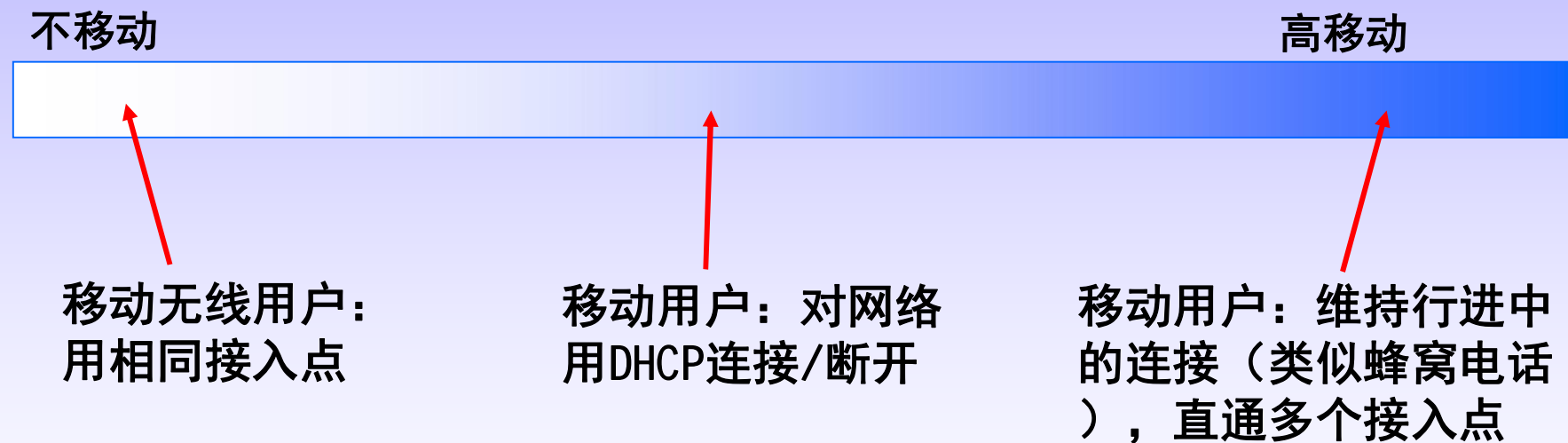


## 3.4 互联网的移动接入

### 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

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

广域网

通信方

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

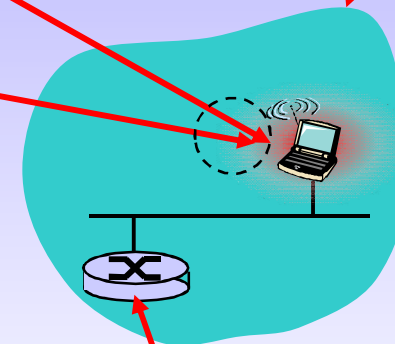
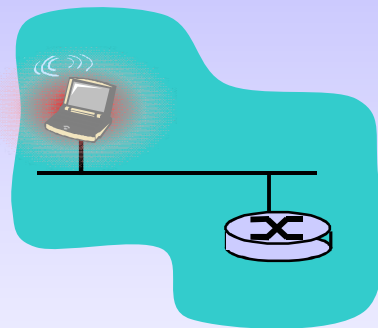
Care-of-address  
visited network  
foreign agent  
correspondent

**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**

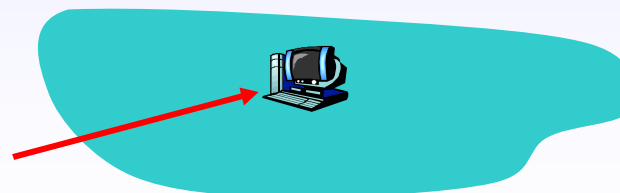
**被访网络:** 移动机当前所  
在网络 (79.129.13/24)

**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？

我想知道 Alice 现在何处？



## 3.4.2 移动寻址与路由

### ◆ 让路由处理:

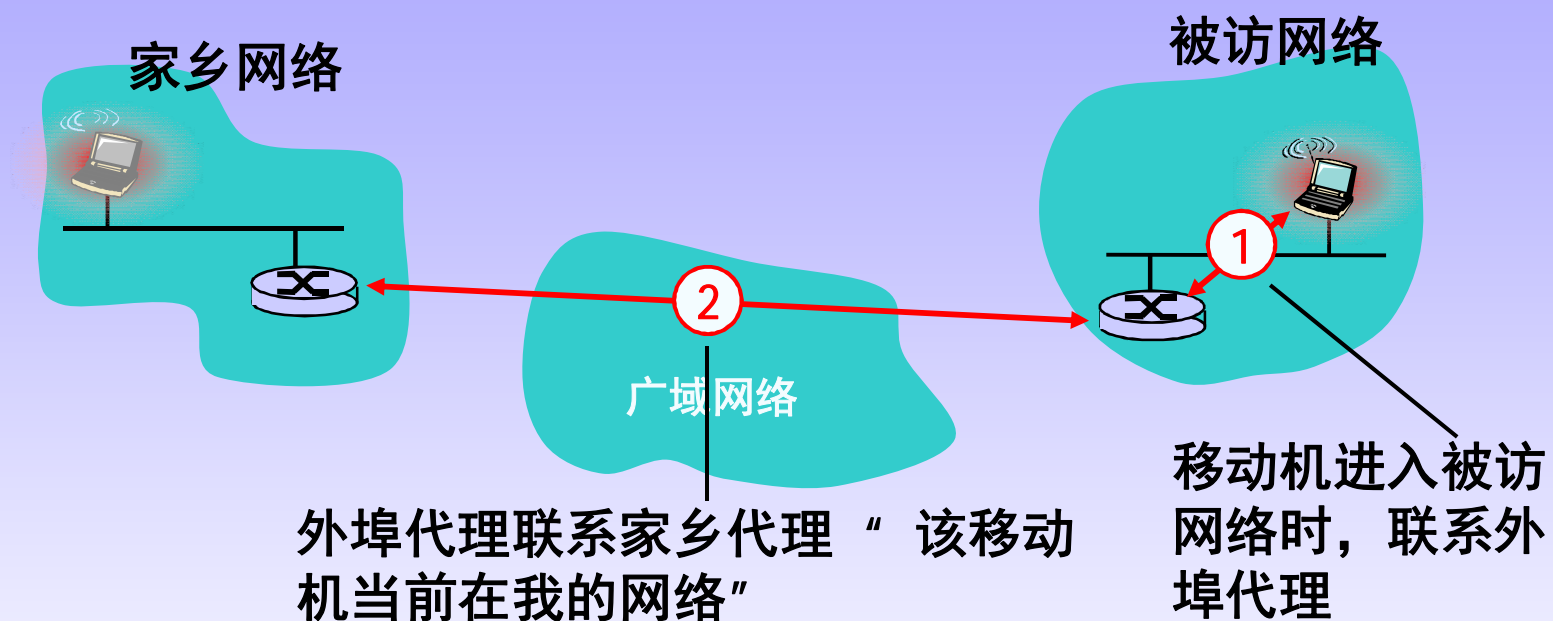
- 路由器由常规路由表交换，通告移动地址
  - ☞ 路由表指明每个定位后的移动体
  - ☞ 对端系统没有改变

不可扩展  
到成千上万的移动地址  
节点

### ◆ 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

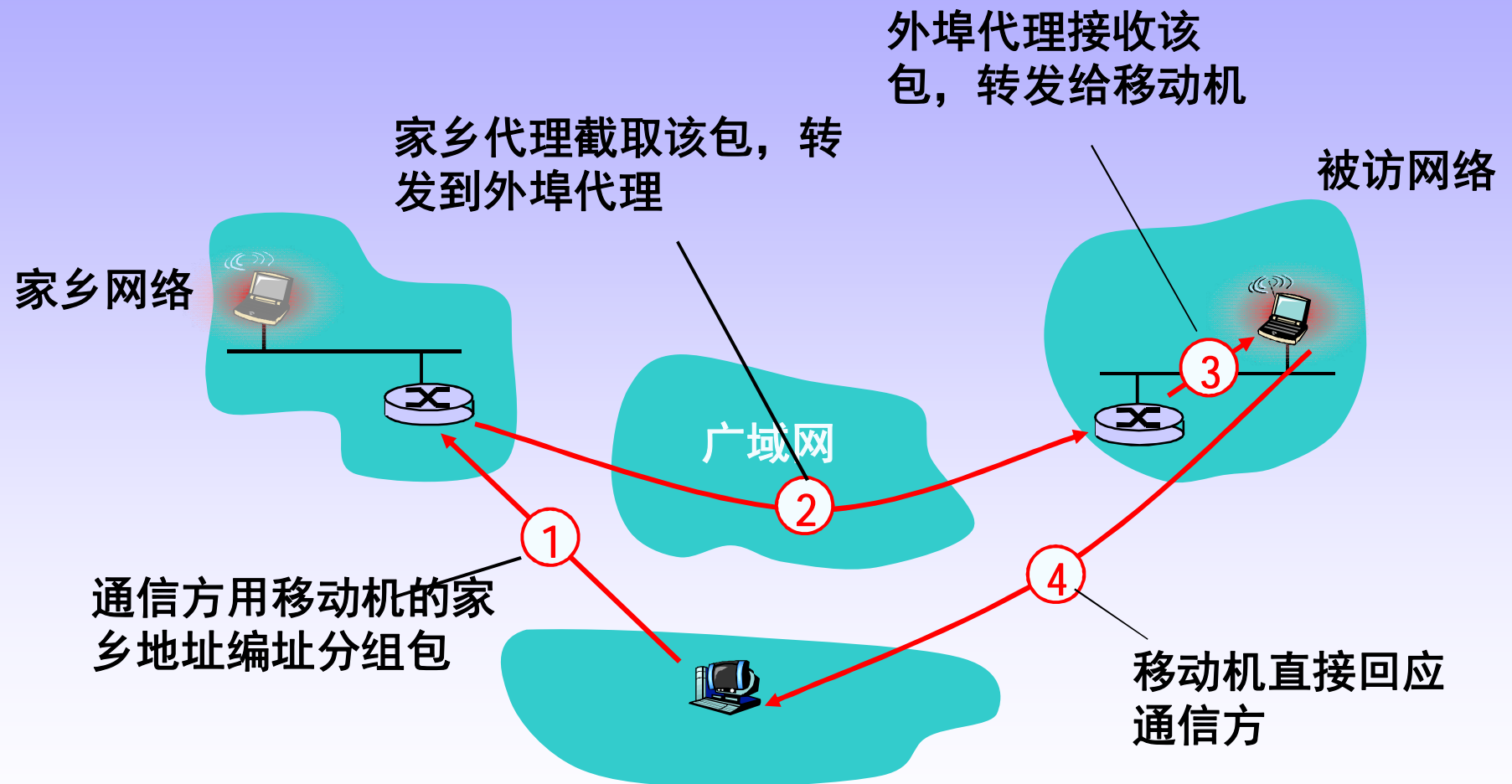
# 注册登记



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



# 说明

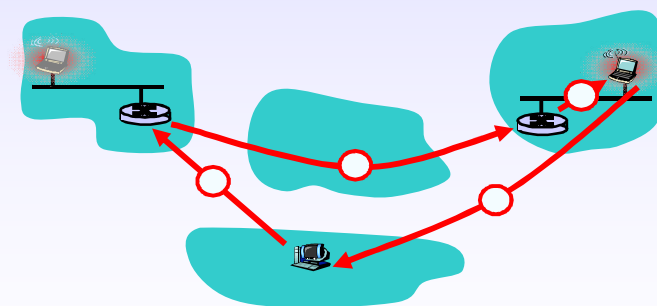
## ◆ 移动机使用两个地址

- **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

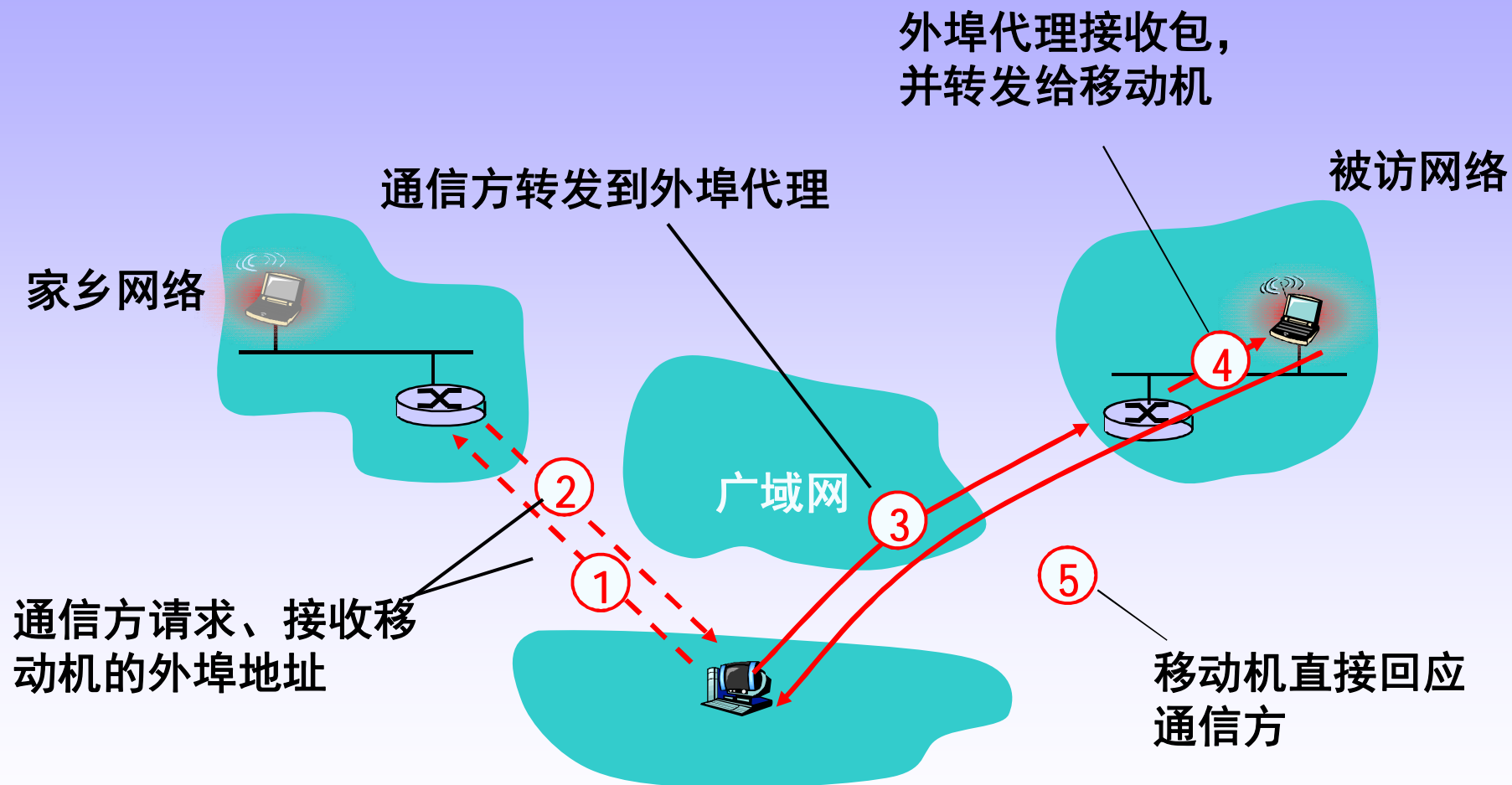




# 间接路由：在网络间移动

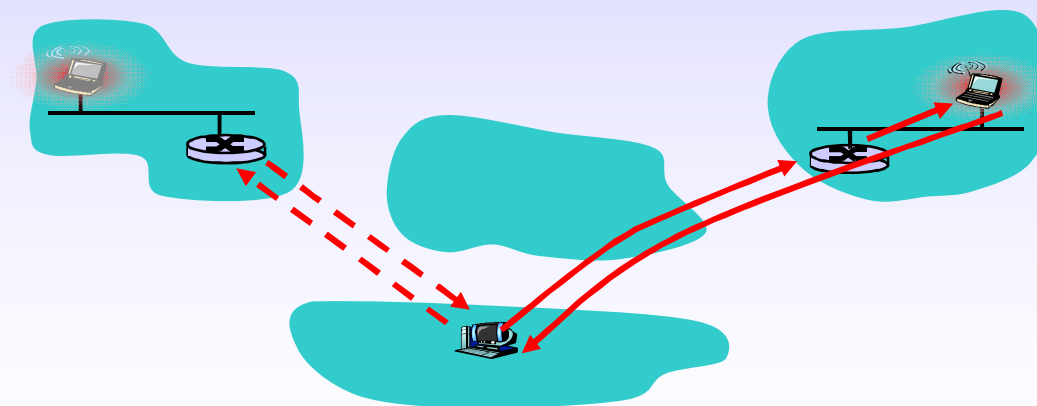
- ◆ 移动用户移动到另一网络
  - 注册到新的外埠代理
  - 新外埠代理注册到其家乡代理
  - 家乡代理更新移动机的转交地址
  - 把包持续转发到移动机（用新的转交地址）
- ◆ 移动，改变外埠网路的透明性： 维持正在进行的连接

# 直接路由移动



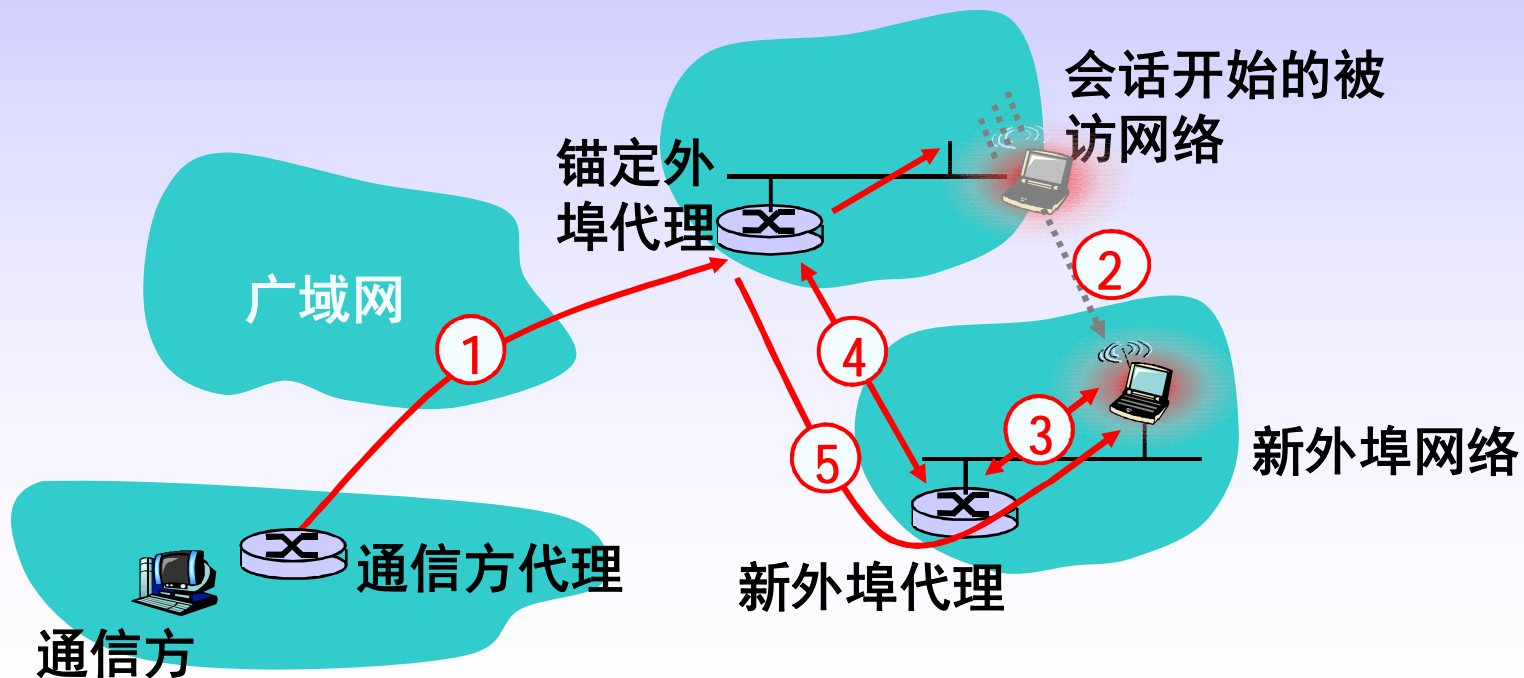
# 说明

- ◆ 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

- ◆ 锚定外埠代理：首次被访网络的FA
- ◆ 数据总是首先路由到锚定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

# Wi rel ess网络漫游 (Roami ng)

## ◆ Wi rel ess漫游概念

- STA可在属于**同一个ESS**的AP接入点接入
- STA可在Wi rel ess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**

## ◆ Wi rel ess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**）

# 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）

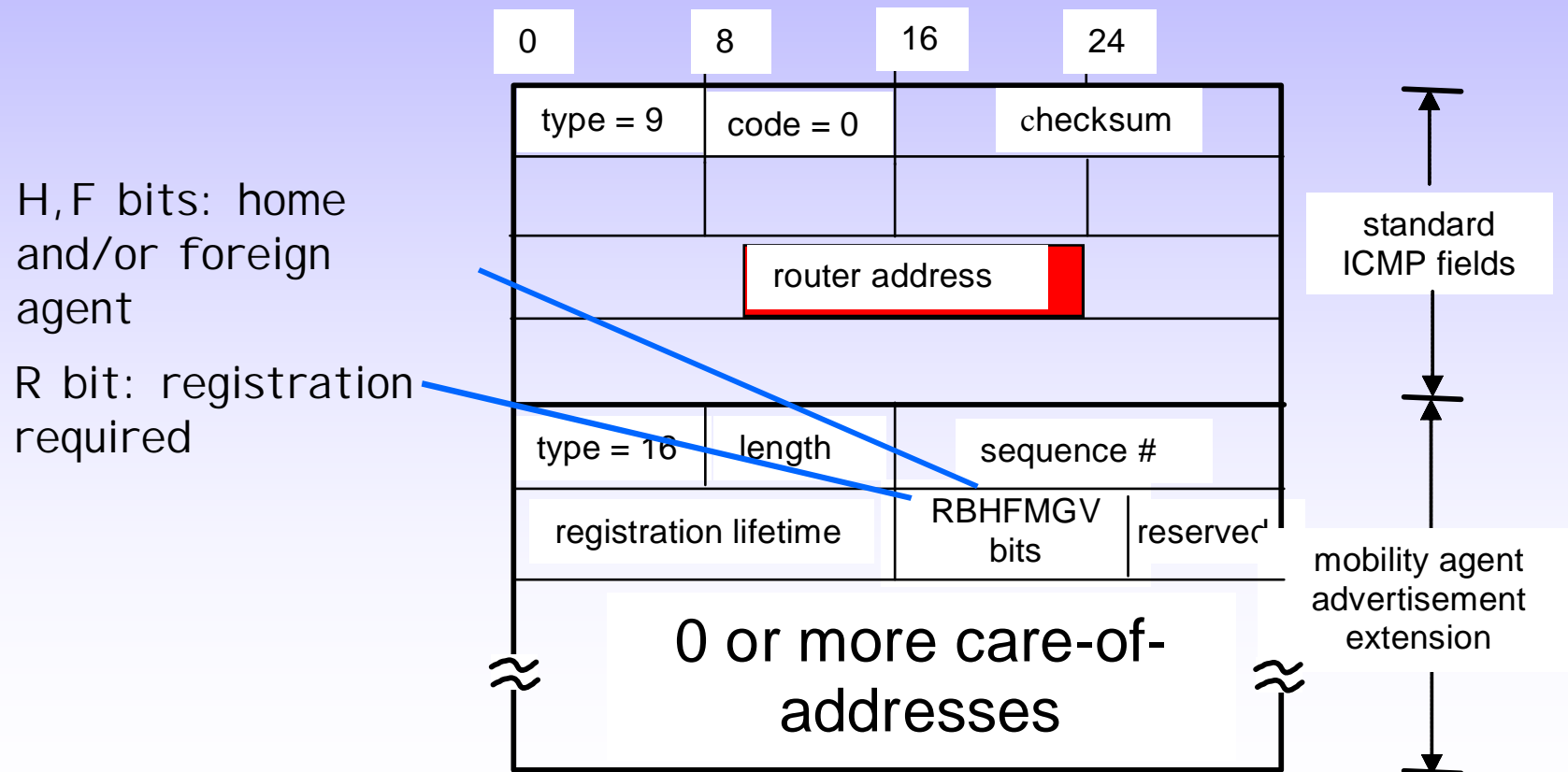
## ◆ 注册登记机制

- 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

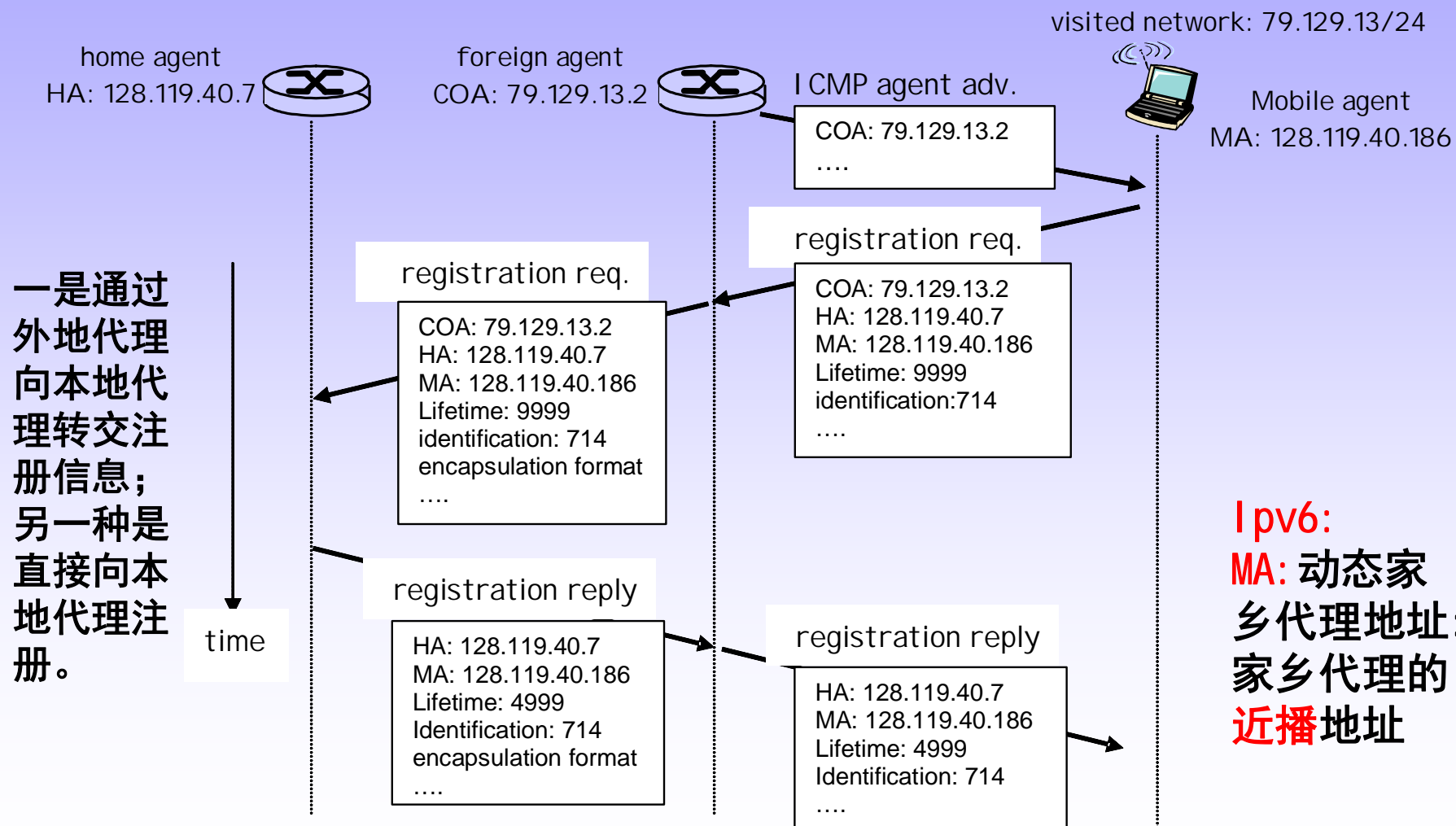
## ◆ 代理通告 (UDP报文)

- 外埠/家乡 代理通过广播ICMP 消息 (type field = 9)发布其服务





# 移动IP: 注册登记一例



# 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

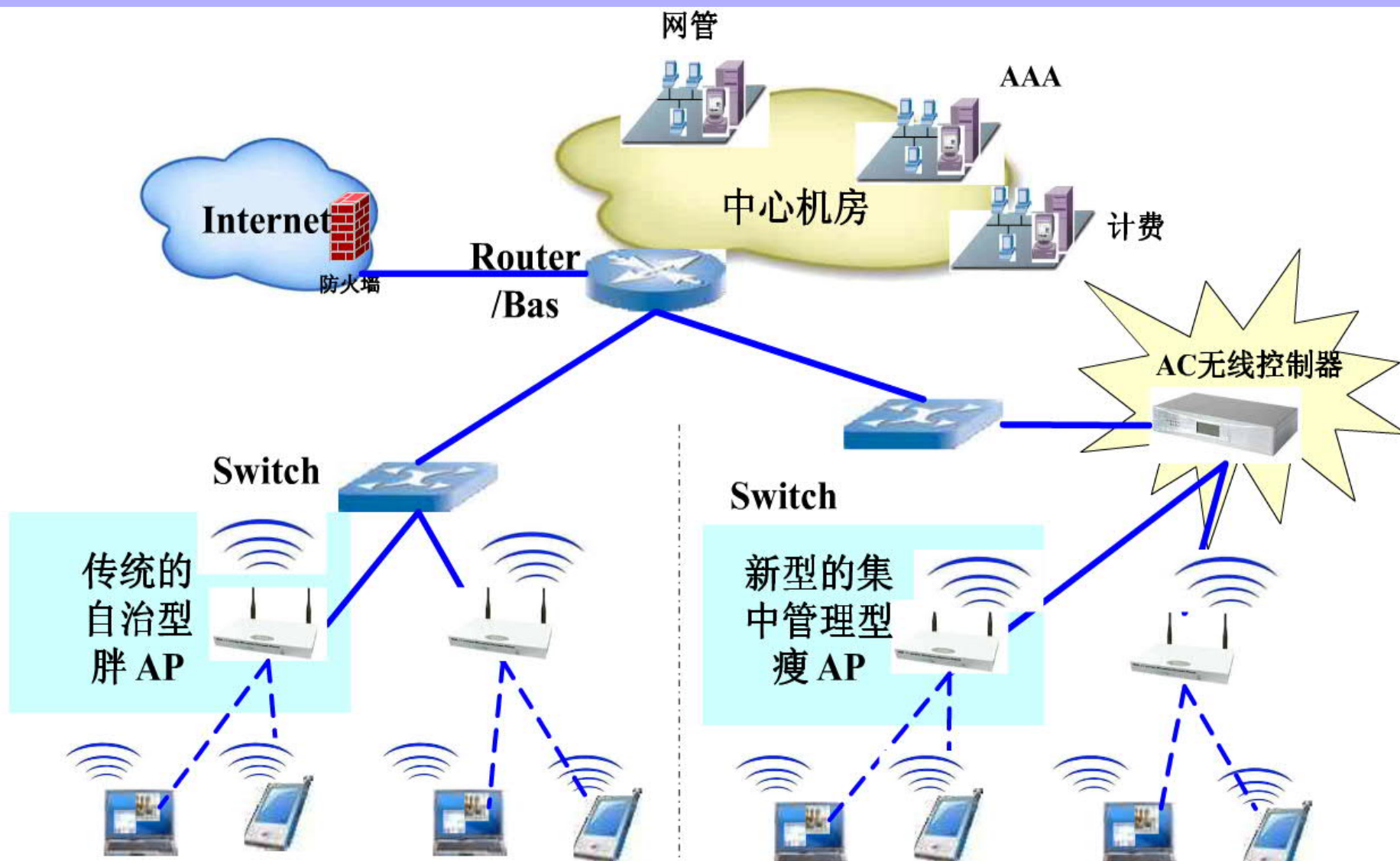
### 3.6.1 无线网络的部署方式

➤ 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



# 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

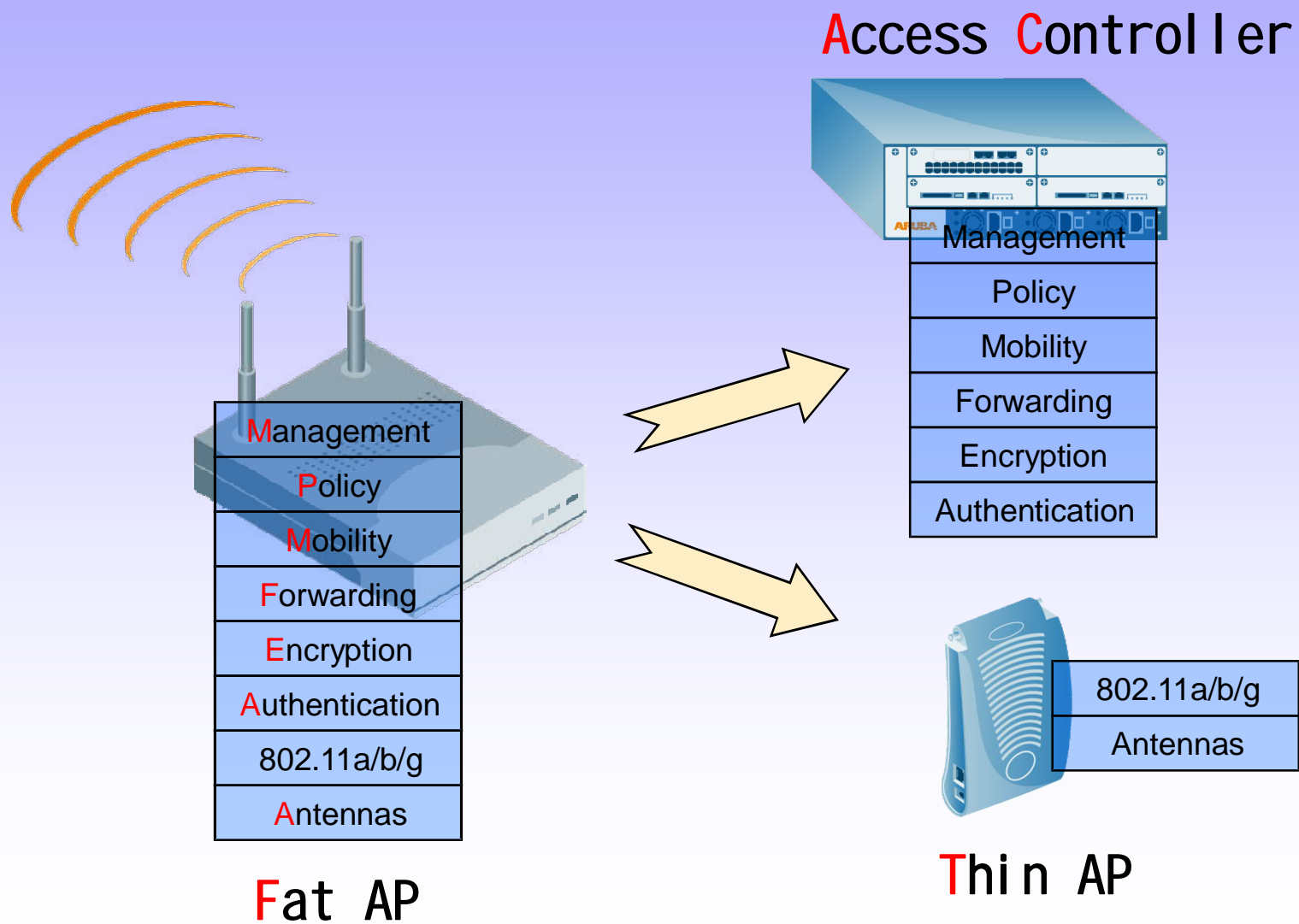
## ◆ 接入控制

- 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

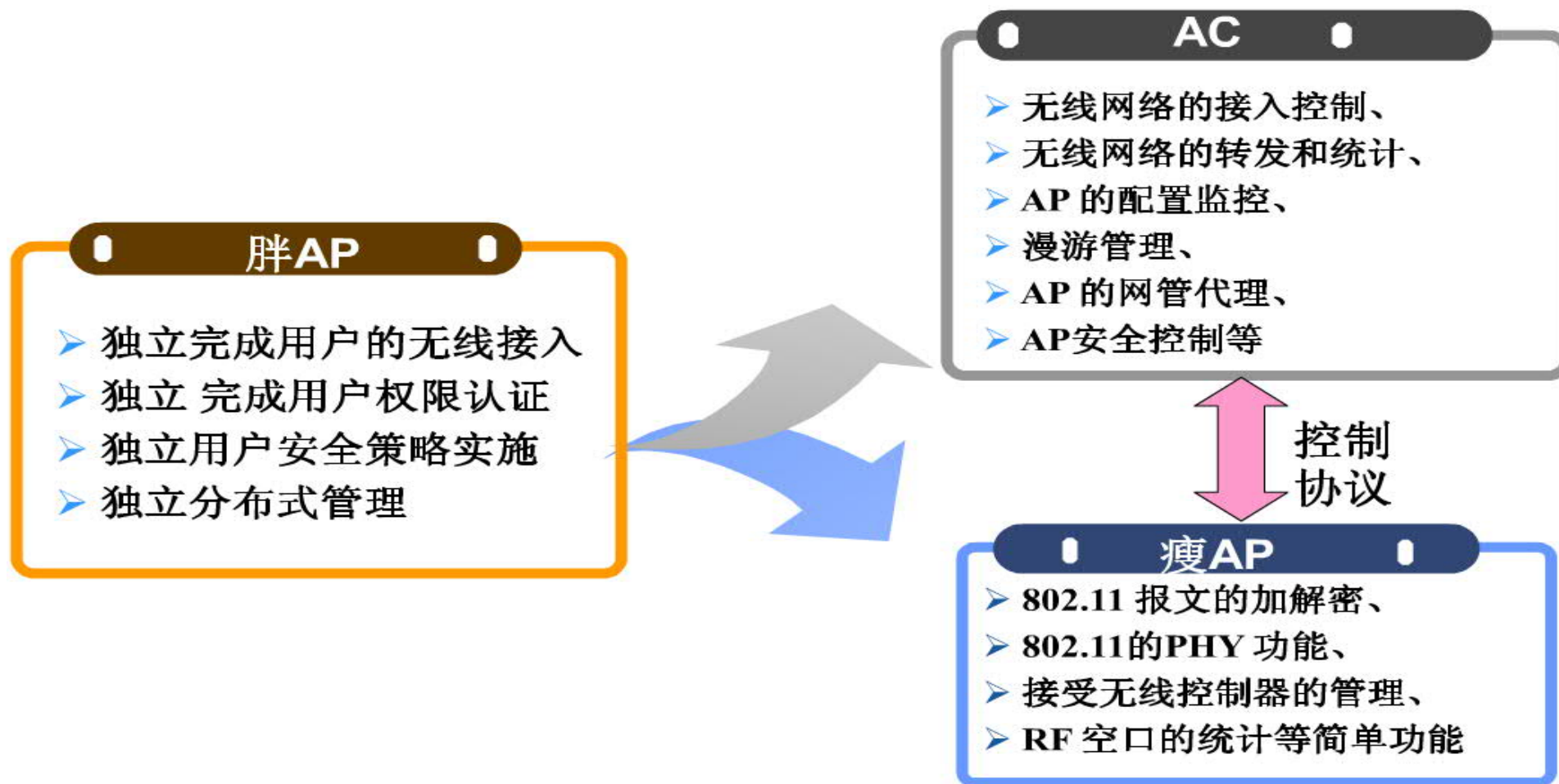
- 需要对每个AP进行个别设置和策略控制
- 不适应大规模部署，缺乏整体性联系
- VLAN划分困难，无法针对无线用户移动性整体考虑规则
- 缺乏对漫游的支持
- 难以融合进现有有线网络、网管和接入管理

# 胖AP? 瘦AP?





# 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

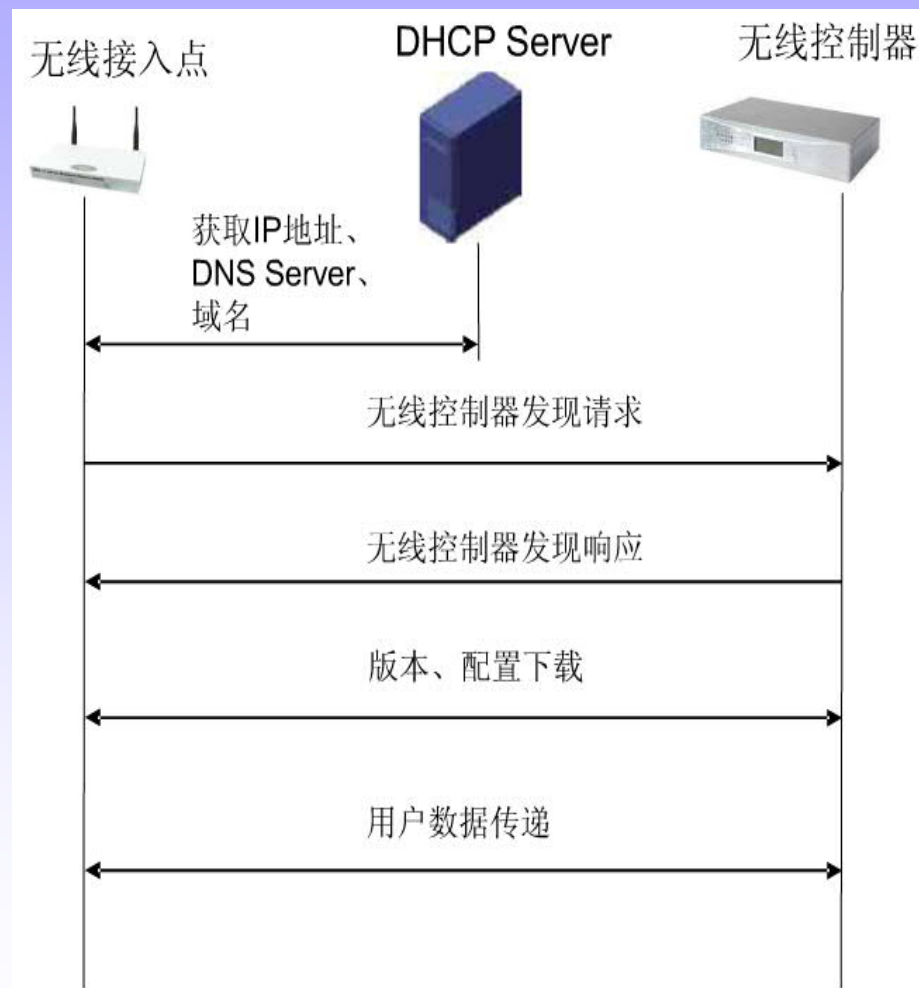
- 独立设备智能化、自治型组网
- 产品和组网成熟度高
- 整网分布部署、可靠性高
- 初期投资低
- 适用于规模不大、AP间关联程度低、初期投资有限的场合

## ◆ AC+瘦AP

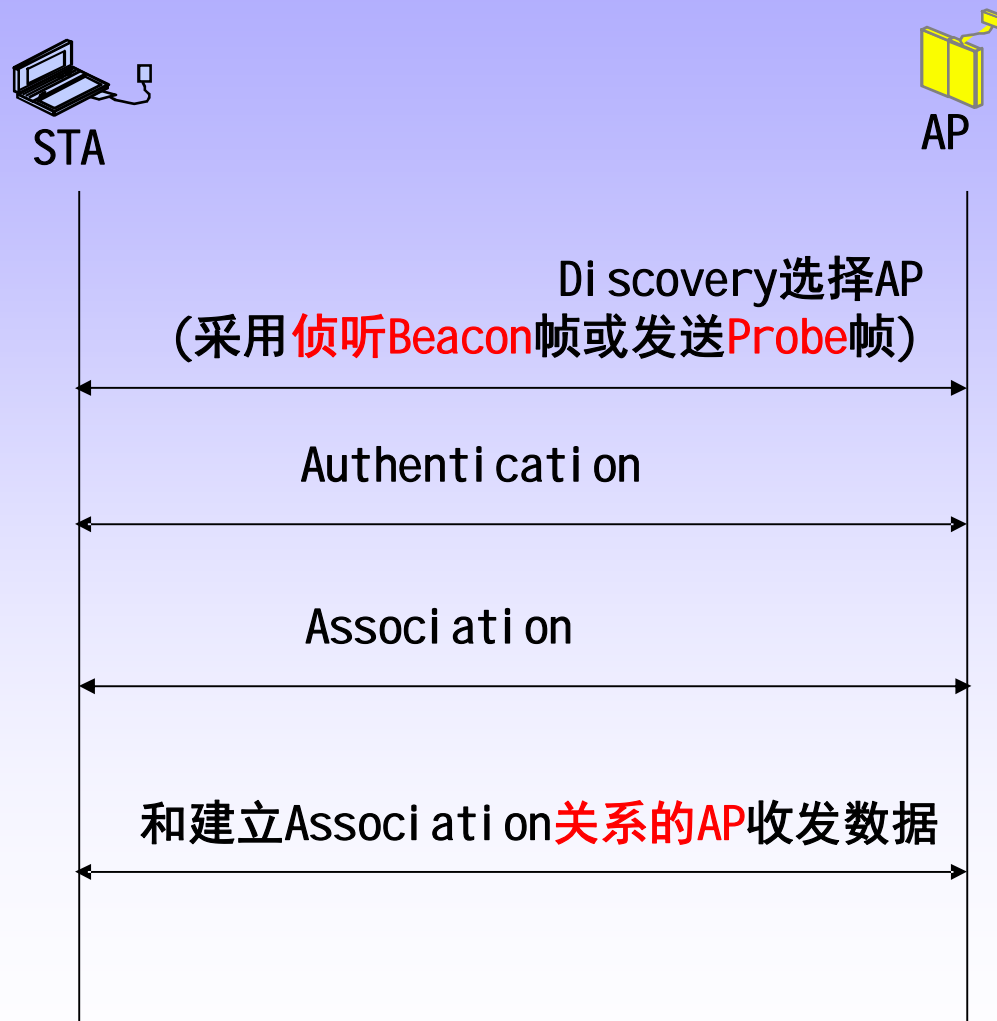
- 轻型AP设备、非智能化、操作简单
- 集中管理、便于维护和管理
- 更高安全可控性
- 无缝漫游
- 适用大规模密集部署、对控制要求高、有音视频漫游的场合

## 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建立隧道连接到AC  
从AC下载image文件（TFTP）
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



# 管理功能之一：用户接入



## 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(Independent BSS, ad hoc)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

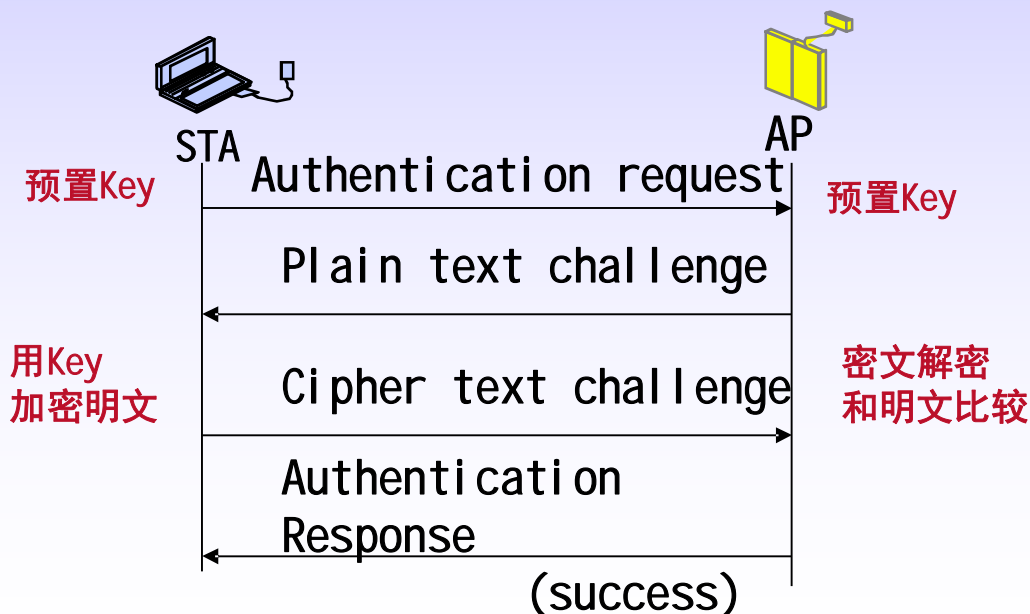
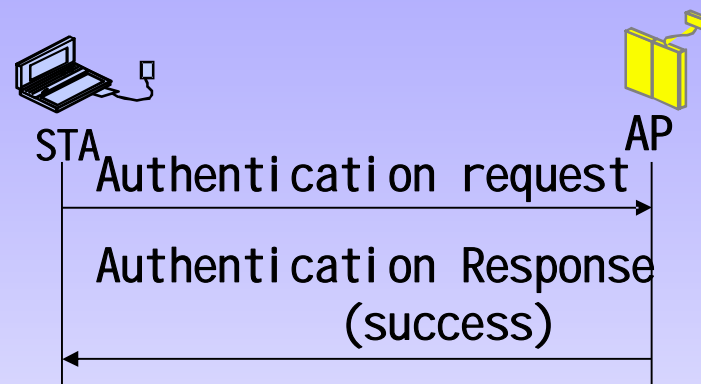
- 等同于**不需要认证**，没有任何安全防护能力
- 通过其它方式来保证用户接入网络的安全性，例如**Address filter**、用户报文中的**SSID**

## ◆ Shared-Key Authentication

- 采用**WEP**加密算法（已淘汰，WPA，WPA2）
- 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**

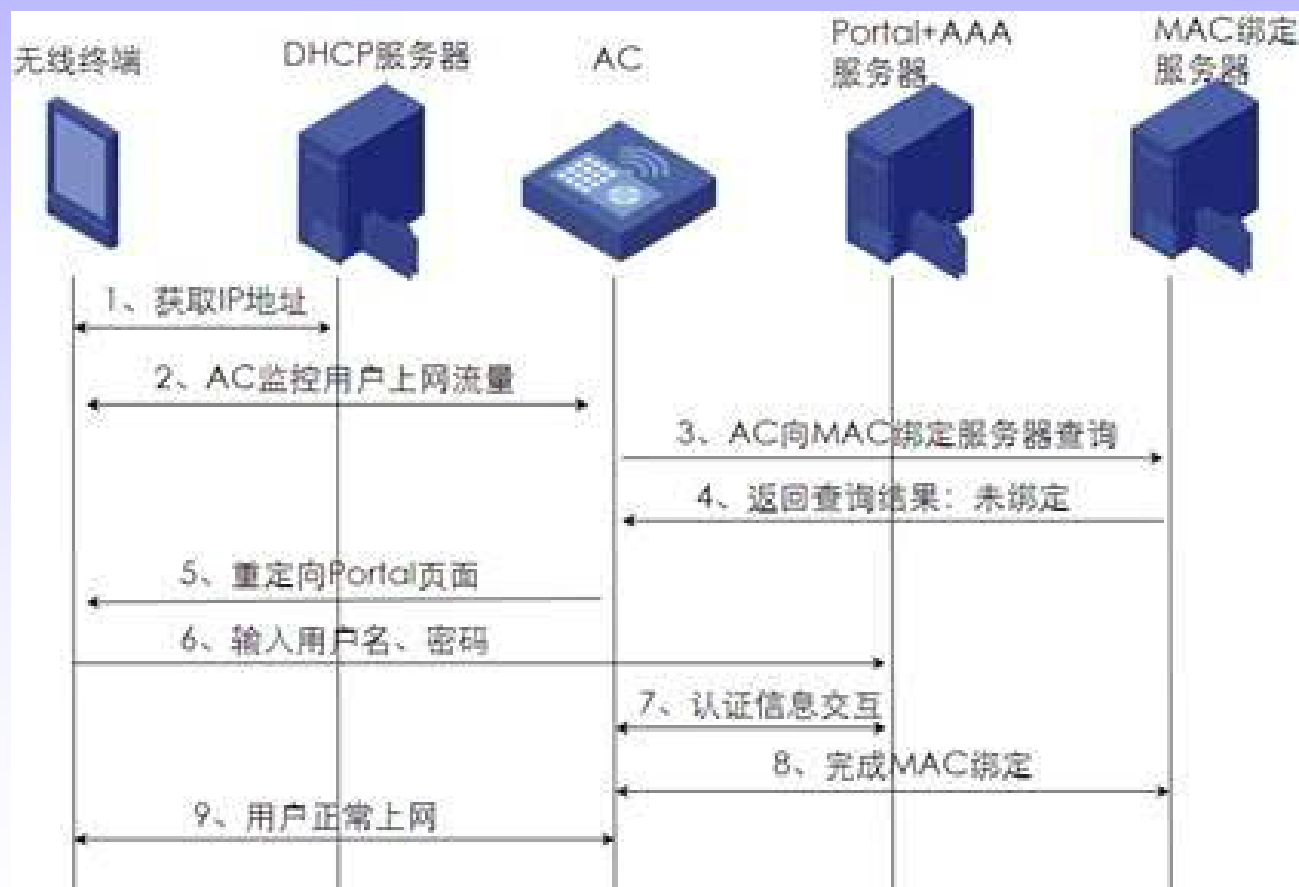
## ◆ STA可以通过

- Deauthentication来终结认证



# 管理功能之三：两种基本认证方式

## ◆ Portal 认证方式（华中科技大学Wi Fi）





## 管理功能之四：关联的建立

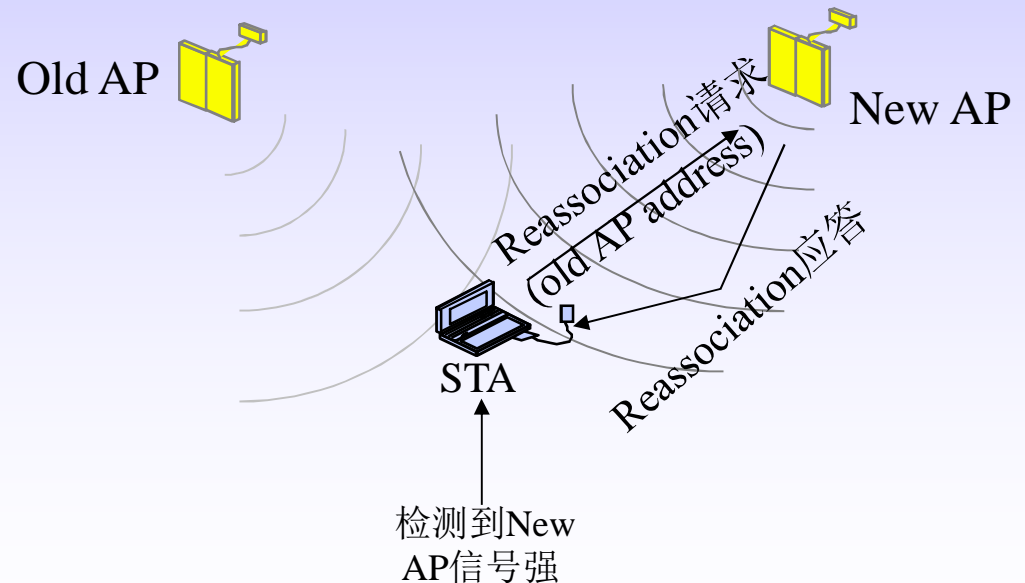
### ◆ Association

- 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重建关联
- 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

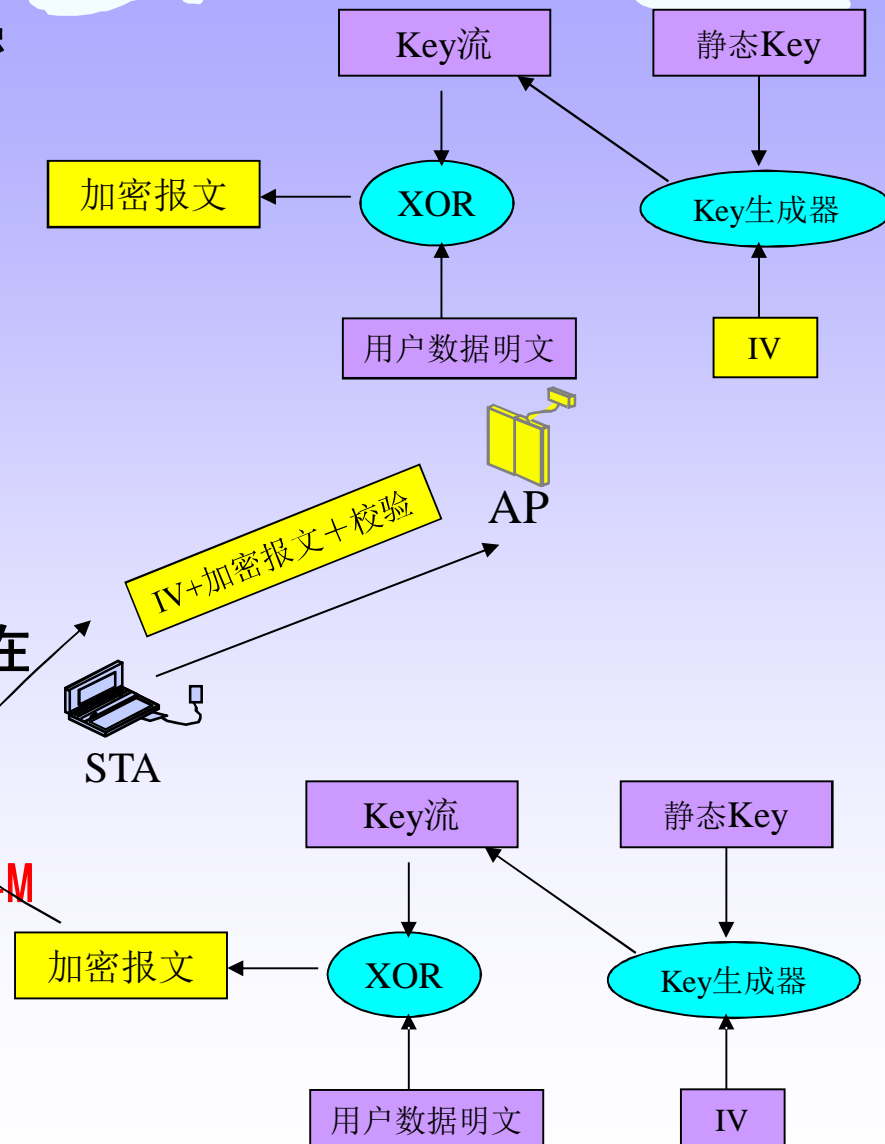
- STA和AP**预先配置相同静态Key**，Key长40 bit或104bit
- 每次数据加密Key=静态Key+24bit IV值（动态生成）

### ◆ 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

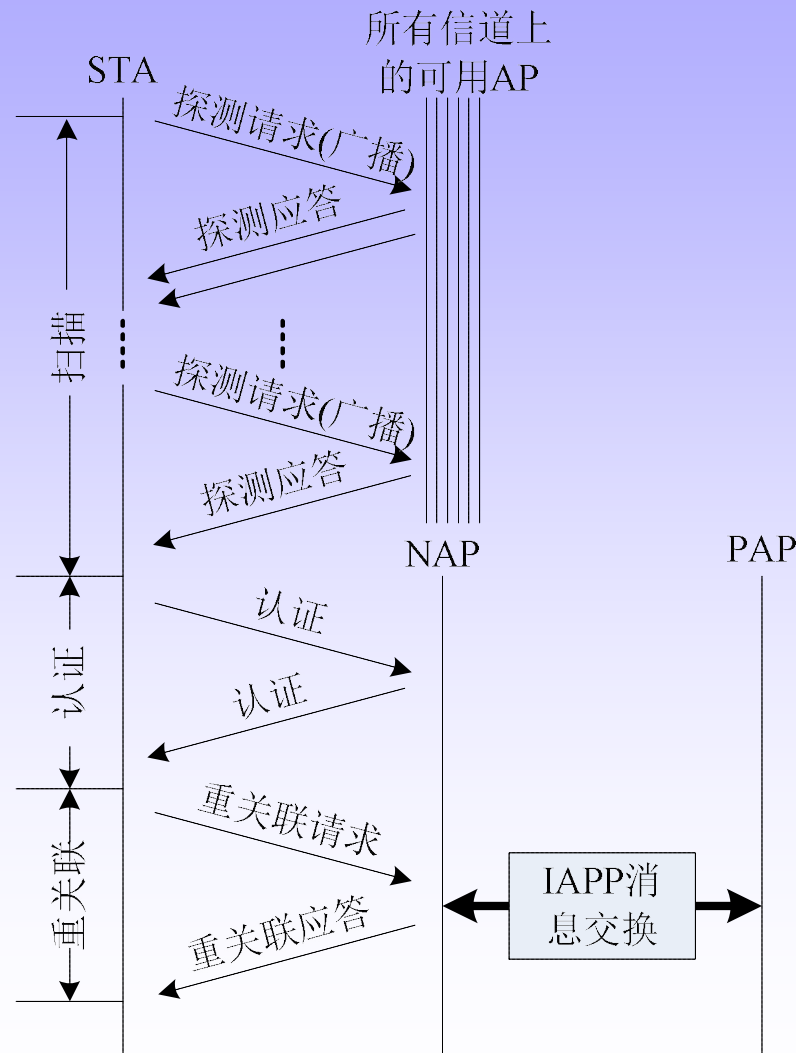
### ◆ 24位IV值太短造成：

- Attacker可以在分析侦听到**1M-4M**用户报文后破解加密Key



# IEEE 802.11切换

- ◆ 定义：STA从当前关联的AP（PAP: Previous Access Point）转移到另一个AP（NAP: New Access Point）的过程
- ◆ 切换发起：STA监测到当前无线链路的信噪比（SNR: Signal to Noise Ratio），当SNR低于“搜索门限”
- ◆ 扫描
  - 被动扫描：在每个信道上监听信标帧(Beacon)
  - 主动扫描：在每个信道上主动发送探测请求
- ◆ IAPP: Inter Access-Point Protocol，用于AP之间信息交互(例如认证状态信息)，以加快切换过程



# 切换优化考虑

- ◆ 不考虑认证延时，扫描占总延时的90%以上
- ◆ 主动扫描过程
  - 广播探测请求
  - 启动一个探测定时器（ProbeTimer）
  - 如果在ProbeTimer到达之前还未检测到信道忙，那么扫描下一个信道，否则当ProbeTimer到达时，处理所有接收到的探测应答，并且继续扫描下一个信道
- ◆ 扫描优化
  - 减少不必要的扫描：平滑SNR
  - 减少扫描信道的数量：获取相邻AP的工作信道集合

# 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**(paper)

[http://v.qq.com/x/page/m00155yv10y.html?ptag=di gi \\_myl ove1314\\_net](http://v.qq.com/x/page/m00155yv10y.html?ptag=di gi _myl ove1314_net)

- 加密Key**易被破译**，用户数据易被窃听
- 802.11**i** 解决上述问题

## ◆ QoS支持能力差，不适合Voice业务

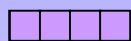
- DCF模式：无线所有用户**平等竞争**无线资源
- 数据报文**未划分优先级**，AP**无法分类**处理

2016/10/19 ➤ 802.11**e**(WMM)解决上述问题

# 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

优先级队列1



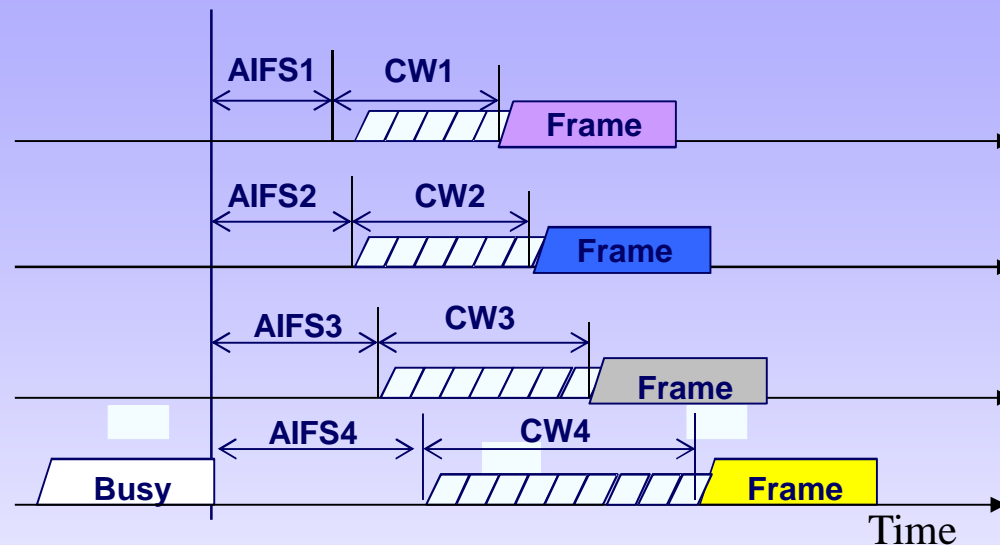
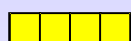
优先级队列2



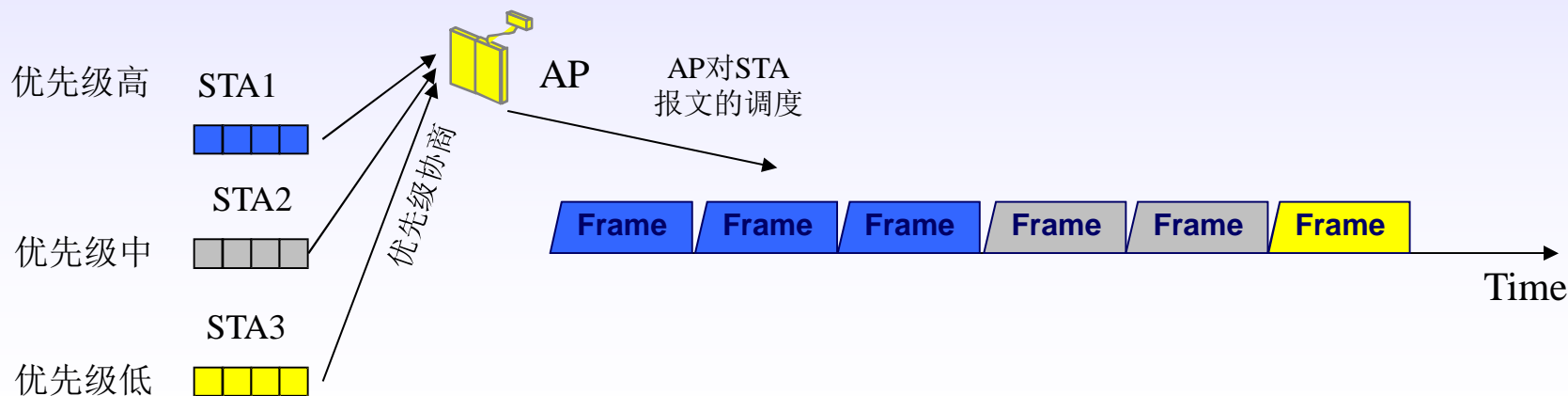
优先级队列3



优先级队列4



- 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



# 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

## 3.7 无线网安全

### 3.7.1 什么是无线网安全

- 资源的机密性、完整性、可用性和实体的真实性受到威胁

### 3.7.2 无线网面临的安全威胁

#### a) 资源扫描

- 利用正常AP要广播服务集标识SSID、链路速率、功耗等配置信息；
- 伪装AP、弱配置AP、Ad-hoc移动台等攻击
- 攻击工具：Windows下Netstumbler, Linux下Kismet...

#### b) 嗅探

- WLAN报文对于距离内相同频道的任何无线设备可见，有线等效保密协议WEP加密的不安全性，
- 在获取链路上报文，解密而获得原文；
- 攻击工具：WEP破解、字典攻击：Wepcrack/AirSnort/Cain...



### c) 伪装

- 非法移动站点通过扫描、监听获取WLAN中合法移动站点的相关信息
- 据此修改自己的标识和配置信息，从而掩盖自己的真实身份并窃取WLAN中得信息；可伪装移动站点或AP
- 攻击工具：Ai rSnarf/Hotspotter/HostAP...

### d) 注入

- 向无线链路会话中注入数据，来修改会话主体的链路状态；
- 向AP发送大量伪随机数据包，来增大网络的流量，继而破解密钥
- 攻击工具：I rpass/Ai rpwn/Chop...

### e) DOS（WLAN各层均可实施）

- 物理层：发送干扰信号，从而占用大量信道资源；
- 链路层：伪装成AP，发送伪造的去认证/去关联报文，使受害站点认为AP已切断服务，变断开与AP的连接，导致网络瘫痪；
- 其它有线网络上的DOS，仍可施用Wl an
- 攻击工具：Ai rJack/voi d11/I KECrack...

## 3.7.2 已有安全机制的缺陷

### ◆ 欺骗MAC地址过滤

- AP手工配置接入终端MAC地址→过滤表
- 无线终端繁多，MAC地址复杂→过滤表手工配置繁琐
- 通过无线链路监听获取别站MAC地址→伪装别站→欺骗AP

### ◆ 嗅探获取SSID标识

- 基本服务集BSS是Wlan基本单位（1组站点+1个AP），共享一个SSID。AP定时广播自己的SSID，或站点向AP请求；
- 未注册站点可搜索出周围的SSID，不认证也能加入

### ◆ WEP未保护源目地址信息

- 流密码→密文→安全强度低
- 未保护源目地址→重定向；无签名→不能抗重放攻击

### ◆ 接入认证（现有：开放系统认证、共享密钥认证）

- 开放：请求报文中SSID与AP的一致，且移动MAC未被虑掉
- 共享：AP产生128位随机质询文本给移站，移站用共享密钥对此加密回AP，AP解密并认证，使用的是本身有漏洞的WEP算法

## 3.7.3 Wlan安全协议

### ◆ WPA

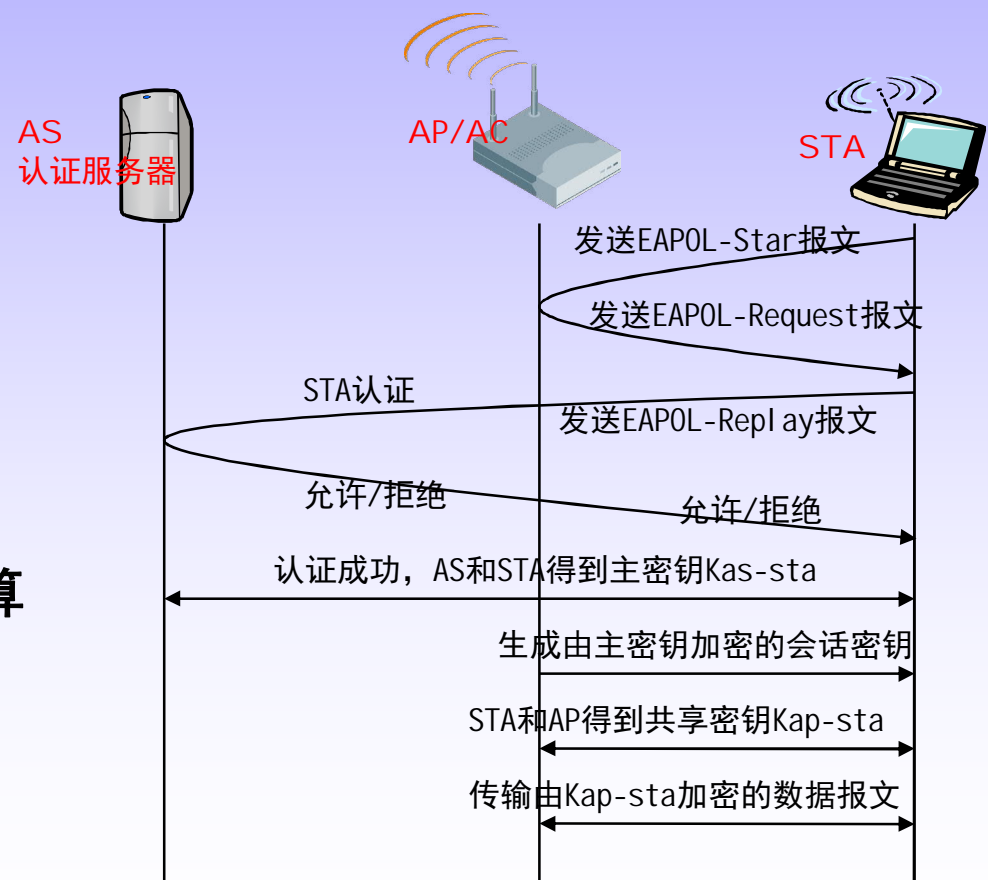
- 802.1x可扩展认证协议（EAP）
- 临时密钥集成协议TKIP

### ◆ 802.1X

- 基于端口的访问控制协议
- EAP over LAN→EAPOL

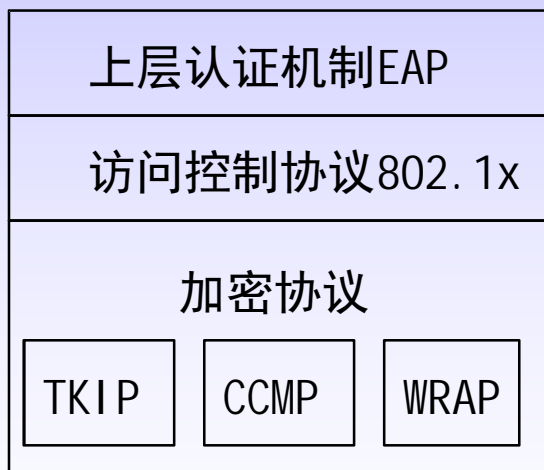
### ◆ TKIP

- 使用消息**完整性**校验码MIC
- 防止篡改和伪造
- 使用成对临时密钥，弥补RC4算法的漏洞...



# 802.11i 协议工作流程

- ◆ WPA: Wi-Fi Protected Access
- ◆ TKIP: Temporal Key Integrity Protocol
- ◆ CCMP: Counter-Mode/CBC-MAC Protocol
- ◆ WRAP: Wireless Robust Authenticated Protocol



802.11i 协议结构

