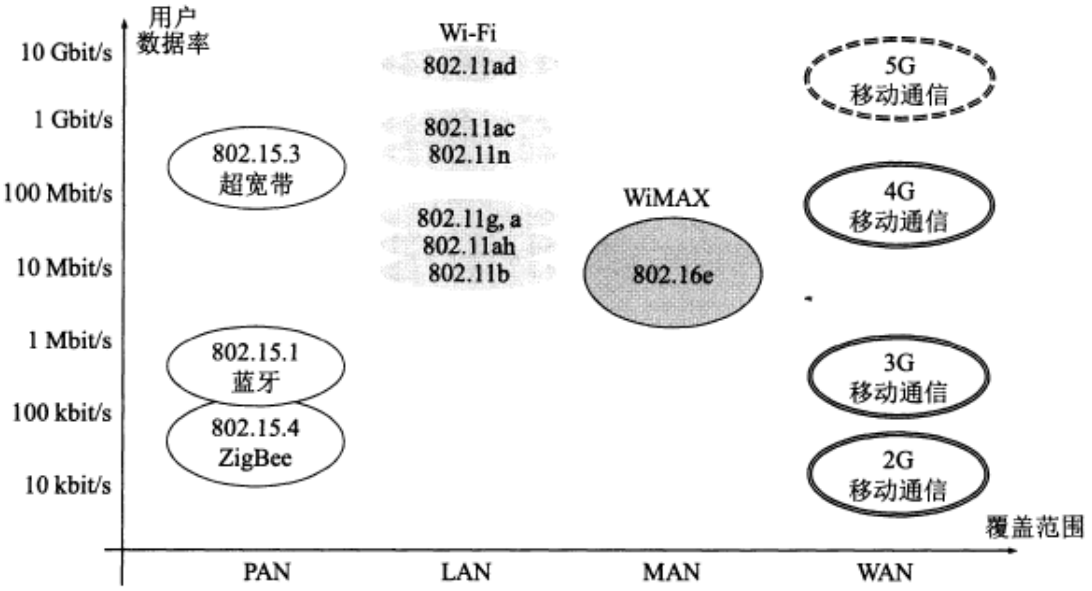
第二十二节 无线局域网 WLAN、蜂窝移动通信和移动 IP

一、课程目标

了解教材 9.1-9.2。

二、课程内容

1、常见无线网络。



2、Wi-Fi 是 IEEE 802.11 系列标准化的 WLAN（Wireless Local Area Network, 无线局域网），是一个有固定基础设施的无线局域网的国际标准。

其主要特点包括：

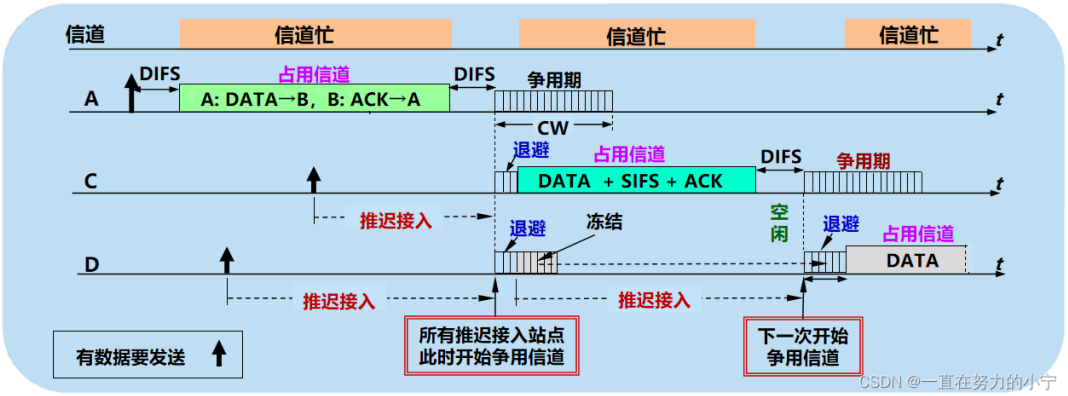
（1）**使用星形拓扑**，中心叫做接入点 AP（Access Point），AP 是无线局域网的基础设施，也是一个链路层的设备，AP 也叫做无线接入点 WAP（Wireless Access Point）；无线局域网中的站点对网内或网外的通信都必须通过 AP。

（2）**在 MAC 层使用 CSMA/CA（带有冲突避免的载波侦听多路访问）协议**。其特点是发送包的同时不能检测到信道上有无冲突，只能尽量“避免”。

CSMA/CA 工作原理：

（1）当主机需要发送一个数据帧时，首先检测信道，在持续检测到信道空闲达一个长帧间隔 DIFS 之后，主机发送数据帧。接收主机正确接收到该数据帧，等待一个短帧间隔 SIFS 后马上发出对该数据帧的确认。若源站在规定时间内没有收到确认帧 ACK，就必须重传此帧，直到收到确认为止，或者经过若干次重传失败后放弃发送。

（2）当一个站检测到正在信道中传送的 MAC 帧首部的“持续时间”字段时，就调整自己的网络分配向量 NAV。NAV 指出必须经过多少时间才能完成这次传输，才能使信道转入空闲状态。因此，信道处于忙态，或者是由于物理层的载波监听检测到信道忙，或者是由于 MAC 层的虚拟载波监听机制指出了信道忙。

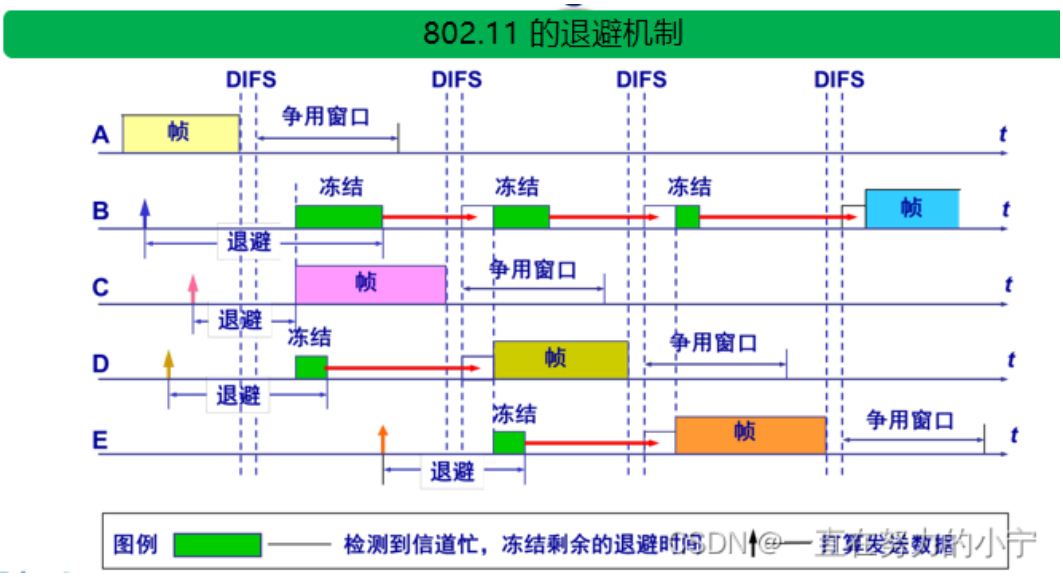


处理流程：

（1）在站点 A 和 B 通信的过程中，站点 C 和 D 也要发送数据。但 C 和 D 检测到信道忙，因此必须推迟接入(defer access)，以免发生碰撞。

（2）在等待信道进入空闲状态后，都经过规定的时间间隔 DIFS 再同时发送数据必然产生碰撞。因此 CSMA/CA 规定：所有推迟接入的站都必须在争用期执行统一的退避算法开始公平地争用信道。

（3）争用期也叫做争用窗口 CW (Contention Window)。争用窗口由许多时隙(time slot)组成。例如，争用窗口 CW=15 即窗口大小是 15 个时隙。



（4）时隙长度的确定方法：在下一个时隙开始时，每个站点都能检测出在前一个时隙开始时信道是否忙（这样就可采取适当对策）。时隙长短在不同 802.11 标准中可以有不同数值。例如：802.11g 一个时隙时间为 9us；SIFS=10us；DIFS=SIFS+(2*Slot time)=28us。

（5）退避算法：站点在进入争用期时，应在 0~CW 个时隙中随机生成一个退避时隙数，并设置退避计时器(backoff timer)。 当几个站同时争用信道时，计时器最先降为零的站首先接入媒体，发送数据帧。这时信道转为忙，而其他正在退避的站则冻结其计时器，保留计时器的数值不变，推迟到下次争用信道时接着倒计时。这样的规定对所有的站是公平的。

- **建议值： 15 (最小) ≤ 争用窗口 CW ≤ 1023 (最大)。**
- **CSMA/CA规定：如果未收到确认帧，则必须重传。但每重传一次，争用窗口的数值就近似加倍。**
- **假定：选择初始争用窗口 CW = $2^4 - 1 = 15$，第 i 次退避就在 $2^{4+i} - 1$ 个时隙中随机地选择一个，即：**
  - **第 1 次重传时，随机退避的时隙数应在 0 ~ 31 之间生成。**
  - **第 2 次重传时，随机退避的时隙数应在 0 ~ 63 之间生成。**
  - **第 3 次重传时，随机退避的时隙数应在 0 ~ 127 之间生成。**
  - **第 4 次重传时，随机退避的时隙数应在 0 ~ 255 之间生成。**
  - **第 5 次重传时，随机退避的时隙数应在 0 ~ 511 之间生成。**
  - **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 不再增大了。**

CSDN @一直在努力的小宁

“推迟接入”和“退避(backoff)”的区别

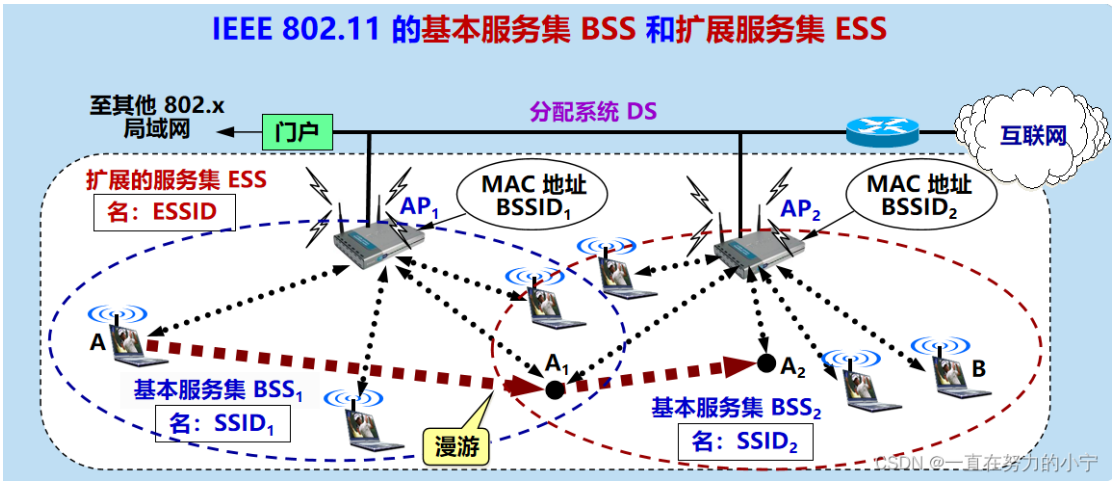
推迟接入：发生在信道处于忙的状态，为的是等待争用期的到来，以便执行退避算法来争用信道。这时退避计时器处于冻结状态。

退避：是争用期各站点执行的算法，退避计时器进行倒计时。这时信道是空闲的，并且总是出现在时间间隔 DIFS 的后面。

(6)退避时机：要发送数据时检测到信道忙；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）。此外，当站点想发送数据，检测信道连续空闲时间超过 DIFS 时，即可立即发送数据，不必经过争用期。

3、基本服务集 BSS 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。

- **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。
- 一个 BSS 所覆盖的地理范围叫做一个**基本服务区 BSA** (Basic Service Area)。
- **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。
- 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)。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** 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。
- 移动站 A 漫游到位置 A1 时，选择和信号较强的一个 AP 联系。当漫游到位置 A2 时，就只能和 AP2 联系了。BSS 的服务范围是由 AP 所发射的电磁波的辐射范围确定的。移动站只要能够和其中一个 AP 联系上，就可以一直保持与另一个移动站 B 的通信。一个移动站若要加入到一个 BSS，就必须先与某个 AP 建立关联。



Wi-Fi 名称和 SSID 的区别与联系：

SSID 是无线局域网的唯一标识符，不同的网络必须具有不同的 SSID。Wi-Fi 名称是人们在移动设备或计算机中看到的网络名称，它通常是 SSID 的可读版本。

1、名称不同：Wi-Fi 名称是无线网络的名称，用于显示在设备中的列表中，让用户可以轻松识别和连接。而 SSID 是一个标识符，它是无线网络的唯一标识符，用于识别和区分不同的无线网络。

2、可见性不同：Wi-Fi 名称是公开的，任何人都可以在搜索 Wi-Fi 网络时看到它。而 SSID 是隐藏的，除非用户明确搜索或连接该网络，否则无法看到它。

3、格式不同：Wi-Fi 名称可以使用字母、数字、特殊字符等来描述，通常有更友好的名称。而 SSID 通常是由路由器生成的随机字符串，可能不太易于识别。

4、安全性不同：Wi-Fi 名称不会影响网络的安全性。而 SSID 是网络的唯一标识符，它可以被黑客用于攻击和入侵，因此隐藏 SSID 可以提高网络的安全性。

4、移动站加入选定的 AP 所属子网途径：主动扫描和被动扫描。

- 被动扫描：AP 周期性发出信标帧 (beacon frame)，其中包含 SSID、速率等系统参数；移动站 A 扫描 11 个信道，选择加入到 AP2 所在的基本服务集 BSS2，向 AP2 发出关联请求帧； AP2 同意移动站 A 发来的关联请求，向移动站 A 发送关联响应帧。
- 主动扫描：移动站 A 发出广播的探测请求帧，让所有能够收到此帧的接入点知道有移动站要求建立关联；两个 AP 都回答探测响应帧(Probe Response frame)；移动站 A 向 AP2 发出关联请求帧(Association Response frame)；AP2 向移动站 A 发送关联响应帧，与移动站 A 建立关联。

5、安全建立关联

初期加密方案：有线等效的保密 WEP (Wired Equivalent Privacy)。

现在加密方案：无线局域网受保护的接入 WPA (WiFi Protected Access)或 WPA2。

6、移动自组网络

移动自组网络也就是移动分组无线网络。例如，无线传感器网络 WSN 是由大量传感器结点通过无线通信技术构成的自组网络。

7、802.11 局域网物理层

根据物理层的不同（如工作频段、数据率、调制方法等），对应的标准也不同。

802.11 的物理层有以下几种实现方法：

① 扩频

② 多入多出 MIMO (Multiple Input Multiple Output)

③ 正交频分复用 OFDM (Orthogonal Frequency Division Multiplexing)

④ 调频扩频 FHSS （已很少用）

⑤ 红外线 IR （已很少用）

标准	别名	频段	最高数据率	物理层	优缺点
802.11b (1999年)	Wi-Fi 1	2.4 GHz	11 Mbit/s	扩频	最高数据率较低，价格最低，信号传播距离最远，且不易受阻碍
802.11a (1999年)	Wi-Fi 2	5 GHz	54 Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，价格最高，信号传播距离较短，且易受阻碍。
802.11g (2003年)	Wi-Fi 3	2.4 GHz	54 Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，信号传播距离最远，且不易受阻碍，价格比 802.11b 贵。
802.11n (2009年)	Wi-Fi 4	2.4 / 5 GHz	600 Mbit/s	MIMO OFDM	使用多个发射和接收天线达到更高的数据传输率，当使用双倍带宽 (40 MHz) 时速率可达 600 Mbit/s。
802.11ac (2014年)	Wi-Fi 5	5 GHz	7 Gbit/s	MIMO OFDM	完全遵循 802.11i 安全标准的所有内容，使得无线连接能够在安全性方面达到企业级用户的需求。
802.11ax (2019年)	Wi-Fi 6	2.4 / 5 GHz	9.6 Gbit/s	MIMO OFDM	侧重解决密集环境下（如火车站、机场）提高吞吐量密度（即单位面积的吞吐量）

CSDN @一直在努力的小宁

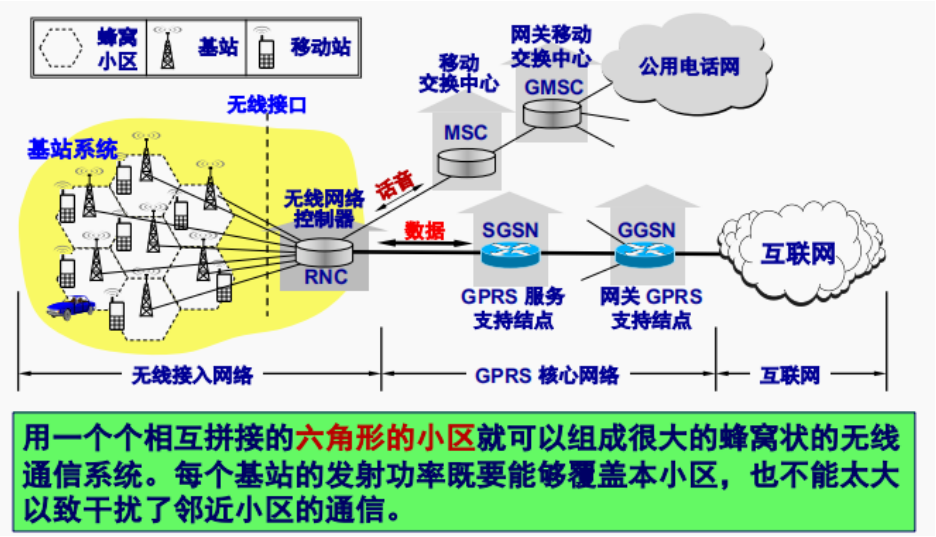
8、802.11 帧结构

- 802.11 帧三种类型：控制帧、数据帧、管理帧。
- 802.11 数据帧包括首部（30B）、帧主体（数据部分，不超过 2312B。802.11 帧的长度通常都小于 1500B）、帧检验序列 FCS（尾部，4B）。

【蜂窝通信】

9、移动通信包括蜂窝移动通信、卫星移动通信等。

蜂窝移动通信是小区制的移动通信，它把整个网络划分成许多小区（也就是蜂窝），每个小区设置一个基站。移动站的通信都必须通过基站完成。



10、移动通信发展回顾

第一代（1G）蜂窝无线通信是为话音通信设计的模拟 FDM 系统。

第二代（2G）蜂窝无线通信提供低速数字通信（短信服务），其代表性体制就是最流行的 GSM 系统。

2.5G 技术是从 2G 向第三代（3G）过渡的衔接性技术，如 GPRS 和 EDGE 等。

第三代（3G）移动通信和计算机网络的关系非常密切，它使用 IP 的体系结构和混合的交换机制（电路交换和分组交换），能够提供移动宽带多媒体业务（话音、数据、视频等，可收发电子邮件，浏览网页，进行视频会议等），如 CDMA2000，WCDMA 和 TD-sCDMA。

从 3G 开始以后的各代蜂窝移动通信都是以传输数据业务为主的通信系统，而且必须兼容 2G 的功能（即能够通电话和发送短信），这就是所谓的向后兼容。

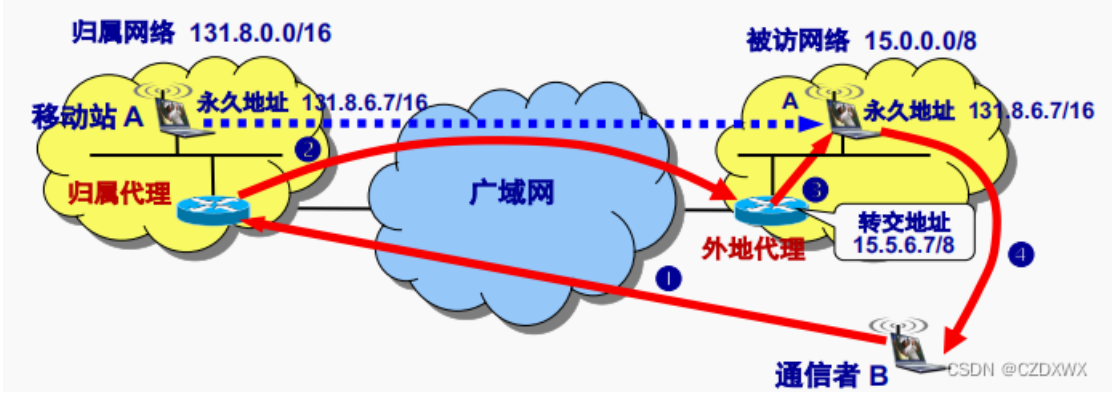
第四代（4G）正式名称是 IMT-Advanced（International Mobile Telecommunications-Advanced），意思是高级国际移动通信。4G 的一个重要技术指标就是要实现更高的数据率。目标峰值数据率是：固定的和低速移动通信时应达到 1Gbit/s，在高速移动通信时（如在火车。汽车上）应达到 100 Mbit/s。4G 代表性方案包括 LTE 和 LTE-A。

- LTE （Long-Term Evolution）分为时分双工 TD-LTE 和频分双工 FDD-LTE 两种。把带宽增加到 20 MHz，采用了高阶调制 64 QAM 和 MIMO 技术。
- LTE-A（LTE-Advanced）是 LTE 的升级版，俗称为 3.9G。带宽高达 100 MHz。

第五代（5G）移动通信技术高速率、低时延、大连接是最突出的特征，用户体验速率达 1Gbps，时延低至 1ms，用户连接能力达 100 万连接/平方公里。目标涵盖三大类应用场景，即**增强移动宽带（eMBB）、超高可靠低时延通信(uRLLC)和机器类通信(mMTC)**。增强移动宽带（eMBB）主要面向移动互联网流量爆炸式增长，为移动互联网用户提供更加极致的应用体验；超高可靠低时延通信(uRLLC)主要面向工业控制、远程医疗、自动驾驶等对时延和可靠性具有极高要求的垂直行业应用需求；机器类通信(mMTC)主要面向智慧城市、智能家居、环境监测等以传感和数据采集为目标的应用需求。

【移动 IP】

11、移动 IP（Mobile IP）又称为移动 IP 协议，允许计算机移动到外地时仍然保留其原来的 IP 地址。目的：使用户的移动性对上层的网络应用是透明的。



相关概念：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）**。归属网络中使用的代理叫做**归属代理（home agent）**。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）**。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）**。

12、通信者 B 和移动站 A 的四个重要通信步骤：

（1）B 发送给 A 的数据报被 A 的归属代理截获了（只有当 A 离开归属网络时，归属代理才能截获发给 A 的数据报）。

（2）由于归属代理已经知道了 A 的转交地址（外部代理向归属代理报告转交地址路由选择），因此归属代理把 B 发来的数据报进行再封装，新的数据报的目的地址是 A 现在的转交地址。新封装的数据报发送到被访网络的外地代理。这里使用的是隧道技术或 IP-in-lP。

（3）被访网络中的外地代理把收到的封装的数据报进行拆封，取出 B 发送的原始数据报。然后转发给移动站 A。这个数据报的目的地址就是 A 的永久地址。A 收到 B 发送的原始数据报后，也得到了 B 的 IP 地址。

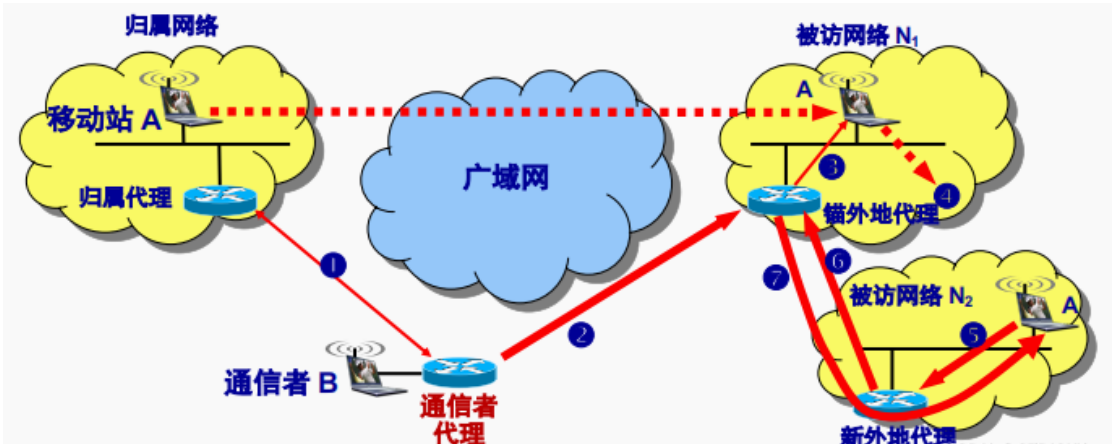
（4）如果现在 A 要向 B 发送数据报，那么情况就比较简单。A 仍然使用自己的永久地址作为数据报的源地址，用 B 的 IP 地址作为数据报的目的地址。这个数据报显然没有必要在通过 A 的归属代理进行转发了。

13、三角路由问题

间接路由选择是把数据报发往移动站的归属网络，由归属代理完成以后的寻址工作，进而完成数据报转发的方式。

问题描述：间接路由选择可能会引起数据报转发的低效，文献中称之为三角形路由选择问题（triangle routing problem）。意思是本来在 B 和 A 之间可能有一条更有效的路由，但现在要走另外两条路：先要把数据报从 B 发送到 A 的归属代理，然后再转发给漫游到被访网络的 A。

解决办法：让通信者 B 创建一个通信者代理（correspondent agent），让这个通信者代理向归属代理询问到移动站在被访网络的转交地址。然后由通信者代理把数据报用隧道技术发送到被访网络的外地代理，最后再由这个外地代理拆封，把数据报转发给移动站。但这是以增加复杂性为代价的。



三、重点习题

P443：全部

四、参考资料