第4章 介质访问子层

- 信道分配问题
- 多路访问协议**CSMA**
- 以太网
- 数据链路层交换
- 无线局域网

信道分配问题

- 信道的静态分配
- 信道的动态分配

信道的静态分配

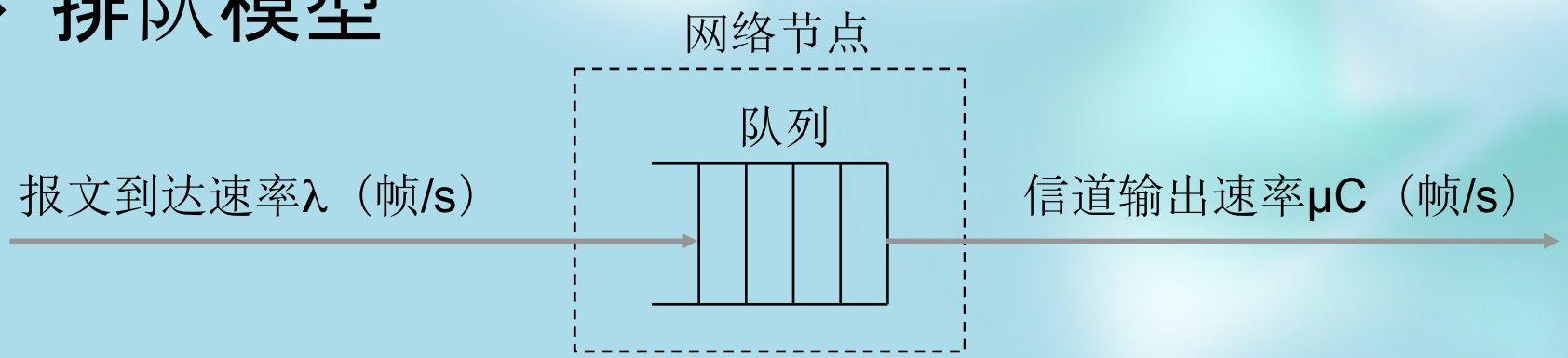
- 频分多路复用FDM
  （Frequency Division Multiplexing）
- 时分多路复用TDM
  （Time Division Multiplexing）
- 静态分配的问题
  - 延迟时间长
  - 信道利用率低

排队论模型

❖ 模型假设

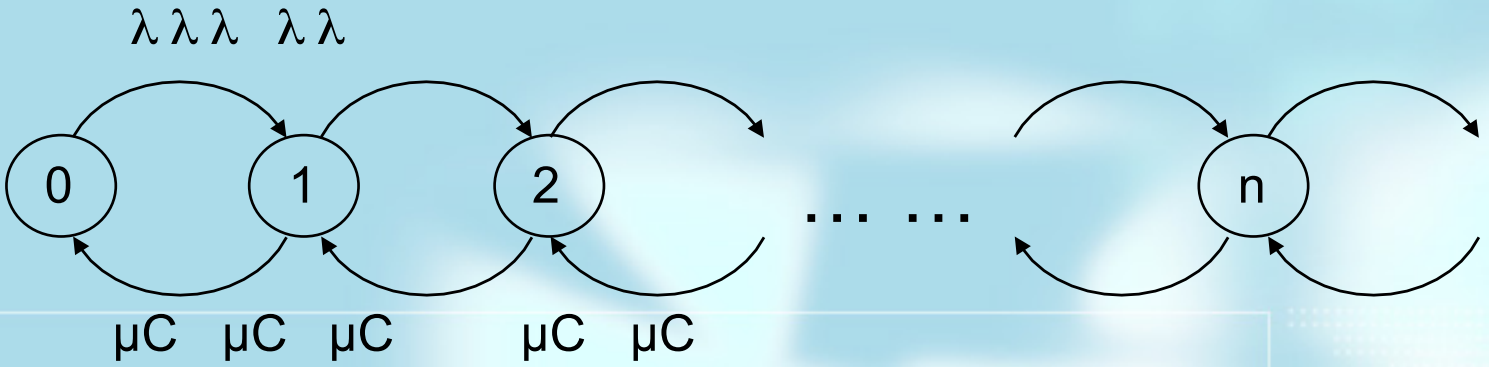
信道容量	C b/s
信道数据到达平均速率（服从泊松分布）	λ 帧/秒
帧的长度平均值（服从指数分布）	1/μ bit/帧
平均延时	T

❖ 排队模型



生灭过程

- 一个稳定的生灭过程



如该过程稳定，则

$\lambda p_0=\mu C p_1$ ①

$\lambda p_1+\mu C p_1=\lambda p_0+\mu C p_2$ ②

$\lambda p_2+\mu C p_2=\lambda p_1+\mu C p_3$ ③

… …

解得： $p_i=p_0\rho^i$

其中： $\rho=\lambda/(\mu C)$

则： $p_0=1-\rho$

则系统中的平均顾客数

$$N=\sum_{i=0}^{\infty} ip_i=\frac{\rho}{1-\rho}$$

Little定理

- 在稳定状态下，存储在网络中的报文平均数，等于报文的平均到达率乘以这些报文在网络中经历的平均时间

即：$N = \lambda T$

则：$$N = \frac{\rho}{1-\rho} = \frac{\lambda / \mu C}{1-(\lambda / \mu C)} = \lambda T$$

得：$$T = \frac{1}{\mu C - \lambda}$$

在频分多路复用条件下，每个信道的容量为C/N，每个信道的报文到达率为λ/N

所以：$T_{FDM} = NT$　　即平均增加N倍

静态FDM的性能

- 频段分成N段，平均延时增加N倍
- 频段分成N段，当用户数小于N时，不产生争用，但并非每个被分配的用户每时每刻都在通信，所以，信道的利用率较低，且不能调整

时分多路复用TDM（Time-Division Multiplexing）与FDM相似

信道分配问题

- 信道的静态分配
- 信道的动态分配

信道的动态分配

有关动态分配的五个假设：

- 站模型(Station Model)
- 单信道假设(Single Channel Assumption)
- 冲突假设(Collision Assumption)
- 时间假设:
  - 时间连续（Continuous Time）
  - 时间分时隙（Slotted Time）
- 侦听假设:
  - 载波侦听（Carrier Sense）
  - 非载波侦听（no Carrier Sense）

站模型

- 由N个独立的站(计算机、电话、个人通信设备)组成
- 每个站都可产生待发送的帧
- 在时间Δt内，生成一帧的概率为λΔt，其中λ是常量(新帧到达速率)
- 一旦生成一帧，就等待发送，直到成功发送

各站都是相互独立地、都以固定速率产生数据帧，某站一旦产生新帧，即被阻塞，亦即不会再有新的帧产生，每个站只有一个用户

信道的动态分配

有关动态分配的五个假设：

- 站模型(Station Model)
- 单信道假设(Single Channel Assumption)
- 冲突假设(Collision Assumption)
- 时间假设:
  - 时间连续（Continuous Time）
  - 时间分时隙（Slotted Time）
- 侦听假设
  - 载波侦听（Carrier Sense）
  - 非载波侦听（no Carrier Sense）

单信道假设

- 所有通信，包括发送和接收，都通过单信道进行
- 所有的站都在该信道上发送或接收信息
- 所有站都是平等的，各站没有主从之分

信道是共享的，任何时刻只允许一个站点可以发送，并且任何站点都必须通过竞争才能取得发送权（如有主从之分，则存在单点故障）

信道的动态分配

有关动态分配的五个假设：

- 站模型(Station Model)
- 单信道假设(Single Channel Assumption)
- 冲突假设(Collision Assumption)
- 时间假设:
  - 时间连续（Continuous Time）
  - 时间分时隙（Slotted Time）
- 侦听假设
  - 载波侦听（Carrier Sense）
  - 非载波侦听（no Carrier Sense）

冲突假设

- 如两帧同时发送，则发生冲突
- 所有的站点都能检测到冲突
- 冲突的帧必须重发，除了冲突引起的差错外，没有其它差错

由于每个站点都必须通过竞争才能取得发送权，所以冲突是不可避免的，但在某些共享信道中采用特殊的机制来消除冲突（令牌网）

信道的动态分配

有关动态分配的五个假设：

- 站模型(Station Model)
- 单信道假设(Single Channel Assumption)
- 冲突假设(Collision Assumption)
- 时间假设:
  - 时间连续（Continuous Time）
  - 时间分时隙（Slotted Time）
- 侦听假设
  - 载波侦听（Carrier Sense）
  - 非载波侦听（no Carrier Sense）

时间假设

- 时间连续(**Continuous Time**)

  帧的发送可在任意时刻

- 时间分时隙(**Slotted Time**)

  时间被分为时隙，帧只能在时隙的开始处发送，一个时隙中可发送0、1或多帧，在一个时隙的开始处，如果只有一个站点发送则成功，如有多个站点发送则将发生冲突

信道的动态分配

有关动态分配的五个假设：

- 站模型(Station Model)
- 单信道假设(Single Channel Assumption)
- 冲突假设(Collision Assumption)
- 时间假设:
  - 时间连续（Continuous Time）
  - 时间分时隙（Slotted Time）
- 侦听假设
  - 载波侦听（Carrier Sense）
  - 非载波侦听（no Carrier Sense）

侦听假设

- 载波侦听(**Carrier Sense**)

  所有的站在使用信道前，都可检测到当前信道是否正被使用，如信道正忙，则等待

- 非载波侦听(**no Carrier Sense**)

  所有的站在使用信道前，都不检测当前信道是否正被使用，只是盲目发送

在局域网中，常采用载波侦听

第4章 介质访问子层

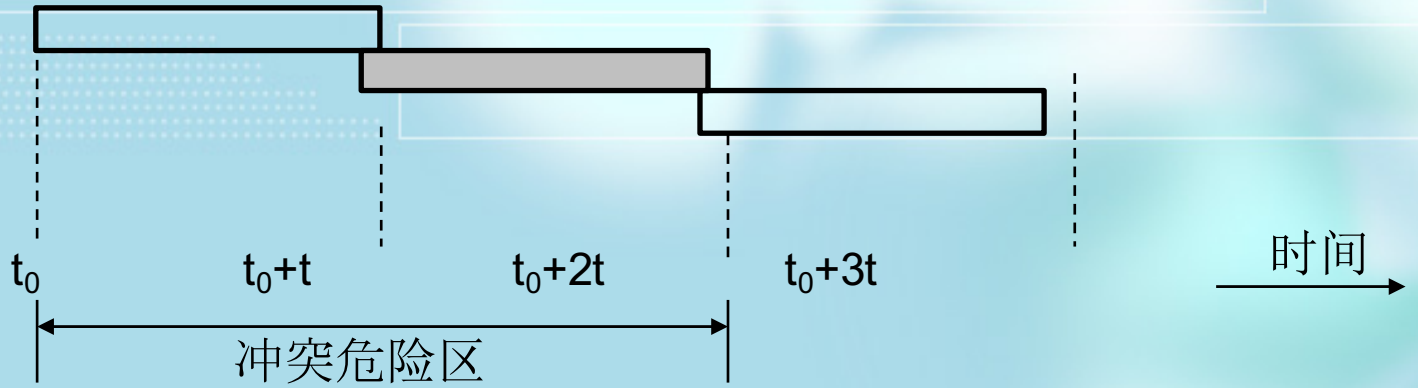
- 信道分配问题
- 多路访问协议**CSMA**
- 以太网
- 数据链路层交换
- 无线局域网

多路访问协议CSMA

- 纯ALOHA
- 分隙ALOHA
- 载波侦听多路访问协议

纯ALOHA的原理

- 在纯**ALOHA**中，站点一旦产生新帧则立即发送，如果一个标准长度的帧的发送时间为**t**，在t_0+**t**时刻允许生成一个新帧，除此新帧之外，在$t_0 \sim t_0$+**2t** 时间内不能有其它帧产生，否则冲突，即冲突危险区为**2t**



Tnbm P253 Fig. 4-2 阴影帧的冲突危险区

纯ALOHA的原理（续）

- 任何一个站都可以在帧生成后立即发送(可能冲突)，并通过信号的反馈，检测信道，以确定发送是否成功，如发送失败，则经随机延时后再发送

纯ALOHA信道的效率

帧时(Frame Time)：发送一个标准长度的帧所需的时间

设:**无限多个用户产生新帧的概率服从泊松分布**

平均每个帧时产生S个新帧

则： **当S > 1时，将每个帧都冲突**

所以，吞吐率应为 0 < S < 1

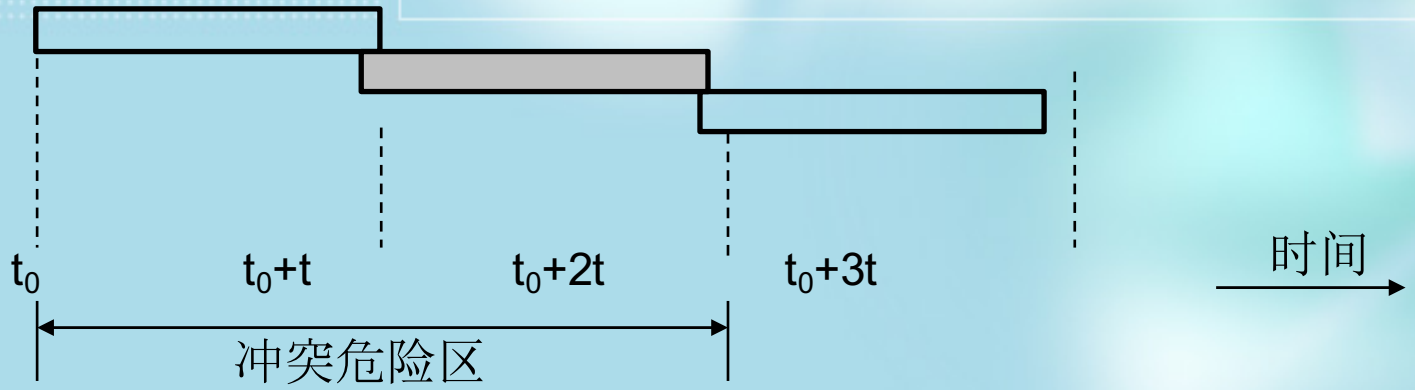
除新帧外，凡冲突的帧也要重发

纯ALOHA信道的效率（续）

设：帧发送的平均值为G帧/帧时， G中包括每个帧时内产生的新帧S和由于冲突而需重发的帧

当轻负载(S << 1 → 0)时，几乎无冲突，则G ≈ S

当重负载(S → 1)时，冲突频繁，则G > S



纯ALOHA的吞吐率

设：在任一帧时内生成k帧（包括新旧帧）的概率服从泊松分布，为：

$$P_k = \frac{G^k}{k!}e^{-G}$$

则：生成0帧的概率为$P_0 = e^{-G}$

两个帧时内产生的平均帧数为2G

即：$P_k = \frac{(2G)^k}{k!}e^{-2G}$，$P_0 = e^{-2G}$

由于$S = GP_0$

所以$S = Ge^{-2G}$

纯ALOHA的吞吐率（续）

对于：$S = Ge^{-2G}$

得：$S' = e^{-2G} + Ge^{-2G}(-2)$ 并令其为0

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

$$2G = 1$$

G = 0.5时，S有最大值

$$S = 1/(2e)$$

$$S \approx 0.184$$

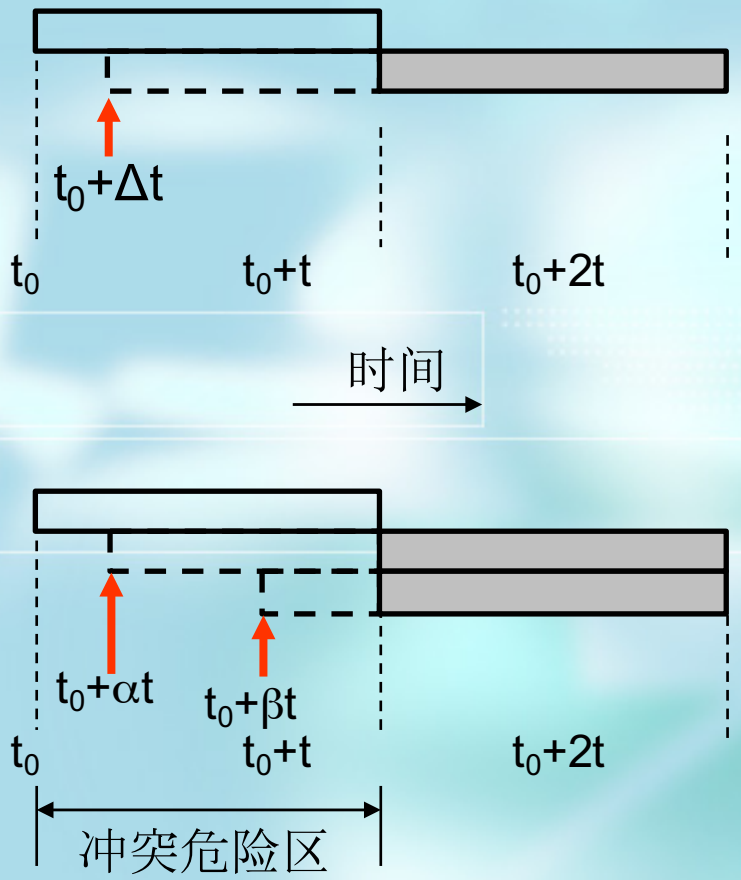
在纯ALOHA中，其吞吐率最大为0.184

多路访问协议

- 纯**ALOHA**
- 分隙**ALOHA**
- 载波侦听多路访问协议

分隙ALOHA的原理

- 在一个时隙内只产生一个新帧，新帧不允许立即发送，将在下一个时隙的开始处 t_0+t 时发送，不会发生冲突
- 在一个时隙内产生一个以上新帧，下一个时隙的开始处 t_0+t 时，一个以上的帧同时发送，将发生冲突，即冲突危险区为t



分隙ALOHA的原理（续）

- 分隙ALOHA的时间以时隙(Time Slot)为单位
- 时隙的长度对应一帧的传输时间，其起点由专门的信号来标志
- 新帧的产生是随机的，但分隙ALOHA不允许随机发送，凡帧的发送必须在时隙的起点，即冲突危险区是原来的一半

  冲突主要发生在时隙的起点处，一旦发送成功，则不会出现冲突，即生成新帧并等待发送的这一帧时内，是冲突危险区，时间长度为t，是原来的一半

分隙ALOHA的吞吐率

- 在一个时隙的起点没有其它帧发送的概率为: $P_0 = e^{-G}$

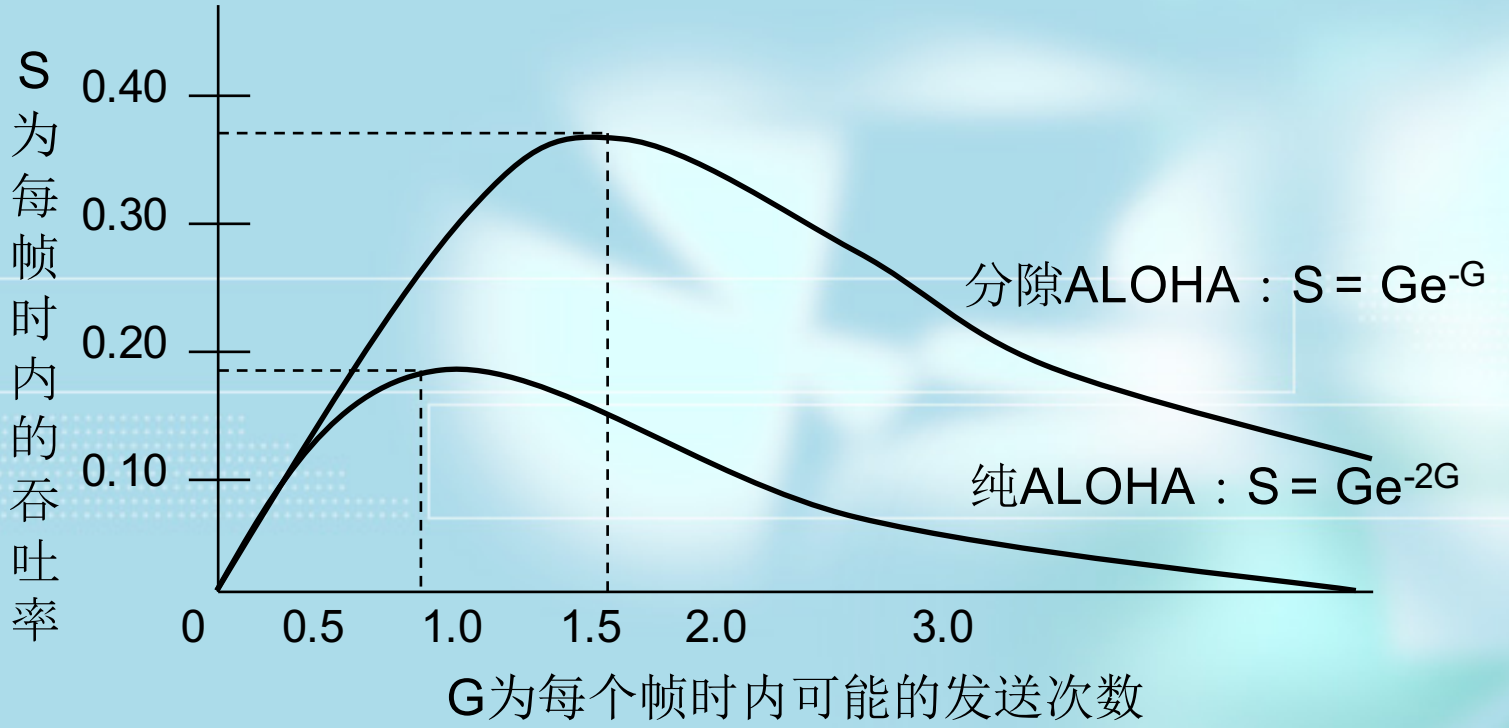
  所以: $S = GP_0 = Ge^{-G}$

- 当G = 1时，吞吐量S为最大 $S \approx 0.368$

纯ALOHA和分隙ALOHA的比较

- 纯ALOHA中，一旦产生新帧，就立即发送，全然不顾是否有用户正在发送，所以发生冲突的可能伴随着发送的整个过程
- 分隙ALOHA中，规定发送行为必须在时隙的开始，一旦在发送开始时没有冲突，则该帧将成功发送

纯ALOHA和分隙ALOHA的比较（续）



Tnbm P254 Fig. 4-3 ALOHA系统中吞吐率和帧产生率之间的关系

多路访问协议

- 纯**ALOHA**
- 分隙**ALOHA**
- 载波侦听多路访问协议

载波侦听多路访问协议CSMA

- 载波侦听协议(**Carrier Sense Protocol**)
- **持续和非持续CSMA（Carrier Sense Multiple Access**，载波侦听多路访问）
  - **1 – 持续CSMA**
  - **非持续CSMA（Nonpersistent CSMA）**
  - **p – 持续CSMA（p-persistent CSMA）**
- **CSMA**协议的冲突和冲突检测

1 – 持续CSMA

- 每个站在发送前，先侦听信道，如信道正忙，则等待并持续侦听，一旦信道空闲，立即发送，即发送的概率为1；如冲突，则延时一随机时隙数后，重新发送

载波侦听多路访问协议CSMA

- 载波侦听协议(Carrier Sense Protocol)
- 持续和非持续CSMA（Carrier Sense Multiple Access，载波侦听多路访问）
  - 1 – 持续CSMA
  - 非持续CSMA（Nonpersistent CSMA）
  - p – 持续CSMA（p-persistent CSMA）
- CSMA协议的冲突和冲突检测

非持续CSMA（Nonpersistent CSMA）

- 每个站在发送前，先侦听信道，如信道正忙，则不再继续侦听，而是延时一随机时隙数后，再侦听信道

载波侦听多路访问协议CSMA

- 载波侦听协议(Carrier Sense Protocol)
- 持续和非持续CSMA（Carrier Sense Multiple Access，载波侦听多路访问）
  - 1 – 持续CSMA
  - 非持续CSMA（Nonpersistent CSMA）
  - p – 持续CSMA（p-persistent CSMA）
- CSMA协议的冲突和冲突检测

p – 持续CSMA（p-persistent CSMA）

- 用于分隙信道
- 先侦听信道，如信道正忙，则等到下一时隙；如信道空闲，则以概率p发送，而以概率q=(1-p)把本次发送延至下一时隙，直至发送成功

载波侦听多路访问协议CSMA

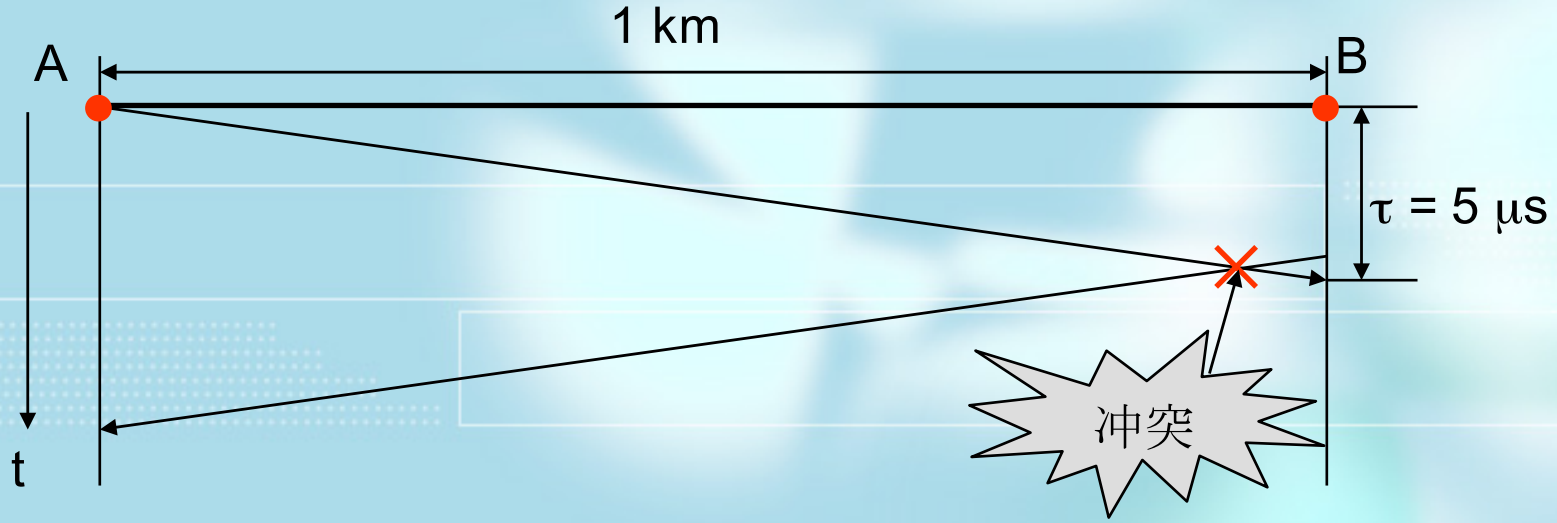
- 载波侦听协议(Carrier Sense Protocol)
- 持续和非持续CSMA（Carrier Sense Multiple Access，载波侦听多路访问）
  - 1 – 持续CSMA
  - 非持续CSMA（Nonpersistent CSMA）
  - p – 持续CSMA（p-persistent CSMA）
- CSMA协议的冲突和冲突检测

CSMA协议的冲突和冲突检测

- 带冲突检测的CSMA
- 无冲突的多路访问协议
- 有限竞争协议

传播时延对载波侦听的影响

- **CSMA并不能完全解决冲突问题**



如两个或多个准备发送的站都检测到信道空闲而同时发送将发生冲突

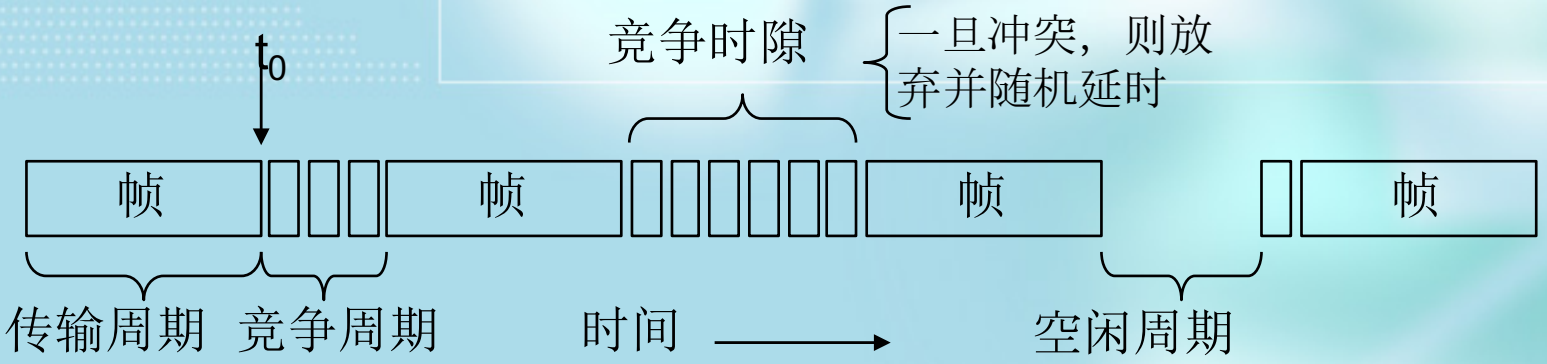
带冲突检测的CSMA

- **CSMA/CD**

  Carrier Sense Multiple Access / Collision Detection

  带冲突检测的载波侦听多路访问

  CSMA/CD的概念模型：



Tnbm P258 Fig. 4 – 5 CSMA/CD有三种状态：竞争、传输或空闲

CSMA/CD的要点

- 在一帧传输完成后的时刻t_0，想要发送的站点都可以尝试发送
- 如两个或多个站点同时发送则发生冲突
- 判断出冲突后，立即停止发送，并延时一个随机时隙数后，通常其中的一个站点将发送成功

冲突的检测

- 信号电平法

  基于基带传输，两个帧信号叠加后，电压大一倍

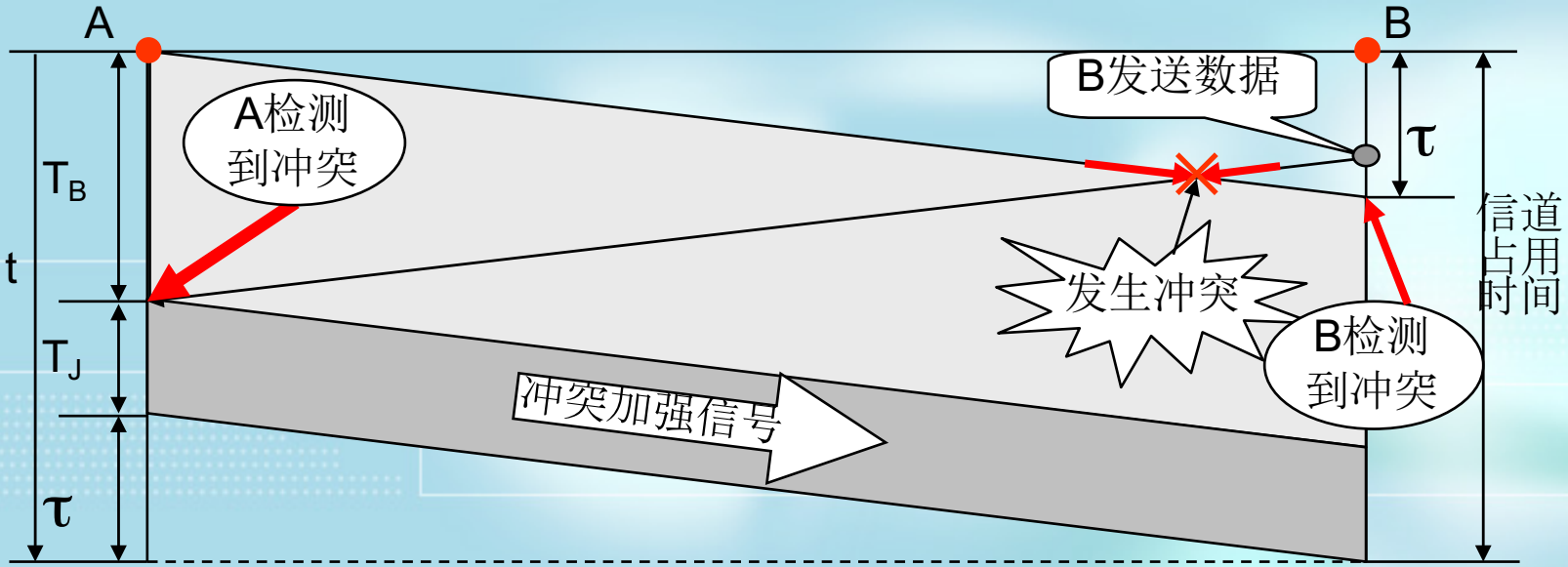
- 过零点检测法

  用曼切斯特编码时，零点在每比特的正中央，当有干扰时，则可能偏移

- 自收自发检测法

  在发送数据的同时也在接收，并逐个比特比较

CSMA/CD发生冲突时对信道占用时间的影响



如一个站点发送并经2τ后，没有冲突，即发送成功

典型地，一公里长的同轴电缆，$\tau \approx 5\mu s$　$2\tau \approx 10\ \mu s$

CSMA协议的冲突和冲突检测

- 带冲突检测的CSMA
- 无冲突的多路访问协议
- 有限竞争协议

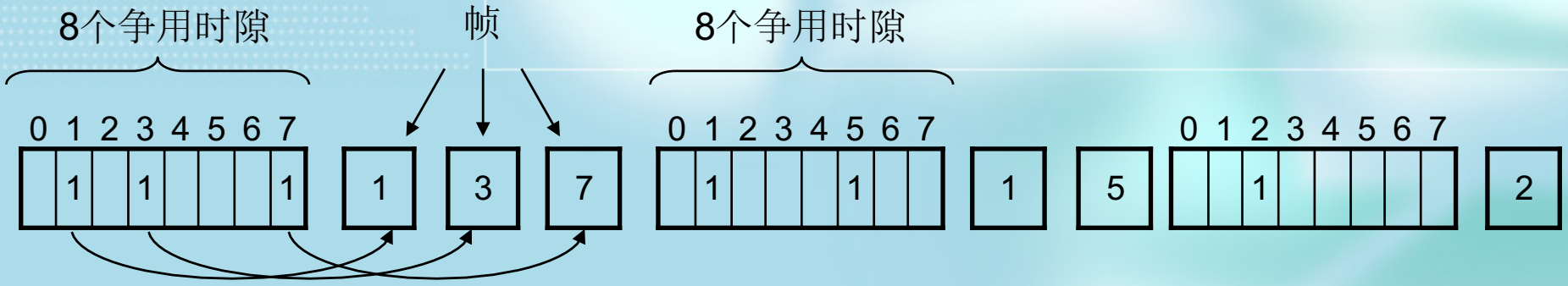
无冲突的协议

信道的争用势必发生冲突，冲突将降低信道的利用率

- 位图协议
- 二进制倒计数法

位图协议

- 如有N个站点共享信道，编号为0 ~ N-1，其竞争周期将分为N个时隙，每个站点占有一个时隙，如某站准备发送，则可在属于它的时隙内填入1，一个竞争周期后，则将按顺序发送，不会产生冲突



Tnbm P259 Fig. 4 – 6　基本位图协议

位图协议的效率分析

- 在低负荷条件下，如每帧的数据量的d bit，额外比特数为N，则效率为d/(d+N)
- 在高负荷条件下，即所有的站都希望一帧接一帧发送，位图按平均分配给每一帧，一帧只占一位，则效率为d/(d+1)

缺点：位图协议无法考虑优先级

无冲突的协议

信道的争用势必发生冲突，冲突将降低信道的利用率

- 位图协议
- 二进制倒计数法

二进制倒计数法

- 需要一个仲裁机构决定哪个站点发送
- 把站号按相同长度的二进制数编号，需要发送的站点逐个按高位到低位在争用周期开始时发送，凡低序号的站点发现有高序号站点也希望发送，则退出竞争，即:高序号站点优先

二进制倒计数法举例

如有四个准备发送的站的站号分别为**0010(2#)**、**0100(4#)**、**1001(9#)**和**1010(10#)**，当争用周期开始后，分别将最高位送出，仲裁机构作或运算结果送回。**2#** 和**4#** 检测到**1**，则知道有高序号的站点也希望发送，则退出竞争，不再发送下一位，**9#** 和**10#** 继续送出次高位，仍不分高下，再继续，**9#** 退出，最后**10#** 得到帧的发送权

信道效率分析

- **N个站的二进制编码所需位数是$\log_2 N$位**
- **信道的效率为：$d/(d+\log_2 N)$**
- 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%

CSMA协议的冲突和冲突检测

- 带冲突检测的CSMA
- 无冲突的多路访问协议
- 有限竞争协议

有限竞争协议

有限竞争协议(Limited Contention Protocol)

即:在低负荷时使用竞争法

在高负荷时使用无冲突法

- 对称竞争协议
  (Symmetric Contention Protocol)
- 适应树搜索协议
  (Adaptive Tree Walk Protocol)

对称竞争协议

- 对称竞争协议的性能：

  每个站申请使用信道的概率相同，都为p

  设：有k个站点参与信道竞争

  每个站点在每个时隙中的发送概率为p

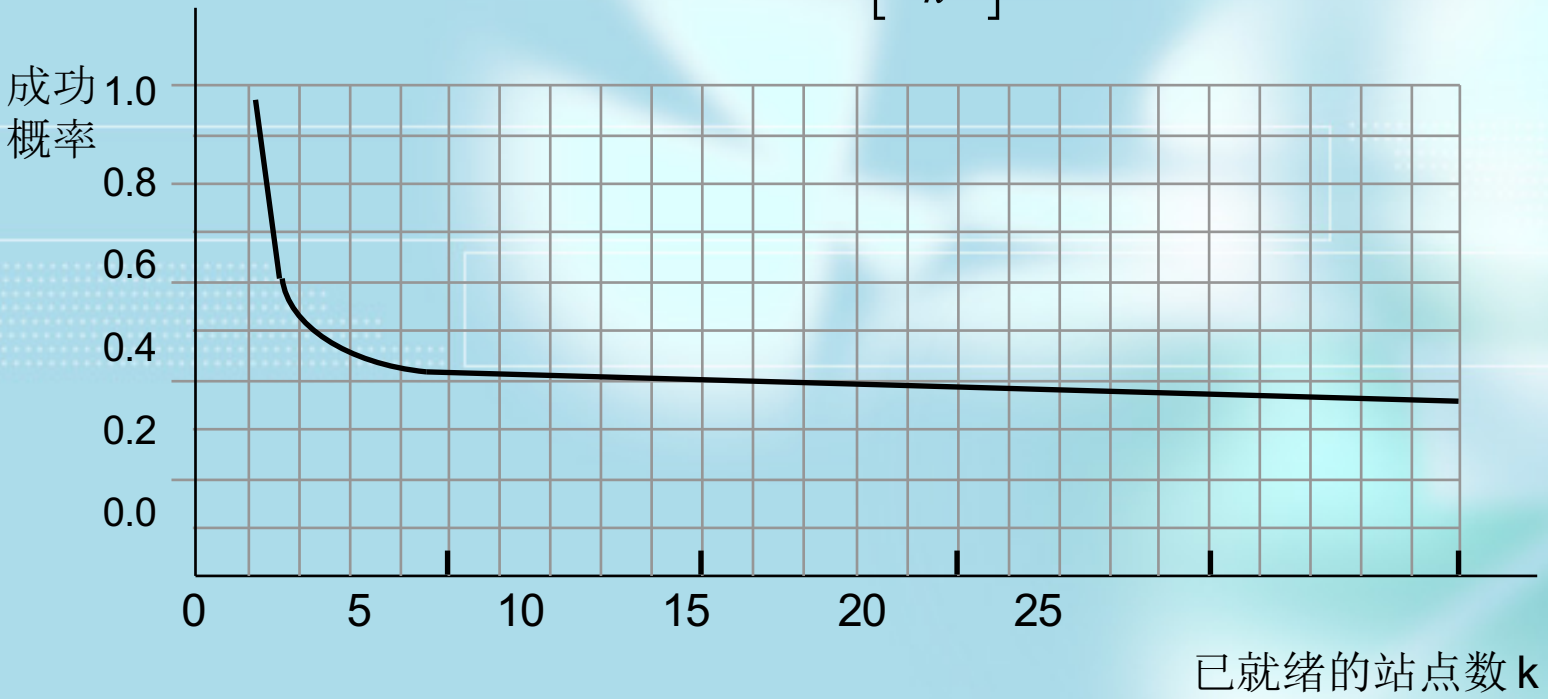
  那么：某个给定时隙内，站点成功获得信道的概率为：

$$k p (1-p)^{k-1}$$

当pk = 1 时成功率最高

- 当pk = 1 时，站点成功获得信道的概率最高

Pr [pk = 1的成功率] $= \left[\frac{k-1}{k}\right]^{k-1}$



Tnbm P263 Fig. 4 – 8　对称竞争信道获取概率

当pk = 1 时成功率最高（续）

- k 较小时，成功率较高；k → ∞ 时，成功率为 1/e
- 当站点数为2 ~ 4时，成功概率急剧下降
- 当站点数达5时，成功概率将逐渐接近1/e

k	2	3	4	5	8	10	∞
Pr [pk = 1]	0.5	0.444	0.422	0.410	0.393	0.387	0.368

有限竞争协议

有限竞争协议(**Limited Contention Protocol**)

即:在低负荷时使用竞争法

在高负荷时使用无冲突法

- 对称竞争协议

  (**Symmetric Contention Protocol**)

- 适应树搜索协议

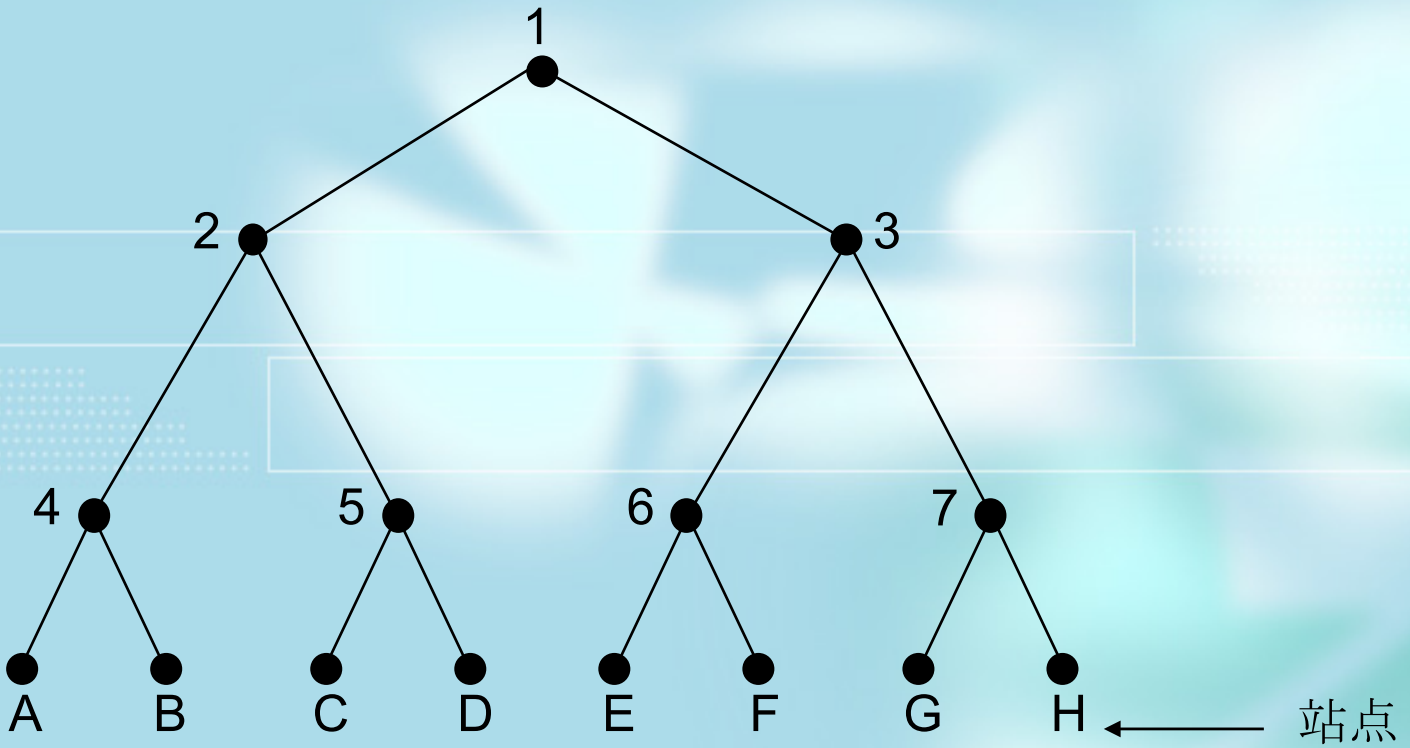
  (**Adaptive Tree Walk Protocol**)

适应树搜索协议

- 适应树搜索协议(**Adaptive Tree Walk Protocol**)
- 在某一次成功传输后的第一个竞争时隙，所有希望发送的站点都允许竞争，如果只有一个站点申请，则获得信道，否则在下一竞争时隙，只允许一半站点参与竞争(递归)
- 即将所有站点构成一棵完全二叉树，对二叉树作深度优先的遍历

8个站点的适应树搜索

- 包含8个站点的适应树搜索举例



Tnbm P264 Fig. 4-9 包含8个站点的树

8个站点的适应树搜索举例

- 如当前有站点G、H请求获得信道
  - 在时隙0，因有两个站点请求获得信道，所以冲突
  - 在时隙1，按深度优先搜索节点2，但发现节点2 所属的站点无信道请求
  - 在时隙2，跳过节点3，搜索节点3 下属节点6，但发现节点6 所属的站点也无信道请求
  - 在时隙3，跳过节点7，搜索节点7 下属节点G，G获得信道

第4章 介质访问子层

- 信道分配问题
- 多路访问协议**CSMA**
- 以太网
- 数据链路层交换
- 无线局域网

以太网

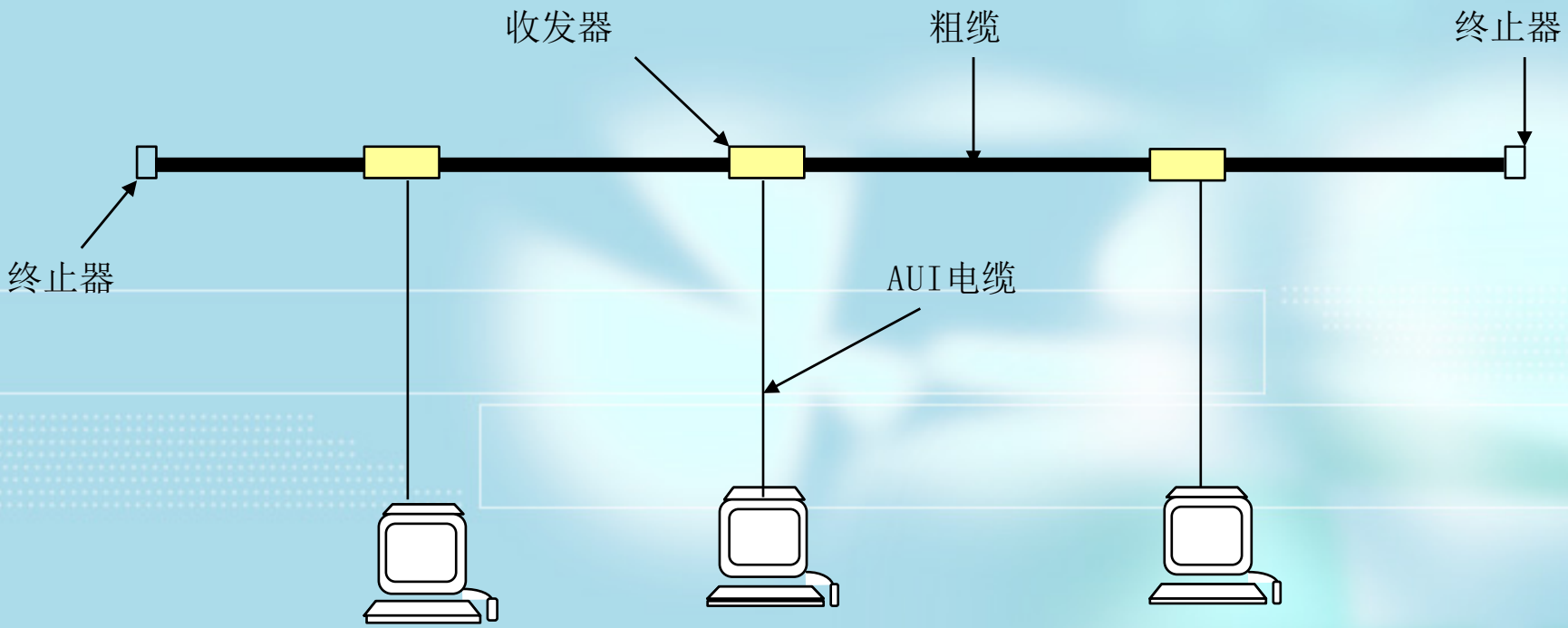
- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

802.3的电缆

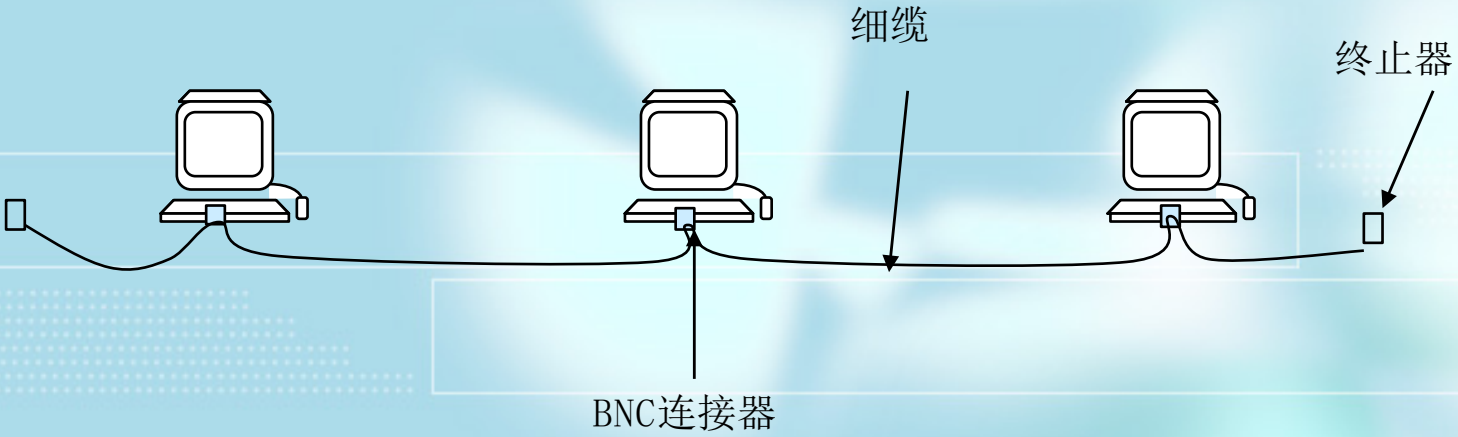
- 传输电缆分以下四种

名称	电缆	最大区间长度	节点数/段	优点	接口
10Base5	粗缆	500m	100	用于主干 已基本淘汰	AUI
10Base2	细缆	185m	30	廉价 已基本淘汰	BNC
10Base-T	双绞线	100m	1024	易于维护	RJ-45
10Base-F	光纤	2km	1024	用于楼间	ST

粗缆以太网（10BASE5）

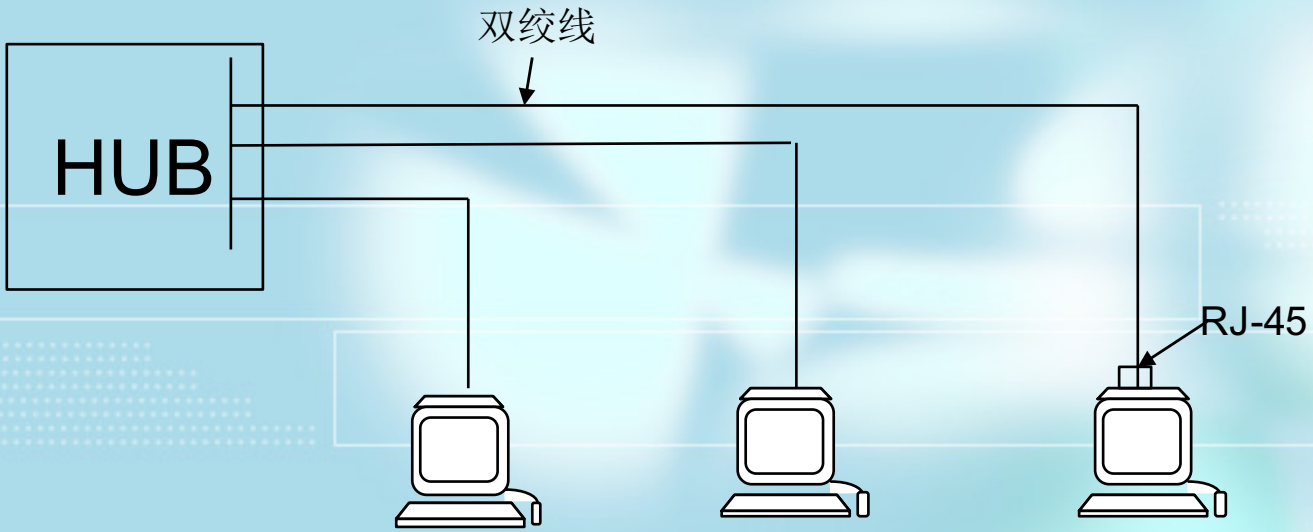


细缆以太网(10BASE2)



双绞线以太网(10BASE-T)

- 其物理接口为**RJ-45**
- 连线采用**3**类(或**5**类)双绞线，仅用两对线，且全双工
- 距离为**100 m**
- 编码采用曼切斯特编码


双绞线
HUB
RJ-45

RJ-45接口接线标准T-568B

- T-568B的直通线缆

Pin	color		name
1		white orange	TxData +
2		orange	TxData -
3		white green	RecvData +
4		blue	
5		white blue	
6		green	RecvData -
7		white brown	
8		brown	

10Base-T 直通线缆

- 交换机（或HUB）的RJ-45端口与主机网卡的RJ-45端口的连接电缆为直通（Straight-Through）的8芯5类线缆

RJ-45插座

Pin	color	name
1	white orange	TxData +
2	orange	TxData -
3	white green	RecvData +
4	blue	
5	white blue	
6	green	RecvData -
7	white brown	
8	brown	

以太网

- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

以太网MAC子层协议

❖ 以太网的帧结构

7	1	2/6	2/6	2	0~1500	0~46	4
先导字段 10101010		目的地址	源地址		数　据	填充字符	校验和

帧开始字符10101011　类型：表示上层使用的协议
如IP协议为800H，ARP协议为806H

❖ 802.3的帧结构

7	1	2/6	2/6	2	0~1500	0~46	4
先导字段 10101010		目的地址	源地址		数　据	填充字符	校验和

帧开始字符10101011　　数据字段长度

帧结构字段说明

- 先导字段
- 两个地址
- 数据字段长度
- 校验和
- 填充字段

先导字段

- 7个字节的10101010，实际上下一个字符也是先导字段，只是最后的两位为1，表示紧接着的是真正的MAC帧
- 8个字节的10101010的曼切斯特编码将产生10MHz，持续6.4μs的方波，周期为0.1μs，可用于时钟同步

帧结构字段说明

- 先导字段
- 两个地址
- 数据字段长度
- 校验和
- 填充字段

两个地址

- 目的地址和源地址都允许为2字节或6字节，在10M bps的基带以太网中是6字节
- 目的地址最高位为0：普通地址

  1：多点发送（Multicast）

  目的地址全1：广播发送（Broadcast）
- 在6个字节（共48位）的地址中有46位用于地址的指定，即有$2^{46}=7.03687\times10^{13}$个地址
- 网卡地址是一个全局地址

  如：44-45-53-54-00-00

帧结构字段说明

- 先导字段
- 两个地址
- 数据字段长度
- 校验和
- 填充字段

数据字段长度和校验和

- 指明数据的字节数，数据字段长度允许为0
- 4个字节共32位的CRC码

帧结构字段说明

- 先导字段
- 两个地址
- 数据字段长度
- 校验和
- 填充字段

填充字段

- 为保证帧的最短长度为64个字节

即：在数据字段长度为0时

两个地址（12字节）+ 类型 或 数据长度（2个字节）+ 填充字节+校验和（4个字节）= 64

18字节+ 填充字节 = 64

填充字节 = 46

所以填充字节为:0 ~ 46字节

为什么帧的最短长度为64个字节

- 为了确认发送帧是否正确到达目的站点，必须保证可能的冲突信号返回时帧的发送尚未结束，如在2τ 内没有冲突信号返回，则发送成功，如果发送端在2τ时间内帧已经发送结束，则即使冲突也无法检测，即最短帧长应与2τ相当

2τ的计算

- 在极限条件下，802.3局域网中发送方和接收方间允许接有4个中继器，最大距离为2500 m，往返5000 m，同轴电缆的传播时延特征为5 μs/km（相当于电磁波以2/3的光速在电缆上传播），即如遇冲突，端到端并返回的时延为25μs。然而这是理想的时延，考虑到中继器的额外时延，最坏的情况下估计时延为45μs，再加上强化冲突需发送的48bit，接收方需收到48bit 后才确认冲突，即再增加了4.8 μs，共49.8 μs。再考虑 2的整次幂的因素，所以通常取51.2 μs为争用时隙的时间长度（51.2 μs即传输512 bit，即64字节所耗费的时间），所以帧的长度至少为64个字节

以太网

- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

二进制指数后退算法

- 发送方在检测到冲突后，双方(或多方)都将延时一段时间，所谓一段时间到底是多长?
- 检测到冲突后，时间被分成离散的时隙
- 时隙的长度等于信号在介质上往返的传播时间（在以太网中，一个时隙，即2 τ为51.2μs ）
- 一般地，经i次冲突后，发送站点需等待的时隙数将从0 ~ 2^i - 1中随机选择

二进制指数后退算法举例

在一个时隙的起始处，两个CSMA/CD站点同时发送一个帧，求前4次竞争都冲突的概率？

- 第一次竞争冲突的概率为1；
- 第一次冲突后，A、B都将在等待0个或1个时隙之间选择，选择的组合有：00、01、10、11，共4种，其中00和11将再次冲突，所以第二次竞争时，冲突的概率为0.5
- 第二次冲突后：A、B都将在0、1、2、3之间选择，选择的组合有：00、01、02、03、10、11、12、13、20、21、22、23、30、31、32、33共16种，其中00、11、22、33将再次冲突，所以第三次竞争时，冲突的概率为0.25
- 第三次冲突后：A、B都将在0、1、2、3、4、5、6、7之间选择，选择的组合共有64种，其中00、11、……、77将再次冲突，所以第四次竞争时，冲突的概率为0.125
- 前四次竞争都冲突的概率为：1 x 0.5 x 0.25 x 0.125 = 0.015625

二进制指数后退算法的优化

以上讨论的是发送方怎样避免冲突，或冲突后怎样再次竞争以成功发送，一旦发送成功后，如果接收方需发确认帧，则必须通过竞争才能得到信道的使用权，但是，如把一次成功发送后的第一个时隙留给接收方，则可保证发送方能及时收到确认，然而标准中并不允许

以太网

- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

802.3的性能

对某个站点来说，从站点产生新帧到允许发送的等待时间越短越好；对信道来说，在保证每个站点性能的基础上，能支持的站点数越多越好，很显然，这与共享网络中的站点数和每个站点在单位时间内发送帧的概率有关，所以，设：

- 在稳定重载荷的情况下，有k个站点参与信道竞争
- 每个站点在每个时隙中的发送概率为p

802.3的性能（续）

$$\text{信道效率} = \frac{\text{每帧发送时间（P）}}{\text{每帧发送时间（P）} + \text{平均竞争时间（T）}}$$

平均竞争时间 = 平均竞争时隙数 x 时隙长度(2 τ)

那么：某个给定时隙内，站点成功获得信道的概率为：A

$= kp(1-p)^{k-1}$

$$A = \left[\frac{k-1}{k}\right]^{k-1}$$

显然，当p = 1/k时，A将取最大值

当k →∞时，A →1/e

即，当竞争时隙数正好是j个时隙的概率=$A(1-A)^{j-1}$

平均竞争时隙数= $\sum_{j=0}^{\infty} j \times A \times (1-A)^{j-1} = \frac{1}{A}$ = e

最佳信道效率

由于802.3采用的是CSMA/CD(带冲突检测的载波侦听多路访问)，τ 是发送站点到最远站点的信号传播延时，为保证冲突信号的回传时间，所以每个时隙的时间为2 τ，平均竞争时隙数为e，所以平均竞争时间为2 τe

$$\text{信道效率} = \frac{\text{每帧发送时间（P）}}{\text{每帧发送时间（P）} + \text{平均竞争时间（T）}}$$

$$= \frac{P}{P + \frac{2\tau}{A}} = \frac{P}{P+2\tau e}$$

对更一般的情况

如：帧长为F，网络带宽为B，电缆长度为L信号传播速率为c（典型的为5μs/km）

每帧传输时间为P=F/B

信号的最大传播延迟 τ =L/c

在有e个竞争时隙的情况下

$$\text{即最佳的信道效率} = \frac{\frac{F}{B}}{\frac{F}{B}+\frac{2Le}{c}} = \frac{1}{1+\frac{2BLe}{cF}}$$

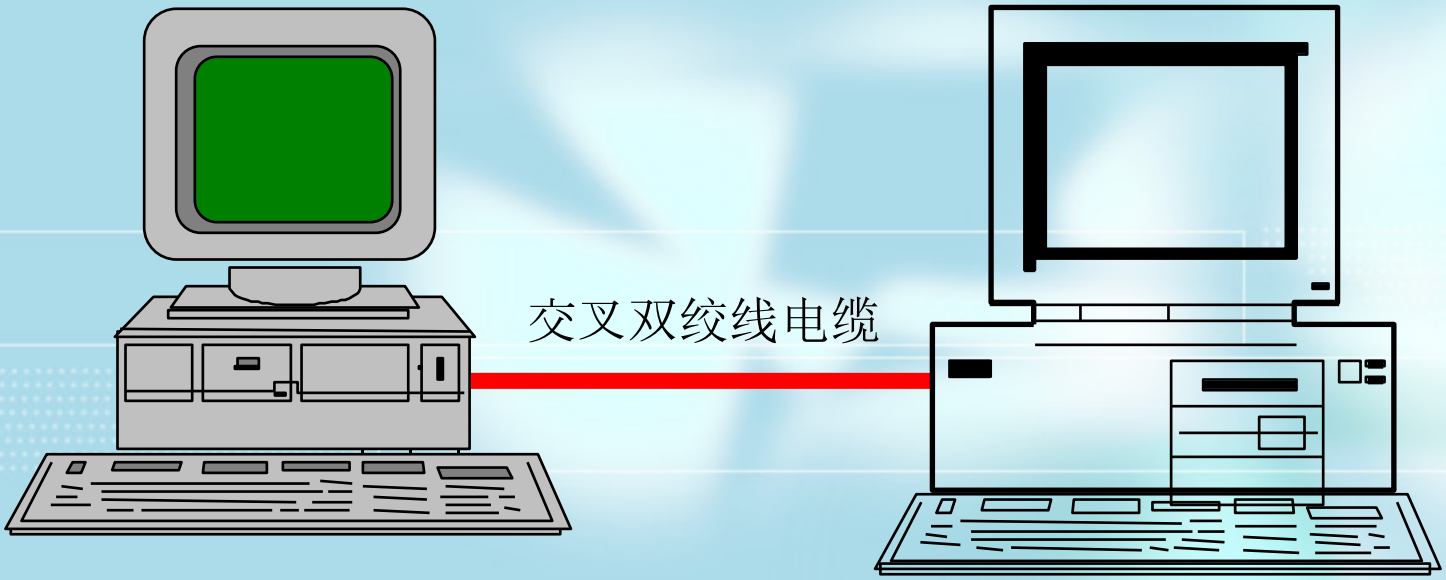
可见，增加网络带宽或远距离传输，将使信道效率降低

所以，在高带宽或广域网条件下，以太网可能不是最合适的

以太网

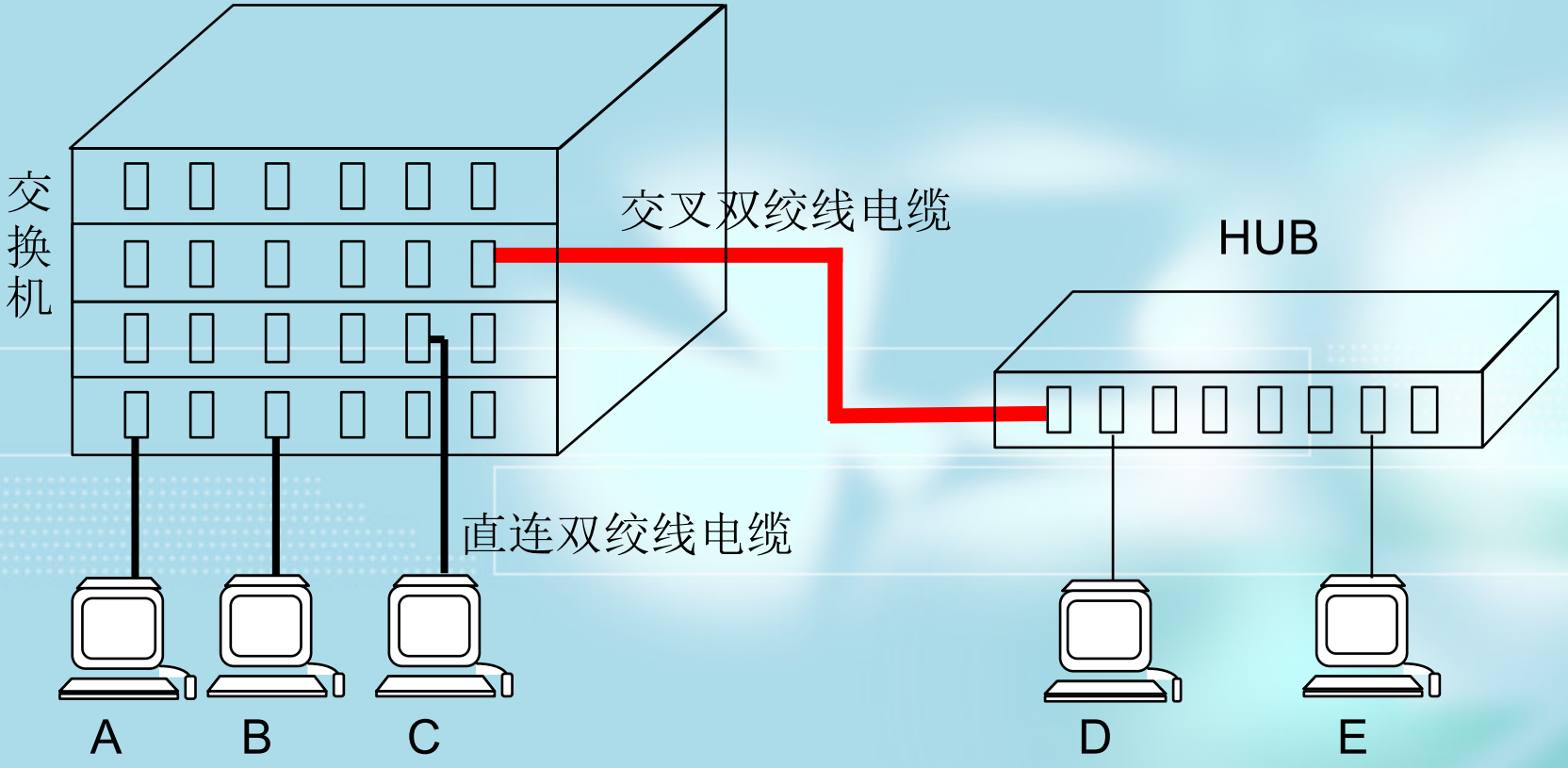
- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

最简单的以太网络



Tnbm P287 Fig. 4-22 (a) 两个站点的以太网

交换式以太网图例



Tnbm P287 Fig. 4-22 (b) 多站点以太网

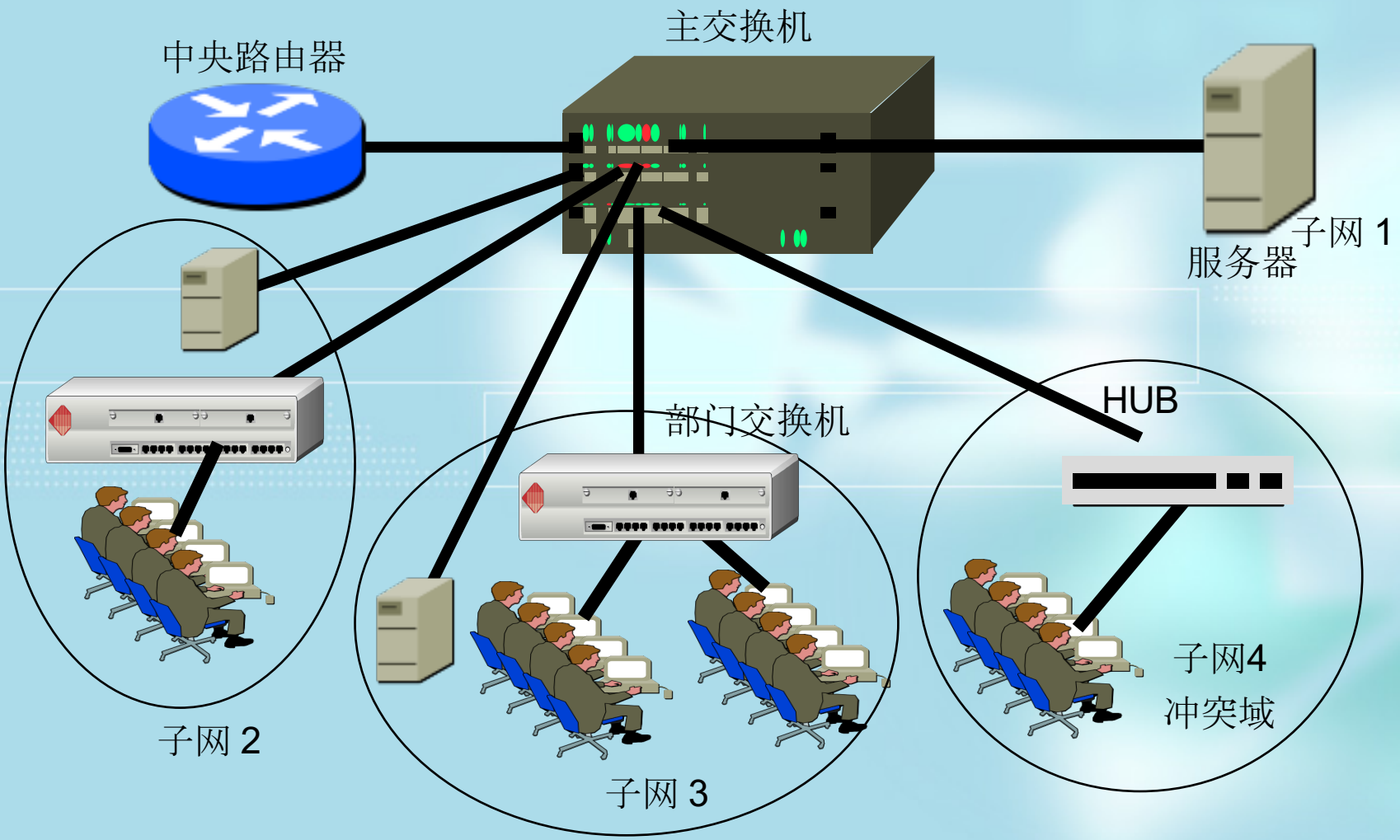
以太网交换机

- 交换机有一个高速的背板，速率可达1G b/s或更高
- 背板上可插入若干个模块(有的模块还可插入子模块)
- 每个模块(或子模块)上有4 ~ 8个RJ-45的端口，甚至更多，每个模块实际上是一个规模较小的局域网，即一个模块就是一个共享域(以太网中，共享域即冲突域)
- 一个模块上任一时刻只能有一个站点发送，但分属不同模块上的端口可并行工作，这可理解为组交换：模块内共享，模块间交换
- 当每个模块都退化成只有一个端口时，即一个共享域中只有一个端口，则该交换机是全交换的

交换式局域网

- 交换式局域网通常以百兆以太网交换机或千兆以太网交换机作为局域网的核心交换设备，交换机的每个端口都可用于连接一个网段或一台主机
- 每个端口连接的网段形成一个冲突域，端口之间帧的传输不受CSMA/CD的限制
- 交换机上不同类型的端口支持不同类型的传输介质，不同类型的端口其最大传输距离也不尽相同

交换式局域网示例



以太网

- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

Fast Ethernet（802.3u）

- 结构简单，兼容性好，价格相对低廉
  - 双速10/100 Mb/s MAC功能（自动协商 ）
  - 优选全双工操作，采用星型连接方式
  - 提供对cat3、cat5和STP（屏蔽双绞线）的支持，也支持光纤介质，但不支持同轴电缆
  - 采用 4B/5B的二进制编码

100Base-TX

- 其物理接口为RJ-45
- 连线采用5类双绞线cat5，仅用双对线，且全双工
- 802.3u必须与802.3完全兼容，即802.3u的帧格式与802.3的帧格式完全一致，及最短帧长为64B，然而，由于802.3u的传输速率为100M bps，所以64B的发送时间是5.12 μs，即在802.3u中， 2τ为5.12 μs
- 由于要求802.3u支持共享设备，即802.3u必须支持CSMA/CD，考虑竞争发送的冲突检测，在CSMA/CD机制中 ，τ决定了其最长的传输距离为250m
- 据此，规定单根双绞线的长度不超过100（125）m

100Base-FX

- 其物理接口为ST（圆型）或SC（方型）
- 连线采用一对光纤，全双工，且免受电磁干扰
- 配置光纤端口的交换设备通常不会是共享设备，所以不必考虑冲突检测问题
- 传输距离取决于采用的光源和在光纤中光信号的衰减，通常：多模光纤的传输距离为2 km；单模光纤的传输距离为10 km

快速以太网交换机是目前使用最广泛的交换机，中小规模的局域网或大规模局域网中的部门级交换机，首选的通常都是100 Mbps交换机

100Base-FX

- 其物理接口为ST（圆型）或SC（方型）
- 连线采用一对多模光纤，全双工，且免受电磁干扰
- 距离为2 km
- 编码采用4B/5B编码

快速以太网交换机是目前使用最广的交换机，无论是新建局域网还是原有局域网的升级，通常首选的总是快速以太网

以太网

- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

Gigabit Ethernet（802.3z）

千兆以太网的标准802.3z，1998年6月公布

- 千兆以太网支持两种工作模式：
  - ➢全双工工作模式

    使用两根信道，通常是光纤，不会产生冲突

    传输距离取决于信号的衰减
  - ➢半双工模式

    允许使用共享设备（如HUB），采用CSMA/CD机制来实现信道的共享

    传输距离必须考虑冲突检测，即必须考虑时隙问题

802.3z的两个特性

- 802.3z允许链路中使用共享设备（如HUB），为进行冲突检测，则帧的传输时间必须大于最长距离的信号往返的传播时间，即2τ
- 为保证与HUB的最长距离允许为100 m， 802.3z把时隙定为4.096 μs（传输4096比特的时间），为与802.3及802.3u兼容，不能增加最小帧的长度，所以采用了载波扩展技术
- 又为了提高有效数据的传输率，还采用了短帧突发技术

- **载波扩展**
- **短帧突发**

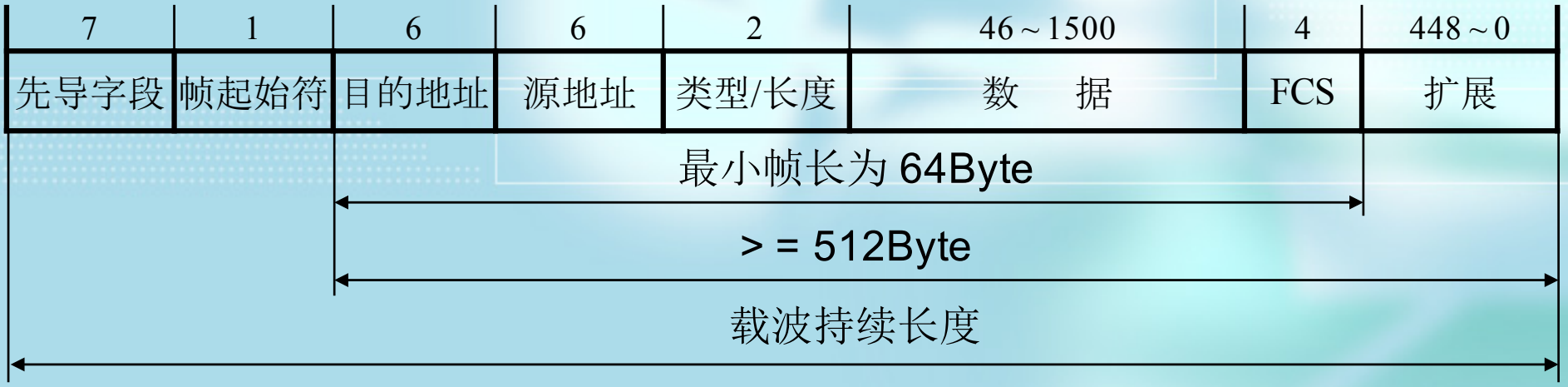
载波扩展

	传输速率 Mbps	往返距离 m	一个时隙2τ内可传输的Byte
802.3	10	5000	64 B（51.2 μs）
802.3u	100	500	64 B （5.12 μs）
802.3z	1000	400	512 B （4.096 μs）

- 为保证与**802.3及802.3u兼容，不能增加最小帧的长度，即最小帧的长度仍为64 Byte，但在帧传输完后，如尚未到达4.096 μs时，则以载波信号充斥其余时间**

千兆以太网的帧格式

- 千兆以太网的最短帧长与时隙不相关
- 采用载波扩展技术



对小于64Byte的以太帧，本来就必须填充，与千兆以太网格式无关

载波扩展带来的问题

- 如长度为**64 Byte**的短帧，都必须在**512 Byte**的时隙内传输，将严重影响性能，其信道效率为：

$$\frac{\text{帧长64 B}}{\text{扩展成512 B + 帧前导8 B + 帧间隙12 B}} = \frac{64}{532} = 12\%$$

- **64 Byte**的短帧扩展成**512 Byte**，如冲突在前**64 Byte** 之后，帧的重发将是无意义的

802.3z的两个特性

- 802.3z允许链路中使用共享设备（如HUB），为进行冲突检测，则帧的传输时间必须大于最长距离的信号往返的传播时间，即2τ
- 为保证与HUB的最长距离允许为100 m， 802.3z把时隙定为4.096 μs（传输4096比特的时间），为与802.3及802.3u兼容，不能增加最小帧的长度，所以采用了载波扩展技术
- 又为了提高有效数据的传输率，还采用了短帧突发技术

- **载波扩展**
- **短帧突发**

短帧突发

- 当短帧突发时，让一个站发送多个帧，而只对第一个帧进行载波扩展，紧接着发送后面的帧，这些帧毋需载波扩展

IFG（Inter Frame Gap）：帧间隔

迟冲突不重发

- 发生在扩展位的冲突被认为是一次迟冲突，IEEE 802.3z规定发送方在检测到迟冲突之后不能进行重传

1000 Base-X标准

- 1000 Base-SX
- 1000 Base-LX

标准类型	多模62.5 μm	多模50 μm	单模10 μm
1000 BASE-SX（波长850 nm）	220 m	550 m	----
1000 BASE-LX（波长1300 nm）	550 m	550 m	5000 m

1000Base-X标准（续）

- 1000Base-CX
- 1000Base-T

标准类型	两对屏蔽双绞线	四对非屏蔽双绞线（5类线）
1000BASE-CX	25 m	----
1000BASE-T	----	200 m

1000BASE-XX	200 m 两对非屏蔽双绞线（超5类线）

与100BASE-TX的主要区别

- 介质无关接口用GMII替代原MII
- 采用8B/10B的二进制编码
- 时钟为125M Hz，倍频电路生成时钟1250M Hz
- 帧格式的载波扩展，时隙取512 Byte（4096 bit）的传输时间4.096 μs
- 短帧突发处理
- 迟冲突者不重发

千兆以太网主要参数

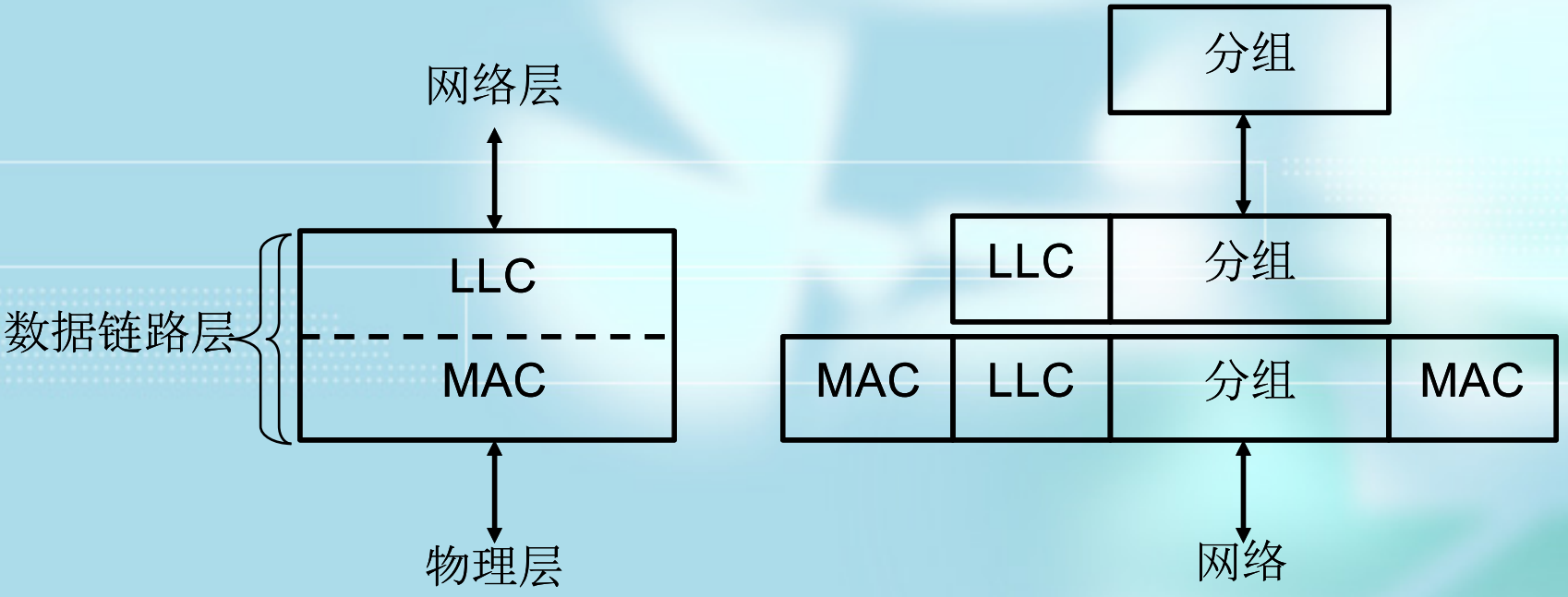
参数	值
时隙	4.096 μs， 即4096 bit (512Byte)的传输时间
帧间间隔	0.096μm（96bit）
拥塞序列大小	32 bit
最大帧长度	1518 Byte（数据长1500 Byte）
最小帧长度	512 bit（64 Byte）

以太网

- 以太网的电缆
- 以太网MAC子层协议
- 冲突后的避让算法
- 以太网的性能
- 交换式以太网
- 快速以太网
- 千兆以太网
- IEEE802.2 LLC

IEEE802.2 LLC

- 逻辑链路控制LLC（Logical Link Control），即IEEE 802.2标准



Tnbm P291 Fig. 4-24 (a) LLC的位置 (b) 协议格式

LLC的作用

- 由于不同的网络类型有不同的介质访问子层与之对应，而逻辑链路控制子层LLC则掩盖了不同物理网络之间的差别，以统一的格式为网络层提供服务
- LLC子层把网络层的分组（在TCP/IP中即IP包）加上LLC头，交给MAC子层组成相应的802.X帧发送

第4章 介质访问子层

- 信道分配问题
- 多路访问协议**CSMA**
- 以太网
- 数据链路层交换
- 无线局域网

数据链路层交换

- 网桥
- 网络互联设备
- 虚拟局域网**VLAN**

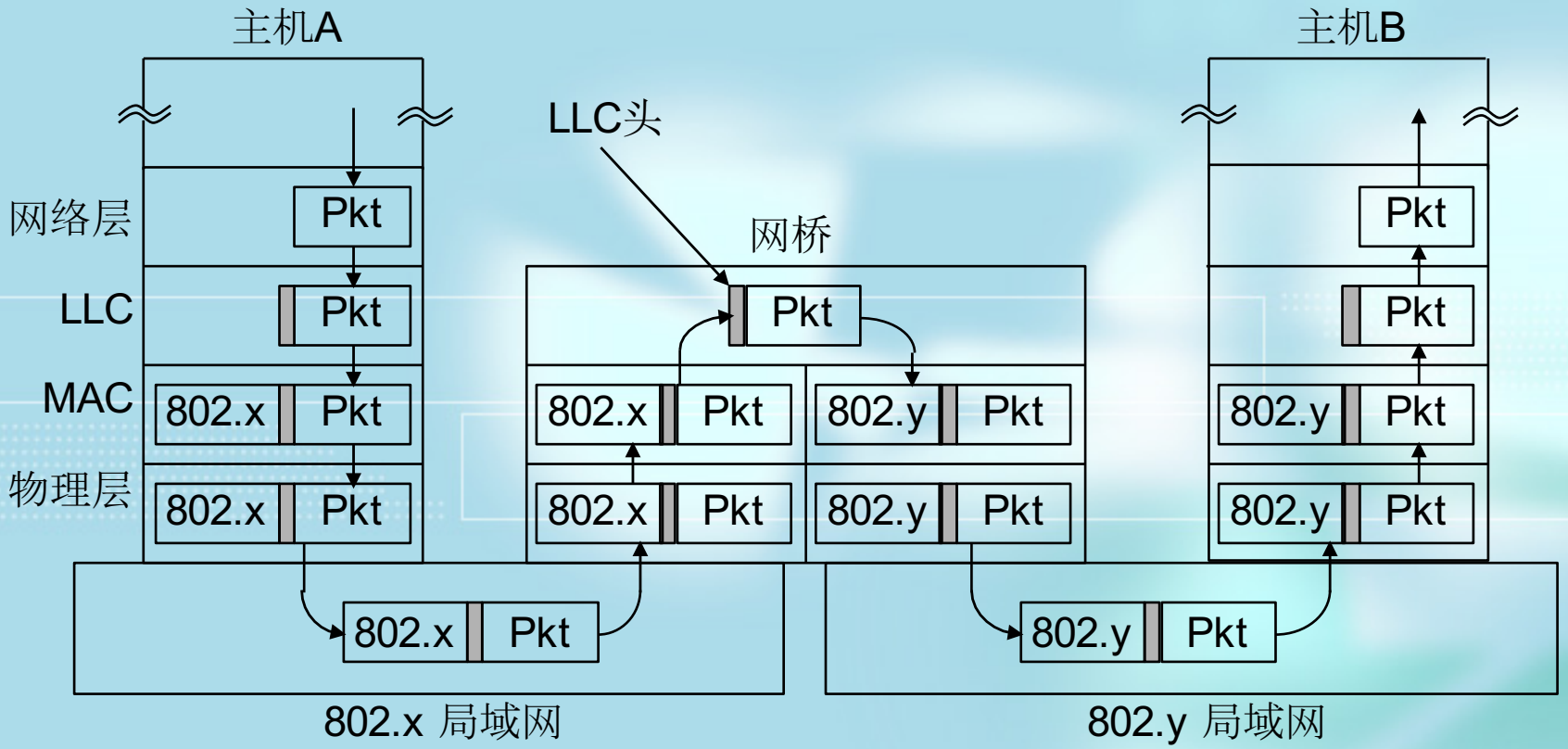
网桥（Bridge）

- 网桥是连接多个局域网的工作在数据链路层的设备
- 如把数据链路层细分为LLC子层和MAC子层，则所谓协议的不同是在数据链路层的MAC子层上
- 网桥作为不同数据链路层的网段之间的转换设备，则其相应的端口属于不同的网段
- 网桥的使用越来越少

网桥属数据链路层设备

- 网桥的工作原理
- 本地网间互联
- 生成树网桥
- 远程网桥

网桥的工作原理



Tnbm P320 Fig. 4-40 从802.x 到802.y 的局域网桥

网桥互联的问题

- 不同的LAN可能具有不同的帧格式，互联时必须进行帧格式的转换，将增加CPU的开销
- 不同的LAN可能具有不同传输速率，互联时必须进行缓存
- 不同的LAN可能具有不同的帧的最大长度，通常在数据链路层不支持对长帧的分帧功能，其处理方法是简单地丢弃
- 有的LAN支持数据链路层的加密功能，有的LAN却不支持
- 有的LAN支持QoS功能，有的LAN也不支持

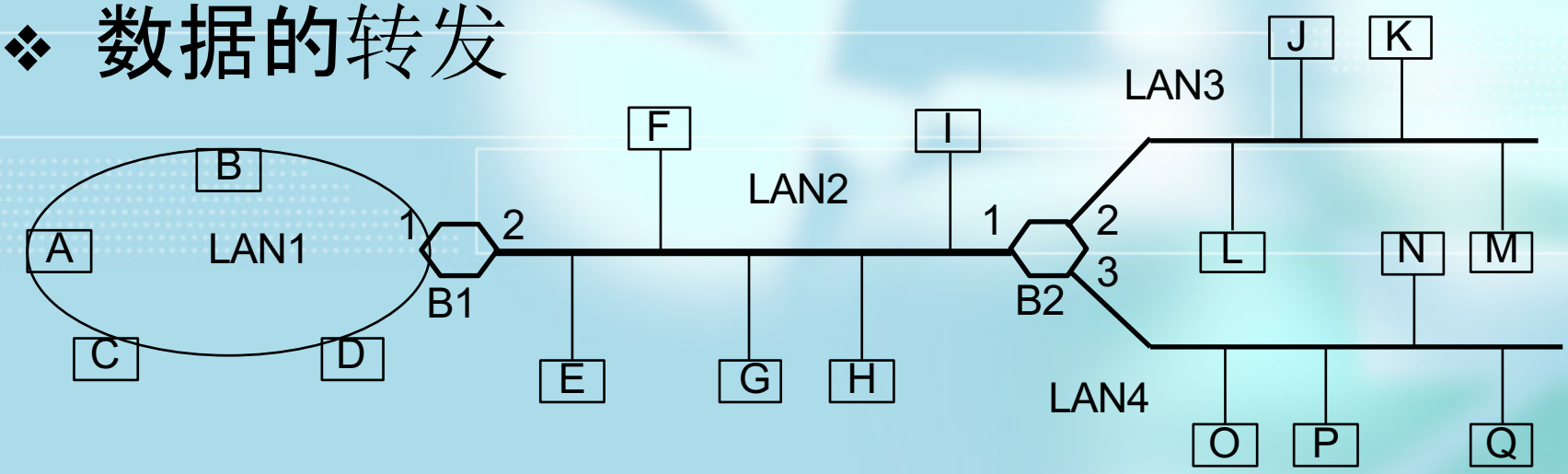
网桥 （Bridge）

- 网桥的工作原理
- 本地网间互联
- 生成树网桥
- 远程网桥

本地网间互联

所谓透明网桥，是指把网桥与相关的网络在物理上连接后，不需要做任何配置，即可实现网络互联的数据链路层设备

- **数据的转发**



Tnbm P322 Fig. 4-42 4个局域网和2个网桥的配置

网桥中的数据转发

- 透明网桥算法
  - 如目的站点所属LAN和源站点所属LAN相同，则丢弃该帧
  - 如目的站点所属LAN和源站点所属LAN不同，则转发该帧
  - 如目的站点所属LAN未知，则进行扩散

每个网桥都有一张散列表（即路由表），用来存放目的站点所属的LAN，该张散列表通过自学习法建立，并且是动态维护的

逆向学习算法

- 散列表的建立采用逆向学习算法
- 初始化时，散列表为空，此时，某源站点（假如是C）发送一帧到某目的站点（假如是H）时，网桥B1将记录该源站点和它进入的网桥端口（C/B1-1），并将该帧扩散(即转发到所连接的其它端口（B1-2）中，不必向源端口转发)

散列表的维护

- 散列表的更新是动态的，每一表项都有一个时间项，记录更新的时间，每个站点发送的帧到达时，都将更新其散列表项
- 按最长时间无收发帧的站点优先出散列表的原则，以保证散列表不会溢出

上例中网桥B1和网桥B2的散列表

网桥B1						网桥B2					
站点	端口	时间	站点	端口	时间	站点	端口	时间	站点	端口	时间
A	1		J	2		A	1		J	2	
B	1		K	2		B	1		K	2	
C	1		L	2		C	1		L	2	
D	1		M	2		D	1		M	2	
E	2		N	2		E	1		N	3	
F	2		O	2		F	1		O	3	
G	2		P	2		G	1		P	3	
H	2		Q	2		H	1		Q	3	
I	2					I	1				

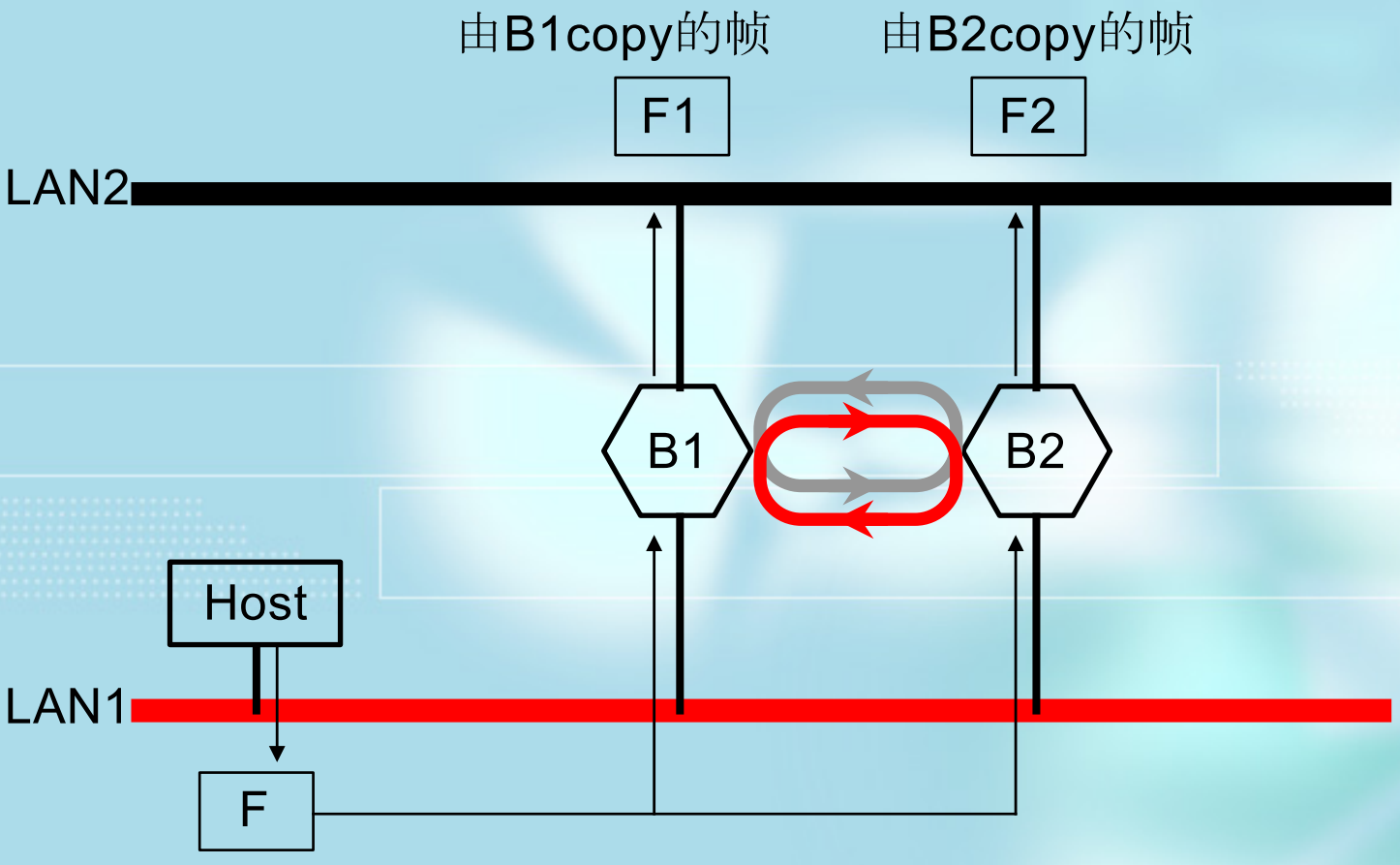
网桥 （Bridge）

- 网桥的工作原理
- 本地网间互联
- 生成树网桥
- 远程网桥

生成树网桥

- 如在LANs之间为提高可靠性，并行连接有2台(或多台)采用逆向学习算法的透明网桥，则可能由于无限制的循环扩散而使流量骤增，最后导致网络瘫痪
- 从原理上说，如网络中存在回路，常规算法的透明网桥都不能正常工作

包含回路的LANs



Tnbm P324 Fig. 4-43 两个并行的透明网桥

生成树算法

- 所谓生成树算法就是在物理上存在回路的拓扑中，生成一棵在逻辑上无回路的树，即生成树
- 生成树算法将以某指定节点为根节点，构建一棵生成树
- 对于原包含回路的拓扑，从生成树的根节点出发，沿生成树，可以到达任意一个节点，却不包含回路，但不能保证其路径是最优的

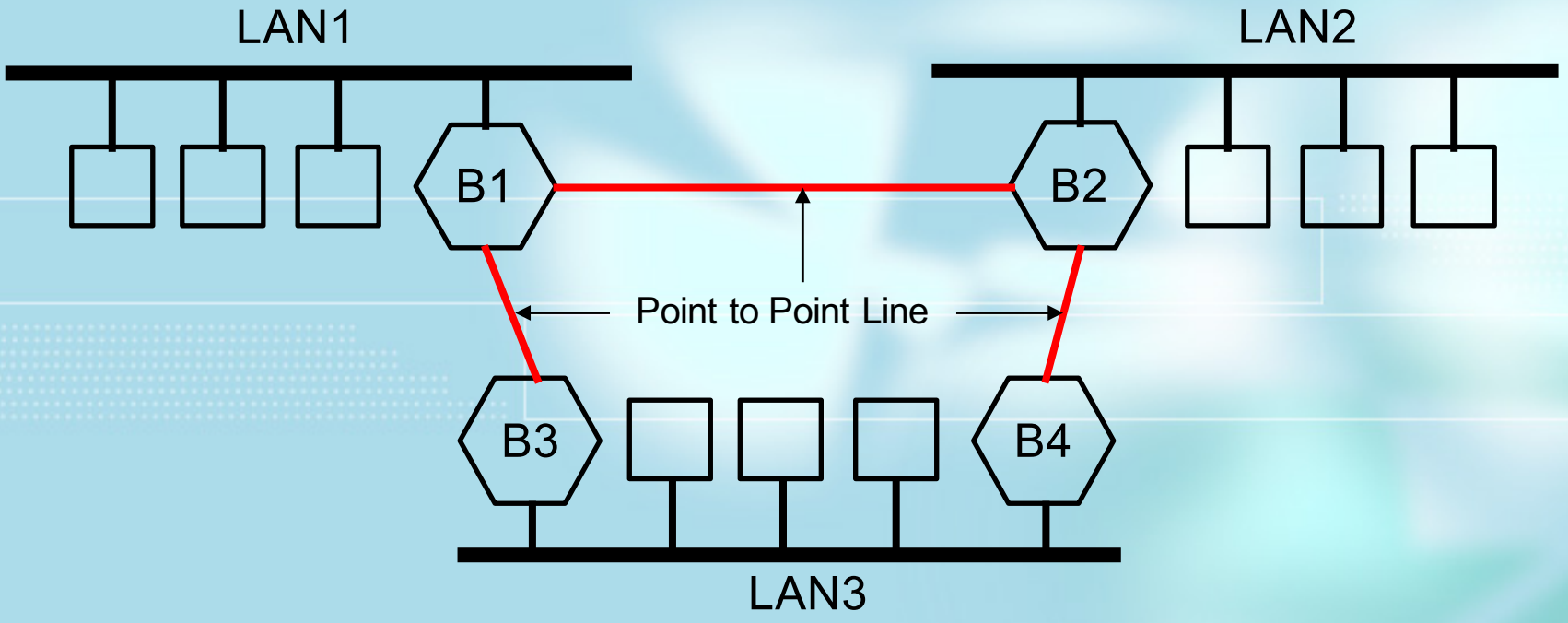
网桥 （Bridge）

- 网桥的工作原理
- 本地网间互联
- 生成树网桥
- 远程网桥

远程网桥

- 距离相对较远的LANs的连接可采用远程网桥和一对点到点的线路(如租用电信线路)来实现
- 点到点线路可看作是一个没有主机的LANs
- 点到点线路上可选用各种协议，如PPP

远程LANs的互联



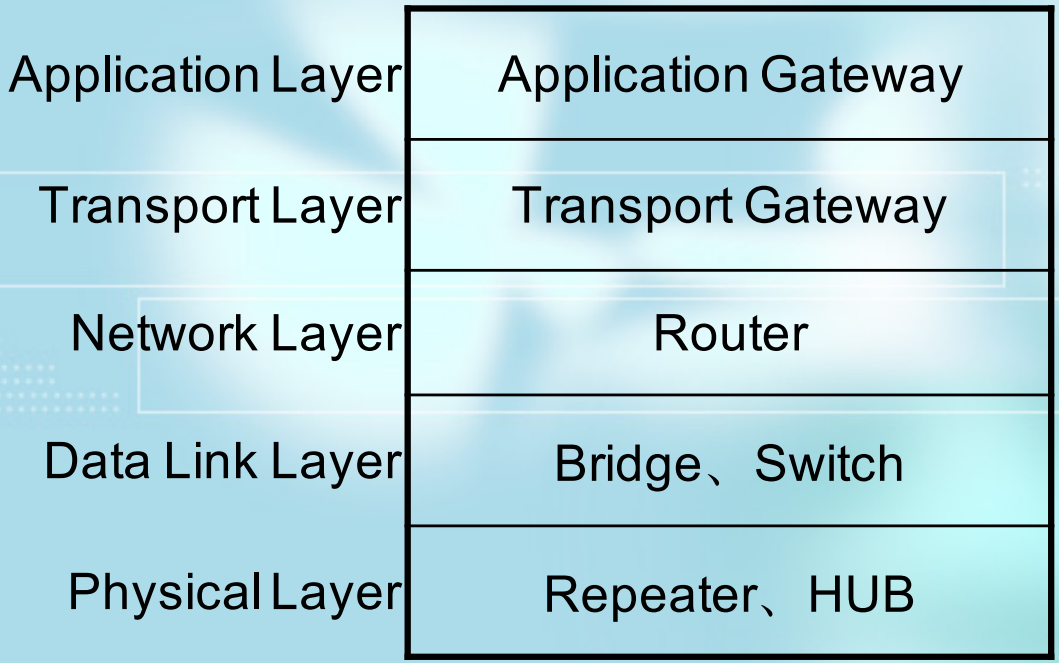
Tnbm P325 Fig. 4-45 远程网桥连接远距离的LANs

数据链路层交换

- 网桥
- 网络互联设备
- 虚拟局域网**VLAN**

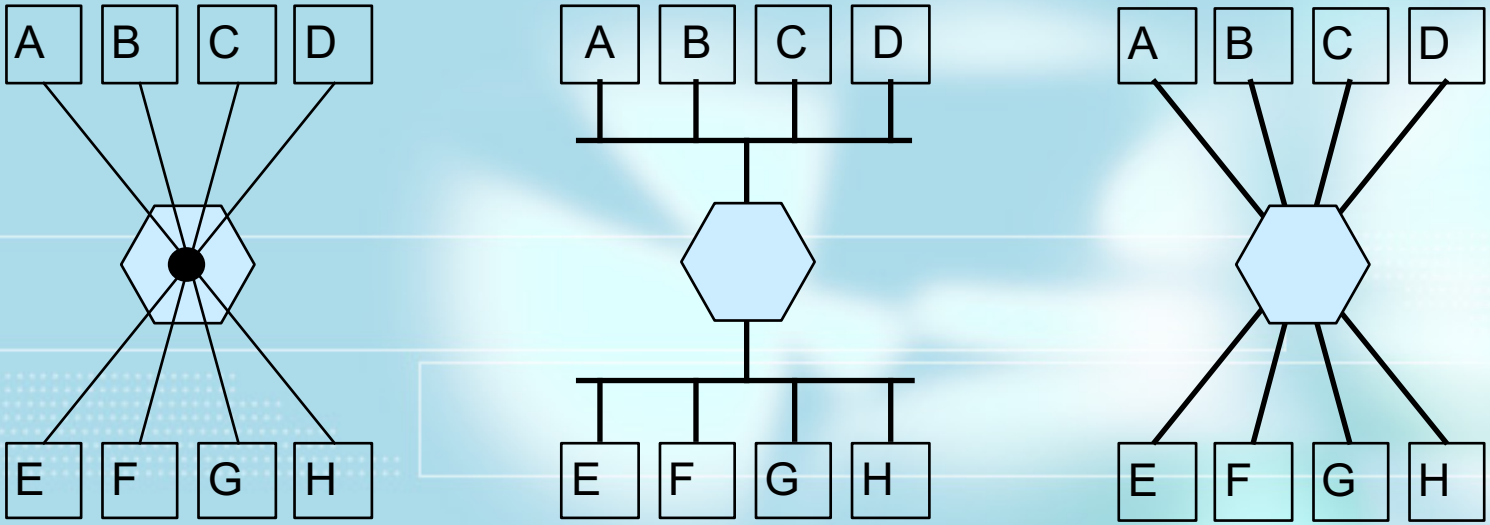
网络互联设备

- 不同的协议层有不同的网络互联设备



Tnbm P326 Fig. 4-46 不同的协议层的网络互联设备

HUB、网桥和交换机



数据链路层交换

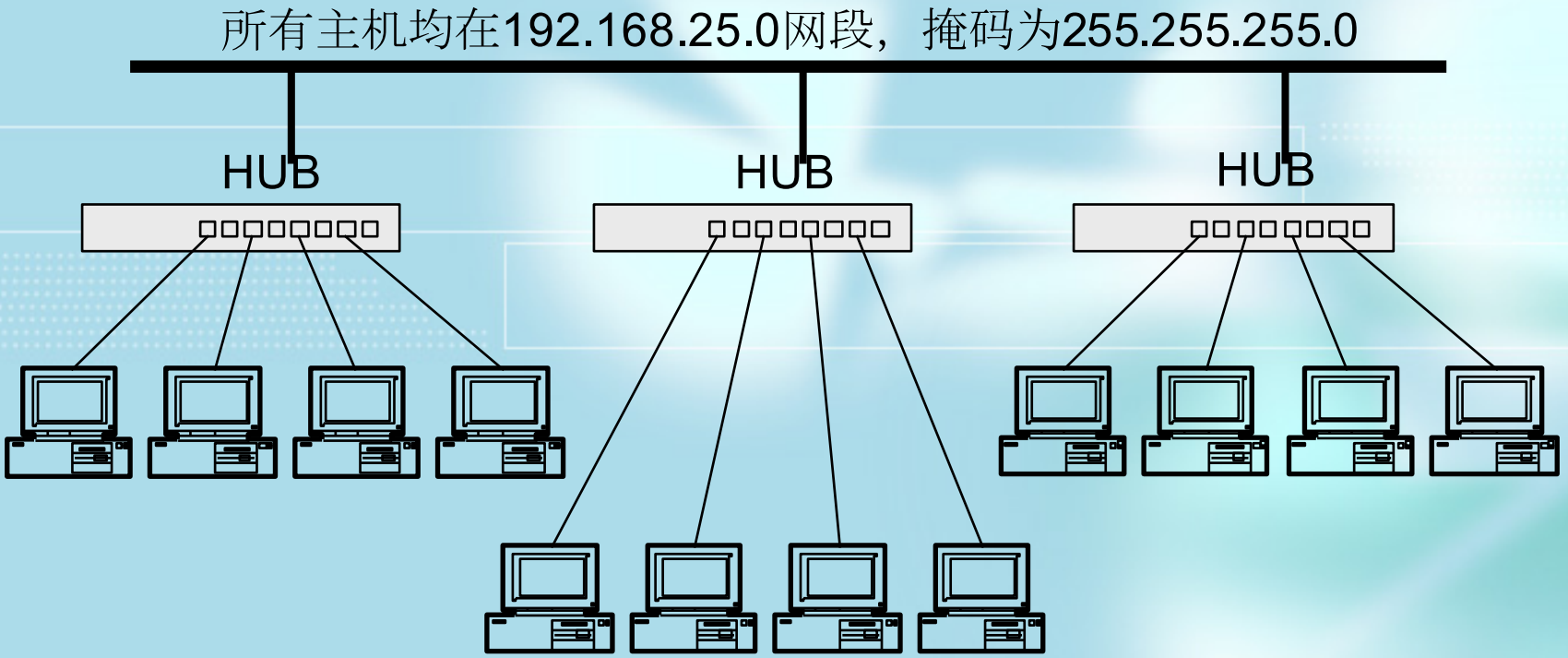
- 网桥
- 网络互联设备
- 虚拟局域网**VLAN**

虚拟局域网VLAN

- 局域网的广播域
- 局域网的网段分隔
- 局域网的子网划分
- 虚拟局域网VLAN
- IEEE 802.1Q 标准

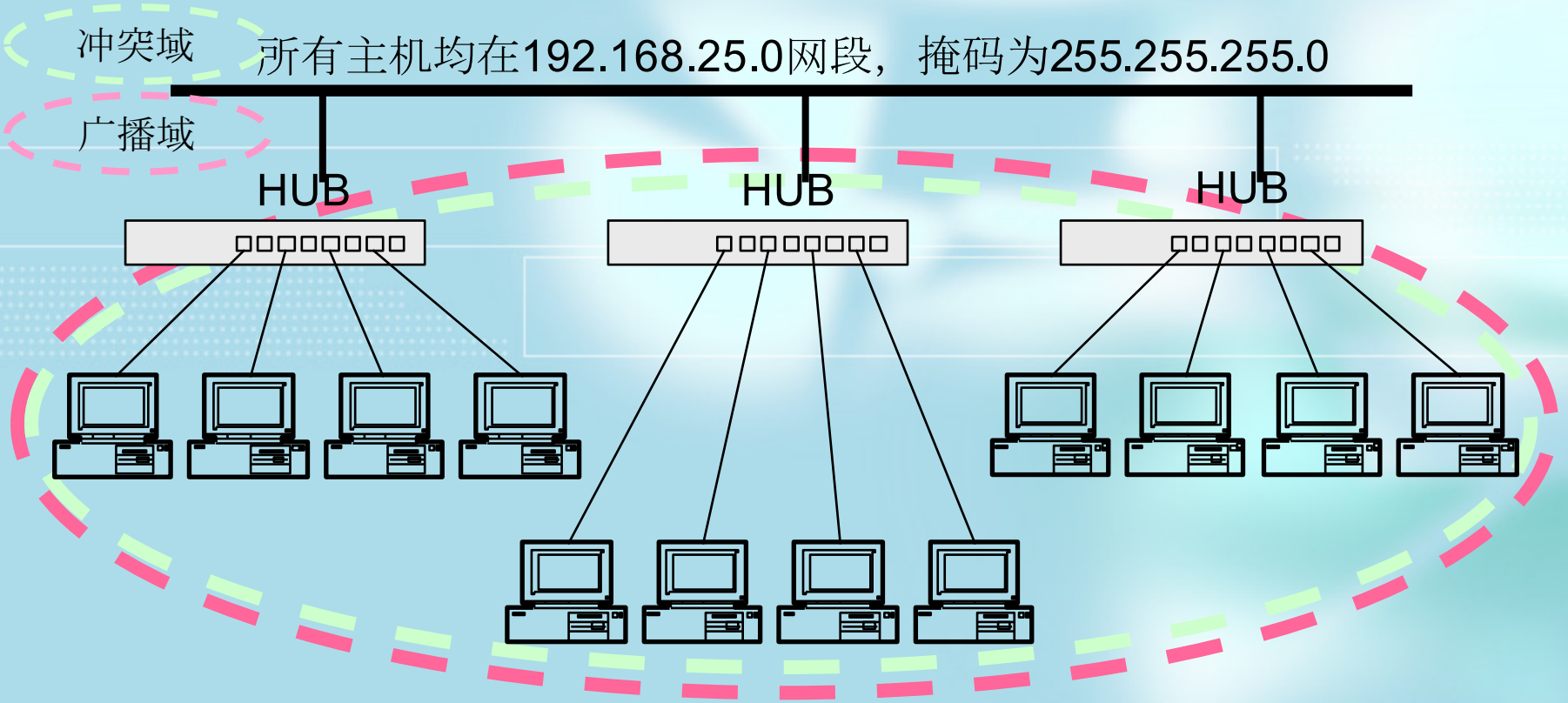
局域网的广播域

- 局域网的广播域



局域网的广播域（续）

- 局域网的广播域(共享域、冲突域)

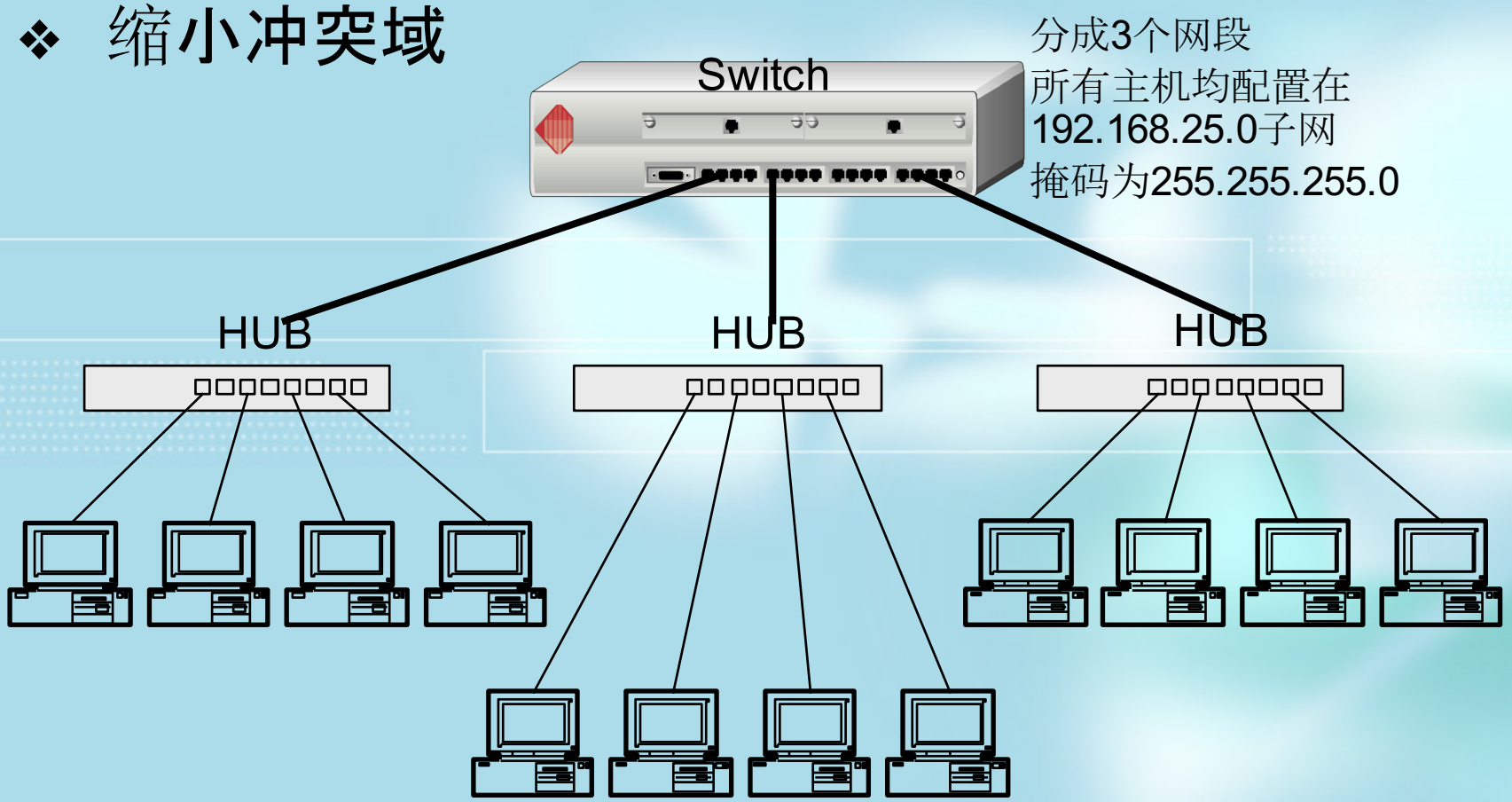


虚拟局域网VLAN

- 局域网的广播域
- 局域网的网段分隔
- 局域网的子网划分
- 虚拟局域网VLAN
- IEEE 802.1Q 标准

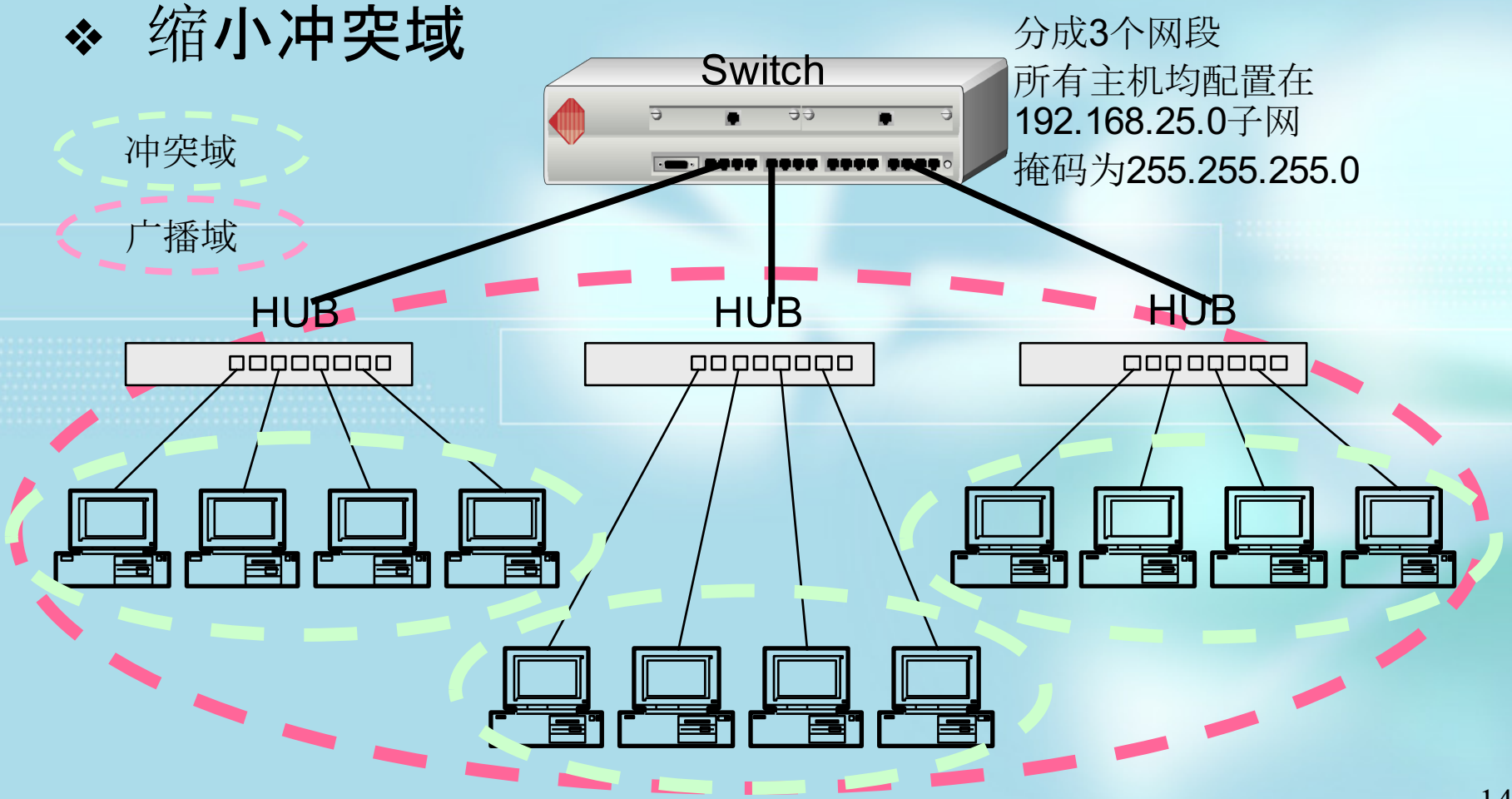
局域网的网段分隔

- 使用网桥和交换机来分隔网段
- 缩小冲突域



局域网的网段分隔（续）

- 使用网桥和交换机来分隔网段
- 缩小冲突域

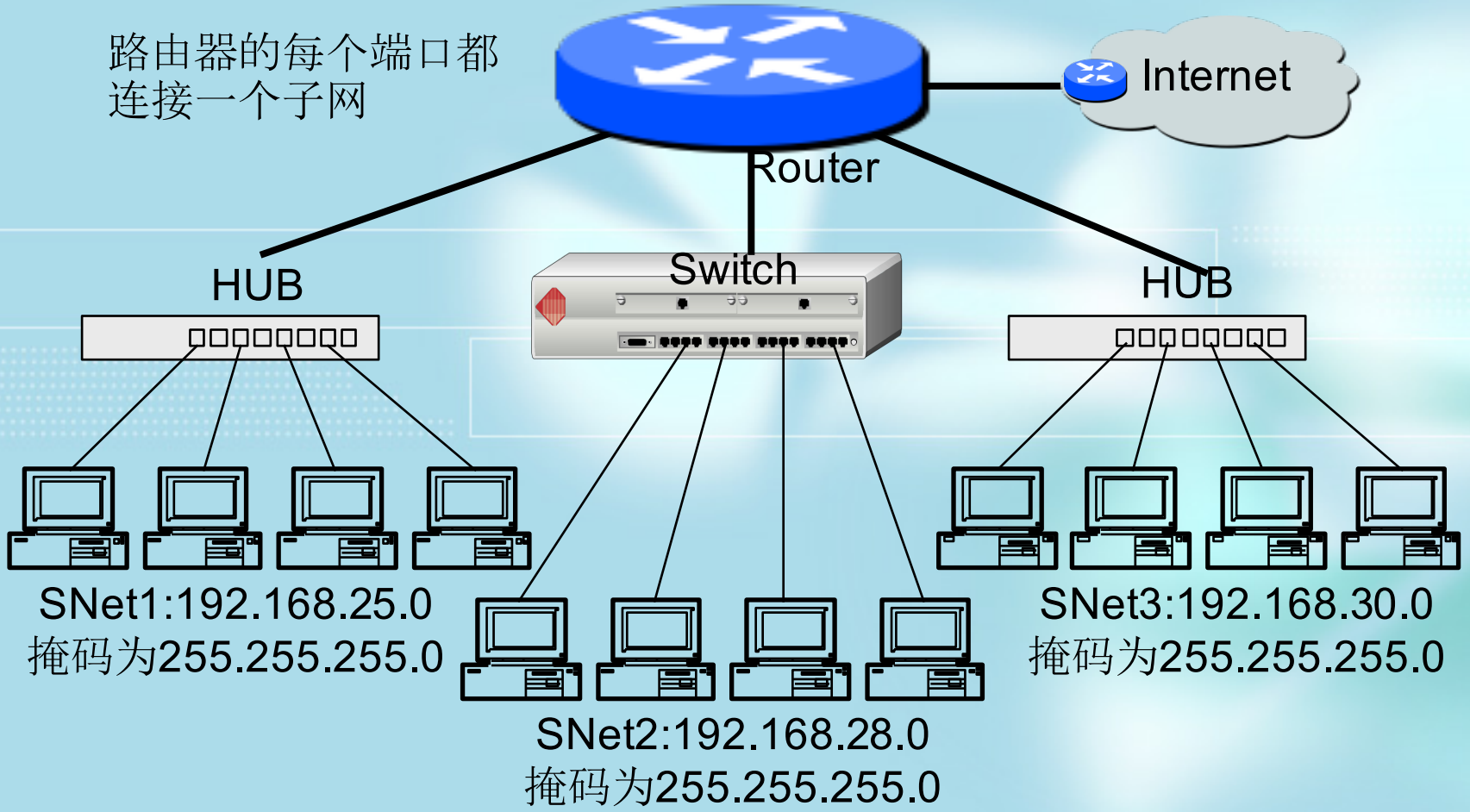


虚拟局域网VLAN

- 局域网的广播域
- 局域网的网段分隔
- 局域网的子网划分
- 虚拟局域网VLAN
- IEEE 802.1Q 标准

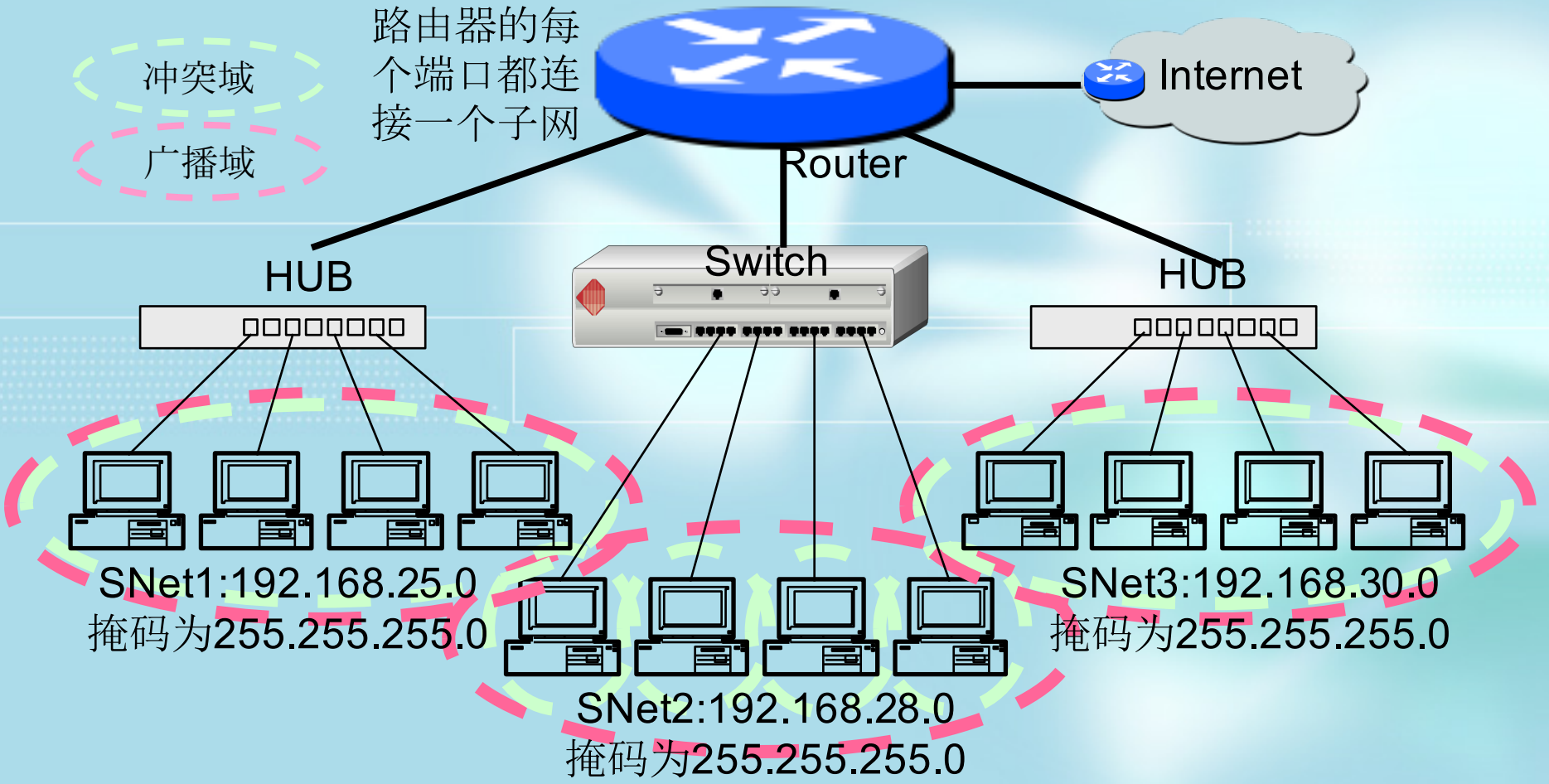
局域网的子网划分

- 局域网中使用路由器来划分子网并与**Internet**连接



局域网的子网划分（续）

- 局域网中使用路由器来划分子网并与**Internet**连接



网段和子网

- 网段(一个网段即一个冲突域)
  - 将若干个网络（网段）通过交换机（网桥）连接，以增加网络内的主机数并扩大覆盖范围，交换机（网桥）的每个端口连接一个网段，网段是链路层概念
  - 一个网段内的主机为一个冲突域，所有的主机是一个广播域，不同网段的主机间的通信则由交换机（网桥）负责转发或扩散
- 子网(一个子网即一个广播域)
  - 将若干个网络（子网）通过路由器连接，以实现网络的互联并组成一个更大的网络，路由器的每个端口连接一个子网，子网是网络层概念
  - 一个子网就是一个广播域，子网间的通信必须由路由器控制

虚拟局域网VLAN

- 局域网的广播域
- 局域网的网段分隔
- 局域网的子网划分
- 虚拟局域网VLAN
- IEEE 802.1Q 标准

虚拟局域网VLAN

VLAN是采用交换机技术，将原有网络分成若干个逻辑上的子网，逻辑子网也具有物理子网相同的网络性能，一个VLAN是一个广播域

- **VLAN基于交换技术**
- **VLAN的划分**
- **VLAN的技术特点**

VLAN基于交换技术

- VLAN技术属交换机的技术
- 交换机将维护一张交换表
- 交换表是交换端口的编号、MAC地址和所连接主机的MAC地址的关联表
- 交换表可以静态配置，也可以动态维护

虚拟局域网VLAN

VLAN是采用交换机技术，将原有网络分成若干个逻辑上的子网，逻辑子网也具有物理子网相同的网络性能，一个VLAN是一个广播域

- **VLAN基于交换技术**
- **VLAN的划分**
- **VLAN的技术特点**

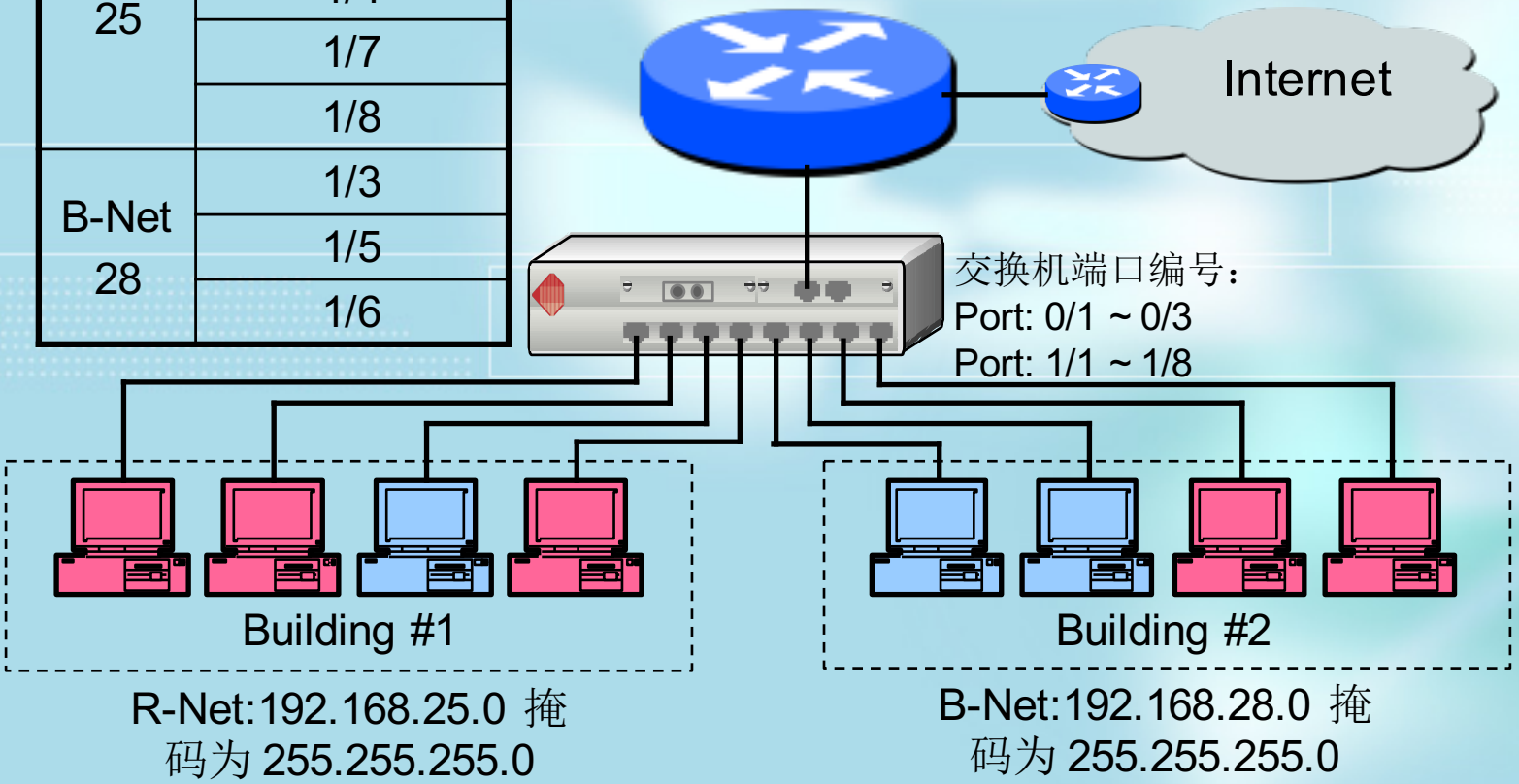
VLAN的划分

- 按端口划分
- 按主机的MAC地址划分
- 按主机的IP地址划分
- 局域网VLAN划分举例

按端口划分

VLAN	交换机端口号
R-Net 25	1/1
	1/2
	1/4
	1/7
	1/8
B-Net 28	1/3
	1/5
	1/6

- 按交换机的端口来配置(静态)



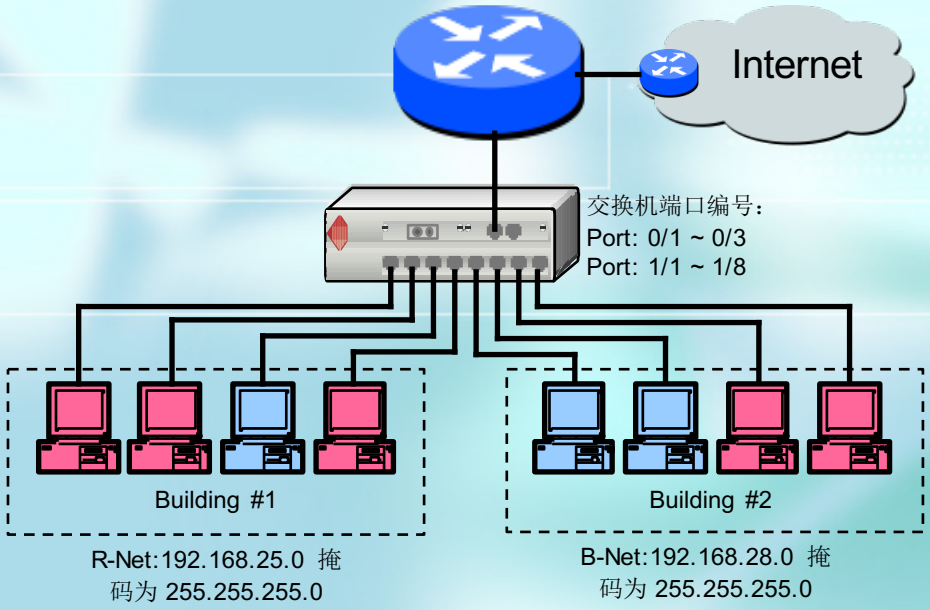
VLAN的划分

- 按端口划分
- 按主机的MAC地址划分
- 按主机的IP地址划分
- 局域网VLAN划分举例

按MAC地址划分

- 按主机的MAC地址来配置(动态)
- 必须先为每个注册用户(MAC)划分VLAN

VLAN	主机的MAC
R-Net 25	121235415121
	238923483756
	304537848445
	546372896745
	424872064821
B-Net 28	246879015426
	987461200455
	357878840212



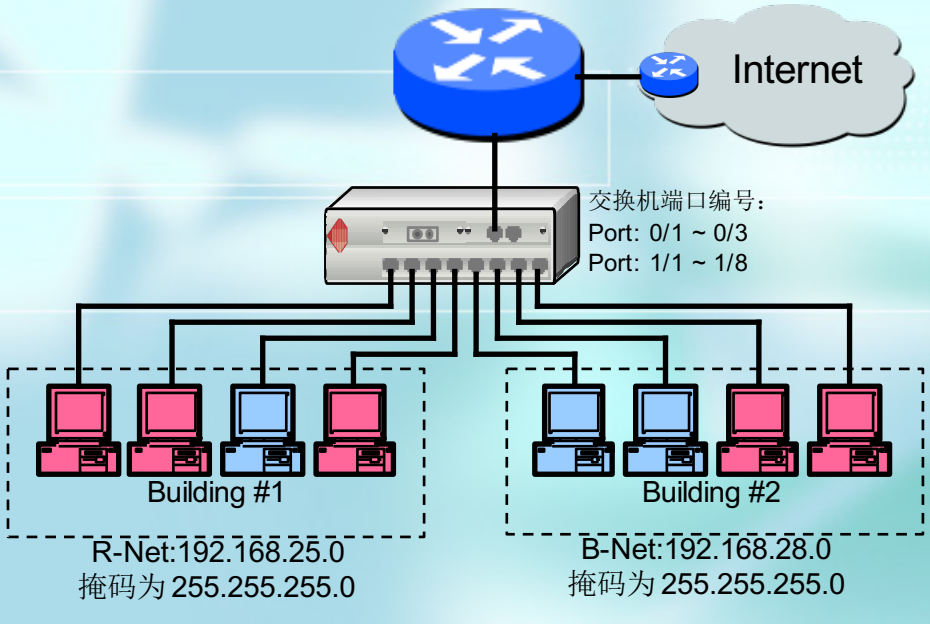
VLAN的划分

- 按端口划分
- 按主机的MAC地址划分
- 按主机的IP地址划分
- 局域网VLAN划分举例

按主机的IP地址划分

- 按主机的IP地址来配置(动态)
- 必须先为每个注册用户(IP)划分VLAN

VLAN	主机的IP地址
R-Net 25	192.168.25.41
	192.168.25.42
	192.168.25.43
	192.168.25.44
	192.168.25.45
B-Net 28	192.168.28.65
	192.168.28.66
	192.168.28.67

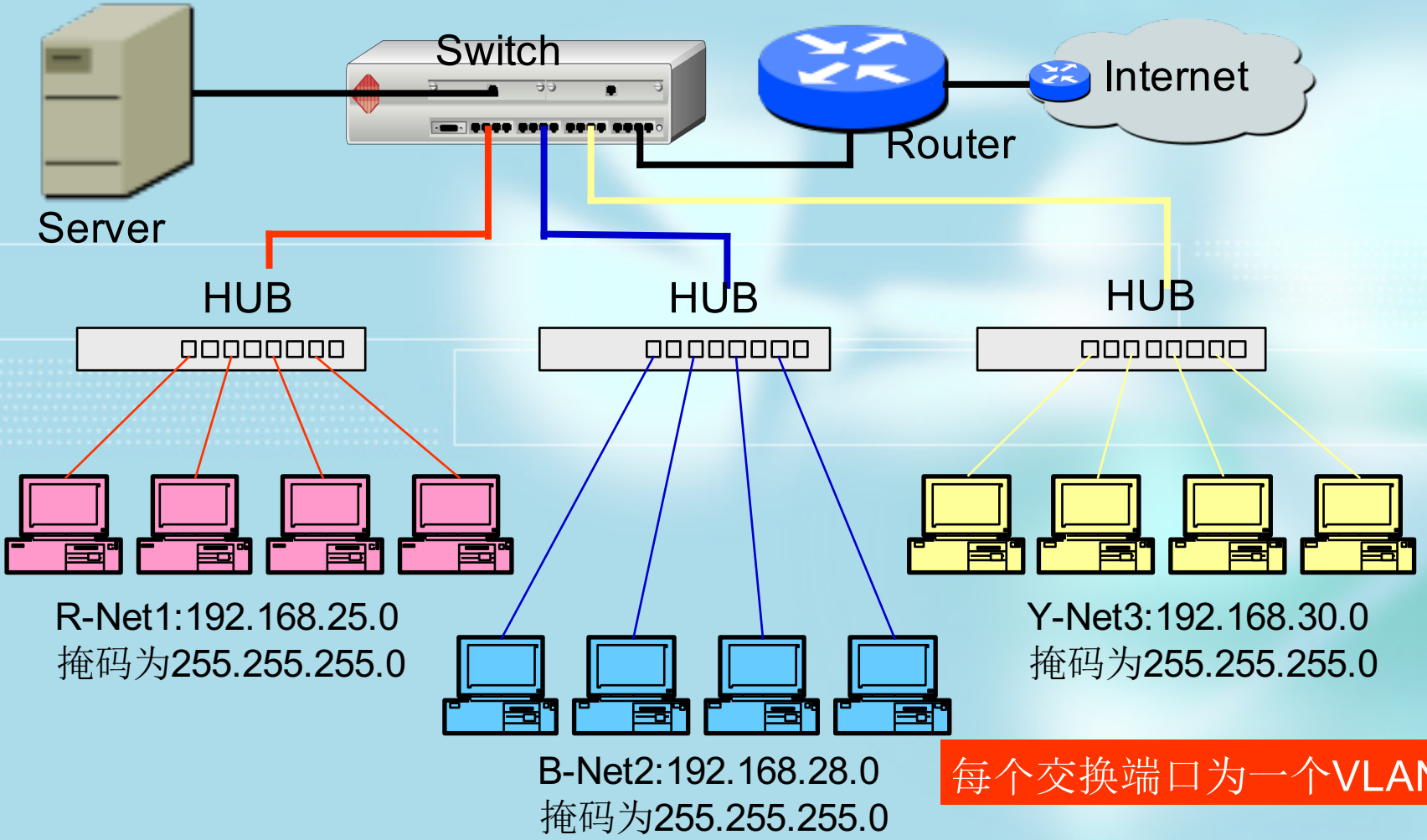


VLAN的划分

- 按端口划分
- 按主机的MAC地址划分
- 按主机的IP地址划分
- 局域网VLAN划分举例

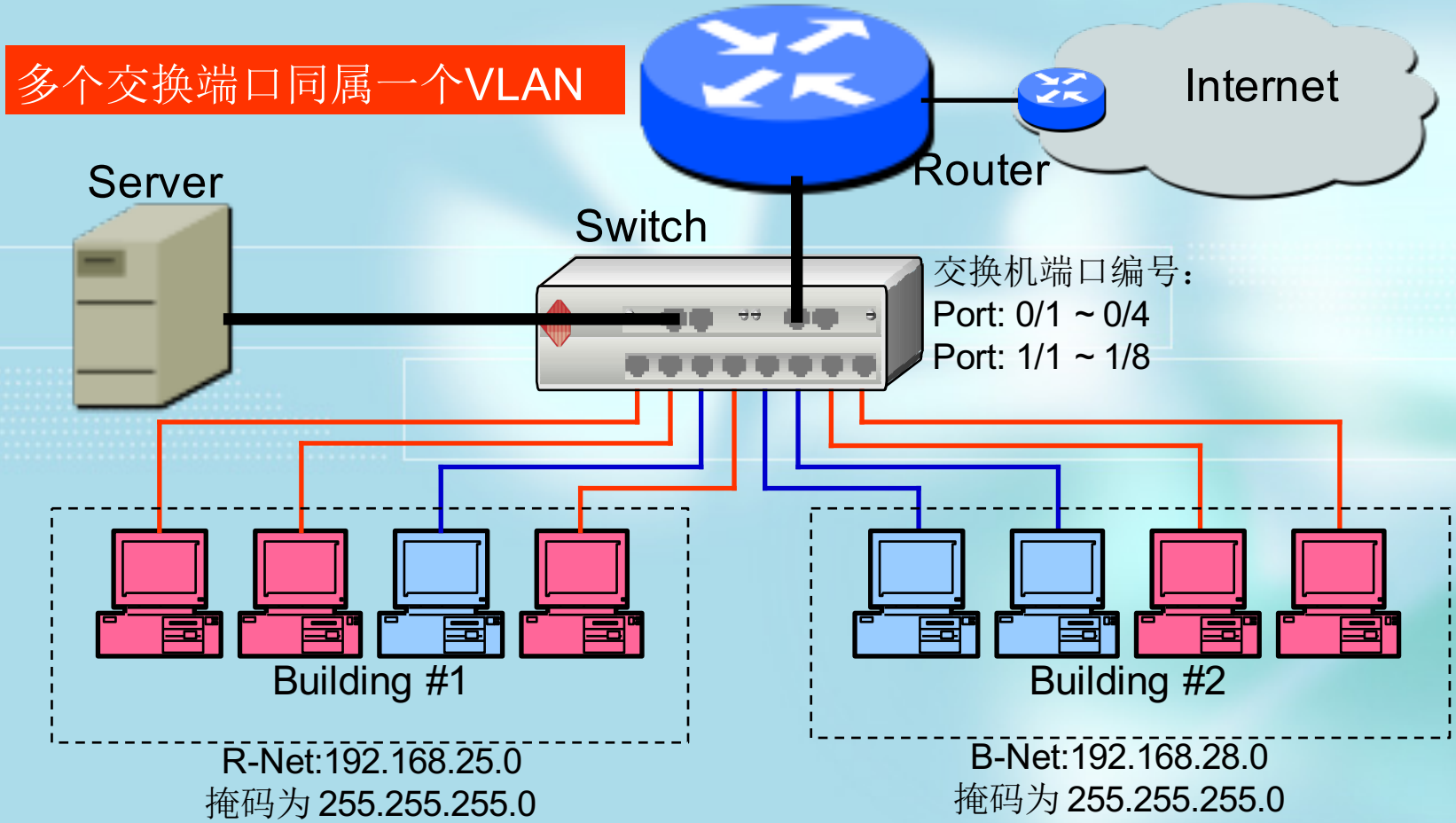
局域网VLAN划分举例

- 局域网中VLAN的路由及与Internet的连接



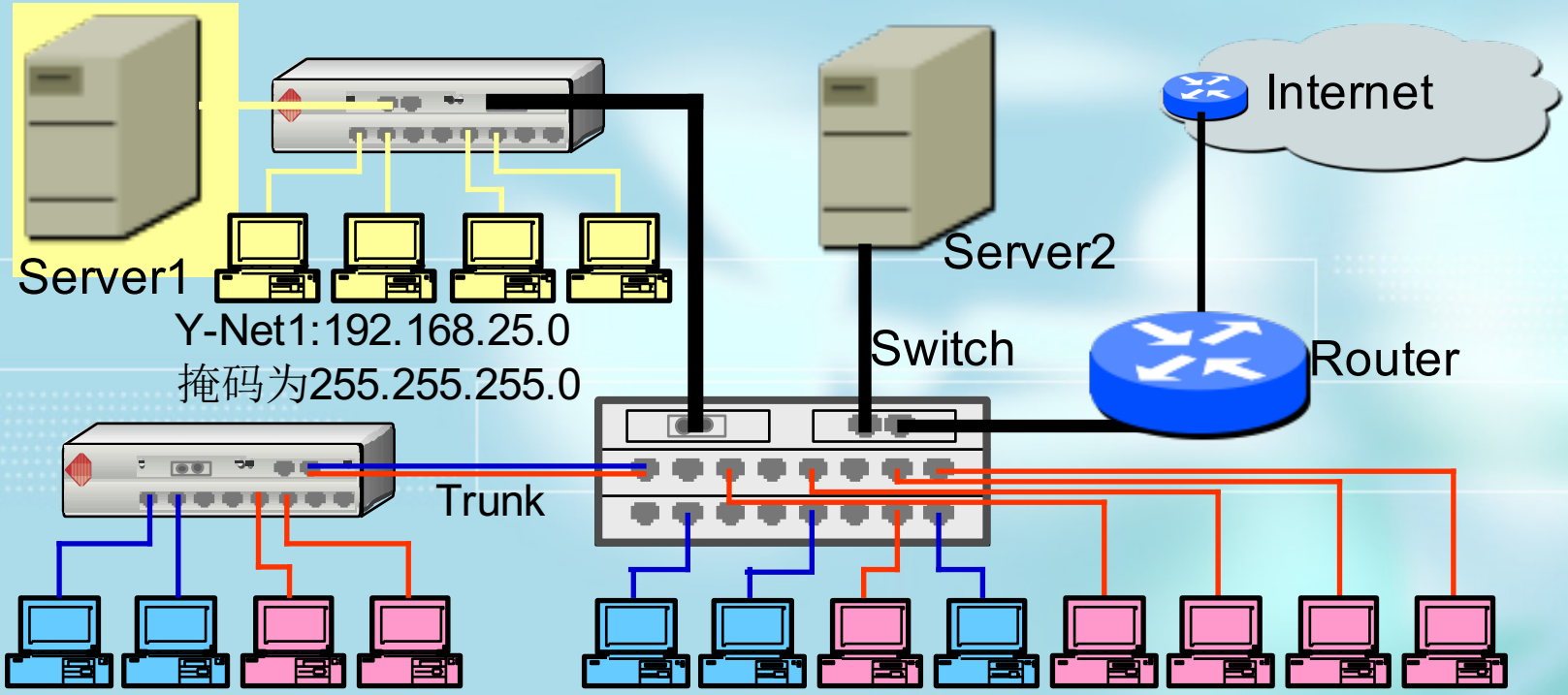
局域网VLAN划分举例（续1）

- 局域网中VLAN的路由及与Internet的连接



局域网VLAN划分举例（续2）

- 局域网中使用路由器来划分网段并与Internet连接



分属不同交换机的交换端口可同属一个VLAN

VLAN的技术特点

- 提高网络的可管理性，便于建立虚拟工作组
  - ➢不同物理网络中的主机可定义在同一个**VLAN**内， 同一物理网络内的主机也可定义在不同的**VLAN**中
- 提高网络的安全性
  - ➢不在一个**VLAN**中的主机，无法监听
- 有效地避免广播风暴，以提高信道利用率，并降低路由器的投资成本
  - ➢在一个物理网络（一个路由器端口连接的网络）内可划分多个逻辑子网
- 减少主机因网络逻辑拓扑改变而在物理上的移动

虚拟局域网VLAN

- 局域网的广播域
- 局域网的网段分隔
- 局域网的子网划分
- 虚拟局域网VLAN
- IEEE 802.1Q 标准

IEEE 802.1Q 标准

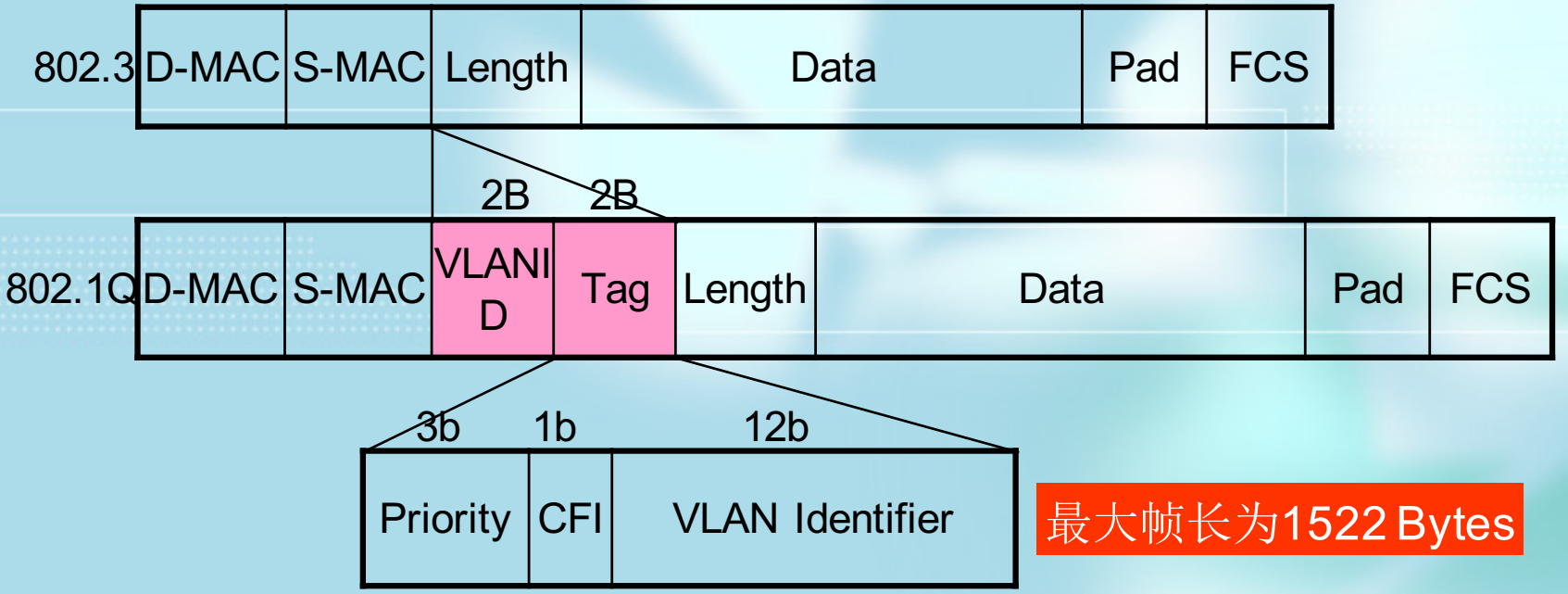
VLAN标准802.1Q于1998年公布

- **802.1Q必须解决的两个问题:**
  - **VLAN必须有一个VLAN的field来标志**
  - **802.1Q必须与802.3标准相兼容**

数据帧的成帧工作由数据链路层完成，即由网卡完成，但现有网卡不支持802.1Q

以太帧中的VLAN标志域

- **802.1Q 的以太帧格式**



Tnbm P335 Fig. 4-51 802.3和802.1Q以太帧格式

802.1Q 的以太帧格式说明

- VLAN-ID 16 bit
  - VLAN协议标识，恒为0x8100
- Priority 3 bit
  - Priority，暂且保留
- CFI 1 bit
  - 标准格式标志位
- VLAN Identifier 12 bit
  - VLAN标识，VLAN编号

IEEE 802.1Q 标准

VLAN标准802.1Q在1998年公布

- **802.1Q必须解决的两个问题:**
  - **VLAN必须有一个VLAN的field来标志**
  - **802.1Q必须与802.3标准相兼容**

数据帧的成帧工作由数据链路层完成， 即由网卡完成，但现有网卡不支持802.1Q

与802.3标准兼容

802.3的帧长为1518 Bytes

- **802.3**协议包括:
  - **802.3 10M bps**的以太网协议
  - **802.3u 100M bps**的快速以太网协议
  - **802.3z 1000M bps**的千兆以太网协议
- 千兆以太网的网卡已支持**VLAN**
  - 可识别和生成帧长为**1522 Bytes**的帧

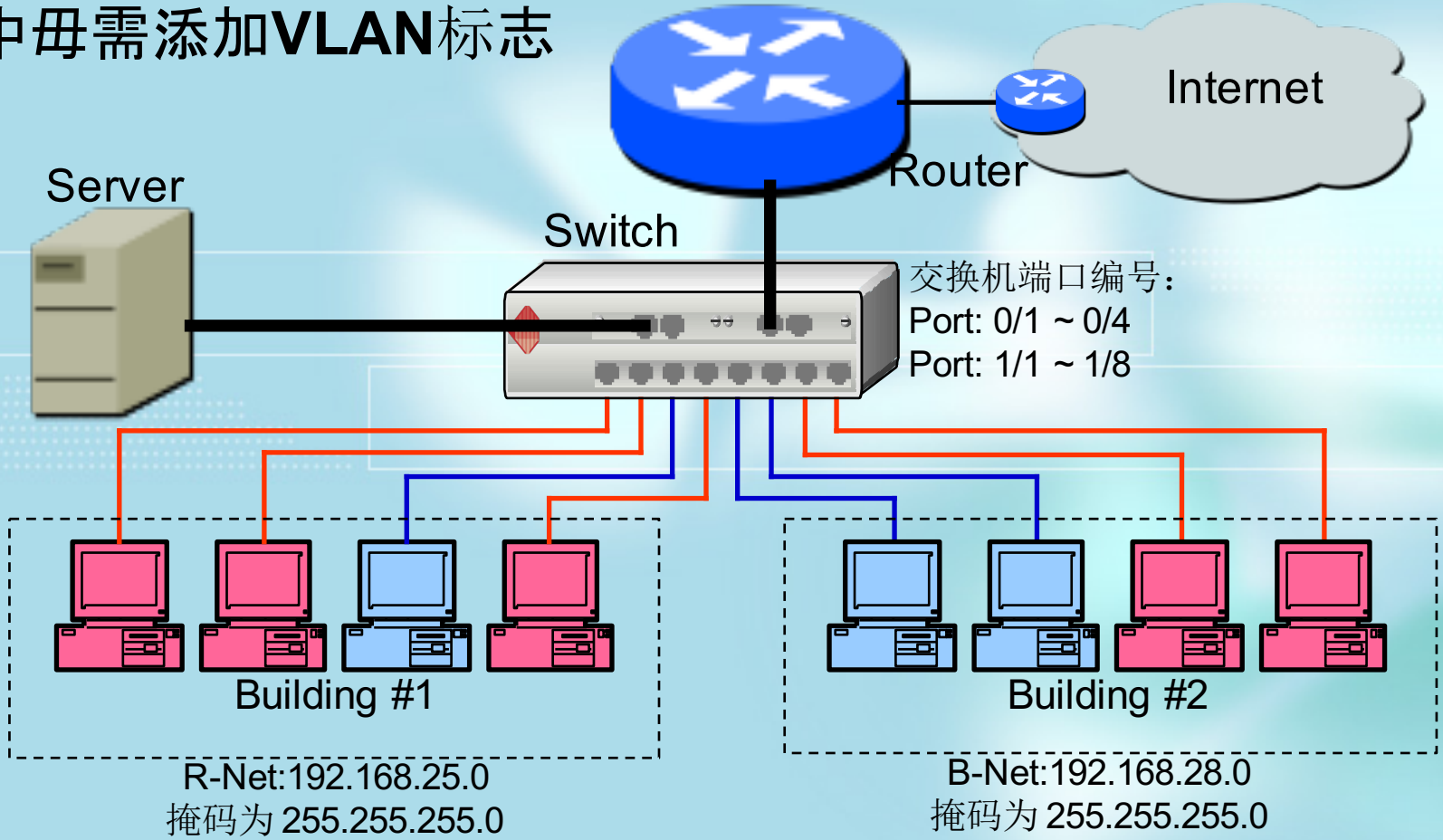
传统帧格式与VLAN兼容

对VLAN 敏感（aware）的和不敏感的
交换机必须允许混合使用

- VLAN标志是供交换机(网桥)来识别该帧的源站点主机属哪个VLAN
- 目前使用的网卡基本都对VLAN不敏感，即不允许帧长超过1518 Bytes：既不能识别或也不能生成VLAN标志
- 如一个VLAN涉及多台交换机，则在帧的传输中，第一台VLAN敏感的交换机负责在帧格式中添加VLAN标志，并由最后一台交换机删除VLAN标志

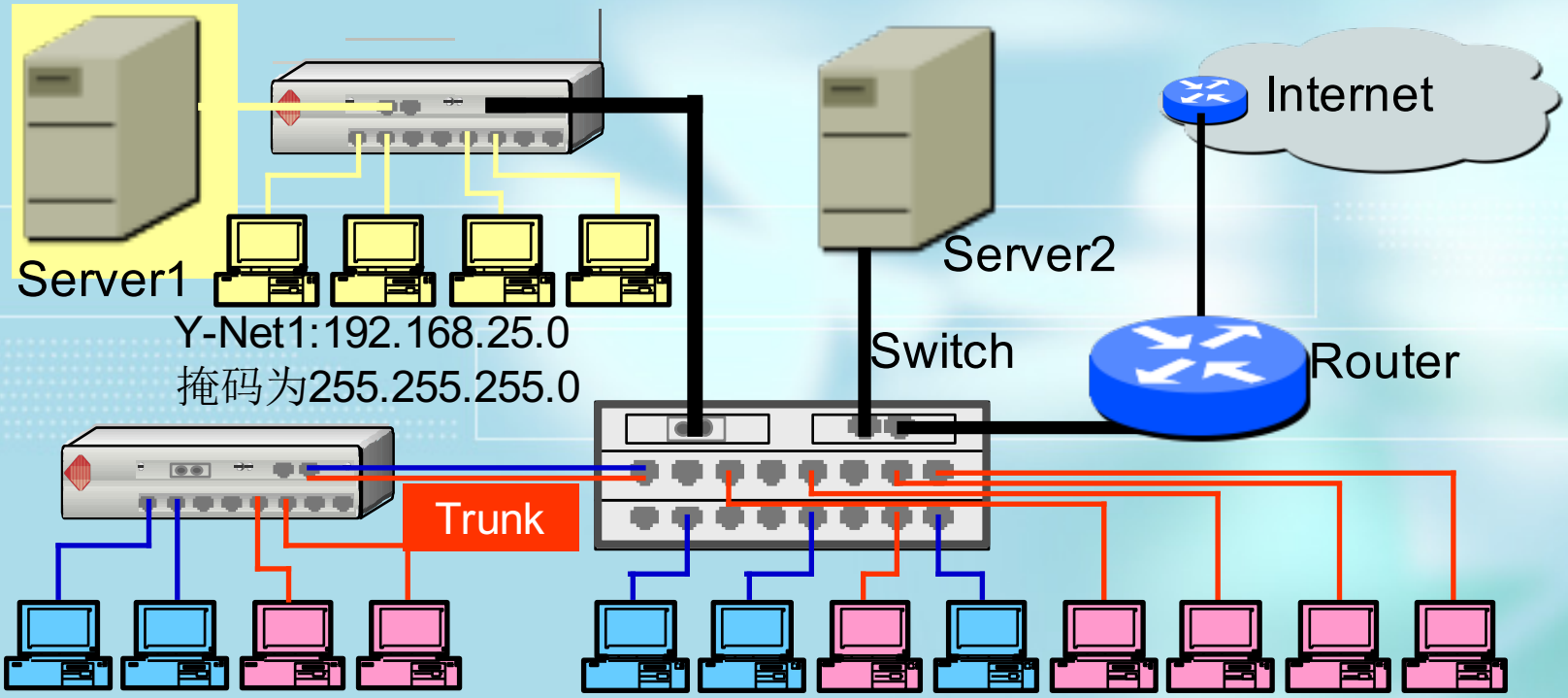
VLAN的标志

- 各主机所属VLAN由交换机识别，送给主机的帧格式中毋需添加VLAN标志



VLAN的标志（续）

- 两台交换机间要传输VLAN信息，帧格式中必须包含VLAN标志，这就是Trunk功能



第4章 介质访问子层

- 信道分配问题
- 多路访问协议**CSMA**
- 以太网
- 数据链路层交换
- 无线局域网

无线局域网

- 无线局域网的组成
- 802.11物理层
- 802.11MAC子层协议

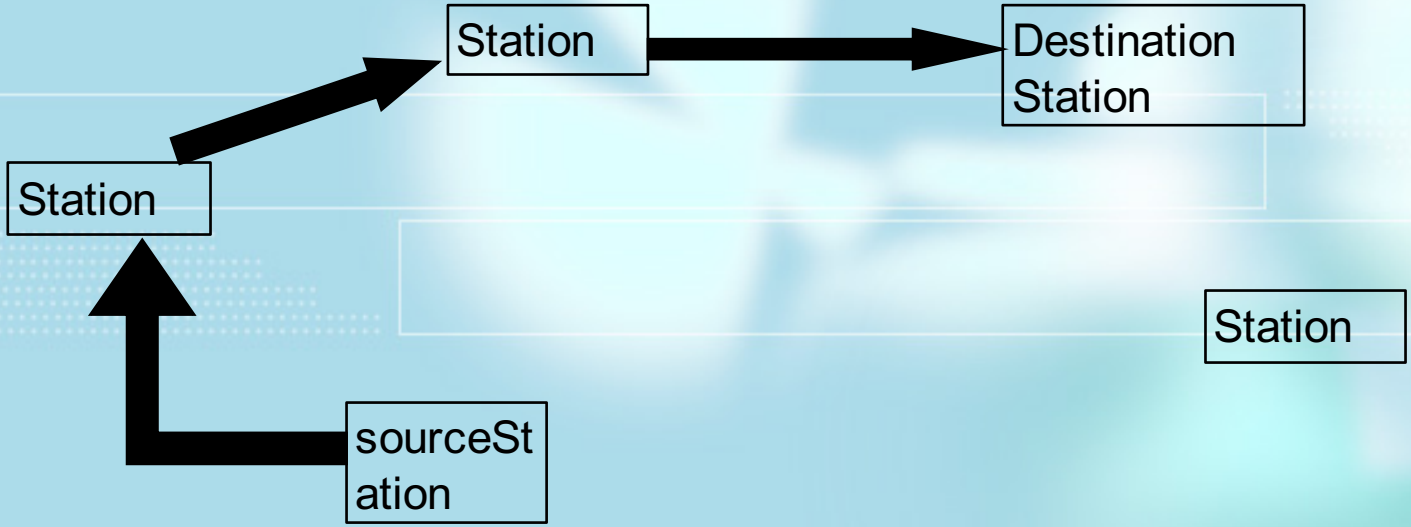
802.11的组网模式

802.11定义了两种组网模式

- **Ad-Hoc 模式**
- **Infrastructure 模式**
  - 基本服务集合 **BSS**
  - 扩展服务集合 **ESS**

Ad-Hoc模式

- 所有的移动站之间互相平等，每个节点既是主机又是路由器

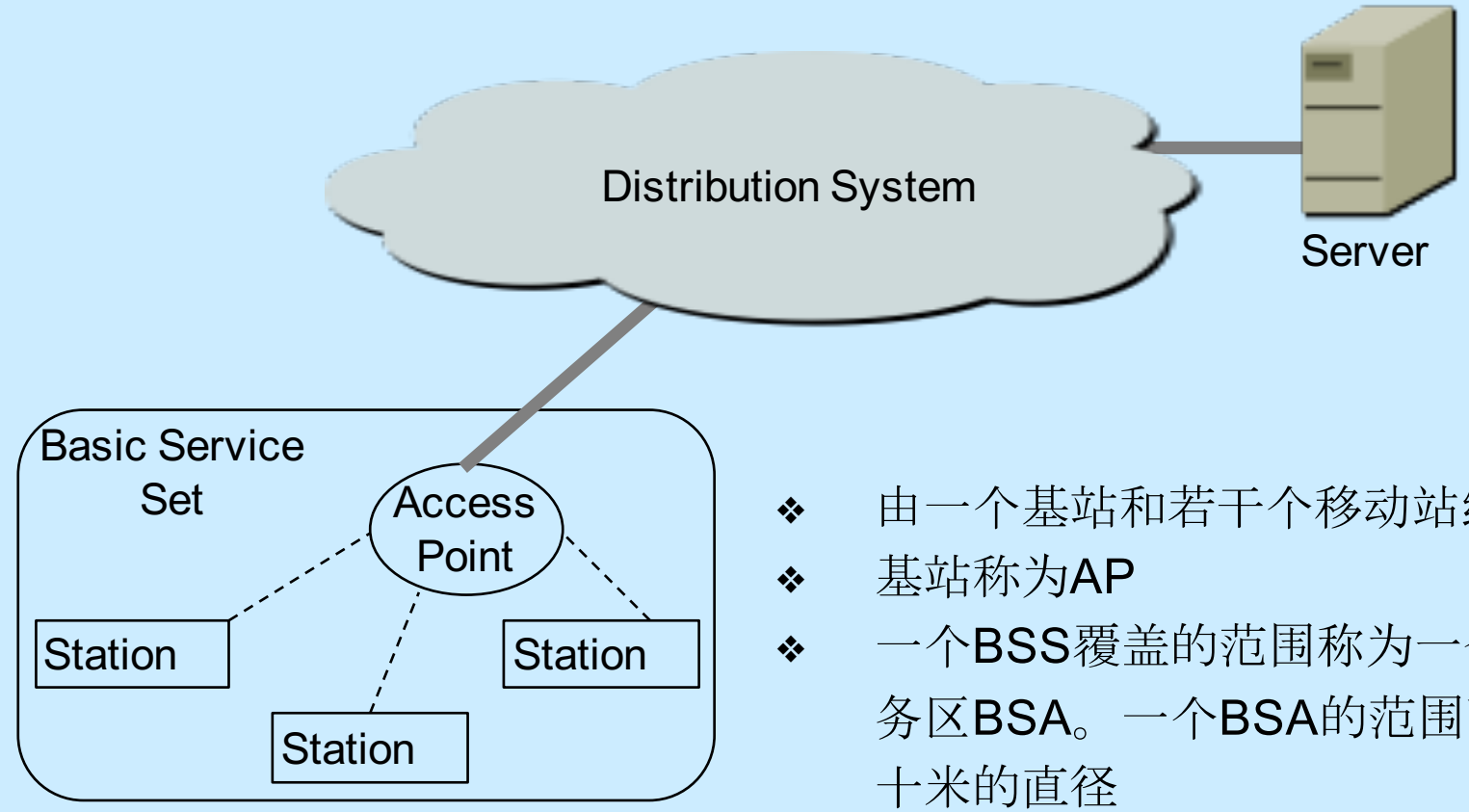


802.11的组网模式

802.11定义了两种组网模式

- **Ad-Hoc 模式**
- **Infrastructure 模式**
  - 基本服务集合 **BSS**
  - 扩展服务集合 **ESS**

基本服务集BSS



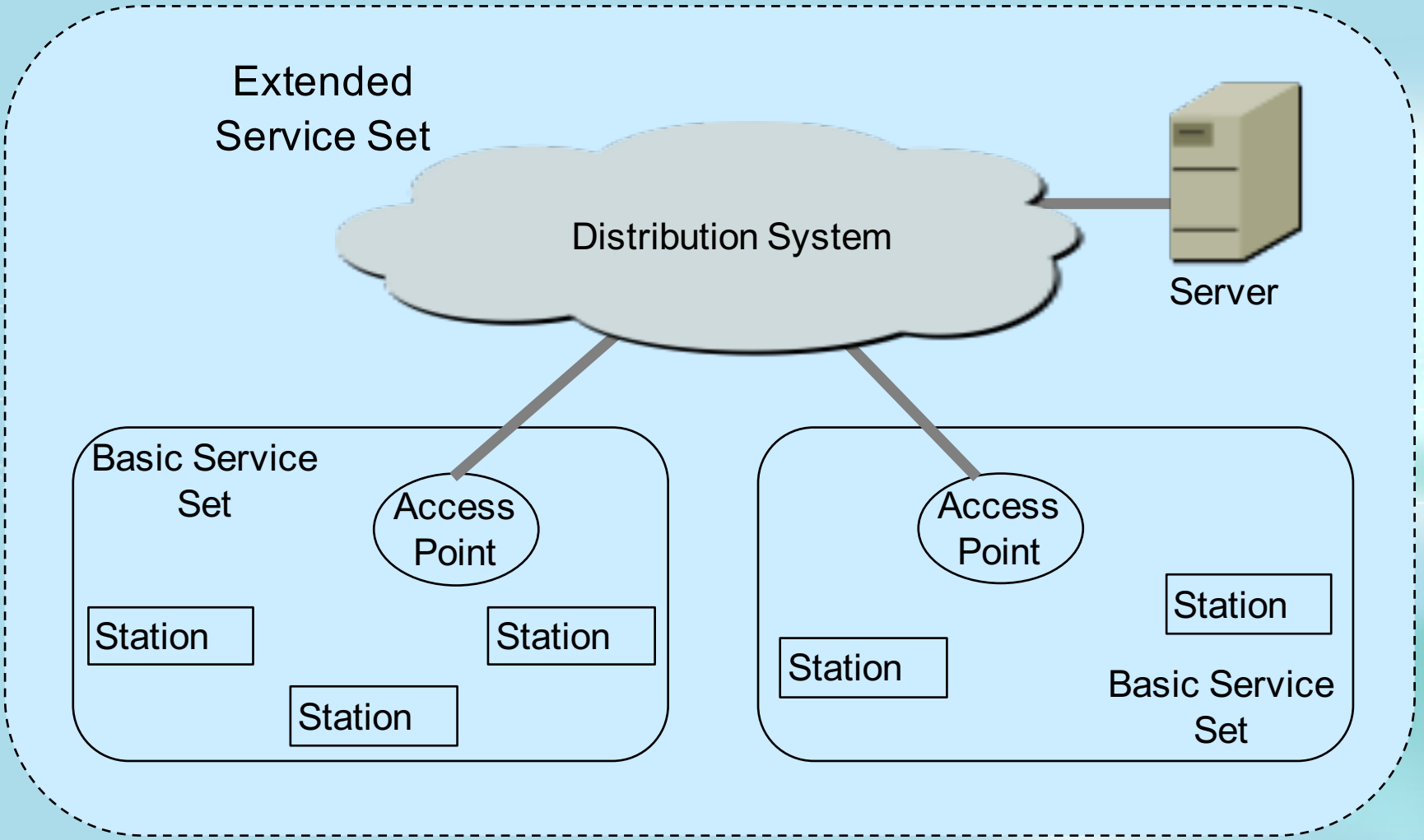
- 由一个基站和若干个移动站组成
- 基站称为AP
- 一个BSS覆盖的范围称为一个基本服务区BSA。一个BSA的范围可以有几十米的直径

802.11的组网模式

802.11定义了两种组网模式

- **Ad-Hoc 模式**
- **Infrastructure 模式**
  - 基本服务集合 **BSS**
  - 扩展服务集合 **ESS**

扩展服务集ESS


Extended
Service Set
Distribution System
Server
Basic Service
Set
Access
Point
Station
Station
Station
Access
Point
Station
Station
Basic Service
Set

扩展服务集合ESS

- ESS：Extended Service Set 扩展服务集合
- 由多个BSS通过一个分布式系统DS（Distribution System）互联而成，就像一个逻辑上的局域网
- 一般来说，DS是一个有线主干局域网，通常表现为以太网
- BSS之间的通信将通过DS实现，BSS在LLC子层上相统一，至此，一个移动主机可以漫游在不同的BSS之间

无线局域网

- 无线局域网的组成
- 802.11物理层
- 802.11MAC子层协议

802.11标准中的物理层

- 802.11：制定于1997年
- 802.11a：制定于1999年
- 802.11b：制定于1999年
- 802.11n：2008年，300-600Mbps
- 802.11ac：2012年，1Gbps

802.11物理层

- **FHSS** 跳频扩频 :使用**2.4G**的**ISM**频段。有**79**个信道供跳频使用，每个频道带宽**1MHz**。使用一个伪随机数发生器产生跳频序列。
- **DSSS** 直接序列扩频:也用**2.4G**的**ISM**频段
- 红外线**IR**:用于室内传送数据，接入速率**1- 2Mb/s**

802.11a的物理层

- OFDM 正交频分多路复用:工作在5GHz频带，可以使用的速率为6，9，12，18，24，36，48，56Mb/s
- OFDM将信号分割成许多个窄的频段，基于相移调制，形成多个正交子信道，将高速数据信号转换成并行的低速子数据流，调制到在每个子信道上进行传输，速度可以达到更高。

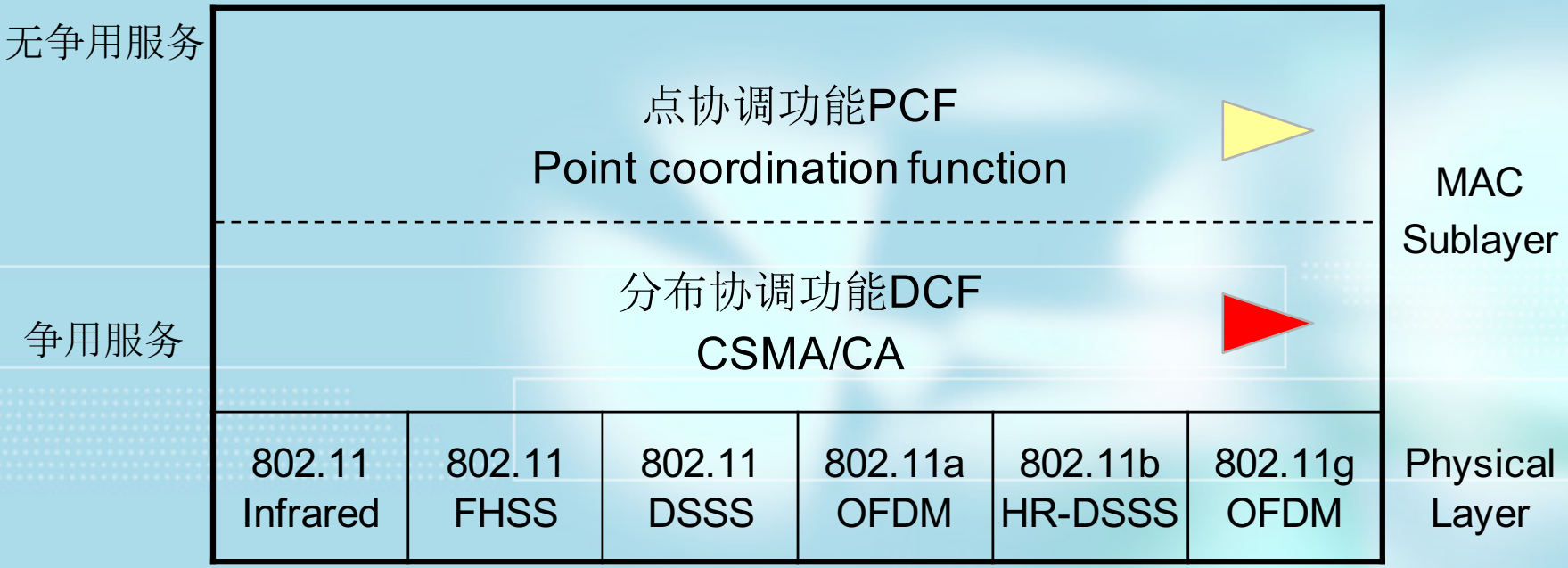
802.11b的物理层

- HR-DSSS(高速率的直接序列扩频)使用工作在2.4G的DSSS，数据率为5.5或11Mb/s

无线局域网

- 无线局域网的组成
- 802.11物理层
- 802.11MAC子层协议

802.11的MAC层协议栈



分布式协调功能

- DCF模型中每个站点都是相互独立的，没有主从关系，如同在Ethernet中一样，必须通过竞争获得信道DCF采用CSMA/CA，即带冲突避让的载波多路侦听
  CSMA/CA：CSMA with Collision Avoidance
- 无线局域网为什么不能使用CSMA/CD?
  - CSMA/CD要求每个站点在发送数据的同时还必须不间断地检测信道，而在无线局域网的设备中要实现这个功能花费过大
  - 即使发送端能够实现碰撞检测，在接收端仍可能发生碰撞

信号发送半径

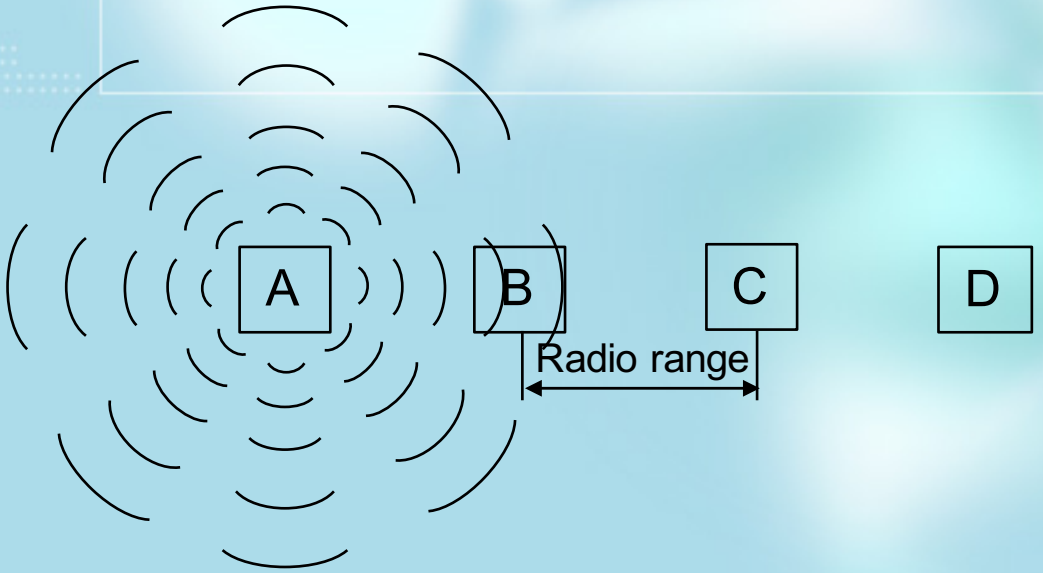
每个移动主机的发射功率有限，其发出的信号只能使一定半径范围内的主机能够检测到，从而存在两种错误的判断

- 信号发送半径引起的错误判断 1
- 信号发送半径引起的错误判断 2

信号发送半径引起的错误判断1
A、C同时发数据给B

- A发送报文给B，但因C在A的信号范围之外，C没有察觉A的发射信号，如果C同时也发报文给B，则会干扰B对A信号的接收。这个问题称为隐藏站点的问题。

（Tnbm P268 Fig. 4-11a）



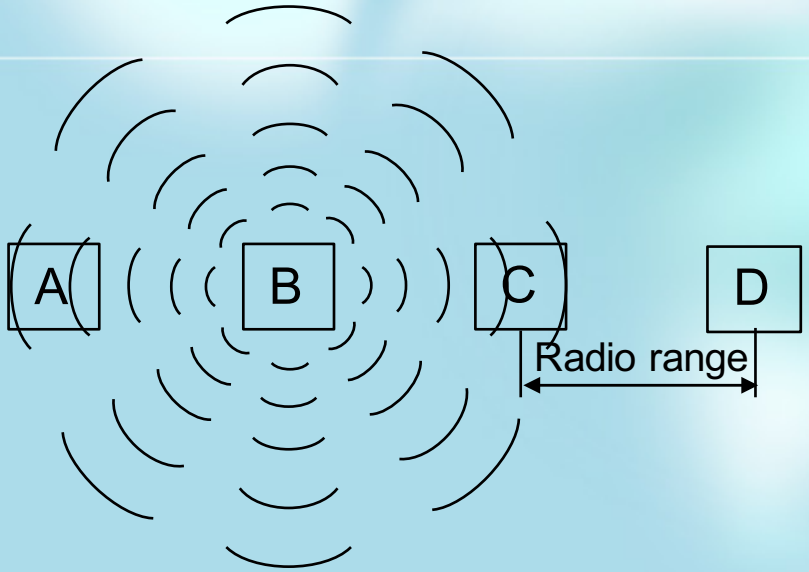
信号发送半径

每个移动主机的发射功率有限，其发出的信号只能使一定半径范围内的机器能够检测到，从而存在两种错误的判断

- 信号发送半径引起的错误判断 1
- 信号发送半径引起的错误判断 2

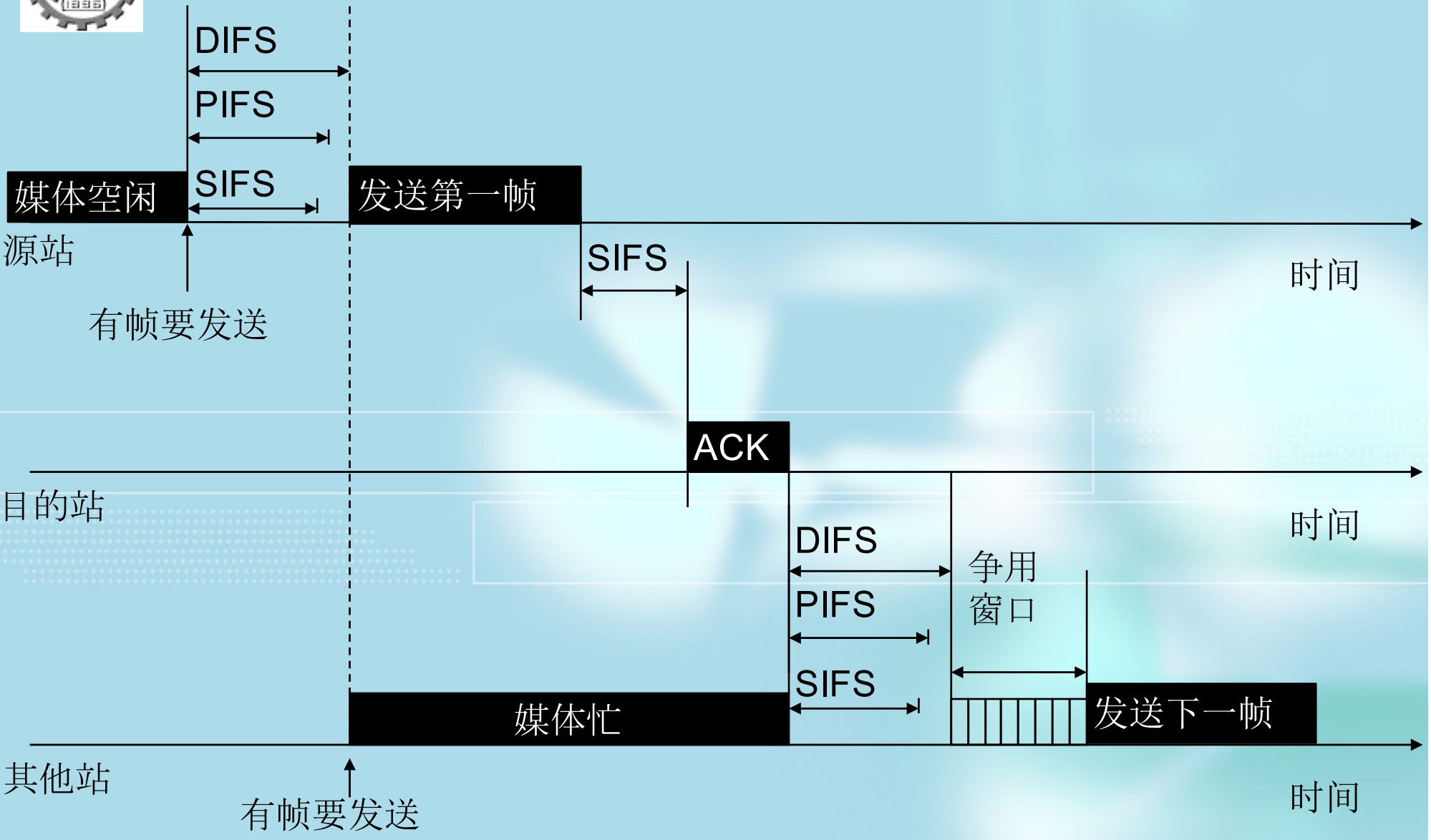
信号发送半径引起的错误判断 2
B向A发数据影响C向D发数据

- 如果B正发送报文给A，C也暴露在B的发送信号范围之内，如果此时C希望发送报文给D，但由于C检测到信道上有信号，就不会发送，其实，此时C发报文给D应该是没有问题的。这个问题称为暴露站的问题（Tnbm P268 Fig. 4-11b）



CSMA/CA

- 任何站在完成发送后必须等待一段很短的时间才能发送下一帧，这段时间称为帧间间隔IFS(InterFrame Space)。间隔时间的长短取决于该站打算发送的帧类型。高优先级的帧等待时间短，低优先级的帧等待时间长。
- 争用：当信道从忙转为空闲时，任何站在发送数据前，都要采用二进制后退算法减少发生冲突的概率。与以太网不一样的是第i次后退是从2^{2+i}个时隙中选取一个


DIFS
PIFS
SIFS
媒体空闲
发送第一帧
源站
时间
有帧要发送
SIFS
ACK
目的站
时间
DIFS
争用
窗口
PIFS
SIFS
媒体忙
发送下一帧
其他站
时间
有帧要发送

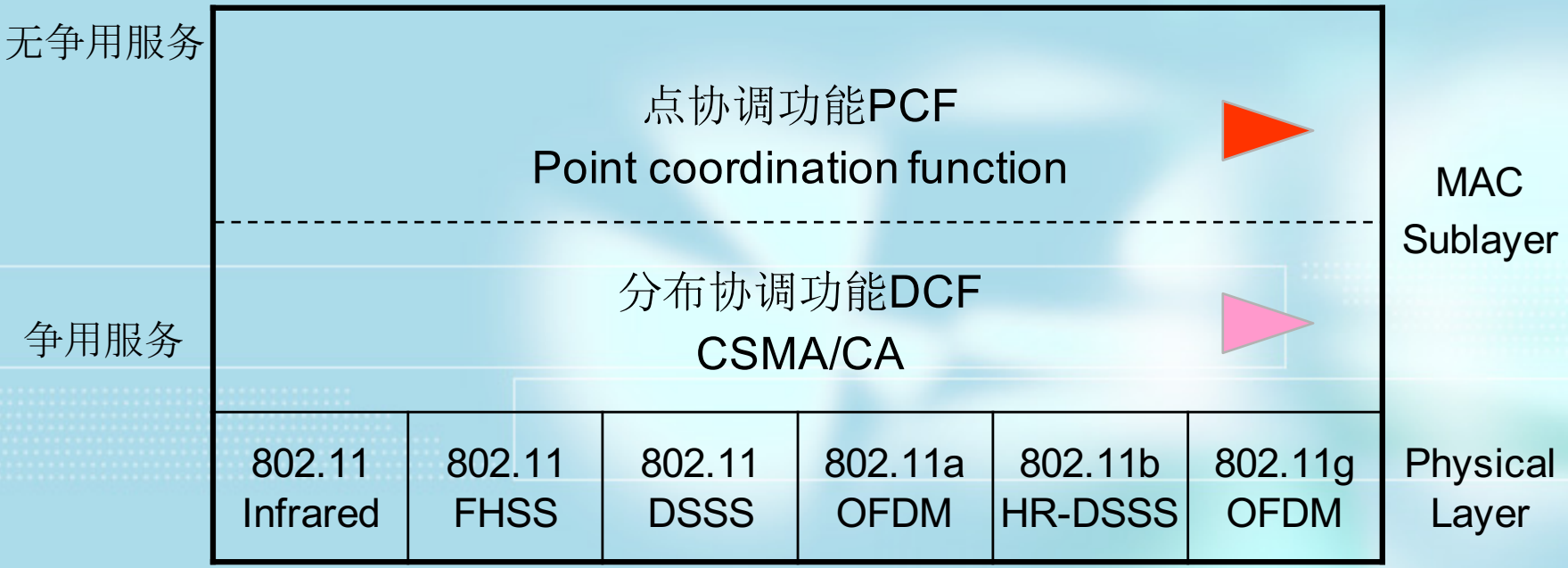
帧间间隔IFS

- **SIFS**：短帧间间隔，长度为**28μs**，用来分隔一次对话的各帧。使用**SIFS**的帧类型有**ACK**、**CTS**、如果长的帧分片后的数据帧以及所有回答**AP**探寻的帧和在**PCF**方式下**AP**发出的任何帧
- **PIFS**：比**SIFS**长。为了在开始使用**PCF**方式时优先获得接入到媒体中。它的长度是**SIFS**加一个时隙，为**78 μs**。
- **DIFS**：最长的**IFS**。用在**DCF**方式中发送数据帧和管理帧。长度为**PIFS**加一个时隙，为**128 μs**

虚拟载波侦听

- 源站将占用信道的时间(包括发送确认的时间)通知所有其他站，使他们在这一段时间都停止发送
- 实现方式：源站将所需时间填入MAC帧的“持续时间”字段中，其他站根据该字段值调整自己的网络分配向量NAV。NAV指出需要多少时间才能使信道转为空闲

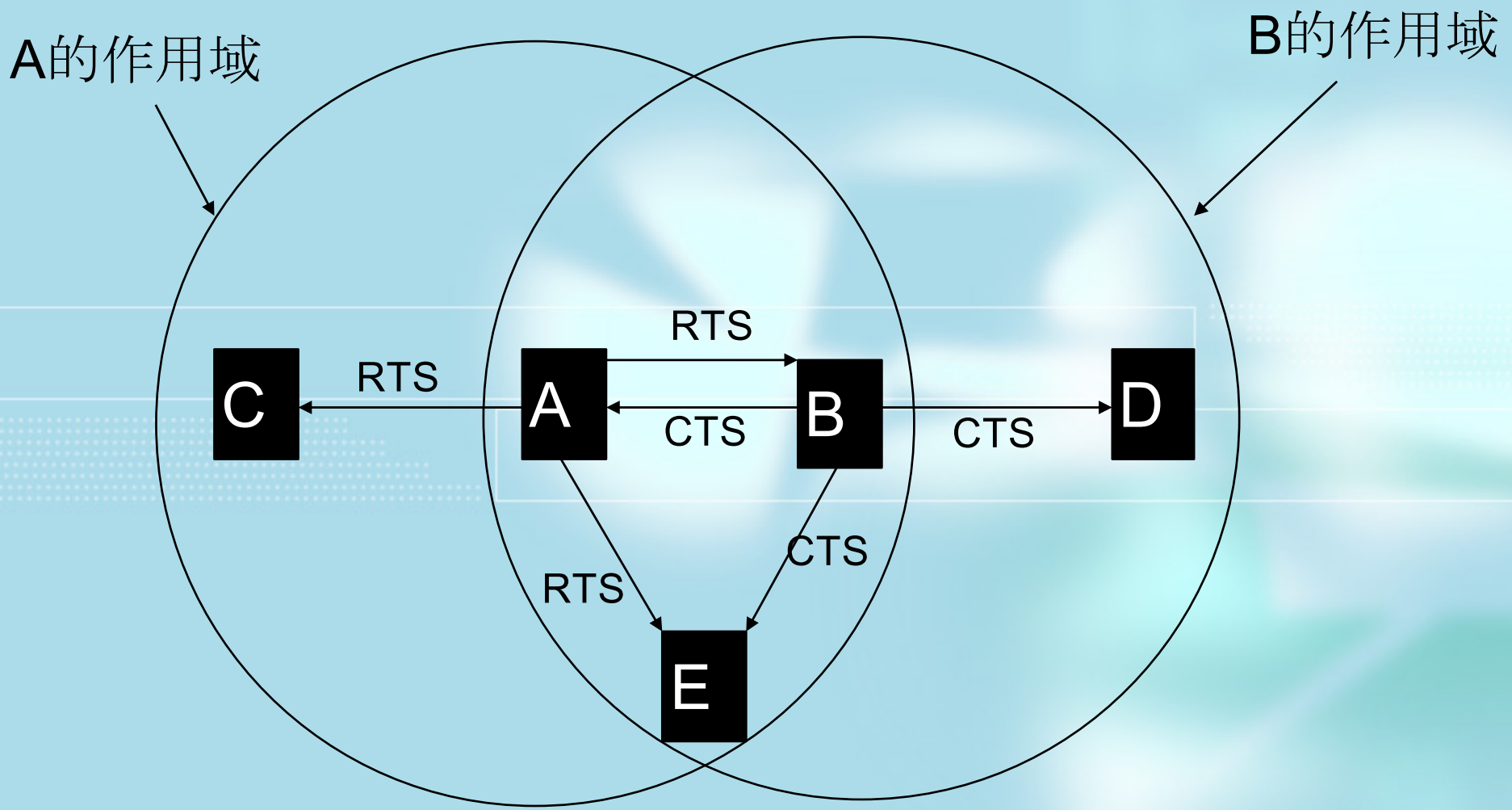
802.11的MAC层协议栈



点协调功能PCF
--对信道进行预约

- 源站A在发送数据前先发送一个控制帧RTS(请求发送)，它包括源地址、目的地址和所需时间。若信道空闲，目的站B发回一个控制帧CTS(允许发送)。A收到CTS后就可开始发送数据帧。

其他站点的反应



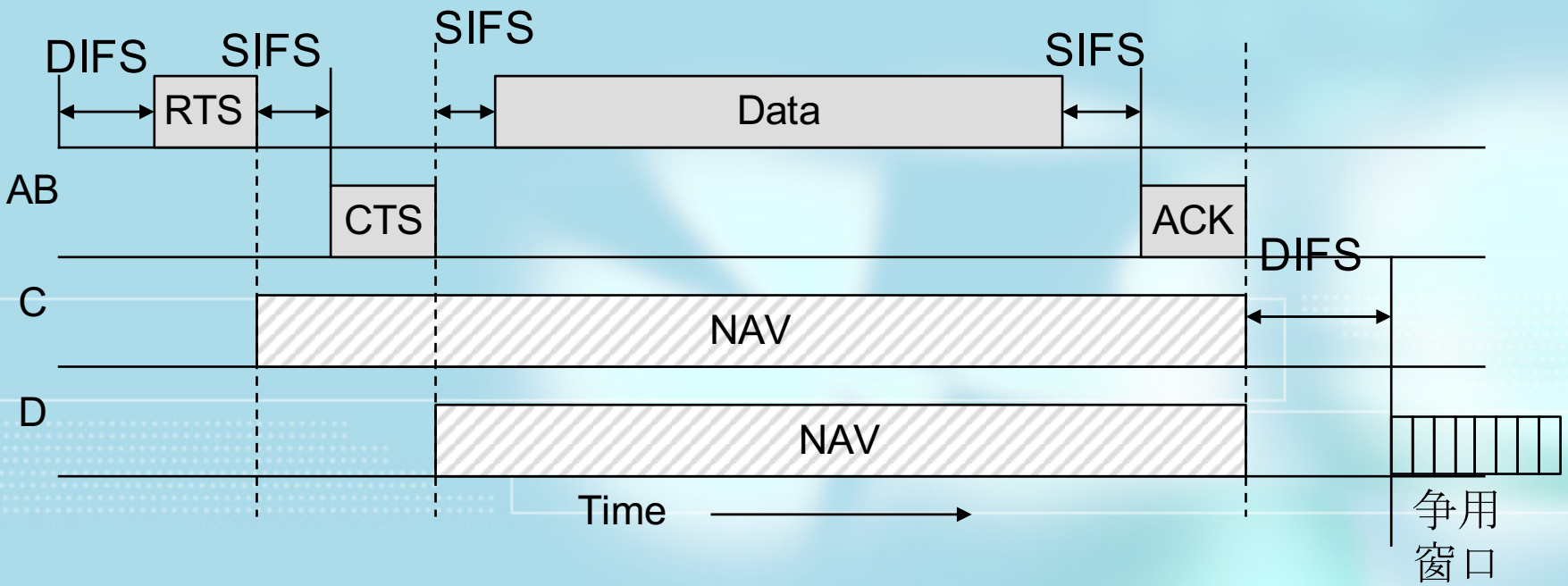
其他站点的反应

- C能收到RTS但收不到CTS，因此在A、B通信期间，C也可以和其他站点通信，而不会干扰B接收数据
- D收到CTS，因此D知道B将和A通信，在这段时间内，D不能发送数据
- E既能收到RTS又能收到CTS，因此在A、B通信期间，E不能和其他站点通信

碰撞的解决

- 当B、C同时向A发RTS时，将会发生碰撞
- 碰撞后将会采用二进制后退算法解决

ＰＣＦ的实现过程



Tnbm P297 Fig.4-27 使用CSMA/CA的虚拟信道侦听

第4章 习题

Tnbm P338

#2、#5、#6

#19、#20