

多址接入协议 (MAC, 多路访问协议)：信道划分协议 (TDM (时分多址)、FDM (频分多址)、CDMA (码分多址))、**随机接入协议** (ALOHA: 纯ALOHA、时隙ALOHA, 载波侦听多路访问CSMA: CSMA/CA、CSMA/CD)、**轮流协议** (轮询、令牌传递)

CSMA/CA与CSMA/CD最主要的不同:

CSMA/CD在发送过程中检测冲突, 不使用确认机制

CSMA/CA在发送过程中不检测冲突, 使用确认机制

由此带来的协议处理方面的不同:

在CSMA/CD中, 节点侦听到信道空闲时立即发送 (不怕冲突, 冲突后立即停发, 损失不大)

在CSMA/CA中, 节点侦听到信道空闲后随机回退 (冲突对无线网络损害很大, 要尽量避免冲突)

最长前缀匹配: 将IP地址172.16.2.1与路由条目2的目的网络掩码255.255.255.0进行“逻辑与”运算, 将运算结果与路由条目2的目的网络地址的前24比特对比, 发现每一个比特位都相同, 因此该目的IP匹配这条路由, 而且匹配结果是172.16.2.0/24, 也就是说匹配长度是24。与路由条目2逻辑与运算完成, 不管结果是不是需要的匹配原则都会继续匹配路由条目三、四... ..

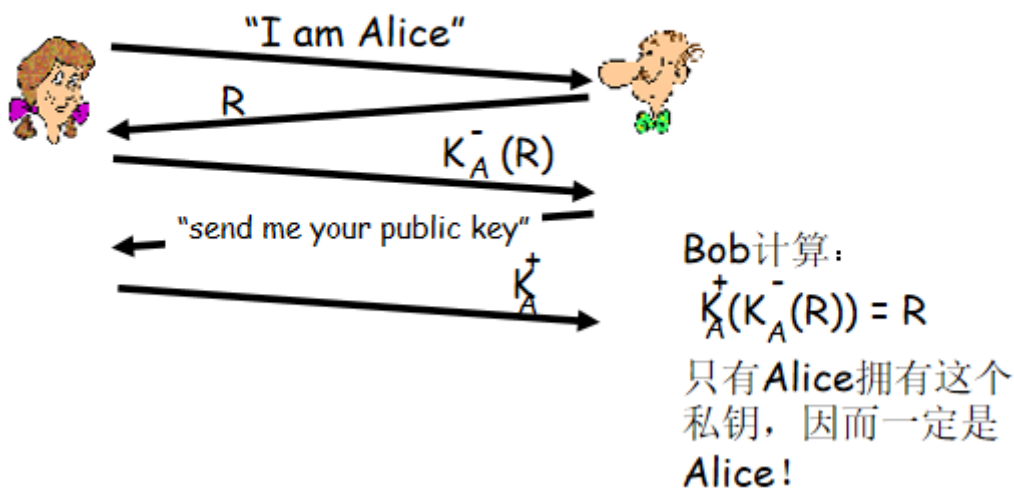
差错检测和纠正技术: 奇偶校验、检验和方法、循环冗余检测CRC

数字签名: 私钥加密报文摘要, $K_A^-(H(m))$, 起源鉴别, 防抵赖, 防止接收方修改 (完整性)

MAC报文鉴别码: $H(m + s)$, 其中s为共享密钥, 完整性, 发送方鉴别

鉴别: 利用不重数R防止重放攻击, 利用发送方私钥加密不重数提供起源鉴别

ap5.0: 采用公开密钥算法加密不重数



电子邮件安全PGP: 机密性、发送方鉴别、压缩、兼容电子邮件、分段

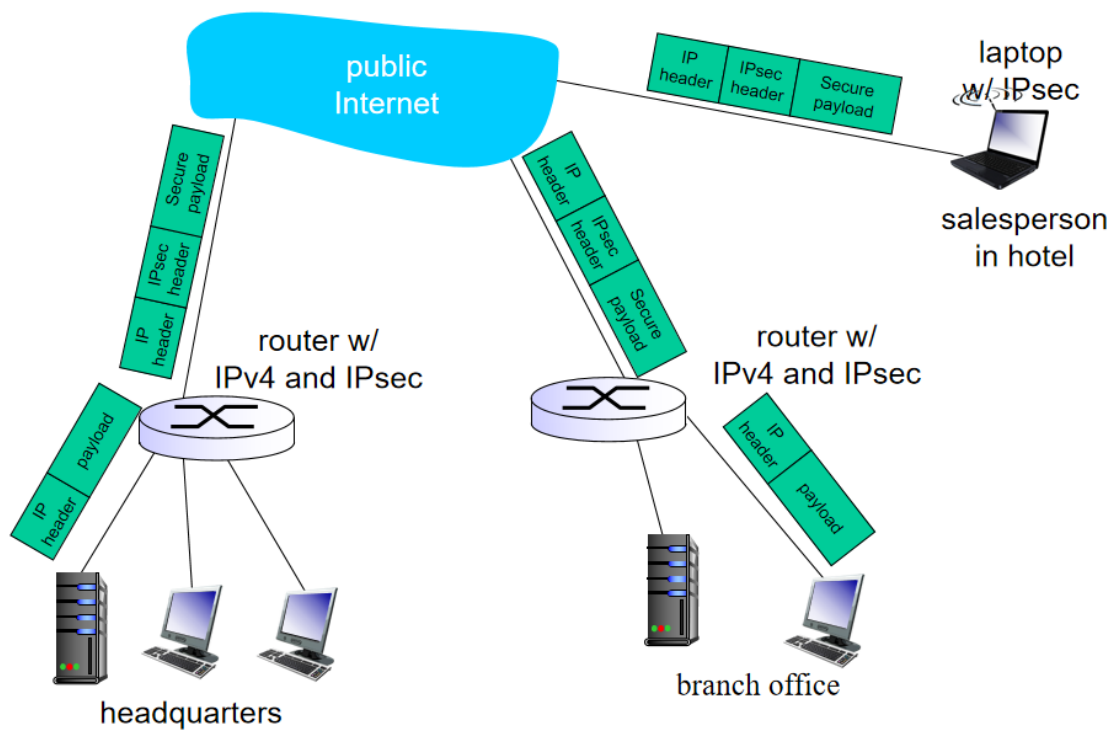
$Encode_{Base64}(K_B^+(K_{A-B}|| (K_{A-B}(zip(sgn||data)))))$, 其中sgn为数字签名

SSL安全套接字层: 机密性、数据完整性、服务器鉴别、客户鉴别

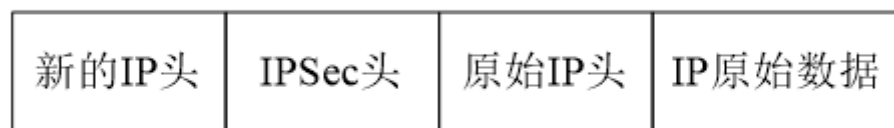
$E_B(data||(H(data||M_B||序号)))$

隧道技术:

1. VPN隧道技术



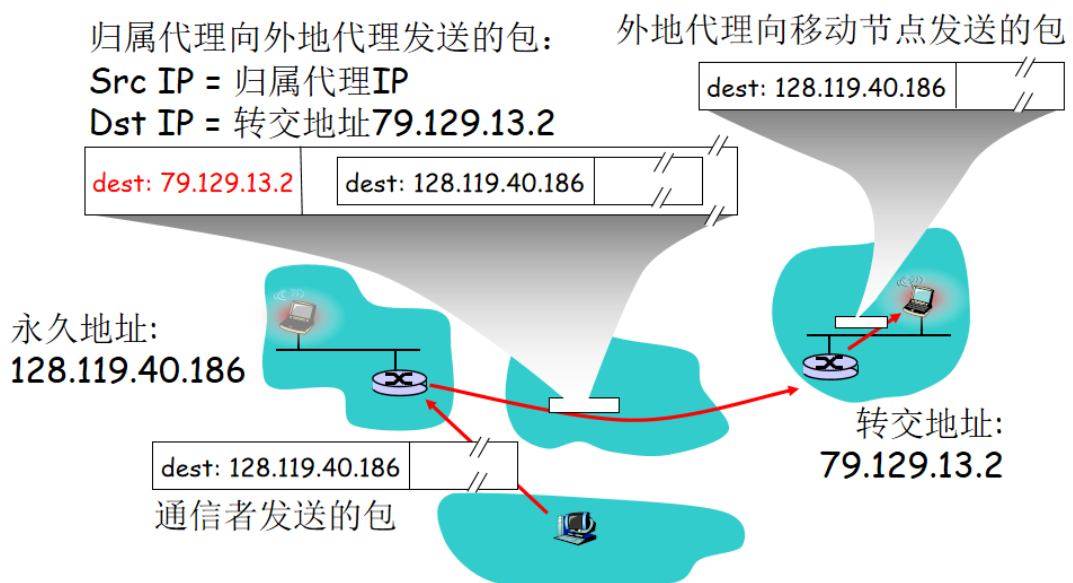
2. IPsec隧道模式



(b) 隧道模式

3. 归属代理通过隧道技术转发数据包

归属代理通过隧道转发数据包



4. 直接路由选择的通信者代理，和归属代理使用的隧道技术相似

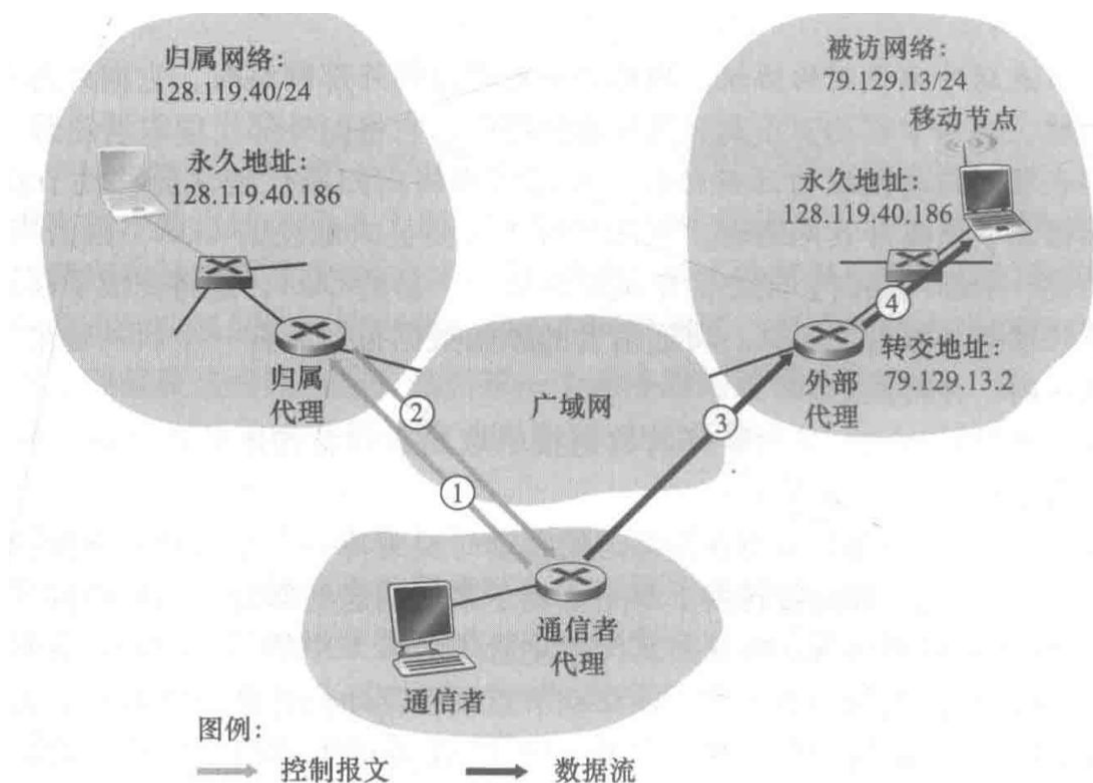


图 7-26 到某移动用户的直接路由选择

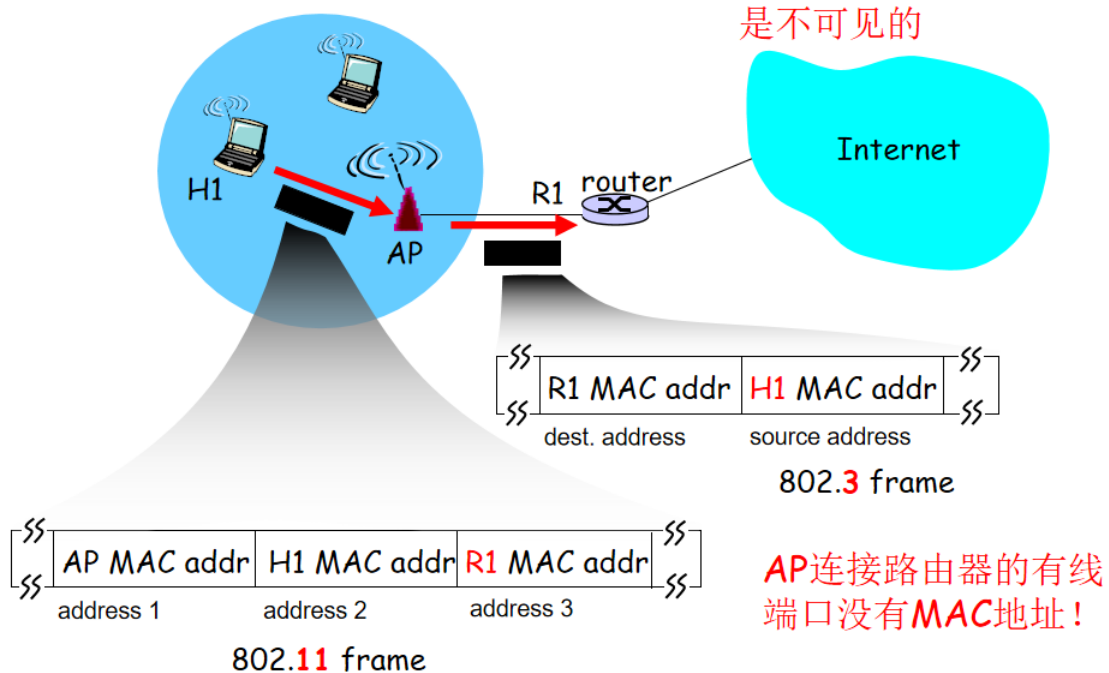
5. Ipv6数据包穿越到Ipv4网络

6. 多播分组穿越单播网络

转交地址(COA, care of address)

AP和归属代理永久地址的对比 (如上)

802.11帧: 寻址举例



交换式以太网的最小帧长及规模：*交换式以太网不再使用CSMA/CD协议，理论上不再需要限制帧的最小长度；但为了向后兼容，帧格式及最小帧长度的限制仍然保持不变；由于交换式以太网不再使用CSMA/CD协议，网络直径不再受到信号最大往返时间的限制。**

交换机自身对子网中的主机和路由器是**透明的**

交换机vs路由器：

交换机工作于链路层，根据MAC地址存储转发帧；路由器工作于网络层，根据IP地址存储转发数据报

交换机不能连接异构链路（即MAC协议不同的网络），因为交换机只是按原样转发帧；路由器可以连接异构链路，因为路由器需重新封装链路层帧

交换机不能阻断广播帧的传播：

交换机只能学习到单播MAC地址，所有广播帧都会扩散发送

通过交换机连接的所有主机在同一个广播域中

路由器可以阻断广播帧的传播：

路由器根据IP地址转发包（看不到MAC地址）

每个路由器端口是一个独立的广播域

RIP报文封装在UDP报文中发送，使用UDP端口520（RIP是一个应用层协议！）

OSPF分组被封装在IP包中传输

一对BGP speaker通过一条半永久的TCP连接（端口179）建立BGP会话，交换BGP报文（BGP是应用层协议！）

ICMP报文被封装在IP包中传输：这是因为ICMP报文可能需要经过几个网络才能到达源节点；ICMP通常被认为是IP协议的一部分，因为IP协议使用ICMP向源节点发送错误报告。