3.3 蜂窝互联网接入及其结构

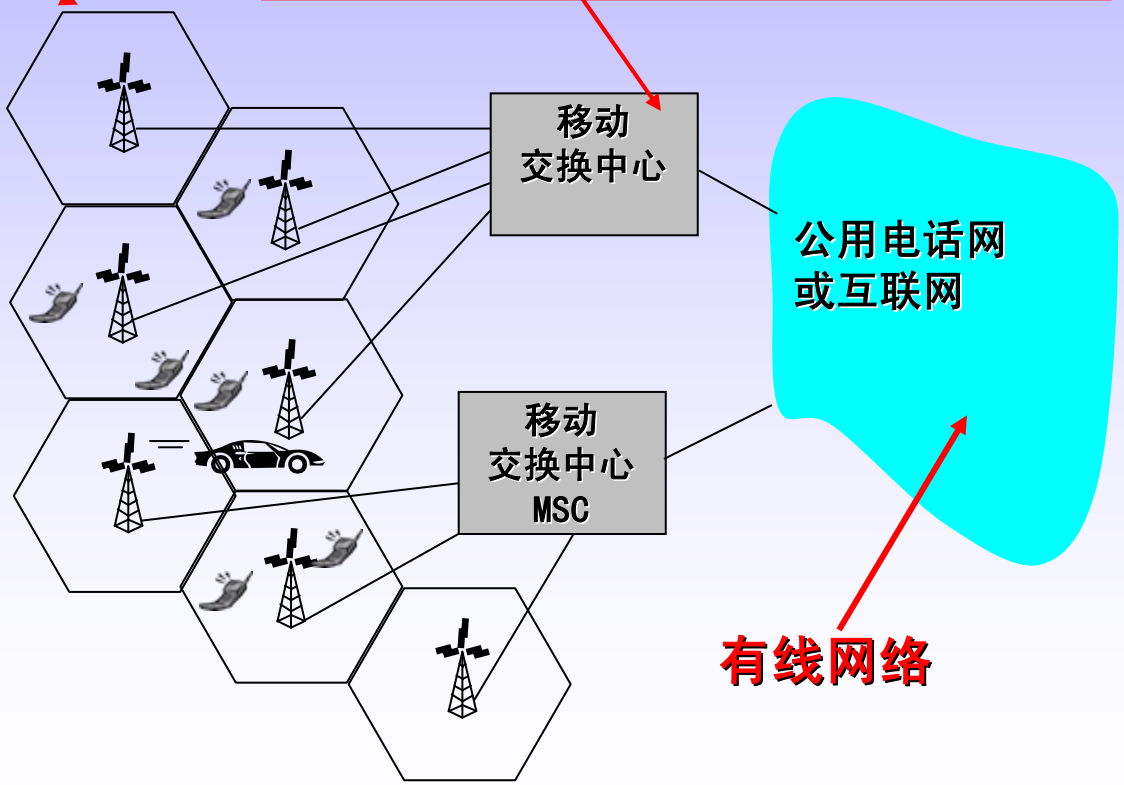
3.3.1 蜂窝网结构

cell

- 覆盖地理范围
- 基站：类 802.11 AP
- 移动用户：通过BS连接到网络
- 空气接口：移动机和基站间的物理和链路层协议

MSC

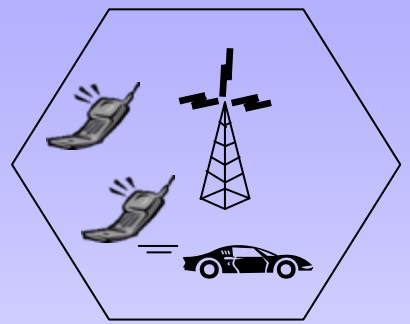
- 连接所有蜂窝到广域网
- 管理呼叫建立
- 处理移动

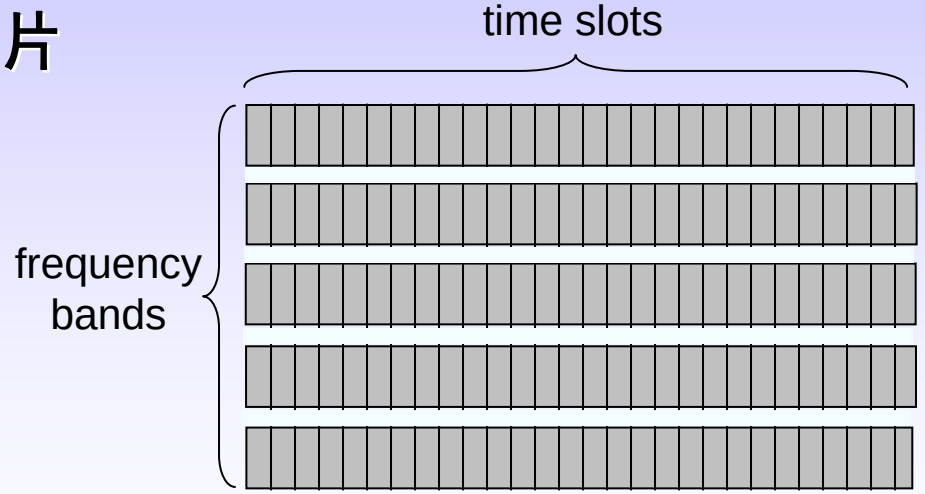


蜂窝网：第一跳

共享Mobile-to-BS 无线频谱
两个技术

- 组合 FDMA/TDMA：
  - 频分：分频谱为频率通道
  - 时分：分每个通道为时片
- CDMA：码分多路接入

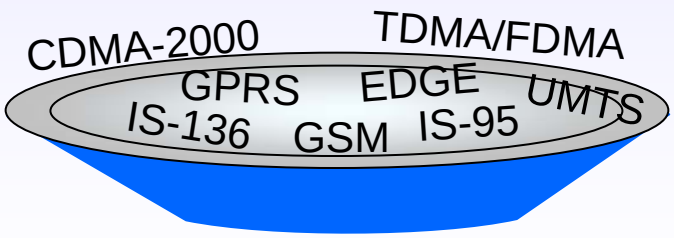




3.3.2 蜂窝标准概要

2G 系统：语音通道

- IS-136 TDMA：组合 FDMA/TDMA（北美）
- GSM（global system for mobile communications）：组合 FDMA/TDMA
  - 更广泛使用
- IS-95 CDMA：码分多路接入



仅参考，
并非全部

2.5 G 系统

语音与数据通道

- 为不能等待 3G 的服务: 2G 扩展
- general packet radio service (GPRS)
  - 由GSM演进
  - 在多个通道上发送数据 (if available)
- 推进全球发展，提高数据率 (EDGE)
  - 也由 GSM发展而来，用提高性调制
  - 数据率升到 384K
- CDMA-2000 (phase 1)
  - 数据率达144K
  - 由IS-95发展而来

3G 系统

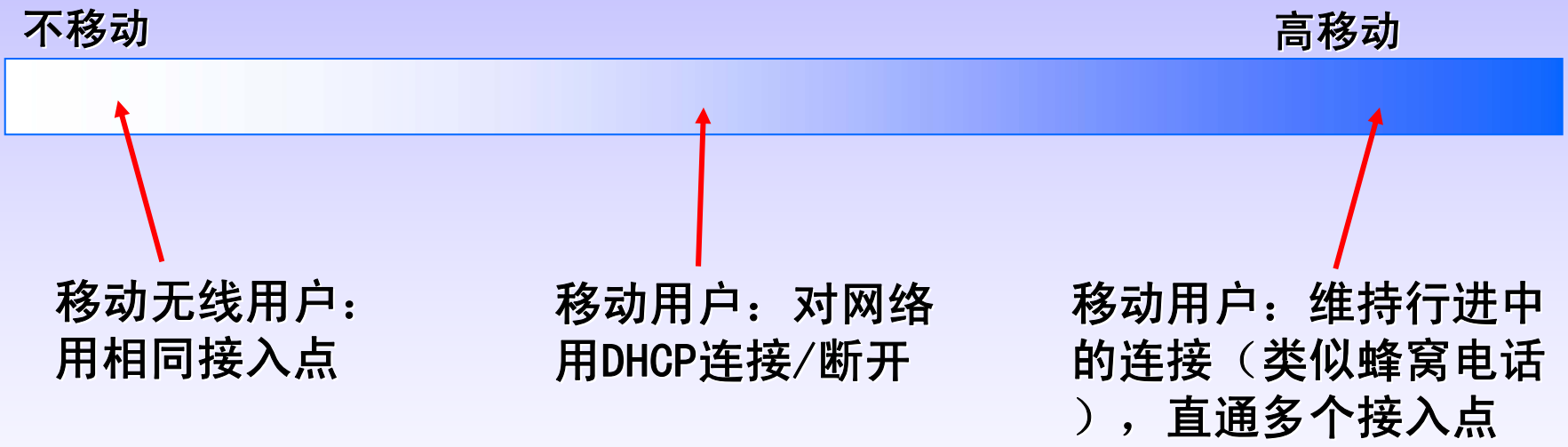
语音/数据

- 通用移动电信服务(UMTS)-Universal Mobile Telecommunications Service
  - 数据服务: 高速上行/下行包接入 (HSDPA/HSUPA): 3 Mbps
- CDMA-2000: CDMA in TDMA slots
  - 数据服务: 数据优化(1xEVDO) 到14 Mbps

3.4 移动接入

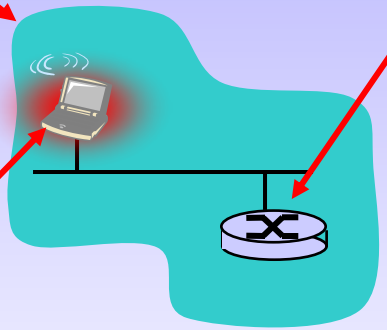
3.4.1 移动的基本概念

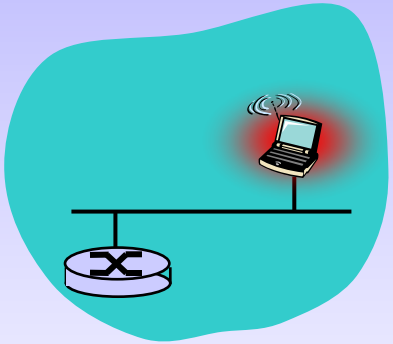
- 从网络视角看：移动谱



家乡网络： 移动机固定地网络
(e.g., 128.119.40/24)

家乡代理HA： 执行远程移动功能的实体





广域网

家乡地址： 家乡常驻网络中的移动机地址
e.g., 128.119.40.186

通信方

home network
home agent
Permanent address
（固定/家乡地址）

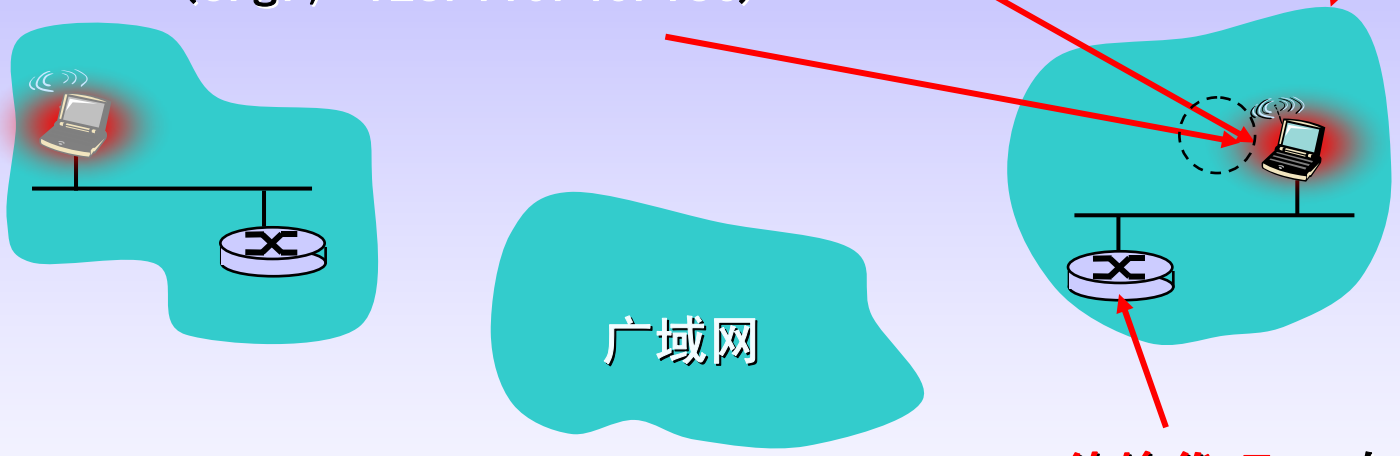
Care-of-address
visited network
foreign agent
correspondent

转交地址: 被访网络中的移动机地址 (e.g., 79.129.13.2)

care-of address : 是分配给移动机的**临时外埠IP地址**

被访网络: 移动机当前所在网络(79.129.13/24)

家乡地址: 保留不变 (e.g., 128.119.40.186)

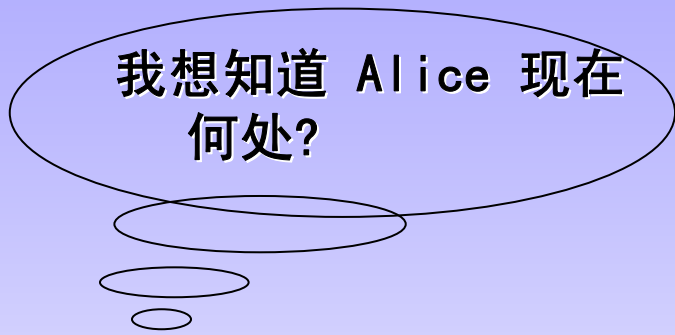


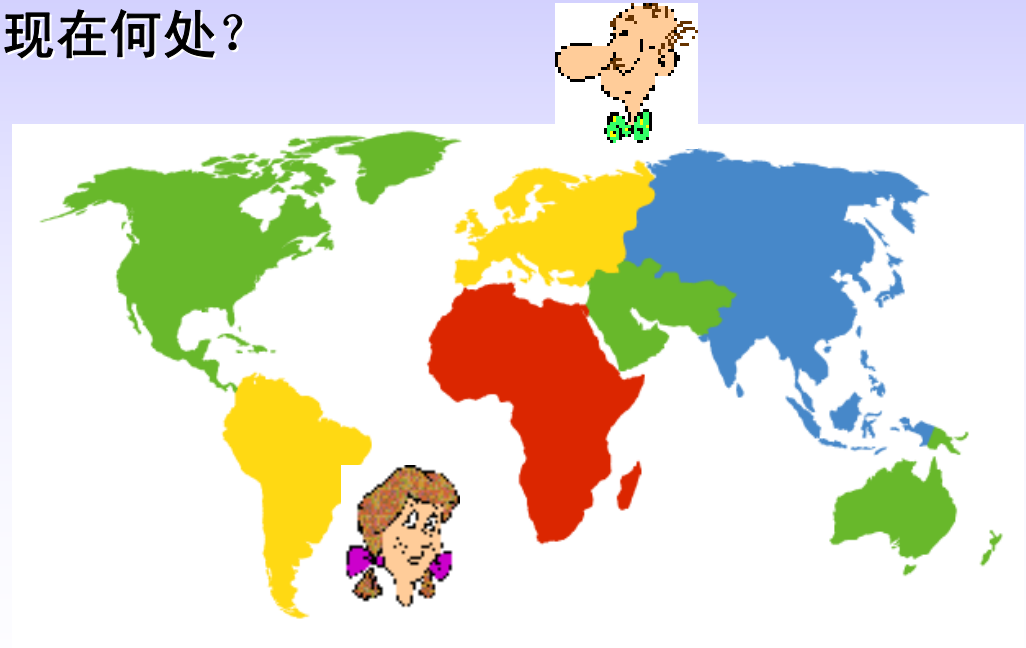
外埠代理FA:在被访网络中执行移动的实体

通信方: 要与移动方通信的对象

怎样联系一个移动的友人

- 考虑友人频繁移动而改变地址，怎样找到他（她）？
  - 搜索所有电话簿?
  - 呼叫他（她）的父母?
  - 让他（她）告诉你他（她）现在何处?



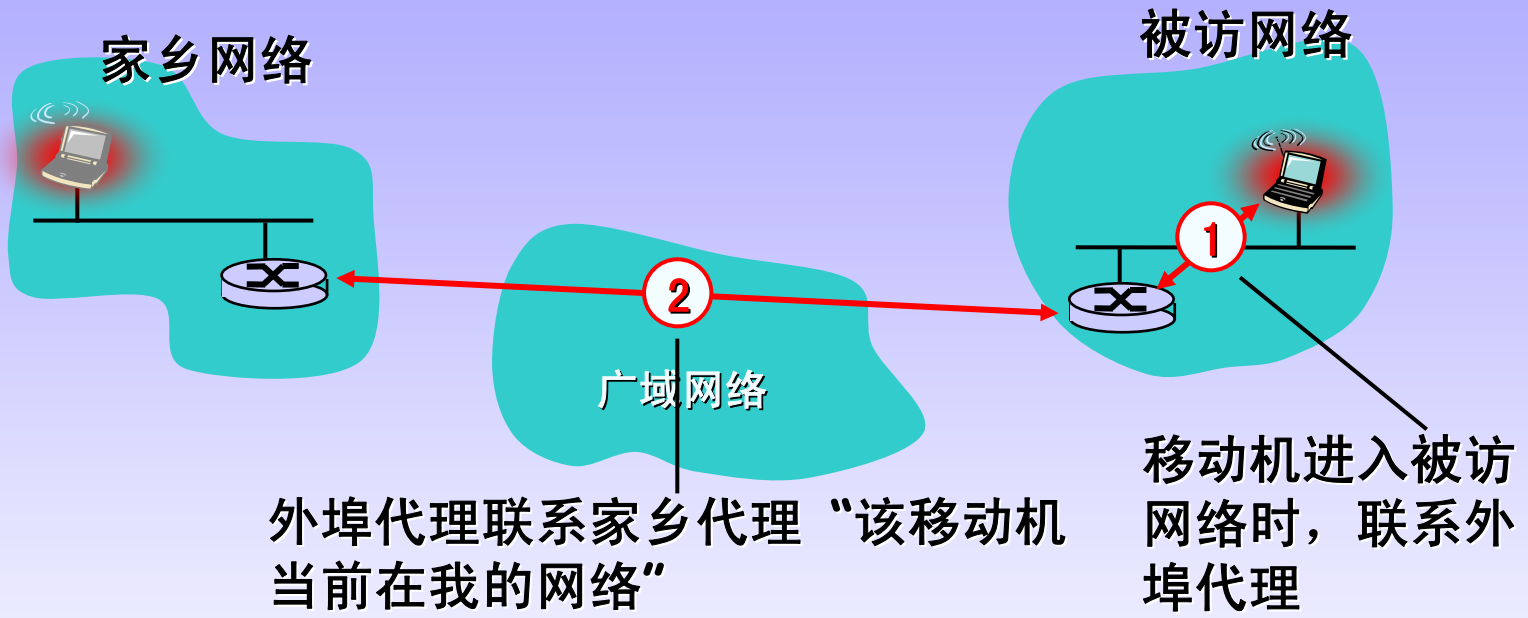


3.4.2 移动寻址与路由

- **让路由处理：**
  - 路由器由常规路由表交换，通告移
    - 路由表指明每个定位后的移动体
    - 对端系统没有改变

- **让端系统处理：**
  - **间接路由：** 通信方到移动机的通信经由家乡网关，然后转发到远程移动机
  - **直接路由：** 通信方得到移动体的外埠地址，直接发送到移动机

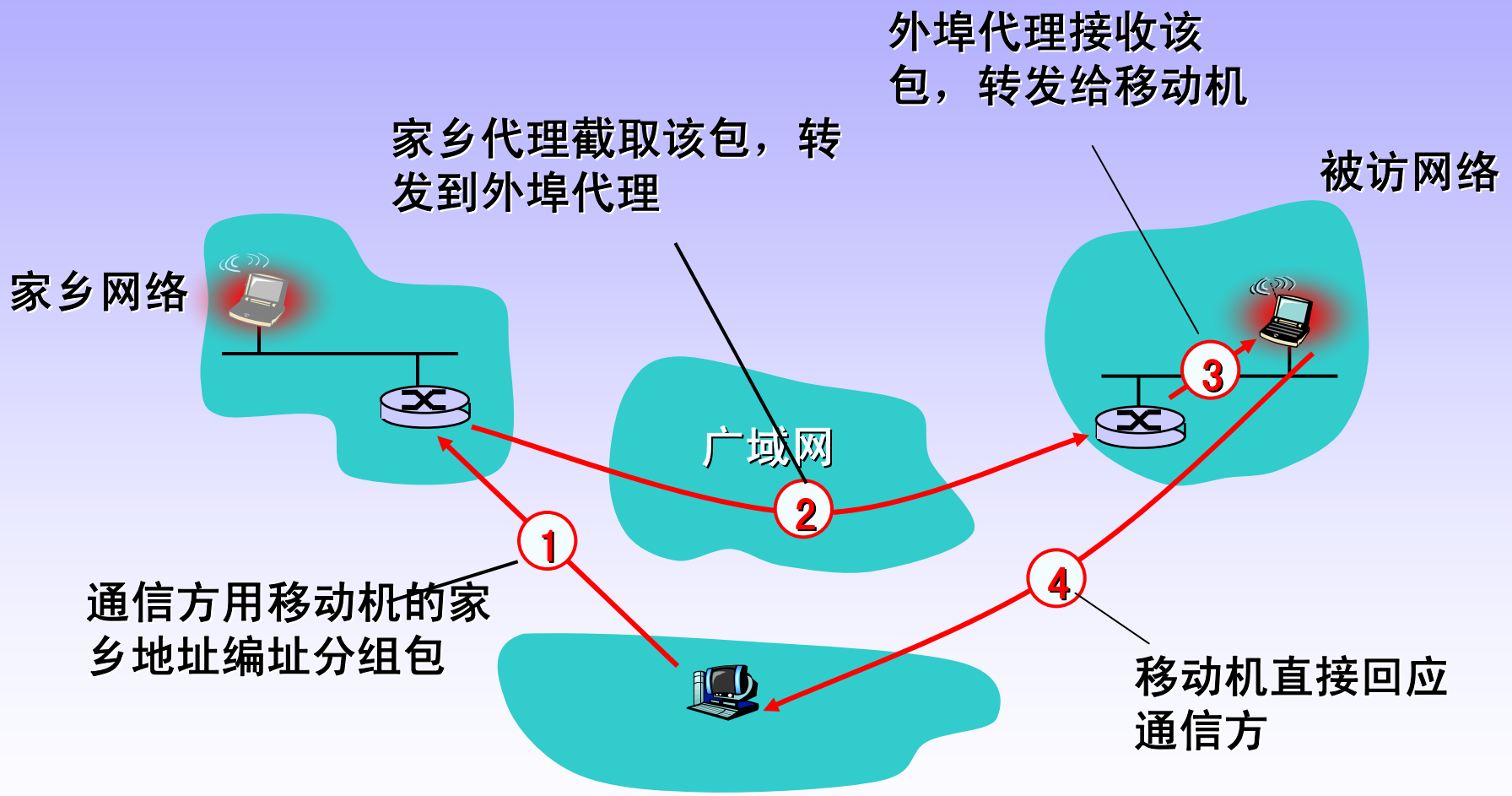
注册登记



最终结果：

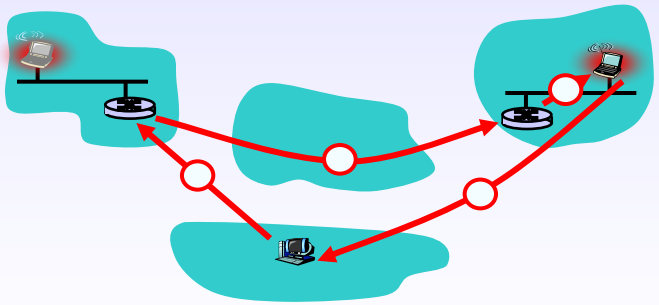
- 外部代理知道移动机
- 家乡代理知道移动机当前位置

间接路由移动


外埠代理接收该包，转发给移动机
家乡代理截取该包，转发到外埠代理
被访网络
家乡网络
广域网
1
2
3
4
通信方用移动机的家乡地址编址分组包
移动机直接回应通信方

说明

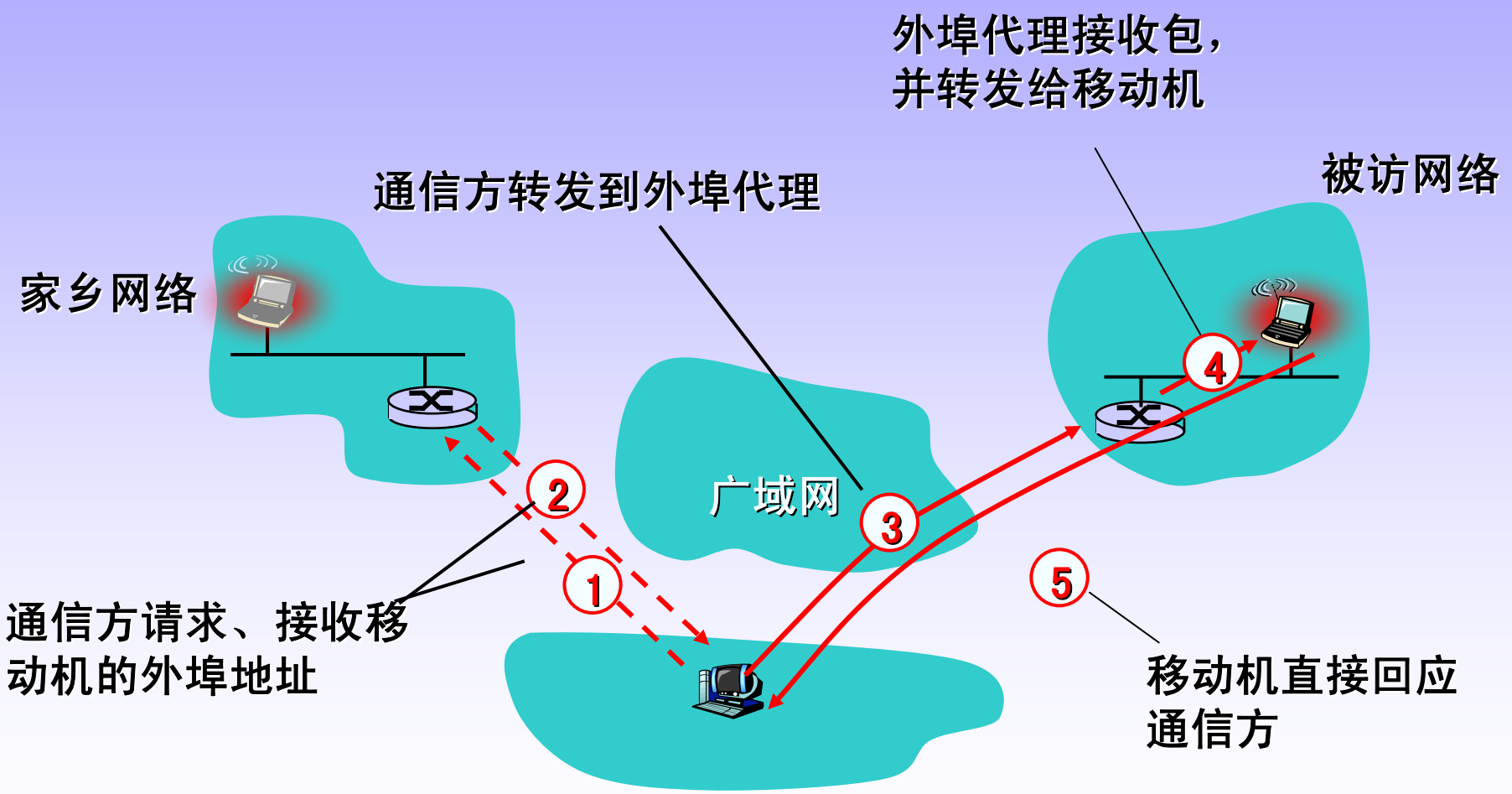
- 移动机使用两个地址
  - 家乡地址：被通信方使用（故移动机位置对通信方是透明的）
  - 转交地址：被家乡代理用来转发数据包到移动机
- 外埠代理功能可由移动机自己做
- 三角路由：通信方-家乡-网络-移动机
  - 当与通信方在同一网络时效率很低



间接路由：在网络间移动

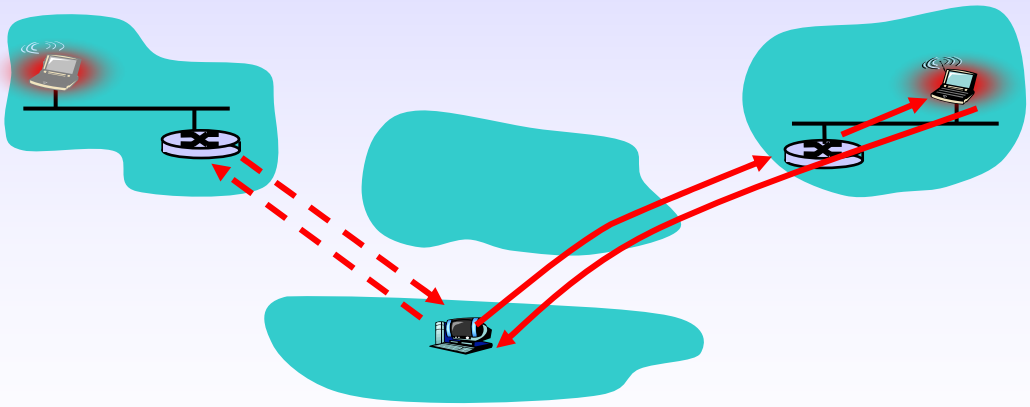
- 建设移动用户移动到另一网络
  - 注册到新的外埠代理
  - 新外埠代理注册到其家乡代理
  - 家乡代理更新移动机的转交地址
  - 把包持续转发到移动机（用新的转交地址）
- 移动，改变外埠网路的透明性： 维持正在进行的连接

直接路由移动


外埠代理接收包，
并转发给移动机
通信方转发到外埠代理
被访网络
家乡网络
广域网
2
3
4
1
5
通信方请求、接收移
动机的外埠地址
移动机直接回应
通信方

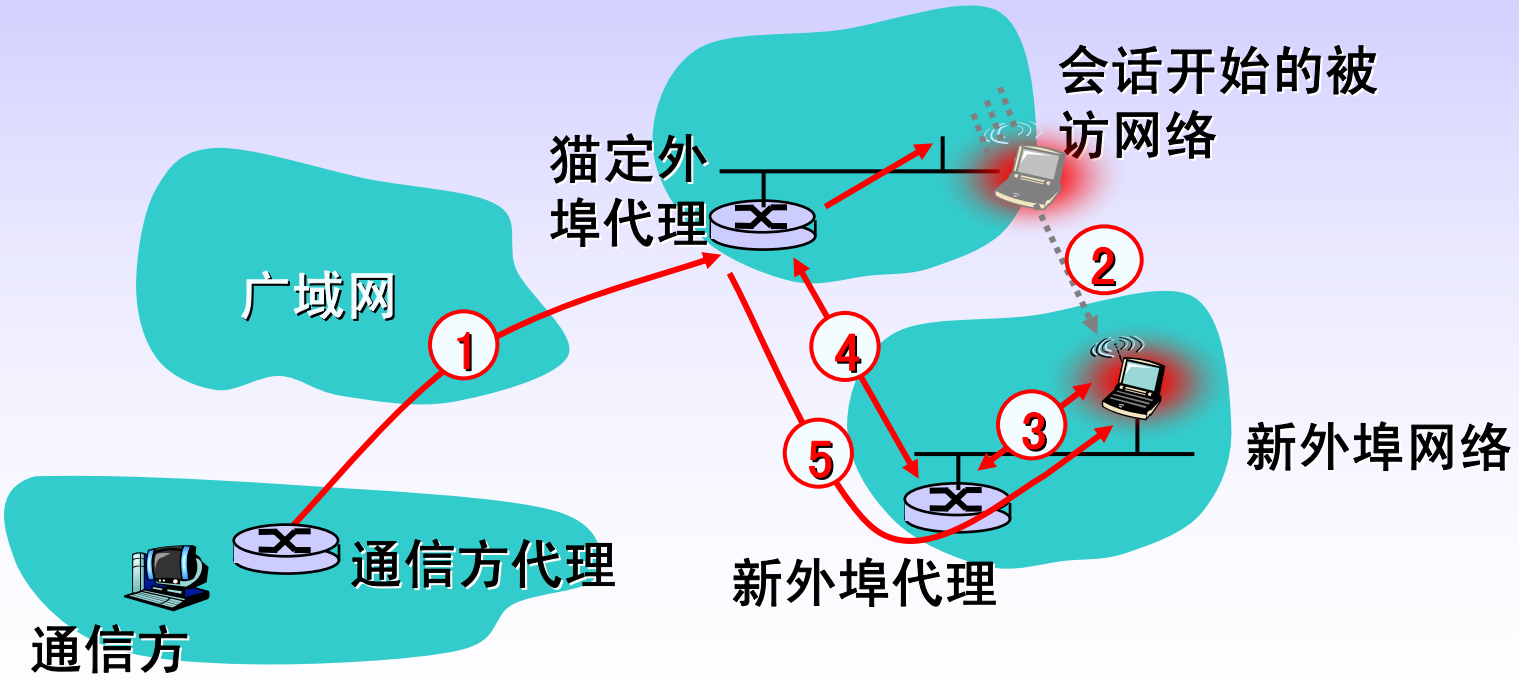
说明

- 克服了三角路由
- **对通信方不透明**
  - 通信方必须由家乡代理才能得到转交地址
  - 若移动机改变被访网络?



适应移动的直接路由

- 猫定外埠代理：首次被访网络的FA
- 数据总是首先路由到猫定FA
- 当节点再移动时：新 FA 让老FA 转发数据 （FA链）



3.5 移动 IP

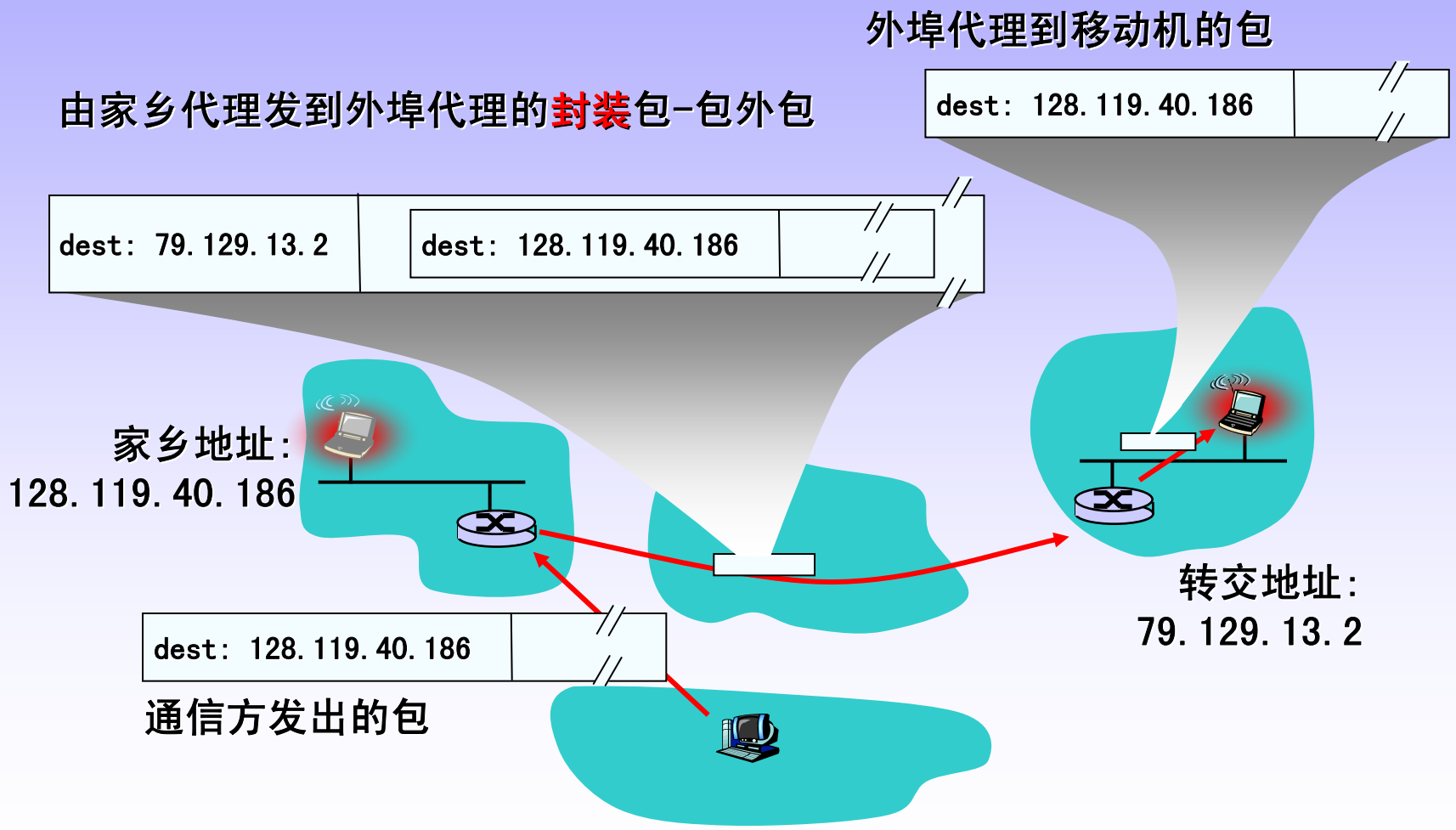
3.5.1 移动IP的特点与基本要素

- 移动IP（RFC 3344）：
  - 允许移动机从一个无线IP子网漫游到另一个子网时，**不重建立连接**而透明地收发IP数据包。**链路层改变，但IP层连接不变**！
- 区别：
  - 固定IP连接：IP地址和TCP端口号必须不变
  - 移动IP连接：**IP地址会变化**
- 基本特点：
  - 引入**蜂窝移动通信**机制
  - 家乡代理、外埠代理、外埠代理注册，转交地址，隧道封装
- 三个基本要素
  - 数据报间接路由
  - 代理发现
  - 注册家乡代理

Wireless网络漫游（Roaming）

- Wireless漫游概念
  - STA可在属于同一个ESS的AP接入点接入
  - STA可在Wireless网络中任意移动，同时保证已有业务不中断，用户标识（IP地址）不改变
- Wireless漫游分类
  - 二层漫游
    - 在同一个子网内的AP间漫游
    - 不涉及子网变化，只需保证用户在AP间切换时访问网络的权限不变即可。
  - 三层漫游
    - 在不同子网内的AP间漫游（连接不变）

3.5.2 IP移动过程
——间接路由



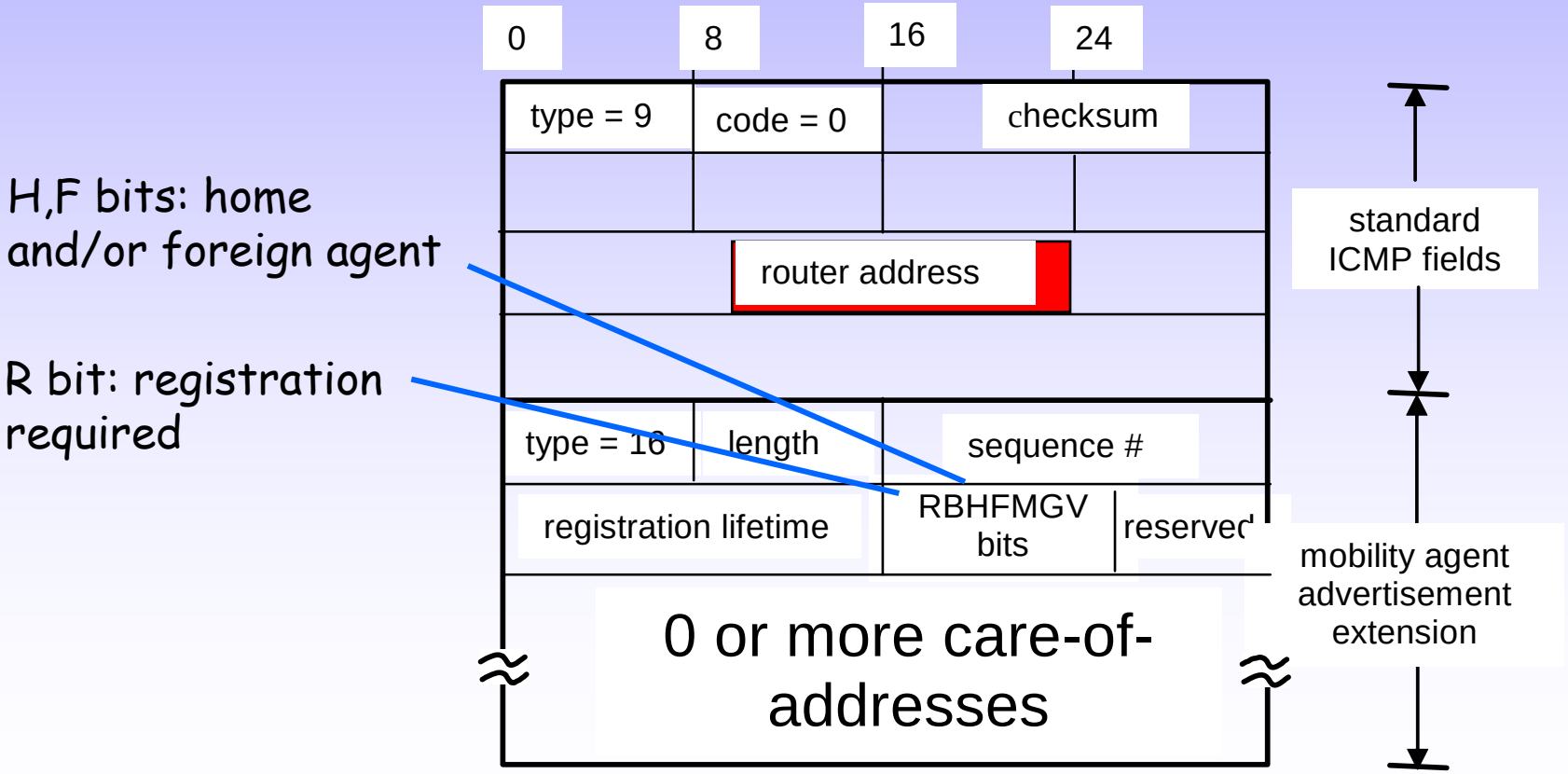
代理发现与注册

- **代理发现**机制
  - 移动机广播/多播其ICMP**请求**信息：求其所在网络路由器的IP地址？
  - 或路由器周期性在其本地链路上广播其路由器**通告**信息（服务信息）
- **注册登记**机制
  - 必须在一定的注册时间内完成
  - 在本地代理生成或修改一个移动性捆绑，使其家乡地址与当前转交地址发生关联。
  - 当移动节点回到本地网络时，也可用注册信息来更新移动性捆绑以终止或注销外地代理。
  - **两种途径**完成注册：
    - 通过外地代理向本地代理转交注册信息；
    - 另一种是直接向本地代理注册。
  - 根据下面情形选择确定：

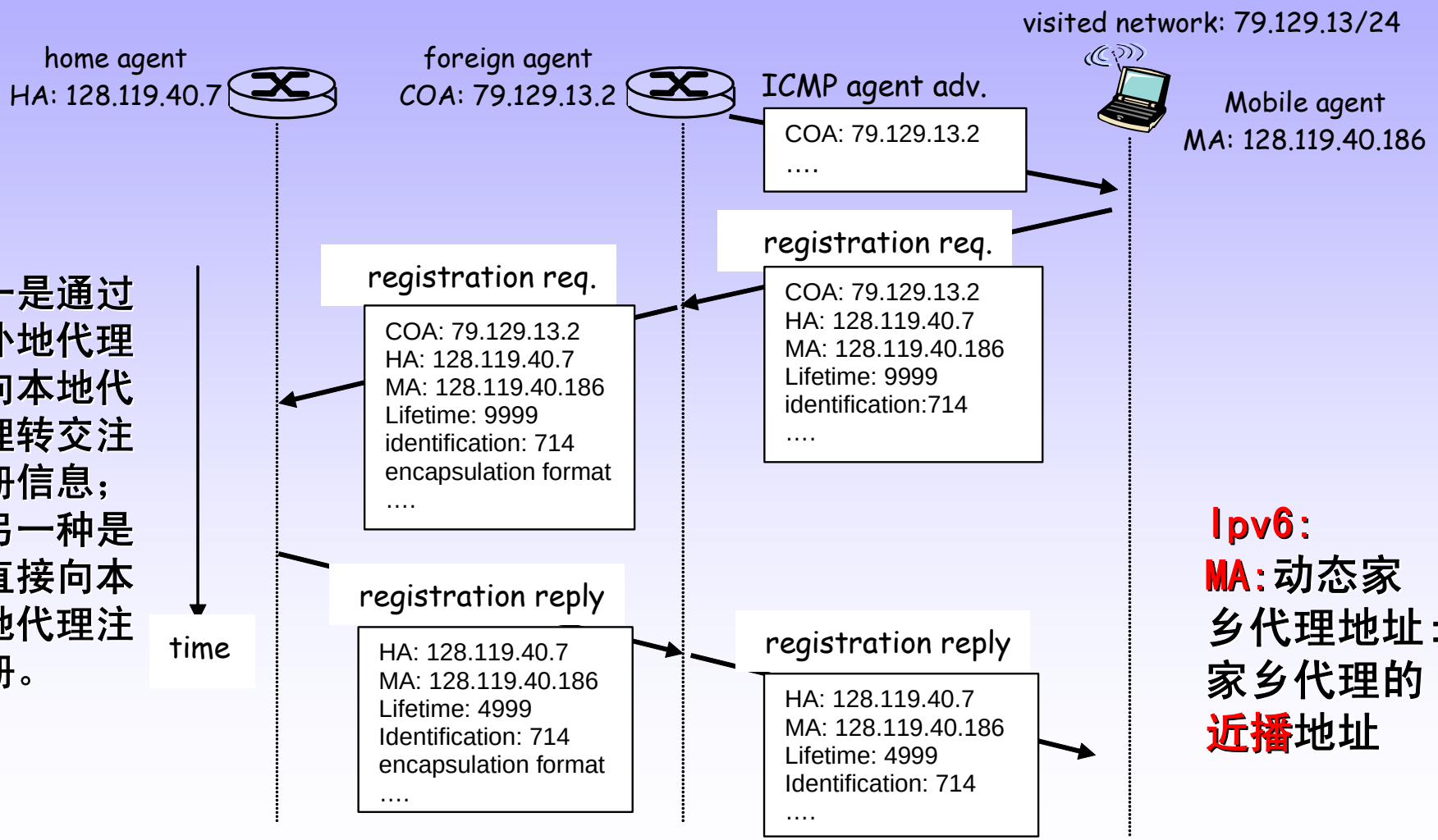
    1．如果移动节点使用了外地代理的转交地址，则必须通过外地代理注册；
    2．移动代理在其广告信息指定了经由外地代理时要通过外地代理注册；
    3．移动节点返回本地网络时，必须直接访问本地代理的注册表；
    4．只获得外地代理的协同定位转交地址，则直接向本地代理发注册信息

移动 IP：代理发现

- **代理通告（UDP报文）**
  - 外埠/家乡 代理通过广播ICMP 消息 (typefield = 9)发布其服务



移动IP：注册登记一例



一是通过外地代理向本地代理转交注册信息；另一种是直接向本地代理注册。

Ipv6:
MA:动态家乡代理地址：家乡代理的近播地址

无线移动对高层协议的影响

- 逻辑上影响很小 …
  - 尽力服务模式仍未改变
  - TCP/ UDP仍能在无线、移动上运行
- 性能？
  - 丢包/延迟：链路层重传引起的比特错和转交
  - TCP 把丢包解释为拥塞，将不必要减少拥塞窗口
  - 延迟影响实时流量
  - 受限的无线带宽

3.6 无线与移动网络的管理

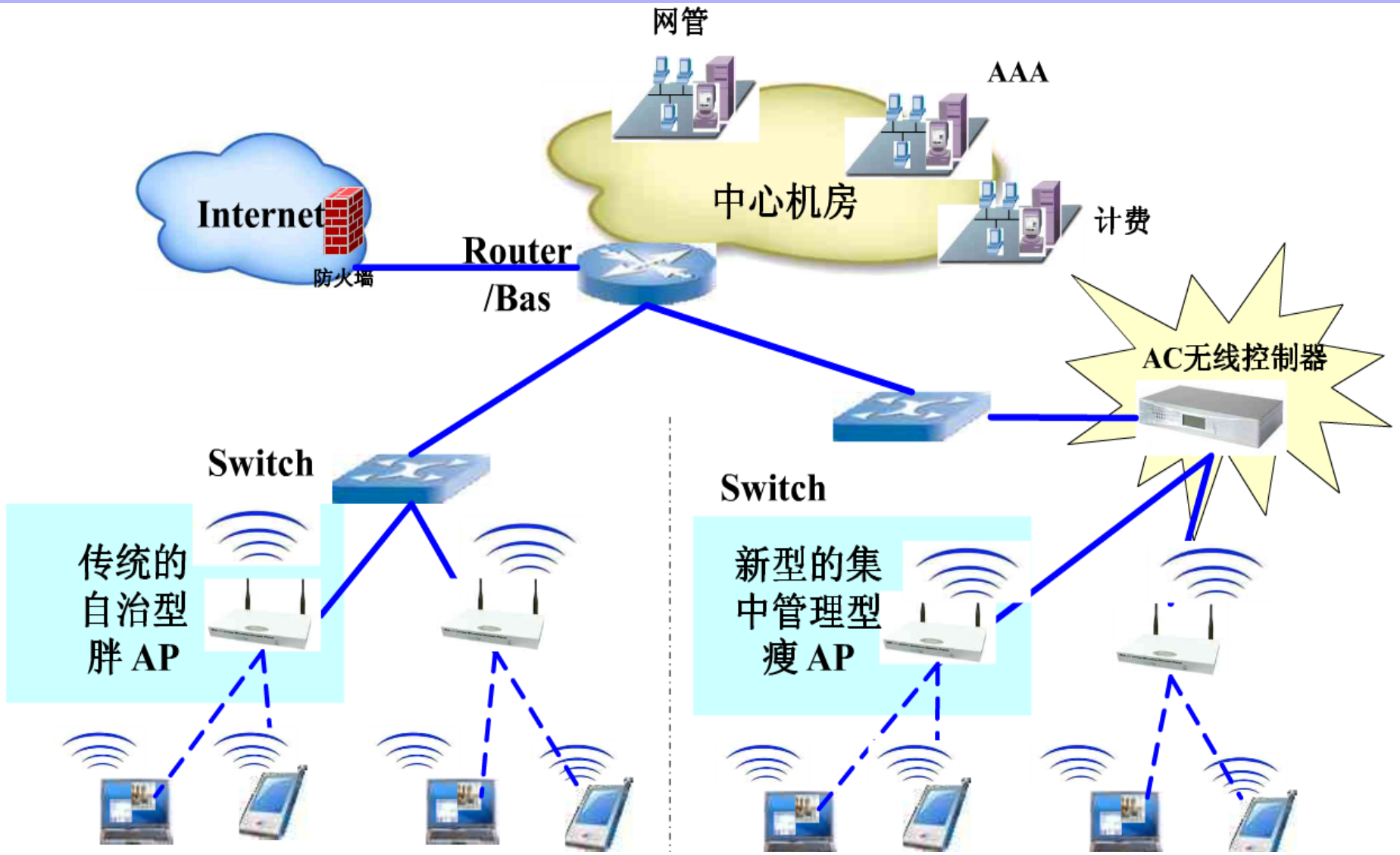
3.6.1 无线网络的部署方式

- 胖/瘦AP的比较

3.6.2 瘦AP会话建立过程

3.6.3 无线网的设置与管理

3.6.1 两种部署方式


网管
AAA
Internet
中心机房
计费
防火墙
Router
/Bas
AC无线控制器
Switch
Switch
传统的
自治型
胖 AP
新型的集
中管理型
瘦 AP

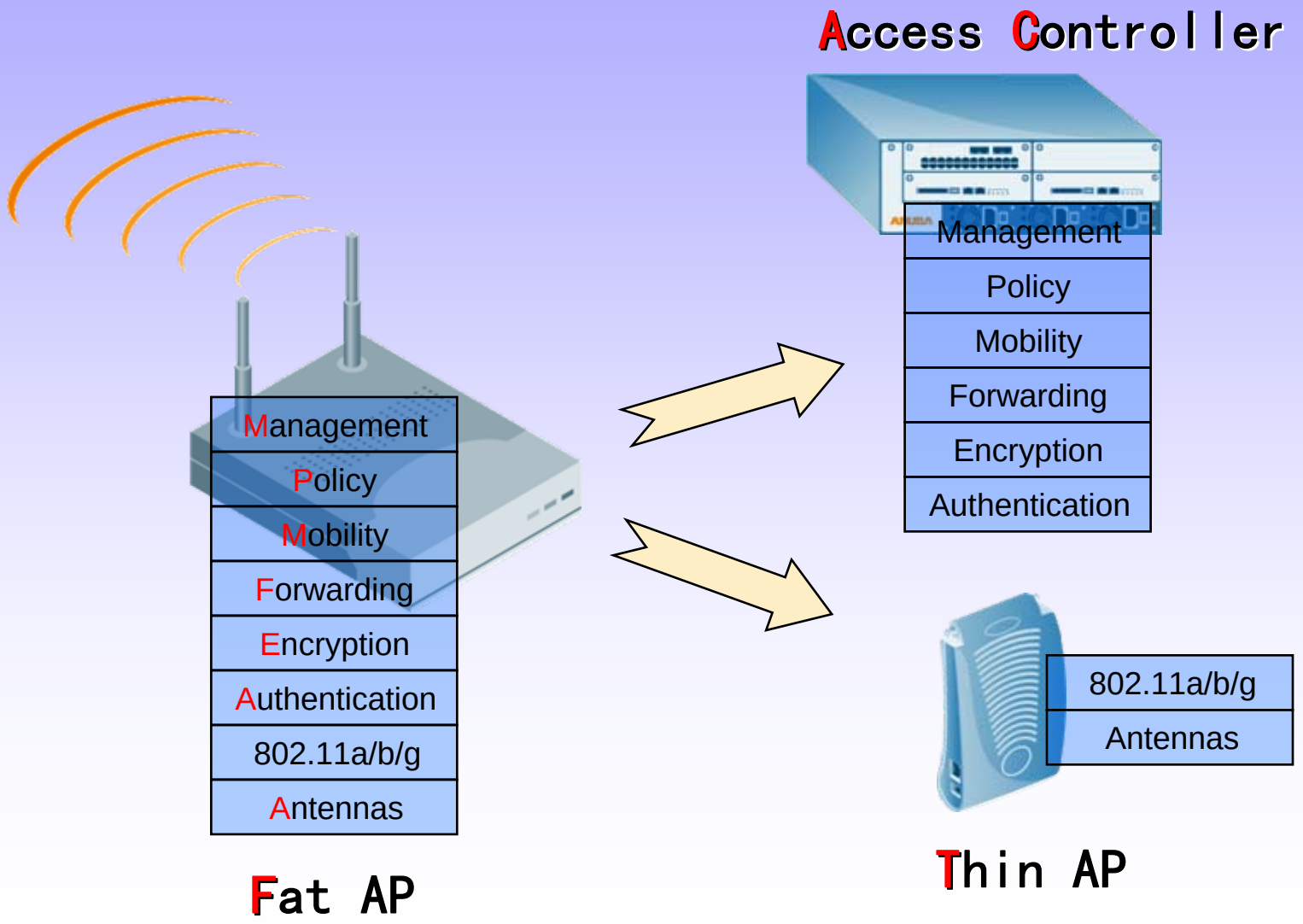
胖/瘦AP的含义

- 胖AP
  - 自主AP，每个AP具备独立功能
- 瘦AP
  - 非自主AP，只具有基本接入功能，大部分管理功能集中到其管理器（AC）上
- 区别：自主性/功能
  - 大规模AP部署：瘦AP方案比胖AP更好管理；
  - 瘦AP的设计思想是Plug and Play，自动得到配置，能够非常方便的集中管理

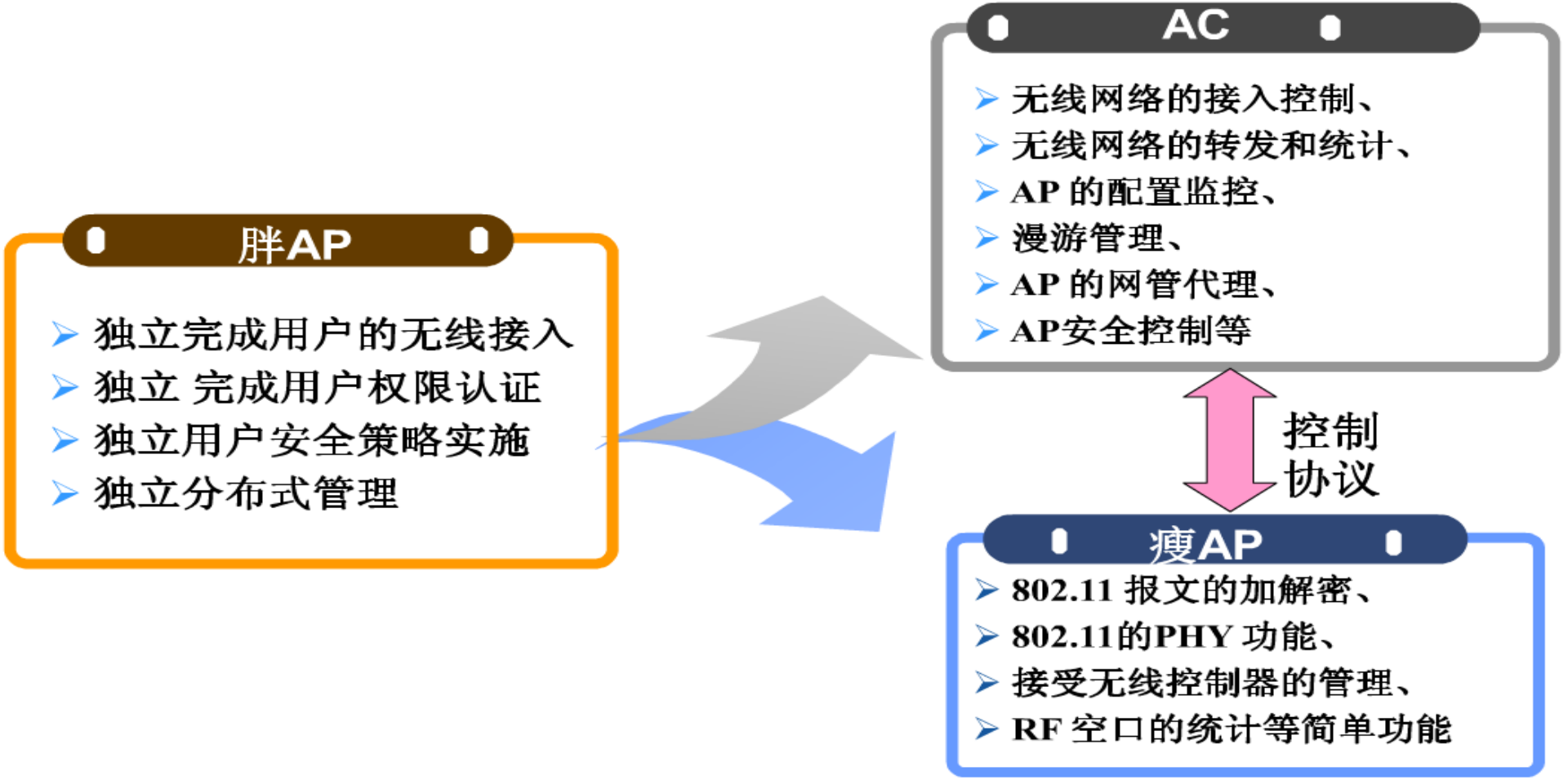
传统胖AP

- 视为**边界接入**技术
  - 无线终端用户和有线网络之间的桥接，有线的补充
- 网络无线部分 = 以AP为中心的**一片片覆盖区域**组合
  - 各**区域独立**工作
  - 以AP为中心承担数据接收、转发、过滤、加密，客户端接入、断开、认证等诸多任务
- 接入控制
  - 其控制策略及用户信息都**局限单个AP上**
  - 一旦用户**切换AP**，新接入AP需要**重新认证**和策略控制
- 缺点
  - 需要对每个AP进行**个别设置**和**策略控制**
  - 不适应大规模部署，**缺乏**整体性联系
  - VLAN**划分困难**，无法针对无线用户**移动性整体**考虑规则
  - **缺乏**对**漫游**的支持
  - 难以融合进现有有线网络、**网管**和**接入管理**

胖AP？瘦AP？


Access Controller
Management
Policy
Mobility
Forwarding
Encryption
Authentication
Management
Policy
Mobility
Forwarding
Encryption
Authentication
802.11a/b/g
Antennas
Fat AP
Thin AP

胖AP向瘦AP的转化



传统的WLAN 的AP功能被分散到AC和瘦AP两个独立的设备来完成，AC和瘦AP之间提供相应的控制协议完成无线功能。

使用瘦AP结构的优点

- 管理**简单**，设置**快速**
  - 完全由控制器设置，不需对每个AP设置。
  - 控制器可列出目前**所有AP状态**及其用户
- 安全性提高
  - 所有**加解密**文档由AC处理。
- 建设速度快
  - 能快速建立无线环境，不需改变有线网络设置。
- 效能比一般FAT-AP好
  - 仅把数据**转发给控制器**，不做**加解密**动作。

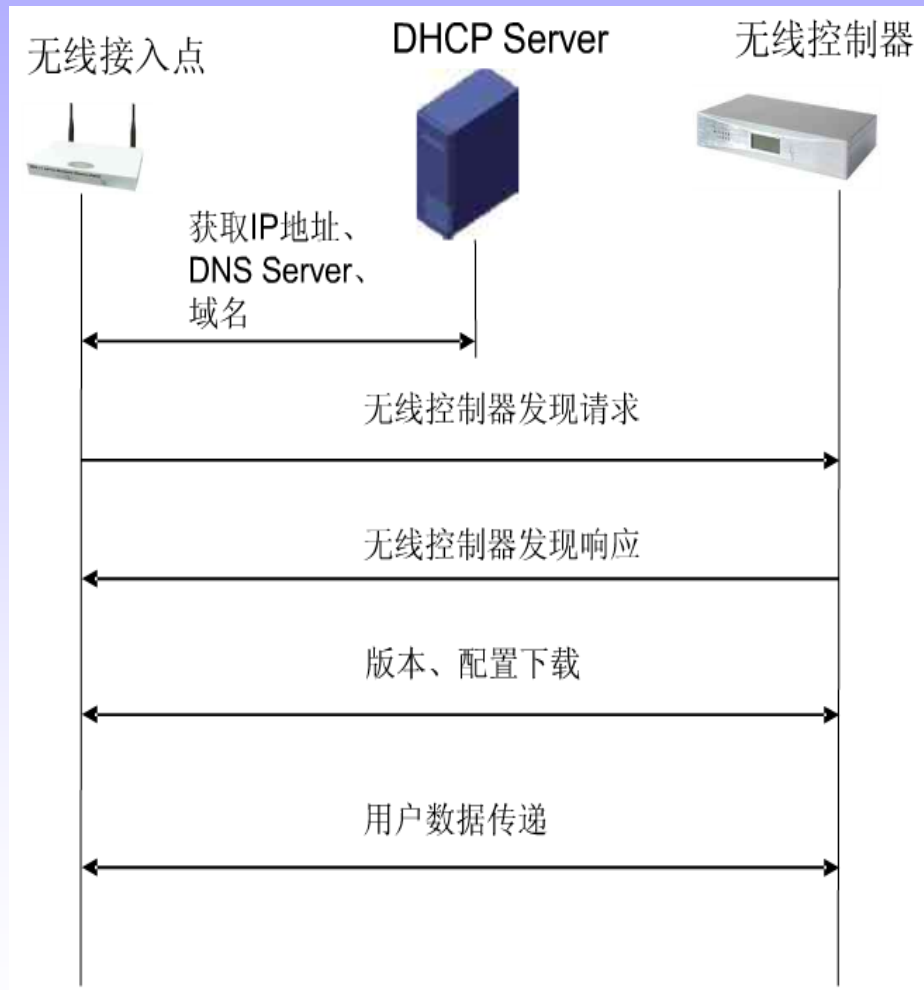
- 抗干扰性强
  - 主备双天线加大信号发射和接受效率，适应复杂环境
- 稳定性
  - 在802.11a和802.11g上/下行传输速率可达30Mbps以上
- 支持无缝切换
  - 独立AP的路由切换时间40S左右
  - 瘦AP切换时间可以达到8-9mS
- 安装简便统一配置
  - 下载软件激活程序
  - 远程配置
- 软件统一管理
  - 方便故障点查询单点AP损坏
  - 自动发现故障点，调节周边AP发射功率至将损坏AP范围覆盖为止
- 适合大规模部署

胖瘦AP组网的选择

- 胖AP
  - 独立设备智能化、自治型组网
  - 产品和组网成熟度高
  - 整网分布部署、可靠性高
  - 初期投资低
  - 适用于规模不大、AP间关联程度低、初期投资有限的场合
- AC+瘦AP
  - 轻型AP设备、非智能化、操作简单
  - 集中管理、便于维护和管理
  - 更高安全可控性
  - 无缝漫游
  - 适用大规模密集部署、对控制要求高、有音视频漫游的场合

3.6.2 瘦AP会话建立过程

1. AP接入交换机端口，获得IP地址（DHCP或静态配置）
2. AP查找AC地址（DHCP/DNS/静设）
3. AP从AC下载image文件（TFTP），建立隧道连接到AC
4. AP认证后建立AP到交换机之间的隧道连接
5. AP从AC下载相应的配置文件完成自身配置
6. 终端用户与AP通信，AP将数据通过隧道传送到AC，由AC集中转发/也可设置成AP本地转发
7. AC集中管理所有AP



瘦AP可自动发现AC/完成更新和配置，实现即插即用

管理功能之一：用户接入

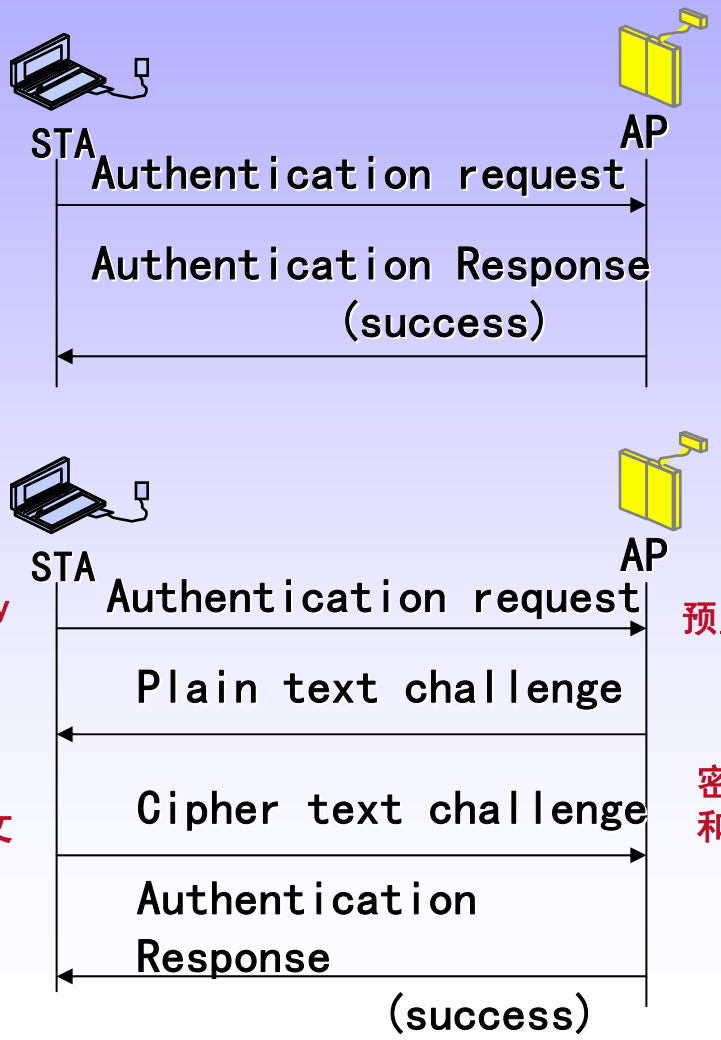

STA
AP
Discovery选择AP
（采用侦听Beacon帧或发送Probe帧）
Authentication
Association
和建立Association关系的AP收发数据

管理功能之二： AP的发现

- 802.11 MAC 使用Scanning功能来完成Discovery
  - 寻找和加入一个网络
  - 当STA漫游时寻找一个新AP
- Passive Scanning
  - 被动侦听AP定期发送Beacon帧来发现网络， Beacon帧中包含该AP所属BSS基本信息以及AP基本能力级，包括： BSSID（AP的MAC地址）、 SSID、支持的速率、支持的认证方式，加密算法、Beacons帧发送间隔，使用的信道等
  - 当未发现包含期望的SSID的BSS时，STA可以工作于IBSS状态
- Active Scanning
  - 主动发送Probe request报文，从Probe Response中获取BSS的基本信息， Probe Response包含信息和Beacon帧类似

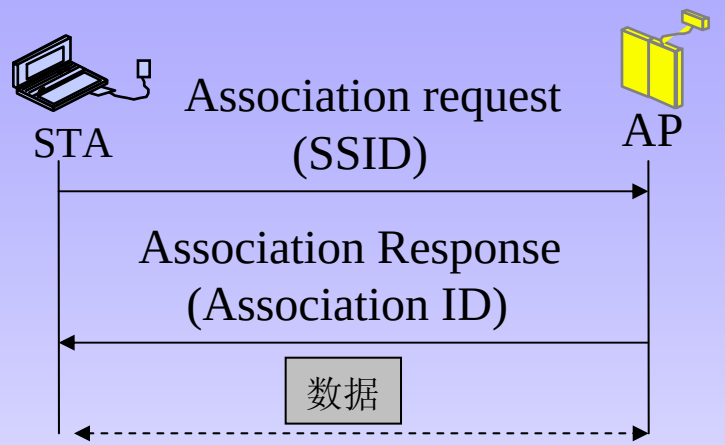
管理功能之三：两种基本认证方式

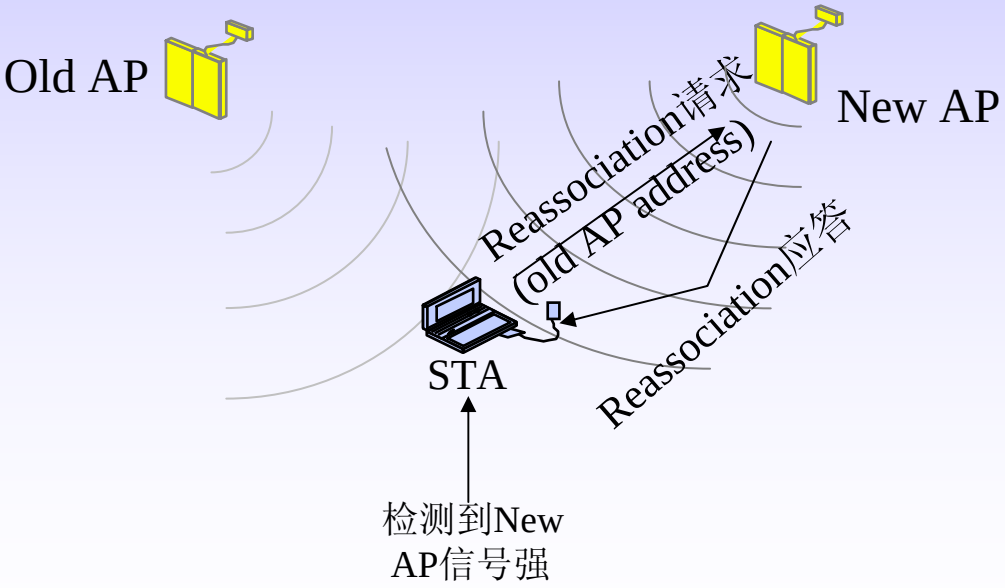
- Open-system Authentication
  - 等同于**不需要认证**，没有任何安全防护能力
  - 通过其它方式来保证用户接入网络的**安全性**，例如**Address filter**、用户报文中的**SSID**
- Shared—Key Authentication
  - 采用**WEP**加密算法（已淘汰）
  - Attacker可以通过监听AP发送的**明文**Challenge text和STA回复的**密文**Challenge text计算出**WEP** KEY
- STA可以通过
  - Deauthentication来终结认证



管理功能之四：关联的建立

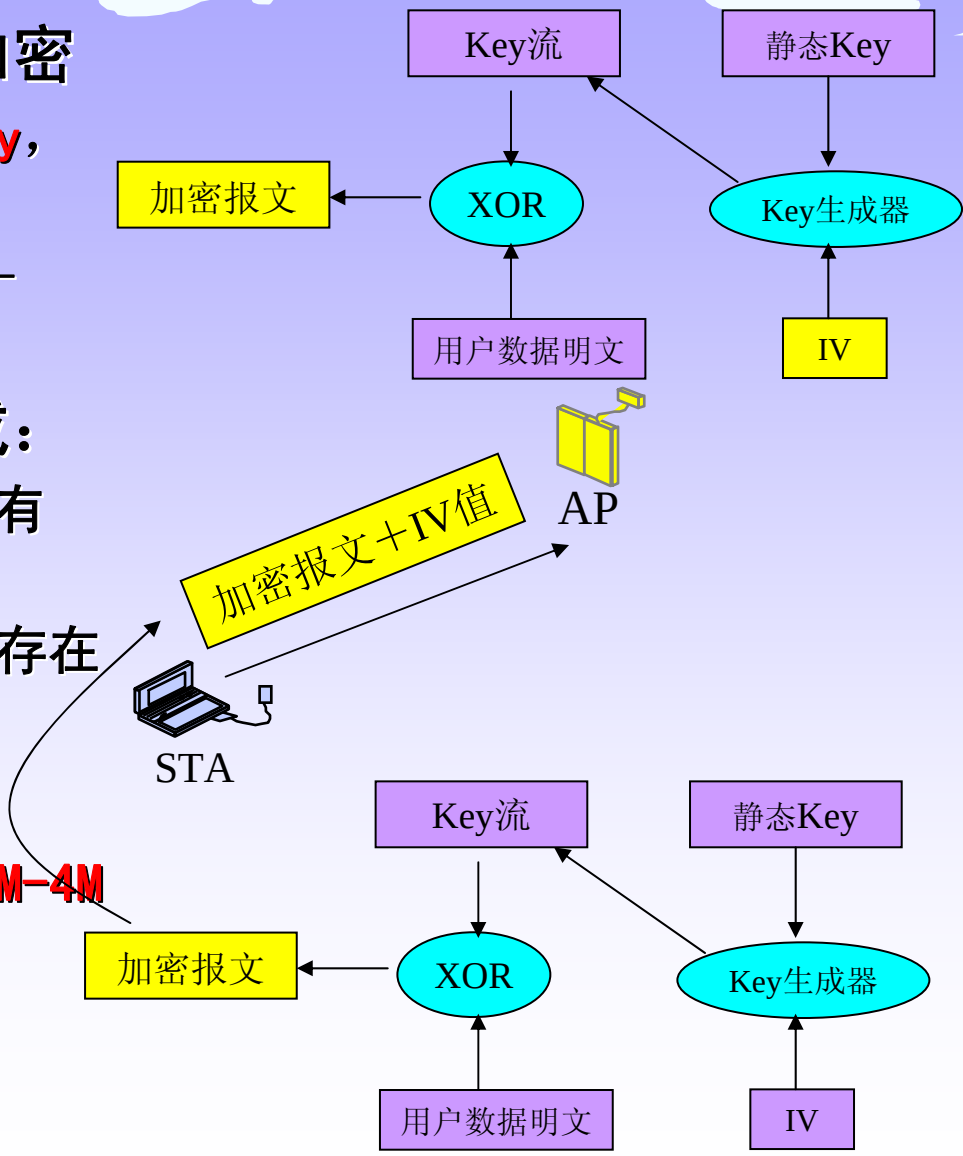
- Association
  - STA通过Association和一个AP绑定，后续的数据报文的收发只能和建立关联AP进行
- Reassociation
  - STA在从一个老AP移动到新AP时，通过Reassociation和新AP再建关联
  - Reassociation前必须经历Authentication过程
- Deassociation
  - STA通过Deassociation和AP解除关联关系





管理功能之五：加密

- RC4对称流加密算法的WEP加密
  - STA和AP**预先配置相同静态Key**，Key长40 bit或104bit
  - 每次数据加密Key＝静态Key＋24bit IV值（动态生成）
- 全STA共用相同静态Key造成：
  - 当STA**丢失**或**离职**时需要对所有STA**重新配置新静态Key**
  - 静态Key**泄漏被发现前**，网络存在安全隐患
- 24位IV值太短造成：
  - Attacker可以在分析侦听到**1M-4M用户报文后破解加密Key**



802.11 协议的主要缺陷和演进

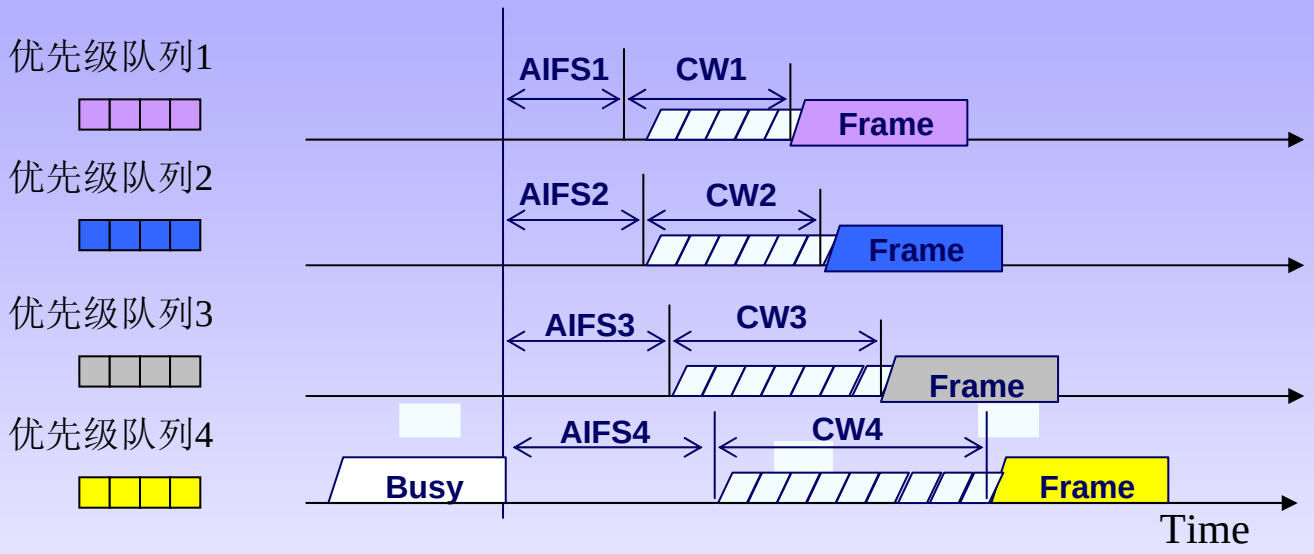
- 严重安全隐患，不适合企业用户
  - 认证体制不完善，认证功能形同虚设
  - 缺乏双向认证手段STA无法识别非法AP
  - 加密Key易被破译，用户数据易被窃听
  - 802.11i解决上述问题
- QOS支持能力差，不适合Voice业务
  - DCF模式：无线空口所有用户平等竞争无线资源
  - 数据报文未划分优先级，AP无法分类处理
  - 802.11e(WMM)解决上述问题

802.11i 协议－安全认证和加密

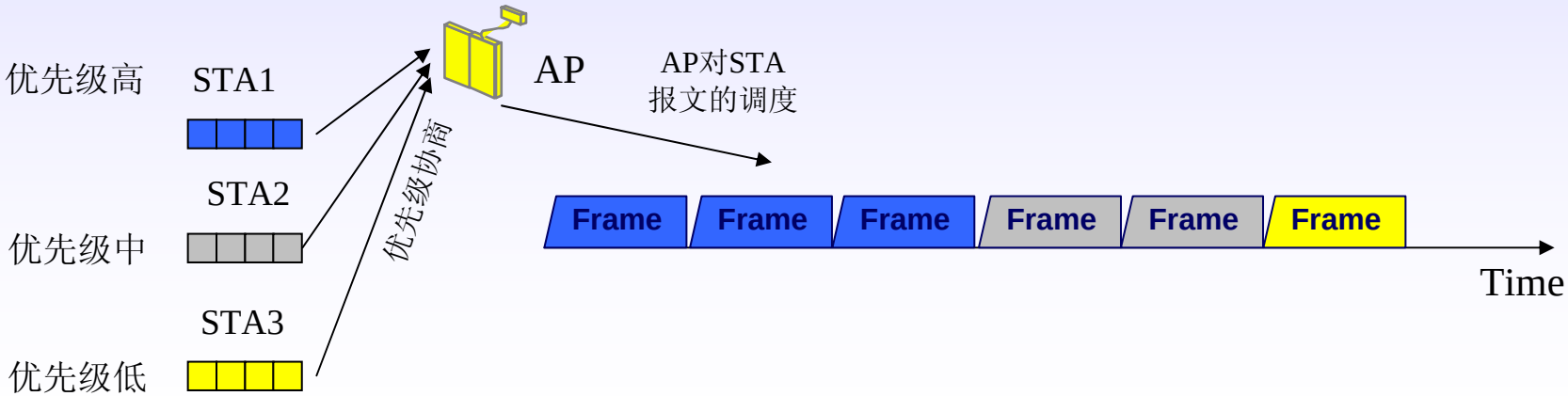
- 引入RSNA (robust security network association)
  - 增强STA和AP认证机制
    - ✓ 支持802.1x，双向认证，有效防止非法AP使用
  - 增加Key生成、管理以及传递机制
    - ✓ 每用户使用独立Key
    - ✓ 非对称密钥算法生成和传递用户数据加密使用Key
  - 增加了两类对称加密算法，加密强度提高
    - ✓ TKIP：核心仍然是RC4算法
    - ✓ CCMP：核心为AES算法

802.11e 协议－QOS保证

•EDCA：增强的分布信道接入调度模式
•根据优先级窗口大小竞争吞吐量



•HCCA：HCF混合协调控制信道接入调度模式
•集中轮询方式接入业务



Thank you!

Questions