



EV-DO系统信令分析



南志刚

2006年 6月

目 录

导 读.....	4
第 1 章 空口流程介绍.....	5
1.1 初始化过程.....	6
1.2 登记过程.....	7
1.2.1 UATI 请求消息.....	9
1.3 空闲状态.....	11
1.3.1 休眠状态.....	12
1.3.2 监视状态.....	12
1.4 连接建立.....	14
1.5 挂起操作模式.....	20
1.6 监视小区导频信号强度.....	21
1.7 会话配置协商.....	23
1.7.1 IS856 会话层协议介绍.....	24
1.7.2 会话配置协商过程.....	24
1.7.3 PPP 连接.....	26
1.7.4 会话维持.....	28
第 2 章 切换.....	30
2.1 前向链路切换介绍.....	30
2.1.1 导频集管理.....	30
2.1.2 虚拟软切换.....	35
2.2 反向链路切换介绍.....	36
2.3 1xEV-DO 和 1x2000 系统间的切换.....	36
第 3 章 功率控制.....	38
3.1 开环功率控制.....	38
3.2 闭环功率控制.....	38
3.2.1 外环功率控制.....	39
3.2.2 内环功率控制.....	40
3.2.3 RPC 信道和 DRCLock 信道.....	40
第 4 章 反向负载控制.....	41
4.1 反向速率控制.....	41
4.1.1 RateLimit 消息.....	41
4.2 反向负荷过载控制.....	42



4.2.1 CSM5500 算法介绍——扇区负荷估算	42
4.2.2 Io/No 测量（总的接收功率谱密度/噪声功率谱密度）	43
第 5 章 整体信令流程	44
5.1 AT 始发的 HRPD 会话建立流程	45
5.2 AN 始发的网络侧重激活流程	49
5.3 AT 始发的连接释放流程	50
5.4 AN 发起的连接释放流程	51
5.5 AT 始发的会话释放流程	52
5.6 软切换流程	52
5.7 AN-AAA 鉴权消息	53
第 6 章 附录	54
6.1 1 UNTI 解释	54
6.2 附录 2 Rati 解释	55
6.3 附录 3 AT 开机后维持的各个状态解释	56

导 读

本文分为以下几大模块介绍EVDO信令：

第 1 章：按照终端从开机到连接的实际流程，结合信令实例讲解终端处于各个阶段的实现过程。

第 2 章：讲解 DO 的切换过程以及过程中涉及的消息及参数。

第 3 章：讲解 DO 的功率控制原理以及过程中涉及的消息及参数。

第 4 章：讲解 DO 的负载控制原理以及过程中涉及的消息及参数。

第 5 章：在前面 4 章的基础上给出各个过程的整体流程信令讲解，读者可以参考前四章内容结合 OMC 跟踪到的消息理解第 5 章内容。

缩略语清单：

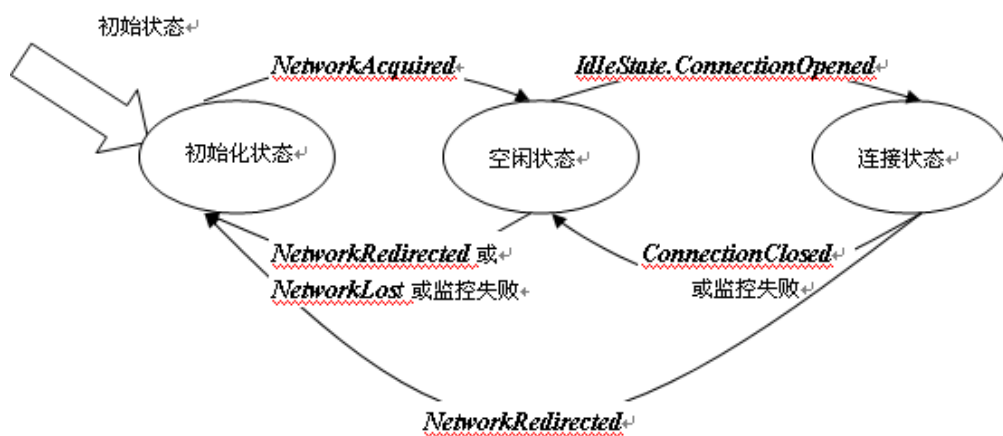
1、AN	Access Network	接入网
2、AT	Access Termination	接入终端
3、DRC	Data Rate Control	数据速率控制（信道）
4、MAC	Medium Access Control	媒体接入控制
5、RA	Reverse Activity	反向激活
6、RLP	Radio Link Protocol	无线链路协议
7、RPC	Reverse Power Control	反向功率控制信道
8、RRI	Reverse Rate Indicator	反向速率指示（信道）
9、UATI	Unicast Access Termination Identifier	唯一终端访问标识

第1章 空口流程介绍

终端进入每一个连接状态都需要经历一个流程。空中链路管理协议维持 AT 和 AN 连接过程中的各个状态，共经历如下三种状态：

- 初始化状态：由初始化状态协议维持，执行与捕获 AN 相关的动作。
- 空闲状态：AT 已经捕获网络但连接是关闭的，即处于空闲状态，由空闲状态协议维持相关的动作，主要用于：支持有效寻呼，引导连接打开的过程，以及支持 AT 的功率保持。空闲状态下，保持 PPP 链路，释放空口和 A8/A9 链路。
- 连接状态：处于连接状态时，由连接状态协议管理 AT 和 AN 之间的无线资源，还用于管理引起连接关闭的过程。分配专有空口资源，建立 A8/A9 链路，可以进行上行或下行数据传输。

下图是终端在各个状态中迁移的概述：



AT 给基站发送数据前，并不知道最近基站的距离，需要有一个接入网络的过程。进入接入模式，AT 决定接入时使用的最小发射功率，避免引入不必要的 RF 干扰。AT 通过发送功率递增的接入试探完成接入过程，只有当发送某个接入试探后收到基站的响应信息时，才停止接入试探的发送。初始接入试探的发射功率是 AT 接收到的信号强度的函数（反向开环功控）。如果 AT 收到的信号强，说明距离基站近，则相应的初始接入探针功率较小。收到基站的响应后，AT 就开始采用最后一个接入探针的功率进行消息发送。

下面介绍 AT 与 AN 之间建立连接的各个状态，以及各状态涉及到的消息。

1.1 初始化过程

AT 获取服务网络信息的过程就是初始化状态，AT 选择一个服务网络，并从该网获得时间同步。

初始化状态协议规定了 AT 捕获服务网络的过程和消息。

消息触发因素：开机、网络重定向。由空中链路管理协议激活其初始化过程，过程经历以下四个步骤：

非激活状态：等待 **Activate** 命令来激活初始化过程；

网络确定状态：AT 选择服务 AN，挑选导频信号最好的扇区；

导频捕获状态：AT 捕获前向导频信道；

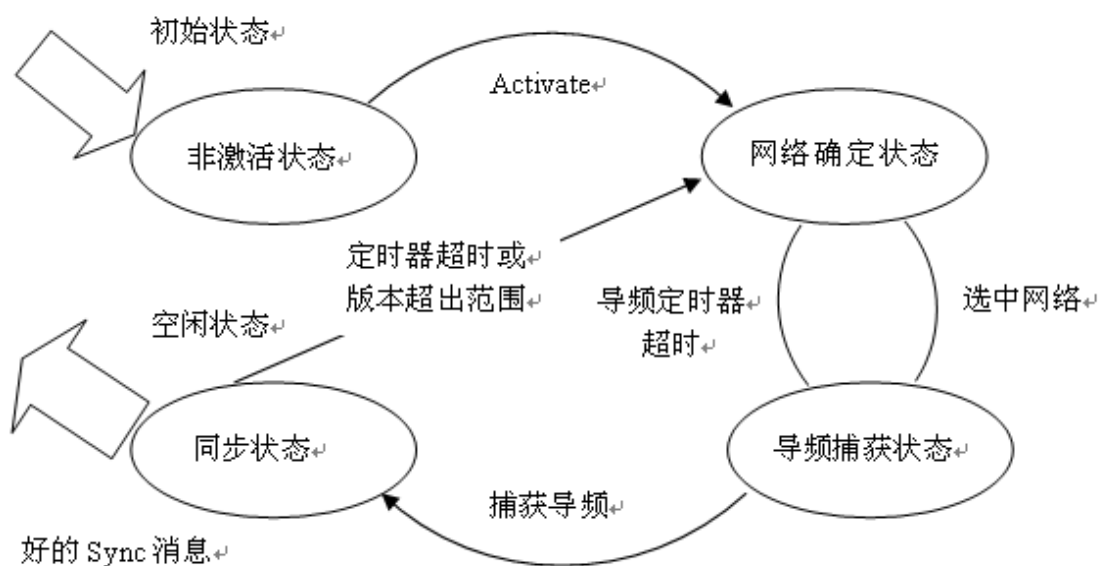
同步状态：AT 与控制信道周期同步，接收 **Sync** 消息并与系统时间同步。**Sync** 消息包括：与基站兼容的 AT 版本范围、基站扇区的 PN、网络系统时间。见下面消息实例的中文标注。

Sync Message: （CAIT 跟踪空口获取的消息实例）



Sync Message.txt

四个状态间的迁移如下图所示：



以上四个状态的消息都是 AN 在前向控制信道（CC）上广播的。

1.2 登记过程

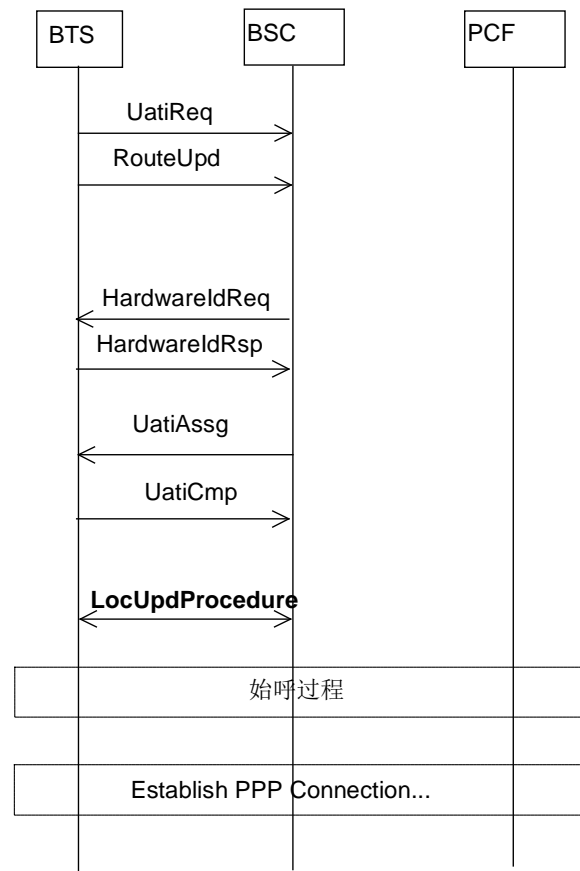
登记即 AT 与 AN 建立会话（session）的过程，AN 会给 AT 分配一个全局唯一的 UATI 标识（UNTI 的解释见附件 1）。会话一旦建立，轻易不会释放（缺省超时 54 小时才释放），会话建立期间可能有多次的连接（connection）建立、释放过程。会话还有一个功能就是可以对 AT 的大概位置进行估计。

AT 发起登记的触发条件：（正常情况下，初始化之后 AT 马上就会自己发起登记）

- (1) 开机；
- (2) 子网改变；

开机登记后 AT 为了与 PDSN 建立 PPP 连接必须先与 AN 建立连接，以后若无数据传输，再释放与 AN 之间的连接。这意味着释放空口链路和 A8/A9 连接，PCF 与 PDSN 之间的 A10/A11 连接会在会话期间一直保持。

过程如下：



在 1xEV-DO 系统中，采用登记的方法对 AT 进行跟踪，有 2 种可能的登记处理方法：

- 基于 UATI Request 消息的登记：第一次开机的登记方式；（消息实例在后面会给出）
- 基于 RouteUpdate 消息的登记：会话建立之后的周期登记、或位置变换登记方式；（消息实例在后面会给出）

以上两种消息都由路由更新协议处理。

AT 捕获网络服务区后开始执行登记：首先给基站发送位置信息，方便网络进行正确下寻呼；之后 AT 会在反向接入信道上发送 UATI Request Message，来请求 UATI 地址的指配，每个 AT 被分配一个唯一的 UATI 地址，这个 UATI 地址跟 IP 地址类似，用于分组数据的正确传送。

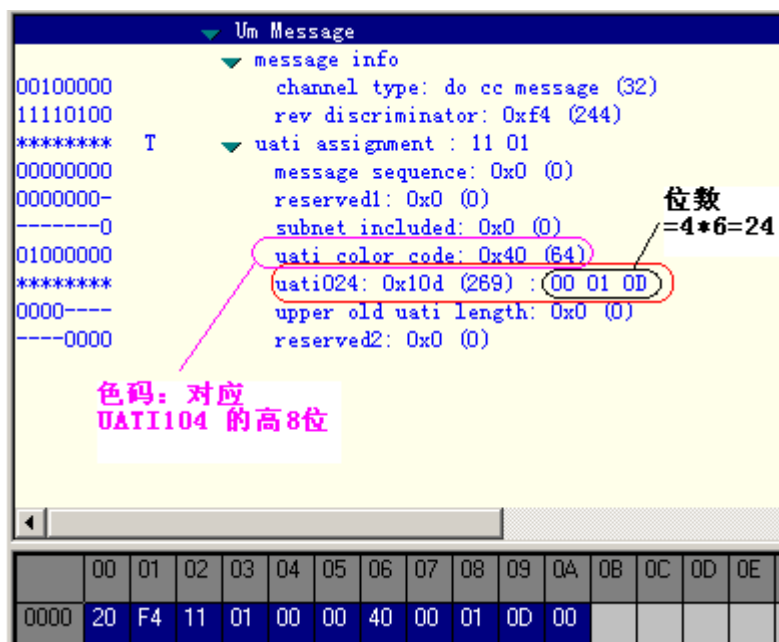
UATI Request Message: (CAIT 跟踪空口获取的消息实例)



1.2.1 UATI 请求消息

初始化结束后，AT 在首次发送 UATI 请求消息时，还没有从 AN 分配到任何标示地址，此时 AT 会挑选一个随机 AT 标识（RATI）（RATI 解释见附录 2），取代 UATI Request 消息中的 UATI。AN 认出 RATI 后，通过 AT 所在的子网指配一个 UATI 值给 AT。UATI 的指配由 IS856 会话层中的地址管理协议处理。UATI 是一个 128bits 的地址值，分为 UATI104 和 UATI24 两个部分。UATI104 是由 SectorParameters 消息（发送扇区信息给终端）发送给 AT 的，而 UATI24 是由 UATI ASSIGNMENT 消息发送的。

- UATIAssignment Message:

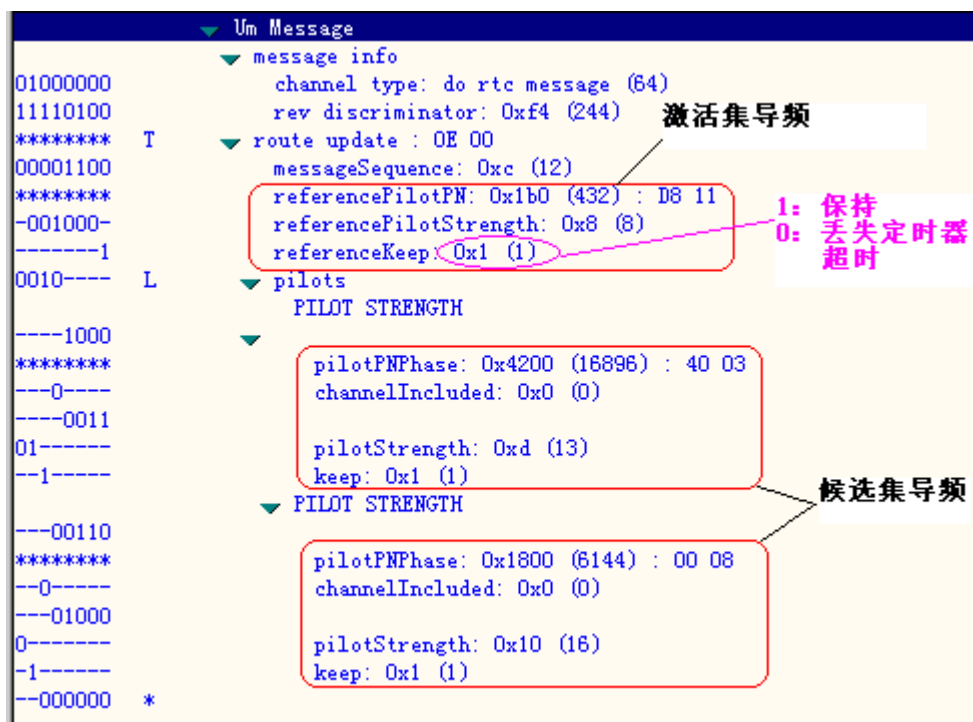


- RouteUpdate message

AT 发送 RouteUpdate 消息以通知 AN 目前的位置，并向它提供它周围无线链路状况的估计，在接入信道以及反向业务信道上发送。AT 发送 RouteUpdate message 遵循以下原则：

当 AT 移动到另一个子网时，通过 AN 控制信道上发送的色码来标识该子网，然后向新的网络发送 RouteUpdate 消息；

- RouteUpdate Message:



Um Message

message info

channel type: do rtc message (64)

rev discriminator: 0xf4 (244)

route update : OE 00

messageSequence: 0xc (12)

referencePilotPN: 0x1b0 (432) : D8 11

referencePilotStrength: 0x8 (8)

referenceKeep: 0x1 (1)

1: 保持 丢失定时器 超时

0: 丢失定时器 超时

PILOT STRENGTH

pilotPNPhase: 0x4200 (16896) : 40 03

channelIncluded: 0x0 (0)

pilotStrength: 0xd (13)

keep: 0x1 (1)

PILOT STRENGTH

pilotPNPhase: 0x1800 (6144) : 00 08

channelIncluded: 0x0 (0)

pilotStrength: 0x10 (16)

keep: 0x1 (1)

候选集导频

红色框表示激活集和候选集中的导频 PN。Keep: 1 表示 Drop Timer 没有超时。

当 AT 通过以下公式算出的 r 值大于 SectorParameters 消息中的 RouteUpdateRadius 域所提供的值时，AT 发送 RouteUpdate 消息；公式中 (x_L, y_L) 是为原 AT 提供服务的扇区的经纬度， (X_c, Y_c) 是目前为 AT 提供覆盖区域的扇区的经纬度。则 r 为：

$$r = \frac{\sqrt{\left[(X_c - x_L) \times \cos\left(\frac{\pi}{180} \times \frac{y_L}{14400}\right) \right]^2 + [y_c - y_L]^2}}{16}$$

- SectorParameters Message: (CAIT 跟踪空口获取的消息实例)



SectorParameters
Message.txt

当 AT 请求业务信道分配前，也会发 RouteUpdate message，告诉 AT 当前接入的网络状态。

1.3 空闲状态

当 AT 已捕获一个服务网络但是连接未打开时，所使用的过程和消息由空闲态协议来提供。此时 AT 处于关闭连接状态，空口资源没有指配给 AT，空闲状态包括以下四种：

- 非激活状态：该状态下，等待 **ACTIVE** 命令；
- 监视状态：该状态下，AT 监视控制信道，侦听寻呼信道，必要时更新从开销协议中接收到的参数。此状态下，AN 可以向 AT 发送单点广播分组；
- 休眠状态：该状态下，AT 关闭部分子系统以节省功率。休眠状态下 AT 不监听前向信道，并且不允许 AN 向它发送单点广播分组；
- 连接建立状态：AT 和 AN 建立连接。

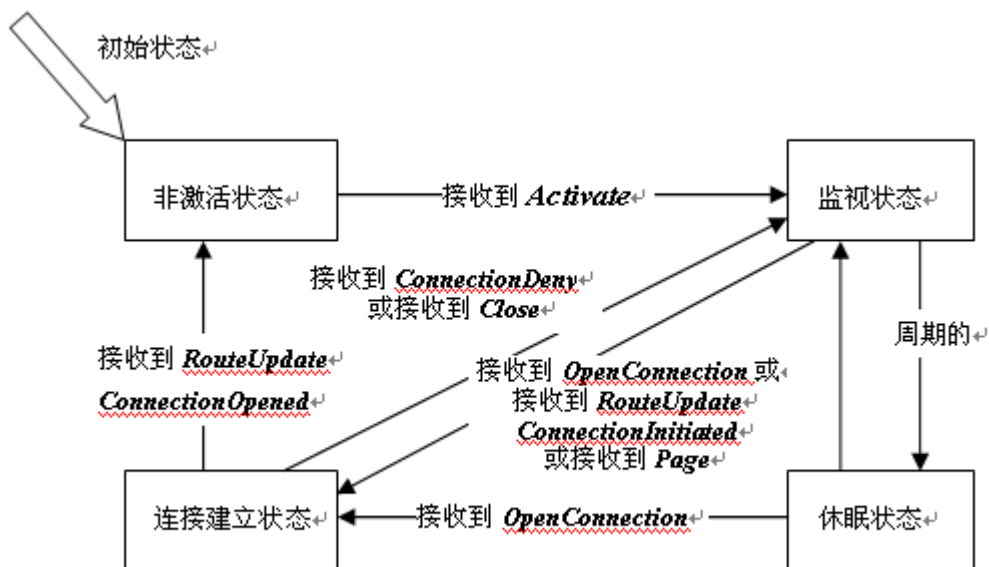


图1-1 空闲状态协议状态转化图 (AT)

为支持这四种状态，AT 支持下列操作模式：

- 连续操作模式：连续监视控制信道；
- 挂起操作模式：AT 连续监视控制信道一段时间，然后在时隙模式下操作。挂起模式遵循空中链路管理协议连接状态下的操作，并允许网络始发的快速连接；
- 时隙模式操作：AT 仅仅监听选中的时隙。

1.3.1 休眠状态

当 AT 处于休眠状态时，停止监听控制信道，并关闭部分处理资源以减少功率消耗，增加电池寿命；当接入网处于休眠态时，它被禁止向 AT 发送单点广播分组。

从前向链路的时隙结构看出，1/2 个时隙中，包括数据码片时隙、MAC 码片时隙、导频码片时隙，控制信道与业务信道共同占用数据码片时隙。

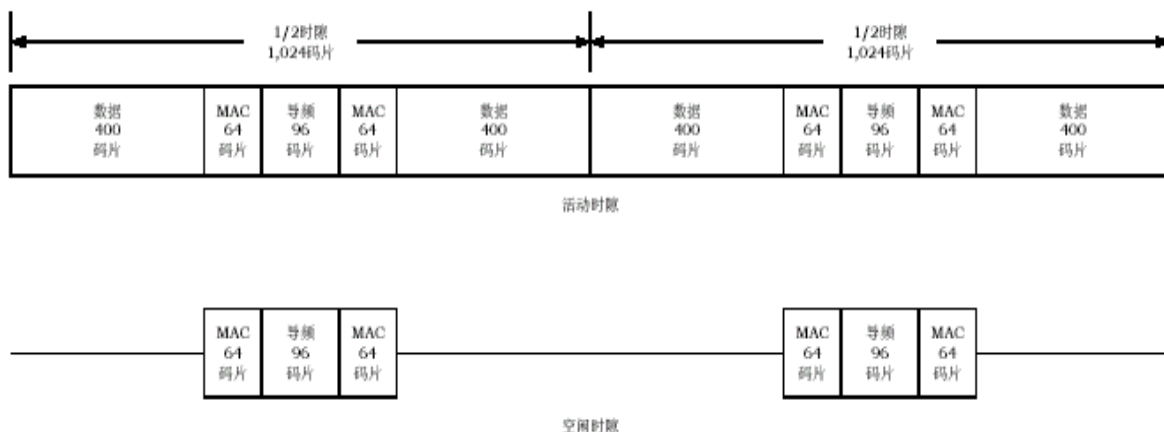


图1-2 前向链路的时隙结构

1.3.2 监视状态

当 AT 处于监视状态时，它连续监视前向控制信道；当 AN 处于监视状态时，它可以向 AT 发送单点广播分组。AT 处于监视状态时，从扇区参数消息的信道列表（参见前面的 SectorParameters 消息）中选择一个 CDMA 信道，如果没有列出信道，AT 使用它当前监视的信道；如果选择了一个新的 CDMA 信道，AT 就调频到该信道监听开销消息。

1. 监视状态下的前向控制信道

在监视状态下，AT 监视控制信道上的单点广播消息和广播消息，控制信道消息以 76.8kbps 速率（MAC Index=2）或者 38.4kbps（MAC Index=3）速率传输。前向控制信道上发送的消息又分两类：

(1) 单点广播消息：需要 AT 应答或者发起请求的消息：

包括 UATIAssignment 消息（需要 AT 以 UATISComplete 消息应答）和 TrafficChannelAssignment 消息（需要 AT 以 TrafficChannelComplete 消息应答）。

(2) 广播消息，包括：

- **QuickConfig Message:** 向 AT 通知一些重要的参数，包括：色码、前向业务信道 MACIndex 等；
- **SyncMessage:** 服务基站和网络信息，包括 AT 和基站的配套版本、扇区的 PN 相位、网络系统时间等；
- **SectorParameter:** 提供邻区信息、可用信道列表、地区时间偏置、经纬度等；
- **AccessParameters:** 向 AT 广播在接入网络时使用的参数等；
- **ReverseLinkRateLimit Message:** 指示 AT 可以使用的最大反向速率；
- **Redirect Message:** 将 AT 指向另一个 1xEV-DO 载波或者 IS2000 系统。

下面给出前五条消息的消息实例：

QuickConfig Message: SyncMessage: SectorParameter:
AccessParameters:



QuickConfig
Message.txt



Sync Message.txt



SectorParameters
Message.txt



AccessParameters
Message.txt

ReverseLinkRateLimit Message:



UnicastReverseRateLimit
Message.txt

AT 迁移到连接态：当 AT 需要建立连接、或者需要对寻呼进行应答、或者收到经由快速连接信道发送的 TCA（Traffic Channel Assignment message）消息时，AT 发送连接请求消息，进入连接建立状态。

2. AT 由监视态迁移到休眠状态

满足下列所有要求时，AT 可迁移到休眠状态：

- AT 在当前的控制信道周期内（5.12S）已经接收到至少一个控制信道的同步休眠包，且确定扇区参数消息是最新的；
- 进入监视状态后，AT 接收到与 AccessChannelMAC.TxStarted 对应的 AccessChannelMAC.TxEnded 指示；
- AT 没有接到挂起状态通知。

1.4 连接建立

1. 开连接状态和闭连接状态：

- 闭连接状态：当连接关闭时，AT 未分配任何专用空口链路资源，AT 和 AN 网络之间的通讯在接入信道和控制信道上进行。
- 开连接状态：当连接打开时，AT 能被分配前向业务信道、MAC 信道的反向功率控制子信道和反向业务信道。AT 和 AN 网络之间的通讯通过以上分配的专用信道和控制信道进行。

2. AT 和 AN 使用连接建立状态协议来执行正常的连接建立，支持以下两种连接：

- 正常连接（AT 发起的连接）：由 AT 发起 ConnectionRequest Message 去应答 Page Message 消息，来表示连接请求是由 AT 发起的（见下图）。

19	[A9] A9-BS Service Request	192.168.1.79->192.168.1.70
21	[Um] Page	CC
20	[A9] A9-BS Service Response	192.168.1.70->192.168.1.79
17	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
18	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
22	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
23	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
24	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
25	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
26	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
27	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
28	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
29	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
30	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
31	[Abis] Abis-DO-CCH Msg Transfer	BSC->BTS
34	[Um] RouteUpdate	AC
35	[Um] ConnectionRequest	AC
32	[A9] A9-Setup-A8	192.168.1.70->192.168.1.79
33	[A9] A9-BS Service Request	192.168.1.79->192.168.1.70

- 快速连接（AN 发起的连接）：由 AN 发送 TrafficChannelAssignment 消息（消息实例见后），来表示连接是由 AN 发起的。TrafficChannelAssignment 消息由最后收到的 AT 发送的一条 RouteUpdate 消息触发（见下图），无须 AT 发送 ConnectionRequest Message。快速连接不需要 AN 和 AT 之间进行寻呼消息和连接请求消息之间的信令交互，从而节约了连接建立时间。

27	ConfigurationComplete	FTC	244
28	ConnectionClose	FTC	244
29	ConnectionClose	RTC	244
30	ConnectionClose	RTC	244
31	RouteUpdate	AC	244
32	XonRequest	AC	244
33	XonResponse	CC	244
34	TrafficChannelAssignment	CC	244
35	TrafficChannelComplete	RTC	244
36	NeighborList	FTC	244
37	UnicastReverseRateLimit	FTC	244
38	LocationRequest	FTC	244
39	RouteIndicate	RTC	244

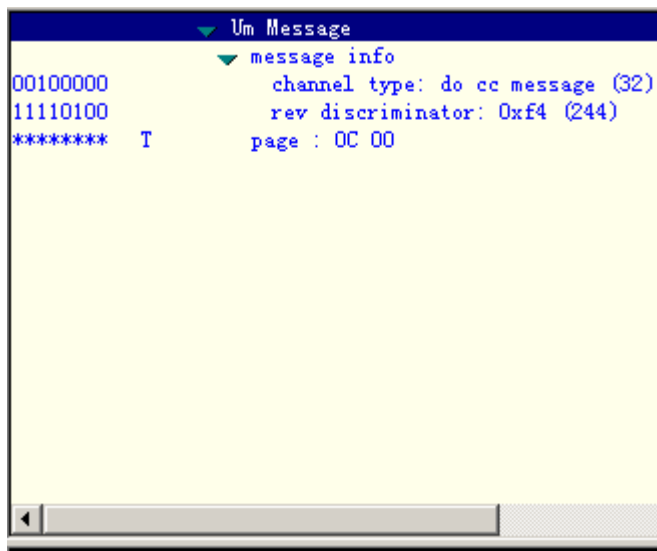
3. 下面详细讲解这两种连接方式下的消息流程。

(1) 正常连接

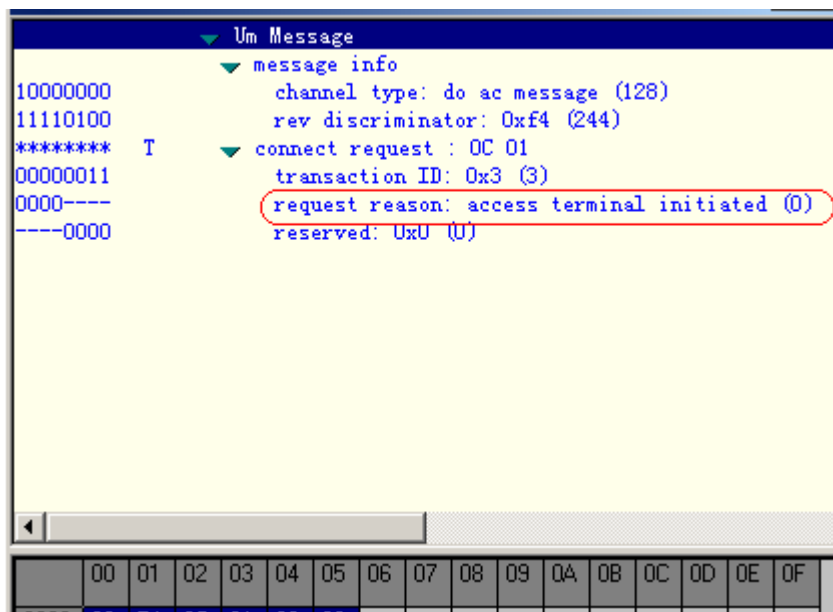
正常连接总是运行于 AT 主动的情况下。当 AT 想打开会话或者 AT 需要响应 Page 消息时，就会激发正常连接建立。当 AT 用 RouteUpdate 和 ConnectionRequest 消息去请求业务信道连接。

14	[Um] ConnectionClose	FTC
15	[A11] A11-Registration Reply	10.99.99.230->192.168.1.19
16	[Um] ConnectionClose	RTC
17	[Um] RouteUpdate	AC
18	[Um] ConnectionRequest	AC
19	[A9] A9-Setup-A8	192.168.1.10->192.168.1.19
20	[A9] A9-Connect-A8	192.168.1.19->192.168.1.10
21	[Abis] Abis-DO-BTS Setup	BSC->BTS
22	[Abis] Abis-DO-Connect	BTS->BSC

• Page Message:



• ConnectionRequest Message:



RouteUpdate 和 ConnectionRequest 消息一起捆绑在接入信道的 MAC 层分组中，消息交互如图 2-1：

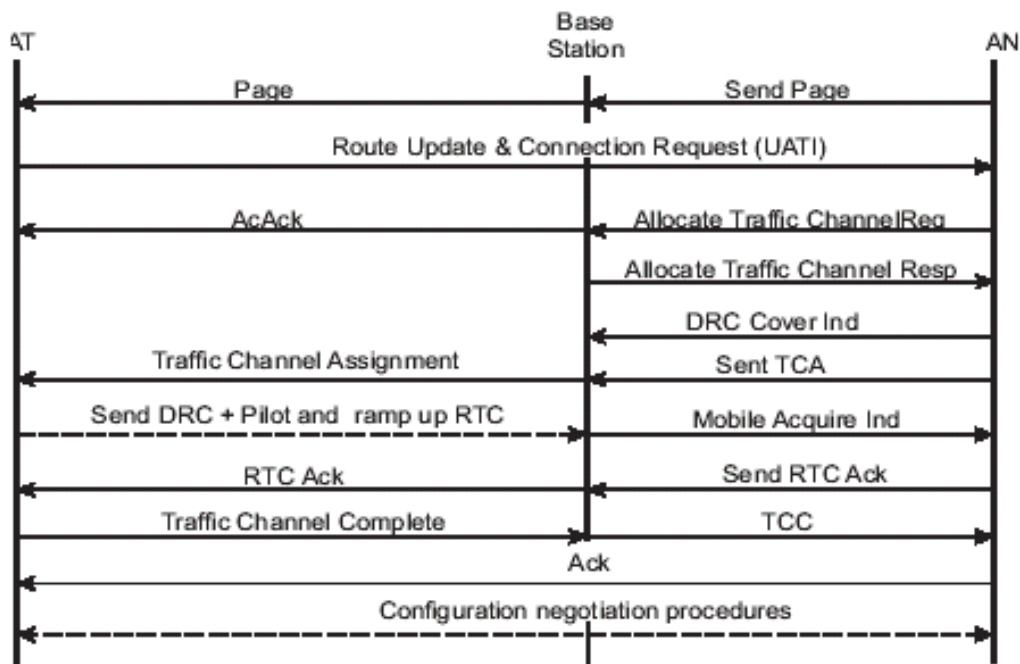


图1-3 正常连接建立流程图

注：能够发起正常连接的前提条件：AT 已经通过登记的方式获取了 UNTI 地址，如果连接的时候 AT 还没有分配到 UNTI 地址，那么就需要 AT 首先进行登记，由 AN

来分配 UNTI 地址。发起正常连接之前之所以要发 Route Update 消息，是因为 AT 要经由 RouteUpdate message 报告其位置。

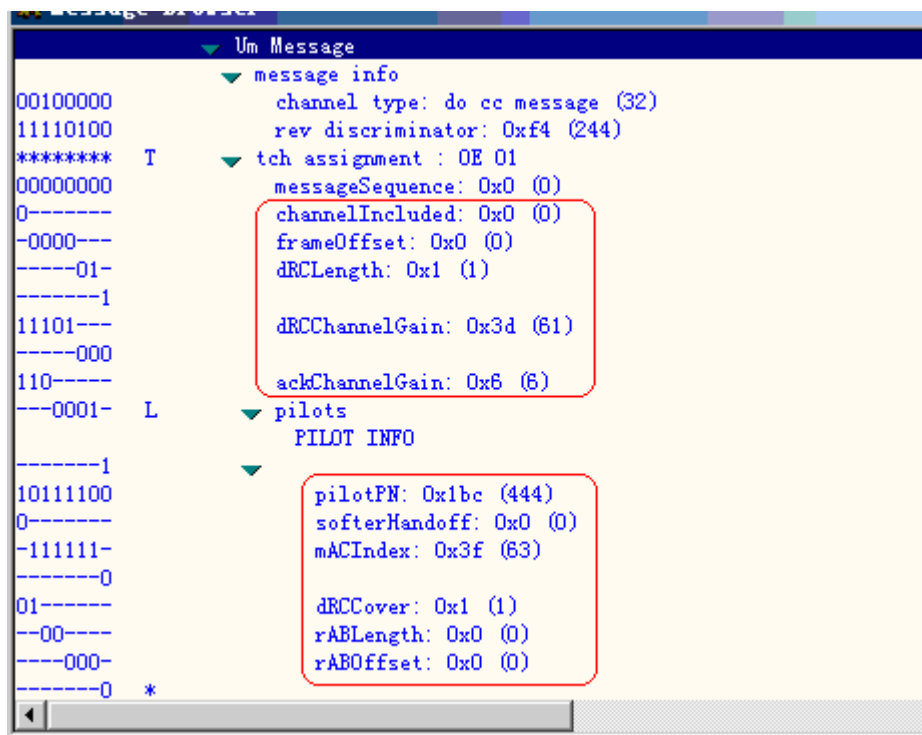
图 2-1 解释：

AT 处于空闲状态下时，基站给 AT 下发寻呼消息，指示 AT 发起请求建立连接，AT 发送路由更新和连接请求消息响应寻呼。RouteUpdate 消息中包括激活集和候选集中每个导频的 PN，导频强度，去掉计数器状态。

收到连接请求消息后，AN 给基站发送 Allocate Traffic ChannelReq 消息，基站给 AN 回 Allocate Traffic ChannelResp 消息。接着由 AN 发送业务信道指配消息 TAC（包含 DRC 和信道信息）给 AT，TCA 消息包括：DRC cover, length, channel gain, RAB（反向负荷指示，AT 根据当前的 RAB 值决定是否增降传输速率）等信息。收到 TCA 消息后，AT 的 MAC 层获取反向业务信道（RTC），并回复一个获得反向业务信道指示，此时 AN 和 AT 之间就处于开连接状态，AT 开始在指配的反向业务信道 RTC 上传输数据，发射功率为前向 RPC 信道的指示值。

TrafficAssignment 消息中有两类参数，一类是 AT 当前所在的 RTC 的参数，一类是 AT 服务扇区的参数。

- TrafficAssignment Message:



AT 当前所在的 RTC 的参数包括：

- Frame Offset: 帧偏置，用以指示 AT 发送反向业务信道的开始时间；

- **DRC Length**: 每帧中 AT 用于传输单个 DRC 值的时隙数;
- **DRC Channel Gain**: 指示在当前指配的业务信道上, DRC 信道功率增益相对于反向业务导频功率增益的比值;
- **Ack Channel Gain**: 指示在当前指配的业务信道上, ACK 信道功率增益相对于反向业务导频功率增益的比值。

服务扇区的参数包括:

- **MAC Index**: 在反向业务信道中指定的 Walsh 码;
- **DRC Cover**: 切换候选扇区的 DRCWalsh 码索引;
- **RAB Offset**: 扇区开始发送新的反向激活比特的时隙;
- **RAB Length**: 表示 AT 用于传输反向激活比特的时隙数。

表 1-1详细介绍了 TrafficAssignment 消息各个字段的含义:

表1-1 TrafficAssignment 消息参数说明

域名	长度 (比特)	含义	备注
Frame Offset	4	为使基站的处理延时达到最低,使用了帧偏置。基站覆盖区域内的所有用户的数据传输按照 FrameOffset 指示的时隙开始进行。	帧偏置随机指配给同一扇区载频的每个 AT。这样,不同 AT 的数据到达基站的时间不同。
DRC Length	2	规定了在每帧内 DRC 信息传送的重复次数。DRC 以每秒 600/DRCLength 的速率传输 (DRC 速率与 DRCLength 成反比)。 假设 DRCLength 取值为 1, 则 DRC 每秒传播 $600/1=600$ 次, 传播一次需要的时长为 $1/600s$; 所以每帧的 DRC 重复 16 次 (DO 帧长 $=26.67ms$)。	DRC Length 设置大时, DRC 信道的数据传输使用的功率较少, 引入的反向干扰较小, 增加了反向容量, 代价是影响前向链路吞吐量。 原因: DRC 信道的信息交互较慢, 基站不能及时进行数据速率调整以改变 AT 所处的 RF 环境: 在无线环境好时, 错失快速数据传输的机会; 在无线环境差时, 出现反复重传的情况。
DRC Channel Gain	6	指示在当前指配的反向业务信道上, DRC 信道功率增益相对于反向导频功率增益的比值。	
ACK Channel Gain	6	指示在当前指配的反向业务信道上, ACK 信道功率增益相对于反向导频功率增益的比值。	有效范围是[-3dB, 6dB], 单位 0.5dB。

域名	长度 (比特)	含义	备注
MAC Index	6 — 63	规范中定义了 64 个 MAC Index，代表 64 个 Walsh 码。其中 6~63 指配给反向用户的业务信道。MACIndex 值 2 用于 CC 以 76.8kbps 的数据速率，MACIndex 值 3 用于 CC 以 38.4kbps 的数据速率。MAC 4 标识 RA 信道。	每个激活用户分配一个唯一 MAC Index。这样，IS856 标准规定了每个扇区载频的最大激活用户数为 58。
DRC Cover	3	表示扇区相关的 DRC 覆盖索引	AT 监测 TCA 消息中的导频 C/I，估算出最好导频可支持的传输速率，并将这些信息在 DRC 信道上承载传输。DRC 信道上的 DRC Cover 指向 AT 认为前向信道质量最好的扇区。
RAB Offset	2	指示了 AT 激活集导频对应的扇区传送反向激活比特的开始时间，范围为 [0, 7]。	RAB 在 RA 信道上传输，由 MAC 标识 4 识别。每个邻区必须设置不同的 RAB 偏置。不同的偏置设置使得一个扇区降低上行数据速率后，允许其相邻小区在决定 RAB 传送前重新估算现有干扰影响。 对应的时隙数 $= \text{RABOffset} * \text{RABLength} \text{ (slots)} / 8$
RAB Length	3	规定了传输 RAB 的时隙数，范围为 {0, 1, 2, 3}。	对应{8, 16, 32, 64}个时隙数。

(2) 快速连接

快速连接运行于 AN 主动为用户重建一个业务信道的情况。当 AN 有待传数据要发送到 AT 时，快速连接节省了 Paging 和 ConnectionRequest 交互的过程。除了没有 Paging 消息、ConnectionRequest 消息和 RouteUpdate 消息外，快速连接的流程跟正常连接相同。如下图：

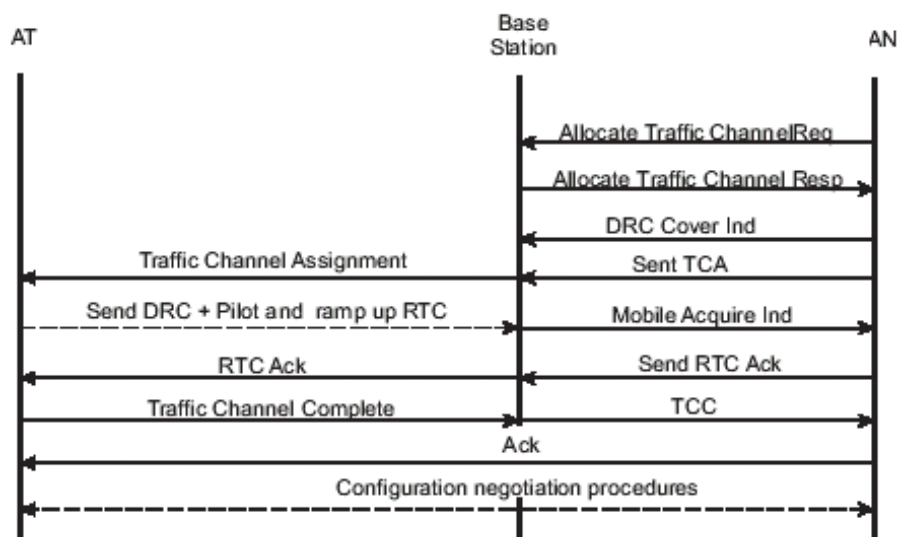


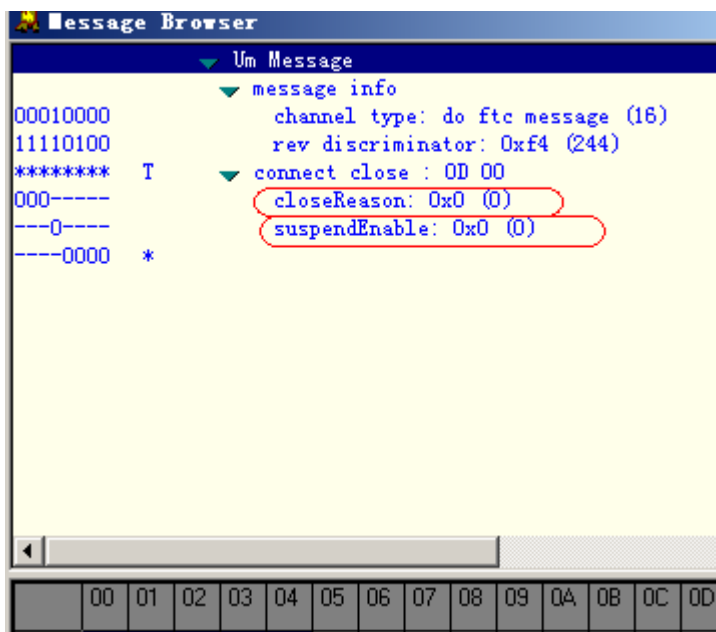
图1-4 快速连接流程图

为了执行快速连接，AN 必须得知 AT 当前位置的估计信息。如果 AT 处于挂起状态，AN 基于最后接收到 AT 的 RouteUpdate 消息，通过发送 TCA（TrafficChannelAssignment Message）消息触发快速连接。AT 在挂起期间连续监视控制信道，所以不会造成快速连接过程的延时；不过转入休眠态后，AT 进入时隙模式监听控制信道（隔 256 个时隙或 16 个帧监听一次，一个时隙 1.667us），可能会造成快速连接过程的延时。

1.5 挂起操作模式

触发 AT 挂起的因素有：在开连接状态下没有数据传输，AN 发送一条 ConnectionClose 消息给 AN，接着释放业务信道资源，AT 进入挂起模式。

- ConnectionClose Message:



消息解释：

- CloseReason :

0x00 正常关闭 0x01 Close Reply 0x02 连接错误

SuspendEnable: AT 允许转入挂起模式时候发送 0, 不允许设置 1; 挂起持续 80ms。

SuspendTime: 挂起时长，但是在我们的消息字段中无此值。

在挂起模式下，AT 连续一段时间监听控制信道，在一定时间内没有操作则进入休眠状态（时隙模式）。Connection Close 消息中指示了 AT 进入时隙模式前是否执行挂起模式。协议中规定此消息中还有挂起时长，单是在消息实例中找不到此字段。如果在挂起模式下 AN 有数据发送给 AT，则 AN 发送 TrafficChannelAssignment Message 而不是 Page message 给 AT（参考前面讲解的快速连接部分）。

1.6 监视小区导频信号强度

AT 除了监听控制信道消息外，还需要监测导频信号强度，并将之与其它扇区的导频强度相比较，以确保得到最好的小区服务，获取最高的数据传输速率。AT 监测 Neighborlist 消息中的导频集内的导频信号，当发现有更好的导频时发生切换。

- Neighborlist Message:

```

▼ Um Message
  ▼ message info
    00010000 channel type: do ftc message (16)
    11110100 rev discriminator: 0xf4 (244)
    ***** T ▼ nbt list : 0E 04
    10101--- count: 0x15 (21) ——— 邻区列表中的导频个数
               pliotPn
    -----110
    110000-- ▼ BIT9: 0x1b0 (432)
    -----10 ▼
    0001000- ▼ BIT9: 0x108 (264)
    -----0 ▼
    11011000 BIT9: 0xd8 (216)
    ***** BIT9: 0x10c (268) : 86 6D
    -1101101 ▼
    00----- BIT9: 0x1b4 (436)
    --000110 ▼
    000----- BIT9: 0x30 (48)
    ---00110 ▼
    0100----- BIT9: 0x64 (100)
    ----0110 ▼
    01100--- BIT9: 0xcc (204)
    -----010 ▼
    111100-- BIT9: 0xbc (188)
    -----10 ▼
    1100100- BIT9: 0x164 (356)
    -----1 ▼
    00000000 BIT9: 0x100 (256)
    ***** BIT9: 0x1ec (492) : F6 05
    -0000101 ▼
    00----- BIT9: 0x14 (20)
    --110000 ▼
    000----- BIT9: 0x180 (384)
    ---10100 ▼
    0100----- BIT9: 0x144 (324)
    ----1011 ▼
    10000--- BIT9: 0x170 (368)
    -----000 ▼
    100000-- BIT9: 0x20 (32)
    -----00 ▼
    1001100- BIT9: 0x4c (76)
    -----1 ▼
    10001100 BIT9: 0x18c (396)
    ***** BIT9: 0x9c (156) : 4E 16
    -0010110 ▼
    00----- BIT9: 0x58 (88)
               ▼ channel
               ▼ CHANNEL INFO

```

AT 监测 RF 环境中的所有导频信号强度，并将之进行分类：

激活集：当前服务于 AT 的所有扇区的导频集合（由导频信号的 PN 偏置和导频 CDMA 信道指定）。当连接打开时，指为 AT 指配了前向业务信道、反向业务信道和反向功率控制信道的所有扇区导频的集合；当处于空闲态时，激活集中只有一个导频。

候选集：不在激活集中，但 AT 接收到的导频信号强度（由导频 PN 偏置和导频 CDMA 信道指定）表明传送它们的扇区是可以被激活集包含的良好候选；

相邻集：不在上述两个集合中，但是可能被激活集包含的候选的导频集合（由导频 PN 偏置和导频 CDMA 信道指定）；

剩余集：除了包含在上述三个集合中的导频，目前信道指配上所有可能导频的集合。

从 Neighborlist 消息（遵从路由更新协议）中得到的导频归属于以上四种导频集合中的一类。当 AT 处于空闲状态时，通过 Neighborlist 消息获取相邻扇区的信息，消息中列出了邻区导频信道和它们的 PN 偏置以及 CDMA 信道号，AT 测量导频强度从而得到最好的服务小区。由于存在多径效应，实际导频信号强度是由多个多径分量合成的，为确保得到有效的多径分量合成，在 Neighborlist 消息中应该包含搜索窗信息。

AT 使用 SearchWindowActive 规定激活集和候选集的搜索窗口大小，使用 SearchWindowSize、SearchWindowRemaining 规定相邻集和剩余集的搜索窗大小。搜索窗以 chips 为单位，设置范围为[0, 15]，0 对应的窗口大小为 4chips，15 对应窗口大小为 452chips，搜索窗大小与小区半径、搜索多径的时间分配等因素有关，在大覆盖范围的扇区中使用小搜索窗口会导致导频搜索失败。

在空闲状态下，服务于 AT 的扇区导频是激活集中的唯一导频，AT 监测 RF 环境中处于同一频率的所有导频信号强度，执行如下操作：

如果候选集中的任一导频的 Eb/No 减去激活集导频的 Eb/No 超过 PilotCompare 值，就会发生空闲切换，用较大的 Eb/No 值对应的导频取代原激活集导频为 AT 服务；原激活集导频根据其当前的 Eb/No，进入其余三个集合之一；

为确保激活集或候选集中的导频能为 AT 提供可靠的服务，AT 将这些导频与 PilotDropThreshold 参数值对比，一旦有导频强度低于该值，就对该导频启动一个去掉定时器，如果去掉定时器期间该导频强度上升超过了 PilotDropThreshold 值，则停止定时器，否则等待定时器超时，将该导频移出当前导频集合。如果空闲状态下激活集中导频的去掉定时器超时，表明 AT 掉网。

1.7 会话配置协商

给 AT 分配了业务信道和 UATI 后，为打开 AN 和 AT 间的会话，需要执行一个配置协商过程。要打开 AT 与 AN 之间的会话，须确保执行了以下操作：

- UATI 地址已经成功指配给 AT；

- 业务信道已经建立。AT 为了建立会话，需要先进行一次建立连接的过程，会话建立起来后没有数据业务流会关闭连接；
- 成功协商了会话配置；
- 在 AT 和 PDSN 之间建立了 PPP 连接，此时，用户记录已经被创建并存储在 PDSN 中。

在单个会话期间，AT 和 AN 可多次打开和关闭一个连接。AT 因为去激活而进入休眠状态时，就会关闭连接，此时会话进入 dormant 模式，AT 会释放业务信道，但仍然维持 PPP 连接。

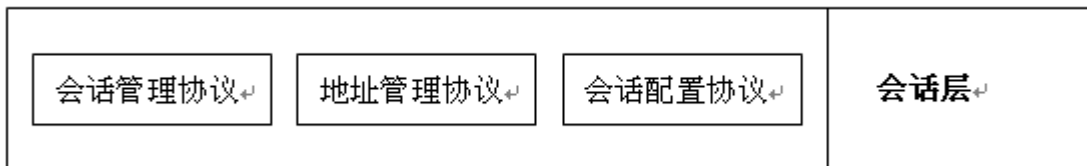
1.7.1 IS856 会话层协议介绍

会话层协议用于协商 AT 和 AN 间的会话。

会话定义为：AT 和 AN 之间维持的共享状态，包含信息如：

- AT 的单点广播地址 UATI；
- AT 和 AN 在空中链路上通信时使用的一系列协议；
- 这些协议的配置设置（如：鉴权密钥、连接层和 MAC 层协议参数等）；
- 当前 AT 的位置估计。

IS856 的会话层包含以下三种协议：



- 会话管理协议：控制地址管理协议和提供会话配置协议激活和去激活，它也提供 keep-active 的机制。
- 地址管理协议：管理 AT 的 UATI 地址的指配和维护 AT 的 UATI 地址；
- 会话配置协议：说明会话期间使用的协议，并为这些协议协商配置参数；为会话配置协商过程指明方法，通过 ConfigurationRequest 和 ConfigurationResponse 消息在 AT 和 AN 之间交互地进行参数的协商和配置。

1.7.2 会话配置协商过程

会话配置协议支持由 AT 始发的协商，也支持由 AN 始发的协商。AT 始发的协商，一般发生在手机开机建立会话时，很多参数在 AT 和 AN 间按缺省值配置；AN 始发的协商，AT 和 AN 执行由各个协商协议规定的配置过程。

为了跟踪协商参数，AN 设置了会话配置标志（SessionConfigurationToken），每当 AT 接入一个新的扇区，AT 将返回该扇区的会话配置标志。AN 如果发现返回的值与扇区处设置的不匹配，启动重新协商过程，协商后 AT 的标志将重新设置。

AT 和基站之间通过 ConfigurationRequest 消息和 ConfigurationResponse 消息的交互改变配置参数，发送 ConfigurationRequest 消息就启动了协商。配置协商在业务信道上进行，可以在会话开始且 AT 已经指配了业务信道后的任何时间发生。

AT 和 AN 之间会有很多 ConfigurationRequest 和 ConfigurationResponse 消息交互，协商完成的标志是发送 ConfigurationComplete 消息。下图为会话配置协商的过程：

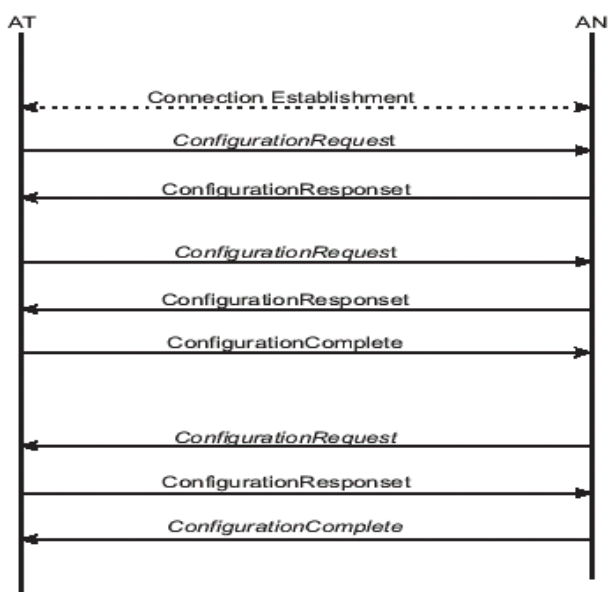
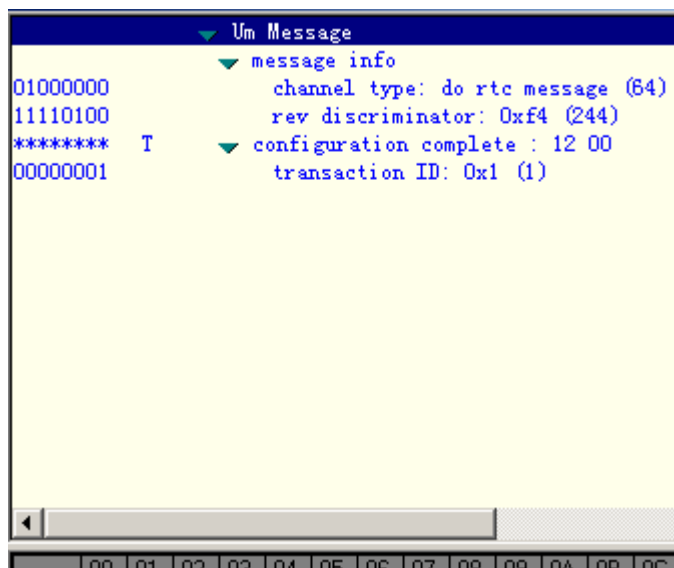


图1-5 会话配置协商流程

- ConfigurationComplete Message:



1.7.3 PPP 连接

会话配置协商之后，进入空闲态，发起连接会在在 AT 和 AN 之间开始建立 PPP 连接，PPP 的连接建立如下图：

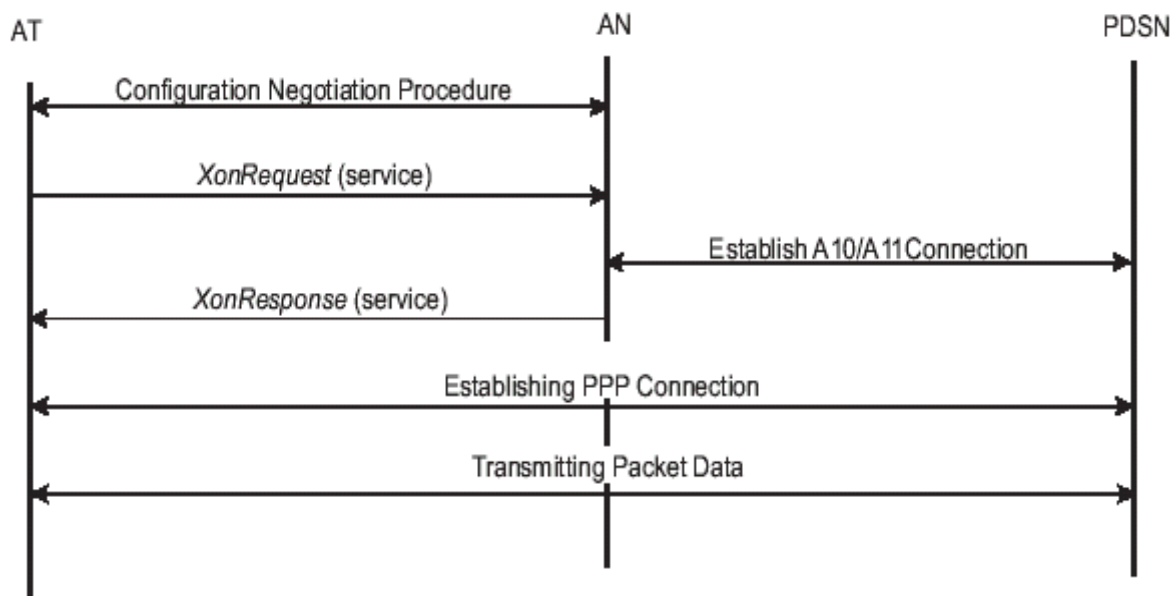


图1-6 建立 PPP 连接流程图

OMC 上跟踪到的消息流程如下图所示：

28	RouteUpdContigResponse	RTC	244
29	ConfigurationComplete	FTC	244
30	ConnectionClose	FTC	244
31	ConnectionClose	RTC	244
32	RouteUpdate	AC	244
33	XonRequest	AC	244
34	XonResponse	CC	244
35	ConnectionRequest	AC	244
36	TrafficChannelAssignment	CC	244
37	TrafficChannelComplete	RTC	244
38	NeighborList	FTC	244
39	UnicastReverseRateLimit	FTC	244

完成业务信道分配和会话配置协商之后，AT 发送 XonRequest 消息给 AN，该消息由流控协议生成（来自 IS856 应用层协议中的缺省分组应用协议）。流控协议提供缺省分组应用协议所要求的各种过程和消息，来为缺省分组应用提供流控制。

流控协议有两种状态：

- 闭状态：缺省分组应用不发送或接收任何 RLP 分组；
- 开状态：缺省分组应用能发送或接收 RLP 分组。

流控协议两种状态间的转换如下图：

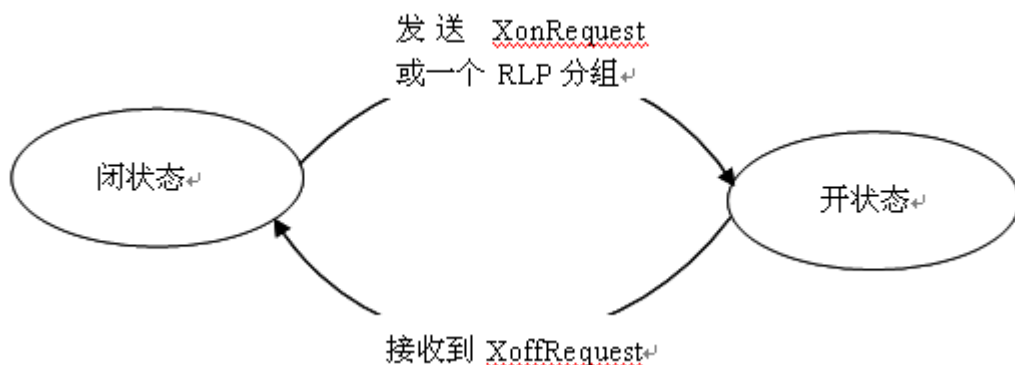


图1-7 流控协议状态图（AT）

当 AN 接收到 XonRequest 消息时，流控协议由闭状态转到开状态，开状态 AT 和 AN 之间的会话一直维持，直到 AN 收到 AT 发出的 XoffRequest 消息时，流控协议又转回闭状态。

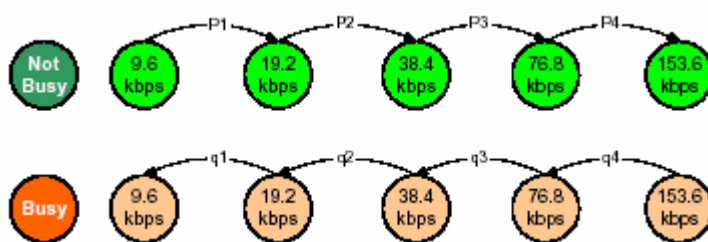
在 AN 收到 XonRequest 消息后 PCF 与 PDSN 建立 A10/A11 连接；连接建立后，AN 返回 XonResponse 应答，这个应答表明 A10/A11 的连接已经建立成功；A10/A11 连接建立成功之后，用户通过 IP 登陆到 PDSN，去 AAA 进行鉴权，鉴权成功后 PPP 连接建立，连接状态会一直维持到 AT 要求终结。

1.7.4 会话维持

维持 AT 和 AN 之间的会话需要有如下几种呼叫处理功能：

- (1) **Keep-Alive 功能**：AT 和 AN 周期性得进行 **KeepAliveRequest** 和 **KeepAliveResponse** 消息的交互以确保会话处于开状态。此处需解释一下 **KeepAliveTimer** 定时器，如果 AT 发出 **KeepAliveRequest** 消息后在 **KeepAliveTimer** 定时器设置的时间内没有收到 **KeepAliveResponse** 消息，会话将被释放，定时器的时长可以通过命令修改；
- (2) **休眠/Active 功能**：AN 监测到 AT 停止活动达一定时间，AT 进入休眠状态；
- (3) **调度**：通过给 RF 条件最好的 AT 分配前向链路时隙，来确保系统内所有扇区达到最大吞吐量；**FAIR 调度**：每个用户的 **DRC** 申请被保存在基站系统，并计算出一段时间内单个用户的平均 **DRC** 值，只有当此用户申请的 **DRC** 速率大于平均 **DRC** 时，此用户才能得到服务，否则不给予服务。
- (4) **速率控制**：通过传送反向负荷指示 **RAB** 来控制反向链路干扰。基站广播 **RAB** 给扇区下的所有 AT，告诉它们增加或降低发射功率；
 - **RAB=1**，以相应概率 **q** 降低速率
 - **RAB=0**，以相应概率 **p** 提高速率
 - 如果低于 **9.6k**，就不再降低
 - 如果高于最大限制速率，不再提高
 - 如果功率不足，不再提高

过程如下图：



- **切换**：AT 不断监测服务扇区和邻区的导频信号强度，对邻区信号进行估算，通过接受的数据速率控制值 **DRC** 来识别导频信号最强的小区，发现比当前服务小区好的扇区时，AN 允许 AT 进行切换。切换在 2.5 节有详细介绍。
- **功率控制**：由于 **1xEV-DO** 系统前向满功率发射，这里的功率控制指的是反向。反向功控 **RPC** 的目的：使 AT 在理想的 **PER** 下发射功率最小，从而使扇区容量达到最大。功率控制在第 3 章有详细介绍。

- 负荷控制：在 1xEV-DO 系统中，除了功率控制外，还需要进行负荷过载控制。在前向链路预算设计中，需要对于干扰影响留有一定的余量；反向负荷控制算法，控制因反向干扰而造成的系统性能下降。反向负荷控制不仅能提高反向链路的容量，而且对前向链路容量也有很大的影响，因为反向负荷控制算法维护了反向 MAC 信道（DRC 子信道和 ACK 子信道）的完整接收。如果 DRC 信道受到干扰，基站不能正确接收到 DRC 信道的可靠反馈，调度算法无法进行前向链路数据分组的正常传送和调度；同样，如果 ACK 信道反馈信息出错，会导致不必要的前向数据重传，最终浪费了前向链路容量。负载控制将在第 4 章有详细介绍。

下面仅介绍 keep-alive 功能：

2. keep-alive 功能

在 AT 的非激活期间，AT 和 AN 周期性的交互 KeepAliveRequest 和 KeepAliveResponse 消息以确保会话仍然处于开状态。KeepAliveRequest 消息可以由 AT 或 AN 发送。这些消息的交互很多时候在 AT 的休眠状态下进行，因此他们一般在接入和控制信道上传输；如果 AT 的业务信道没有释放，他们也可以在前反向的业务信道上发送。

在 KeepAliveTimer 参数规定的时间内，即使没有数据流传送，系统仍然维持会话开状态，但是在 KeepAliveTimer 时长内一直检测不到 AT 有数据传输时，系统也会将会话释放掉。KeepAliveTimer 参数的取值范围是[0, 65535]，单位是分钟，65535 分钟为 1092.25 小时或 45.5 天，0 表示没有该功能，IS856 中规定了其缺省值为 3240 分钟或 54 小时。

第2章 切换

2.1 前向链路切换介绍

在 1xEV-DO 系统中，由 AT 指示进行前向链路的切换：当 AT 判断某一扇区是最好的服务小区，能够提供比当前扇区更高的数据速率时，发起前向链路切换。AT 通过监测最好的扇区导频，估算该扇区可以支持的最高速率，接着 AT 通过 DRC 信道指示该扇区支持的速率值。然而在进行这些操作前，AT 必须确认目标扇区可以提供空口资源，这样可以立即进行数据流传输，避免不必要的延时。为保证这点，AT 需要连续监测其邻小区的导频信号强度，并选择有足够强度的导频对应的扇区作为切换候选小区，通过 AN 给目标扇区分配业务信道和空口资源，完成切换。

2.1.1 导频集管理

1. 导频集

在空闲状态下，AT 跟踪当前扇区的导频和邻区导频的信号强度，将它们划分为激活集、候选集、相邻集、剩余集（参见 1.6 节内容）。

AT 维护四个导频集，而 AN 仅仅维护激活集，AN 通过 TrafficChannelAssignment 消息来更新 AT 的激活集。

当 AT 处于空闲状态时，激活集导频是目前 AT 正在监视的控制信道相关的导频。当 AT 处于开连接激活状态时，切换经历以下几个步骤：（1）AT 持续监测其所有邻区的导频强度得出切换候选小区；（2）这些激活集中的切换候选小区连同它们的 PN 偏置信息通过 RouteUpdate 消息上报 AN；（3）AN 给 AT 指向的扇区分配资源后，该扇区导频的 PN 偏置进入 AN 维护的激活集，并通过 TrafficAssignment 消息指示更新 AT 的激活集；（4）AT 根据它的 DRC 信道指示去执行切换。

2. 导频去掉定时器维持

对于每个导频，AT 维持一个去掉计数器。当 AT 分配了业务信道后，根据 DynamicThresholds 值启动一个静态或动态的去掉计数器，确保导频集中的导频紧跟 RF 环境的变化。

DynamicThresholds 为 0 时（静态去掉定时器），AT 为激活集和候选集中每个强度低于 PilotDrop 值的导频启动一个导频去掉定时器。定时器超过 PilotDropTimer 时，

AT 设置定时器为超时。若定时器超时前导频强度变得高于 PilotDrop 值，则 PN 保持在现有的导频集合中，重启并禁止定时器；否则，将该导频 PN 从当前的导频集合中移出。

DynamicThresholds 为 1 时（动态去掉计时器），对于候选集中的导频处理跟 DynamicThresholds 为“0”时相同；但是对于 激活集中的导频，则除了用到 PilotDrop、PilotThreshold 和 PilotCompare 外，还需要以下 4 个参数决定导频集合的变化：

- (1) PilotAdd: 信号门限值，如果非激活集的导频强度高于本门限值时，AT 通过 RouteUpdate 消息，请求 AN 将这个导频的 PN 偏置纳入激活集；
- (2) Softslope: 软切换斜率，用于决定动态软切换门限；
- (3) Addintercept: 用于决定动态软切换的加入门限；
- (4) Dropintercept: 用于决定动态软切换的去掉门限。

当使用动态的去掉定时器时，根据激活集中导频的综合信号强度以及 PilotAdd 和 PilotDrop 参数对加入和去掉门限进行调整。下图为动态导频去掉门限（Eb/No）随激活集信号质量（PS_i）的变化曲线：

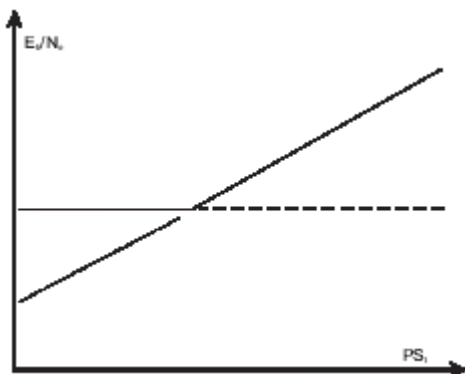


图2-1 动态导频门限随激活集信号质量变换曲线

AT 将激活集中的导频按照信号强度进行排序， $PS_1 < PS_2 < \dots < PS_A$ 。如果导频强度 PS_i 满足以下不等式，则 AT 启动导频去掉定时器：

$$10\log_{10}(PS_i) < \max\left(\frac{SoftSlope}{8} 10\log_{10} \sum_{j>t} PS_j + \frac{DropIntercept}{2} - \frac{PilotDrop}{2}\right)$$

$$t = 1, 2, \dots, N_A$$

如果定时器超时前，相应导频不再满足上述不等式，AT 会重启并禁止定时器，该导频仍保留在激活集中；否则将该导频移出激活集。

3. 激活集管理

(1) 激活集加入/移出导频信令流程：

当一个导频被添加到激活集或者从激活集中移出时，AT 通过 RouteUpdate 给相应的扇区上报无线链路状态的这一变化。在 RouteUpdate 消息中的信息包括导频偏置，导频强度，以及激活集候选集中每个导频的去掉定时器状态（参考前面的 RouteUpdate Message 消息实例），这利于对激活集进行合理调整。

下面讲解导频从激活集加入或者去除时进行的信令交互。下图为当前接收 sector1 服务的 AT 需要增加目标 sector2 导频时的消息交互：

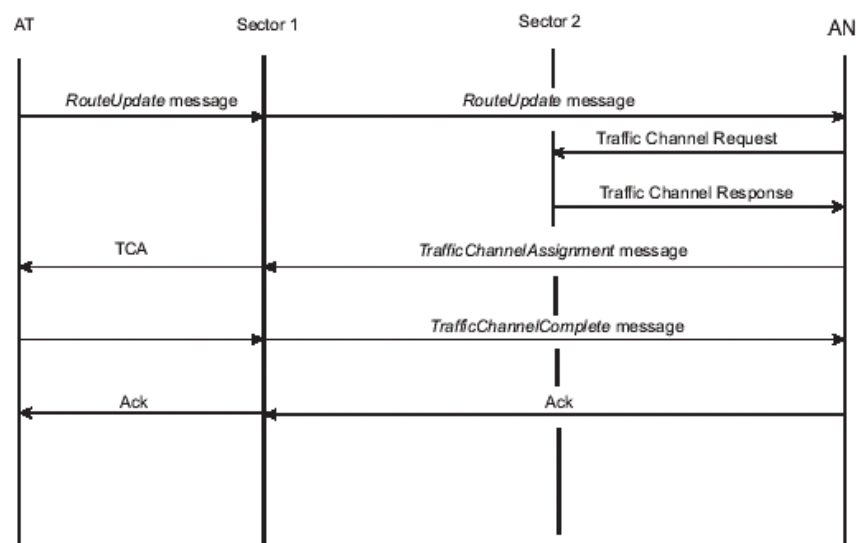


图2-2 激活集中加入一个导频流程图

如果正在接受 sector1 服务的 AT 试图将 sector2 的导频加入激活集，它发路由更新消息（RouteUpdate）到 sector1 再到 AN。AN 需要给 sector2 分配业务信道，以便处理 AT 将其 DRC 指向 sector2 的数据流。sector2 获得业务信道后，将应答发回。如果 RouteUpdate 消息中要求从激活集中去掉导频（看 Keep 值，Keep=0 表示去掉定时器超时），AN 将要求 sector2 释放业务信道；收到分配或释放业务信道的应答后，AN 将从激活集中添加或去除 sector2 的导频偏置，并且通过 sector1 发送一条 TCA 消息到 AT。TCA 消息中包含了 RouteUpdate 消息里面指示的要增加或去除的导频信息。AT 收到 TCA 消息后，用 TCA 消息里指示的导频取代目前激活集中的内容，并回 Traffic ChannelComplete 消息作为应答。

这个过程和正常建立业务信道的区别在于：切换消息流程中有 AN 给目标 Sector 发送的 Traffic Channle Request 消息以及响应消息 TrafficChannelResponse；而正常的业务信道建立过程没有这两个消息。

(2) 激活集中的导频增加或删除判决条件：

由以下条件促使一个导频从激活集中移出：

- 激活集中有导频信号强度低于 **PilotDrop** 时，触发去掉定时器，在去掉定时器超时前强度仍未能恢复到 **PilotDrop** 以上的导频 PN 将被从激活集中删除；
- 一个导频被添加到激活集，使激活集中的导频个数超过 6 个，则强度最小的导频被移出激活集。

当 **DynamicThresholds** 为 “0”，满足以下条件时导频被加入激活集：

- 候选集中的导频强度比激活集中的导频大于 **PilotCompare** 时。

当 **DynamicThresholds** 为 “1”，满足以下任一条件时导频被加入激活集：

- 相邻集或剩余集的导频强度满足以下不等式：

$$10\log_{10}(PS) > \max\left(\frac{SoftSlope}{8}10\log_{10}\sum_{j \in AS} PS_j + \frac{AddIntercept}{2} - \frac{PilotDrop}{2}\right)$$

$j = 1, 2, \dots, N_A$ ；AS 为激活集。

- 候选集中的导频强度满足以下不等式：

$$10\log_{10}(PS) > \frac{SoftSlope}{8}10\log_{10}\sum_{j \in AS} PS_j + \frac{AddIntercept}{2}$$

- 候选集管理

候选集中的最大导频数目为 6 个。当相邻集或剩余集中的导频强度大于 **PilotAdd** 时，可以进入候选集；激活集中的导频在一定条件下也会移到候选集：

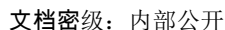
- 当 **DynamicThresholds** 为 “0” 时，激活集中的导频强度小于 **PilotDrop**，触发导频去掉定时器。该导频去掉定时器超时，导频强度仍在 **PilotDrop** 以下，则该导频从激活集中移出到候选集；
- 当 **DynamicThresholds** 为 “1”，激活集中的导频强度小于 **PilotDrop**，触发导频去掉定时器。如果在整个去掉定时器周期内，该导频信号强度高于 **PilotDrop**，但仍然满足以下不等式时，从激活集移出到候选集。

$$10\log_{10}(PS) < \max\left(\frac{SoftSlope}{8}10\log_{10}\sum_{j \in AS} PS_j + \frac{DropIntercept}{2} - \frac{PilotDrop}{2}\right)$$

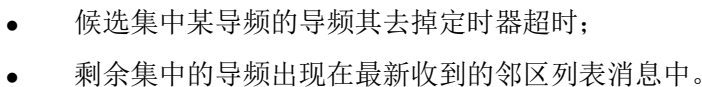
$j = 1, 2, \dots, N_A$ 。

满足以下任意条件，从候选集中移出导频：

- 导频强度增加到足以加入激活集；
- 导频强度下降足以移出候选集；



- 相邻集中导频的最大数目为 20 个。当 AT 进入开连接状态，在前向业务信道上收到的邻区列表消息中包含了相邻集的信息（参见前面介绍的 **NeighborList Message** 消息实例）。相邻集信息包含：邻区的 PN 偏置，CDMA 信道号，导频搜索窗长度，搜索窗偏置（见下图）。当 AT 需要进行邻区更新时，发送邻区列表消息。



导频从相邻集中删除的条件为：

- 剩余集中的导频被加入到激活集或候选集时；
- 相邻集中某导频的 AGE 计数器超过 NeighborMaxAge，并且由于新的加入使相邻集中的导频数目超过 20。

AGE 计数器

AT 为相邻集中的每个导频维持一个计数器 AGE，指示导频在相邻集中的驻留时间。

AGE 计数器的初始值取决于该导频加入相邻集前所属的集合：

从激活集或候选集中到来的导频，其 AGE 计数器为 0；

从剩余集到来的导频，其 AGE 计数器为 NeighborMaxAge；

AT 初始化相邻集时，设置该集合中每个导频的 AGE 计数器为 NeighborMaxAge。

每收到新的邻区列表消息，AT 将 AGE 计数器按照以上规则设置。

2.1.2 虚拟软切换

在 1xEV-DO 系统中，尽管 AT 监测激活集中的所有导频强度，但在前向链路上，AT 只会选择激活集中信号最强的扇区作为自己的服务扇区。AT 用 DRC 掩码（DRC cover）指定发射扇区，DRC 的值用于指定具体的传输速率。最强扇区随着 AT 的移动而不断发生变化。当 AT 选择将其 DRC 指向新扇区，并且新扇区准备好空口和数据连接资源时，发生的切换过程称为虚拟软切换。

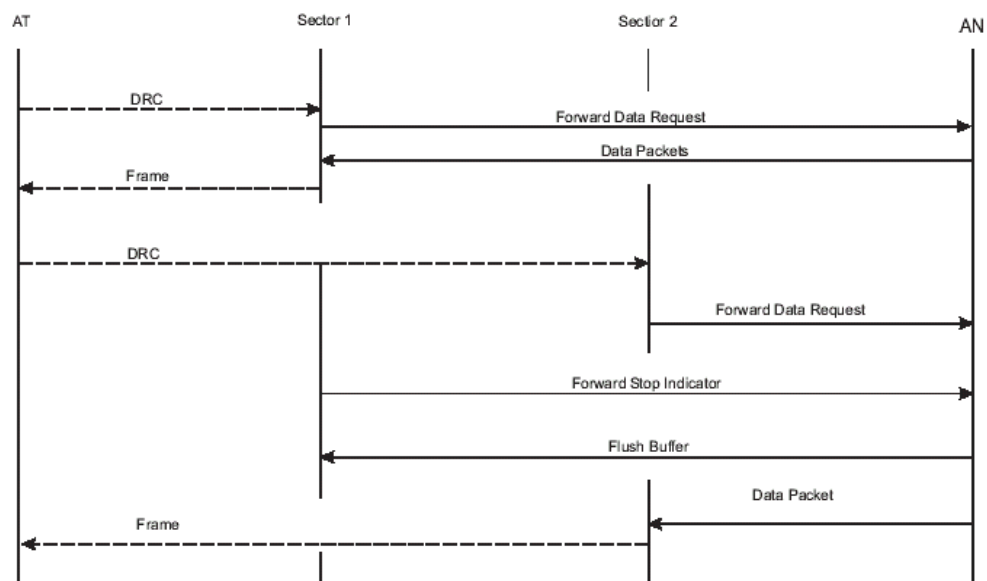


图2-3 图 2-2 虚拟软切换过程

上图流程解释：

当 AT 将其 DRC 指向 sector1 时，sector1 发前向数据请求给 AN，AN 开始数据分组的传送。当 AT 将其 DRC 指向 sector2 时，sector2 发前向数据请求给 AN，紧接着 sector1 给 AN 发前向停止指示，以确认最后一帧的传送。收到 sector2 的前向数据请求后，AN 发送一条 Flush 命令给 sector1，并开始给 sector2 发送分组数据。

2.2 反向链路切换介绍

在 1xEV-DO 系统中，软切换和更软切换仅仅发生在反向链路上。反向链路的软切换和更软切换消息在上述激活集管理中已有论述。

更软切换分支其功率控制比特在基站进行合并。

AN 从软切换分支中收到的相同数据分组被应用层的 RLP 协议丢弃，RLP 执行反向链路上的帧选择。当 AT 处于软切换状态，所有的反向链路分支将给 RLP 发送数据帧，当 RLP 收到相同的帧时，会选择成功通过 CRC 校验的帧，并将其它帧丢弃。

当 AT 处于 dormant 状态时，支持相同 PDSN 不同 AN 之间的切换；此时经由 A13 接口交换会话信息，由目标 AN 给 AT 分配新的 UATI。

2.3 1xEV-DO 和 1x2000 系统间的切换

双模 AT 支持在 1xEV-DO 和 1x2000 系统内的数据发送和接收，以及在 1x2000 系统中的语音呼叫。

在两个系统间的转换由双模终端主导执行，网络侧没有卷入其中，事实上，网络侧并没有意识到这种转换。

例如，一个双模 AT 在 1xEV-DO 系统中进行数据传输，当收到 1x2000 系统的语音寻呼时，如果用户选择接听语音呼叫，AT 会转到 1x2000 系统接听。而 1xEV-DO 系统并不知道 AT 已经离开，因为 AT 并不发送任何信息给它。1xEV-DO 系统最终会发现反向链路丢失或 Dormant 定时器超时，于是释放连接。1x2000 系统也不知道 AT 是断开了与 1xEV-DO 系统的连接才接听电话的。

双模终端在 1xEV-DO 系统的时隙模式下时可以收到 1x2000 的寻呼消息。AT 在特定的时隙内监听 1x2000 的寻呼消息。如果 AT 处于 1xEV-DO 的业务信道上，可通过发送一个空的 DRC 来指示它正监听 1x2000 的寻呼信道，不打算接收任何来自 1xEV-DO 系统的数据。如果 1x2000 系统没有发给 AT 的寻呼消息，AT 回到 1xEV-DO



系统中通过非空的 DRC 信道指示恢复数据连接。如果收到发给 AT 的寻呼消息，AT 可以选择在 1x2000 系统中完成呼叫。

第3章 功率控制

在 EVDO 协议中，前向链路采用时分加码分的复用方式，一直是满功率发射，不存在功率控制。而反向采用的是与 1x2000 系统中类似的码分工作方式，所以 1xEV-DO 系统中的功率控制是针对反向链路而言，以减少干扰和增大容量。有两种算法用于控制 AT 的发射功率，即开环功控和闭环功控。

3.1 开环功率控制

开环功控基于 AT 接收到的信号总功率，来决定 AT 的发射功率。不在软切换状态下时，AT 的接收功率与 AT 到基站的距离直接相关。收到的信号强，说明 AT 离基站很近，或者 AT 与基站之间存在好的无线传播路径，这时 AT 可以以较小的功率进行数据传输，而在基站侧仍然可以获得较好的 PER。通过降低 AT 输出功率，AT 带给本区域内其它用户的干扰也减少了。

开环功控对初始连接建立，以及阴影衰落引起的大路径损耗很有用。但是，开环功控会带来过度补偿，所以开环功控速度相对慢些。闭环功控速度较快，可以修正开环功控不足，从而保证系统良好稳定运行。

1xEV-DO 系统中，反向链路导频信道的初始功率均值等于开环功率控制时最后一个接入探针的平均功率。

3.2 闭环功率控制

闭环功控由外环和内环组成。反向链路外环功控的主要目的是保持反向业务信道的可靠性，通过连续调整反向内环功控中的功率控制阈值（PCT，Power Control Threshold），在反向链路上获得理想的误帧率。

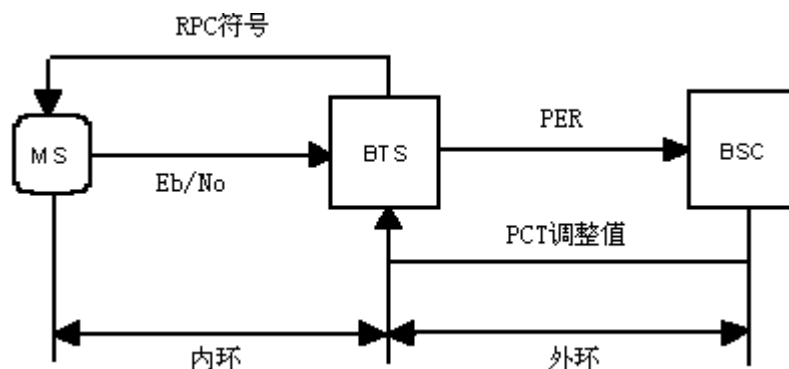


图3-1 1xEV-DO 系统的闭环功率控制图

3.2.1 外环功率控制

AT 在反向 Data 信道上进行数据传输，并通过 RRI（Reverse Rate Indication）信道将传输速率通报基站。RRI 与导频信道时分复用，满功率发射以确保 RRI 的有效可靠传输，并能被基站正确解调。当数据传输时，激活集 PN 对应的扇区载频接收数据并对每个数据帧进行解码。

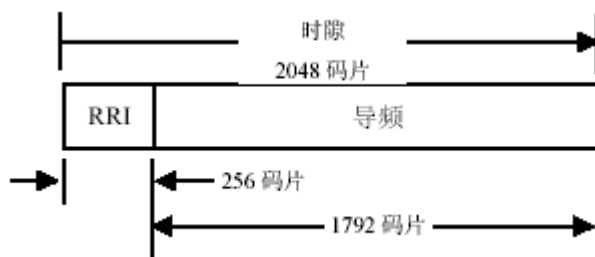


图3-2 反向导频信道和 RRI 信道的时分复用

激活集中的每个扇区根据从 AT 接收到的数据，判断每个数据帧的质量好坏。外环功率控制算法对接收帧质量（好帧/坏帧）进行判断，得出应调整的 PCT 值。

当 RRI 指示传输速率不为 0，而基站又不能证实接收帧为好帧时，算法会放弃该坏帧。当接收帧能正确解出，则算法断定该帧数据为好帧。尽管 RRI 数据是满功率传送，当没有数据传输时 RRI 符号被基站解错，做出坏帧判断的可能性也很小。此时，被解错的 RRI 符号会导致基站试图证实一帧的质量好坏。

当反向链路处于软切换状态，一个扇区的接收帧质量报告未必与激活集中其它扇区报告的相同。外环控制算法根据激活集中每个扇区报告的接收帧质量计算最小的 PCT 调整值，这个值用于该软切换激活集中所有扇区，并且被反向内环功率控制算法用以获取反向链路的目标误帧率。

3.2.2 内环功率控制

反向内环功率控制算法根据 PCT 值决定反向链路可接受的目标帧错率，并通过前向 RPC 信道给 AT 连续发送“0”（上升）和“1”（下降）比特。

如果接收质量好于目标值，传送 RPC 比特“1”，通知 AT 降功率。如果接收质量差于目标值，传送 RPC 比特“0”，提高 AT 发射功率。AT 调整功率步长为 1dB 或 0.5dB。如果执行更软切换，同一基站的不同扇区传输相同的 RPC 值。在每个包含功率控制比特的时隙中，AT 应提供相同 RPC 信道的分集合并，并从相同 RPC 信道的每个时隙最多获得一个功率控制比特。如果所有得到的 RPC 比特都是“0”，AT 提高其输出功率；如果任一个 RPC 比特为“1”，则 AT 降低它的输出功率。

3.2.3 RPC 信道和 DRCLock 信道

RPC 信道和 DRCLock 信道是时分复用的，它们在相同的 MAC 信道上传输。如果 AT 发送 DRC 请求，基站通过 DRCLock 信道告诉 AT 其 DRC 信号是否被解调及正确接收。如果 AT 收到其 DRC 指向的扇区的 DRCLock 比特为 0，则 AT 停止其 DRC 指向该扇区。不论 DRCLock 信道是否传送，RPC 信道是传送的。DRCLockPeriod 规定了在前向 MAC 信道上传输的两个连续 DRCLock 比特传输间的时间间隔。

因为 RPC 信道和 DRCLock 信道在 MAC 信道上时分复用，RPC 的数据速率为 $600 \times (1 - 1/\text{DRCLockPeriod}) \text{bps}$ 。每个 RPC 符号应在一个时隙中被发送 4 次，每次以 64 个码片的突发方式发送。一个突发应紧靠每个时隙中导频突发的前和后被传输。

第4章 反向负载控制

在没有降低服务质量的前提下，链路预算中内含的负荷因子提供了一个空间去处理干扰的波动。除了在链路预算中增加干扰因子来估算性能下降外，系统的过载控制提供了由于干扰带来的性能下降的检测手段。

负荷控制主要包括两个方面：速率控制和负荷过载控制。

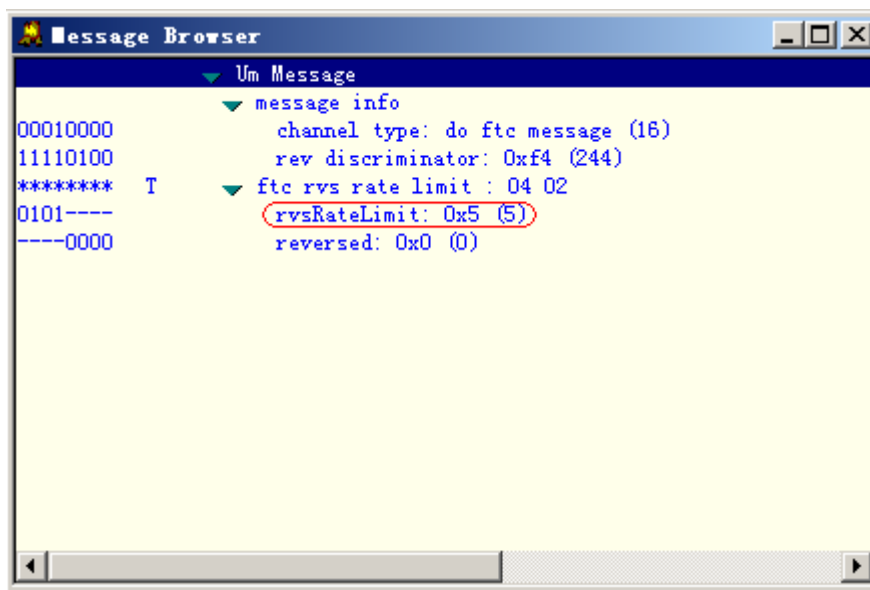
4.1 反向速率控制

EVDO 协议中提供了几种实现反向速率控制的方法，包括利用 **RateLimit** 消息和利用反向激活比特 **RAB**。

4.1.1 RateLimit 消息

AT 接收到的 **BroadcastReverseRateLimit** 消息和 **UnicastReverseRateLimit** 消息中都包含有 **RateLimit** 信息。其中 **BroadcastReverseRateLimit** 消息被 AN 用于控制扇区下所有 AT 反向链路的传输速率；而 **UnicastReverseRateLimit** 消息被 AN 用于控制特定 AT 反向链路的传输速率。

UnicastReverseRateLimit Message:



rvsRateLimit 可以取值为：1、2、3、4、5、0xf，分别代表反向速率固定为 9.6k、19.2k、38.4k、76.8k、153.6kbps、不限制。

DO 系统设计成允许 AT 按照反向激活比特 RAB 的值提高或者降低速率。反向激活比特 RAB 以时隙为周期传送，提供比 BroadcastReverseRateLimit 消息更为快速的速率控制机制。系统将各种速率之间的转移概率以及反向最高速率限制值发送给 AT，然后，系统就根据反向接收总功率等因素，通过判断系统是否过载，设置反向激活比特 RA：“1”代表过载，“0”代表未过载。AT 解调 RA，如果过载，就根据转移概率降低速率，如未过载，则根据相应的转移概率提升速率，最大速率受 RateLimit 值限制。

4.2 反向负荷过载控制

反向过载控制也可以通过限制扇区内的最大用户数得到，不过这属于缓慢的控制。目前的反向负荷控制主要在于控制 RA 值的设置。通过对系统内的 RSSI 上升值或者 CSM5500 对扇区负荷的估算，将之与对应的门限值对比，来进行 RA 的设置。

4.2.1 CSM5500 算法介绍——扇区负荷估算

CSM5500 对最近的 16 个时隙内，激活集中所有 AT 进行的每个分组传输的数据速率（根据 RRI 的信道指示）进行观察，其中包括那些不能被（正确接收了 RRI 的）扇区正确接收的分组。在此基础上，CSM5500 提供对扇区负荷的估算，为每个扇区计算负荷 Y_a ：

$$Y_a = \sum_{k=1}^M f(DataRate_k) \frac{E_{cp}}{I_o}$$

其中 $f(DataRate)$ 是从一个 AT 接收到的总功率与导频功率的比值； E_{cp}/I_o 表示扇区的导频信道码片的平均功率与总的接收功率谱密度的比值。

CSM5500 对每个扇区的负荷进行判断，如果 $Y_a >$ 预设的门限值，则 $RAB=1$ ，否则 $RAB=0$ 。得到 RAB 的值后，在 MAC 信道上发送。该 RAB 在 $RABLength$ 个连续的时隙上传输，开始时隙由 $RABOffset$ 指定。AT 收到 RA 值后，结合速率转移概率，进行速率的调整。

4.2.2 I_o/N_o 测量（总的接收功率谱密度/噪声功率谱密度）

由基站直接测量每个扇区的主分集天线接收到的 I_o/N_o （总的接收功率谱密度/噪声功率谱密度，用 Z_1 和 Z_2 表示），每个时隙进行。然后利用一个 24 时隙的 IIR 滤波器（40ms），获得 Z_1 和 Z_2 的平均值 Z_{1ave} 和 Z_{2ave} 。如果 $\max(Z_{1ave}, Z_{2ave}) >$ 设定门限值，则设置 $RAB=1$ ，否则 $RAB=0$ 。

得到 RAB 的值后，在 MAC 信道上发送。该 RAB 在 $RABLength$ 个连续的时隙上传输，开始时隙由 $RABOffset$ 指定。AT 收到 RA 值后，结合速率转移概率，进行速率的调整。

第5章 整体信令流程

以下文档是一次正常的完整信令流程：下面具体过程的讲解会参考到。（以下消息是在 V2.1 打开版本跟踪的，所以打开时要注意版本配套）

用户接口跟踪消息：



EV-DO用户接口消息
跟踪.bmp



000-0403_153115_U
SER_normal.dat

空口消息跟踪：

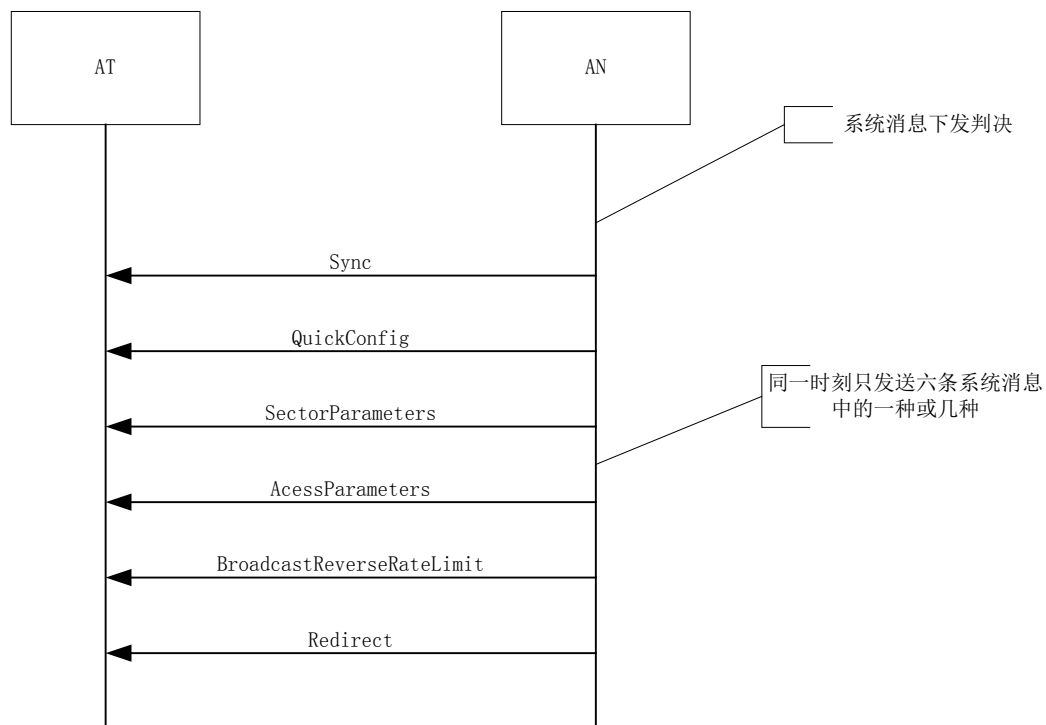


EV-DO空口消息跟踪
.bmp



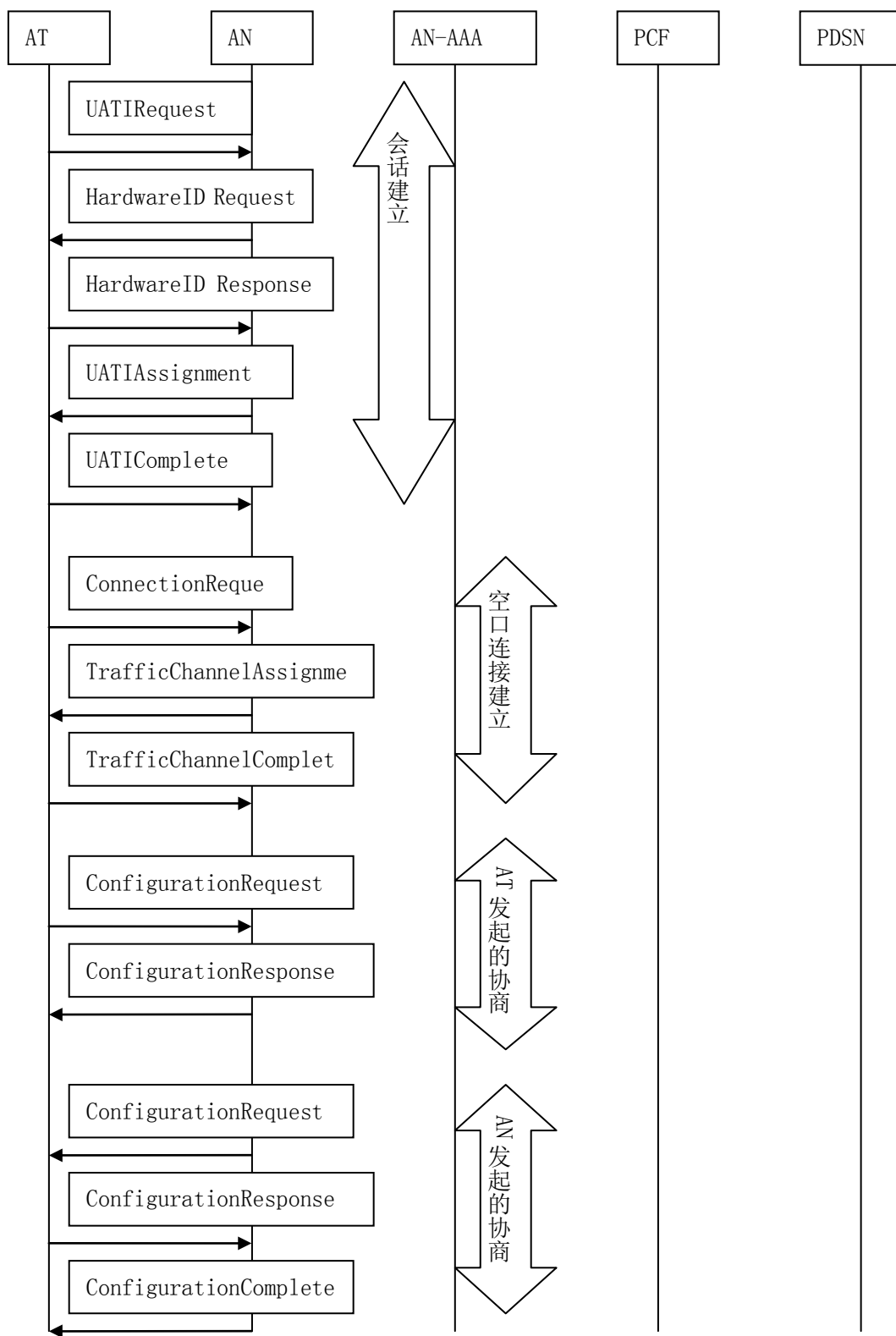
0408_111914_Um_IM
SI0000000000000000 V2.1 打开

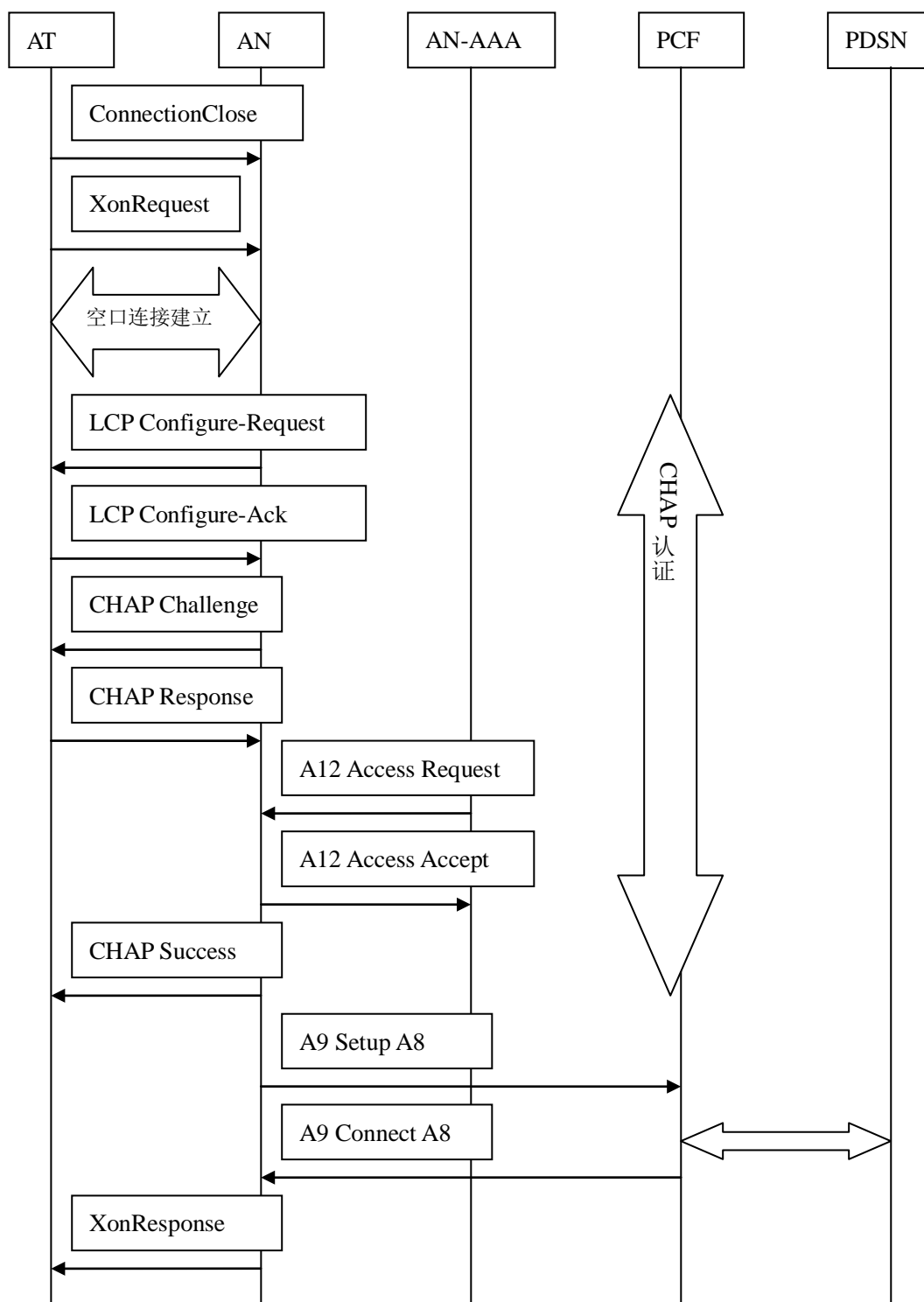
在 OMC 无法跟踪到的系统消息：

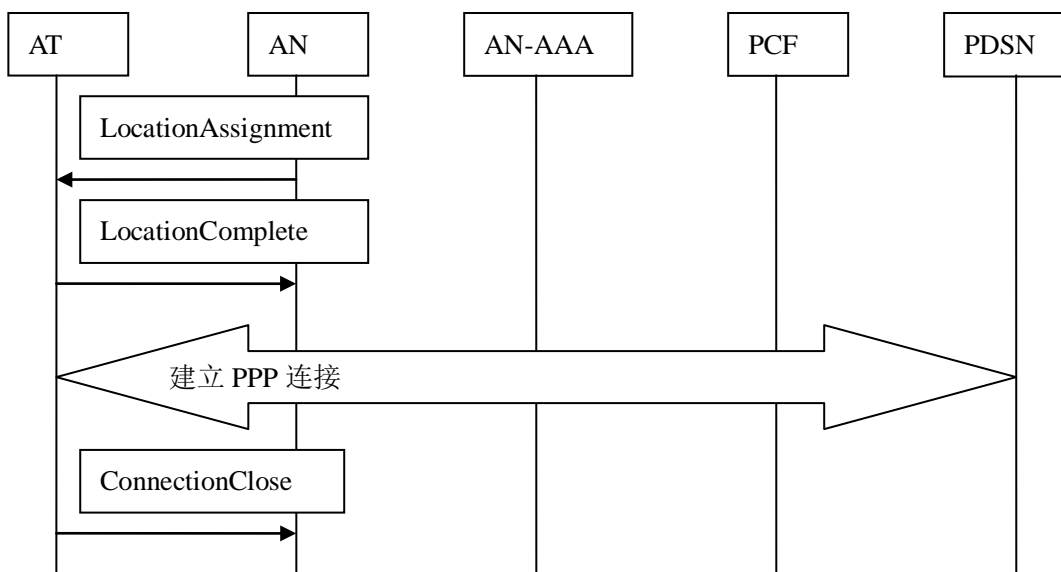


5.1 AT 始发的 HRPD 会话建立流程

从 AT 第一次开机到拨号呼叫、建立连接的信令流程如下：







会话建立过程的具体内容参考 1.2 节讲解；

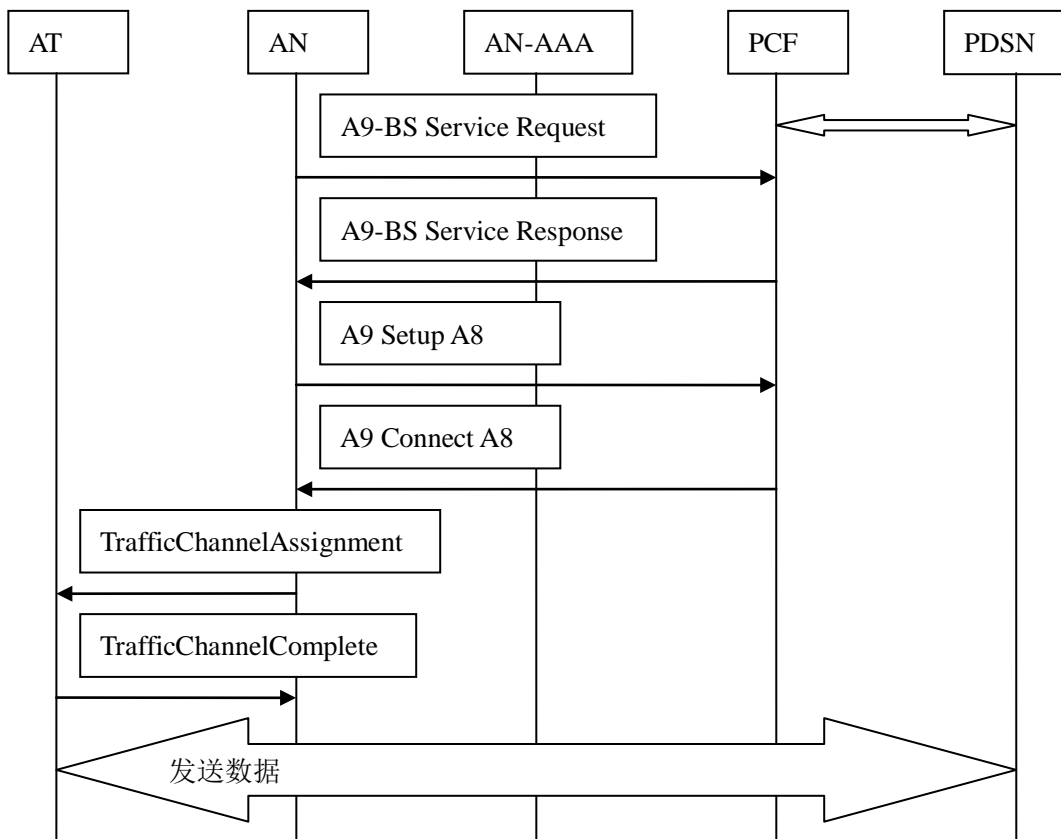
空口连接建立的具体内容参考 1.4 节讲解；

AT 或 AN 发起的协商过程的具体内容参考 1.7 节讲解；

CHAP 认证及之后的具体过程参考 PDSN PPP 连接过程讲解；

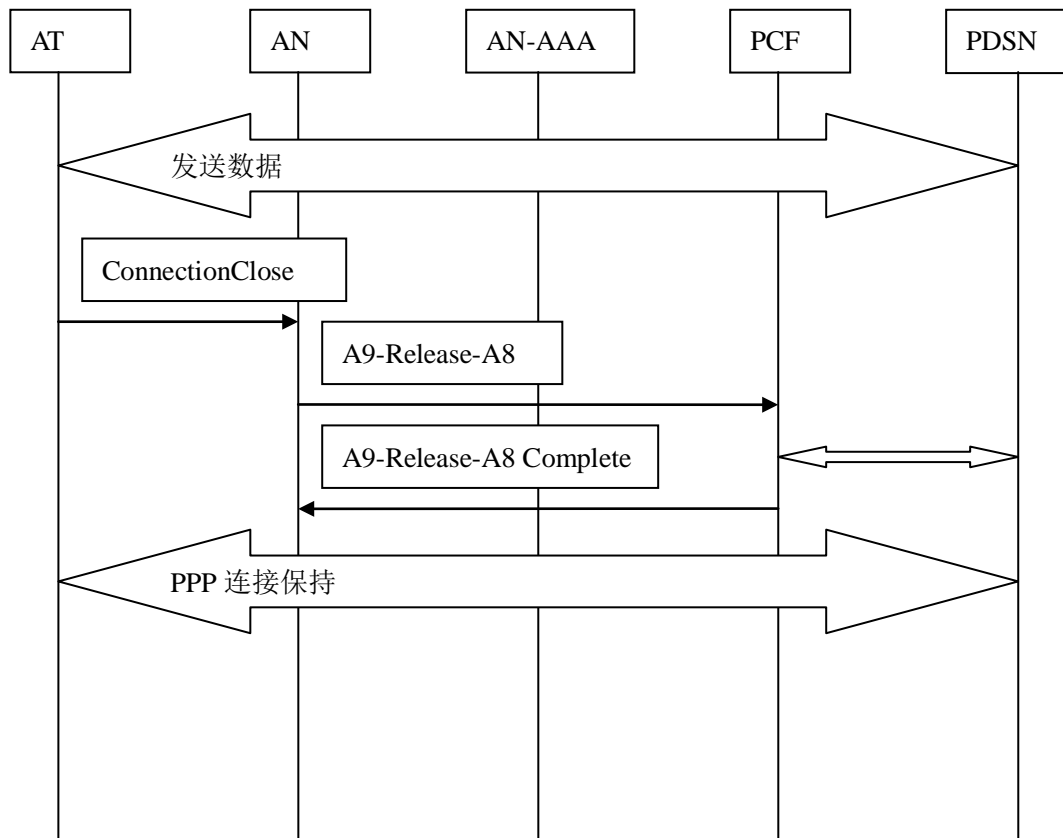
5.2 AN 始发的网络侧重激活流程

当终端处于休眠态时，当网络侧有数据传输时，由网络侧始发的重激活过程如下：



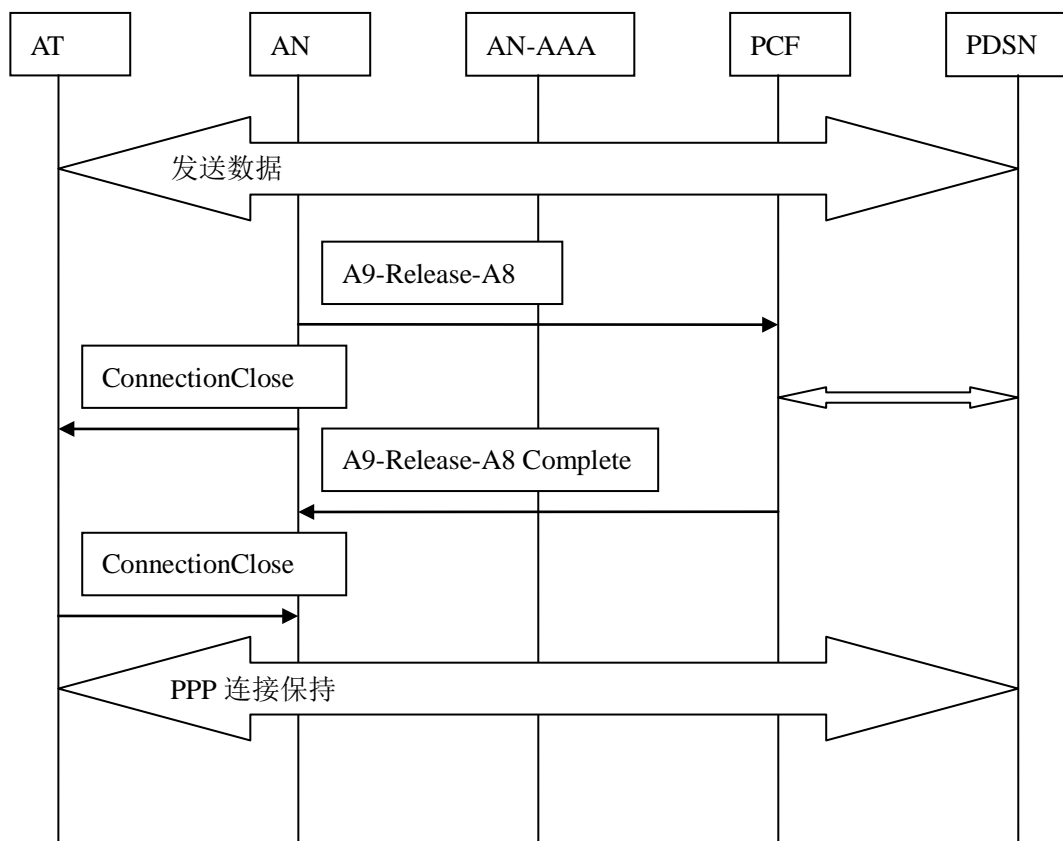
AN 发起的网络侧连接走的是快速连接流程，没有相应寻呼和连接请求过程消息，直接进行业务信道指配。具体内容理解参考 1.4 节的快速连接讲解。

5.3 AT 始发的连接释放流程



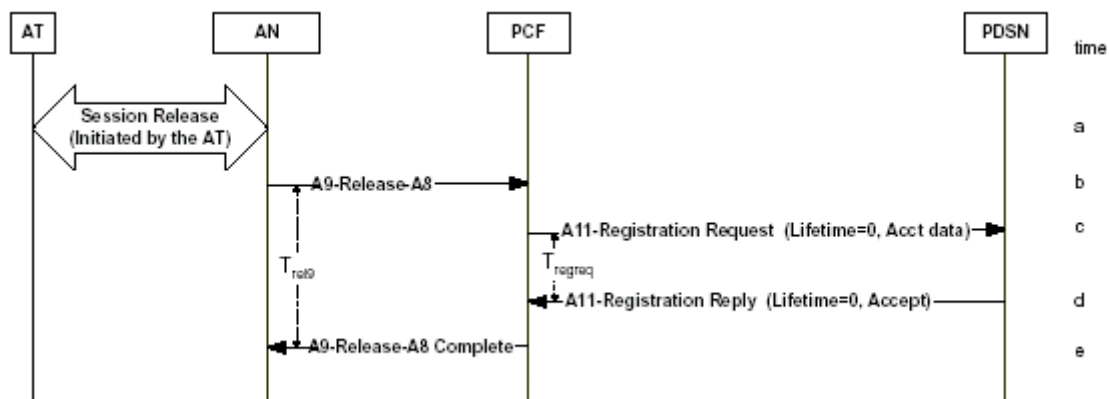
释放流程的理解参考 1.5 届内容的讲解。

5.4 AN 发起的连接释放流程



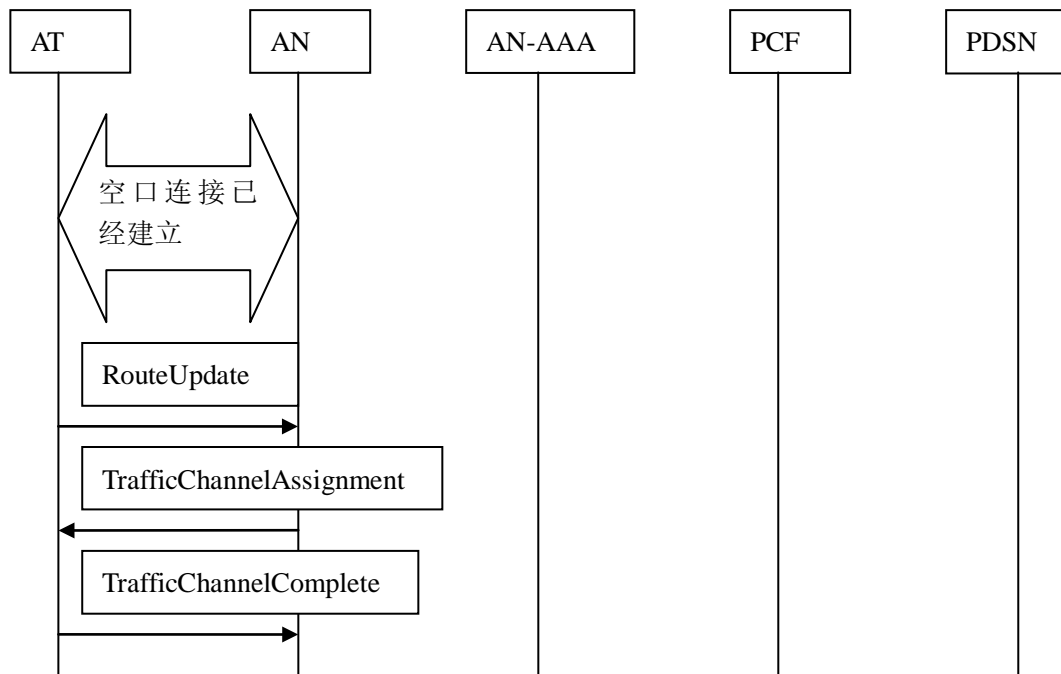
AN 始发的连接释放流程和 AT 始发的区别只有 A9-Release-A8 的位置不同，其他过程都相同。

5.5 AT 始发的会话释放流程



会话释放后将释放 PPP 连接，而前面的连接释放 A10 连接保持，只是释放空口资源和 A8/A9 连接。

5.6 软切换流程



具体内容理解参考 2.1.1 内容的讲解。

5.7 AN-AAA 鉴权消息

1	[A12] A12_Access_Request	SEND
2	[A12] A12_Access_Accept	RECEIVE

A12_Access_Request Message:

```

A12 MESSAGE
00000001 T  access request
00101110  identifier: 0x2e (46)
***** L  packet : 00 65
***** L  authenticator: c4 fc 95 fd 6f 69 a7 6f 9e c1 6f 75 b4 b5 81 8f : C4 FC 95 FD 6F 69 A7 6F 9E C1 6F 75 B4 B5 81 8F
***** L  user name : 01 1A
***** L  0611300103@hrpd.nate.com : 30 36 31 31 33 30 30 31 30 33 40 68 72 70 64 2E 6E 61 74 65 2E 63 6F 6D
***** L  chap password : 03 13
***** L  01 54 53 21 0c c3 30 66 a2 4f ad 68 d2 58 b3 0d e4 : 01 54 53 21 0C C3 30 66 A2 4F AD 68 D2 58 B3 0D E4
***** L  nas ip address : 04 06
***** L  0xc0a8014f (3232235855) : C0 A8 01 4F
***** L  chap challenge : 3C 12
***** L  c4 fc 95 fd 6f 69 a7 6f 9e c1 6f 75 b4 b5 81 8f : C4 FC 95 FD 6F 69 A7 6F 9E C1 6F 75 B4 B5 81 8F
***** L  vendor specific : 1A 0C
***** L  vendor id: 0x159f (5535) : 00 00 15 9F
00111100  vendor type: 0x3c (60)
00000110  vendor length: 0x6 (6)
***** L  vendor value: 0x1 (1) : 00 00 00 01

```

以上 user name : 0611300103@hrpd.nate.com是在 AN-AAA 设置的用户名，终端写码设置时写入 MIN: 0611300103，结合域地址来 AN-AAA 鉴权。（参考终端操作指导书）

A12_Access_Accept Message:

```

A12 MESSAGE
00000010 T  access accept
00101110  identifier: 0x2e (46)
***** L  Can not explain
***** L  : 00 40 FE 4C 4D 74 3B CE BD 6D 08 05 BC E2 78 8A EF
10111101
00000001

```

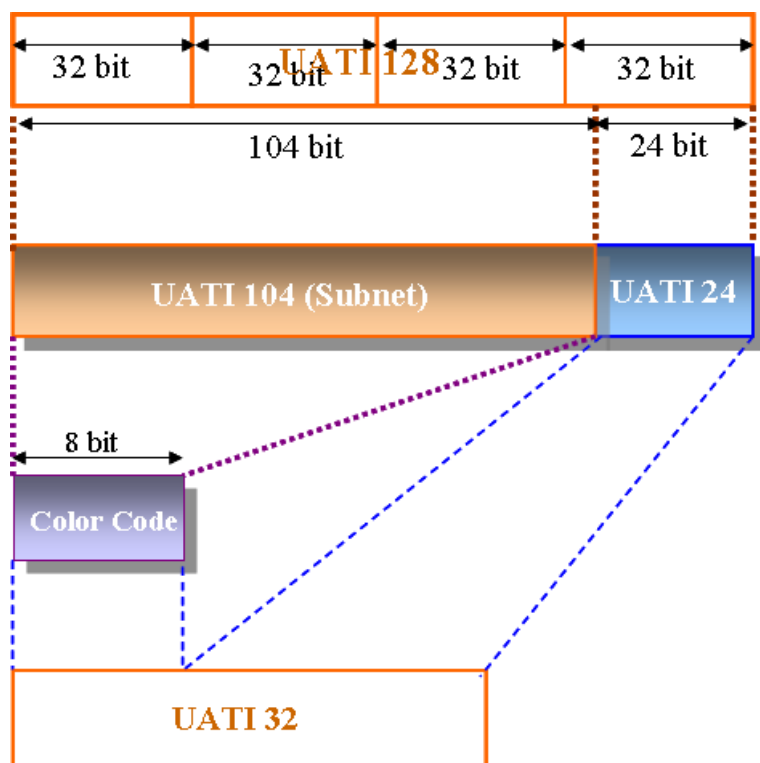
目前的版本中 OMC 跟踪到的短消息看不到是被原因值，如上图红色部分。

注：鉴权成功与否参考下图红色框中内容，RECEIVE 表示 AN-AAA 接入鉴权成功，REJECT 表示 AN-AAA 接入鉴权失败。

1	[A12] A12_Access_Request	SEND
2	[A12] A12_Access_Accept	RECEIVE

第6章 附录

6.1 1 UNTI 解释



如上图所示：

UNTI 的 128 位分为前 104 位和后 24 位，前 104 位的首 8 位即为色码，在进行数据配置时要和扇区的 SECTORID104 对应，用于标识子网，UNTI24 用于标识用户，和起来够成 UATI32，用于在整个网络中唯一标识用户。

6.2 附录 2 Rati 解释

10.5.1 General Procedures

When an access terminal is required to use the pseudo random number generator described in this section, then the access terminal shall implement the linear congruential generator defined by

$$z_n = a \times z_{n-1} \bmod m$$

where $a = 7^5 = 16807$ and $m = 2^{31} - 1 = 2147483647$. z_n is the output of the generator.⁵⁶

The access terminal shall initialize the random number generator as defined in 10.5.2.

The access terminal shall compute a new z_n for each subsequent use.

The access terminal shall use the value $u_n = z_n / m$ for those applications that require a binary fraction u_n , $0 < u_n < 1$.

The access terminal shall use the value $k_n = N \times z_n / m$ for those applications that require a small integer k_n , $0 \leq k_n \leq N-1$.

10.5.2 Initialization

The access terminal shall initialize the random number generator by setting z_0 to

$$z_0 = (\text{HardwareID} \oplus \chi) \bmod m$$

where HardwareID is the least 32 bits of the hardware identifier associated with the access terminal, and χ is a time-varying physical measure available to the access terminal. If the initial value so produced is found to be zero, the access terminal shall repeat the procedure with a different value of χ .

6.3 附录 3 AT 开机后维持的各个状态解释

激活态：AT 与 AN 建立了连接，并且有数据传输。

空闲态：AT 开机后要捕获网络，这样要经历初始化状态，捕获到网络之后在所捕获的网络登记，登记之后没有发起连接之间的状态就是空闲态；或者 AT 释放连接之后，虽然会话没有释放，但是没有连接，也处于空闲态。

监视态（挂起模式）：空闲态的子状态。

休眠态：空闲态的子状态。

下图为空闲状态下，监视态、休眠态、连接态，三种状态之间的转化关系：

