



中华人民共和国通信行业标准

YD/T 2513-2013

2GHz TD-SCDMA 数字蜂窝移动通信网 家庭基站网关设备技术要求

2GHz TD-SCDMA digital cellular mobile telecommunication network
—Technical requirement of Home Node B gateway

2013-04-25 发布

2013-04-25 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....III

1 范围.....1

2 规范性引用文件.....1

3 缩略语.....2

4 概述.....4

4.1 网络架构.....4

4.2 Iuh协议结构.....4

4.3 Iu协议结构.....5

5 HNB GW基本功能要求.....6

5.1 移动性管理功能.....6

5.2 寻呼优化.....6

5.3 RAB管理功能.....6

5.4 Iu链路管理功能.....6

5.5 用户接入控制功能.....7

5.6 HNB注册功能.....8

5.7 UE注册功能.....8

5.8 HNB GW服务区标识上报功能.....9

5.9 信令消息合法性验证.....9

5.10 QoS标签识别功能.....9

6 SeGW基本功能.....9

6.1 HNB接入认证功能.....9

6.2 防火墙功能要求.....9

6.3 IPSec功能.....9

6.4 网络拓扑隐藏.....10

6.5 NAT穿越.....10

7 HNB GW性能要求.....10

7.1 容量要求.....10

7.2 备份配置.....10

7.3 可用性和可靠性.....10

8 SeGW性能要求.....10

8.1 容量要求.....10

8.2 备份配置.....11

8.3 可用性和可靠性.....11

前 言

本标准是2GHz TD-SCDMA数字蜂窝移动通信网家庭基站系列标准之一，该系列标准的结构和名称如下：

- a) YD/T 2511-2013《2GHz TD-SCDMA 数字蜂窝移动通信网 家庭基站设备技术要求》
- b) YD/T 2512-2013《2GHz TD-SCDMA 数字蜂窝移动通信网 家庭基站设备测试方法》
- c) YD/T 2513-2013《2GHz TD-SCDMA 数字蜂窝移动通信网 家庭基站网关设备技术要求》
- d) YD/T 2514-2013《2GHz TD-SCDMA 数字蜂窝移动通信网 家庭基站网关设备测试方法》
- e) YD/T 2084-2013《2GHz TD-SCDMA/WCDMA 数字蜂窝移动通信网 家庭基站 Iuh 接口技术要求与测试方法》
- f) YD/T 2515-2013《2GHz TD-SCDMA 数字蜂窝移动通信网 家庭基站南向接口网管技术要求》
- g) YD/T 2516-2013《2GHz TD-SCDMA 数字蜂窝移动通信网 家庭基站南向接口网管测试方法》

随着技术的发展，还将制定后续的相关标准。

本标准按照GB/T1.1-2009给出的规则起草。

本标准参考了3GPP TS 25.467《UTRAN 3G家庭基站网络架构；第二阶段》（版本8）、3GPP TS 25.469《UTRAN Iuh接口HNBAP信令》（版本8）和3GPP TS 25.410《UTRAN Iu接口：总则》（2006年12月版）等。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国移动通信集团公司、工业与信息化部电信研究院、中国移动通信集团设计院有限公司、华为技术有限公司、京信通信系统（中国）有限公司、大唐电信科技产业集团、中兴通讯股份有限公司。

本标准主要起草人：蒋 鑫、王晓鸣、夏 铭、宋智源、陈 刚、孙 滔、徐 菲、曹 珏、温建明、周桦、邓 单、黄 河。

9 接口要求.....11

9.1 HNB GW逻辑接口要求.....11

9.2 SeGW逻辑接口要求.....12

9.3 HNB GW物理接口要求.....12

9.4 SeGW物理接口要求.....12

10 同步要求.....12

11 环境要求.....12

12 电源和接地要求.....12

12.1 直流电源电压要求.....12

12.2 设备接地要求.....12

12.3 防护要求.....13

13 安全要求.....13

14 HNB GW操作维护.....13

14.1 人机命令.....13

14.2 配置管理.....13

14.3 告警管理.....13

14.4 维护管理.....14

14.5 性能管理.....14

14.6 安全管理.....15

14.7 其他.....15

15 SeGW操作维护.....15

15.1 人机命令.....15

15.2 配置管理.....16

15.3 告警管理.....16

15.4 维护管理.....16

15.5 性能管理.....17

15.6 安全管理.....17

15.7 其他.....17

附录A（规范性附录） HNB注册过程.....19

附录B（规范性附录） UE注册功能.....21

附录C（规范性附录） HNB认证.....24

2GHz TD-SCDMA数字蜂窝移动通信网

家庭基站网关设备技术要求

1 范围

本标准主要规定了2GHz TD-SCDMA数字蜂窝移动通信网家庭基站网关设备以及安全网关设备的功能要求、性能要求、接口要求、操作维护要求、环境适应性要求、电源要求、同步要求和安全要求等。

本标准适用于不支持闭合用户群（CSG）的2GHz TD-SCDMA数字蜂窝移动通信网家庭基站网关设备和安全网关设备。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 4943.1-2011 信息技术设备 安全 第1部分：通用要求

YD/T 1082-2000 接入网设备过电压过电流防护及基本环节适应性技术条件

YD/T 1132-2001 防火墙设备技术要求

3GPP TS 23.234 3GPP系统到无线局域网的互操作；系统描述(Release 8)(3GPP system to Wireless Local Area Network (WLAN) interworking; System description, Release 8)

3GPP TS 25.410(Release 6,2006/12) UTRAN Iu 接口：概述与原则(UTRAN Iu interface: General aspects and principles)

3GPP TS 25.411(Release 6,2006/12) UTRAN Iu接口：层1(UTRAN Iu interface layer 1)

3GPP TS 25.412(Release 6,2006/12) UTRAN Iu 接口：信令传输(UTRAN Iu interface signalling transport)

3GPP TS 25.413(Release 6,2006/12) UTRAN Iu接口：无线接入网应用部分(RANAP)信令(UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling)

3GPP TS 25.414(Release 6,2006/12) UTRAN Iu接口：数据传输与传输信令(UTRAN Iu interface data transport and transport signalling)

3GPP TS 25.415(Release 6,2006/12) UTRAN Iu接口：用户平面协议(UTRAN Iu interface user plane protocols)

3GPP TS 25.467(Release 8,2009/06) UTRAN 3G家庭基站网络架构；第二阶段(UTRAN architecture for 3G Home Node B (HNB); Stage 2)

3GPP TS 25.468(Release 8,2009/06) UTRAN Iuh接口RUA信令(UTRAN Iuh Interface RANAP User Adaption (RUA) signalling)

3GPP TS 25.469(Release 8,2009/06) UTRAN Iuh接口HNBAP信令(UTRAN Iuh interface Home Node B (HNB) Application Part (HNBAP) signalling)

IETF RFC 2356 Sun公司跳过防火墙穿越的移动IP(Sun' s SKIP Firewall Traversal for Mobile IP)

IETF RFC 2401	因特网协议的安全架构(Security Architecture for the Internet Protocol)
IETF RFC 2402	IP认证报头(IP Authentication Header)
IETF RFC 2406	IP封装安全有效载荷(IP Encapsulating Security Payload(ESP))
IETF RFC 2409	因特网密钥交换(The Internet Key Exchange(IKE))
IETF RFC 2647	防火墙性能的基准术语(Benchmarking Terminology for Firewall Performance)
IETF RFC 3947	NAT协商—IKE中的穿越(Negotiation of NAT-Traversal in the IKE)
IETF RFC 3948	IPSecESP报文的UDP封装(UDP Encapsulation of IPSec ESP Packets)
IETF RFC 4301	因特网协议的安全架构(Security Architecture for the Internet Protocol)
IETF RFC 4303	IP封装安全有效载荷(IP Encapsulating Security Payload(ESP))
IETF RFC 4306	因特网密钥交换协议(IKEv2)(Internet Key Exchange(IKEv2)Protocol)

3 缩略语

下列缩略语适用于本文件。

3GPP	The 3rd Generation Partnership Project	第三代合作伙伴项目
AAA	Authentication, Authorization and Accounting	鉴权、认证与计费
AAL	ATM Adaptation Layer	ATM适配层
AAL2	ATM Adaptation Layer Type 2	ATM适配层类型2
AAL5	ATM Adaptation Layer Type 5	ATM适配层类型5
AKA	Authentication and key agreement	鉴权与密钥协商
AMR	Adaptive Multi-Rate	自适应多速率
ATM	Asynchronous Transfer Mode	异步传输模式
CN	Core Network	核心网
CSG	Close Subscribers Group	闭合用户组
EAP	Extensible Authentication Protocol	扩展认证协议
FE	Fase Ethernet	快速以太网
GE	Gigabit Ethernet	千兆以太网
GPRS	General Packet Radio Service	通用分组无线业务
GSM	Global System for Mobile communications	全球移动通信系统
GTP-U	GPRS tunneling Protocol for User Plane	GPRS隧道协议用户面部分
HLR	Home Location Register	归属位置寄存器
HMS	Home NodeB Management System	家庭基站管理系统
HNB	3G Home NodeB	家庭基站
HNBAP	Home NodeB Application Protocol	家庭基站应用协议
HNB GW	3G Home NodeB Gateway	家庭基站网关
HSS	Home Subscriber Server	归属用户服务器
IETF	Internet Engineering Task Force	互联网工程任务组
IKE	Internet Key Exchange	因特网密钥交换
IMSI	International Mobile Subscriber Identity	国际移动用户标识符

IP	Internet Protocol	互联网协议
IPSec	IP Security	IP安全协议
LAC	Location Area Code	位置区码
MTBF	Mean Time Between Failure	平均无故障时间
MSC	Mobile Switching Center	移动交换中心
NAT	Network Address Translation	网络地址翻译
NTP	Network Time Protocol	网络时钟协议
PS	Packet Switched	分组交换
PVC	Permanent Virtual Channel	永久虚通路
PLMN	Public Land Mobile Network	通用陆地移动网络
QoS	Quality of Service	服务质量
RAB	Radio Access Bearer	无线接入承载
RAC	Routing Area Code	路由区码
RANAP	Radio Access Network Application Part	无线接入网信令
RNC	Radio Network Controller	无线网络控制器
RRC	Radio Resource Control	无线资源控制
RTP	Real Time Protocol	实时协议
RUA	RANAP User Adaptation Layer	RANAP用户适配层
SAC	Service Area Code	服务区码
SAI	Service Area Identifier	服务区域标识符
SCTP	Simple Control Transmission Protocol	简单控制传输协议
SeGW	Security Gateway	安全网关
SGSN	Serving GPRS Support Node	服务GPRS支持节点
STM	SDH Transport Module	SDH传输模块
SPC	Signaling Point Code	信令点编码
SVC	Switched Virtual Circuit	交换虚电路
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access	时分同步码分多址
TMSI	Temporary Mobile Subscriber Identity	临时移动用户标识符
TrE	Trusted Environment	信任域
UE	User Equipment	用户设备
UMTS	Universal Mobile Telecommunications System	通用移动通信系统
UTRAN	UMTS Terrestrial Radio Access Network	UMTS 陆地无线接入网
VC	Virtual Circuit	虚电路
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

4 概述

4.1 网络架构

TD-SCDMA HNB系统主要包含HNB、HNB GW、AAA和HMS等。TD-SCDMA HNB是一种小型、低功率蜂窝技术，通过固网宽带接入到移动核心网，为用户提供包括TD-SCDMA业务在内的固定移动融合业务，主要用于家庭及中小企业等室内场所，是室内覆盖增强方案之一。从CN来看，HNB GW类似于RNC。HNB需要通过公共IP网络连接到HNB GW。相关网元的接口如图1所示。

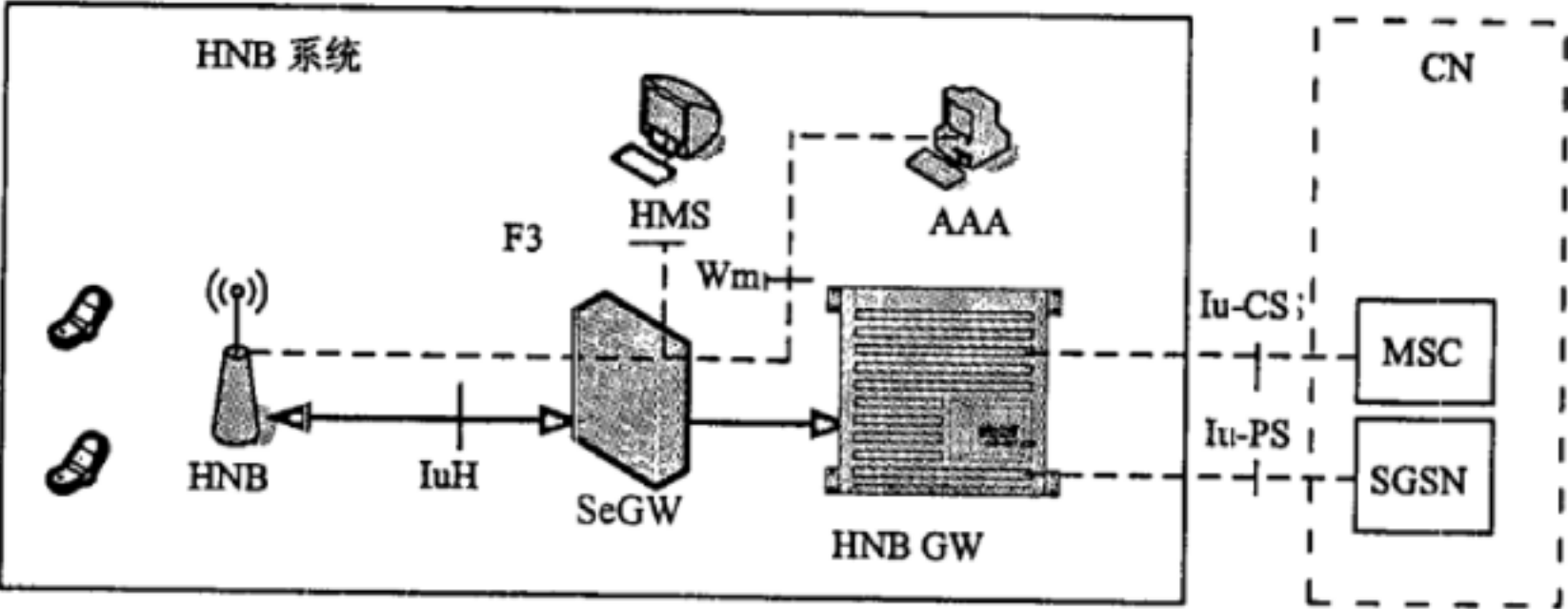


图1 HNB GW、SeGW 在 TD-SCDMA 网络中位置

HNB GW和SeGW的功能，可以作为两个单独的物理实体，或者是一个物理实体。主要网元和接口的功能如下：

- HNB GW：是 Iuh 接口的终结网元，负责对 HNB 和 CN 之间的信令和数据进行汇聚和分发，同时 HNB GW 负责对 HNB、UE 的注册和接入控制等。
- SeGW：位于 HNB 和 HNB GW 之间，负责 HNB 鉴权、建立 TR-069 和 Iuh 的 IPsec 安全隧道，保证 HNB 到 HMS 和 HNB GW 的安全接入；SeGW 可以集成在 Femto GW，也可作为独立网元存在。SeGW 中可以集成防火墙，防火墙也可以作为独立网元设置。
- HNB：HNB 属于用户端设备，集成了 Node B 和 RNC 的主要功能，并通过公共 IP 网络接入 CN。
- HMS：基于 TR-069，负责为 HNB 提供配置参数，实现 HNB 的位置认证功能，可以实现 HNB GW 发现功能，并且为 HNB 分配合适的服务网元，为 HNB 提供性能管理，告警管理。
- AAA：用于对 HNB 认证。
- Iuh 接口：位于 HNB GW 与 HNB 之间，支持 HNBAP 和 RUA 两个应用层协议，HNBAP 负责 HNB 和 UE 的注册，RUA 负责 RANAP 协议的适配和传送。
- Iu 接口：HNB GW 与 CN 之间采用原有的 Iu，负责疏通 HNB GW 与核心网的信令和话路。
- F3 接口：位于 HNB 和 HMS 之间，基于 TR-069，用于 HMS 对 HNB 的管理。
- Wm 接口：位于 SeGW 和 AAA 间，用于传送 HNB 的认证和签约信息。

4.2 Iuh 协议结构

HNB到HNB GW之间的接口称为Iuh接口，所有信令消息和数据流都通过Iu接口进行交互。由于RNC功能实体部分下移到HNB上，RNC到核心网的接口功能将由HNB和HNB GW来承担。HNB将数据和语音等业务数据流经过IP打包以及IPSec加密等后经过Iuh接口送至HNB GW。

Iuh接口协议栈如图2所示。

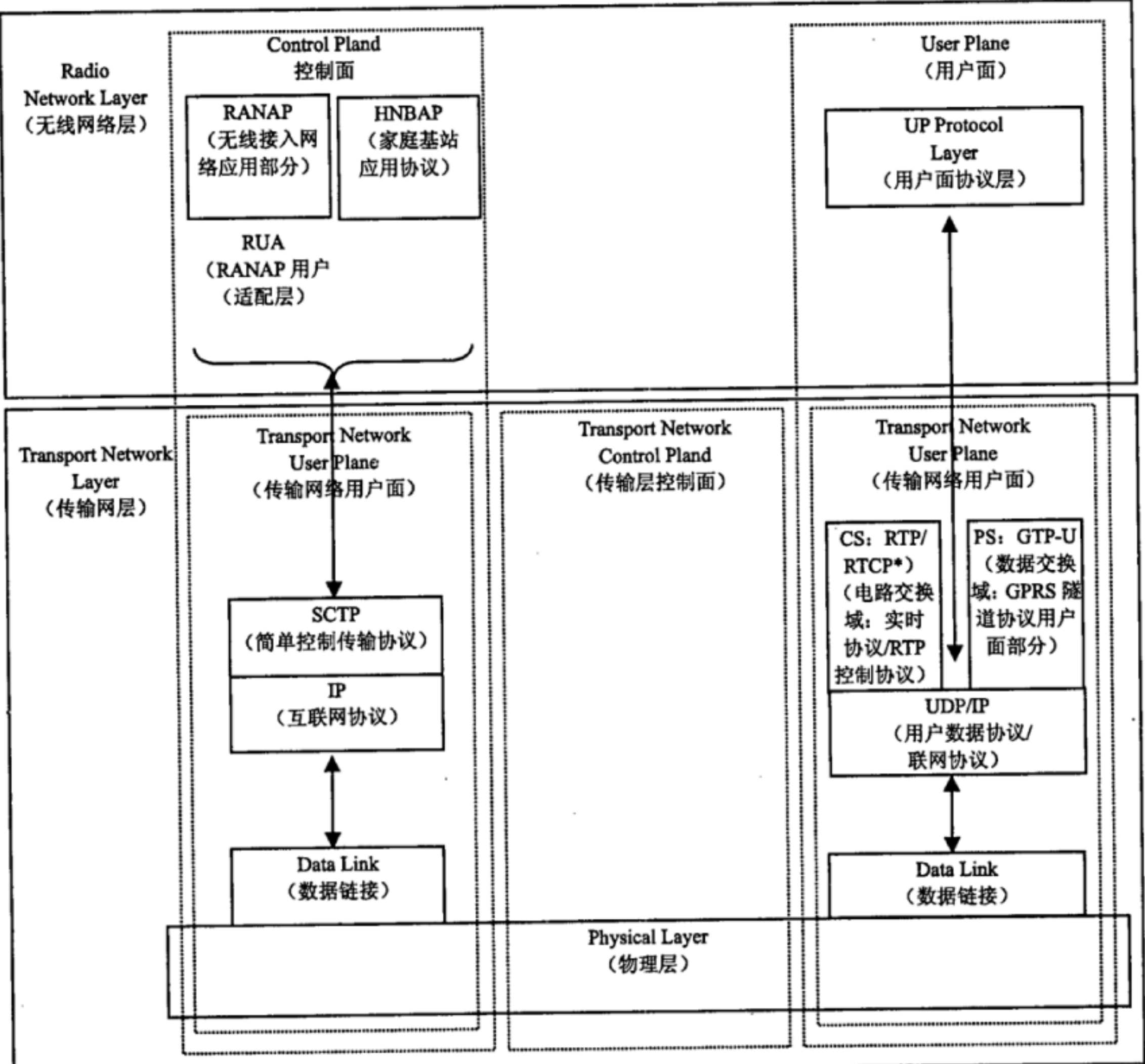


图2 Iuh 接口协议结构

Iuh接口协议栈中，RUA为SCTP与RANAP之间的适配层。RANAP为标准RANAP协议。HNBAP为针对HNB定义的应用协议，如HNB注册、用户准入管理等方面。HNBAP与RANAP在同一协议层，但是直接承载在SCTP协议层上。

Iu UP终结于CN和HNB，不终结于HNB GW。PS域的IP数据包直接承载于GTP-U隧道，用GTP隧道标识区分不同用户业务。

4.3 Iu 协议结构

CN和HNB接入网之间要求支持Iu接口。从Iu方面看，HNB的接入点是HNB GW。

HNB系统中可以有多个HNB GW，因此对于CN，HNB系统可以有多个Iu接入点。至少，每个Iu接入点（HNB GW或CN）可以独立完成相关Iu接口技术规范（3GPP TS 25.410、3GPP TS 25.411、3GPP TS 25.412、3GPP TS 25.413、3GPP TS 25.414和3GPP TS 25.415）的要求。

Iu接口的无线网络信令是RANAP。RANAP协议包括处理CN和HNB GW间的所有过程的机制。RANAP能够在CN和UE间透明传输消息。

5 HNB GW 基本功能要求

5.1 移动性管理功能

5.1.1 TD-SCDMA 系统内移动性管理

HNB GW配合实现如下类型的TD-SCDMA系统内切换:

- 支持从HNB向宏网络切换,采用SRNS重定位方式;
- 支持从HNB向宏网络重定向或直接重试;
- 支持HNB之间的切换。

5.1.2 系统间移动性管理(可选)

HNB GW配合实现如下类型的系统间切换:

- 对于AMR语音业务,从HNB到GSM宏网络的单向切换;
- 对于AMR语音业务,从HNB向GSM宏网络重定向;
- 对于PS业务,支持HNB到GPRS网络的单向切换,在切换之后,可根据实际承载网络能力对PS业务速率进行降速处理。

5.1.3 小区重选

HNB GW配合实现小区选择和重选:

- 支持HNB和TD-SCDMA宏网络之间的双向小区重选;
- 支持HNB和GSM宏网络之间的双向小区重选。

5.2 寻呼优化

HNB GW在执行寻呼转发的过程中,要求HNB GW支持寻呼优化功能,在保证寻呼成功率的前提下,尽量减少用户被叫时HNB GW发送的寻呼数量,降低寻呼对HNB GW的处理能力和容量要求。

5.3 RAB 管理功能

5.3.1 RAB 建立、修改、释放

RAB是根据签约、业务和被请求的QoS等在UE和CN之间建立时定义,不同的RAB将被使用。CN对RAB建立、修改和释放进行控制。RAB的标识由CN分配,且对于指定的UE在特定的CN域,RAB标识对无线承载和Iu承载有全局意义。HNB和CN均支持RAB的建立、修改和释放功能。当HNB不能保持HNB和UE连接的时候就触发RAB释放请求。

HNB GW应实现RAB建立、修改、释放消息的汇聚和转发功能。

HNB GW可以根据设备使用资源等进行判断,当HNB GW不能建立或保持HNB和UE连接的时候可以拒绝新建RAB或者触发RAB释放请求(可选)。

5.3.2 RAB 与 Iu 传输承载的映射特性

RAB映射特性功能用于把无线接入承载映射到Iu接口传输承载,映射在RAB建立期间完成。

如果使用AAL2,HNB GW将建立AAL2连接,HNB GW将完成与AAL2承载之间的映射。

对于PS域的RAB,HNB GW将完成无线接入承载和IP层之间的映射。

5.4 Iu 链路管理功能

5.4.1 Iu 信令链路管理

Iu信令链路管理功能在HNB GW和CN之间提供可靠的传递,以传递无线网络信令,CN和HNB GW都管理这个功能。HNB GW的Iu信令链路管理功能应支持:

——Iu 信令连接的建立（可以由 CN 或 HNB GW 建立）；

——Iu 信令释放（由 CN 控制，可能是 HNB GW 请求）。

5.4.2 ATM VC 管理

这个功能指处理CN和HNB GW之间的ATM虚连接，HNB GW应支持：

——建立、维持和释放 ATM VC/PVC，VC/PVC 可以承载多种链路，例如 SCCP 连接、AAL2 连接或 AAL5 连接；

——选择用于承载特定 RAB 的虚电路，选择对 Iu 无线接入承载业务请求的 ATM VC 选择，被选择 VC/PVC 将满足请求的要求。

5.4.3 AAL2 建立和释放

这个功能用于接受到无线接入承载业务请求时，在CN和HNB GW之间建立和释放AAL2连接，应支持：

——HNB GW 和 CN 参与 AAL2 连接的建立，HNB GW 支持 AAL2 连接的建立和释放；

——在异常情况下，CN 可以启动 AAL2 连接的释放。

5.4.4 AAL5 管理

在系统初始化时将预先配置CN和HNB GW之间的AAL5连接。基本配置是PVC，对用户数据，可能是SVC。

AAL5管理是由CN和HNB GW处理的功能。

5.4.5 GTP-U 隧道管理

这个功能用于根据无线接入承载业务请求建立和释放CN和HNB GW之间的GTP-U隧道，这涉及为每一方向分配隧道识别符和创建包含隧道信息的上下文。CN分配上行链路的隧道识别符，HNB GW应支持：

——保存隧道信息的上下文；

——GTP-U 状态检测。

5.4.6 缓冲区管理

当使用缓冲区管理而且没有流量控制的机制时，应对下行Iu用户平面采用拥塞控制：

——在接收时，对于不能处理的接收分组数据，缓冲区管理功能存储这些从对等 CN 节点接收的分组单元到缓冲区；

——在接收时，对于基于 IP 的语音包，缓冲区管理功能能够实现语音的防抖动（可选）。

对上行包的缓冲功能在HNB中实现。

5.4.7 RTP 会话管理

根据无线接入承载业务请求在CN和HNB网络之间建立和释放RTP，包括对每个方向RTP会话标识的分配和带有RTP会话信息的上下文的建立。CN、HNB和HNB GW都应该维护RTP会话上下文，RTP的使用取决于核心网的类型。

5.5 用户接入控制功能

根据运营商和HNB所有者的协议，运营商应该能够构建HNB的开放接入模式或者封闭接入模式。

——封闭模式：当 HNB 为封闭接入模式时，只有在准入列表中的用户才能接受服务。HNB 系统通过准入判断，确定用户是否有权使用该 HNB 资源；如果通过准入控制，那么允许接入，否则拒绝；

——开放模式：当 HNB 为开放接入模式时，为该 PLMN 下所有用户提供服务，与封闭模式相比，开

放模式下，HNB GW 不进行用户准入控制。

当用户发起紧急呼叫时，在封闭模式下，即使是非授权用户也可以使用HNB资源，在开放模式下，HNB能够提供正常紧急呼叫功能。

准入列表需满足：

- 在运营商的监管下，HNB 的所有者应该能够添加、删除和查看准入列表中用户；
- 在运营商的监管下，网络运营商和 HNB 所有者可以设置准入列表中 UE 的最大限制数目。该参数是静态参数，只有在配置和维护时才能设置和更改。

HNB GW必须根据用户标识（IMSI或者MSISDN）、用户准入列表和HNB的开放接入模式、封闭接入模式，支持对用户接入控制功能。HNB GW该部分的功能支持由HNBAP来提供。具体流程参见附录B。

5.6 HNB 注册功能

5.6.1 HNB 注册功能

HNB注册功能是在HNB得到自己的服务（Serving）HNB GW信息并与其建立两者之间的SCTP偶联后，告知HNB GW相关信息的过程，其中：

- HNB GW 能够根据 HNB 信息进行 HNB 接入控制，判断是否接受 HNB 的注册并给予响应；
- HNB GW 能够通过 HNB 注册过程获得 HNB 标识、HNB 位置信息、HNB 运营参数、IP 地址等；
- HNB GW 接受注册，应标识相应的 HNB 为已注册状态；HNB GW 拒绝注册，应返回适当原因值。

5.6.2 HNB 始发去注册功能

当HNB初始去注册过程时，HNB发送去注册消息给HNB GW，HNB GW应：

- 删除所有与该 HNB 相关的资源。

5.6.3 HNB GW 始发去注册功能

当HNB GW需要终止HNB运行时，初始去注册过程，HNB GW应：

- 携带原因值；
- 删除所有与该 HNB 的相关资源。

5.7 UE 注册功能

5.7.1 UE 注册功能

UE注册过程是在UE尝试通过初始NAS消息（例如位置更新请求）接入HNB时，并且HNB没有这个UE的上下文信息时发生，NB GW可以通过UE注册过程对UE进行准入控制，同时获得UE所在的具体HNB，其中：

——HNB GW 能够通过 UE 注册过程获得 UE 的相关信息，例如 MSISDN、IMSI、TMSI 和 UE 的能力等参数，且 HNB GW 能够通过 UE 注册过程获得 UE 所处的 HNB 信息；

——HNB GW 能够根据 UE 标识进行用户准入控制，判断是否接受 UE 注册请求，如果 UE 通过准入控制则进入正常的用户鉴权流程；

——UE 注册成功后，HNB GW 应标识该 UE 为已注册状态；否则，应返回适当原因值（比如非准入用户、鉴权失败等）。

该注册过程适用于Release 8版本以前不支持CSG的终端与HNB系统。

UE注册的具体流程见附录B.1。

5.7.2 HNB 始发 UE 去注册功能

当HNB初始去注册过程时，HNB发送去注册消息给HNB GW，HNB GW应：

——删除 UE 的相关信息；

UE 注册的具体流程见附录 B.2。

5.7.3 HNB GW 始发 UE 去注册功能

当HNB GW需要去注册UE时，初始去注册过程，HNB GW应：

——携带原因值；

——删除 UE 的相关信息；

UE 注册的具体流程见附录 B.3。

5.8 HNB GW 服务区标识上报功能

HNB GW支持在用户接入时，通过Iu接口直传消息应将HNB上报的用户所在SAI参数发送给CN中的MSC和SGSN设备。

5.9 信令消息合法性验证

HNB GW支持对HNBAP信令消息的合法性验证，防止用户非法改装HNB，发送非法的信令消息对网络造成影响。

5.10 QoS 标签识别功能

HNB GW应具有QoS标识的管理功能，能够区分CN和HNB之间IP传输中QoS标签。用户业务优先级应该由HNB根据3GPP UMTS业务分类和QoS定义设置，HNB GW透传HNB的优先级标识。

6 SeGW 基本功能

6.1 HNB 接入认证功能

IKE协议目前有IKEv1和IKEv2两个版本，HNB系统的SeGW要求必选使用IKEv2来动态建立IPsec安全关联。

SeGW支持对HNB设备和对HNB宿主认证，对HNB设备的认证是必选的，如果HNB支持宿主认证，则要求宿主与HNB设备绑定。

SeGW的HNB接入认证功能应支持EAP AKA双向鉴权方式或基于IKEv2协议的证书方式，对于HNB设备采用EAP AKA方式或者证书，对于宿主只采用EAP AKA方式。

支持为HNB分配IP地址。

支持周期性密钥协商功能，即每隔一段时间HNB与SeGW之间的IPSec隧道的密钥更新一次。

支持检测对端（HNB）离线并释放隧道资源。

6.2 防火墙功能要求

防火墙可以作为功能集成在SeGW中，也可以作为独立网元设置，为需要安全保护的网元提供保护。

防火墙系统的功能应符合IETF相关规范（RFC 2356和RFC 2647）及YD/T 1132-2001的要求。

6.3 IPSec 功能

SeGW支持在HNB和HNB GW之间构建安全通道，使用IPSec可以在IP网络上生成安全隧道，为用户在IP网络上建立安全的点对点连接，保护HNB的控制面和用户面数据不受窃听和篡改。IPSec为SeGW必选功能，应支持：

——ESP 的隧道模式和传输模式的工作方式；

——提供多种主流的加密算法和完整性算法，例如 DES、3DES、AES（必选）、MD5，SHA-1（必

选)等。

IPSec功能应符合IETF相关规范RFC 2401、RFC 2402、RFC 2406、RFC 2409、RFC 4301、RFC 4303和RFC 4306等。

6.4 网络拓扑隐藏

SeGW支持对外界隐藏与其连接的网元,包括HNB GW、MSC以及SSGN等。

6.5 NAT 穿越

为了解决NAT和IPSec共存问题,引入了穿越功能,NAT穿越技术要求见IETF相关规范RFC 3947、RFC 3948。NAT穿越主要原理为在内层IP头与外层IP头之间加入一个UDP的头封装。这样,当此数据包穿过NAT网关时,被修改的只是最外层的IP地址,而对其真正的IP地址没有进行改动。

——要求设备支持ESP下的NAT穿越功能,支持多重NAT穿越,以使IPSec设备能够识别使用同一个NAT地址的多个IPSec终端发出的不同隧道协商请求,并建立彼此独立的安全关联;

——IPSec必须能够自动检测到NAT设备为IPSec主机提供的当前映射地址及端口,并在映射地址及端口发生变化时及时更新安全关联中的地址参数,保证远程VPN主机与VPN网关的通讯始终畅通。

7 HNB GW 性能要求

7.1 容量要求

HNB GW最小容量要求如下:

- HNB GW支持的HNB数量不低于5千;
- HNB GW支持的BHCA(全部等效为语音接入)不低于3万;
- HNB GW支持的分组流量不低于1Gbit/s。

HNB GW一般配置的要求如下:

- HNB GW支持的HNB数量不低于5万HNB;
- HNB GW支持的BHCA(全部等效为语音接入)不低于30万;
- HNB GW支持的分组流量不低于1Gbit/s。

7.2 备份配置

HNB GW各部件应提供适当的冗余配置。冗余配置要求如下:

- 网元级别1+1备份或通过HNB GW池的方式实现备份;
- 关键部件全部1+1热备份,其他部件可提供一个或多个备份单元($N+1$, $N+m$);
- 热倒换时间不大于10min。

7.3 可用性和可靠性

平均故障间隔时间MTBF不小于200000h;系统平均故障修复时间MTTR不大于30min。

8 SeGW 性能要求

8.1 容量要求

SeGW小容量配置要求如下:

- 同时支持不低于5千个IPSec并发隧道;
- IPSec隧道建立和释放至少20个/s;
- 数据包加/解密吞吐量至少100万个(数据包)/s;

- 支持转发语音数据流 BHCA（全部等效为语音接入）不低于 3 万；
- 支持转发分组流量不低于 1Gbit/s。

SeGW一般配置的要求如下：

- 同时支持不低于 5 万个 IPSec 并发隧道；
- IPSec 隧道建立和释放至少 420 个/s；
- 数据包加/解密吞吐量至少 240 万个（数据包）/s；
- 支持转发语音数据流 BHCA（全部等效为语音接入）不低于 30 万；
- 支持转发分组流量不低于 3Gbit/s。

8.2 备份配置

SeGW各部件应提供适当的冗余配置。冗余配置要求如下：

- 网元级别采用 VRRP 1+1 双机热备份当网内设备的下一跳设备出现故障时，可以及时地由另一台设备来代替，从而保持通信的连续性和可靠性；或者通过池的方式实现备份（SeGW 可以集成在 HNB GW 中）；
- 关键部件全部 1+1 热备份，其他部件可提供一个或多个备份单元（ $N+1$ ， $N+m$ ）；
- 热倒换时间不大于 10min。

8.3 可用性和可靠性

平均故障间隔时间MTBF不小于200000h；系统平均故障修复时间MTTR不大于30min。

9 接口要求

9.1 HNB GW 逻辑接口要求

9.1.1 Iu 接口

在HNB GW Iu接口SPC长度的使用有3种方式：

- HNB GW 使用 14 位比特；
- HNB GW 使用 24 位比特；
- HNB GW 同时支持 14 位和 24 位比特。

设备必须支持第1种；第2种和第3种方式为可选方式。

HNB GW和CN之间的接口，Iu接口是一个开放的标准接口。

Iu接口基于以下规范：

- 3GPP TS 25.410（Release 6，2006/12）；
- 3GPP TS 25.411（Release 6，2006/12）；
- 3GPP TS 25.412（Release 6，2006/12）；
- 3GPP TS 25.413（Release 6，2006/12）；
- 3GPP TS 25.414（Release 6，2006/12）；
- 3GPP TS 25.415（Release 6，2006/12）。

9.1.2 Iuh 接口

Iuh接口基于以下规范：

- 3GPP TS 25.467（Release 8，2009/06）；
- 3GPP TS 25.468（Release 8，2009/06）；

——3GPP TS 25.469 (Release 8, 2009/06)。

9.2 SeGW 逻辑接口要求

9.2.1 Wm 接口要求

Wm接口位于SeGW和AAA间，用于传送HNB的认证和签约信息。Wm接口基于3GPP TS 23.234。

9.3 HNB GW 物理接口要求

HNB GW应支持STM-1、GE、STM-4（可选）、FE（可选）、E1（可选）。

9.4 SeGW 物理接口要求

求SeGW支持与HMS、HNB、HNB GW之间接口，提供HNB到HMS和HNB GW的安全接入，支持10Mbit/s、100Mbit/s、1000 Mbit/s以太网接口。

10 同步要求

HNB GW支持外部2MHz、2Mbit/s时钟同步（E1接口），或支持从STM链路提取时钟，或者ATM时钟同步。HNB GW还支持NTP方式完成设备的时间同步。

11 环境要求

环境要求是指导性的，适用于HNB GW设备。

HNB GW 设备应在以下环境条件下正常工作，见表1。

表1 温度、湿度要求

设备名称	温度（℃）		相对湿度（%）	
	长期条件	短期条件	长期条件	短期条件
HNB GW及外围设备	15℃~30℃	0℃~45℃	40%~65%	20%~90%
注1：温度、湿度的测量点指地板以上2m和设备前方 0.4m处测量的数值（机架前后没有保护板时测量）。				
注2：短期条件指连续不超过48h和每年累计不超过15天				

12 电源和接地要求

12.1 直流电源电压要求

HNB GW 应在下述直流电源性能范围内正常工作，见表2。

表2 电源要求

项 目		交换机用的直流电源（DC）	
标称值		-48V	
电压波动范围		-40V~-57V	
杂音电压	0~300Hz	≤100mV 峰-峰值	
	300Hz~3400Hz	≤2mV 杂音计衡重杂音	
	3.4kHz~150kHz	单频≤5mV 有效值，宽带≤100m 有效值	
	150kHz~200kHz	单频≤3mV 有效值	宽带
	200kHz~500kHz	单频≤2mV 有效值	150k 30MHz
	500kHz~30MHz	单频≤1mV 有效值	≤30m 有效值

12.2 设备接地要求

设备接地应采用联合接地方式。

HNB GW在接地电阻小于5Ω时应能正常工作。

12.3 防护要求

应满足YD/T 1082-2000。

13 安全要求

应满足GB 4943.1-2011。

14 HNB GW 操作维护

14.1 人机命令

可支持图形界面、命令行接口这两种用户接口中的一种：

对图形界面，应提供基于HNB GW物理设备操作维护的图形界面，简化用户输入；输出界面直观易于理解，并根据实际输出情况提供相对应图形界面；提供完整、详尽的用户操作手册。

对命令行接口，应提供简明命令行输入接口，提供命令行在线帮助功能；提供完整、详尽的用户操作手册。

14.2 配置管理

HNB GW设备应满足以下配置管理要求：

- 系统扩容：在不中断业务的情况下进行扩容（可选）。
- 离线数据配置：提供离线配置功能，实现数据添加、修改和删除。
- 在线数据配置：支持在不中断业务的情况下对部分配置数据进行修改，并动态生效。
- 配置数据查询、保存和恢复：按操作员的要求查询指定的配置数据。
- 配置数据有效性校验：校验出输入 HNB GW 系统的无效配置数据，并给出提示。
- 数据配置同步功能：支持网元上配置数据同步到网管中来，以保持网元和网管配置数据的一致性，支持手动，自动和定时同步。
- 支持手动数据备份和自动数据备份。
- 支持批处理功能：批处理功能支持从网管拓扑界面上批量处理（如创建和删除网元）（可选）。

HNB GW 设备要满足以下拓扑管理要求：

- 支持拓扑对象管理，如创建、删除拓扑网元、修改拓扑对象属性等；
- 支持批量拓扑对象管理；
- 支持自动呈现网元之间的物理链路，自动发现 HNB 功能；
- 支持拓扑对象查询功能，如网元的信息、连接状态等；
- 支持拓扑地图管理：支持用子网分层显示网元和链路，各子网可以采用不同的拓扑地图；
- 支持快捷操作入口：拓扑地图还提供了快捷的操作入口，查询网元/链路的配置信息、告警信息和性能测量结果。

14.3 告警管理

HNB GW设备要求满足以下告警管理要求：

- 告警采集，当故障产生时，设备能产生相应的告警；
- 告警屏蔽、告警确认、告警清除、告警恢复等；
- 告警显示/查询；
- 告警存储：支持设定历史告警的存储时间，超过时间或超过容量限制的告警可自动被删除；

——声光告警，系统应给出声光提示；

——支持告警模板功能：告警模板功能支持用户将告警分类浏览过滤条件和告警实时浏览条件保存为模板；

——支持告警拓扑定位功能：支持用户在告警查询和实时浏览窗口中，选择一条告警执行拓扑定位操作，直接定位到拓扑图上发生该告警的网元，使网元在拓扑图的可视区域中聚焦显示；

——支持告警自动同步功能：确保网管与网元告警信息的一致性，支持自动、手动以及定时同步；

——支持告警级别网管重定义：支持用户修改网管上的告警级别；

——支持长时间未恢复故障告警提示：系统自动检测长时间仍然未恢复的故障告警，把这些告警在界面上加亮显示以提示用户及时处理。

14.4 维护管理

HNB GW设备要满足以下维护管理要求：

——复位：按操作员指令进行系统级复位、板级复位；

——支持接口跟踪：提供接口跟踪功能，包含信令消息跟踪和单 HNB 或单用户信令消息跟踪；

——能够查询物理及逻辑状态，包括电路板、传输设备等物理资源；

——能够进行电路板测试；

——能够进行线路/链路自环测试；

——能够进行传输层的管理和维护；

——支持闭塞/解闭功能；

——支持主备板倒换。

对于非电路板设计的设备，以上板级功能为可选。

14.5 性能管理

HNB GW设备要求满足以下性能管理要求：

——操作员可通过建立测量任务的形式进行对系统的测量和统计，提供业务和系统状态以及整个系统性能的常规报告。测量任务中至少包括测量的指标、测量粒度周期、测量的时间等，并支持测量任务管理，包括创建、删除测量任务，查询、挂起、唤醒以及修改测量任务；

——支持对测量结果的管理，能够查询测量结果，并且可以保存相应的测量结果；

——支持性能阈值告警：性能告警功能支持对测量指标设置性能告警阈值，当指标值超过阈值范围时产生性能告警；

——支持性能测量模板功能：支持将用户设置的测量信息，包括测量的周期、测量的对象、测量的指标等设置情况导出到文件里作为性能测量模板使用，用户可以通过导入模板文件设置测量的指标和周期信息等；

——支持自定义指标管理：支持用户在系统提供的原始指标和已有的自定义指标的基础上定义新的性能指标，从而满足网络运维中超出原始指标范围的性能测量指标需求（可选）。

统计例如：

a) 传输测量：Iuh、Iu 口流量统计。

b) 传输信令测量：MTP3、SAAL 的拥塞、失效等测量。

c) 业务测量，包括：

- 1) 准入控制测量: 包括 HNB 接入请求次数、成功/失败次数等;
- 2) 呼叫测量: 包括 RAB 建立和释放成功、失败次数等;
- 3) 寻呼测量: 包括寻呼次数。
- d) 服务质量指标项至少应包括:
 - 1) HNB 呼叫接通率;
 - 2) Iu 口数据带宽占用率;
 - 3) 切换次数。

14.6 安全管理

HNB GW设备要满足以下安全管理要求:

支持多个级别操作员权限, 可设置操作员级别、业务权限、操作时段、有效期、口令等;

——支持对操作员信息的保护, 当操作员长时间未操作时, 清除操作员的信息或操作员主动清除自己的信息, 该时间长度间隔应可设置;

——支持用户组管理: 支持基于角色的用户组管理和权限管理, 操作权限根据角色分配给用户组;

——支持集中用户鉴权: 支持对全网操作维护用户进行鉴权;

——支持用户管理: 可设置用户级别、操作权限、有效期、密码等;

——支持用户在线检控: 支持用户集中监控所有在线网管用户。在监控界面上可实时显示用户名、用户操作、操作时间、操作结果、操作终端等信息;

——支持自锁功能: 在一定时间段内没有任何操作的网管客户端将被系统自动锁定。

14.7 其他

HNB GW的操作维护还应满足一些其他方面的要求, 包括:

——支持标准接口跟踪: 并能保存跟踪结果, 并通过 IMSI、T-IMSI、P-TMSI 跟踪用户 (可选);

——支持操作日志: 记录操作员对 HNB GW 系统发出的每一个命令、命令执行结果 (成功/失败)、时间等;

——支持在线升级: 在不中断业务的情况下对软件升级, 并能够根据操作员指令返回到原状态, 当新版本软件无法正常工作, 可回退到原版本;

——提供远程维护 (可选);

——支持日志管理: 在系统运行中, 各种信息都被记录到日志中, 网管日志包括操作日志、运行日志和安全日志等 3 种;

——支持夏令时 (可选);

——支持系统备份: 为保证系统数据安全, 网管支持对数据库的自动备份。

15 SeGW 操作维护

15.1 人机命令

可支持图形界面、命令行接口这两种用户接口中的一种:

对图形界面, 应提供基于 SeGW 物理设备操作维护的图形界面, 简化用户输入; 输出界面直观易于理解, 并根据实际输出情况提供相对应图形界面; 提供完整、详尽的用户操作手册。

对命令行接口, 应提供简明命令行输入接口, 提供命令行在线帮助功能; 提供完整、详尽的用户操作手册。

15.2 配置管理

设备满足以下配置管理要求：

- 支持数据的添加、修改和删除功能，包括 IP 地址、网络宽带设置、路由设置等参数，支持在不中断业务的情况下对部分配置数据进行修改并动态生效；
- 支持配置文件的查询、保存和恢复；
- 支持对包过滤规则的配置，包过滤规则表包括过滤标准、动作及记录选项，过滤标准包括源和目标地址、源和目标端口、协议类型、源接口类型等；
- 数据配置同步功能：支持网元上配置数据同步到网管中，以保持网元和网管配置数据的一致性，支持手动、自动和定时同步；
- 支持手动数据备份和自动数据备份；
- 支持数据有效性校验：命令行验证输入系统的无效配置数据，并给出提示；
- 系统扩容：在不中断业务的情况下进行扩容。

HNB GW设备要满足以下拓扑管理要求：

- 支持拓扑对象管理，如创建、删除拓扑网元，修改拓扑对象属性等；
- 支持批量拓扑对象管理；
- 支持自动呈现网元之间的物理链路，自动发现 HNB 功能；
- 支持拓扑对象查询功能，如网元的信息、连接状态等；
- 支持拓扑地图管理：支持用子网分层显示网元和链路，各子网可以采用不同的拓扑地图；
- 支持快捷操作入口：拓扑地图还提供了快捷的操作入口，查询网元/链路的配置信息、告警信息和性能测量结果。

15.3 告警管理

设备满足以下告警管理要求：

- 告警采集，当故障产生时，设备能产生相应的告警；
- 支持告警显示、查询、确定、屏蔽、清除、恢复等；
- 支持告警存储功能；
- 提供告警参考手册，供用户参考；
- 声光告警，系统应给出声光提示；
- 支持告警模板功能：告警模板功能支持用户将告警分类浏览过滤条件和告警实时浏览条件保存为模板；
- 支持告警拓扑定位功能：支持用户在告警查询和实时浏览窗口中，选择一条告警执行拓扑定位操作，直接定位到拓扑图上发生该告警的网元，使网元在拓扑图的可视区域中聚焦显示；
- 支持告警自动同步功能：确保网管与网元告警信息的一致性，支持自动、手动以及定时同步；
- 支持告警级别网管重定义：支持用户修改网管上的告警级别；
- 支持长时间未恢复故障告警提示：系统自动检测长时间仍然未恢复的故障告警，把这些告警在界面上加亮显示以提示用户及时处理。

15.4 维护管理

设备满足以下维护管理要求：

——提供单板在位检测、热插拔检测、单板复位、运行灯/调试灯控制、风扇监控、电源监控和版本查询等功能；

——支持按操作员指令进行系统级复位、单板级复位；

——监控路由协议、VPN 协议等相关状态的迁移变化；

——提供业务运行的调试功能，在线记录用户指定的业务运行时刻的关键事件、报文处理、报文解析、状态切换等信息（可选）；

——提供种类丰富、内容详尽的调试信息，帮助诊断网络故障（可选）；

——支持主备网元倒换。

15.5 性能管理

设备满足以下性能管理要求：

——操作员可通过建立测量任务的形式进行对系统的测量和统计，提供业务和系统状态以及整个系统性能的常规报告。测量任务中至少包括测量的指标、测量粒度周期、测量的时间等；并支持测量任务管理，包括创建、删除测量任务，查询、挂起、唤醒以及修改测量任务；

——支持对测量结果管理，能够查询测量结果，并且可以保存相应的测量结果；

——支持性能阈值告警：性能告警功能支持对测量指标设置性能告警阈值，当指标值超过阈值范围时产生性能告警；

——支持性能测量模板功能：支持将用户设置的测量信息，包括测量的周期、测量的对象、测量的指标等设置情况导出到文件里作为性能测量模板使用，用户可以通过导入模板文件设置测量的指标和周期信息等；

——支持自定义指标管理：支持用户在系统提供的原始指标和已有的自定义指标的基础上定义新的性能指标，从而满足网络运维中超出原始指标范围的性能测量指标需求（可选）。

性能统计，例如：

——HNB 认证次数；

——HNB 认证成功数；

15.6 安全管理

设备满足以下安全管理要求：

——支持全面的安全业务，强大的攻击防范能力，保护网络安全的同时保证设备自身安全；

——支持管理用户访问验证，确保非法用户无法登录设备；

——支持命令分级保护，确保未授权用户无法对设备进行配置；

——支持创建本地用户：可设置用户级别、操作权限、密码等；

——支持用户组的管理；

——支持基于域对用户进行管理。

安全管理应提供数据机密性和完整性：

——机密性防止无权实体得到通信实体间传送的消息的内容，保证数据从起点到终点的正确传送；

——完整性防止对存储的数据或实体间传送的信息的无权修改，保证数据只被传送到预定的目的地；

——保证数据的存储和恢复。

15.7 其他

SeGW的操作维护还应满足一些其他方面的要求，包括：

- 支持操作日志：记录操作员对 SeGW 系统发出的每一个命令、命令执行结果（可选）、时间等；
- 支持在线升级：在不中断业务的情况下对软件升级，并能够根据操作员指令返回到原状态，当新版本软件无法正常工作时，可回退到原版本；
- 提供远程维护（可选）；
- 支持日志管理：在系统运行中，各种信息都被记录到日志中，网管日志有操作日志、运行日志和安全日志等 3 种；
- 支持系统备份：为保证系统数据安全，网管支持对数据库的自动备份。

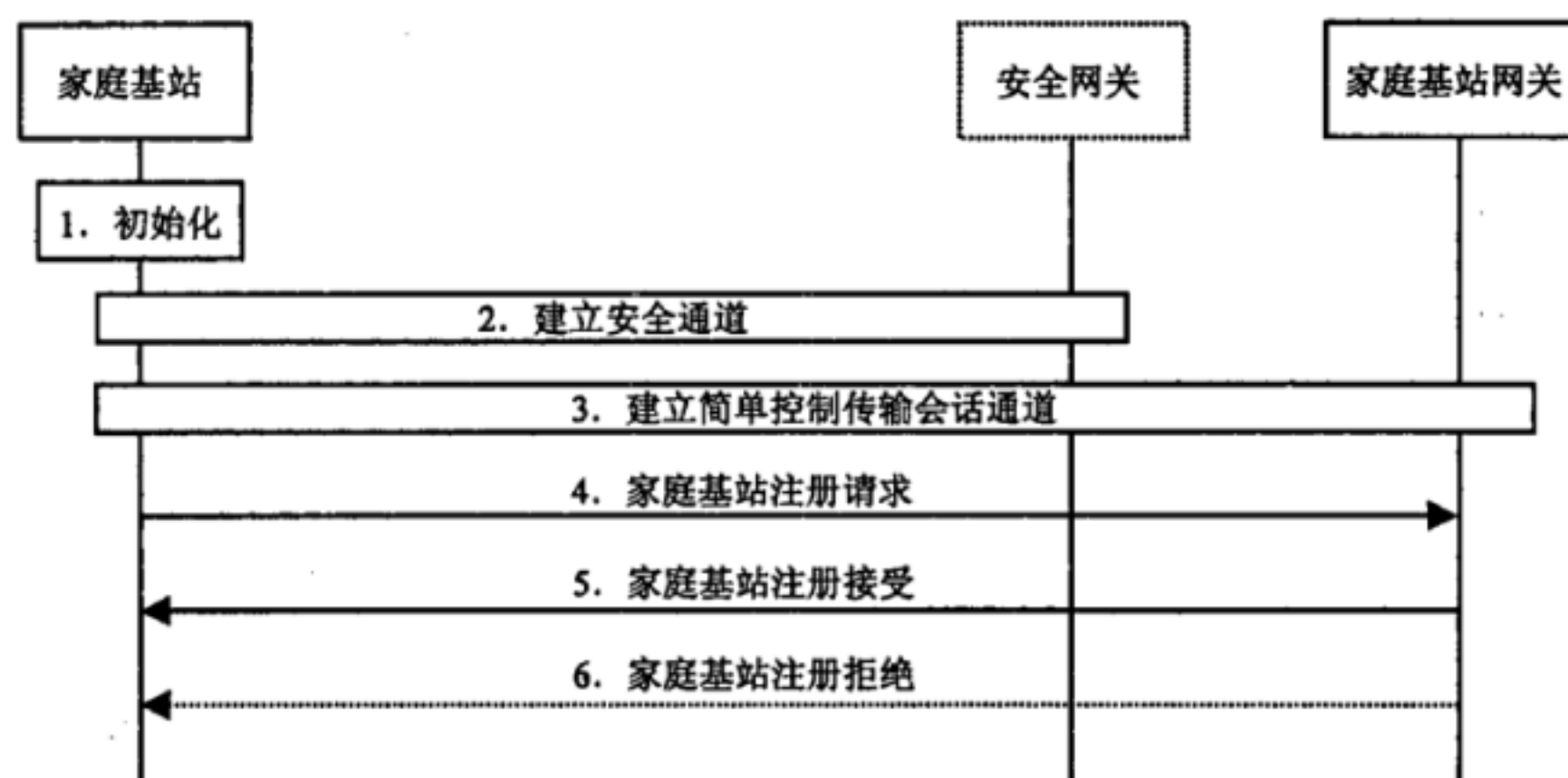
附录 A

(规范性附录)

HNB 注册过程

A.1 HNB注册

HNB注册过程如图A.1所示。



图A.1 HNB 注册过程

步骤1) HNB 初始化是用来从 HMS 中获取 HNB 配置。在该过程中, HNB 首先根据本地默认配置连接到初始 HNB GW (该过程需要 IPsec 隧道), 进而连接到 HMS 获取服务 HNB GW 地址;

步骤2) HNB 建立到服务 HNB GW 的 SeGW 的安全隧道 (如果该隧道与 HNB 到 HMS 是一个隧道, 该过程可被忽略);

步骤3) HNB 建立到 HNB GW 的 SCTP 传输会话通道;

步骤4) HNB 通过 HNB REGISTER REQUEST 消息试图向服务 HNB GW 注册, 消息中包括:

a) HNB 位置信息: HNB 通过一个或者多个机制提供位置信息:

- 检测到的宏小区覆盖信息 (例如 GERAN 和/或 UTRAN 小区信息);
- 地理信息 (例如, 通过 GPS 获得的);
- Internet 连接信息 (例如 IP 地址);

b) HNB 标识: HNB 拥有全球唯一且永久的标识;

c) HNB 运营参数: 例如 LAC、RAC、SAC 等标识的选择;

步骤5) HNB GW 应该使用 HNB REGISTER REQUEST 消息中的信息对 HNB 进行鉴权。如果 HNB GW 接受注册会回送 HNB REGISTER ACCEPT 消息;

步骤6) 否则, HNB GW 应该拒绝注册请求 (例如, 由于网络拥塞、HNB 黑名单、非授权 HNB 位置等)。在这种情况下, HNB GW 应该回送 HNB REGISTER REJECT 携带拒绝原因值。

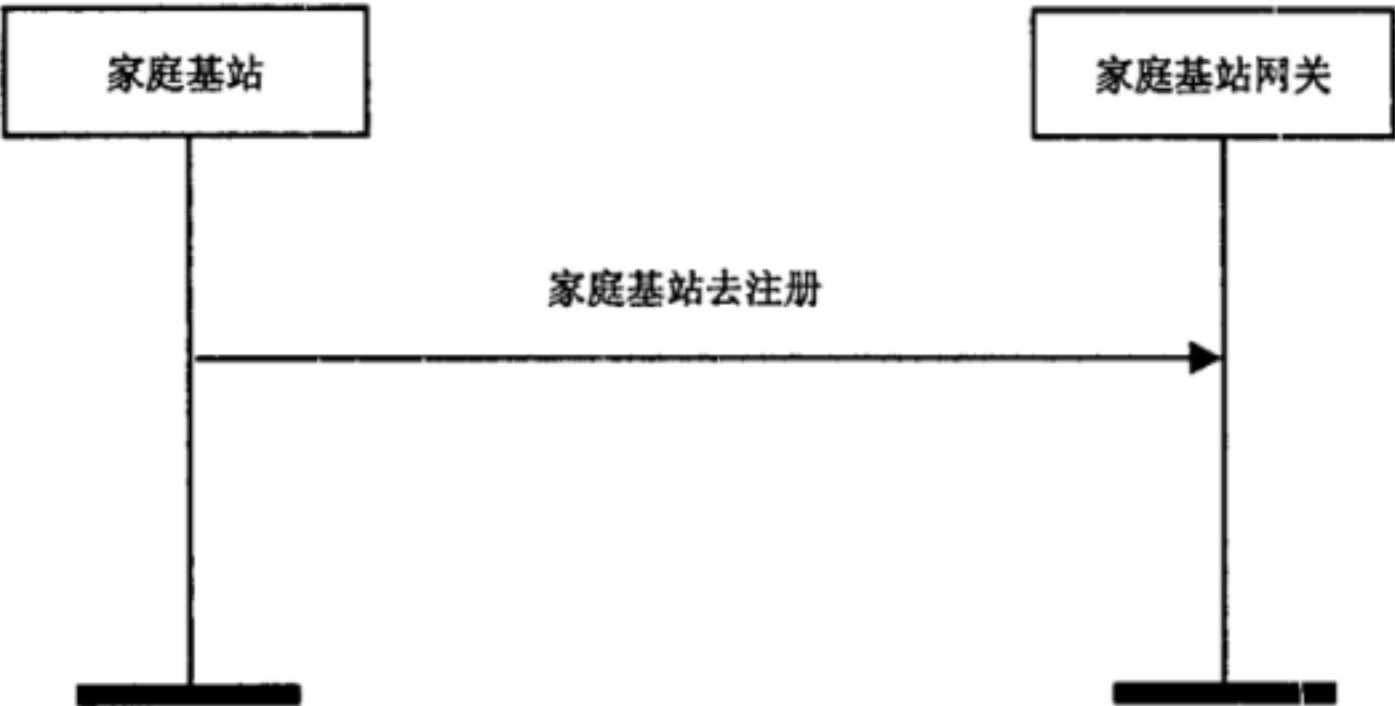
无线网络层原因:

- 非授权位置 (Unauthorised Location);
- 非授权 HNB (Unauthorised HNB);
- 过载 (Overload);
- HNB 参数不匹配 (HNB Parameter Mismatch);

— 未指明（Unspecified）。

A.2 HNB始发去注册

HNB 去注册过程如图 A.2 所示。



图A.2 HNB 去注册过程（HNB 始发）

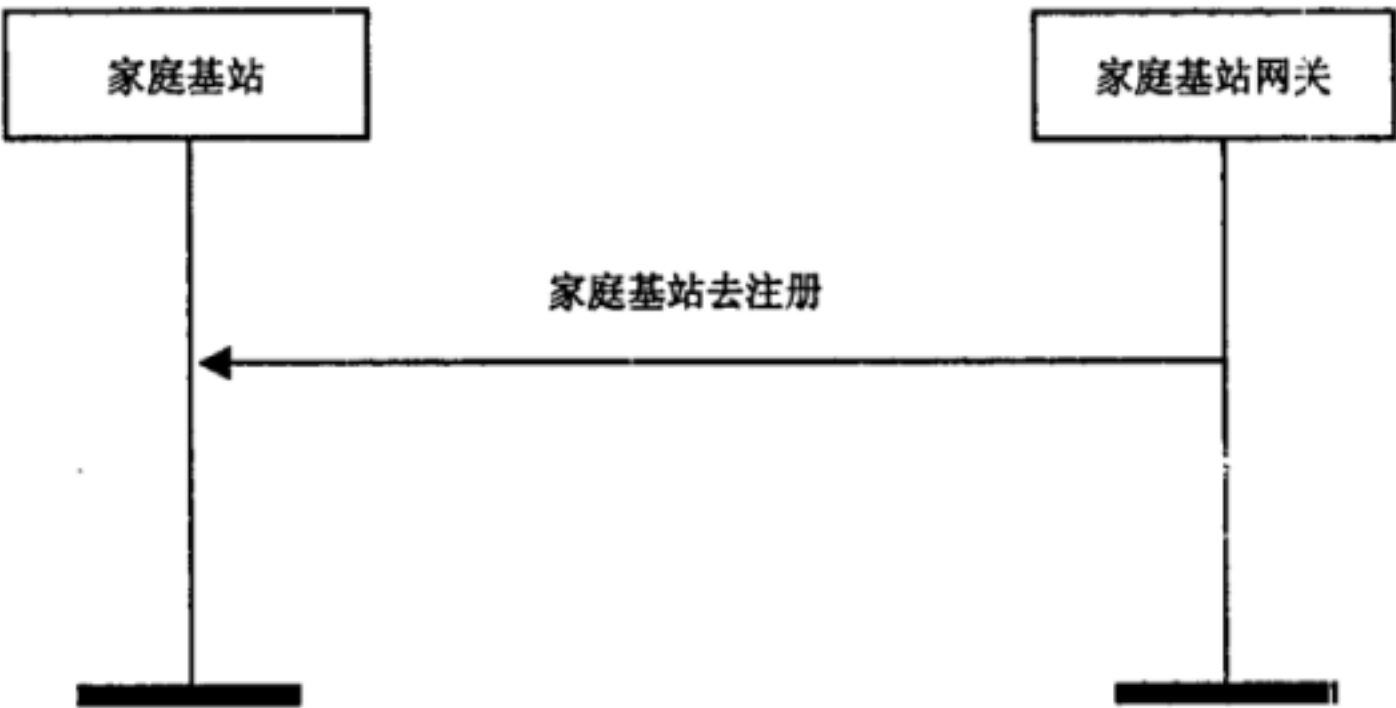
当 HNB 初始去注册过程时，HNB 发送去注册消息给 HNB GW。

无线网络层典型原因值：

- 正常释放（Normal）；
- 未指明（Unspecified）。

A.3 HNB GW始发去注册

HNB GW 始发去注册过程如图 A.3 所示。



图A.3 HNB 去注册过程（HNB GW 始发）

当HNB GW需要终止HNB提供服务时，初始去注册过程。

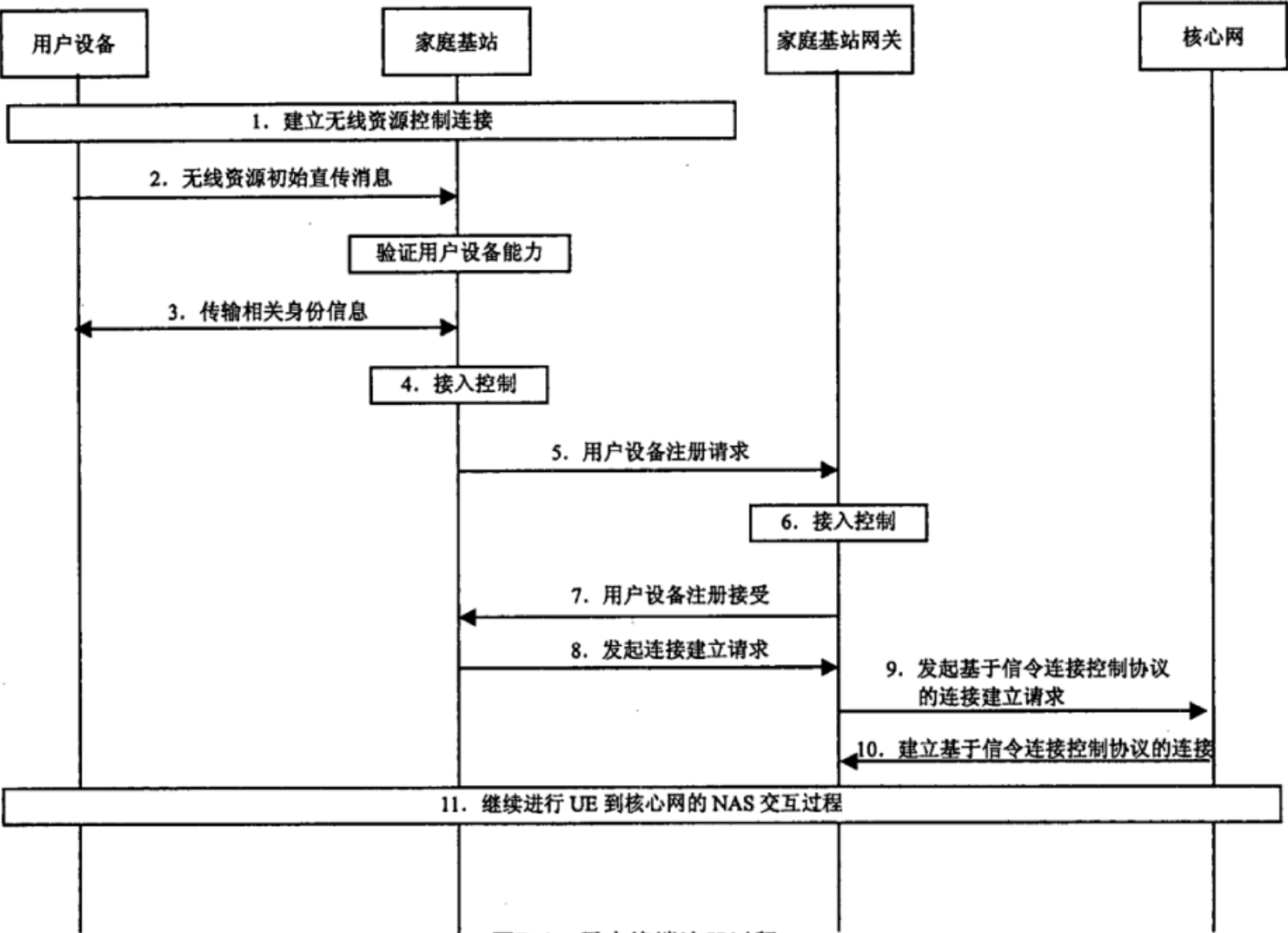
无线网络层典型原因值：

- 正常释放（Normal）；
- 未指明（Unspecified）。

附录 B
(规范性附录)
UE 注册功能

B.1 UE注册

用户终端注册过程如图B.1所示。



图B.1 用户终端注册过程

- 步骤1) 用户驻留在 HNB 后，建立与 HNB 的 RRC 连接以发起初始 NAS 过程（例如位置更新过程、呼叫建立请求等）。UE 标识、UE 能力和建立原因等作为 RRC 连接建立过程发送给 HNB；
- 步骤2) 之后 UE 发送 RRC Initial Direct Transfer 消息，携带 UE 初始 NAS 消息（例如位置更新请求消息、呼叫建立请求等）和 UE 标识；
- 步骤3) HNB 验证第一步中的 UE 能力，如果 UE 的标识在 HNB 中未注册过，HNB 就触发 UE 到 HNB GW 的注册。在 UE 注册过程开始之前，如果在非紧急呼叫情况下，UE 标识没有在 RRC Connection Establishment 中给出，HNB 触发取标识过程向 UE 索取 MSISDN。如果 UE 已经在 HNB 中注册，UE 注册过程将不会触发；
- 步骤4) HNB 根据 MSISDN 准入控制列表，可选的运行接入控制功能；
- 步骤5) HNB 试图向 HNB GW 发送 UE REGISTER REQUEST 实现注册，该消息至少包含：UE 的 IMSI、TMSI 和 UE 的能力；
- 步骤6) HNB GW 验证 UE 能力和注册原因。如果 UE 非紧急呼叫，HNB GW 应该运行接入控制；

步骤7) 如果 HNB GW 接受 UE 注册, 将返回 HNBAP 的 UE REGISTER ACCEPT 消息; 反之, 将返回 HNBAP UE REGISTER REJECT 消息;

步骤8) HNB 之后发送 RUA CONNECT 消息, 包含 RANAP Initial UE 消息;

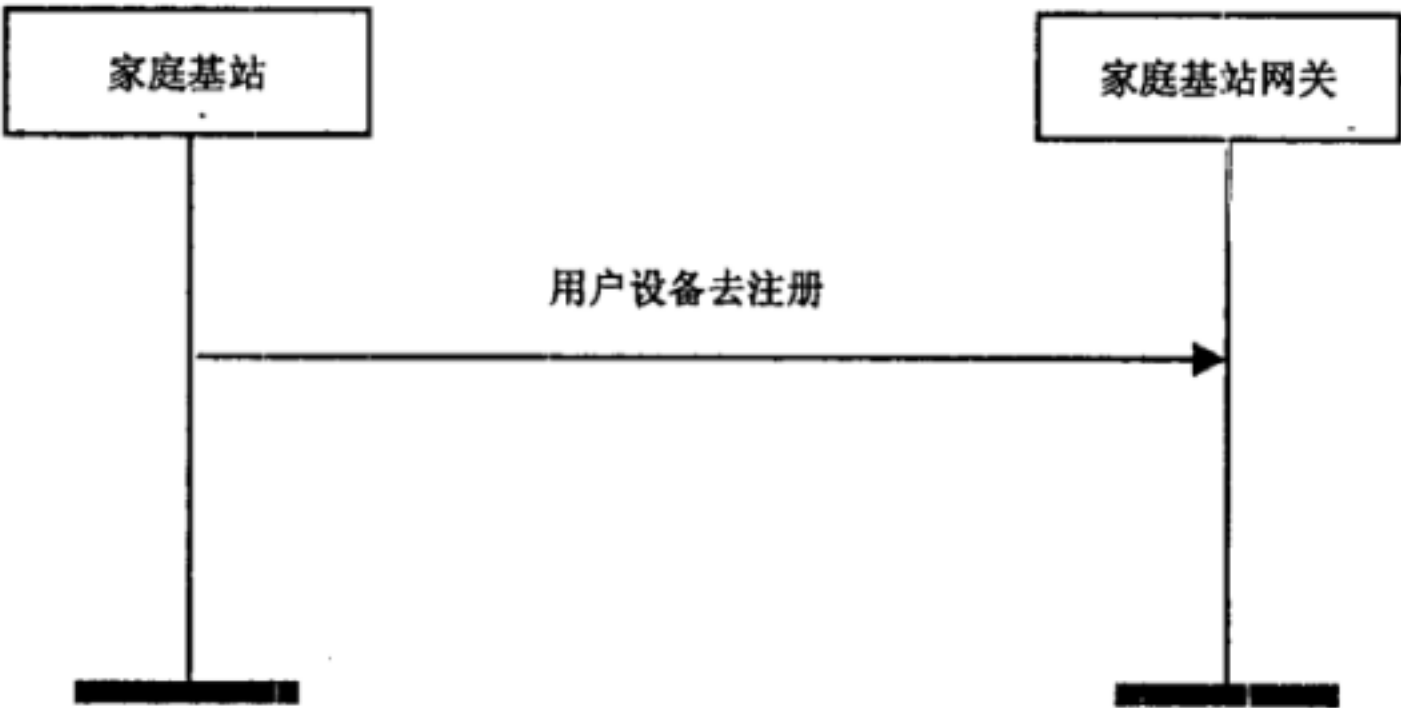
步骤9) HNB GW 接受 RUA CONNECT 消息触发了 HNB GW 到 CN 的 SCCP 连接的建立。HNB GW 发送 RANAP Initial UE 给 CN;

步骤10) CN 返回 SCCP 连接证实消息;

步骤11) UE 通过 HNB 和 HNB GW 继续到 CN 的 NAS 过程。

B.2 HNB始发UE去注册

HNB始发UE去注册成功过程如图B.2所示。



图B.2 HNB始发UE去注册成功过程

当HNB初始去注册过程时, HNB发送去注册消息给HNB GW。

典型原因值有无线网络层原因值:

- UE 连接丢失 (Connection with UE lost) ;
- UE RRC 释放 (UE RRC Release) ;
- UE 重定位 (UE relocated) ;
- 未指明 (Unspecified) 。

B.3 HNB GW始发UE去注册

HNB GW始发UE去注册成功过程如图B.3所示。



图B.3 HNB GW始发UE去注册成功过程

当HNB GW需要去注册UE时，初始去注册过程。

典型原因值有无线网络层原因值：

- UE 注册到其他 HNB (UE Registered in another HNB) ；
- 未指明 (Unspecified) 。

附录 C
(规范性附录)
HNB 认证

HNB可以支持对HNB设备和对宿主认证，HNB设备和网络之间的认证是双向的，网络侧需要对HNB标识进行认证，网络标识由HNB认证；网络对宿主的认证是可选的，对宿主的认证可以是独立的流程，也可以是与HNB设备认证绑定，如果宿主与HNB设备绑定，在HNB设备认证流程完成后，没有额外的认证过程。

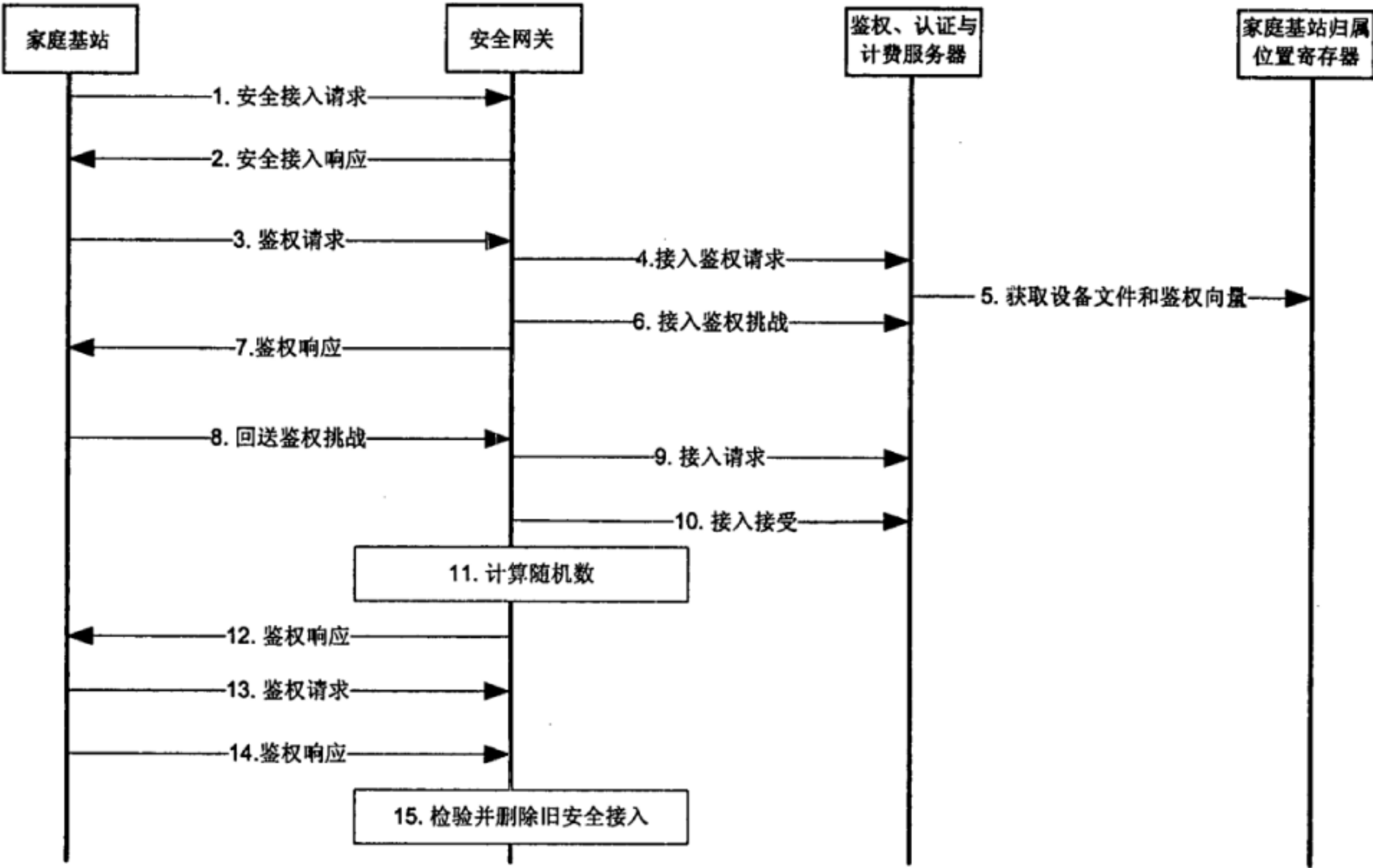
基于证书和 EAP-AKA 的认证可以用于 HNB 设备认证过程，也可以用于宿主认证，因此，HNB 认证可以有以下组合方式：

- 基于证书的 HNB 设备认证；
- 基于 EAP-AKA 的 HNB 设备认证；
- 基于证书的 HNB 设备+基于 EAP-AKA 的宿主认证；
- 基于 EAP-AKA 的 HNB 设备+基于 EAP-AKA 的宿主认证。

对宿主认证只考虑使用 EAP-AKA 认证方式。

C.1 EAP-AKA认证

基于 EAP-AKA 的 HNB 设备认证如图 C.1 所示，通过 HNB 和 SeGW 之间的 IKEv2 过程实现 HNB 和核心网之间的双向认证。鉴权流程如下：



图C.1 基于EAP-AKA鉴权过程

步骤1) HNB 发送一个 IKE_SA_INIT 请求给 SeGW;

步骤2) SeGW 发送 IKE_SA_INIT 响应, 向 HNB 请求一个证书;

步骤3) HNB 在 IKE_AUTH 中发送 HNB ID、AUTH 负荷、HNB 证书, 并且向 SeGW 请求一个证书;

步骤4) SeGW 检查从 HNB 得到的 AUTH 正确性, 并且计算 AUTH 参数用来认证下一个 IKE_SA_INIT 消息, SeGW 还认证从 HNB 得到的证书;

步骤5) SeGW 发送 AUTH 参数和它的证书给 HNB;

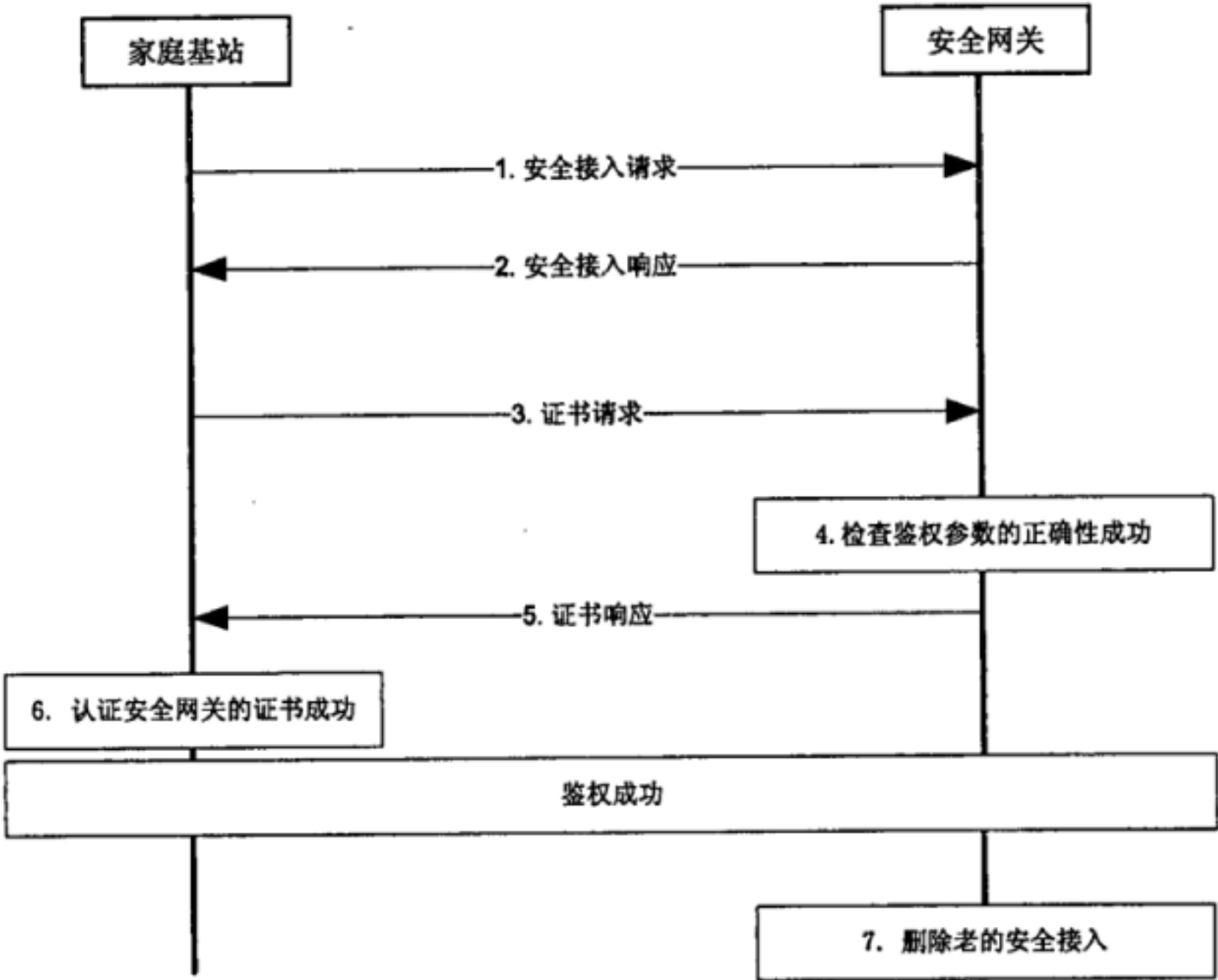
步骤6) HNB 利用存储的根证书认证 SeGW 的证书, SeGW 的根 signing public key 等用来认证 SeGW 证书的数据被存储在 TrE。为了更加安全, 整个认证过程都在 TrE 中进行;

步骤7) 如果 SeGW 检查到对于 HNB 存在老的 IKE SA, 会删除该 IKE SA, 发送一个 INFORMATIONAL 给 HNB, 携带了 Delete payload, 用来删除 HNB 中旧的 IKE SA。

- 步骤1) HNB 发送 IKE_SA_INIT 请求给 SeGW;
- 步骤2) SeGW 发送 IKE_SA_INIT 响应;
- 步骤3) HNB 在第一条鉴权消息中发送其设备标识和使用者标识, SeGW 判断使用 EAP 认证;
- 步骤4) SeGW 发送一条空 EAP AVP 的鉴权请求消息给 AAA 服务器, 携带在 IKE_AUTH 中获得的身份标识;
- 步骤5) 如果需要, AAA 服务器将从 HSS/HLR 中获得设备文件和鉴权向量;
- 步骤6) AAA 服务器将初始鉴权挑战;
- 步骤7) SeGW 发送 IKE_AUTH 响应给 HNB。从 AAA 服务器收到的 EAP-Request/AKA-Challenge 应包含在内。SeGW 的标识、证书和 AUTH 参数也应该包含在内, 以便 HNB 需要对 SeGW 进行认证;
- 步骤8) HNB 回送鉴权挑战的响应。HNB 可以验证 SeGW 的证书, 计算 EAP-AKA RES;
- 步骤9) SeGW 发送 EAP-Response/AKA-Challenge 给 AAA 服务器;
- 步骤10) 当所有认证都成功, AAA 服务器发送鉴权结果, 包含一个 EAP 成功和 SeGW 的 key material。key material 应该包含认证过程中产生的 MSK;
- 步骤11) MSK 是 SeGW 用来产生 AUTH 认证 IKE_SA_INIT 的;
- 步骤12) EAP 成功消息发送给 HNB;
- 步骤13) HNB 应该以 MSK 为输入产生 AUTH 参数来认证 IKE_SA_INIT 消息。之后 HNB 将 AUTH 发送给 SeGW;
- 步骤14) SeGW 检验 AUTH 的正确性, 并且计算 AUTN 参数认证第二条 IKE_SA_INIT 消息;
- 步骤15) SeGW 检验旧 IKE SA, 删除该 IKE SA 并发送 INFORMATIONAL exchange 用来删除 HNB 中的 IKE SA。

C.2 证书认证

基于证书HNB设备认证如图C.2所示, 通过HNB和SeGW之间的IKEv2过程实现HNB和核心网之间的双向认证。IKEv2的证书认证遵循IETF RFC-4306。



图C.2 基于证书鉴权过程

中华人民共和国
通信行业标准
2GHz TD-SCDMA 数字蜂窝移动通信网
家庭基站网关设备技术要求
YD/T 2513-2013

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880 × 1230 1/16 2013 年 5 月第 1 版
印张：2.25 2013 年 5 月北京第 1 次印刷
字数：55 千字

15115 • 199

定价：30 元

本书如有印装质量问题，请与本社联系 电话：(010)67114922