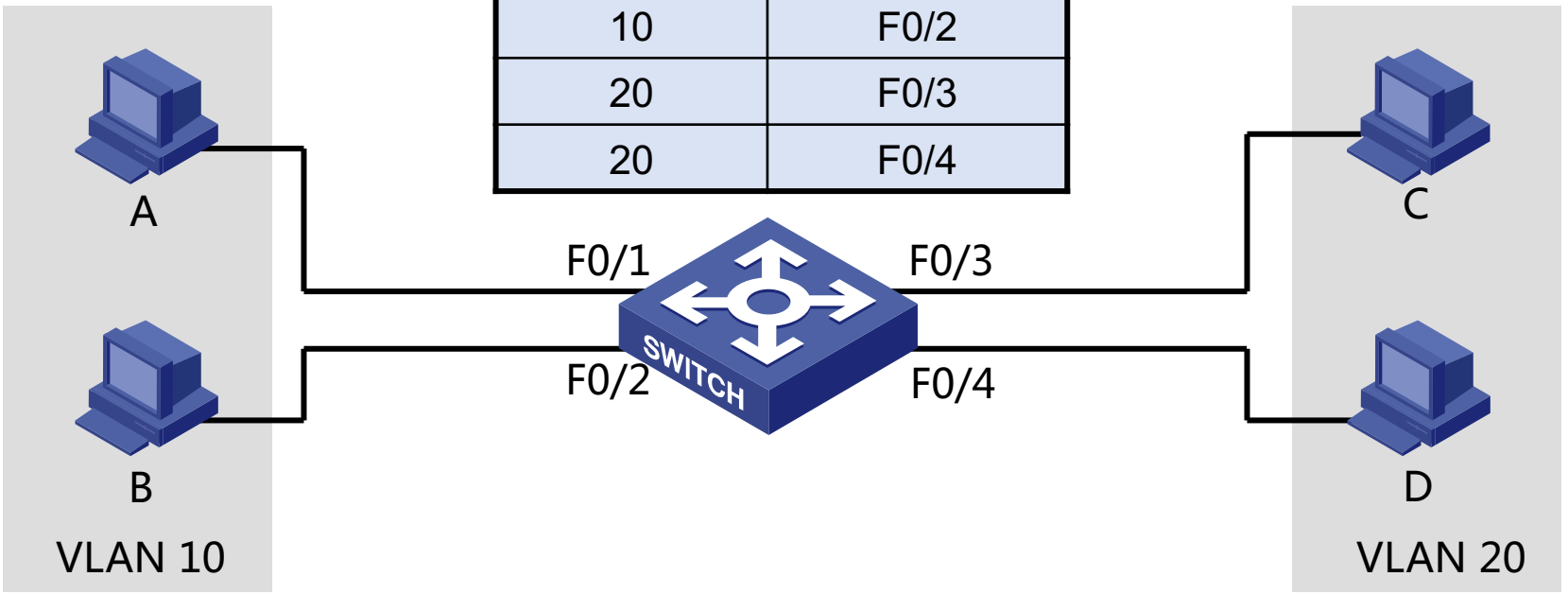
- VLAN类型
  - 基于端口的VLAN（最常见）
  - 基于MAC地址的VLAN
  - 基于协议的VLAN
  - 基于子网的VLAN



虚拟局域网

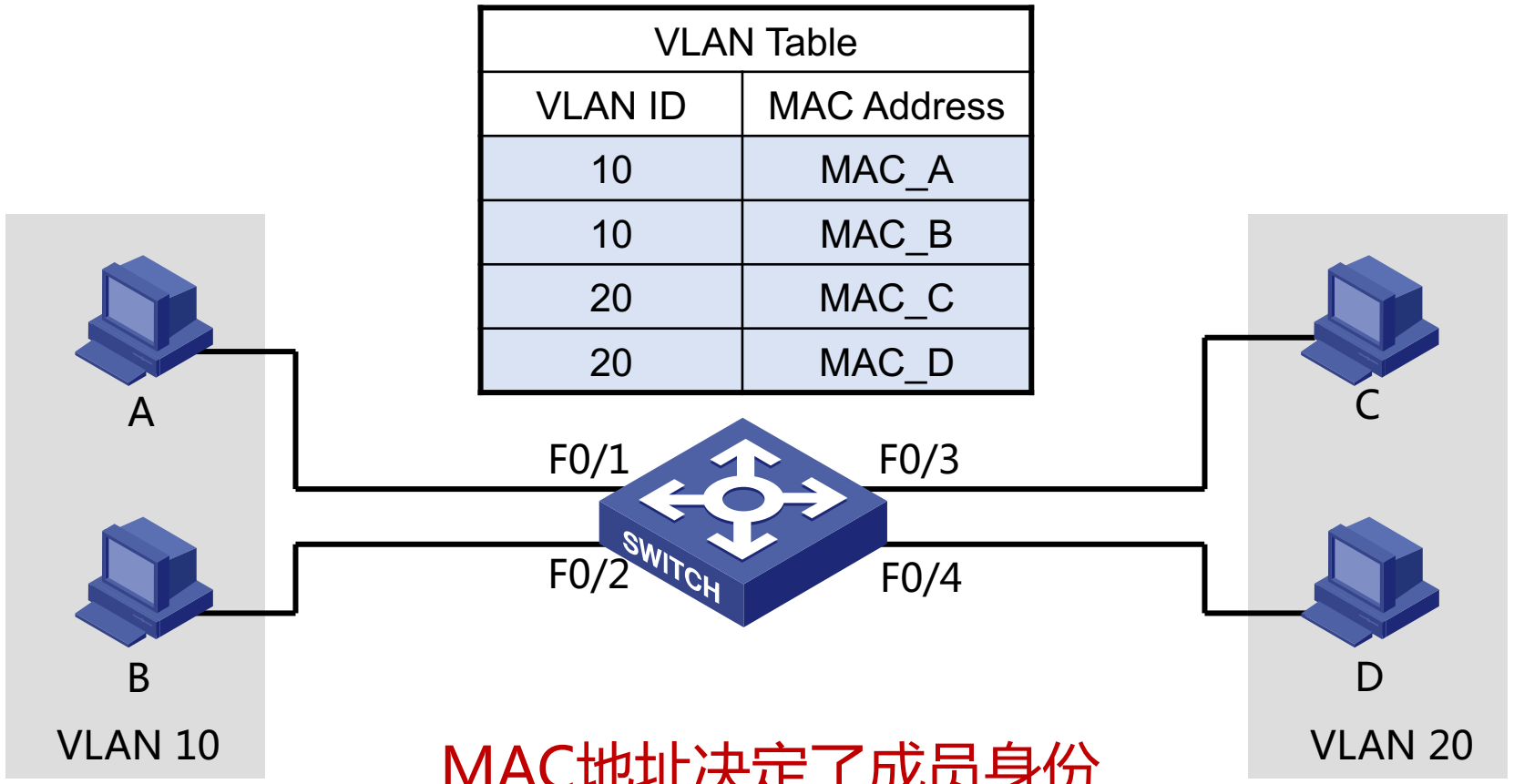
- 基于端口的VLAN
  - 创建VLAN
  - 指定成员端口

VLAN Table	
VLAN ID	Port
10	F0/1
10	F0/2
20	F0/3
20	F0/4



虚拟局域网

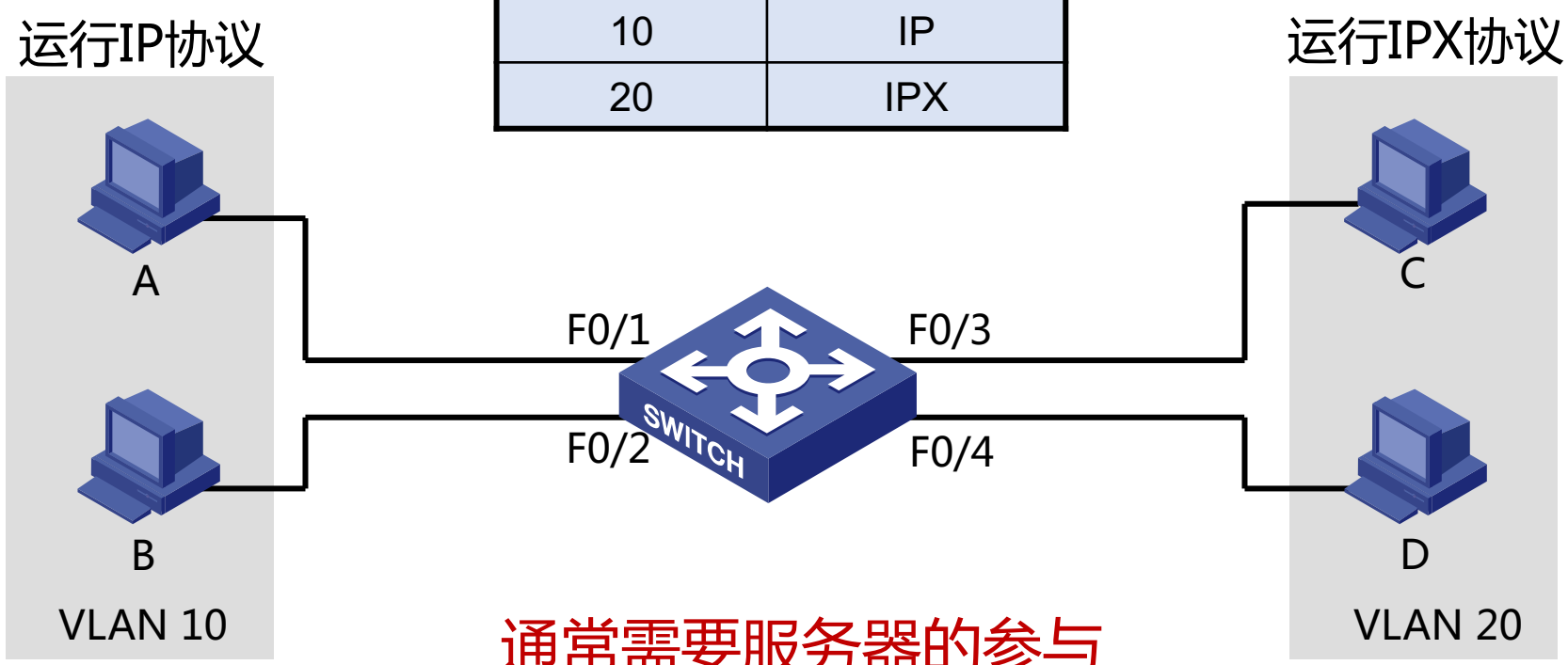
- 基于MAC地址的VLAN



虚拟局域网

- 基于协议的VLAN

VLAN Table	
VLAN ID	Protocol
10	IP
20	IPX

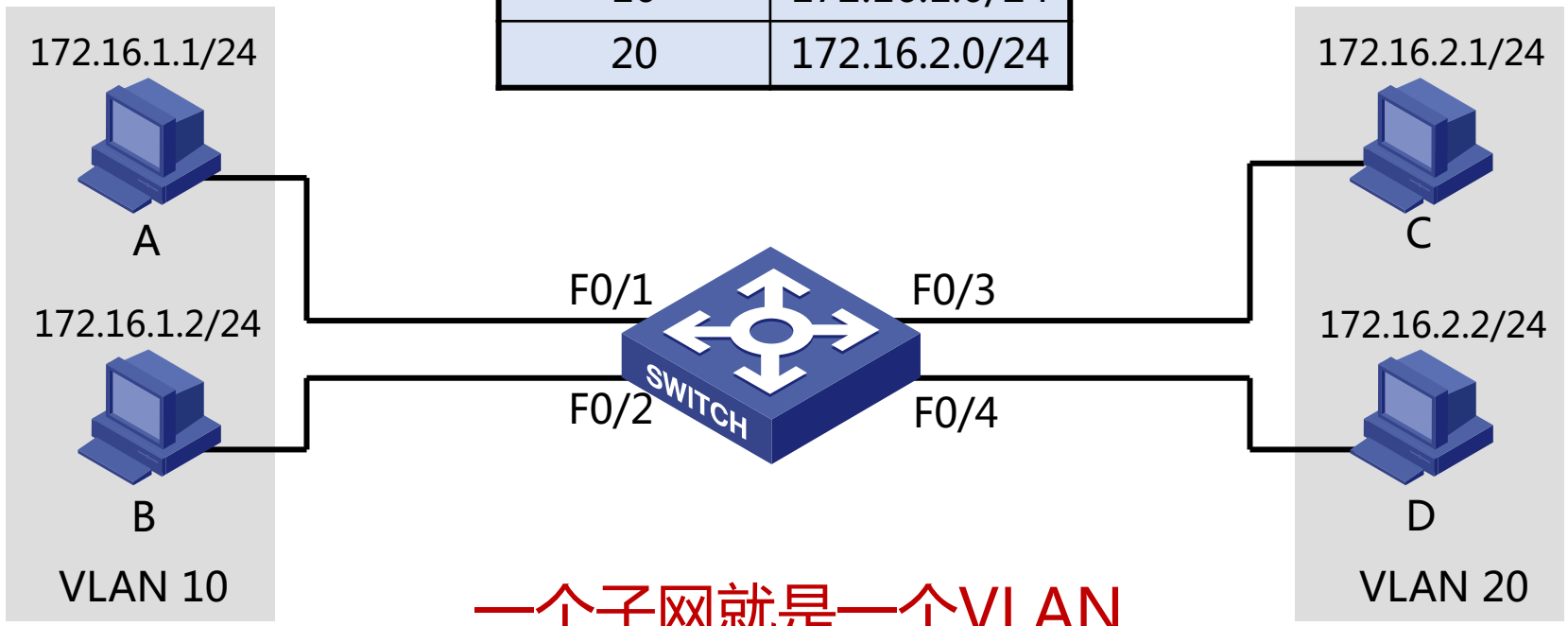


通常需要服务器的参与

虚拟局域网

- 基于子网的VLAN

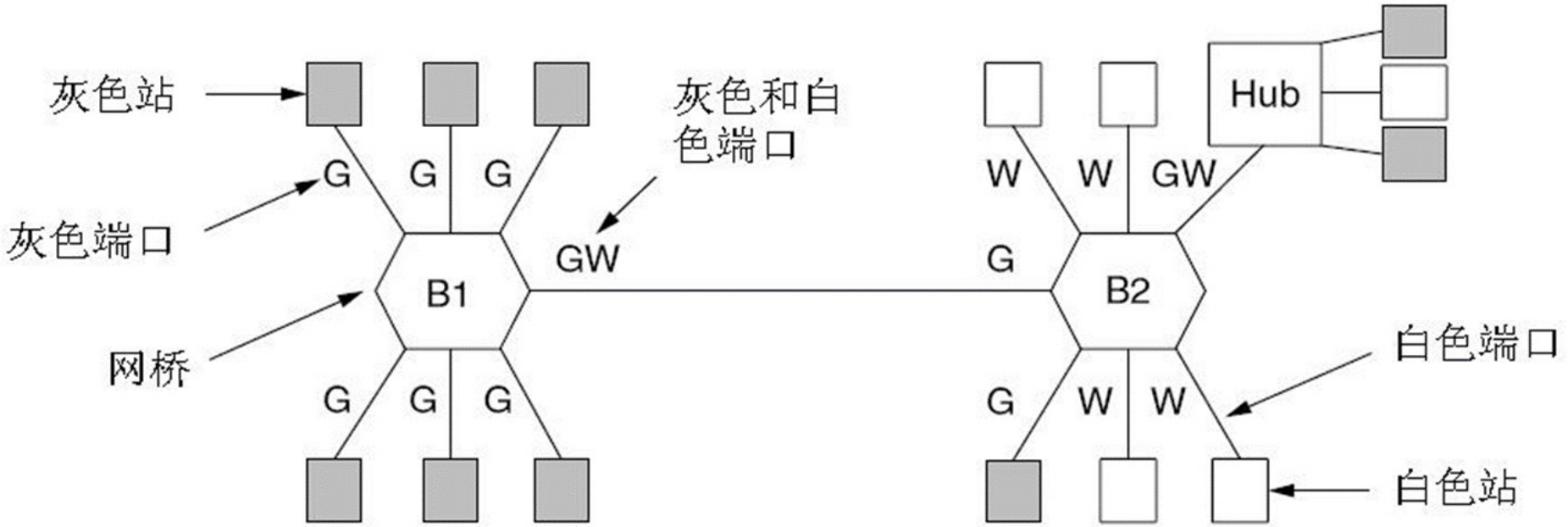
VLAN Table	
VLAN ID	IP子网
10	172.16.1.0/24
20	172.16.2.0/24



一个子网就是一个VLAN

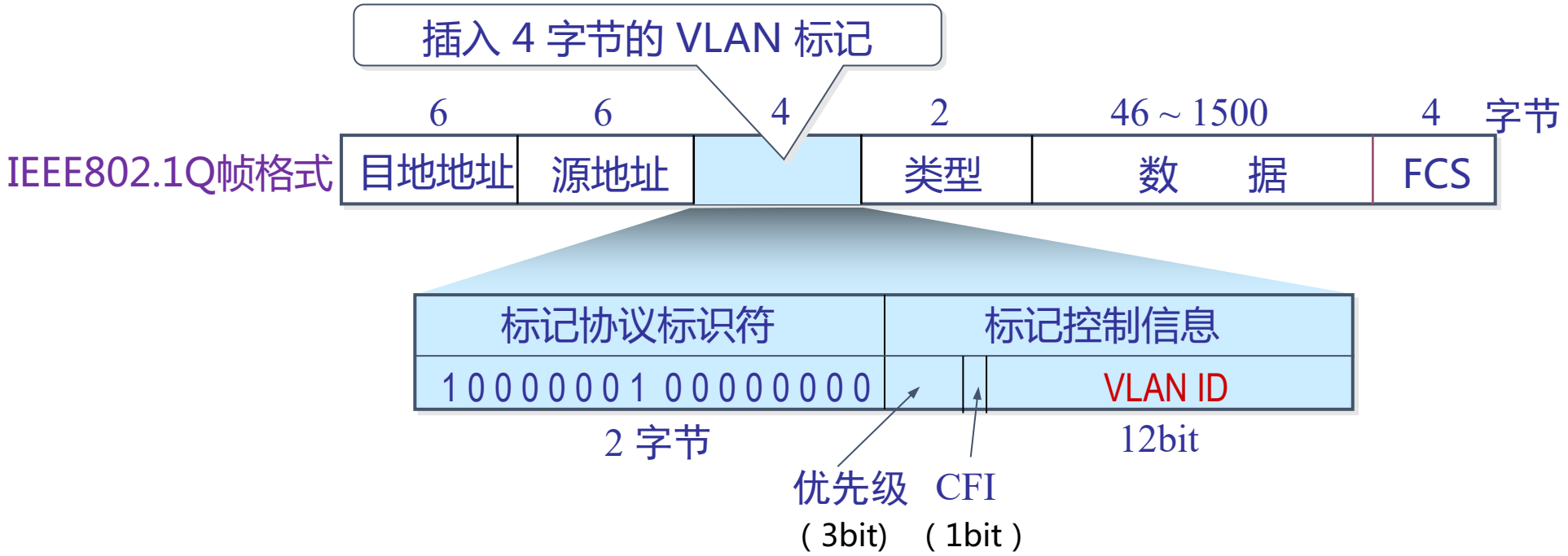
虚拟局域网

- 如何区分不同VLAN的数据帧？
  - 在数据帧中携带VLAN标记；
  - VLAN 标记由交换机添加/剥除，对终端站点透明；



虚拟局域网

- 帧标记标准：IEEE802.1Q
  - 带VLAN标记的帧称为标记帧（Tagged Frame）
  - 不携带VLAN标记的普通以太网帧称为无标记帧（Untagged Frame）

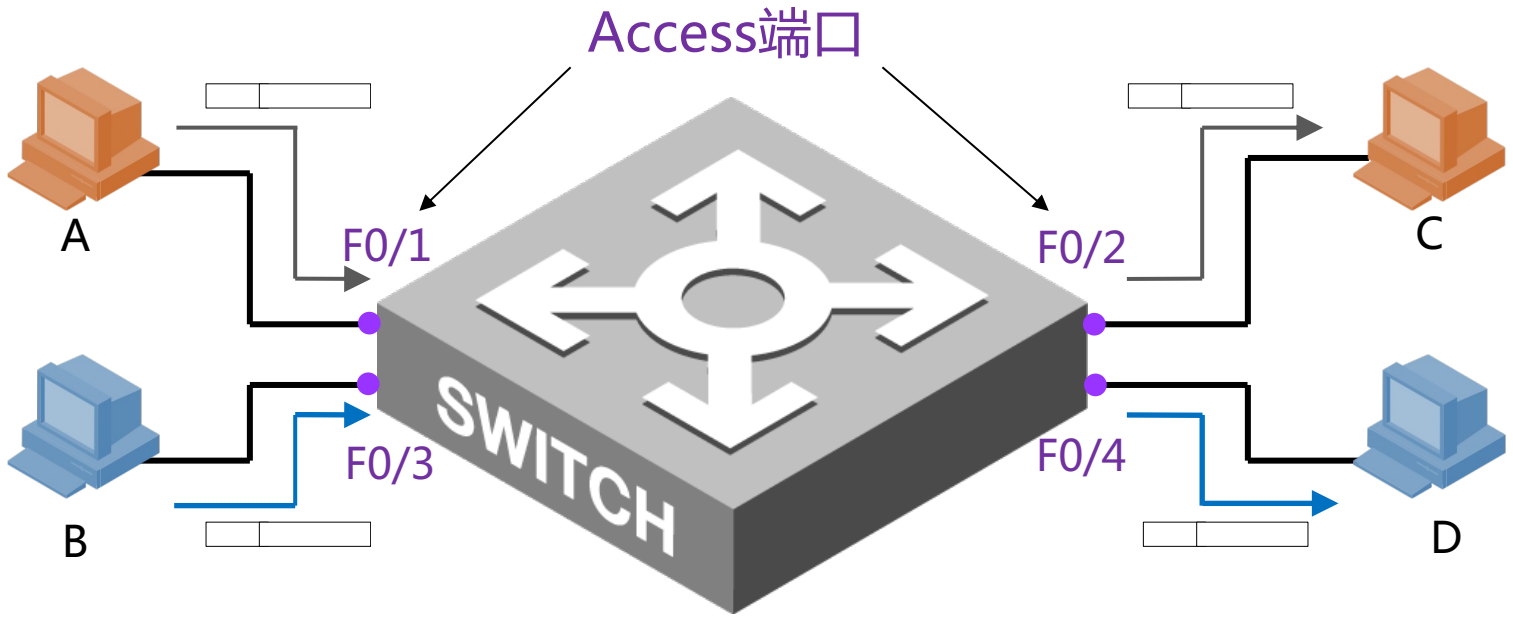


虚拟局域网

➢ Access链路类型端口

- 一般用于连接用户设备（无需识别802.1Q帧的设备）；
- 如何采用基于端口的VLAN划分，Access端口只能加入一个VLAN；
- 一旦Access端口加入了特定的VLAN，连接在该端口的设备被视为属于该VLAN。

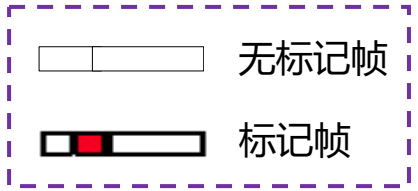
VLAN Table	
VLAN ID	Port
10	F0/1
10	F0/2
20	F0/3
20	F0/4



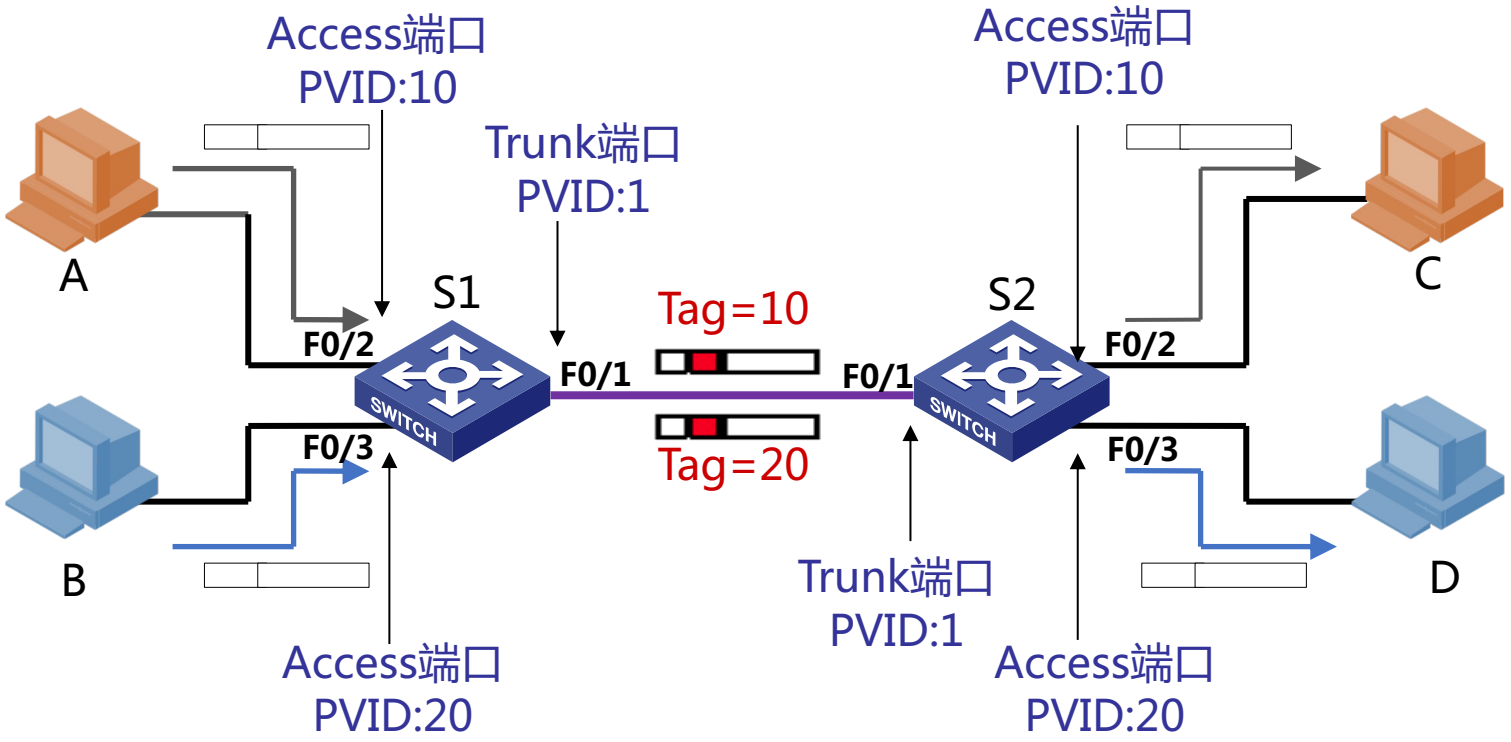
虚拟局域网

➢ Trunk链路类型端口与Trunk链路

- Trunk端口一般用于交换机之间连接；
- 干道链路允许多个VLAN的流量通过。



S1 VLAN Table	
VLAN ID	Port
10	F0/2
20	F0/3



S2 VLAN Table	
VLAN ID	Port
10	F0/2
20	F0/3

虚拟局域网

- VLAN优点
  - 有效控制广播域范围
    - 广播流量被限制在一个VLAN内；
  - 增强网络的安全性
    - VLAN间相互隔离,无法进行二层通信,不同VLAN需通过三层设备通信；
  - 灵活构建虚拟工作组
    - 同一工作组的用户不必局限于同一物理范围；
  - 提高网络的可管理性
    - 将不同的业务规划到不同VLAN便于管理。