

无线网络

无线网络接入方式

固定接入

- 在作为网络用户期间，用户设置的地理位置保持不变。

移动接入

- 用户设置能够以车辆速度移动时进行网络通信。当发生切换时，通信仍然是连续的。

便携接入

- 在受限的网络覆盖面积中，用户设备能够在以步行速度移动时进行网络通信，提供有限的切换能力。

游牧接入

- 用户设备的地理位置至少在进行网络通信时保持不变。如用户设备移动了位置，则在此进行通信时可能还要寻找最佳基站。

WiFi

基本服务集

基本服务集 BSS (Basic Service Set) 是无线局域网的最小构件。一个 BSS 包括一个接入点 AP 和若干个移动站。

一个 BSS 所覆盖的地理范围叫做一个基本服务区 BSA

AP的服务集标识SSID

必须为该 AP 分配一个不超过 32 字节的服务集标识符 SSID (Service Set Identifier) (即该 AP 的无线局域网的名字) 和一个通信信道。

基本服务集标识BSSID

每个 AP 有一个唯一的 48 位 MAC 地址，名称是基本服务集标识符 BSSID。在无线局域网中传送的各种帧的首部中，都必须有节点的 MAC 地址 (即 BSSID，但不是 SSID)。

用户通常都知道所连接的无线局域网 SSID，但可以不知道其 BSSID。

扩展服务集ESS

一个 BSS 可以通过 AP 连接到一个分配系统 DS (Distribution System)，然后再连接到另一个 BSS，构成了一个扩展服务集 ESS (Extended Service Set)。

扩展服务集标识符 ESSID

ESS 也有个标识符，是不超过 32 字符的字符串名字 (不是地址)，叫做扩展服务集标识符 ESSID。

分配系统 DS

DS 的作用：使 ESS 对上层的表现就像一个 BSS 一样。

DS 可以使用以太网 (最常用)、点对点链路或其他无线网络。

与接入点 AP 建立关联

一个移动站若要加入到一个基本服务集 BSS，就必须先选择一个接入点 AP，并与此接入点建立关联。

建立关联

- 表示这个移动站加入了选定的 AP 所属的子网，并和这个 AP 之间创建了一个虚拟线路。
- 只有关联的 AP 才向这个移动站发送数据帧，而这个移动站也只有通过关联的 AP 才能向其他站点发送数据帧。

建立关联的方法

- 被动扫描，即移动站等待接收接入站周期性发出的信标帧
- 主动扫描，即移动站主动发出探测请求帧，然后等待从 AP 发回的探测响应帧

关联

- 重建关联（reassociation）和分离（dissociation）
 - 移动站使用重建关联（reassociation）服务，可把这种关联转移到另一个接入点。
 - 当使用分离（dissociation）服务时，可终止这种关联。

热点

- 热点
 - 公众无线入网点
 - 许多地方，如办公室、机场、快餐店、旅馆、购物中心等都能够向公众提供有偿或无偿接入 Wi-Fi 的服务。这样的地点就叫做。
- 热区
 - 由许多热点和 AP 连接起来的区域叫做（hot zone）。热点也就是
- 无线因特网服务提供者 WISP
 - 用户可以通过无线信道接入到 WISP，然后再经过无线信道接入到因特网。

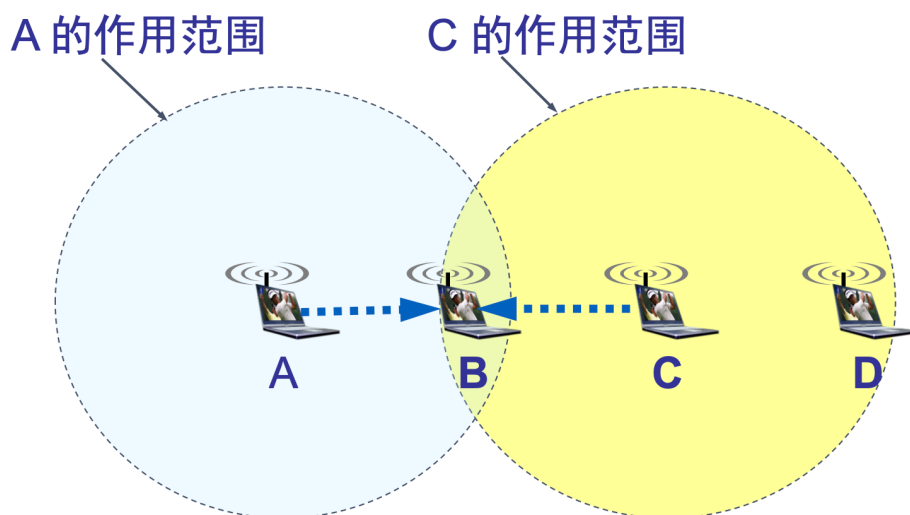
CSMA/CA

问题：无线局域网不能使用CSMA/CD协议

协议	载波监听 (CS)	冲突检测 (CD)
CSMA/CD	发送站在发送前检测有线信道空闲	发送站在发送过程中，不间断检测有线信道是否有冲突
Wi-Fi	发送前检测，即使在发送端无冲突，但可能接收端正在接收来自其他站的数据	1.发送站在同载波的边发边收，来自远端的信号强度远小于发送信号强度；2.发送站在发送过程中检测到发送端信道无冲突，但可能在接收端有冲突

隐蔽站问题

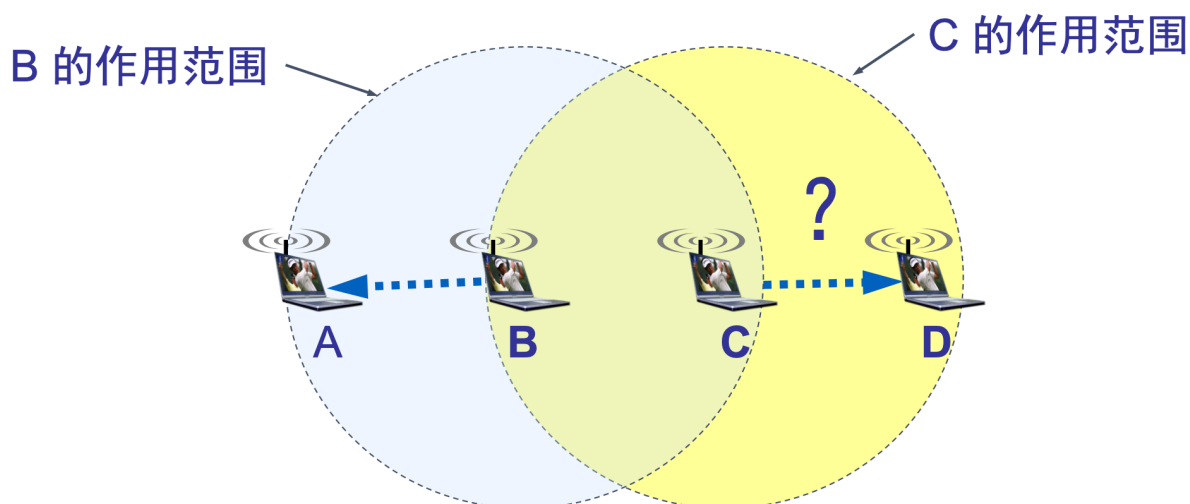
未能检测出媒体上已存在的信号的问题



当 A 和 C 检测不到无线信号时，都以为 B 是空闲的，因而都向 B 发送数据，结果发生碰撞。

暴露站问题

B 向 A 发送数据并不影响 C 向 D 发送数据



B 向 A 发送数据，而 C 又想和 D 通信。
C 检测到媒体上有信号，于是不敢向 D 发送数据。

CSMA/CA 协议

改进：

- 增加碰撞避免 CA (Collision Avoidance)：尽量减少碰撞发生的概率。
- 使用 CSMA/CA 的同时，使用停止等待协议
 - 链路层确认，解决碰撞后重传。

CSMA/CA 四种工作模式：

- 载波监听/随机退避
- 虚拟载波监听

- 点（基站）协调
- 混合协调

方式一：载波监听/随机退避

1. 如果初始时某站监听到信道空闲，将在一个时间间隔（DIFS）的短时间段后发送该帧。
2. 否则，该站点进行推迟接入：选择一个随机退避值并在侦听信道空闲时递减此值；当侦听到信道忙时，此值不变。
3. 当计数值减为0（只能发生在信道空闲时），该站点发送整个数据帧并等待确认。
4. 如果收到确认，发送站知道发送成功。若该站要发送另一帧，将从第2步开始本协议。如果未收到确认，发送站重新进入第2步的回退阶段，并在一个更大的范围内选取随机值。

推迟接入机制

- 信道从忙态变为空闲时，任何一个站要发送数据帧：
 - 等待一个 DIFS 的间隔，递减当前随机退避时间以便再次重新试图接入信道。
 - 各站均要执行退避算法，大大减少发生碰撞的概率。
- 站点每经历一个时隙的时间就检测一次信道。
 - 若检测到信道空闲，退避计时器就继续倒计时。
 - 若检测到信道忙，就冻结退避计时器的剩余时间，重新等待信道变为空闲，并再经过时间DIFS 后，从剩余时间开始继续倒计时。
 - 如果退避计时器的时间减小到零时，就开始发送整个数据帧。

二进制指数退避算法

- 第 i 次退避争用窗口 CW 在 2^{4+i} 个时隙中随机地选择一个，即：
 - 第 i 次退避是在时隙 $\{0, 1, \dots, 2^{4+i} - 1\}$ 中随机地选择一个
 - 第 1 次退避是在 32 个时隙（而不是 2 个）中随机选择一个
 - 第 2 次退避是在 64 个时隙（而不是 4 个）中随机选择一个
 - 第 6 次以及 6 次以上重传时，随机退避的时隙数应在 0 ~ 1023 之间生成，争用窗口 CW 不再增大。
 - **建议值：15 (最小) \leq 争用窗口 $CW \leq$ 1023 (最大)**

• CSMA/CD

- 第 i 次退避争用窗口 CW 是在时隙 $\{0, 1, \dots, 2^i - 1\}$ 中随机地选择一个

退避算法的使用情况

- 不使用退避算法
 - 检测到信道是空闲的，并且这个数据帧是要发送的第一个数据帧。
- 除此以外所有情况，都必须使用退避算法
 - 在发送第一个帧之前检测到信道处于忙态。
 - 已发出的数据帧未收到确认，重传数据帧。
 - 接着发送后续的数据帧（为了防止一个站长期垄断发送权）。

载波监听/随机退避的特点

- 优点
 - 可靠传输
 - 简单
 - 缺点
 - 不能高效解决隐蔽站/暴露站问题
 - 原因：稀缺
 - 无线信道带宽
 - 移动终端电量
-

方式二：虚拟载波监听

- 让源站将它要占用信道的时间（包括目的站发回确认帧所需的时间）通知给所有其他站，以便使其他所有站在这段时间都停止发送数据。
- 大大降低碰撞的机会。
- 其他站并没有监听信道，而是由于其他站收到“源站的通知”才不发送数据。

源站 A 在发送数据帧之前先发送一个短的控制帧，对信道进行预约叫做请求发送 RTS (Request To Send)，它包括源地址、目的地址和这次通信（包括相应的确认帧）所需的持续时间。

若媒体空闲，则目的站 B 就发送一个响应控制帧，叫做允许发送 CTS (Clear To Send)，包括这次通信所需的持续时间。

A 收到 CTS 帧后就可发送其数据帧。

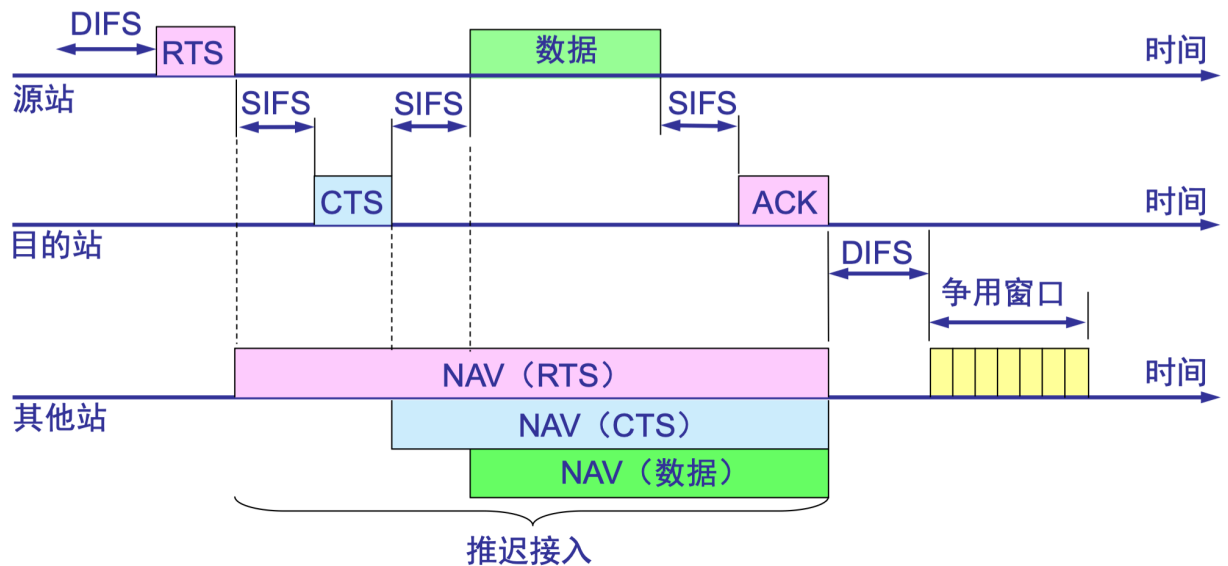
优点：

- 隐蔽终端的问题被解决。
- RTS和CTS帧较短，涉及RTS帧和CTS帧的碰撞持续很短的时间，信令的碰撞代替数据碰撞。
- RTS和CTS被正确传输，后续的DATA帧和ACK帧就能无碰撞的发送。

缺点：

- 暴露站问题仍未解决
- 多一轮信令传输，在低负载的时候降低吞吐率
 - 浪费信道的时间 [RTS + SIFS + CTS + SIFS]
- 不能完全避免碰撞

RTS、CTS、数据帧、ACK 帧的传输间隔



方式三：点（基站）协调

- 基站周期性的广播一个信标帧
 - 包括调频、延迟时间、时间同步等系统参数
 - 邀请新的站参与表决服务
- 基站对其他站进行表决，决定传输顺序。
 - 不会冲突
 - 一旦某站申请到特定速率的表决，即获得带宽保证，可以保证服务质量
- 缺点：
 - 轮询式的表决申请耗费网络带宽。

实际工作：CSMA与RTS/CTS混合

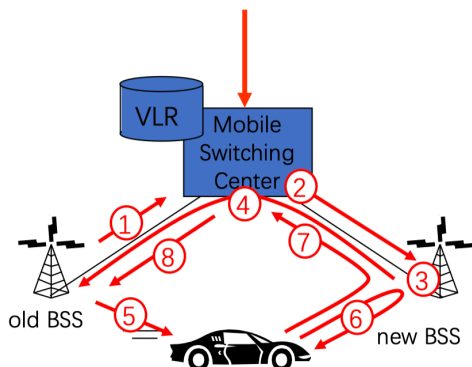
为什么信道空闲还要再等待

- 可能有其他的站有高优先级的帧要发送。
- 时隙长短在不同 802.11 标准中可以有不同数值。

方式五：利用冲突

ZigZag

GSM: MSC内的切换过程



- 1.旧基站通知 MSC 即将发生切换，提供可切换到的新基站列表
2. MSC 建立到新基站的路径，即预留资源
3. 新基站为手机分配信道
4. 新基站通知MSC, 就基站: ready
5. 旧基站通知手机: 切换到新基站
6. 手机、新基站通过以分配信道进行握手。
7. 手机通过新基站通知MSC: 切换成功；MSC将通话信息通过新基站传送。
8. 旧基站释放资源。

移动IP

- 移动 IP (Mobile IP)：由 IETF 开发的一种技术，允许计算机移动到外地时，仍然保留其原来的 IP 地址。
- 移动 IP 要解决的问题：使用户的移动性对上层的网络应用透明。

移动站 A 必须有一个原始地址，即永久地址，或归属地址 (home address)。移动站原始连接到的网络叫做归属网络 (home network)。永久地址和归属网络的关联是不变的。归属代理 (home agent) 让地址的改变对互联网的其余部分透明，它通常就是连接在归属网络上的路由器，代理功能在应用层完成。归属代理既是路由器，也是主机。

当移动站 A 移动到另一个地点，接入的网络称为被访网络 (visited network)或外地网络 (foreign network)。被访网络中使用的代理叫做外地代理 (foreign agent)，它通常就是连接在被访网络上的路由器。为移动站 A 在被访网络中创建的临时地址叫做转交地址 (care-of address)。

移动网络对高层协议的影响

漫游时，会经常更换移动用户到无线网络的连接点，网络连接就会发生很短时间的中断。这种情况对高层协议有没有影响呢？

- TCP 报文段会丢失
- TCP 拥塞控制就会采取措施，减小其拥塞窗口，使 TCP 发送方的报文段发送速率降低。

使用三种方法处理：

1. 本地恢复。差错出现在什么地方，就在什么地方改正。
2. 让 TCP 发送方知道什么地方使用了无线链路。仅在有线网络部分发生了拥塞，TCP 才采用拥塞控制的策略。
3. 把含有移动用户的端到端 TCP 连接拆成两个互相串接的 TCP 连接。从移动用户到无线接入点是一个 TCP 连接（无线信道），而剩下的使用有线网段连接的部分则是另一个 TCP 连接。