

802.11介质访问控制方法

□ 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
- 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在于避免多个站点同时传输引起的冲突

2022/12/16

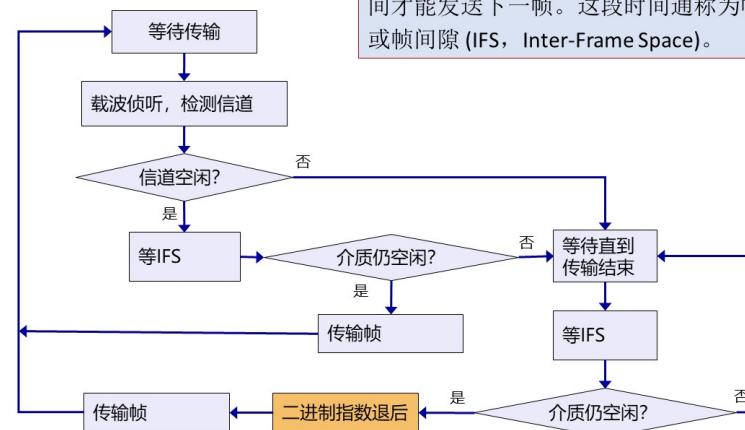
计算机网络与信息安全研究室

36

802.11介质访问控制方法 (续)

□ 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)。



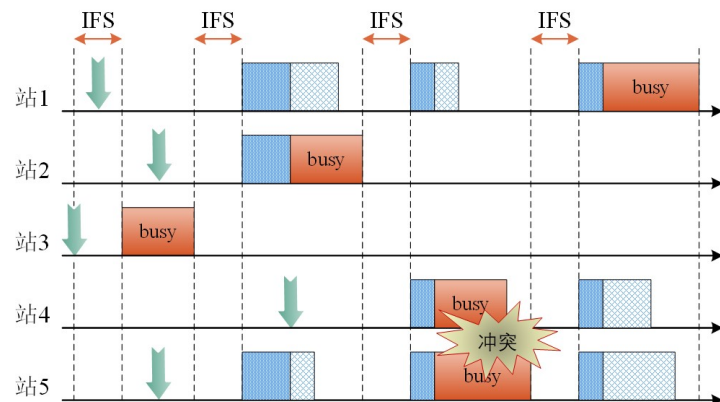
2022/12/16

计算机网络与信息安全研究室

37

802.11介质访问控制方法 (续)

□ CSMA/CA示例



2022/12/16

计算机网络与信息安全研究室

38

802.11介质访问控制方法 (续)

□ 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应网络的负载情况
 - 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

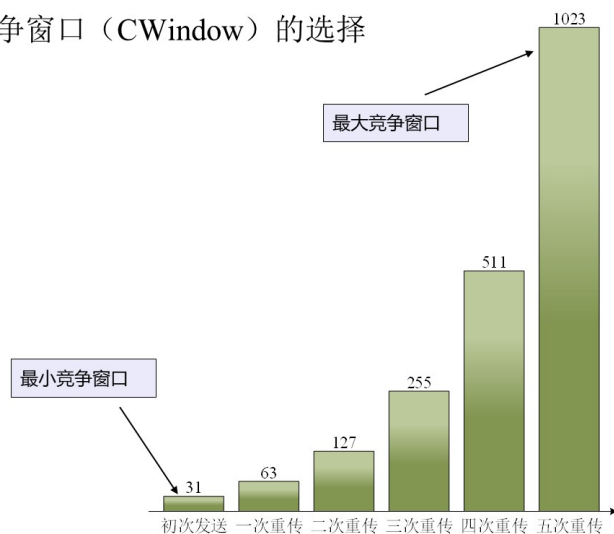
2022/12/16

计算机网络与信息安全研究室

39

802.11介质访问控制方法（续）

❑ 竞争窗口（CWindow）的选择



2022/12/16

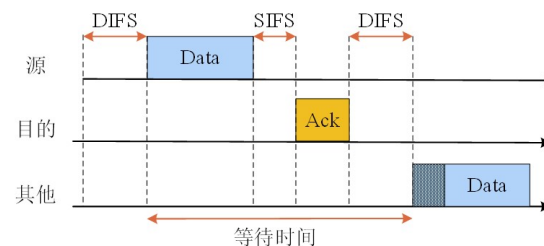
计算机网络与信息安全研究室

40

802.11介质访问控制方法（续）

❑ 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？

2022/12/16

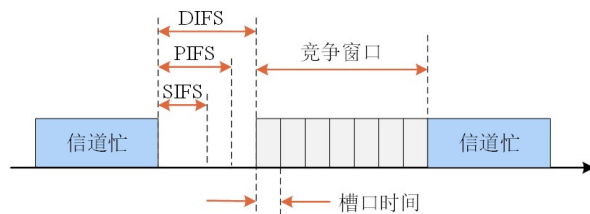
计算机网络与信息安全研究室

41

802.11介质访问控制方法（续）

❑ 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），轮询服务
- DIFS（DCF IFS）：最低优先级（SIFS+2），异步数据服务



2022/12/16

计算机网络与信息安全研究室

42

802.11介质访问控制方法（续）

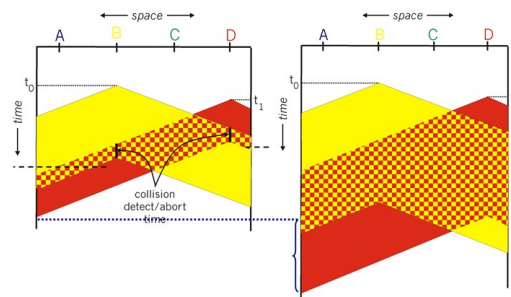
❑ 冲突会发生

- 几乎同时开始发送的节点之间
 - 由于传播延时，类似以太网
- 隐藏终端问题

❑ 超时重传解决传输错误

❑ 长帧冲突的代价更高

- 如何减少长帧冲突？



2022/12/16

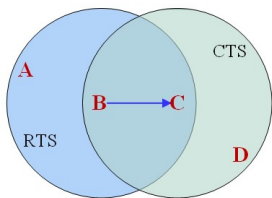
计算机网络与信息安全研究室

43

802.11介质访问控制方法（续）

□ 冲突避免之RTS-CTS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Duration ID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（Network Allocation Vector）
 - 虚拟载波侦听（Virtual Carrier Sense）
- 通过RTS和CTS帧很短，冲突概率小，信道浪费少



2022/12/16

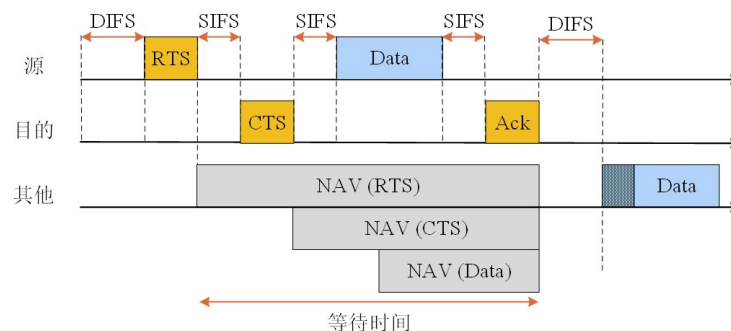
计算机网络与信息安全研究室

44

802.11介质访问控制方法（续）

□ 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



2022/12/16

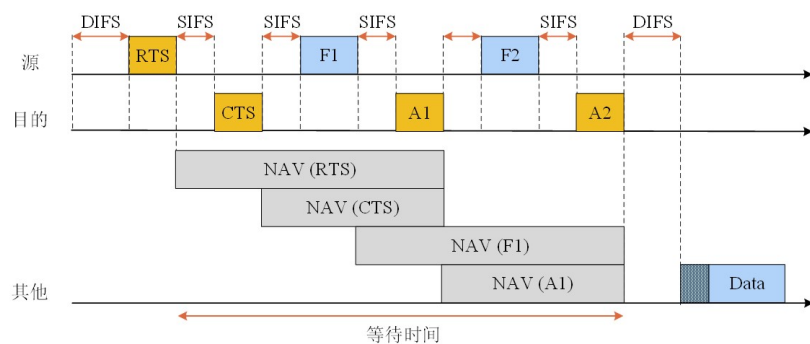
计算机网络与信息安全研究室

45

802.11介质访问控制方法（续）

□ 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

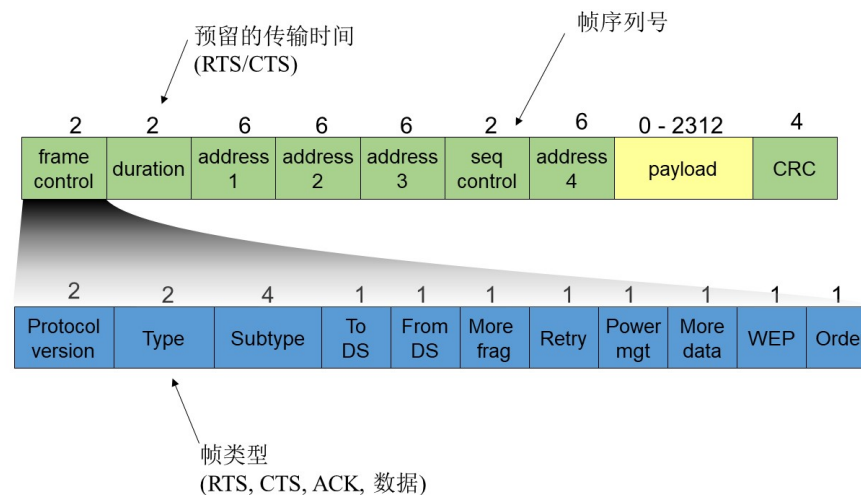


2022/12/16

计算机网络与信息安全研究室

46

802.11帧结构



2022/12/16

计算机网络与信息安全研究室

47

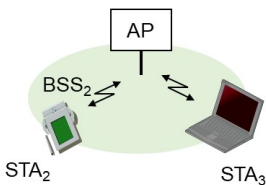
802.11无线局域网组网方法

■ 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: Basic Service Set Identifier
 - AP的MAC地址，标识一个基本服务集
- SSID: Service Set Identifier
 - 32字节网名，标识一个扩展服务集，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）



2022/12/16

计算机网络与信息安全研究室

48

802.11无线局域网组网方法（续）

□ 被动扫描：

- AP周期性发送**Beacon**帧，站点在11个通道上扫描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**

□ 主动扫描：

- 站点依次在11个信道发出包含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

2022/12/16

计算机网络与信息安全研究室

49

802.11无线局域网组网方法（续）

□ 认证：

- 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。只有身份认证通过的站点才能进行无线接入访问。
- 802.11提供几种认证方法，有简单有复杂，如采用802.1x/EAP认证方法时大致过程如下：
 - 站点向AP发送**认证请求**
 - AP向认证服务器发送请求信息要求验证站点身份
 - 认证服务器认证完毕后向AP返回相应信息
 - 如果站点身份不符，AP向站点返回错误信息
 - 如果站点身份相符，AP向站点返回**认证响应**信息

2022/12/16

计算机网络与信息安全研究室

50

802.11无线局域网组网方法（续）

□ 关联：

- 当 AP 向站点返回认证响应信息。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**）
 - Capability, Listen Interval, SSID, Supported Rates
 - AP 向站点返回关联响应（**Association Response**）
 - 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）

2022/12/16

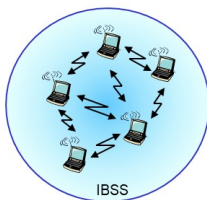
计算机网络与信息安全研究室

51

802.11无线局域网组网方法（续）

□ 自组织模式

- 建立独立基本服务集（IBSS），站点之间直接通信
- 站点设成 Ad-hoc 模式
- 站点先寻找具有指定SSID的IBSS是否存在。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中的所有站点参加发送Beacon，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

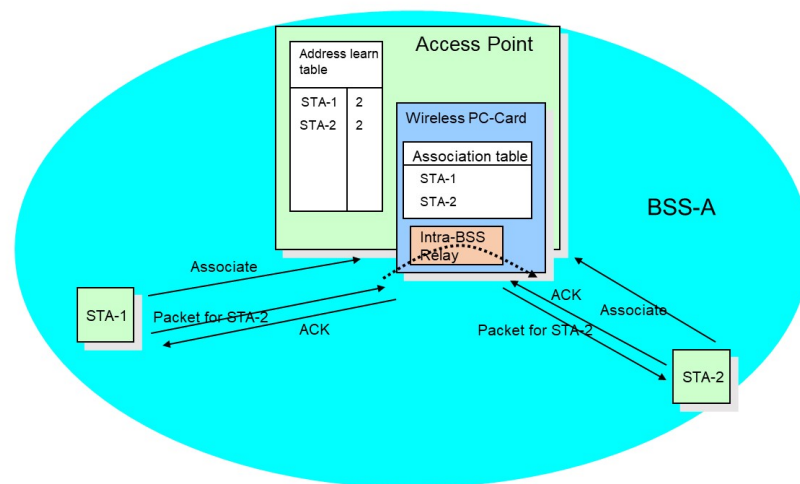


2022/12/16

计算机网络与信息安全研究室

52

BSS内部数据传输

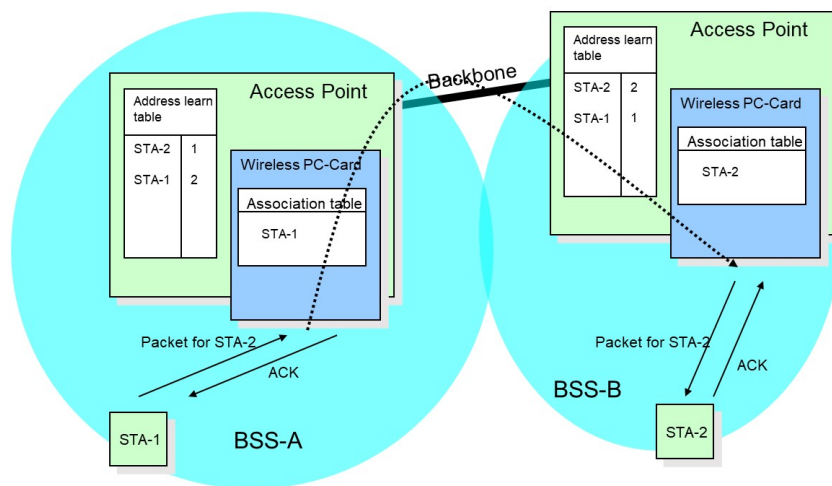


2022/12/16

计算机网络与信息安全研究室

53

BSS之间数据传输



2022/12/16

计算机网络与信息安全研究室

54

- 接口层基础
- 局域网体系结构与组网方法
- 局域网编址与ARP协议
- 链路层差错控制
- 共享式与交换式以太网
- 无线局域网

2022/12/16

计算机网络与信息安全研究室

55