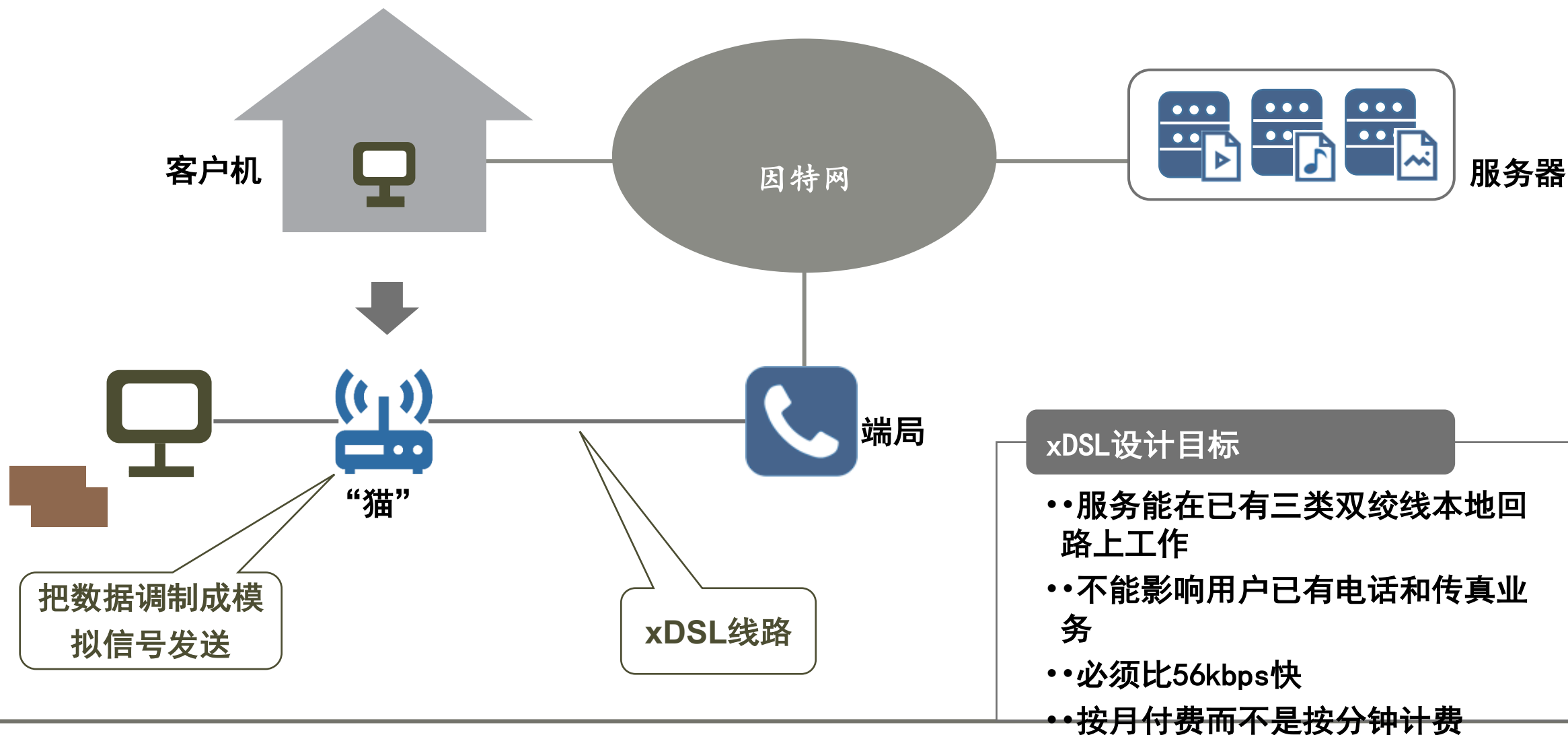


# 案例学习一

## ADSL接入因特网

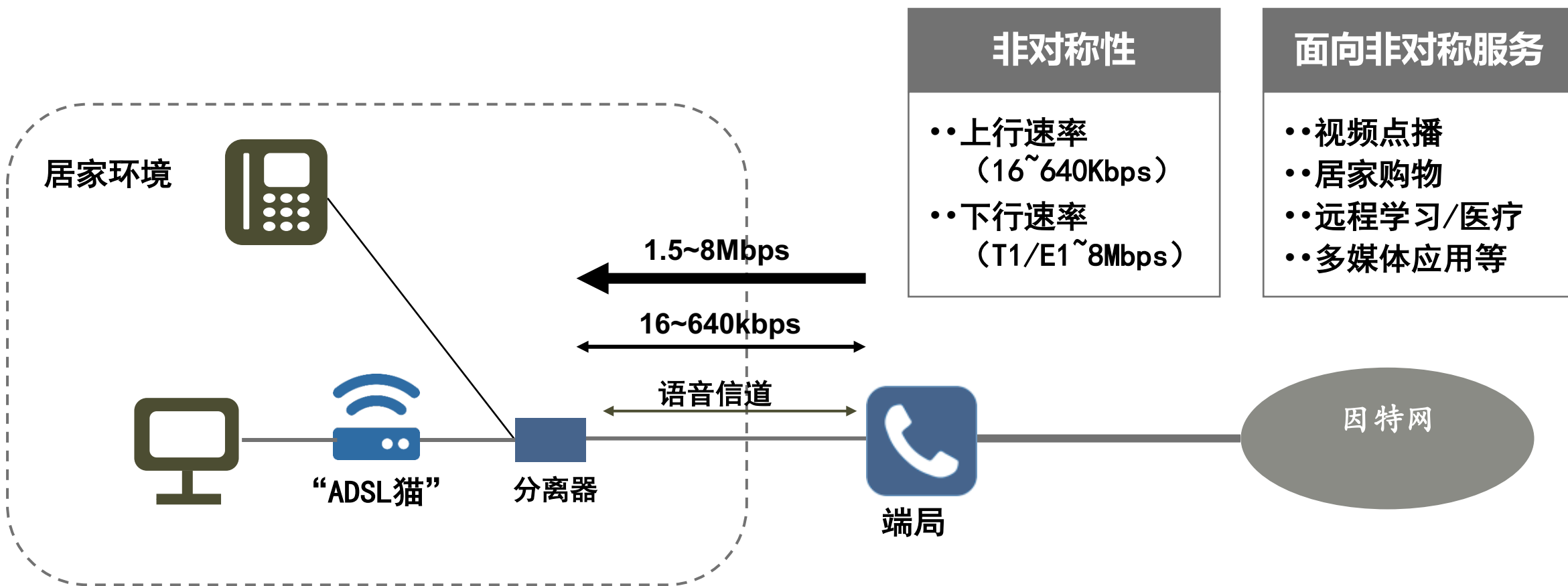


# 数字订户线路 (DSL)



# 非对称DSL(ADSL)

非对称DSL：运行在已有普通电话线上的一种新的高速宽带技术。

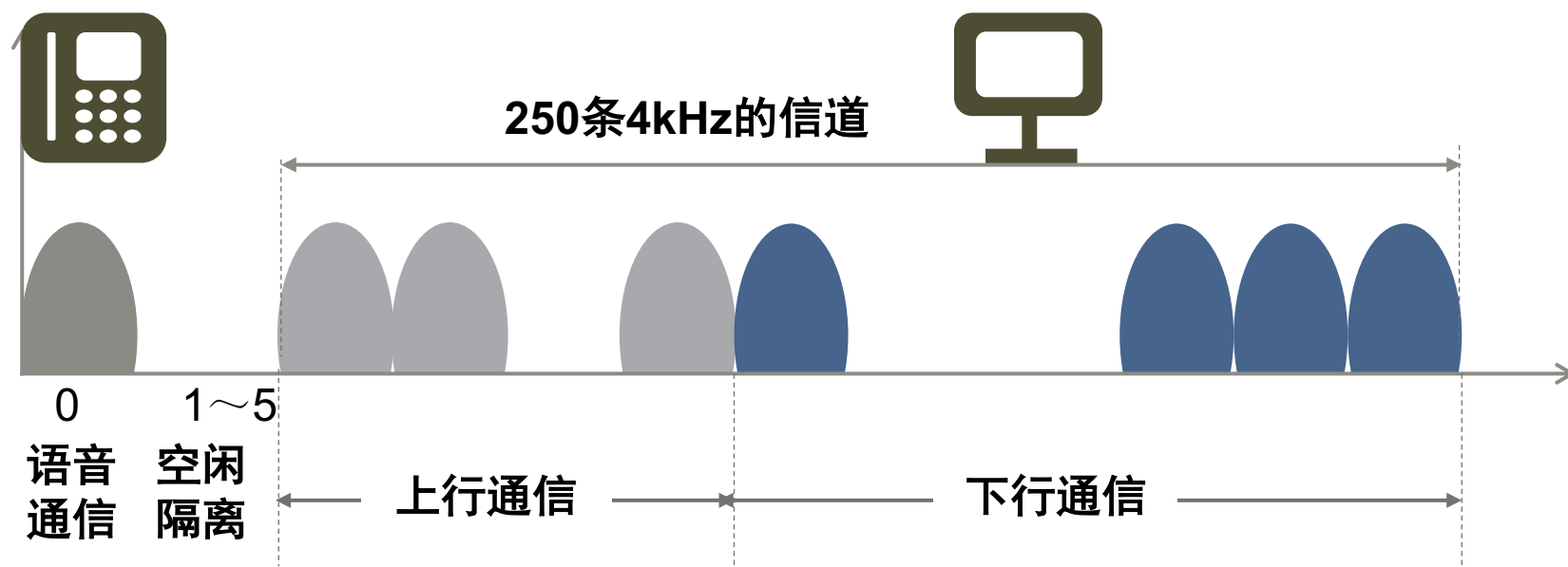


# ADSL标准及信道分配

## 高速率的获得

- 采用积分调幅，4个幅值\*4个相位共有16种组合
- 每个信号携带4个比特

ADSL标准	下行速率	上行速率
G.dmt	8Mbps	1Mbps
ADSL2	12Mbps	1Mbps
ADSL2+	24Mbps	1Mbps



250个信道的上下行分配决定了上下行通道的速率。



# 点到点协议(PPP)

点-点协议是一个可用于调制解调器、比特串行线路、SONET和其他物理层的多协议成帧机制。



## PPP的设计目标

- 给出一种组成帧的方法
- 支持多种网络层协议
- 支持多种链路
- 具备差错检测能力
- 网络层地址可协商

IP/其他

PPP

ADSL电路/  
其他

## PPP不包括功能

- 差错纠正
- 流量控制
- 顺序性
- 多点链路



# PPP标准组成及工作过程

- RFC1661
- RFC1662
- RFC1663

明确的成  
帧方法

••一种将数据封装成  
PPP帧的方法

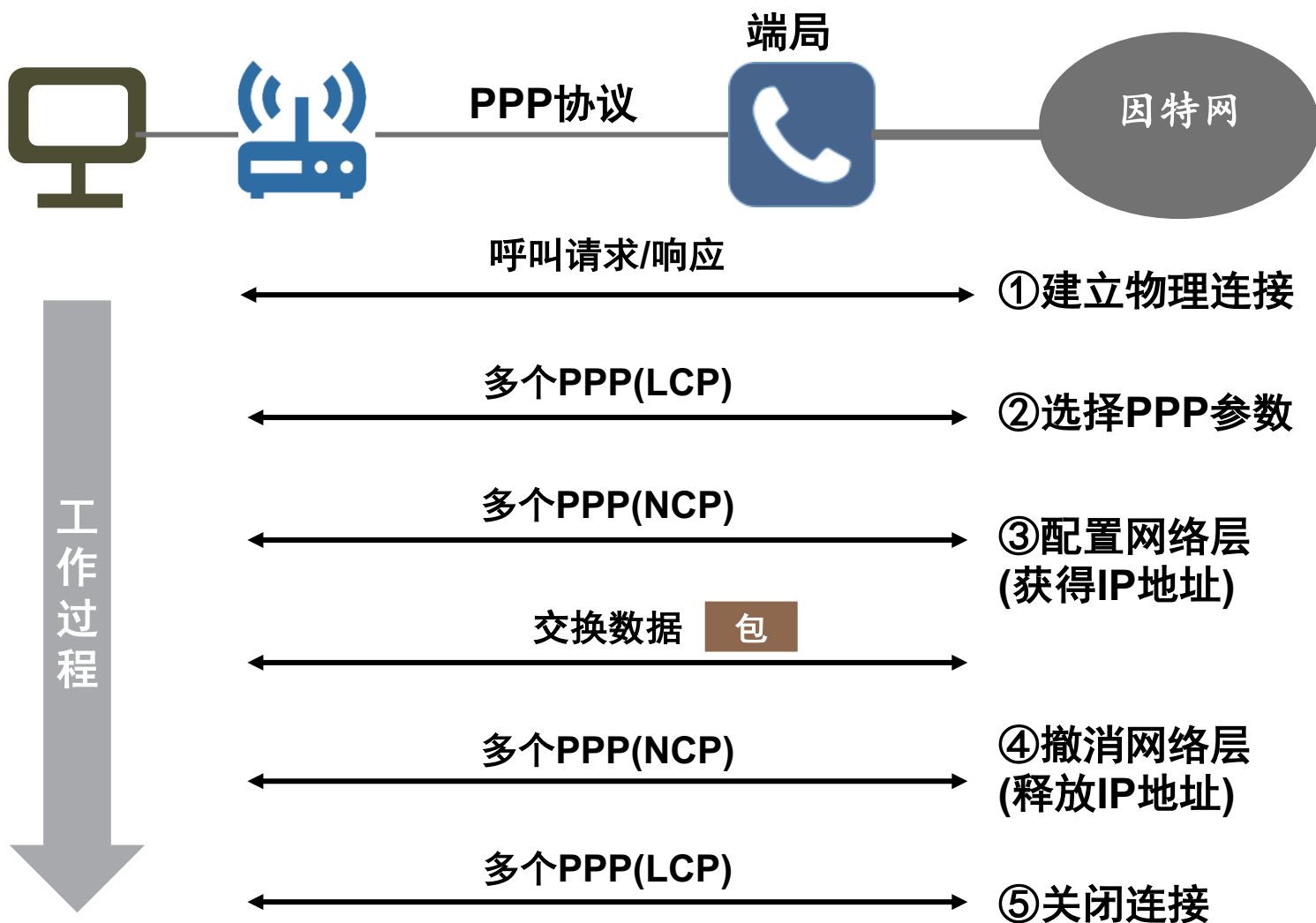
一个链路  
控制协议  
(LCP)

••一个初始化、维护和  
拆除PPP链路的协议

一组网络  
控制协议  
(NCP)

••一组协议，每个用于  
一个高层网络层协议。

工作  
过程



北京大学

network-control protocols : 网络控制协议/ link-control protocol : 链路控制协议

# PPP的成帧方法



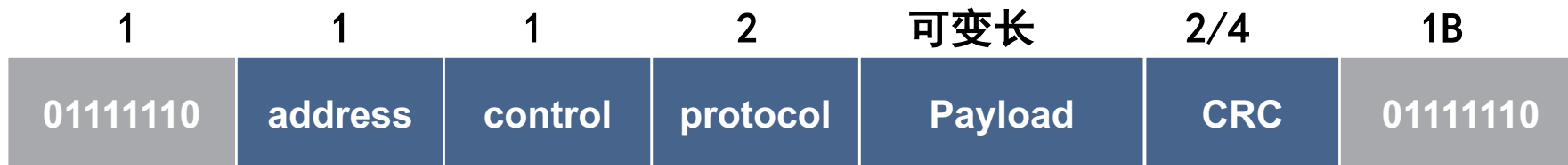
**字节填充技术:** 在数据信息字段, 若出现flag模式则在前面加一个转义字符01111101; 对于信息字段出现转义字符也作相同的处理。

在PPP帧部分出现“01111110”对接收方有什么影响

“01111110” →  
“01111101” “01111110”  
“01111101” →  
“01111101” “01111101”



# PPP帧格式



- **Address**  
地址字段固定为“11111111”
- **Control**  
控制字段固定为“00000011”
- **Protocol**  
协议字段标识其上层用户(IP协议)
- **Payload** (缺省1500B)  
有效载荷运载数据信息/控制信息
- **CRC**  
循环校验码, 2字节/4字节

?

没有序号和确认号  
字段意味着什么

## Protocol 字段定义 (2B)

- 0021: IP
- 0023: OSI CLNP
- 0027: DECnet
- 0029: Appletalk
- 002B: Novell
- C021: PPP Link Control Protocol
- 8021: IP Control Protocol

**RFC1700**

(RFC1332)





# PPP协议的控制帧

**LCP帧：用来协商最大帧长、认证协议等。**

- 哪些字符用于转义
- 是否发送地址字段
- 是否压缩协议字段

1	1	1	2	可变长	2/4	1B
01111110	11111111	00000011	C021	Connection control data	CRC	01111110

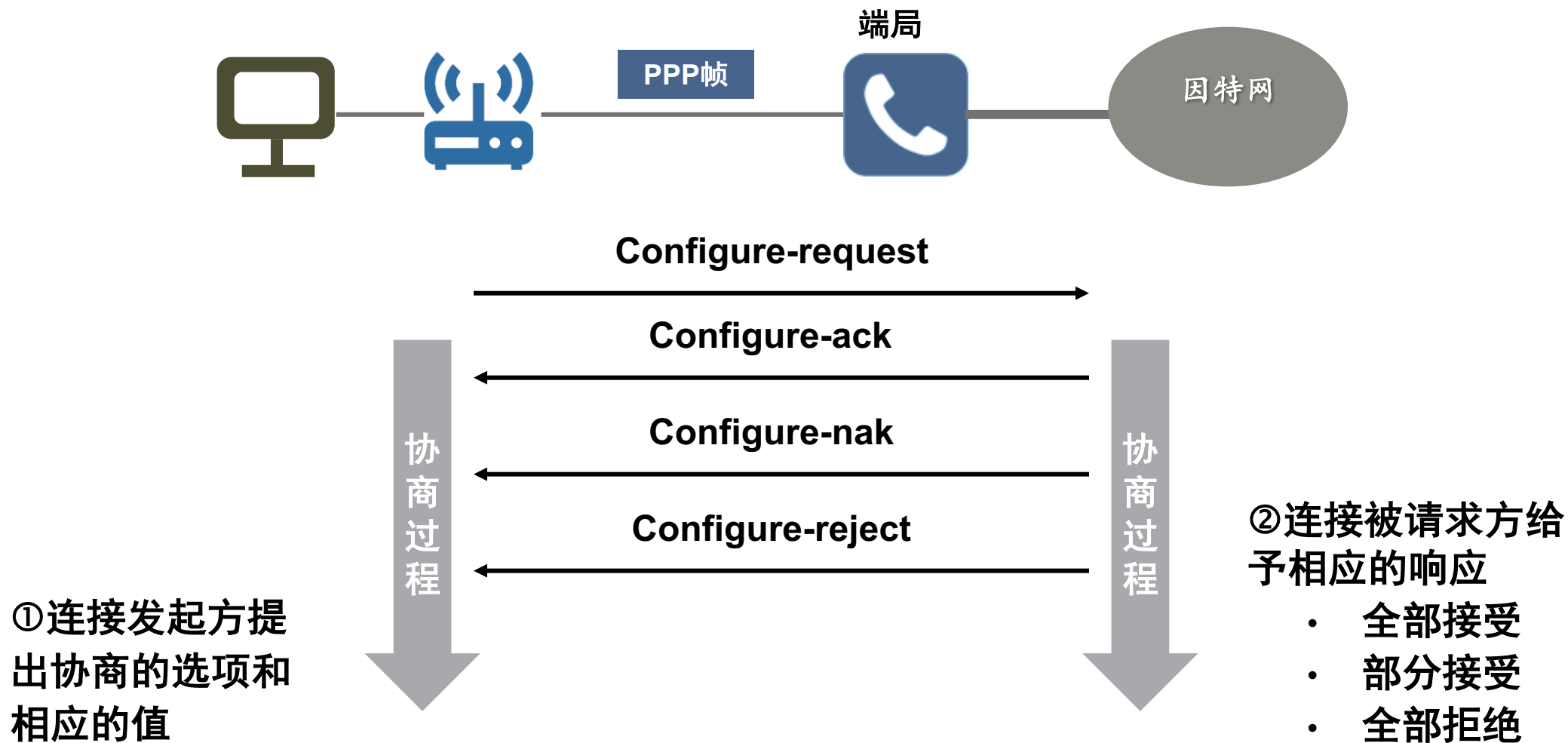
**NCP帧：协商报头是否压缩；协商IP地址**

- 分配网络层地址
- 是否压缩包头

1	1	1	2	可变长	2/4	1B
01111110	11111111	00000011	8021	Connection control data	CRC	01111110



# PPP控制协议的协商过程



# 案例学习二

## 有线电视网接入因特网

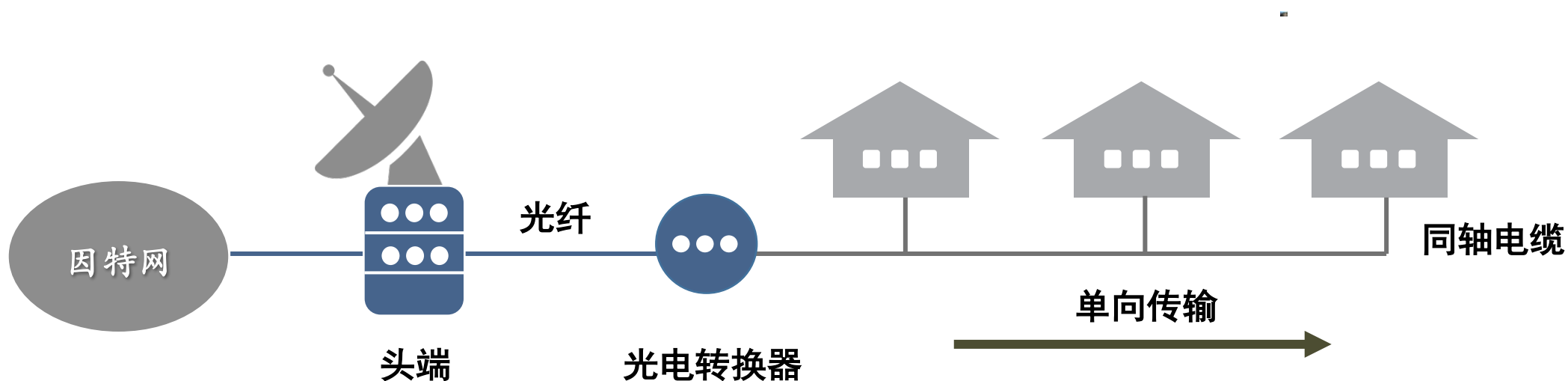


# 有线电视系统

## 公用天线系统

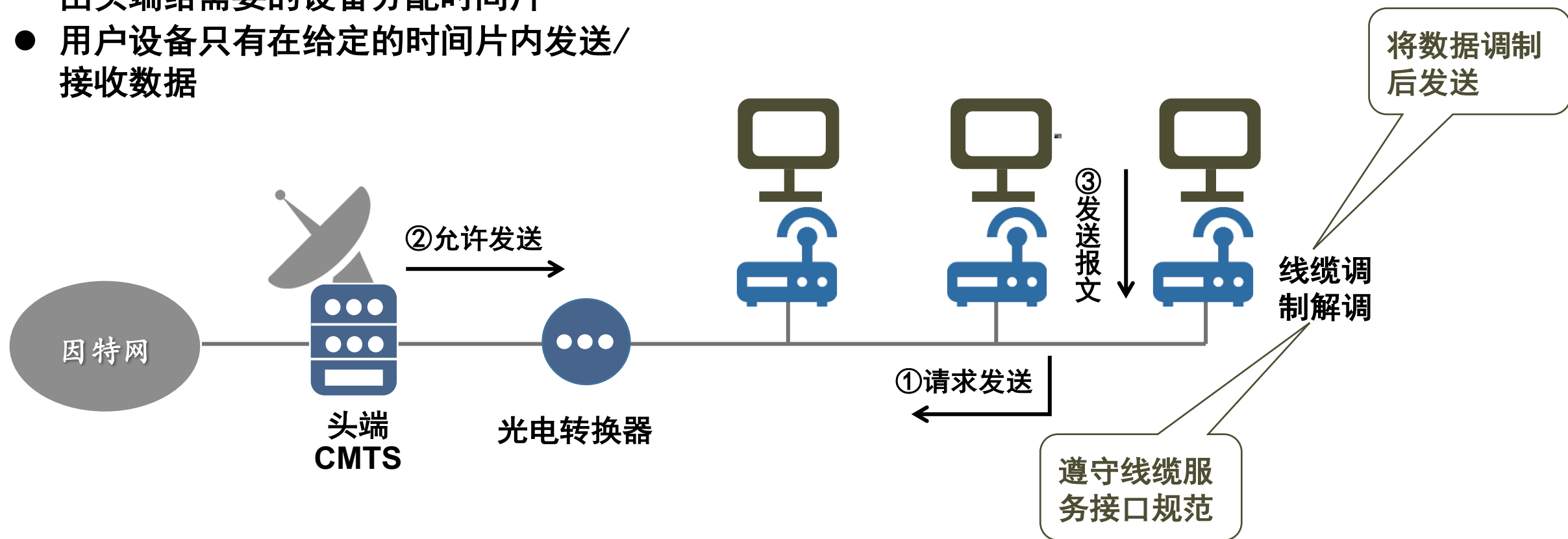
- 天线
- 头端 (head end)
- 有线电视电缆 (线缆)

HFC系统：中长距离使用光纤，连接到家庭使用同轴电缆。



# 通过有线电视线缆访问Internet

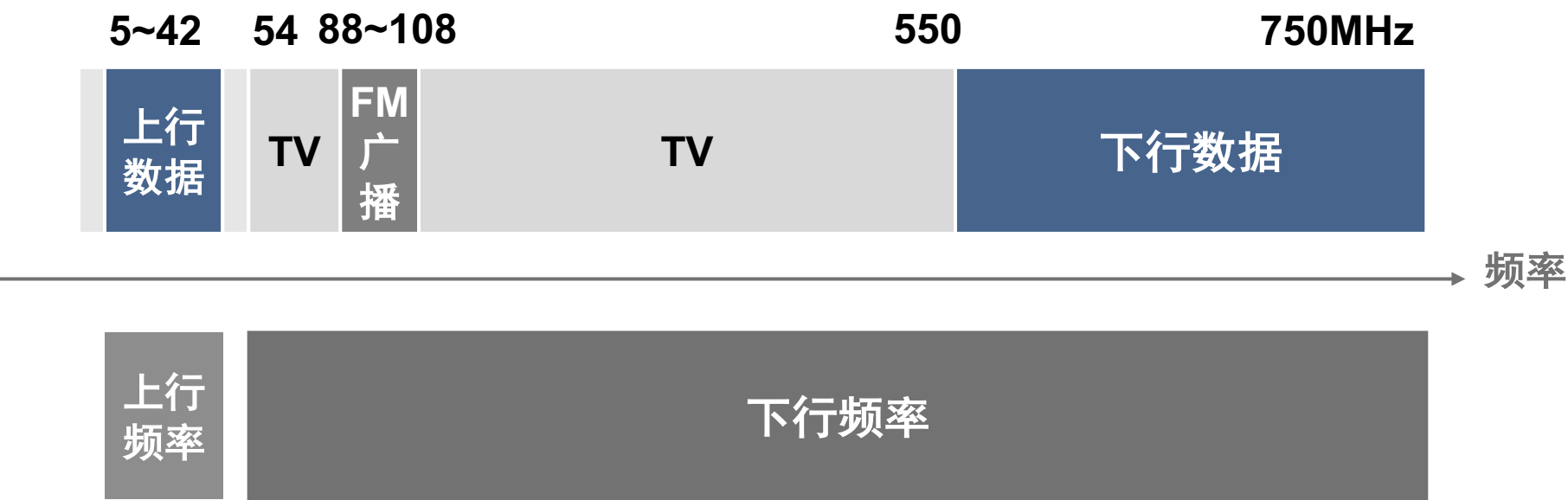
- 多个用户设备共享同一根同轴电缆，由头端给需要的设备分配时间片
- 用户设备只有在给定的时间片内发送/接收数据



# 有线电视电缆信道分配

通过FDM实行双向通信

技术	下行速率	上行速率
FDM	10M~36Mbps	200kbps-2Mbps



# 上下行信道的共享

## 下行信道的使用

- 采用TDM方式
- 固定204字节数据包（纠错码+184字节有效负载）

## 头端

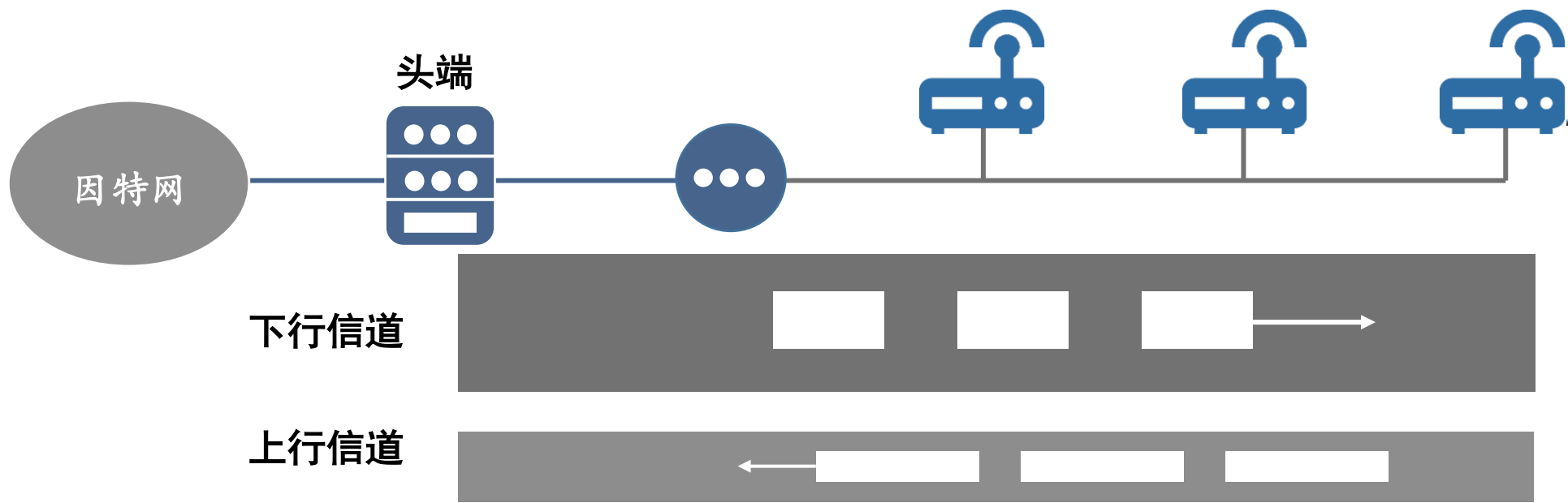
定期周期性地发送信标帧，帧内包括系统参数。

## 上行信道

采用竞争方式（冲突后随机后退）访问信道

## 下行信道

由头端根据当前用户数分配信道带宽，采用TDM技术。

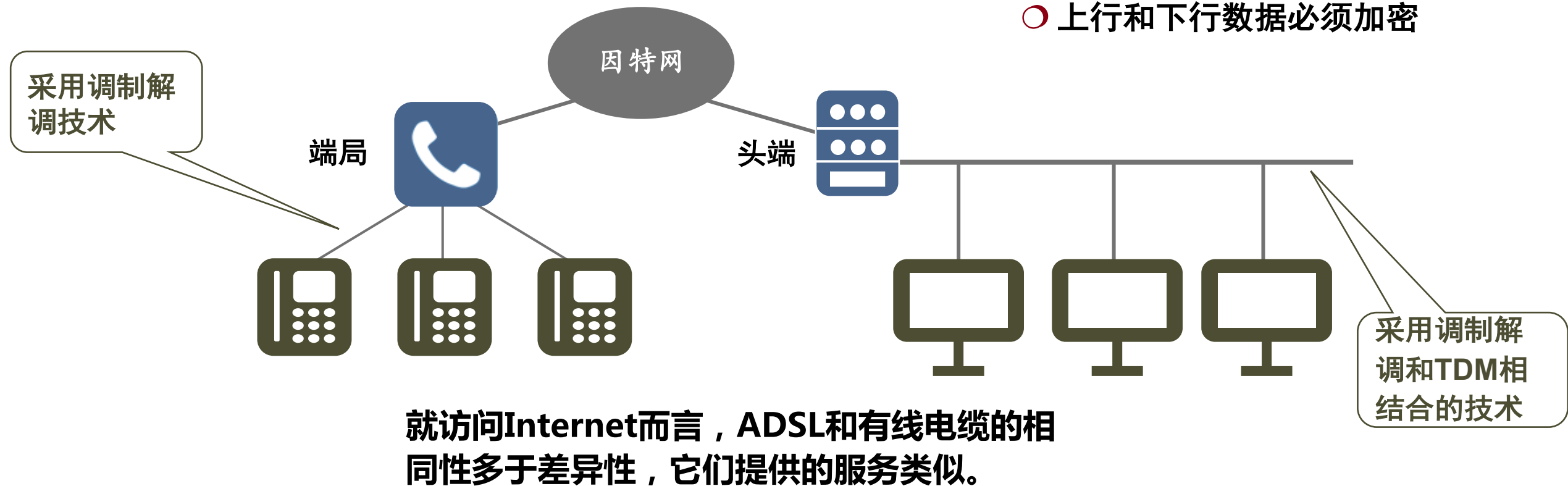


## □ ADSL采用星形结构

- 每个用户具有固定独占带宽
- 点-点通信模式

## □ CABLE 采用总线形

- 带宽由一群用户共享
- 基于广播机制
- 上行和下行数据必须加密



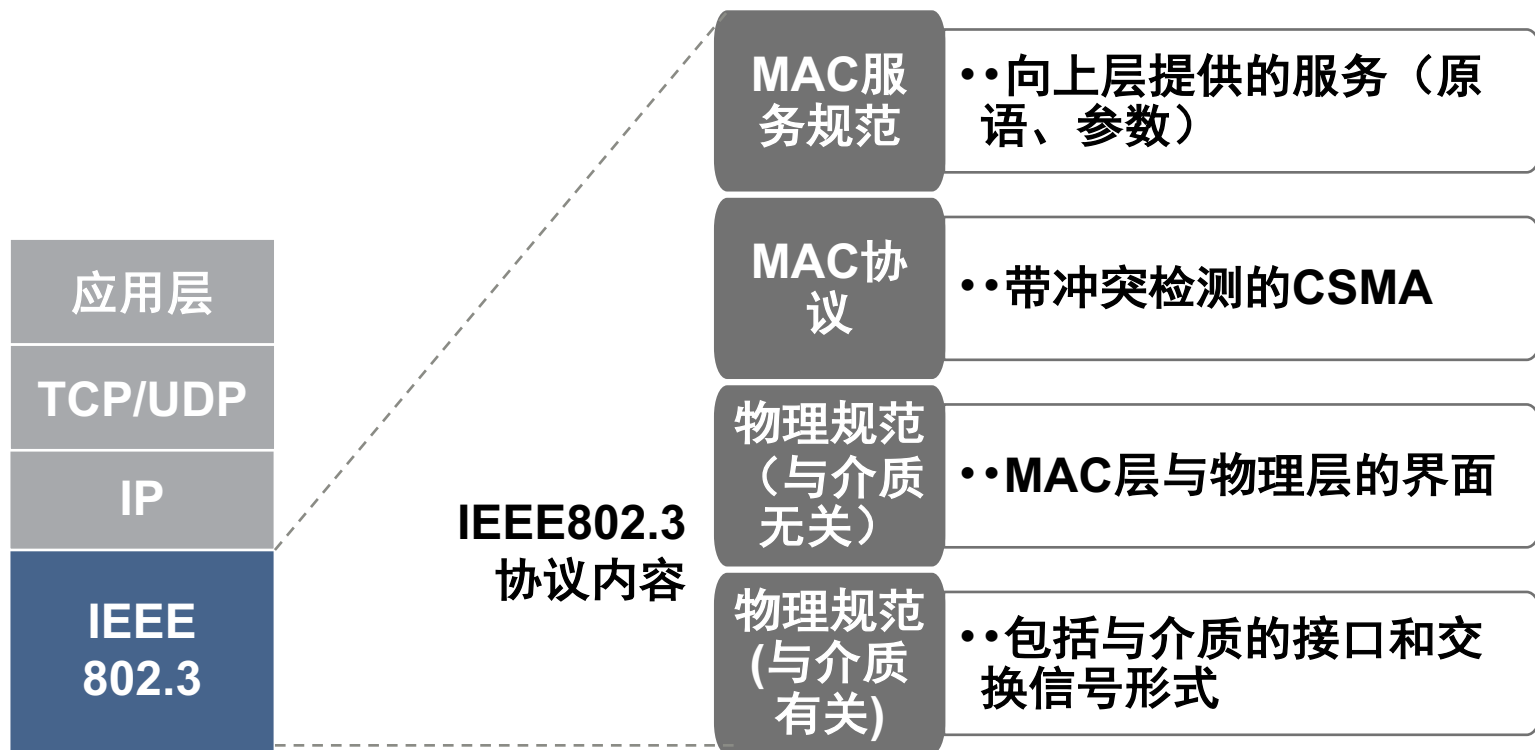


# 案例学习三

## IEEE802.3协议之访问控制



# IEEE802.3协议



David Boggs



Bob Metcalfe



# 带冲突检测的CSMA协议

## CSMA/CD基本思想

- 若介质空闲，则传输；否则
- 若介质忙，一直监听直到信道空闲，马上传输
- 若在传输期间检测到冲突，立即停止传输；等待一个随机时间

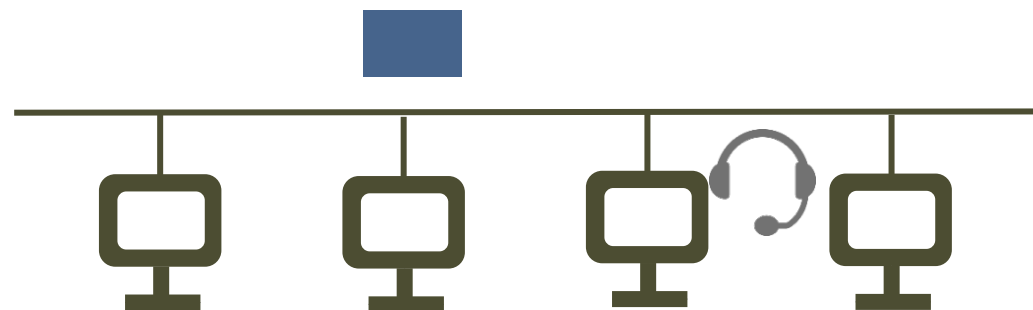
带冲突检测的载波侦听协议：网络节点侦听载波是否存在(即有无传输)并随之采取相应的行动，并在传输过程中检测是否发生冲突。

访问时机  
冲突检测  
重试策略

“讲前先听”



“讲前先听”  
“边讲边听”



# 带冲突检测的CSMA信道模型

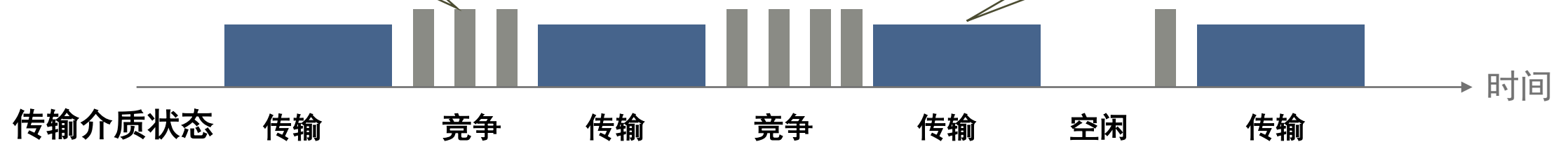
## CSMA/CD模型

- 竞争：发送节点检测到发送帧冲突的最短时间
- 传输：发送节点传输帧，且不会发生冲突
- 空闲：所有节点都处于静止状态(无帧发送)



所有需要发送的节点在此期间竞争信道的使用权

竞争胜出的节点使用信道且其他节点不会干扰

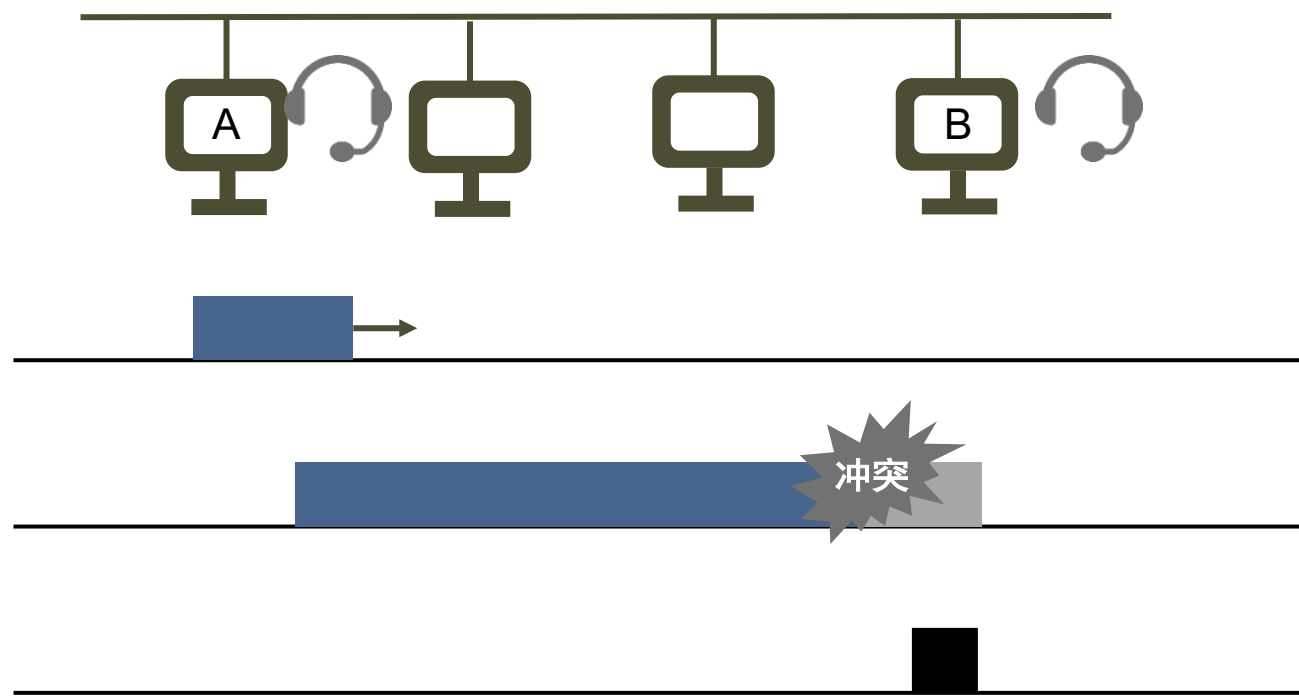


# 如何确定竞争是否胜出？

假设A和B是两个相距最远的节点，并且A到B的传播时延为 $\tau$

等 $2\tau$ 长的时间未听到冲突才能确信竞争成功抓住电缆。

访问时机  
冲突检测  
重试策略



①A发出一个给B的数据帧

②B没有侦听到信道为忙，发出一个给A的帧，该帧刚发出就与A发来的帧冲突

③B检测到冲突，产生一个特殊的加强信号发到信道，该信号经 $\tau$ 被A检测到

冲突信号 A发出的帧 B发出的帧



# IEEE802.3的冲突检测窗口

**冲突窗口：开始发送帧后侦听到是否发生冲突的那段时间。**

?

在广播网络中一个比特发出经过介质传播时间后意味着什么？

$$2\tau(+ t_{CD} + t_{JAM})$$

$2\tau$ ：最远节点之间的往返传播时间

$t_{CD}$ ：冲突检测所需的时间

$t_{JAM}$ ：阻塞信号JAM的传送时间

## 冲突处理

- 立即停止发送帧的其余内容，并发阻塞信号JAM
- 按后退算法计算重发时间延迟
- 若重发16次仍不成功，则放弃



# IEEE802.3的后退算法

CSMA/CD网络的关键问题：冲突控制或冲突分解

访问时机  
冲突检测  
重试策略

## 二进制指数后退算法

平均等待延迟为

$$M_{\text{BEN}} = (2^i - 1) * 2\tau$$

- $i$ 为帧的冲突次数
- $2\tau$ 为冲突窗口

## 截断二进制指数后退算法

平均重发延迟为

$$M_{\text{BEN}} = (2^i - 1) * 2\tau$$

- $i = \min(n, 10)$
- $n$ 为实际冲突次数

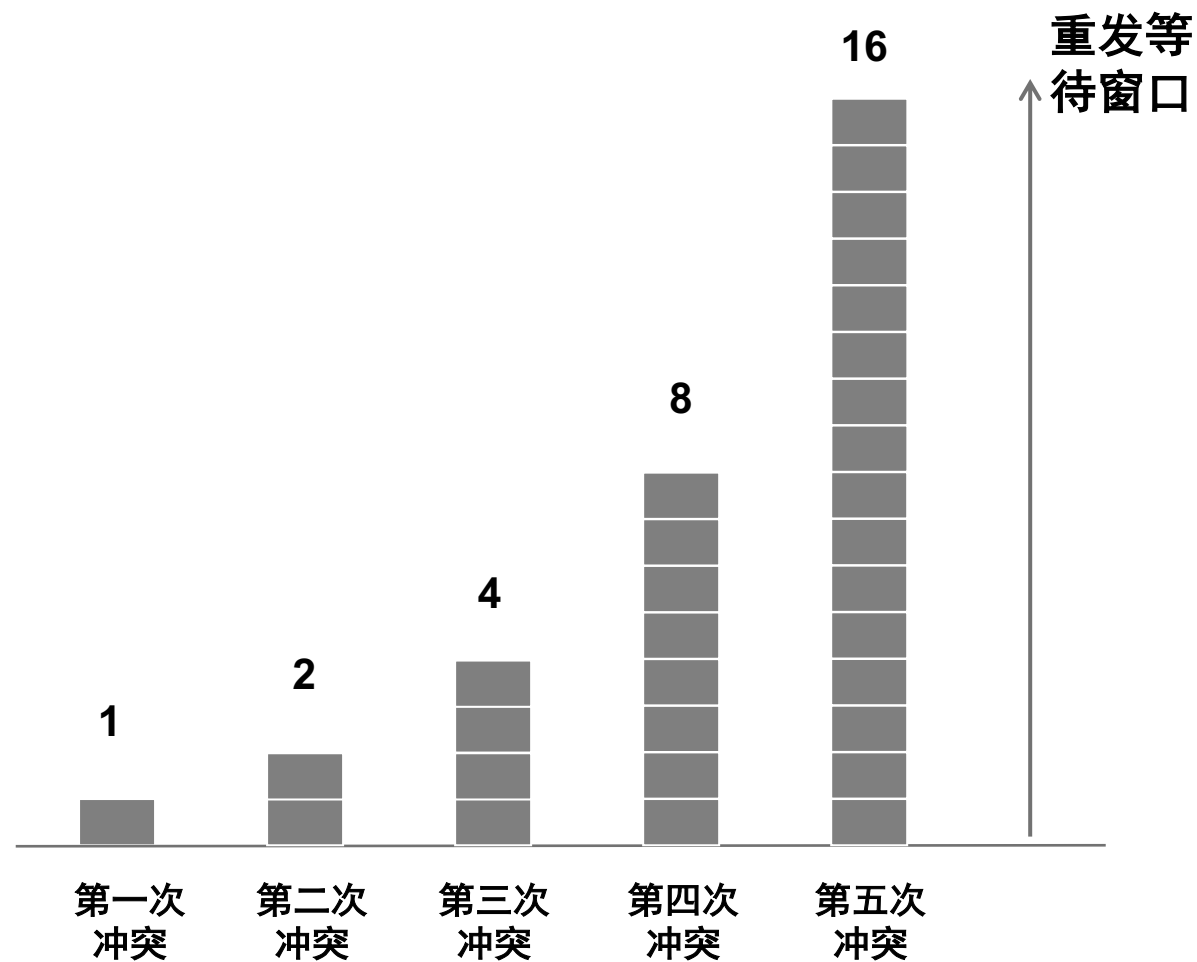


# IEEE802.3重发等待窗口

## 冲突等待重发时间

- 每冲突一次，将等待窗口大小加倍
- 从该窗口中随机选择一个等待时间

重发延迟将随冲突次数的增加而急剧增大



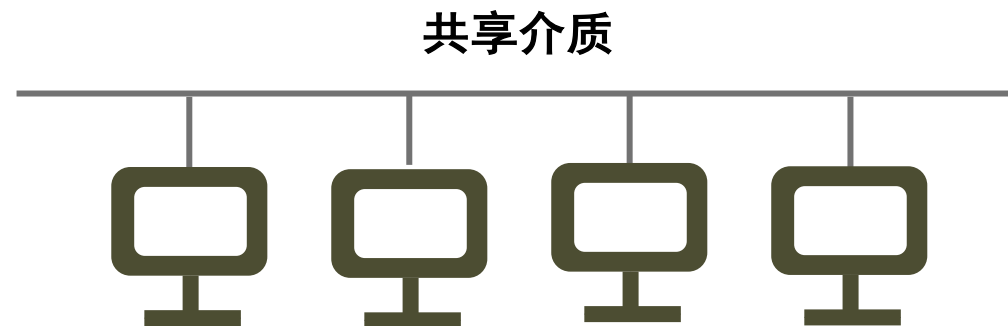


# 竞争系统与介质 访问控制



# 介质访问控制概述

介质访问控制是指将传输介质带宽有效地分配给网上各节点用户的方法。



## 同步

- 为每个节点分配一个专用固定的容量
- 类似频分多路复用或时分多路复用

## 异步

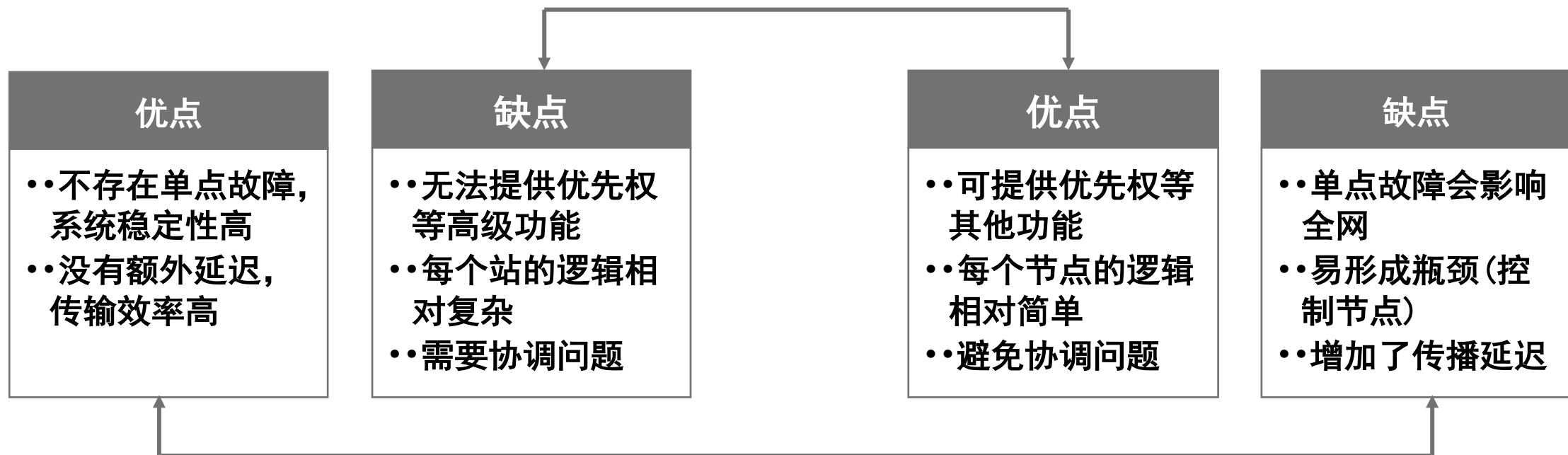
- 把信道容量动态分配给每个需要的节点
- 响应用户的即时需要



# 异步控制的实现方式

**分布式：**由各站共同完成介质访问控制，动态确定站的发送顺序。

**集中式：**指定某个控制器拥有控制网络访问的权利。

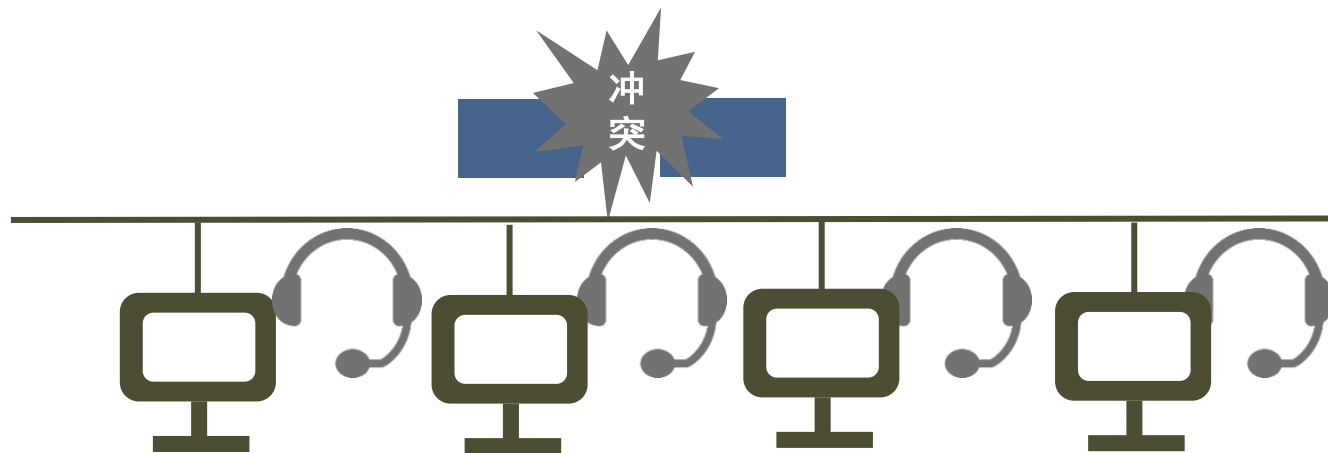


# 共享介质访问控制

## 假设

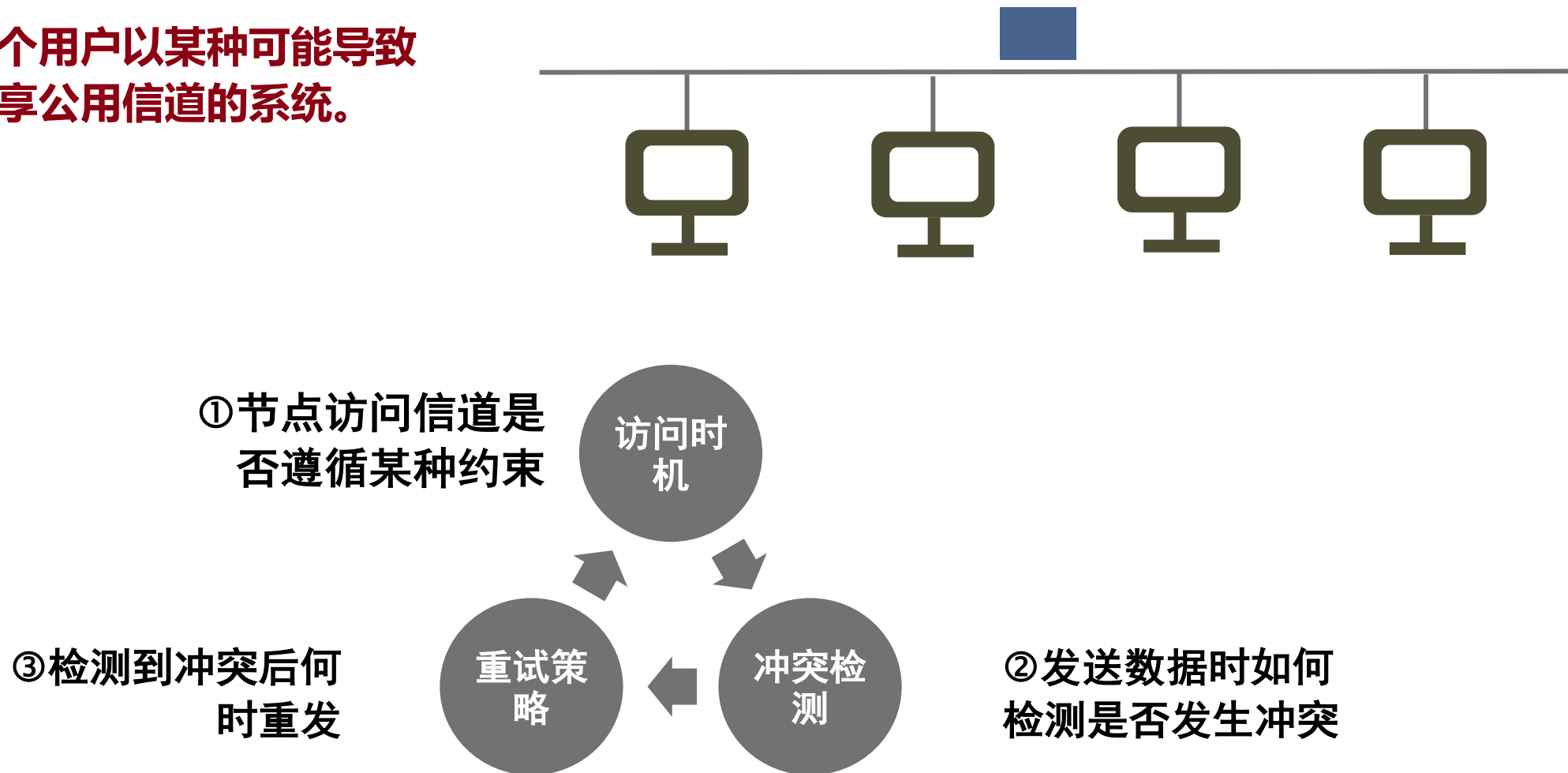
- 节点流量相互独立
- 仅一个信道可用
- 若发送冲突可观察
- 发送时机连续时间
- 发送时机按时间槽
- 发送前可载波侦听
- 发送前无载波侦听

介质访问控制协议（MAC）：将传输介质的容量有效地分配给网上各节点用户的方法。



# 竞争系统及其三大问题

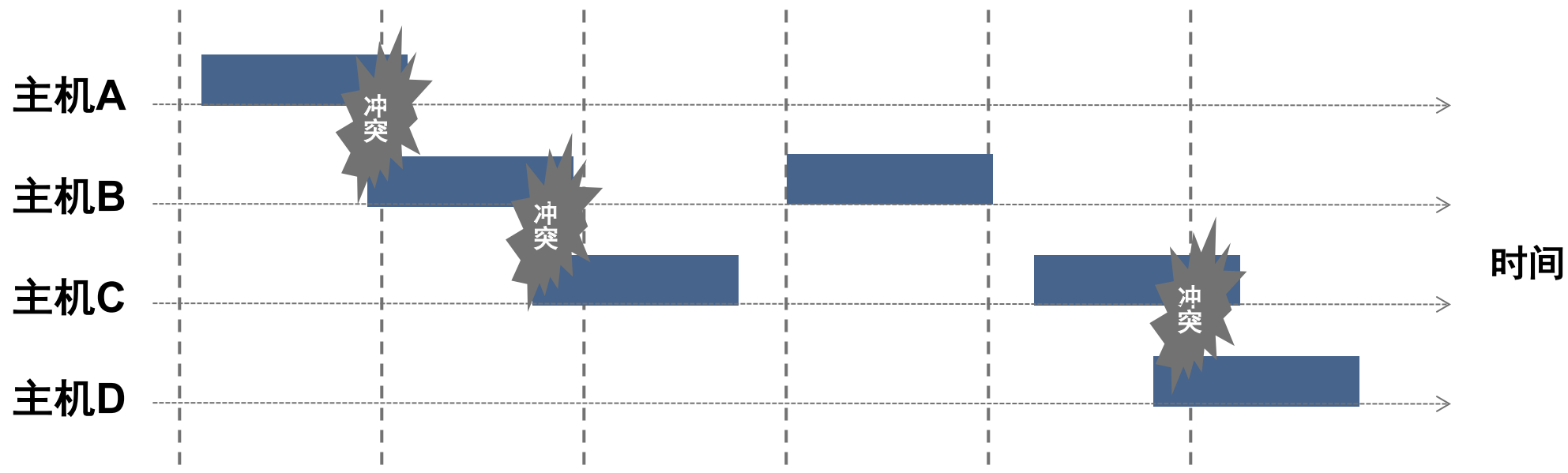
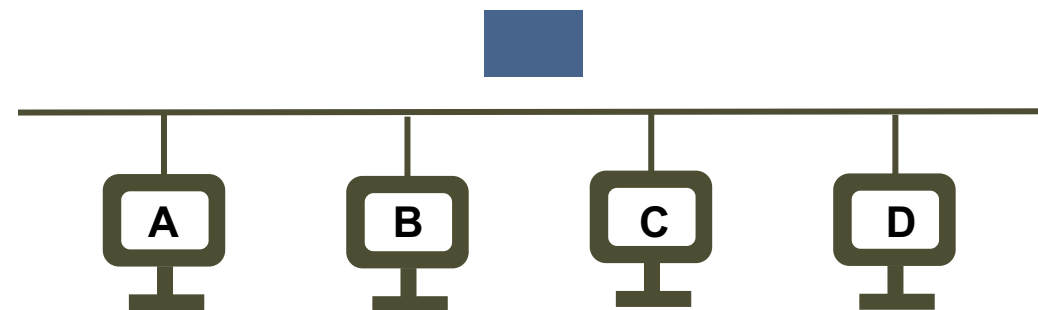
竞争系统：多个用户以某种可能导致冲突的方式共享公用信道的系统。



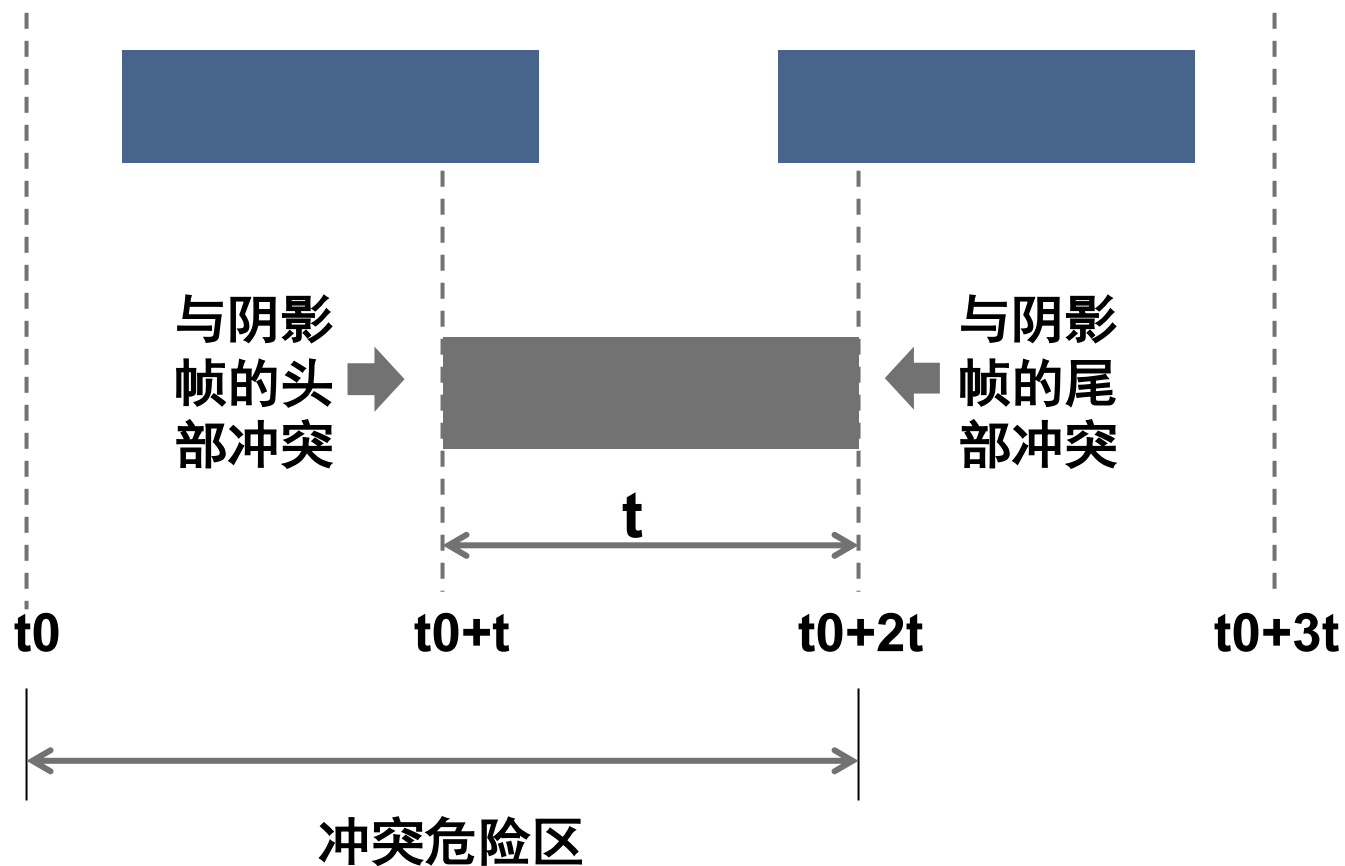
# 纯ALOHA协议基本思想

## 纯ALOHA基本思想

- 按需访问信道
- 不侦听信道
- 发生冲突随机重发



# 纯ALOHA协议访问方式



能够期待的信道利用率  
最多为18%

**冲突危险区：一个帧被发送时，在该时间范围内其他节点的发送必将破坏该帧的传输。**



# 分槽ALOHA协议基本思想

## 分槽ALOHA基本思想

- 访问信道只能在时间槽开始时进行
- 不侦听信道
- 发生冲突随机重发

## 假设

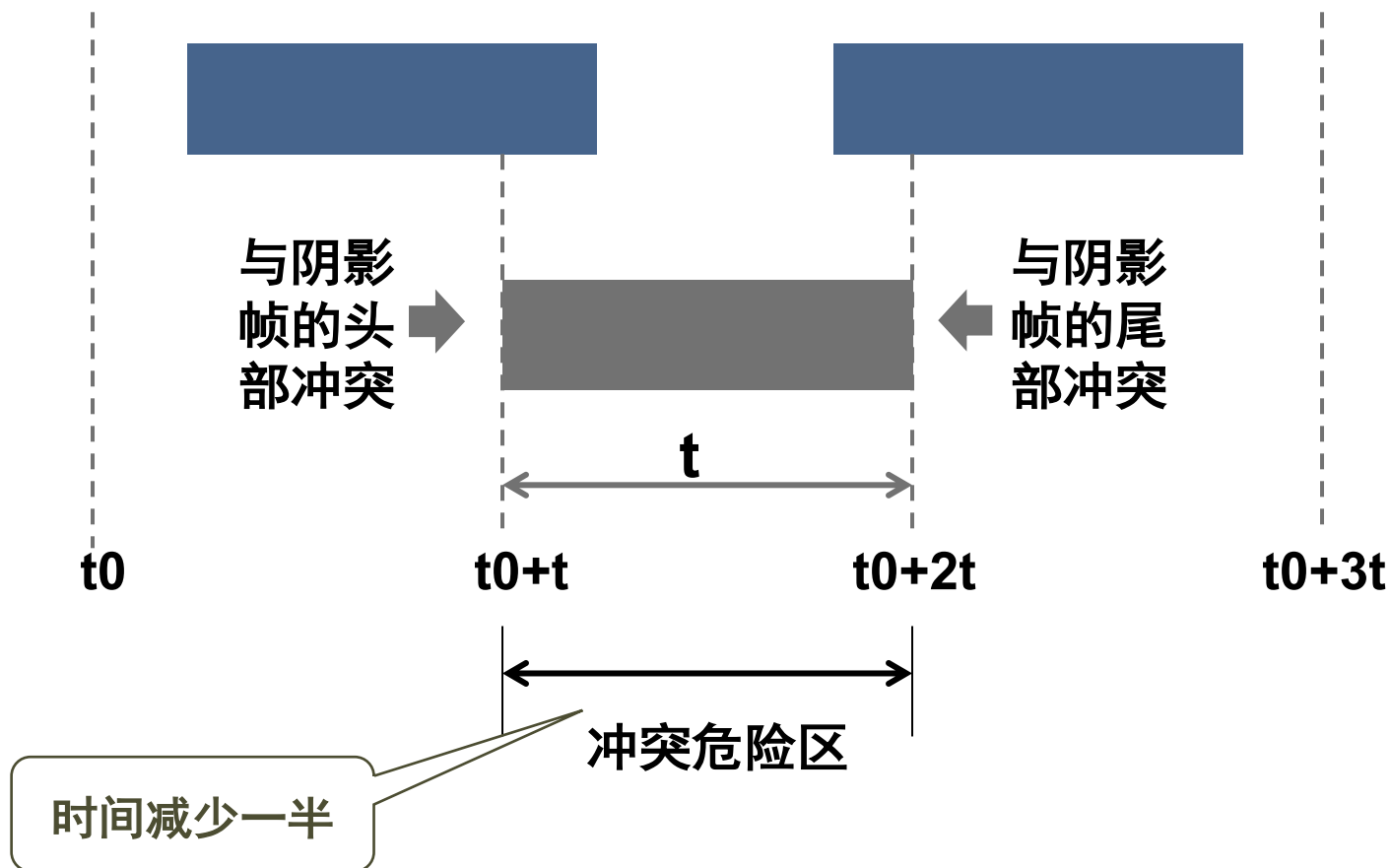
- 时间槽长度 $\geq$ 发送一帧的时间
- 各节点只能在下一时间槽的起始时刻开始发送信息





# 分槽ALOHA协议访问方式

关键：所有用户必须同步



能够期待的信道利用率  
最多为36%

？  
低效率的根本原因是冲突，还可以从哪方面减少冲突提高访问效率？



# 载波侦听多路访问(CSMA)

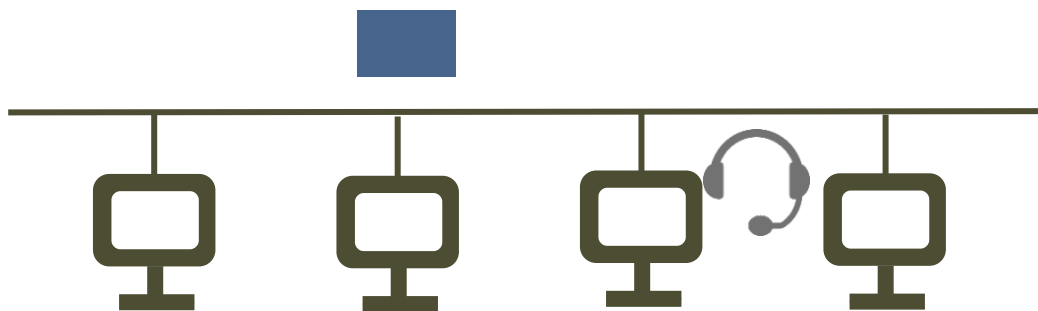
## LAN 主要特性

节点间传播延迟 < 帧传输时间



**载波侦听协议：网络节点侦听载波是否存在(即有无传输)并随之采取相应的行动。**

**“讲前先听”**



## CSMA基本思想

- 想要传输的节点首先听一听介质上是否有其他站点在传输(载波侦听);
- if 介质忙, then 必须等待; else 传输。



# 案例学习三

## IEEE802.3协议之数据帧格式



# IEEE802.3的MAC帧结构

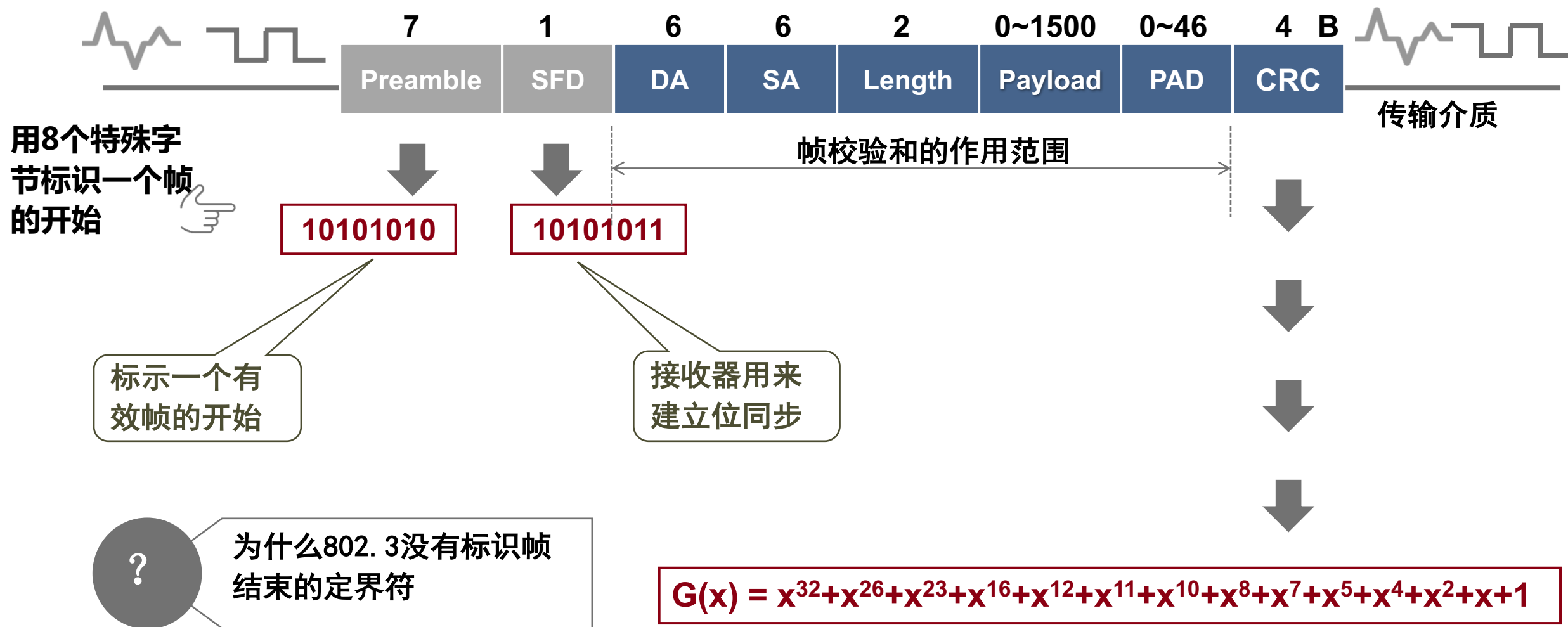


- **DA**  
目的地址，标识帧的接收方
- **SA**  
源地址，标识帧的发送方
- **Length**  
标识有效载荷的字节数
- **Payload**（缺省1500B）  
有效载荷运载数据信息/控制信息
- **PAD**  
满足最小帧长要求
- **CRC**  
循环校验码，4字节

**注意：802.3帧没有序号、确认号、控制、帧类别字段！**

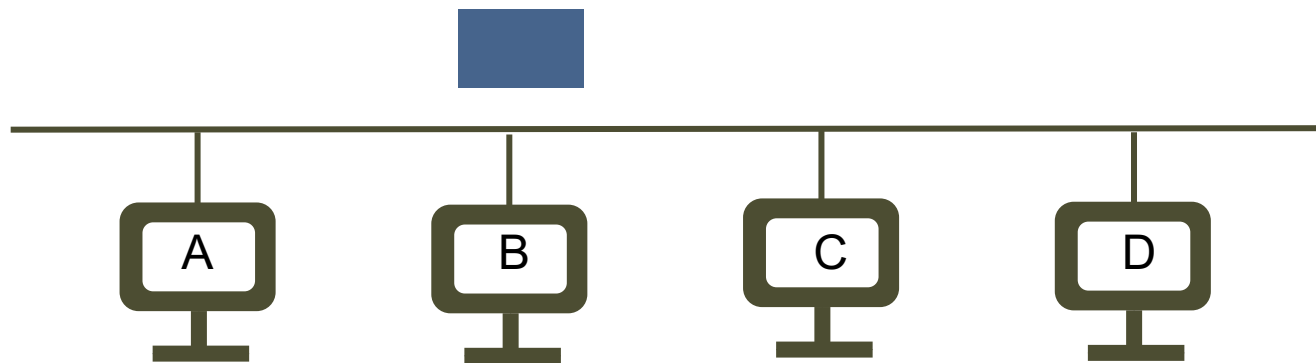


# IEEE802.3 成帧方法及差错检测



# IEEE802.3地址及单播

802.3支持单播、广播和组播通信方式。



目的地址（DA）/源地址（SA） 48位



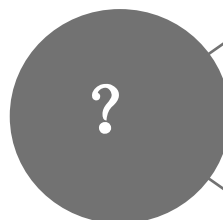
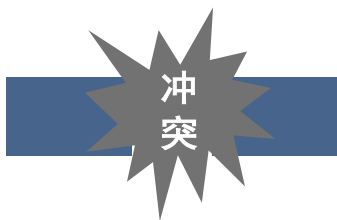
- 广播网络中每个节点必须有标识自己的地址
- 发送的数据帧必须指定接收方和发送方

I/G : 地址类型标志

{	0	单地址
	1	组地址

# IEEE802.3最小帧长要求

7	1	2~6	2~6	2	0~1500	0~46	4 B
Preamble	SFD	DA	SA	Length	Payload	PAD	CRC



当两个帧发送前没有侦听到对方帧后发送必将产生冲突后，冲突后立即停止，此刻共享信道上有什么

## PAD字段的作用

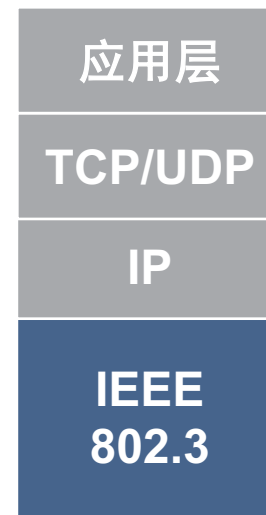
- 为区分有效帧/垃圾802.3规定有效帧必须至少64字节长
- 为了冲突检测规定了最小帧长为 $2\tau$ \*数据速率



# IEEE802.3提供的MAC服务

802.3提供了无连接的不可靠数据传输服务。

假设A节点给B节点发送一个数据帧



①上层用户要求802.3发送数据

`MA_UNITDATA.request (DA, m-sdu, service_type)`

②向上层用户报告发送结果

`MA_UNITDATA_STATUS.indication(send_status)`

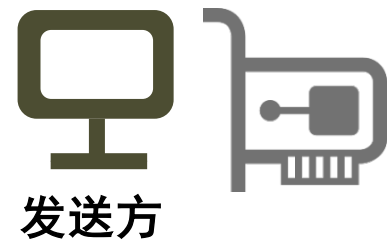
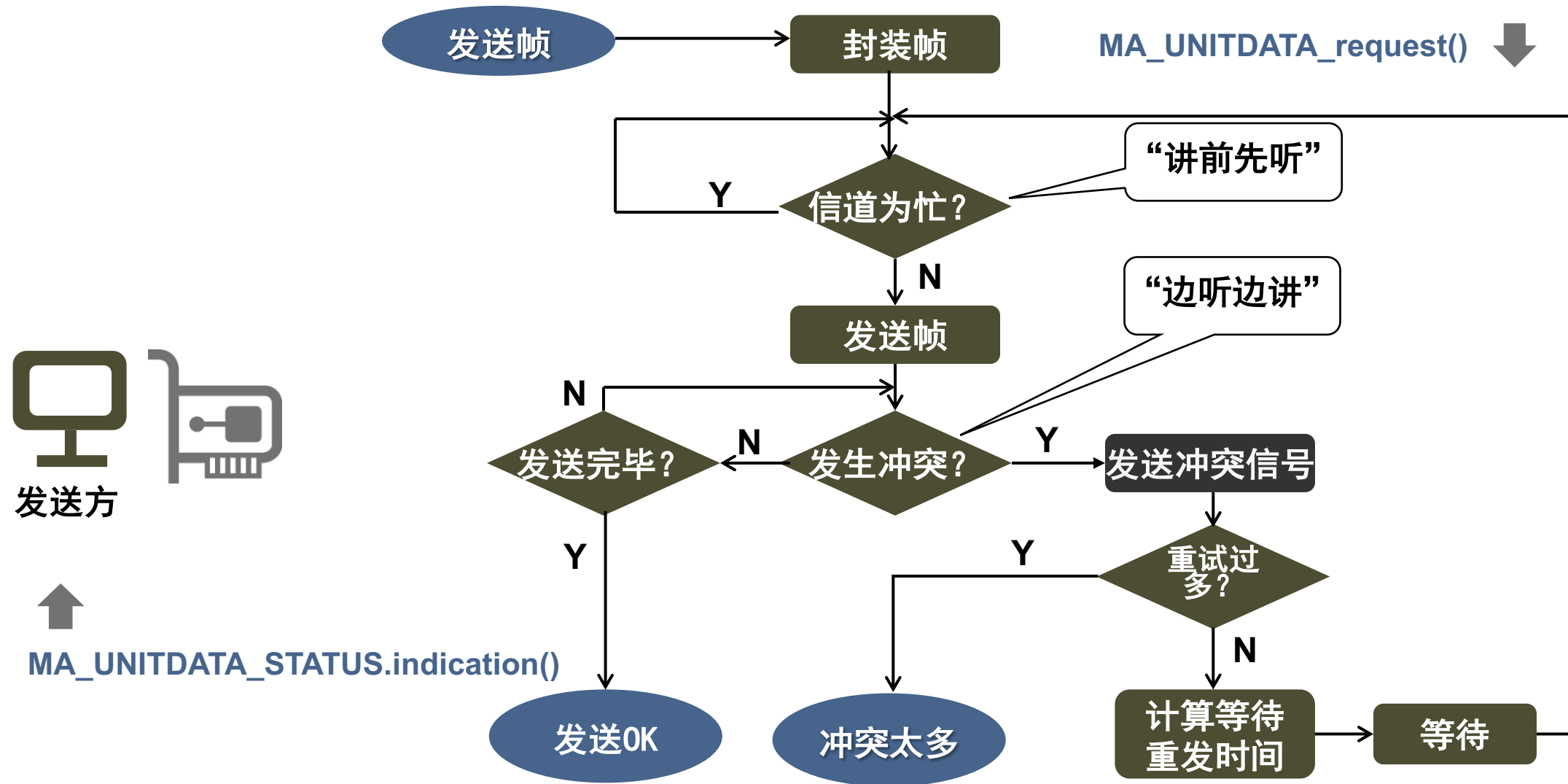
③把收到的数据交给上层用户

`MA_UNITDATA.indication(DA, SA, m-sdu, receive_status)`



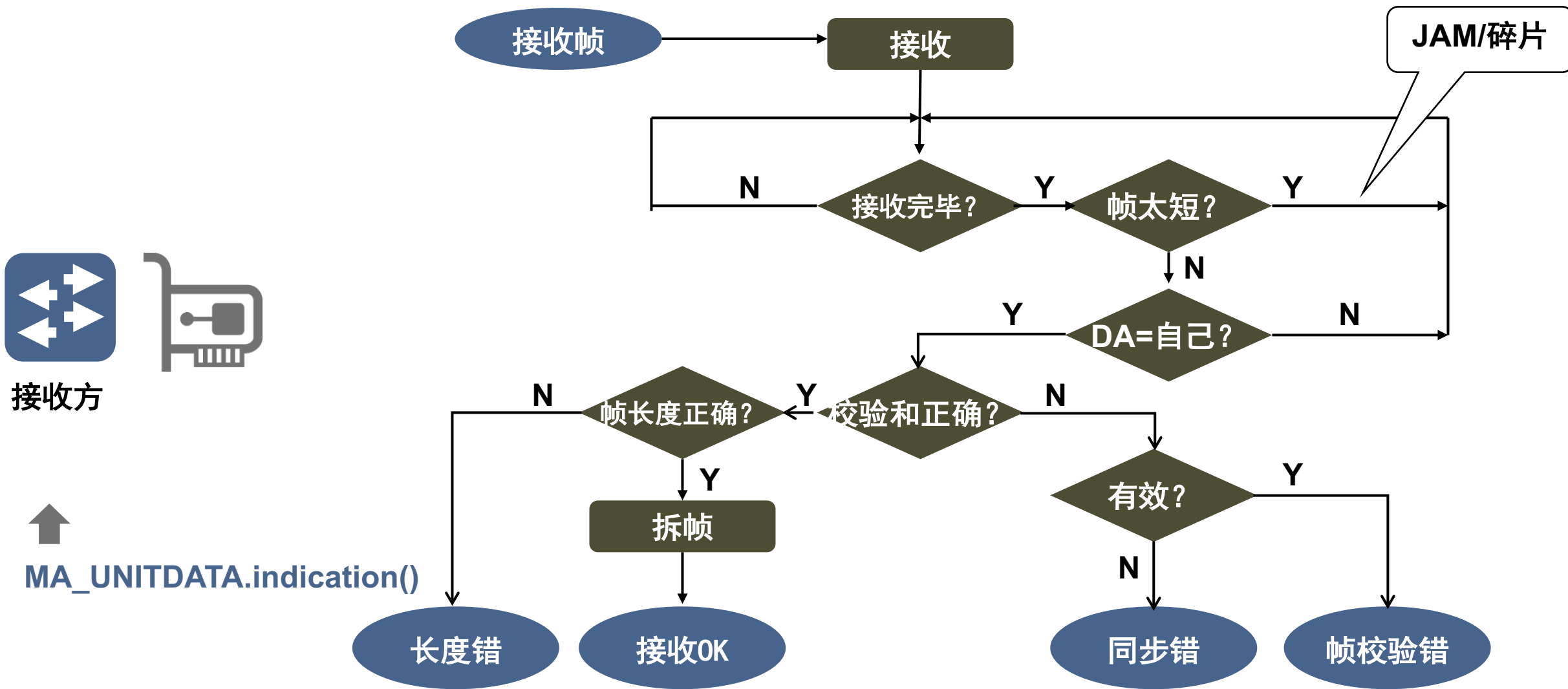


# IEEE802.3 发送流程



MA\_UNITDATA\_STATUS.indication() ↑

# IEEE802.3接收流程

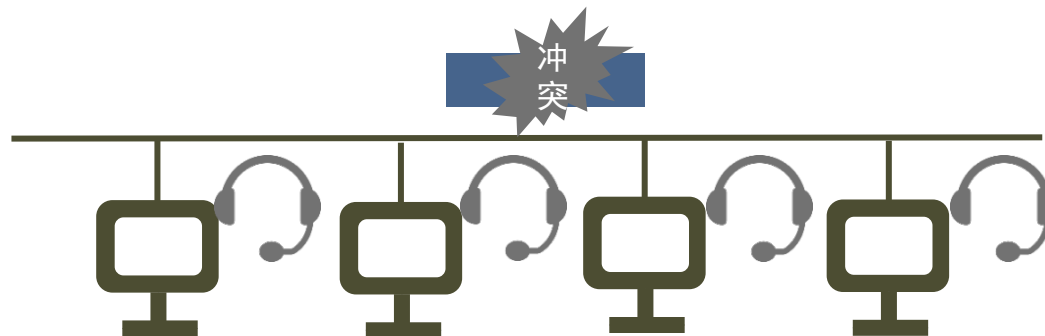


# 无线传输技术概述



# 基于CSMA/CD的有线局域网

- ① 讲前先听
- ② 边讲边听



- 发送前先侦听→减少冲突
- 发送时检测冲突→降低冲突浪费的带宽
- 重发随机等待→降低再次冲突的概率

?

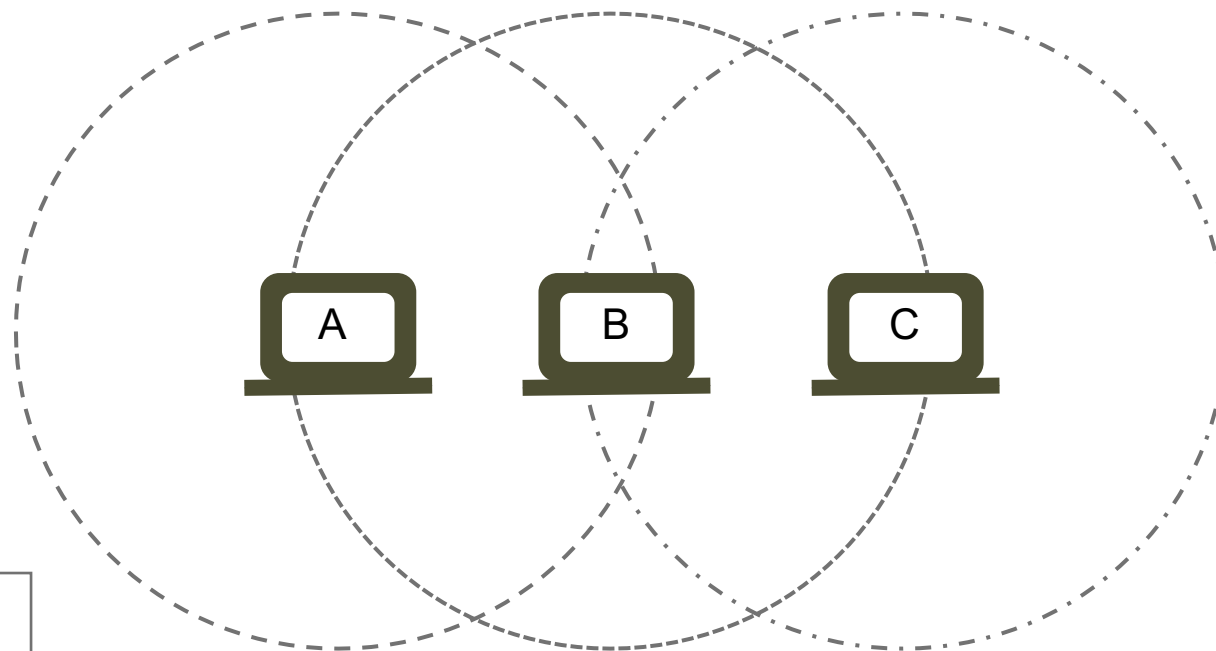
无线局域网是否也能用CSMA/CD?



# 无线局域网

## 无线竞争系统

- 多个移动节点共享同一个空间
- 每个节点的信号覆盖范围有限
- CSMA/CD?



?

- 同一个空间中有节点在发送帧时所有节点都能侦听到?
- 无线网卡能否同时发送和接收?

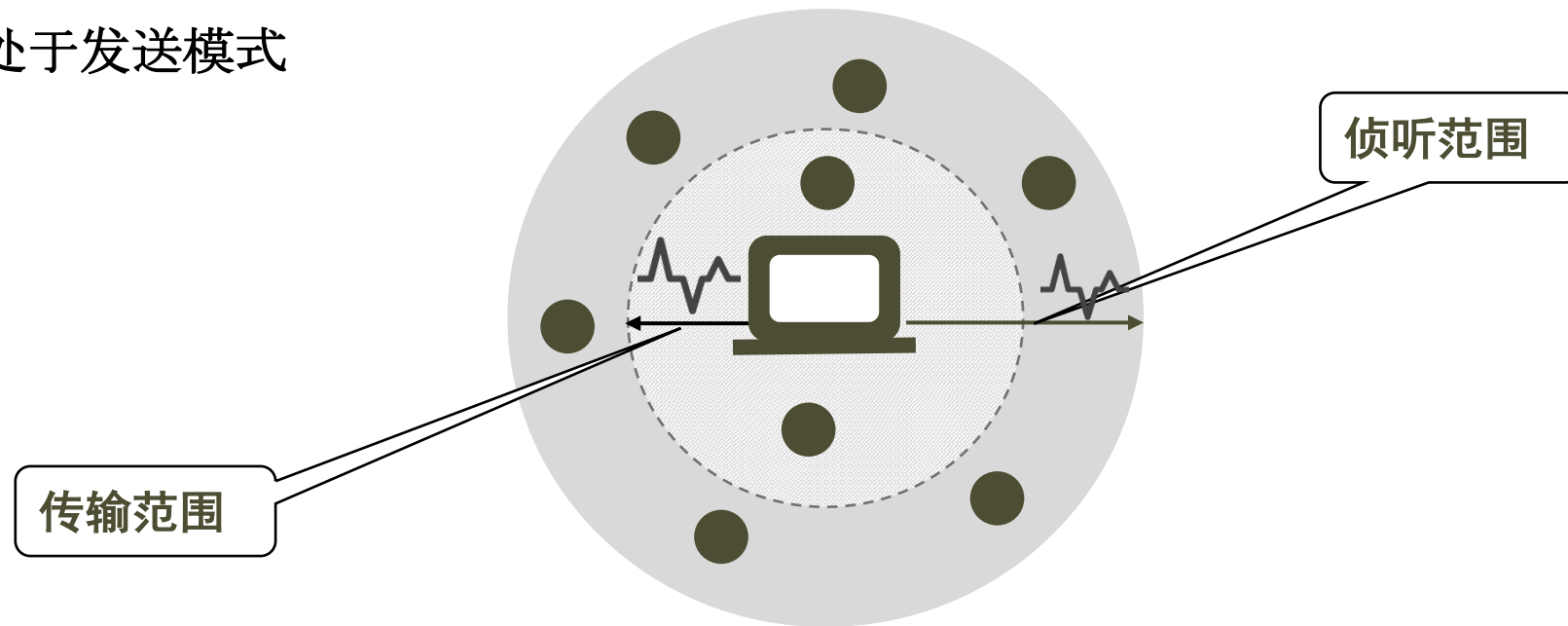


# 与发送相关的传输“范围”

**传输范围(TX\_range)：**成功接收帧的通信范围，取决于发送能量和无线电波传输特性

**侦听范围(PCS\_range)：**可检测到传输的范围，取决于接收器灵敏度和无线电波传输特性。

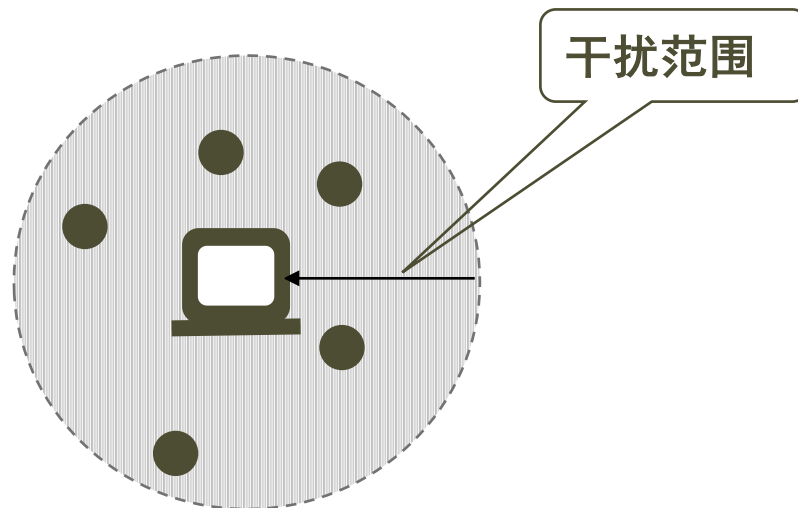
假设:笔记本处于发送模式



# 与接收相关的传输“范围”

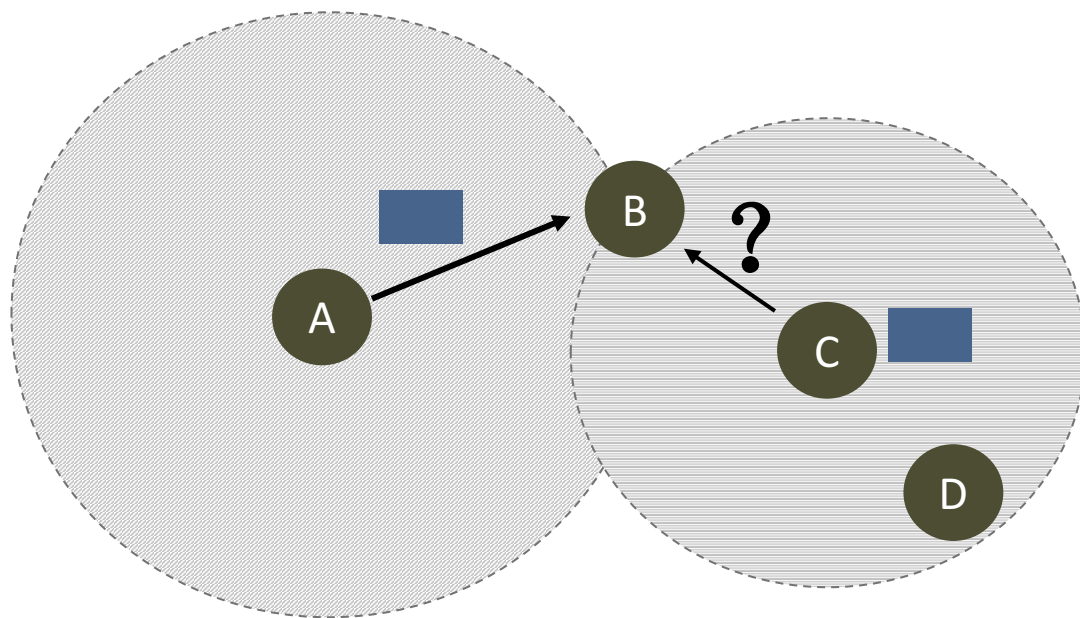
**干扰范围(IF\_range)：**此范围内节点发送帧将干扰接收方的接收并导致丢帧。

假设:笔记本处于接收模式



# “隐藏”节点问题

假设：A正在向B传输数据，C也要向B发送数据。



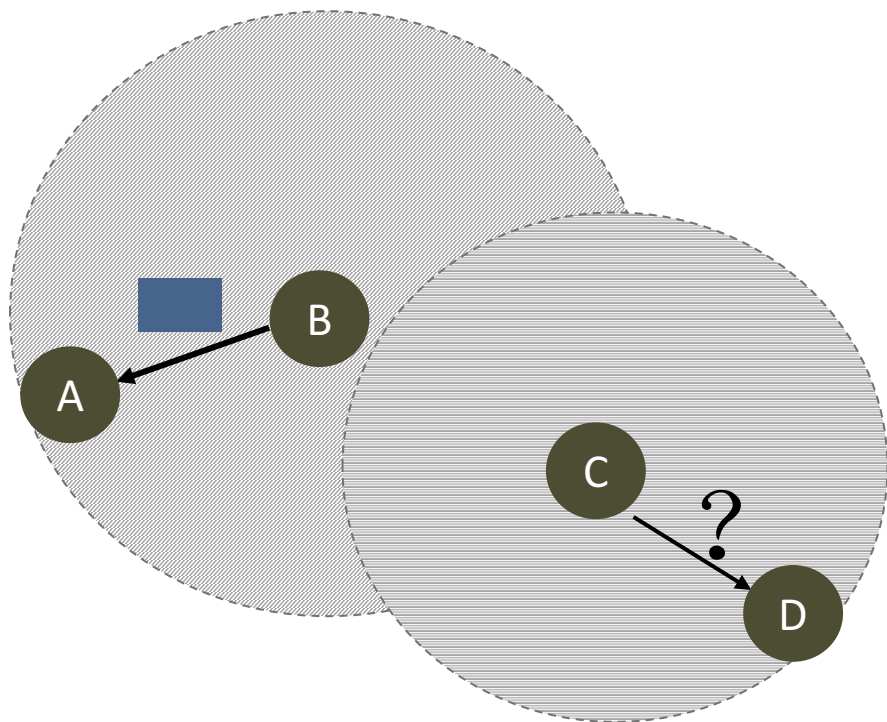
没有侦听到载波  
(信道空闲)  $\neq$  可以传输

**隐藏节点问题：**由于距离太远而导致一个站点无法检测到介质竞争对手的存在。



# “暴露”节点问题

假设：B正在向A传输数据，C要向D发送数据。



侦听到载波存在  
(信道忙)  $\neq$  不能传输

**暴露节点问题：**由于侦听到其他站点的发送而误以为介质忙导致不能发送。



## CSMA/CD机制不适合基于共享介质的无线局域网

- 一个节点的发送行为无法被所有节点感知
- 传统的无线收发器不能并发工作

# IEEE802.11协议 VS. 访问控制机制

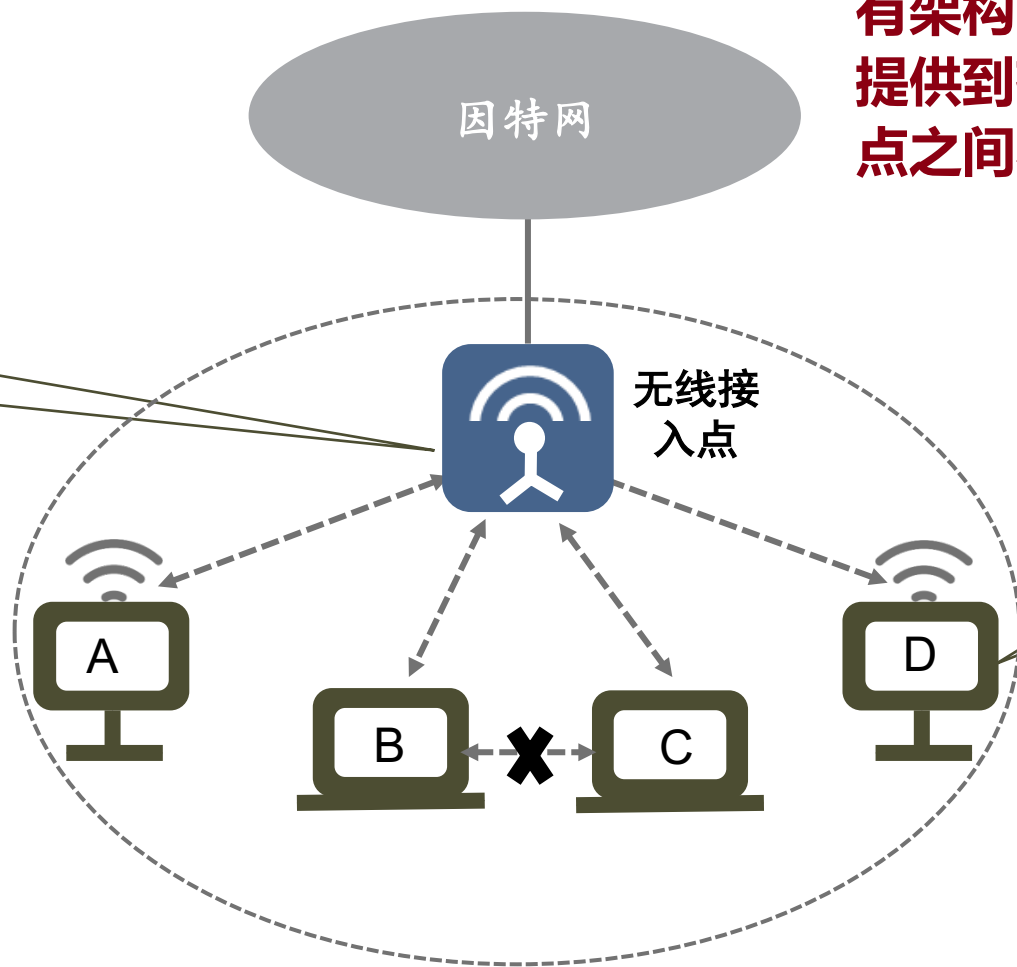


# IEEE 802.11 拓扑结构

**Basic Service Set (BSS)**  
一组能相互通信的站点

**有架构BSS ( IBSS )** : AP(接入点)  
提供到有线网络连接的中继功能 , 节  
点之间不能直接通信.

所有的通信都要经  
过AP进行



A、B、C、D可以  
给任意一个其他  
节点发送帧



# IEEE 802.11介质访问控制和协议栈

## 802.11MAC设计目标

- 单个MAC支持多个PHY
- 抗干扰能力强
- 处理隐藏节点问题
- 支持实时服务、QoS
- 重载下可扩展且稳定
- 提供节能模式
- 提供私密性和访问控制

## 协议栈



**IEEE802.11标准：局域网内固定的、便携的和可移动节点的无线连接规范。**

## 三大功能

- ① 访问控制机制
- ② 可靠数据传递
- ③ 安全保障机制

### IEEE 802.11标准

- CSMA/CA协议（载波侦听多路访问/冲突避免）
- RTS/CTS机制（用来解决“隐藏/暴露”节点问题）
- 将包分成小帧：在噪声干扰大的地区把包分成小帧传送以降低重传成本
- 多信道漫游：移动节点能动态调频到AP设定的频带

# IEEE 802.11基本访问控制机制

基于  
CSMA/CA的  
强制基本功能

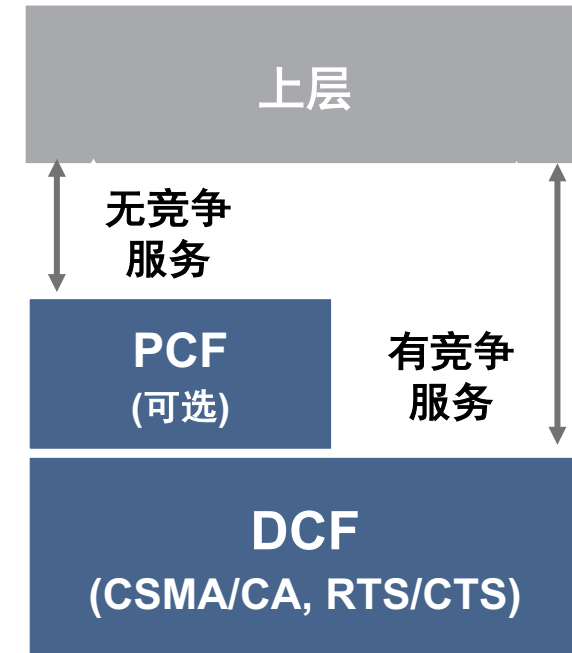
- 竞争方式访问信道
- 提供异步传输模式

避免隐藏节点  
问题的可选功  
能

- 解决隐藏节点问题

实时服务的无  
冲突轮询方法

- 无竞争方式访问信道
- 由AP协调部分信道容量的使用

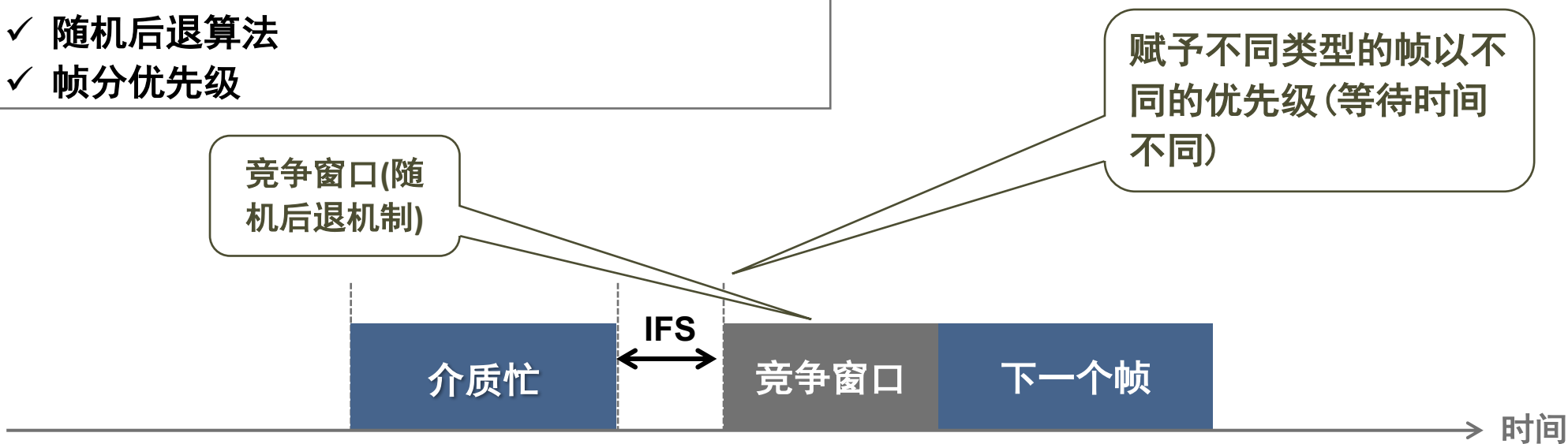


# 基本DCF中的CSMA/CA

## CSMA/CA基本思想

- 载波侦听 (CSMA)
  - ✓ 如果介质为空, 则节点传输帧;
  - ✓ 如果介质为忙, 则等待直到当前传输结束。
- 冲突避免 (Collision Avoidance)
  - ✓ 随机后退算法
  - ✓ 帧分优先级

**带冲突避免的载波侦听协议：网络节点侦听载波是否存在(即有无传输)并随之采取随机发送的行动，以便降低发生冲突的概率。**





# 随机后退过程

## 随机后退算法

- 当介质空闲时间 $\geq$  某个帧间间隔(视待发帧类别而定)和随机等待时间, 则立即传输
- 当介质忙, 延迟访问信道直到 (当前传输结束 + 某个帧间间隔)
- 开始随机后退过程
  - 选择一个随机数 ( 0, CW)
  - 等待选出的随机数所对应的时间
  - 重复上述过程

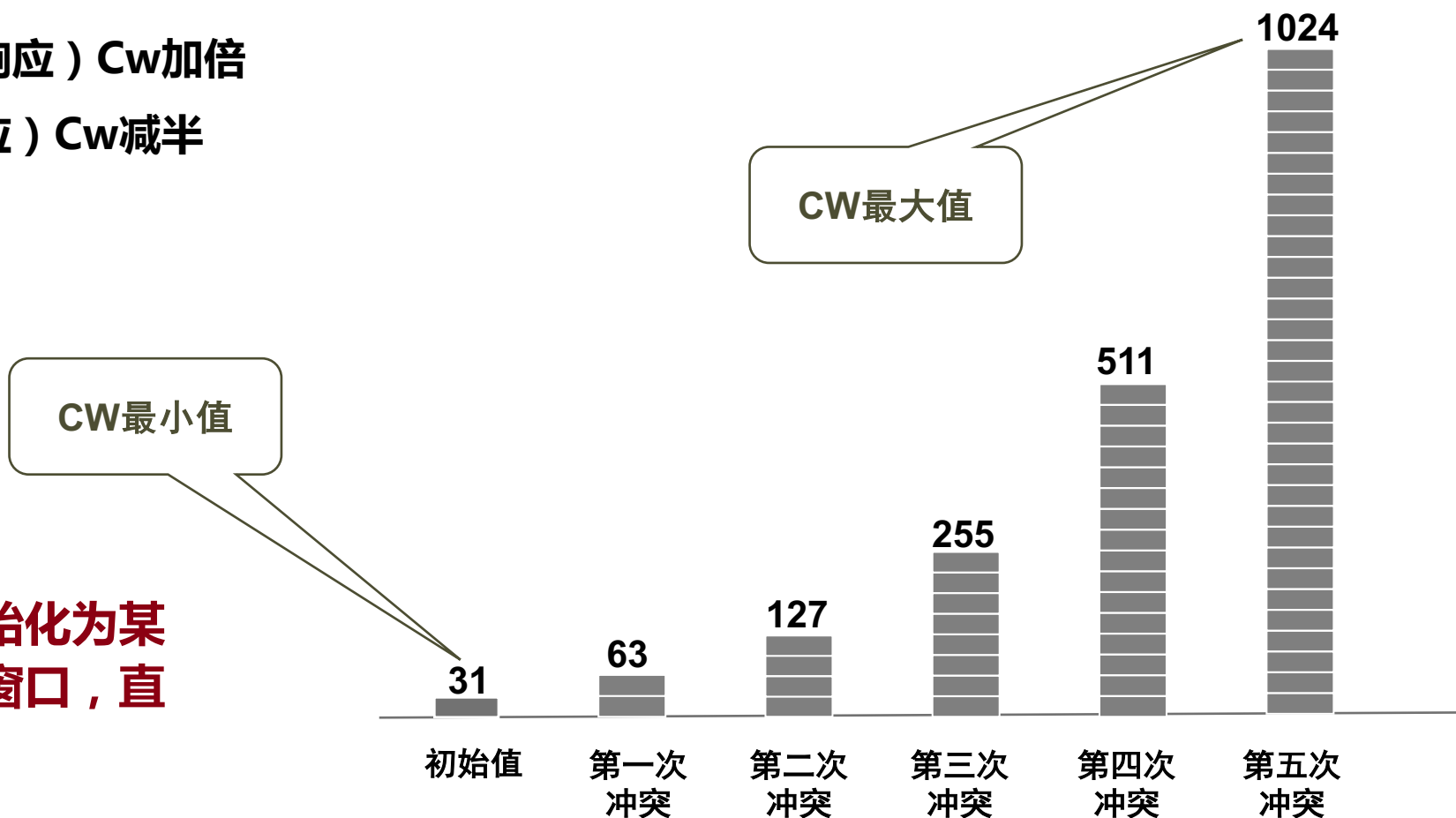
**竞争窗口(CW)：初始化为某个最小值，  
发生冲突时加大窗口，直到达到最大值。**

**使用后退过程延迟发送的目的在于  
避免多个节点同时传输引起的冲突。**



# 随机后退的竞争窗口 (CW)

- 每次不成功传输后（无CTS响应）Cw加倍
- 每次成功传输后（有CTS响应）Cw减半



**指数后退算法：竞争窗口初始化为某个最小值，发生冲突时加大窗口，直达到达到最大值。**



# 优先级——控制等待时间的参数

## 帧间隔定义帧优先级

- SIFS (Short IFS)
- PIFS (PCF IFS)
- DIFS (DCF IFS)

## 最高优先级 SIFS

- ACK
- CTS
- AP 轮询响应

## 中等优先级 PIFS=SIFS+1

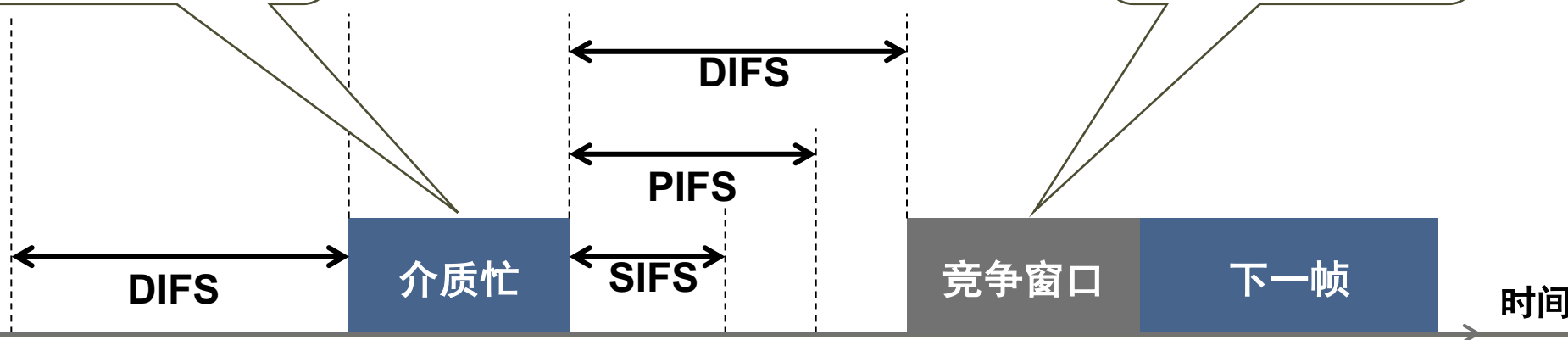
使用 PCF 的时  
限服务

## 最低优先级 DIFS=SIFS+2

异步数据服务

介质空闲时间大  
于 DIFS 则直接访  
问

后退算法选择随  
机等待时间



# 单播数据的可靠传输

**802.11提供了无连接的可靠数据传输服务。**

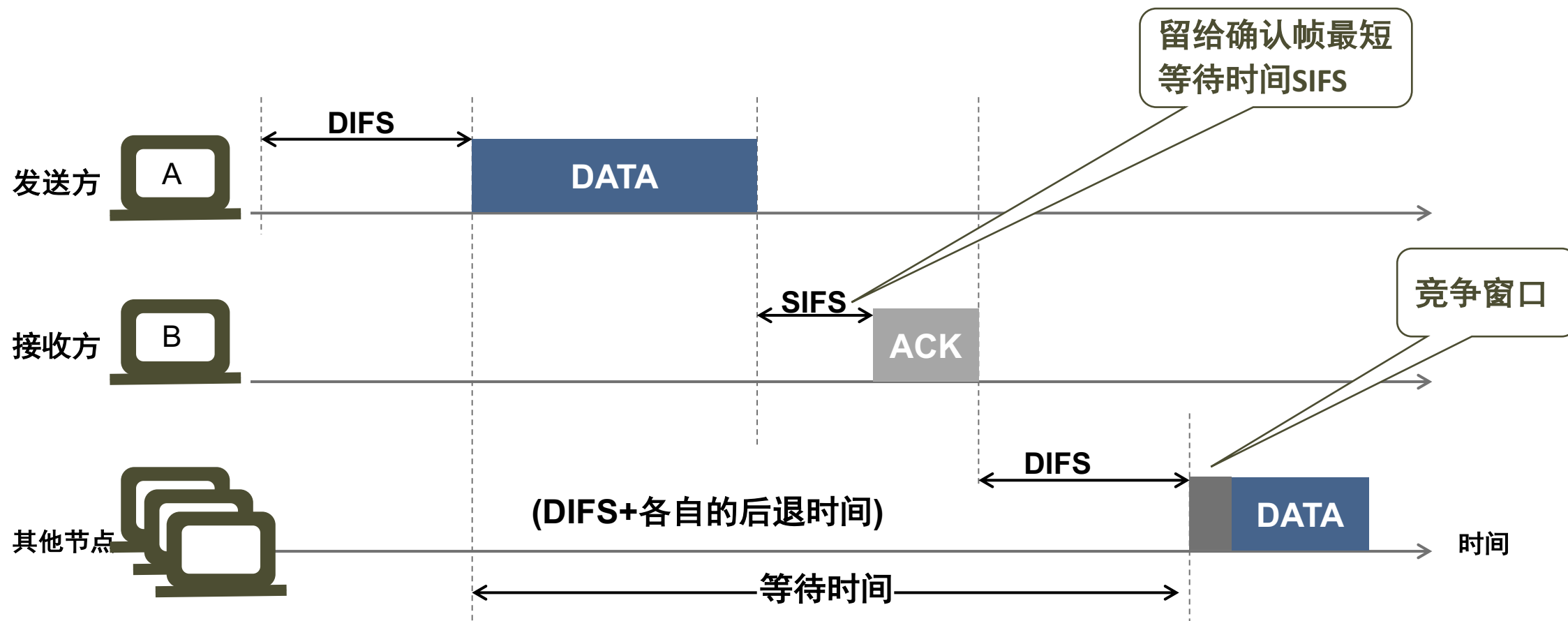
## 802.11的可靠传输

- 接收方在校验CRC正确时立即返回ACK
- 没有收到ACK则随机后退后重传该数据帧



# 可靠数据帧传输示例

假设：节点A给节点B发送一个数据帧



# IEEE802.11协议 VS. RTS/CTS机制

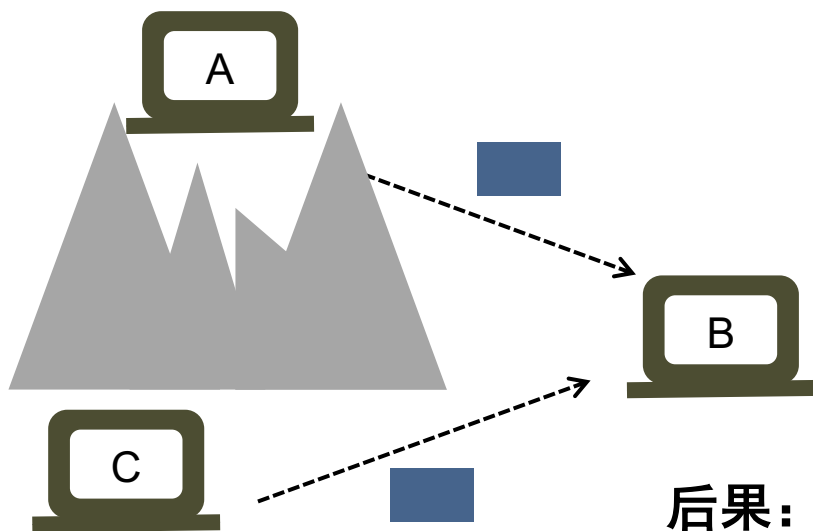


# 如何解决“隐藏节点”问题？

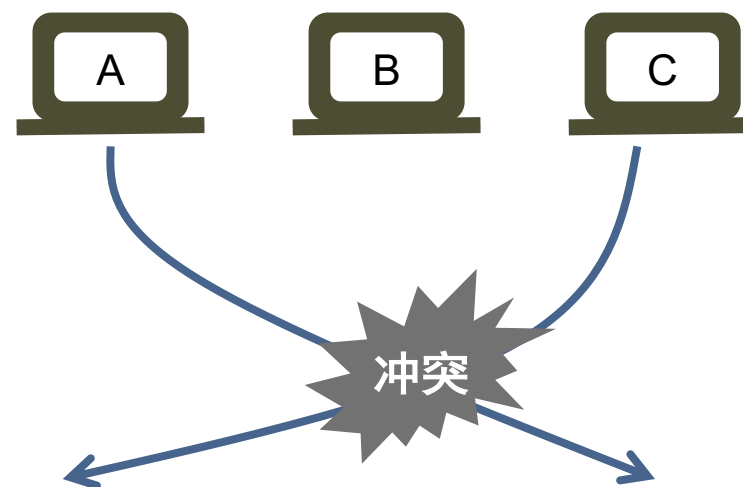
## 隐藏节点的根本原因

- 发送节点A和C互不知道
- 距离较远/障碍物导致信号衰减
- 如果多于两个节点同时发送将在B处冲突

解决办法：通过短的控制包预留带宽



后果：A和C发送长报文  
冲突将导致带宽的浪费



# 带有RTS/CTS的扩展DCF

**RTS/CTS机制：一种针对隐藏节点问题的控制机制，每个802.11节点必须实现该机制，但使用时可选。**

## 明确预留信道

- 发送方发送RTS请求发送
- 接收方用CTS回应发送请求
- CTS为发送方预留带宽的同时通告所有节点（包括隐藏的）
- RTS和CTS长度很短，冲突的概率减少

- 接收方地址
- 发送数据帧时间
- 发送ACK时间



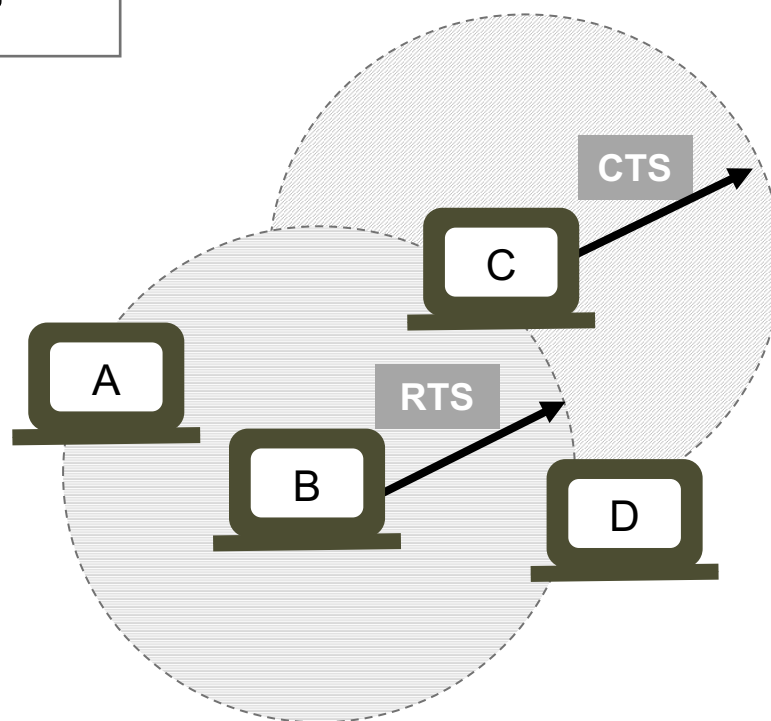


# RTS/CTS机制的作用

## RTS/CTS机制的作用

- 侦听到RTS → 自身在发送方附近
- 侦听到CTS → 自身在接收方附近

① 所有侦听到RTS的节点等待足够长时间

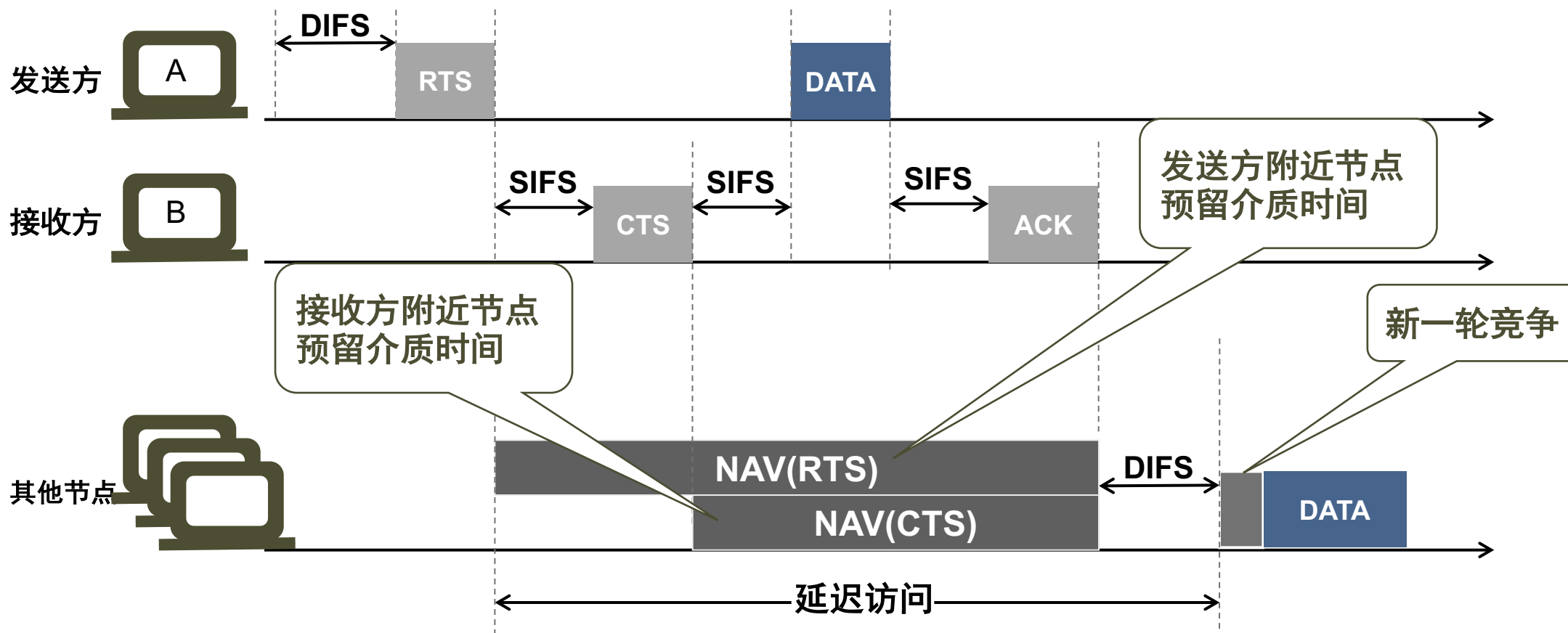


② 被请求节点（接收方）以CTS响应

③ 所有侦听到CTS节点等待足够长时间

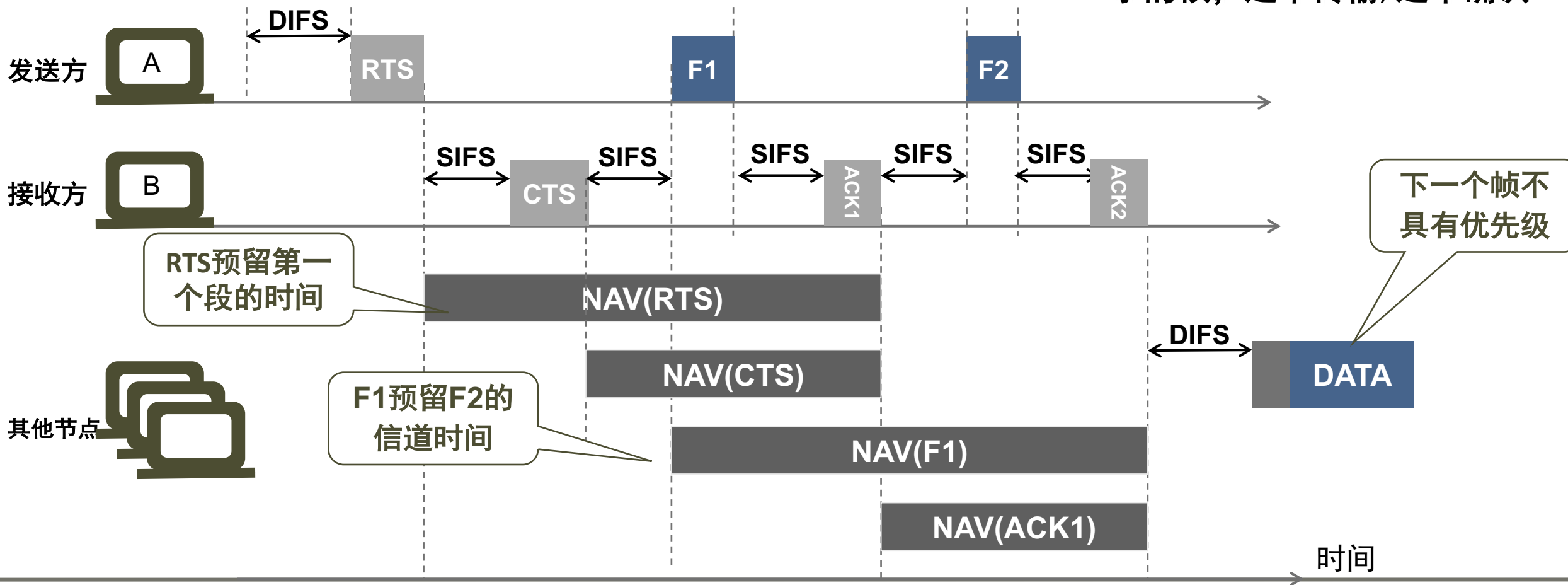
# RTS/CTS应用示例

假设：节点A给节点B发送一个数据帧



# 如何应对无线链路高比特出错率？

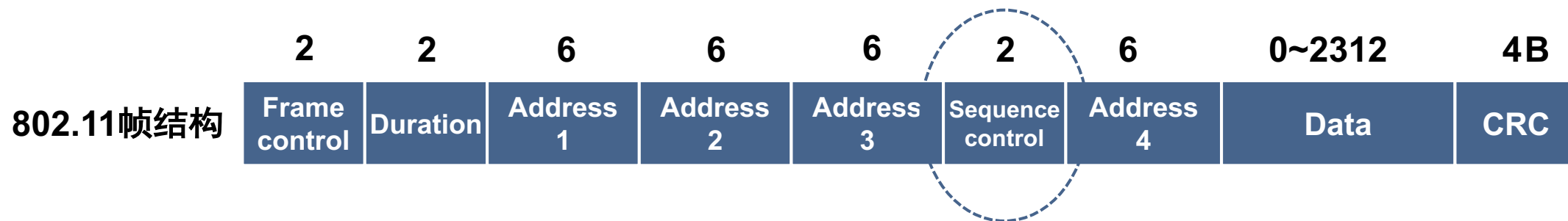
解决方法：将长帧划分为较小的帧，逐个传输，逐个确认



# IEEE802.11协议 VS. 帧格式



# IEEE802.11MAC帧结构



- **Frame control**

两个字节的控制字段具有多种用途

- **Duration/ID**

表示下一个发送帧可能持续的时间

- **Address 1~4**

每个地址含义由”控制”字段的DS解释

- **Sequence control**

序列号用来过滤掉重复帧以及分段

- **Data**

包含任意长度的数据

- **Checksum**

802.11采用4个字节的校验码



# IEEE802.11MAC帧控制字段

控制字段 (2字节)	2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b
	Protocol Version	Type	Subtype	To DS	From DS	More frag	Retry	Power mgmt	More data	WEP	Order
						┆还有数据	┆表明重传	┆节能模式	┆数据缓存	┆帧已加密	┆严格按序

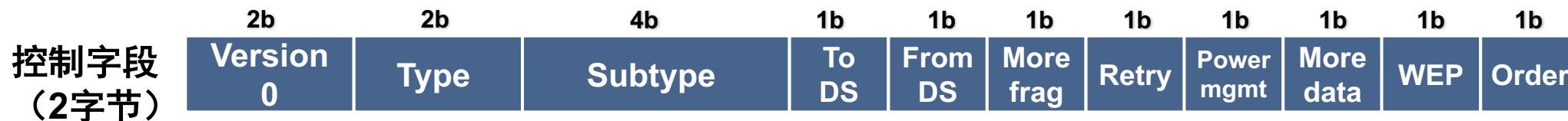
## Type : 确定帧的功能

- 管理 (00)
- 控制 (01)
- 数据 (10)
- 保留 (11)

- 802.11网卡收到一个帧首先进行校验，校验正确后
- 依据TYPE字段区分帧的类型和具体帧的子类别
- 采取协议规定的动作



# IEEE 802.11MAC帧管理帧和控制帧



## 管理帧 ( 11个,type=00 )

- Association request
- Association response
- Re-association request
- Re-association response
- Dissociation
- Probe request
- Probe response
- Beacon
- Announcement traffic indication message
- Authentication
- De-authentication

- 管理帧负责移动节点与AP之间的链路建立和管理事务

## 控制帧 ( 6个,type=01 )

- ACK
- RTS/CTS
- Power save-poll
- 节能模式
- CF-end
- CF-end + CF-ack

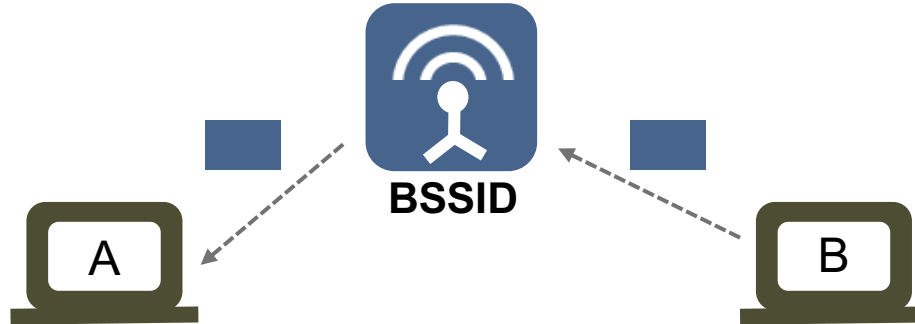
- 控制帧负责与传输和能耗有关的事务



# IEEE802.11MAC帧的地址字段

**A通过AP接收来自B的数据帧**

- **fromDS=1**
- **SA=B的地址**
- **DA=A的地址**
- **BSSID=AP的地址**



**B通过AP给A发送数据帧**

- **toDS=1**
- **SA=B的地址**
- **DA=A的地址**
- **BSSID=AP的地址**

to DS	from DS	Address1 物理接收者	Address2 物理发送者	Address3 逻辑发送/接收者	Address4
0	0	DA	SA	BSSID	--
0	1	DA	BSSID	SA	--
1	0	BSSID	SA	DA	
1	1	RAP	TAP	DA	SA

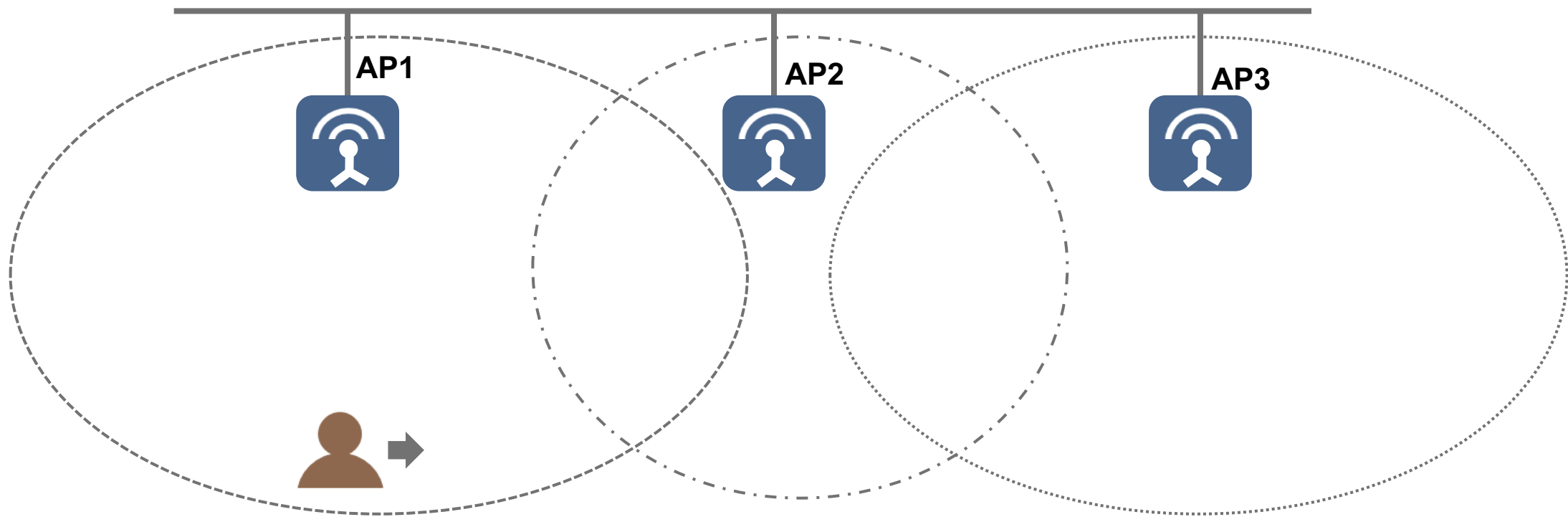
**物理发送者/接收者始终是AP**

- 无线自组织网络
- 接收AP发来的帧
- 通过AP发送帧
- 分属两个AP下通信





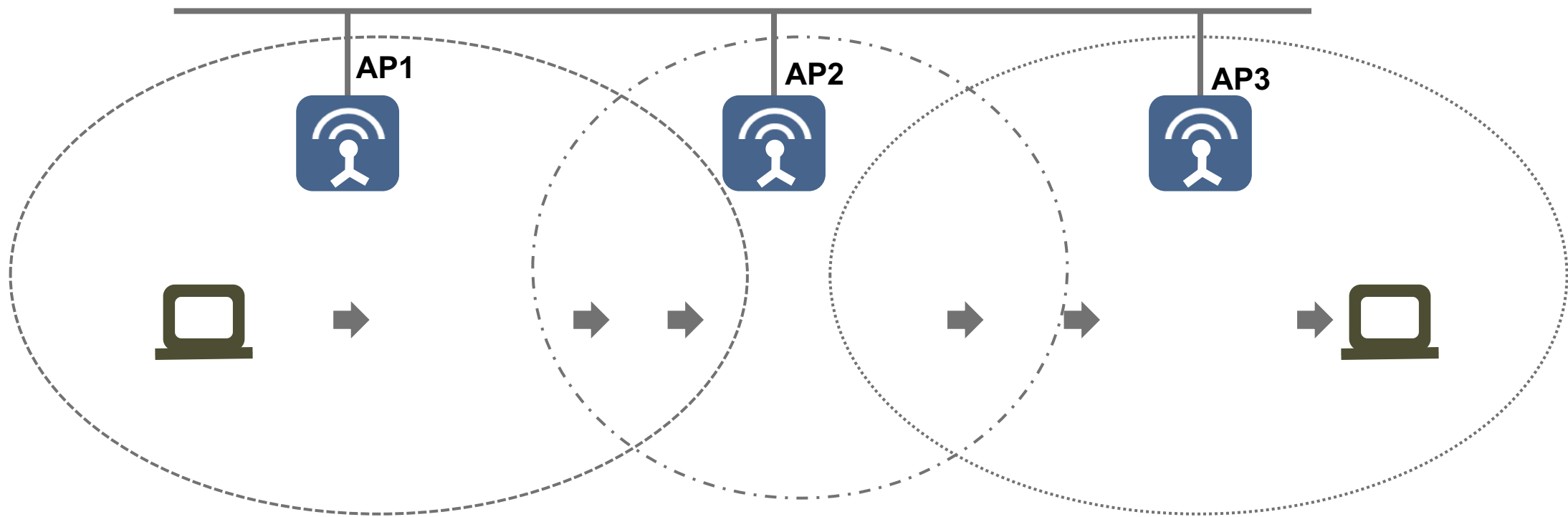
# IEEE802.11使用场景



- 每个AP周期性地在自己的工作信道上发送Beacon帧
- 相邻AP必须工作在不同的信道（以防干扰）
- 各个AP的信号覆盖区必须重叠才能提供无缝的无线接入



# IEEE802.11MAC接入过程



t0: AP1信号最强

t1: AP1信号变弱笔记本开始扫描

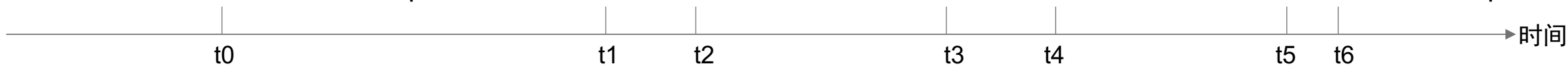
t2: 发送Probe request帧

t3: 收到AP2和AP3的Probe response帧

t4: 选择信号最强的AP3

t5: 发送Reassociation request帧

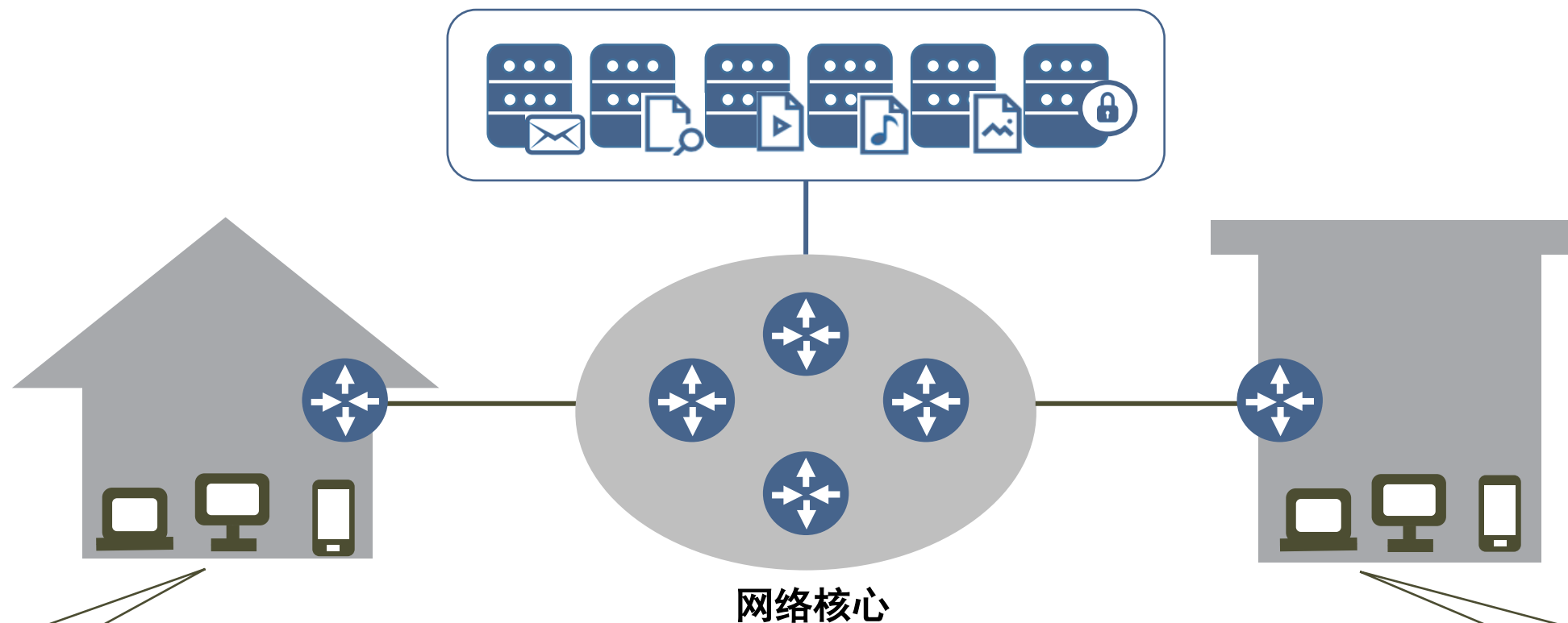
t6: 收到Reassociation response帧



# 局域网互连 vs. 互连设备



# 局域网互连与接入网络



电话网络(ADSL)  
电视网络(CABLE)

有线局域网(802.3)  
无线局域网(802.11)



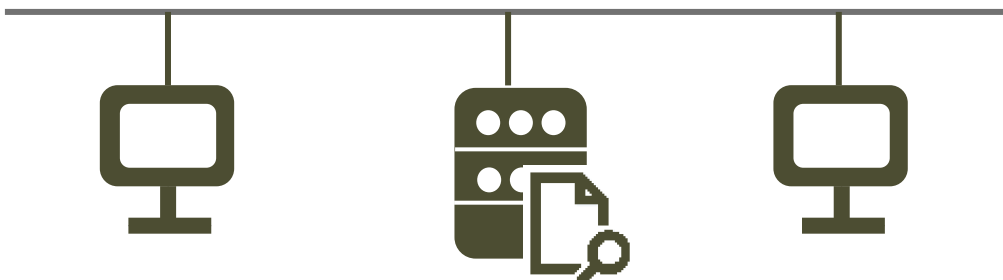
北京大学

# 局域网互连的需求

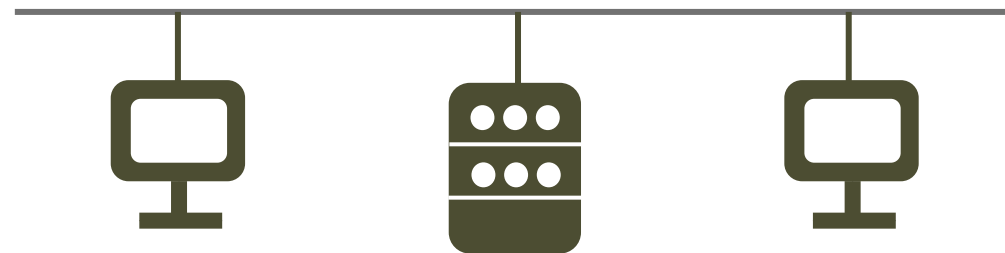
## 局域网互连的需求

- 现有不同LAN需要互联
- 地理位置分散需要
- 网络负载分摊到各LAN
- 扩大覆盖范围
- 故障隔离

研发部门局域网



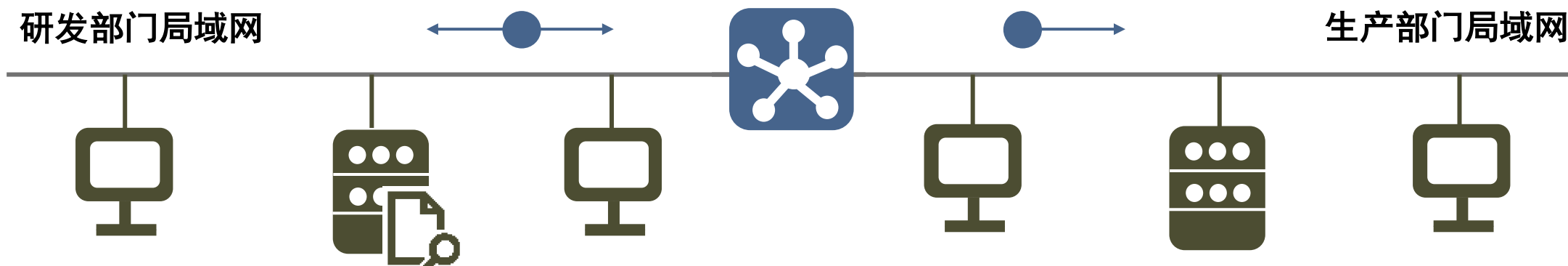
制造部门局域网



# 中继器

## 特性

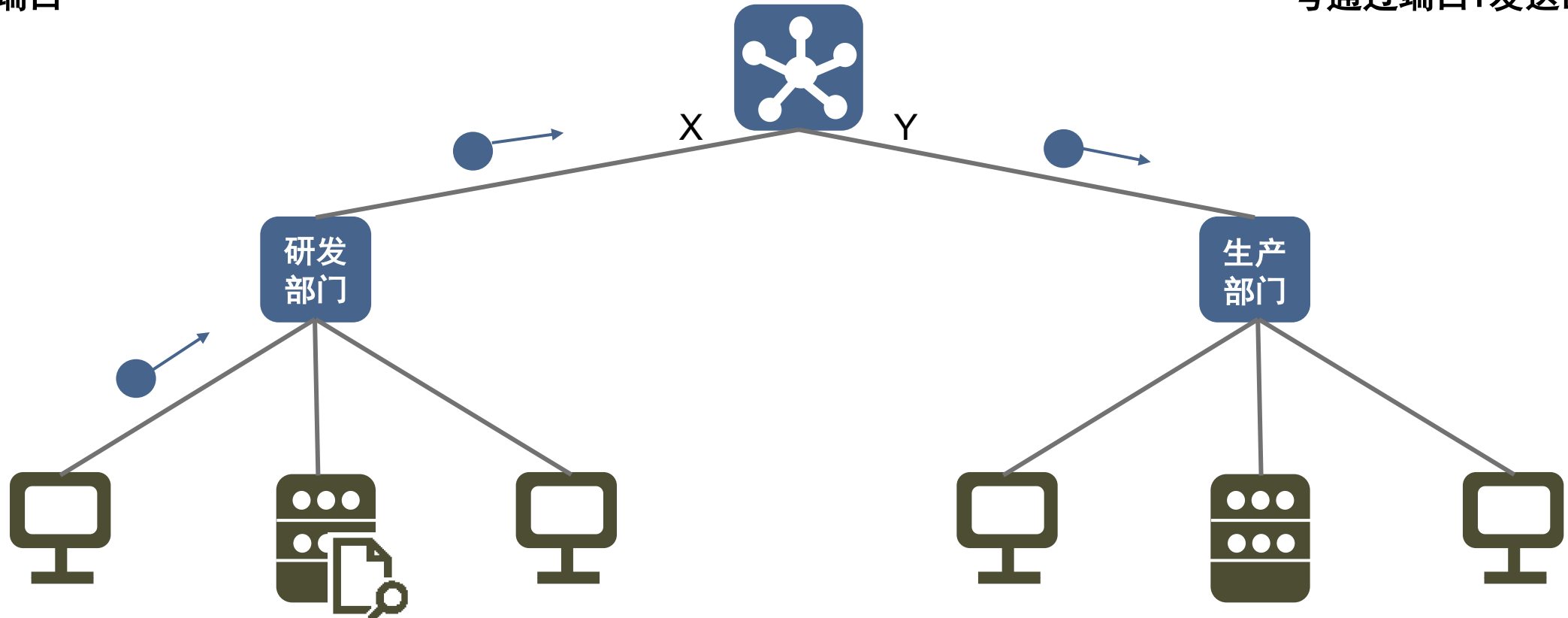
- 工作在物理层的电子信号放大低级设备。
- 它将来自一个接口的比特简单广播到所有的其他端口。



# 中继器的互连功能

- X和Y是中继器连接两个LAN的端口

- 中继器把从端口X入境的信号通过端口Y发送出去



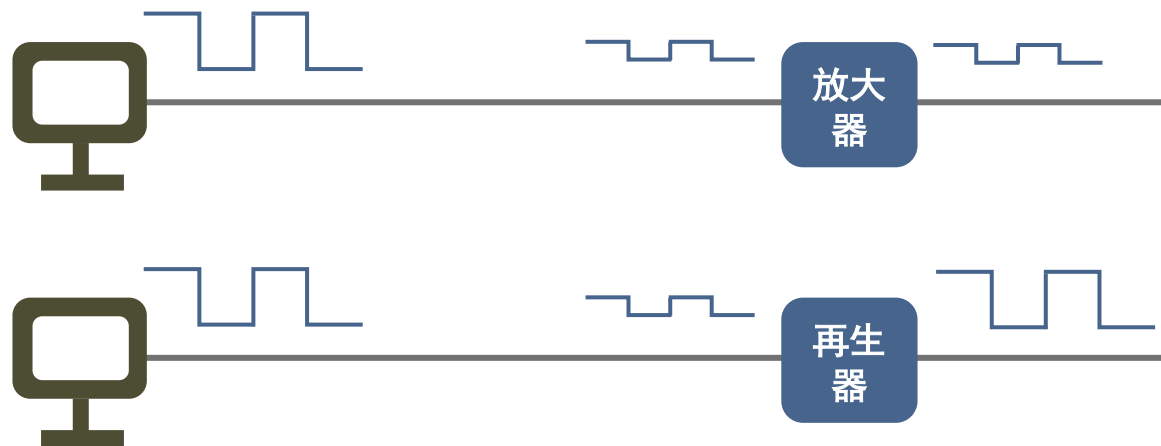
# 中继器分类与不足

## 放大器

把接收信号  
放大后再输出

## 信号再生器

先过滤掉噪  
声再放大输  
出



## 中继器的缺点

- 不具备检错和纠错功能
- 连接的以太网不能形成环



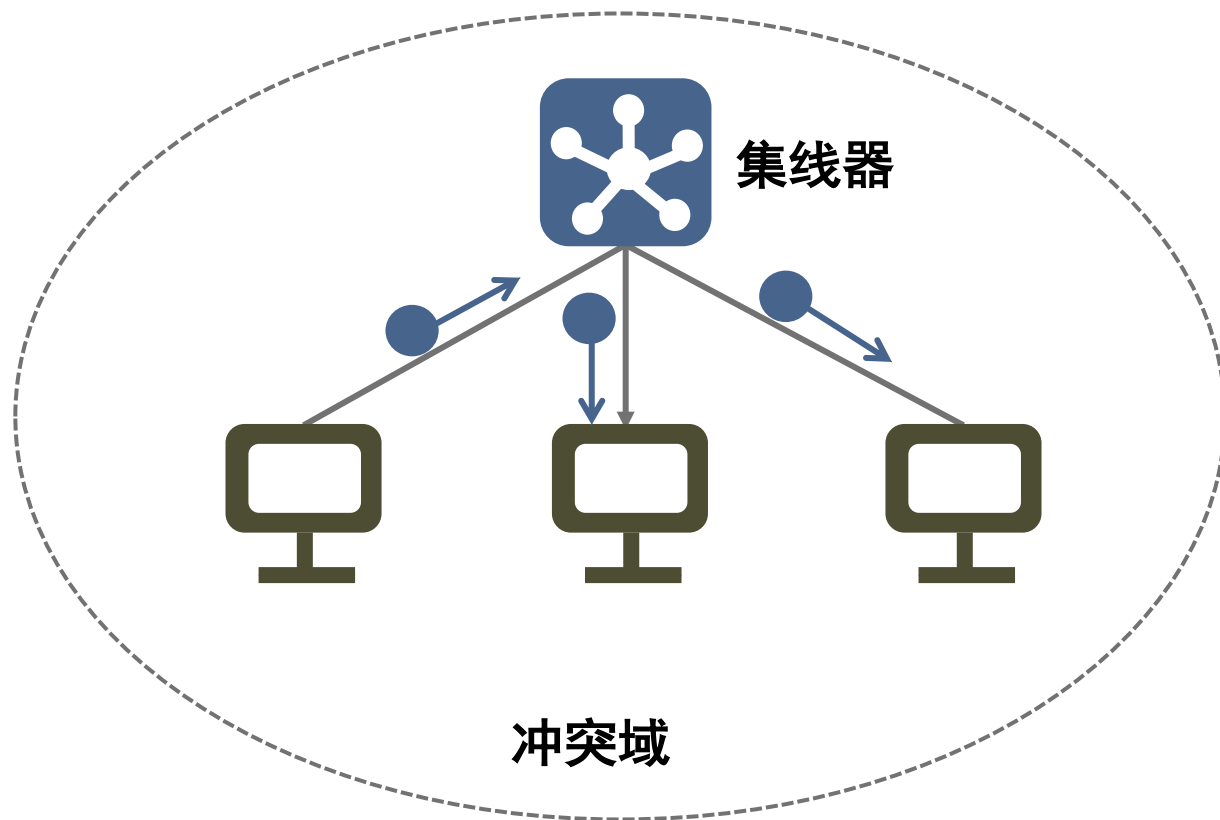
# 集线器

**Hub：“多端口中继器”**

将所有介质(多段粗、细电缆或双绞线)连接到一个中央位置的设备。

组成数据帧的每个比特串行进入集线器的一个端口，被集线器依次转发到所有其他端口

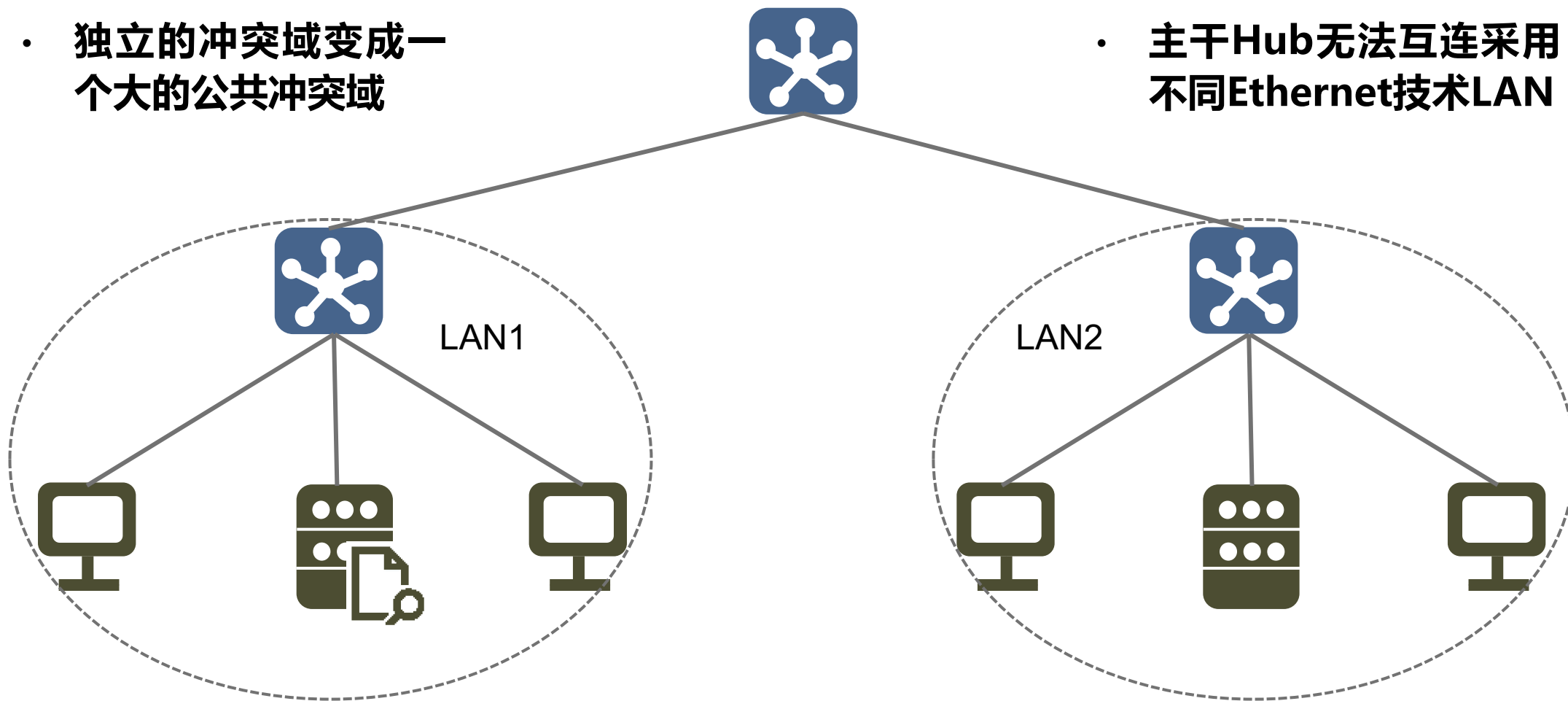
**冲突域：**两个或两个以上节点同时发送将产生冲突的区域。



# 中继器的多级配置

- 独立的冲突域变成一个大的公共冲突域

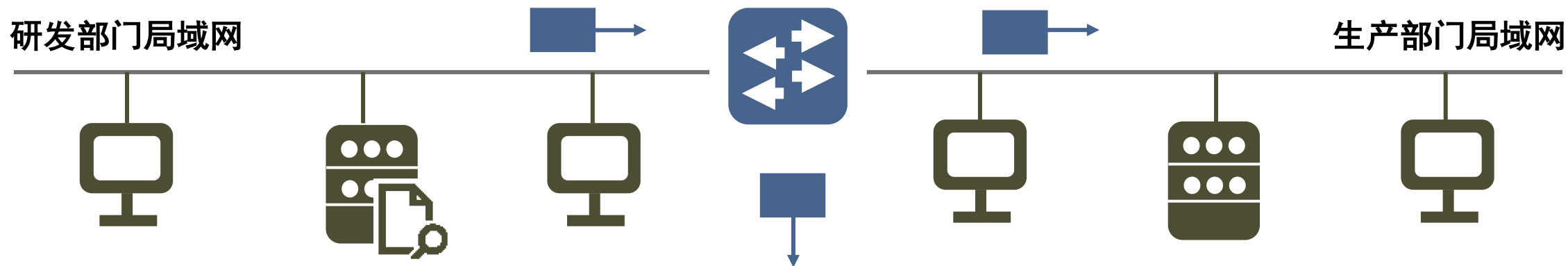
- 主干Hub无法互连采用不同Ethernet技术LAN



# 网桥

## 特性

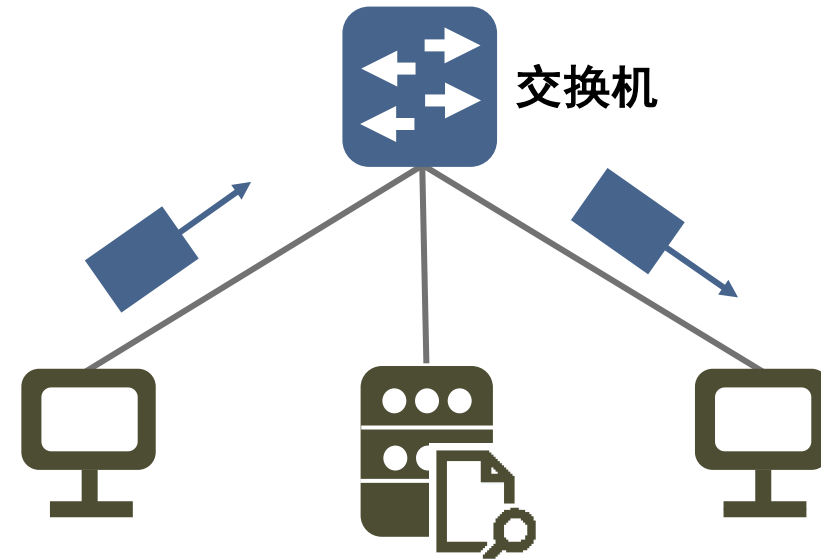
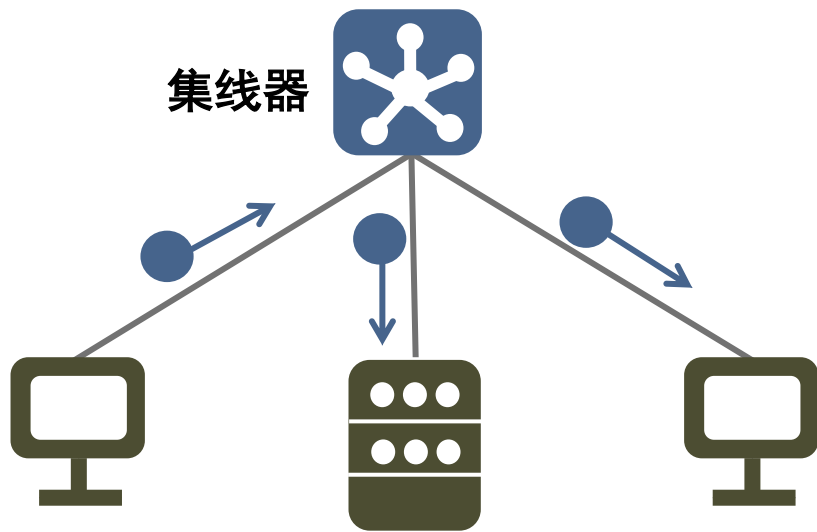
- 工作在数据链路层的存储-转发设备
- 接收整个帧上传至链路层进行校验和检查
- 需要时向上传到物理层转发到不同的网络



# 交换机与集线器

?

- 交换机根据什么判断该不该转发数据帧？



数字/模拟信号



数据帧

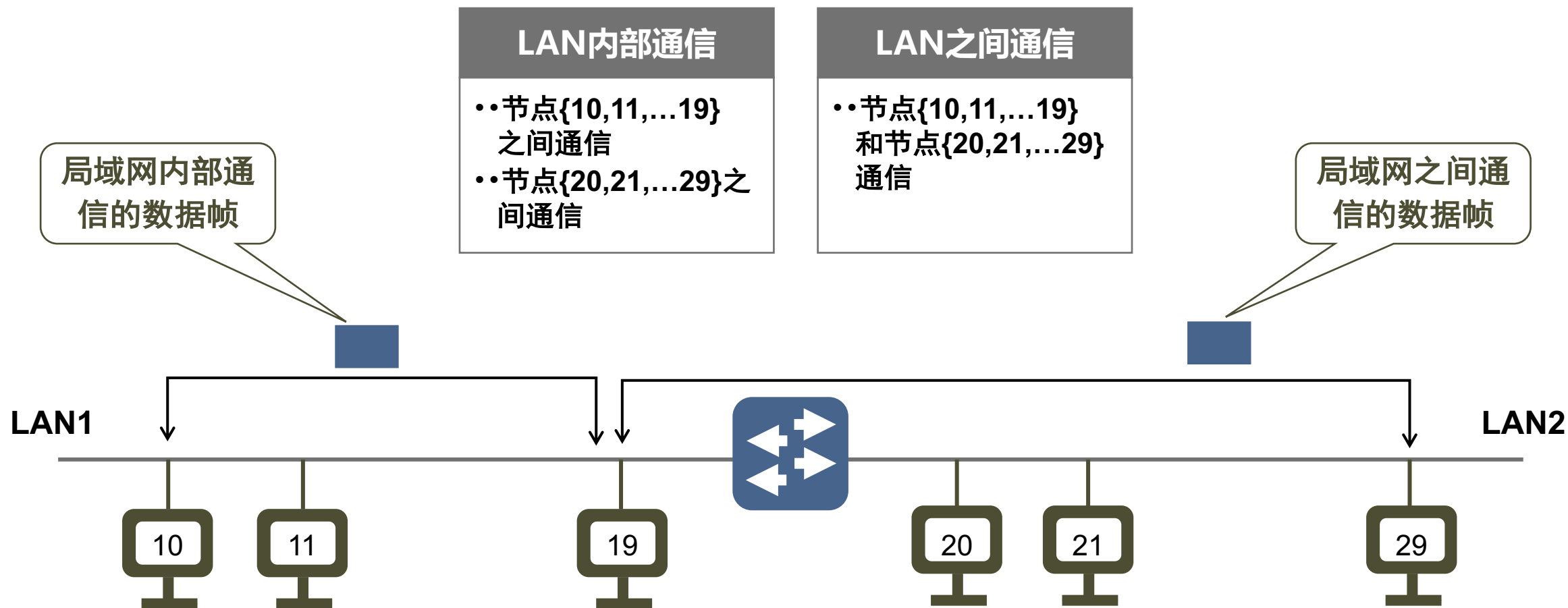


北京大学

# 局域网互连 VS. 网桥工作原理



# 局域网内部和局域网之间通信



# 网桥的基本功能

## 两大功能

- 过滤
- 转发

- 过滤功能

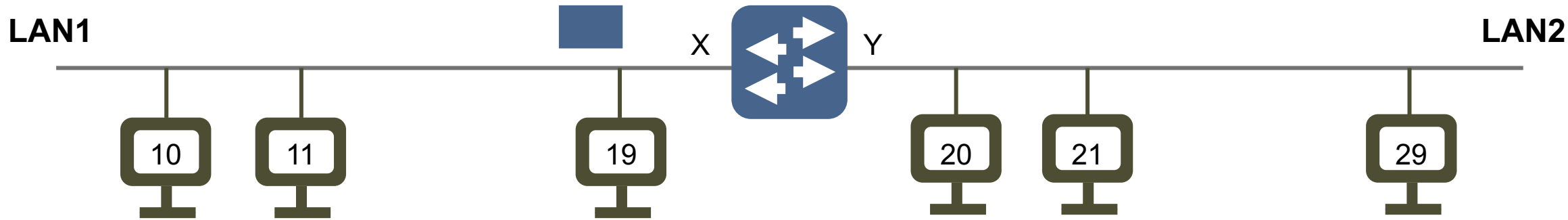
- 过滤掉LAN1内部节点之间通信的帧
- 过滤掉LAN2内部节点之间通信的帧



网桥使得LAN1内通信和LAN2内通信各自独立互不干扰→维持了各自的冲突域

- 转发功能

- 接收并转发从LAN1到20~29的帧
- 接收并转发从LAN2到10~19的帧



# IEEE 802.1透明网桥

## 透明网桥功能

- 将一种LAN上的MAC帧中继到另一个LAN上
- 如果两个LAN使用了不同MAC协议，则将入境帧的内容映射到符合出境LAN的帧格式中
- 路由机制是一种称为生成树的技术

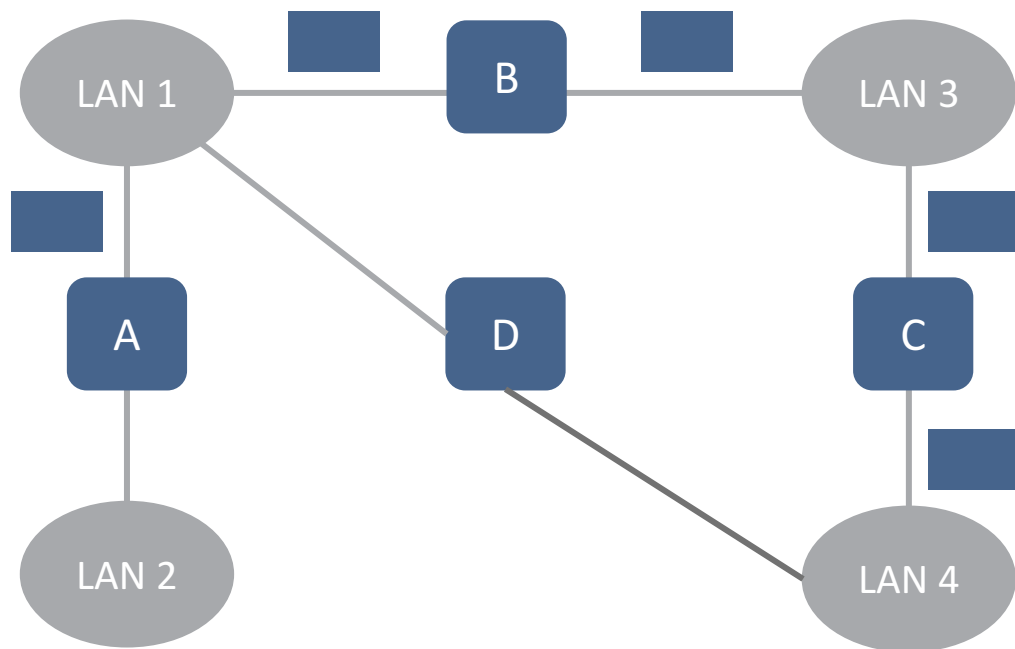
IEEE 802.1D  
IEEE 90e





# 透明网桥的路由功能

假设：A、B、C、D是网桥。



网桥的路由必须自适应网络拓扑的变化

t0：只有A、B、C三个网桥工作  
LAN4通过网桥C连入局域网

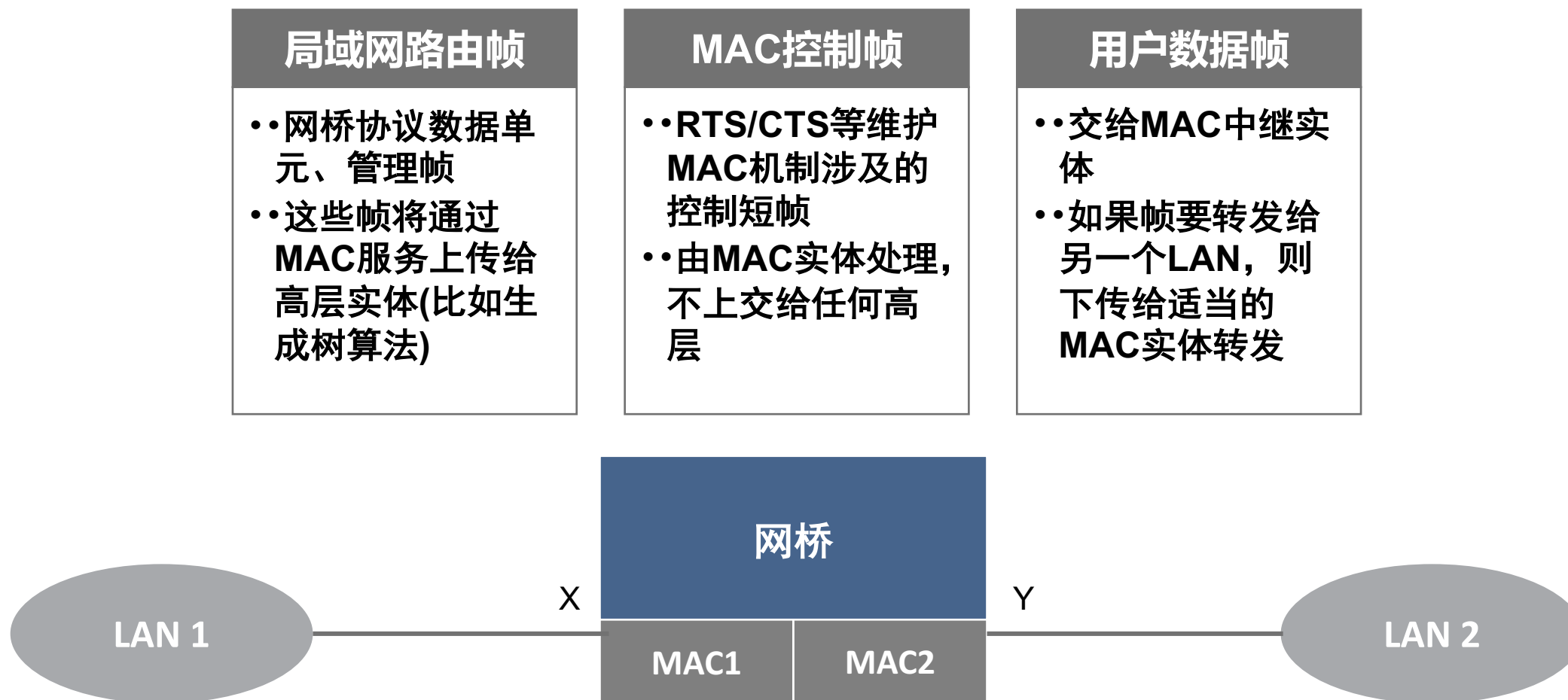
LAN1-LAN4的数据帧必须经过B的转发，而A应该把这样的帧过滤掉

t1：D启动，开始工作  
LAN4切换到网桥D连入局域网  
当D故障时再切换回与C相连

LAN1-LAN4的数据帧经过D转发性能更好；但当D故障后，必须有能力把路由切换回由B转发。



# 网桥要处理的MAC帧



# 802.1过滤数据库

过滤数据库：列出了port号与该port在同一边的节点的地址信息。

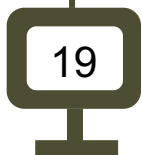
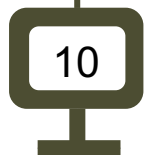
port号 | 一组MAC地址 | 生存期

## 转发规则（当端口X收到一个MAC帧）

- 搜索数据库确定帧目标MAC地址是否列在某个port上
- 如果没找到，则将该帧转发到所有端口（除X外）
- 如果目标地址列在某个端口y ( $y \neq x$ ) 上，则检查端口y状态
  - ① 如果y不阻塞，则将帧转发到与y相连的LAN上
  - ② 如果y阻塞则丢弃该帧

X: 10,11,...,19  
Y: 20,21,...,29

局域网A



X



过滤DB

Y



局域网B

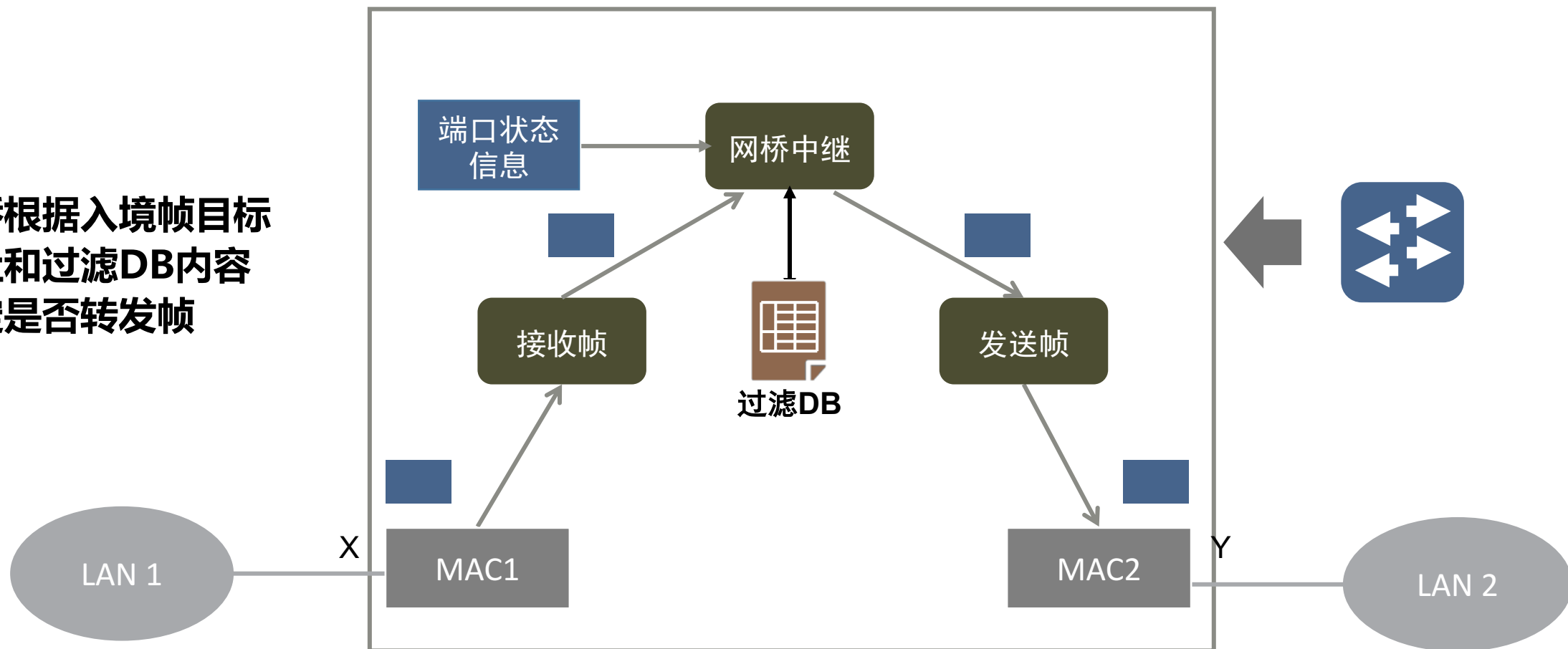


北京大学

filtering DB 过滤数据库

# IEEE 802.1透明网桥转发帧

网桥根据入境帧目标地址和过滤DB内容确定是否转发帧



# IEEE 802.1后向学习能力

?

过滤数据库的内容如何设置才能反应局域网的当前布局?

## 后向学习依据

- 到达某个端口的帧其源地址字段指明了来自入境LAN方向
- 网桥根据该MAC地址更新过滤数据库

## 后向学习过程

- if 已存在相应的地址绑定信息 then
- 更新DB(当方向有变时)并重置计时器;
- else 在DB中创建一条新的绑定信息, 设置计时器

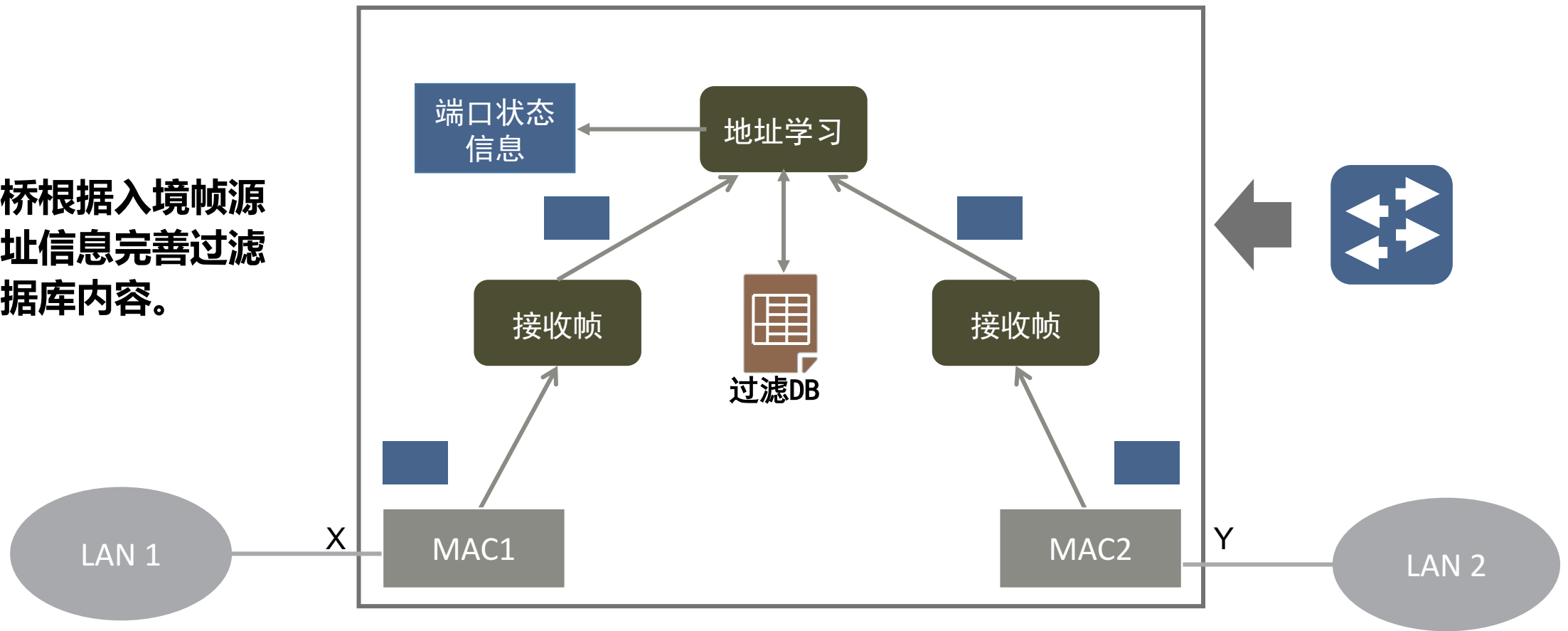
## 生存计时器作用

- 当往数据库增加一条新绑定信息时设置该计时器(缺省300秒)
- 计时器超时从库中删去该条信息
- 每当接收一个帧时将其源地址与DB作比较

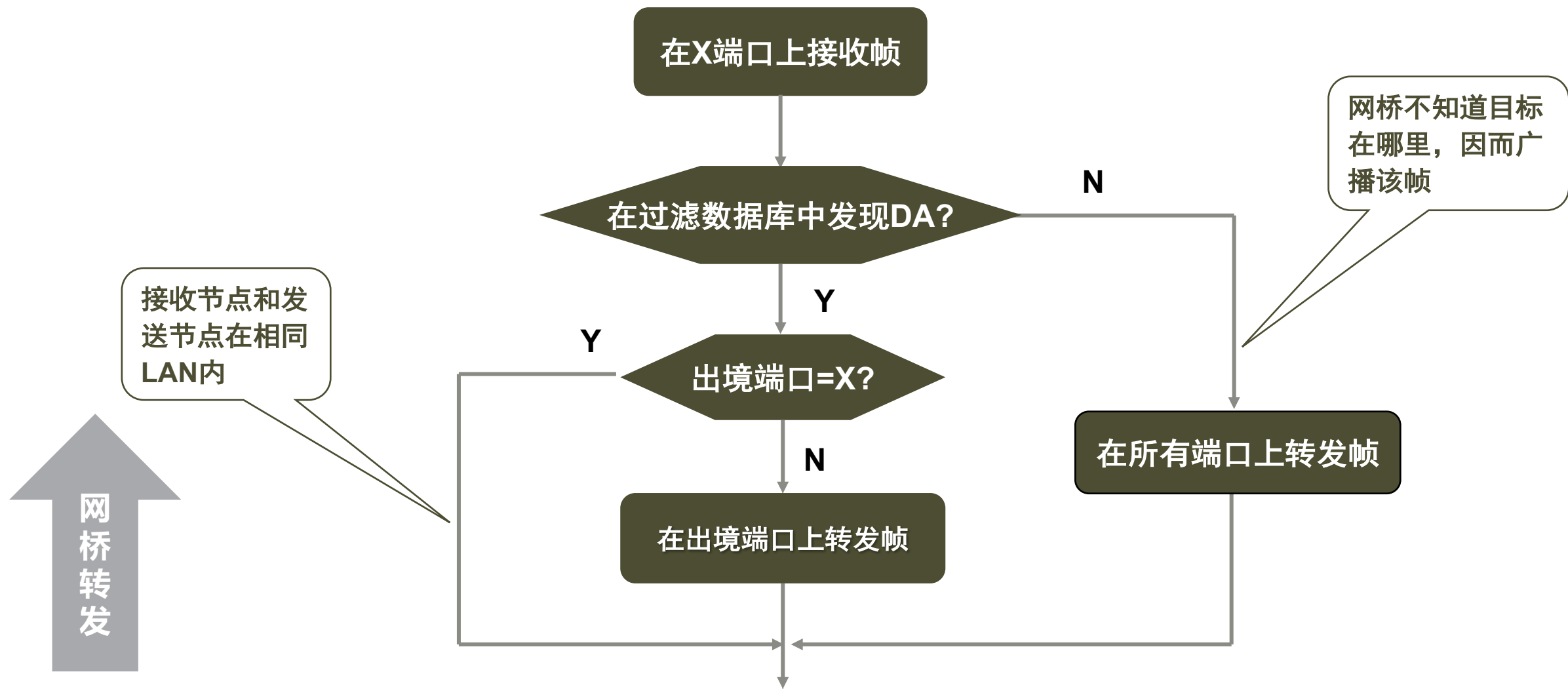


# 802.1 后向学习过程

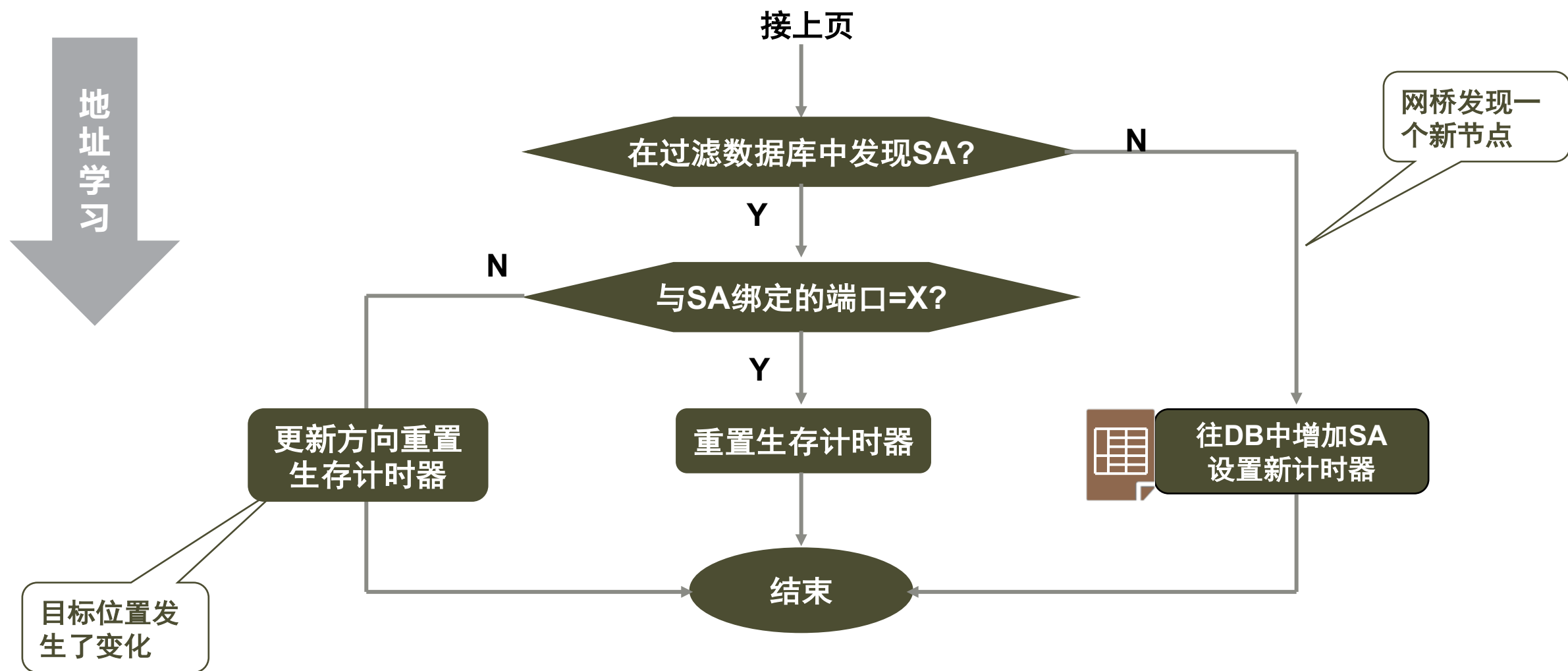
网桥根据入境帧源地址信息完善过滤数据库内容。



# 网桥工作流程——过滤/转发



# 网桥工作流程——反向地址学习





# 网桥工作示例

假设：网络刚初始化，网桥的过滤数据库为空，**X**和**Y**是网桥的两个端口。各节点的发送顺序依次为：

- ① 节点**10**给节点**19**发送一个数据帧
- ② 节点**29**给节点**10**发送一个数据帧
- ③ 节点**11**给节点**10**发送要给数据帧
- ④ 节点**16**给节点**19**再发一个数据帧

试问：网桥的行为和过滤数据库内容变化

过滤数据库内容

端口	主机MAC地址列表			
X	10		11	16
Y		29		

时间 →

• •  
绑定10-X    转发到Y

• •  
绑定29-Y    转发到X

• •  
绑定11-X    过滤帧

• •  
绑定16-X    转发到Y

LAN1

X

Y

LAN2

10

11

16

19

20

21

29



北京大学