

# 中华人民共和国通信行业标准

YD/T 1340.2-2005

---

## 认证、授权、计费 (AAA) 服务器 认证计费接口技术要求 第二部分：宽带网络接入服务器

Technical requirments of Authentication Authorization Accounting (AAA)  
server interface part2: Broad Network Access Server (BNAS)

2005-05-11 发布

2005-11-01 实施

---

中华人民共和国信息产业部 发布

## 目 次

前 言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 定义 .....	1
4 缩略语 .....	2
5 RADIUS 报文格式 .....	2
6 报文和属性定义 .....	3
6.1 报文种类 .....	3
6.2 报文属性定义 .....	4
6.3 RADIUS 报文内容 .....	10
7 流程 .....	15
7.1 普通接入用户认证计费流程（必选） .....	15
7.2 管理用户认证流程（可选） .....	17
8 认证与计费的漫游 .....	17
8.1 认证类报文处理 .....	17
8.2 计费类报文漫游处理 .....	18
附录 A（规范性附录） VPDN 的业务流程 .....	20

## 前 言

认证、授权、计费（AAA）服务器认证计费接口技术要求分 3 部分：

1. 《认证、授权、计费（AAA）服务器认证计费接口技术要求第一部分：窄带网络接入服务器》
2. 《认证、授权、计费（AAA）服务器认证计费接口技术要求第二部分：宽带网络接入服务器》
3. 《认证、授权、计费（AAA）服务器认证计费接口技术要求第三部分：IP 电话》

本部分是第二部分。

本部分是以国际电信联盟标准化组织 (ITU-T)、互联网工程任务组 (IETF)、软交换论坛 (ISC) 制定的相关标准为基础，结合国内网络的实际情况和相关国内标准制定的。

本部分的附录 A 为规范性附录。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：华为技术有限公司

信息产业部电信研究院

本部分主要起草人：柯善阳 唐小光 郑志鹏 杨 崑 方 新

# 认证、授权、计费 (AAA) 服务器

## 认证计费接口技术要求

### 第二部分：宽带网络接入服务器

#### 1 范围

本部分规定了宽带接入服务器等系统与相应的 AAA 服务器之间完成认证、授权和计费功能的远端用户拨入鉴权服务 (RADIUS) 的接口标准。

本部分适用于宽带接入服务器、AAA 服务器。

#### 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

RFC 2865 (2000)	RADIUS 协议（草案标准）
RFC 2866 (2000)	RADIUS 计费协议（报告）
RFC 2867 (2000)	支持隧道协议的 RADIUS 计费协议（报告）
RFC 2868 (2000)	支持隧道协议 RADIUS（报告）
RFC 2869 (2000)	RADIUS 扩展（报告）
RFC 2903 (2000)	通用 AAA 架构

#### 3 定义

下列术语和定义适用于本部分。

##### 3.1

**宽带接入服务器** Broad Network Access Server

宽带接入服务器位于用户终端与 IP 骨干网之间的接入控制设备。可以为用户提供 xDSL、LAN 等接入方式，PC 机用户可以通过 xDSL Modem 或者网线直接接入城域网，经 IP 骨干网达到访问 Internet 的目的。

##### 3.2

**AAA 服务器** Service/Application Server

提供认证 (Authentication)、授权 (Authorization) 和计费 (Accounting) 功能的服务器。

##### 3.3

**RADIUS** Remote Authentication Dial in User Service

认证 (Authentication)、授权 (Authorization) 和计费 (Accounting) 的标准协议。RADIUS 协议采用客户/服务器 (Client/Server) 结构，采用 UDP 作为承载传输协议。RADIUS 的客户端通常运行在接入服务器上，客户端的任务是将用户 (User) 的信息发送到 RADIUS AAA 服务器上，然后根据服务器的不同响应进行处理。RADIUS 服务器通常运行在工作站或小型机上，其任务是接收客户端的请求，认证用户身份并授权合法用户登录。返回客户向用户提供服务时所需的配置信息。RADIUS 服务器的数据库中存放着所有的安全信息。

## 4 缩略语

下列缩略语适用于本部分。

AAA	Authentication Authorization and Accounting	认证、授权和计费
ADSL	Asymmetric Digital Subscriber Line	不对称数字用户线
BNAS	Broadband Network Access Server	宽带网络接入服务器
CHAP	Challenge-Handshake Authentication Protocol	握手认证协议
DSL	Digital Subscriber Line	数字用户线
FTP	File Transfer Protocol	文件传输协议
IANA	Internet Assigned Numbers Authority	互联网编号分配局
IDSL	ISDN DSL	ISDN 数字用户线
IPX	Internet Packet Exchange	因特网分组交换协议
MAC	Media Access Control	媒体接入控制
MTU	Maximum Transmission Unit	最大传输单元
PAP	Password Authentication Protocol	密码验证协议
PPP	Point-to-Point Protocol	点到点协议
PPPoA	PPP over ATM	ATM 网上点到点协议
PPPoE	PPP over Ethernet	以太网上点到点协议
RADIUS	Remote Authentication Dial in User Service	远端用户拨入鉴权服务
SIM	Subscriber Identity Module	用户标识模块
SLIP	Serial Line Internet Protocol	串行线路因特网协议
SSH	Secure Shell	安全外壳
VLAN	Virtual Local Area Network	虚拟局域网
VPDN	Virtual Digital Local Area Network	虚拟数字局域网

## 5 RADIUS 报文格式

(1) RADIUS 协议报文的格式定义如图 1 所示。

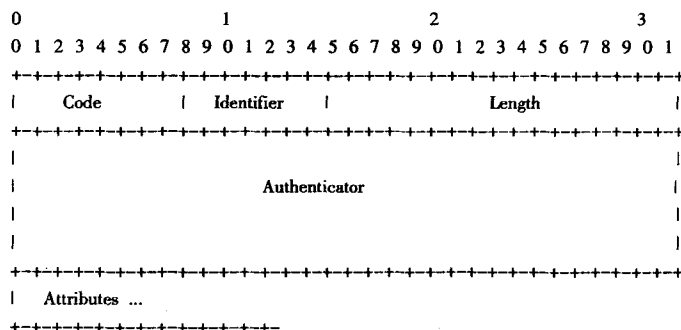


图 1 RADIUS 协议报文的格式定义

图 1 中:

Code: 编码, 表示报文类型。

Identifier: 标识符, 用于匹配请求和响应。重发报文标识符必须相同。

Length: 长度, 包括 Code、Identifier、Length、Authenticator、Attributes 的长度。  
Authenticator: 16 字节, 认证字作为加密随机数或者报文摘要。  
Attributes: 属性。  
(2) 报文属性的格式定义如图 2 所示。

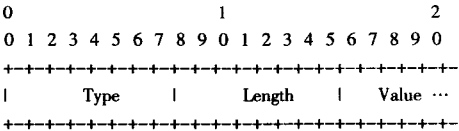


图 2 报文属性的格式定义

图 2 中:  
Type: 属性类型。  
Length: 属性长度, 包括 Type、Length 和 Value 的长度。  
Value: 属性值。

(3) 扩展属性的格式如图 3 所示。

所有的扩展属性都通过 RADIUS 的 Vendor-Specific 属性 (26) 进行扩展。对 Vendor-Specific 属性的扩展采用 RFC 2865 建议的扩展方式, 即一个扩展属性可以带一个或者多个子属性。一个 RADIUS 报文中可以有多个扩展属性。

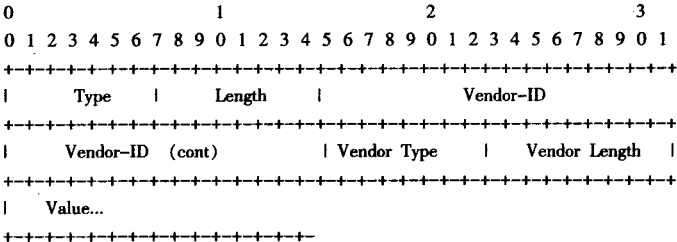


图 3 扩展属性的格式定义

图 3 中:  
Type: 属性类型, 固定为 26。  
Length: 属性长度, 包括 Type、Length、Vendor-ID、Vendor Type、Vendor Length 和 Value 的长度。  
Vendor-ID: 厂商 ID, 用来区分不同厂商。  
Vendor type: 子属性编号, 扩展属性表中的属性编号。  
Vendor length: 子属性的长度, 包括 Vendor Type、Vendor Length 和 Value 的长度。  
Value: 子属性的属性值。

6 报文和属性定义

BNAS 同 AAA 服务器通过 RADIUS 协议交互, 完成对上网用户的认证、授权和计费。

6.1 报文种类

使用以下几种类型的报文, 见表 1。

表 1 报文种类

序 号	编 码 (Code)	M/O	名 称	描 述
1	1	M	Access-Request	认证请求报文
2	2	M	Access-Accept	对 Access-Request 报文认证通过的响应报文
3	3	M	Access-Reject	对 Access-Request 报文认证失败的响应报文
4	4	M	Acct-Start-Request	计费开始报文
5	4	M	Acct-Update-Request	中间计费实时报文
6	4	M	Acct-Stop-Request	计费结束报文
7	4	O	Acct-On-Request	设备计费起始报文
8	4	O	Acct-Off-Request	设备计费终止报文
9	5	M	Acct-Response	计费响应报文 (计费开始、中间计费或者计费结束报文的响应)
10	11	O	Access-Challenge	认证质询报文

注:

表 1 中“M”表示必选,“O”表示可选。

Acct-Start-Request: 用户正常上网后 BNAS 发送该报文, 表示该用户开始计费。如果一定时间 (要求时长可以配置) 后 BNAS 没有收到 AAA 的计费响应, BNAS 需要一定次数的重发 (要求重发次数可以配置)。

Acct-Update-Request: BNAS 定时上报或者 BNAS 检测到用户可用业务量 (时长或者流量) 用完时上报。如果一定时间 (要求时长可以配置) 后 BNAS 没有收到 AAA 的计费响应, BNAS 需要一定次数的重发 (要求重发次数可以配置)。如果上报的 Acct-Update-Request 报文时, 以前的计费报文 (包括 Acct-Start-Request 和 Acct-Update-Request) 还没有收到响应, 则以前的计费报文不再重发。中间计费实时报文中的计费信息是累积的, 即报文中的发送流量包数是从会话开始的总的流量和包数, 而不是从上一个中间计费实时报文以后的流量和包数。

Acct-Stop-Request: 用户下线或者 BNAS 切断用户或者计费响应中的可用业务量 (Session-Timeout 或者 Remanent-Volume) 为 0 时发送。如果一定时间后 BNAS 没有收到 AAA 的计费响应, BNAS 需要重发一定的次数后 (要求重发次数可以配置), 如果还没有收到响应此时必须能记录异常话单, 用于和 AAA 进行异常话单对账。发送计费结束请求后, 其他计费请求不再重发。计费结束报文中的计费信息也是累积的, 即报文中的发送流量包数是从会话开始的总的流量和包数, 而不是从上一个中间计费实时报文以后的流量和包数。

Acct-On-Request 在设备启动时发送, 是针对设备而言的 (Acct-Start-Request 是针对用户而言的)。

Acct-Off-Request 在设备关闭时发送, 是针对设备而言的 (Acct-Stop-Request 是针对用户而言的)。

Acct-Response: 计费请求报文的响应。AAA 收到每个计费报文, 正确处理后都必须给 BNAS 发送该报文。计费响应报文可以包含 Session-Timeout 和 Remanent-Volume 属性, BNAS 根据最后一个 Acct-Response 的这两个属性更新用户的可用时长和可用流量。

Access-Challenge: 认证质询报文。可以作为 Access-Request 的响应从 AAA 服务器发送给 BNAS。AAA 服务器用该报文向用户询问一些信息, 或者和用户的客户端协商认证方式。

## 6.2 报文属性定义

报文属性定义见表 2。

表 2 报文属性定义

编 号	名 称	类 型	描 述
1	User-Name	String	用户名。可以是用户登录名或者网络接入标识（如逻辑端口号）
2	User-Password	String	用户密码。 PAP 认证时的 Access-Request 报文中必须包含本属性，长度为 $N \times 16$ （ $N$ 为小于 9 的正整数）
3	CHAP-Password	String	CHAP 认证密码。长度固定为 17，只对 CHAP 认证时才有效
4	NAS-IP-Address	Address	BNAS 的 IP 地址。同 NAS-Identifier 两者至少必备其一。 此值可能跟 AAA 服务器收到的实际的 RADIUS IP 包的源地址不符（比如 RADIUS 包穿透 NAT 后）
5	NAS-Port	Integer	用户接入的 BNAS 逻辑端口号。与 NAS-Port-ID 属性含义相同，推荐采用 NAS-Port-ID 属性
6	Service-Type	Integer	服务类型： 1 — 登录服务（Login）； 2 — 帧服务（Framed）； 4 — 回呼帧服务（Callback Framed）； 5 — 外部访问服务（Outbound）； 6 — 管理服务（Administrative）； 7 — 提示服务（NAS Prompt）； 8 — 仅认证服务（Authenticate Only）
7	Framed-Protocol	Integer	帧协议。当前标准协议没有能很好的区别 PPPoE 和 VLAN，暂时都填成 PPP。 1 — 点对点协议（PPP）； 2 — 串行 IP 协议（SLIP）； 7 — GRPS PDP Context（3GPP 定义）
8	Framed-IP-Address	Address	用户 IP 地址。 若分配地址，必须是合法地址，不能是 0.0.0.0 或者 127.***.***.***
9	Framed-IP-Netmask	Address	用户所在子网的网络掩码
10	Framed-Routing	Integer	帧路由方法： 0 — 无（None）； 1 — 发送路由包（Send routing packets）； 2 — 监听路由包（Listen for routing packets）； 3 — 发送和监听（Send and Listen）
11	Filter-ID	Text	访问控制列表的名字。名字对应的访问控制列表可以在 BNAS 上配置。如果 BNAS 不支持多 Filter-ID，则只有最后一个 Filter-ID 起作用
12	Framed-MTU	Integer	最大传输单元。64-65535
13	Framed-Compression	Integer	帧压缩协议： 0 — 无压缩（None）； 1 — TCP/IP 头压缩（VJ TCP/IP header compression）； 2 — IPX 头压缩（IPX header compression）； 3 — Stac-LZS 压缩（Stac-LZS compression）



表 2 (续)

编 号	名 称	类 型	描 述
14	Login-IP-Host	Address	Login 主机 IP 地址。用于表示管理用户登录后允许登录的主机地址
15	Login-Service	Integer	表示用户连接到主机所使用的服务, 用于管理用户。 0—Telnet; 1—远程登录 (Rlogin); 2—TCP 透传 (TCP Clear); 50—SSH; 51—Ftp; 52—Terminal
16	Login-TCP-Port	Integer	表示用户连接到主机所使用的 TCP 端口, 用于管理用户。0..65535
18	Reply-Message	Text	认证响应信息。可以用于设备上的调试信息, 在使用 PPPoE/Web 认证时可以向用户显示接入失败的原因
19	Callback-Number	String	主要用于 WLAN 中。认证服务器传递过来可以显示给用户的信息, 如移动电话号码等
22	Framed-Route	Text	AAA 为 BNAS 上用户配置的路由信息
23	Framed-IPX-Network	Integer	AAA 为用户配置的 IPX 网络号
24	State	String	状态。 如果 AAA 服务器在 Access-Challenge 中下发, 要求 BNAS 在下一个 Access-Request 中原封不动地上报
25	Class	String	如果 AAA 服务器在 Access-Accept 中下发, 要求 BNAS 必须在 Accounting-Request 报文中原封不动地上报。BNAS 不需要理解该属性的含义
26	Vendor-Specific	String	厂家自定义属性。一个报文中可以有一个或者多个自定义属性。一个自定义属性中可以有一个或者多个子属性。具体属性扩展参见后续定义
27	Session-Timeout	Integer	表示用户剩余的时间, 以 s 为单位, 可以用于时长预付费。该属性可以在 Access-Accept 和 Acct-Response 中下发, BNAS 根据最后一个响应报文中的该属性确定用户的最大可用时长
28	Idle-Timeout	Integer	表示用户的闲置切断时间, 以 s 为单位。 闲置的标准为一界定流速, 单位为 (0~768000) k 字节/min。由各个设备自己设定
29	Termination-Action	Integer	指示业务结束后的 BNAS 应该动作。 0—一切断用户 (Default); 1—重认证 (RADIUS-Request)
31	Calling-Station-ID	String	用户的 MAC 地址。如果 BNAS 可以获得用户的 MAC 地址, 则应该上报。 格式为 hh: hh: hh: hh: hh: hh
32	NAS-Identifier	String	BNAS 设备的名字。同 NAS-IP-Address 两者至少必备其一
33	Proxy-State	String	代理状态。参照 RFC 2865 定义

表 2 (续)

编 号	名 称	类 型	描 述
40	Acct-Status-Type	Integer	表示计费请求报文的类型： 1 — 计费开始 (Start)； 2 — 计费停止 (Stop)； 3 — 计费更新 (Interim-Update)； 9 — 隧道开始 (Tunnel-Start)； 10 — 隧道停止 (Tunnel-Stop)； 11 — 隧道拒绝 (Tunnel-Reject)； 12 — 隧道链路开始 (Tunnel-Link-Start)； 13 — 隧道链路停止 (Tunnel-Link-Stop)； 14 — 隧道链路拒绝 (Tunnel-Link-Reject)
41	Acct-Delay-Time	Integer	计费延迟时间。用于上报发送该计费包花费的时间，以 s 为单位（不包括网络传输时间）
42	Acct-Input-Octets	Integer	表示 BNAS 从用户端口接收的字节数
43	Acct-Output-Octets	Integer	表示 BNAS 发送给用户端口的字节数
44	Acct-Session-ID	Text	惟一的标识一个会话的值，在很长的时间内都不重复（即使设备重启了）
45	Acct-Authentic	Integer	用户所使用的认证方式： 1 — RADIUS 认证 (RADIUS)； 2 — 本地认证 (Local)； 3 — 远端认证 (Remote)
46	Acct-Session-Time	Integer	计费会话时长，单位为 s
47	Acct-Input-Packets	Integer	表示 BNAS 从用户端口接收的包数
48	Acct-Output-Packets	Integer	表示 BNAS 发送给用户端口的包数
49	Acct-Terminate-Cause	Integer	计费终止原因。 1 — 用户请求 (User Request)； 2 — 载波丢失 (Lost Carrier)； 3 — 服务丢失 (Lost Service)； 4 — 空闲超时 (Idle Timeout)； 5 — 会话超时 (Session Timeout)； 6 — 管理员重置 (Admin Reset)； 7 — 管理员重启 (Admin Reboot)； 8 — 端口错误 (Port Error)； 9 — 设备错误 (NAS Error)； 10 — 设备请求 (NAS Request)； 11 — 设备重启 (NAS Reboot)； 12 — 端口不再需要 (Port Unneeded)； 13 — 端口被抢占 (Port Preempted)； 14 — 端口挂起 (Port Suspended)； 15 — 服务不可用 (Service Unavailable)； 16 — 回呼 (Callback)； 17 — 用户错误 (User Error)； 18 — 主机请求 (Host Request)； 19 — 流量用完 (Volume Exceed)

表 2 (续)

编 号	名 称	类 型	描 述
52	Acct-Input-Gigawords	Integer	表示 Acct-Input-Octets 的溢出次数。 如果计费请求中包含该属性, 表示 BNAS 从用户端口接收的字节数是 $(2^{25} \times \text{Acct-Input-Gigawords}) + \text{Acct-Input-Octets}$
53	Acct-Output-Gigawords	Integer	表示 Acct-Output-Octets 的溢出次数。 如果计费请求中包含该属性, 表示 BNAS 发送给用户端口的字节数是 $(2^{25} \times \text{Acct-Output-Gigawords}) + \text{Acct-Output-Octets}$
55	Event-Timestamp	Integer	计费报文时间戳, 计费报文上报的时间。 表示从 1970 年 1 月 1 日 UTC 00: 00: 00 以来的秒数
60	CHAP-Challenge	String	CHAP 认证随机数。 用于 CHAP 认证, 即使 Challenge 为 16 字节, 也应该在 Authenticator (报文头中的认证字) 和本属性中同时填入, 因为不同的服务器可能从请求包的不同地方去取该值并进行 CHAP 认证
61	NAS-Port-Type	Integer	用户接入端口类型: 11 —SDSL (Symmetric DSL); 12 —ADSL-CAP (Asymmetric DSL, Carrierless Amplitude Phase Modulation); 13 —ADSL-DMT (Asymmetric DSL, Discrete Multi-Tone); 14 —IDSL (ISDN Digital Subscriber Line); 15 —以太网 (Ethernet); 16 —xDSL (Digital Subscriber Line of unknown type); 17 —有线电视电缆 (Cable); 18 —Wireless-Other; 19 —Wireless-IEEE 802.11; 201 —VLAN (包括以太网和 ATM 上的 VLAN); 202 —ATM
64	Tunnel-Type	Integer	隧道协议类型
65	Tunnel-Medium-Type	Integer	隧道媒体种类
66	Tunnel-Client-Endpoint	String	隧道发起端 (BNAS) 的 IP 地址
67	Tunnel-Server-Endpoint	String	隧道终端 (LNS) 的 IP 地址
68	Acct-Tunnel-Connection	String	隧道连接 ID
69	Tunnel-Paseword	String	隧道密码 (密文)
79	EAP-Message	String	携带 EAP 信息
80	Message-Authenticator	String	消息验证字
81	Tunnel-Private-Group-ID	String	用作 VPDN 组号
82	Tunnel-Assignment-ID	String	隧道会话 ID
83	Tunnel-Preference	Integer	隧道优先级。值越小优先级越高
85	Acct-Interim-Interval	Integer	上报中间计费更新报文的时间间隔。单位为 s。如果 AAA 下发了该属性, BNAS 应该根据该属性调整实时计费报文的上报间隔

表 2 (续)

编 号	名 称	类 型	描 述
86	Acct-Tunnel-Packets-Lost	Integer	隧道丢失的包数
87	NAS-Port-ID	String	用户接入的 BNAS 逻辑端口号。与 NAS-Port 属性含义相同, 推荐采用 NAS-Port-ID 属性
88	Framed-Pool	String	用字符串来描述的地址池
90	Tunnel-Client-Auth-ID	Integer	本地隧道名
91	Tunnel-Server-Auth-ID	Integer	终结者隧道名
26-XXXX-1	Input-Peak-Rate	Integer	用户接入到 BNAS 的峰值速率, 以 bit/s 为单位 (如果 AAA 下发该属性, BNAS 应该支持)
26-XXXX-2	Input-Average-Rate	Integer	用户接入到 BNAS 的平均速率, 以 bit/s 为单位 (如果 AAA 下发该属性, BNAS 应该支持)
26-XXXX-3	Input-Basic-Rate	Integer	用户接入到 BNAS 的基本速率, 以 bit/s 为单位 (这个域目前没有意义, 建议不要使用)
26-XXXX-4	Output-Peak-Rate	Integer	从 BNAS 到用户的峰值速率, 以 bit/s 为单位 (如果 AAA 下发该属性, BNAS 应该支持)
26-XXXX-5	Output-Average-Rate	Integer	从 BNAS 到用户的平均速率, 以 bit/s 为单位 (如果 AAA 下发该属性, BNAS 应该支持)
26-XXXX-6	Output-Basic-Rate	Integer	从 BNAS 到用户的基本速率, 以 bit/s 为单位 (这个域目前没有意义, 建议不要使用)
26-XXXX-15	Remanent-Volume	Integer	可以在 Access-Accept 或者 Acct-Response 报文中下发。单位为字节, 表示该连接的剩余可用总流量。BNAS 以 RADIUS Server 最后下发的值为准
26-XXXX-22	Priority	Integer	服务的优先级, 值越小优先级越高
26-XXXX-26	Connect-ID	Integer	此属性代表用户连接索引, 如果 BNAS 在请求报文中上报了该属性, 则 AAA 必须在对应的响应报文中原封不动下发
26-XXXX-27	PortalURL	String	字符串属性, 长度最大为 253。强制用户进入门户网站 URL
26-XXXX-28	Ftp-Directory	String	FTP 用户工作目录, 字符串属性, 长度最大为 64 字节。 对于 FTP 用户, 当 BNAS 作为 FTP 服务器的时候, 设置 BNAS 上的 FTP 目录。AAA 服务器在认证接收报文中, 可以用属性 Ftp-Directory 携带 FTP 用户的 FTP 目录。该属性是针对管理用户的设置
26-XXXX-29	Exec-Privilege	Integer	EXEC 用户优先级。 对于 EXEC 用户, 用来设置 EXEC 用户的优先级。AAA 服务器在认证接收报文中, 可以用属性 Exec-Privilege 携带 EXEC 用户的优先级。该属性是针对管理用户的设置
26-XXXX-59	NAS-Startup-Timestamp	Time	BNAS 系统启动时刻。以 s 为单位, 表示从 1970 年 1 月 1 日 UTC 00: 00: 00 以来的秒数
26-XXXX-135	Client-Primary-DNS	Address	第一 DNS 服务器地址

表 2 (续)

编 号	名 称	类 型	描 述
26-XXXX-136	Client-Secondary-DNS	Address	第二 DNS 服务器地址
26-XXXX-137	DSLAM-Port-Id	String	用户接入的 DSLAM 逻辑端口
26-XXXX-254	Version	String	BNAS 产品的版本号
26-XXXX-255	Product-ID	String	BNAS 产品名称

注:

text: 1~253 个符合 UTF-8 编码格式的字符, 如果长度为“0”则不发送该属性。

string: 1~253 个二进制 (取值包含 0~255) 八位位组, 如果长度为“0”则不发送该属性。

address: 32 比特, 网络字节序。

integer: 32 比特无符号数, 网络字节序。

time: 32 比特, 网络字节序; 表示从 1970 年 1 月 1 日 0 时 0 分 0 秒以来所经历的秒数。

### 6.3 RADIUS 报文内容

#### 6.3.1 认证报文

认证报文的属性见表 3。

表 3 认证报文属性

属性编号	属性名	Access-Request	Access-Accept	Access-Reject	Access-Challenge
1	User-Name	0-1	0-1	0	0
2	User-Password	0-1	0	0	0
3	CHAP-Password	0-1	0	0	0
4	NAS-IP-Address	0-1	0	0	0
5	NAS-Port	0-1	0	0	0
6	Service-Type	0-1	0-1	0	0
7	Framed-Protocol	0-1	0-1	0	0
8	Framed-IP-Address	0-1	0-1	0	0
9	Framed-IP-Netmask	0-1	0-1	0	0
10	Framed-Routing	0	0-1	0	0
11	Filter-ID	0	0+	0	0
12	Framed-MTU	0-1	0-1	0	0
13	Framed-Compression	0+	0+	0	0
14	Login-IP-Host	0+	0+	0	0
15	Login-Service	0	0-1	0	0
16	Login-TCP-Port	0	0-1	0	0
18	Reply-Message	0	0+	0+	0+
19	Callback-Number	0-1	0-1	0	0

表 3 (续)

属性编号	属性名	Access-Request	Access-Accept	Access-Reject	Access-Challenge
22	Framed-Route	0	0+	0	0
23	Framed-IPX-Network	0	0-1	0	0
24	State	0-1	0-1	0	0-1
25	Class	0	0+	0	0
26	Vendor-Specific	0+	0+	0	0+
27	Session-Timeout	0	0-1	0	0-1
28	Idle-Timeout	0	0-1	0	0-1
29	Termination-Action	0	0-1	0	0
31	Calling-Station-ID	0-1	0	0	0
32	NAS-Identifier	0-1	0	0	0
33	Proxy-State	0+	0+	0+	0+
40	Acct-Status-Type	0	0	0	0
41	Acct-Delay-Time	0	0	0	0
42	Acct-Input-Octets	0	0	0	0
43	Acct-Output-Octets	0	0	0	0
44	Acct-Session-ID	0	0	0	0
45	Acct-Authentic	0	0	0	0
46	Acct-Session-Time	0	0	0	0
47	Acct-Input-Packets	0	0	0	0
48	Acct-Output-Packets	0	0	0	0
49	Acct-Terminate-Cause	0	0	0	0
52	Acct-Input-Gigawords	0	0	0	0
53	Acct-Output-Gigawords	0	0	0	0
55	Event-Timestamp	0	0	0	0
60	CHAP-Challenge	0-1	0	0	0
61	NAS-Port-Type	0-1	0	0	0
64	Tunnel-Type	0+	0+	0	0
65	Tunnel-Medium-Type	0+	0+	0	0
66	Tunnel-Client-Endpoint	0+	0+	0	0
67	Tunnel-Server-Endpoint	0+	0+	0	0
68	Acct-Tunnel-Connection	0	0	0	0

表 3 (续)

属性编号	属性名	Access-Request	Access-Accept	Access-Reject	Access-Challenge
69	Tunnel-Password	0	0+	0	0
79	EAP-Message	0+	0+	0+	0+
80	Message-Authenticator	0-1	0-1	0-1	0-1
81	Tunnel-Private-Group-ID	0+	0+	0	0
82	Tunnel-Assignment-ID	0	0+	0	0
83	Tunnel-Preference	0+	0+	0	0
85	Acct-Interim-Interval	0	0-1	0	0
86	Acct-Tunnel-Packets-Lost	0	0	0	0
87	NAS-Port-ID	0-1	0	0	0
88	Framed-Pool	0	0-1	0	0
90	Tunnel-Client-Auth-ID	0+	0+	0	0
91	Tunnel-Server-Auth-ID	0+	0+	0	0
26-XXXX-1	Input-Peak-Rate	0	0-1	0	0
26-XXXX-2	Input-Average-Rate	0	0-1	0	0
26-XXXX-3	Input-Basic-Rate	0	0-1	0	0
26-XXXX-4	Output-Peak-Rate	0	0-1	0	0
26-XXXX-5	Output-Average-Rate	0	0-1	0	0
26-XXXX-6	Output-Basic-Rate	0	0-1	0	0
26-XXXX-15	Remanent-Volume	0	0-1	0	0
26-XXXX-22	Priority	0-1	0-1	0	0
26-XXXX-26	Connect-ID	0-1	0-1	0-1	0-1
26-XXXX-27	PortalURL	0	0-1	0	0
26-XXXX-28	Ftp-Directory	0	0-1	0	0
26-XXXX-29	Exec-Privilege	0	0-1	0	0
26-XXXX-59	NAS-Startup-Timestamp	0-1	0	0	0
26-XXXX-135	Client-Primary-DNS	0	0-1	0	0
26-XXXX-136	Client-Secondary-DNS	0	0-1	0	0
26-XXXX-137	DSLAM-Port-ID	0-1	0	0	0
26-XXXX-254	Version	0-1	0	0	0
26-XXXX-255	Product-ID	0-1	0	0	0

注：26号扩展属性中的XXXX为Vendor-ID，这里为各个厂商向IANA申请的自己的标志。

表格格式说明：

0：属性一定不会出现在报文中；

0+：0个或多个属性可能会出现在报文中；

0-1：0或一个属性可能出现在报文中；

1：确定的一个属性一定会出现在报文中。

### 6.3.2 计费报文

计费报文的属性见表4。

表4 计费报文属性

属性编号	属性名	Acct-Start -Request	Acct-update -Request	Acct-stop -Request	Acct-On -Request	Acct-Off -Request	Acct- Response
1	User-Name	0-1	0-1	0-1	0	0	0
2	User-Password	0	0	0	0	0	0
3	CHAP-Password	0	0	0	0	0	0
4	NAS-IP-Address	0-1	0-1	0-1	0-1	0-1	0
5	NAS-Port	0-1	0-1	0-1	0	0	0
6	Service-Type	0-1	0-1	0-1	0	0	0
7	Framed-Protocol	0-1	0-1	0-1	0	0	0
8	Framed-IP-Address	0-1	0-1	0-1	0	0	0
9	Framed-IP-Netmask	0-1	0-1	0-1	0	0	0
10	Framed-Routing	0-1	0-1	0-1	0	0	0
11	Filter-ID	0+	0+	0+	0	0	0
12	Framed-MTU	0-1	0-1	0-1	0	0	0
13	Framed-Compression	0+	0+	0+	0	0	0
14	Login-IP-Host	0+	0+	0+	0	0	0
15	Login-Service	0-1	0-1	0-1	0	0	0
16	Login-TCP-Port	0-1	0-1	0-1	0	0	0
18	Reply-Message	0	0	0	0	0	0
19	Callback-Number	0-1	0-1	0-1	0	0	0
22	Framed-Route	0+	0+	0+	0	0	0
23	Framed-IPX-Network	0-1	0-1	0-1	0	0	0
24	State	0	0	0	0	0	0
25	Class	0+	0+	0+	0+	0+	0
26	Vendor-Specific	0+	0+	0+	0+	0+	0+
27	Session-Timeout	0-1	0-1	0-1	0	0	0-1
28	Idle-TimeOut	0-1	0-1	0-1	0	0	0



表 4 (续)

属性编号	属性名	Acct-Start -Request	Acct-update -Request	Acct-stop -Request	Acct-On -Request	Acct-Off -Request	Acct- Response
29	Termination-Action	0-1	0-1	0-1	0	0	0
30	Called-Station-ID	0-1	0-1	0-1	0	0	0
31	Calling-Station-ID	0-1	0-1	0-1	0	0	0
32	NAS-Identifier	0-1	0-1	0-1	0-1	0-1	0
33	Proxy-State	0+	0+	0+	0+	0+	0+
40	Acct-Status-Type	1	1	1	1	1	0
41	Acct-Delay-Time	0-1	0-1	0-1	0-1	0-1	0
42	Acct-Input-Octets	0	0-1	0-1	0	0	0
43	Acct-Output-Octets	0	0-1	0-1	0	0	0
44	Acct-Session-ID	1	1	1	0	0	0
45	Acct-Authentic	0-1	0-1	0-1	0	0	0
46	Acct-Session-Time	0	0-1	0-1	0	0	0
47	Acct-Input-Packets	0	0-1	0-1	0	0	0
48	Acct-Output-Packets	0	0-1	0-1	0	0	0
49	Acct-Terminate-Cause	0	0	0-1	0	0-1	0
52	Acct-Input-Gigawords	0	0-1	0-1	0	0	0
53	Acct-Output-Gigawords	0	0-1	0-1	0	0	0
55	Event-Timestamp	0-1	0-1	0-1	0-1	0-1	0
60	CHAP-Challenge	0	0	0	0	0	0
61	NAS-Port-Type	0-1	0-1	0-1	0	0	0
64	Tunnel-Type	0-1	0-1	0-1	0	0	0
65	Tunnel-Medium-Type	0-1	0-1	0-1	0	0	0
66	Tunnel-Client-Endpoint	0-1	0-1	0-1	0	0	0
67	Tunnel-Server-Endpoint	0-1	0-1	0-1	0	0	0
68	Acct-Tunnel-Connection	0-1	0-1	0-1	0	0	0
69	Tunnel-Password	0	0	0	0	0	0
79	EAP-Message	0	0	0	0	0	0
80	Message-Authenticator	0	0	0	0	0	0
81	Tunnel-Private-Group-ID	0-1	0-1	0-1	0	0	0
82	Tunnel-Assignment-ID	0-1	0-1	0-1	0	0	0
83	Tunnel-Preference	0	0	0	0	0	0
85	Acct-Interim-Interval	0	0	0	0	0	0

表 4 (续)

属性编号	属性名	Acct-Start -Request	Acct-update -Request	Acct-stop -Request	Acct-On -Request	Acct-Off -Request	Acct- Response
86	Acct-Tunnel-Packets-Lost	0-1	0-1	0-1	0	0	0
87	NAS-Port-ID	0-1	0-1	0-1	0	0	0
88	Framed-Pool	0	0	0	0	0	0
90	Tunnel-Client-Auth-ID	0-1	0-1	0-1	0	0	0
91	Tunnel-Server-Auth-ID	0-1	0-1	0-1	0	0	0
26-XXXX-1	Input-Peak-Rate	0	0	0	0	0	0
26-XXXX-2	Input-Average-Rate	0	0	0	0	0	0
26-XXXX-3	Input-Basic-Rate	0	0	0	0	0	0
26-XXXX-4	Output-Peak-Rate	0	0	0	0	0	0
26-XXXX-5	Output-Average-Rate	0	0	0	0	0	0
26-XXXX-6	Output-Basic-Rate	0	0	0	0	0	0
26-XXXX-15	Remanent-Volume	0	0	0	0	0	0-1
26-XXXX-22	Priority	0	0	0	0	0	0
26-XXXX-26	Connect-ID	0-1	0-1	0-1	0	0	0-1
26-XXXX-27	PortalURL	0	0	0	0	0	0
26-XXXX-28	Ftp-Directory	0	0	0	0	0	0
26-XXXX-29	Exec-Privilege	0	0	0	0	0	0
26-XXXX-59	NAS-Startup-Timestamp	0	0	0	0	0	0
26-XXXX-135	Client-Primary-DNS	0	0	0	0	0	0
26-XXXX-136	Client-Secondary-DNS	0	0	0	0	0	0
26-XXXX-137	DSLAM-Port-ID	0-1	0-1	0-1	0	0	0
26-XXXX-254	Version	0	0	0	0	0	0
26-XXXX-255	Product-ID	0	0	0	0	0	0

注：26号扩展属性中的XXXX为Vendor-ID，这里为各个厂商向IANA申请的自己的标志。

表格格式说明：

0：属性一定不会出现在报文中；

0+：0个或多个属性可能会出现在报文中；

0-1：0个或一个属性可能出现在报文中；

1：确定的一个属性一定会出现在报文中。

## 7 流程

### 7.1 普通接入用户认证计费流程（必选）

普通接入用户认证计费流程如图4所示。

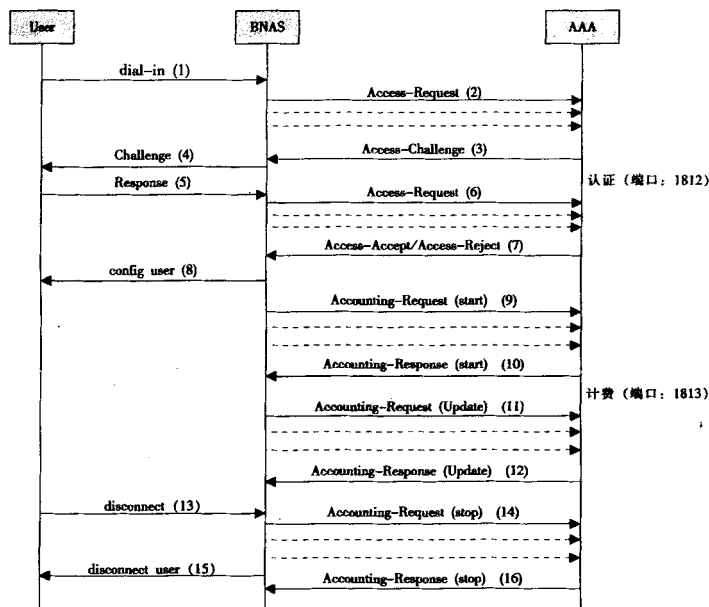


图4 普通接入用户认证计费消息流程

用户拨入后 (1)，所拨入的设备 BNAS 将拨入用户的信息 (如用户名、口令、所占用的端口等) 打包向 AAA 服务器发送 (2)。

如果 AAA 需要和用户协商认证方式 (如 SIM 卡用户)，则 AAA 向 BNAS 发送 (3)；BNAS 将 (3) 转发给客户端 (4)，客户端将协商后的信息发送给 BNAS (5)。然后 BNAS 将协商后的认证信息打包再转发到 AAA (6)。

如果该用户是一个合法的用户，那么 AAA 服务器告诉 BNAS 该用户可以上网，同时传回该用户的配置参数 Access-Accept (7)；否则，AAA 服务器反馈 BNAS 该用户的非法信息 Access-Reject (7)。

如果该用户合法，BNAS 就根据从 AAA 服务器传回的配置参数配置用户 (8)；如果用户非法，BNAS 反馈给用户出错信息并断开该用户连接，以后也不再发送计费报文。

如果用户可以访问网络，BNAS 要向 AAA 服务器发送一个计费请求包表明对该用户已经开始计费 (9)，AAA 服务器收到并成功记录该请求包后要给予响应 (10)。如果 BNAS 一段时间后没有收到计费响应，则需要重发一定次数的计费请求。

用户上网过程中，BNAS 定时向 AAA 发送计费请求 (11)，AAA 服务器收到并成功记录该请求包后要给予响应 (12)。如果 BNAS 一段时间后没有收到计费响应，则需要重发一定次数的计费请求。

当用户断开连接 (连接也可以由 BNAS 断开) (13)，或者用户可用业务量消费完时，BNAS 向 AAA 服务器发送一个计费停止请求包，其中包含用户上网所使用网络资源的统计信息 (如上网时长、进/出的字节/包数等) (14)，同时切断用户的连接 (15)。AAA 服务器收到并成功记录该请求包后要给予响应 (16)。发送计费停止请求后，其他计费请求可以不再重发。

## 7.2 管理用户认证流程 (可选)

### 7.2.1 设备管理用户

设备管理员在对设备进行维护时, 通常使用 Telnet、Rlogin、TCP 透传 (TCP Clear)、SSH、FTP、Terminal 等方式登录设备。为了网络的安全, 需要对协议进行了一定的扩展, 增加对设备管理用户的认证、授权功能。

### 7.2.2 认证请求

设备管理用户的认证报文中属性 Service-Type 的值为 6 (Administrative RFC 定义), 表示本用户为以上几种用户之一, 为设备管理用户。

如果要限制用户访问设备时的主机, 实现设备管理用户的 IP 地址绑定功能, 设备需同时上传属性 Login-IP-Host。

其他属性的上传同普通接入用户。

### 7.2.3 认证响应

如果设备管理用户通过了认证, 则 AAA 服务器下发属性 Login-Service, 值的定义见表 2。对于 EXEC 用户 (包括 Telnet、Rlogin、TCP 透传、SSH、Terminal 等) AAA 服务器还下发 Exec-Privilege (29-扩展属性), 对于 FTP 用户则下发属性 Ftp-Directory (28-扩展属性)。

### 7.2.4 其他

其他交互报文同普通接入用户, 并遵循本规范。

## 8 认证与计费的漫游

当业务接入点和业务登记点不在同一地点时, 就要使用漫游业务。针对漫游业务, RADIUS 报文分为两大类: (1) 认证类报文; (2) 计费类报文。

### 8.1 认证类报文处理

对于认证类报文采取立即转发方式 (即 Forward Mode), 如图 5 所示, 图 5 中的序号表示报文发送的时间顺序。

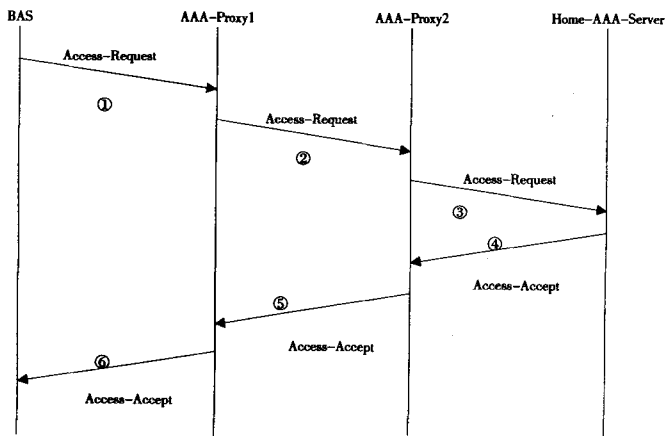


图 5 认证漫游示意

对图 5 中的流程说明如下:

(1) 各级 AAA-Proxy 在收到下级 AAA-Proxy (BNAS) 的请求报文时, 首先根据下级 AAA-Proxy (或 BNAS) 和自己之间的共享密钥对报文进行合法性检验, 若合法性检验失败, 则丢弃报文 (Silent Discard), 否则执行以下流程。

(2) 若报文中包含 User-Password 属性则各级 AAA-Proxy 应该解出密码明文, 用本 AAA-Proxy 和下级 AAA-Proxy (或 HOME-AAA-Server) 之间的共享密码对 User-Password 域进行加密, 对于其他属性内容应该保持不变。

(3) 若报文中包含 CHAP-Password 属性, 并且没有 CHAP-Challenge 属性时, 各级 AAA-Proxy 在转发报文时应该保证报文的 Authenticator 域保持不变。

(4) AAA-Proxy 可以在请求报文中增加 Proxy-State 属性, 如果原来的报文中存在 Proxy-State 属性则增加的 Proxy-State 属性必须放在所有的 Proxy-State 属性之后。下级 AAA-Proxy 必须原封不动的转发 Proxy-State 属性。HOME-AAA-Server 必须在对应的响应报文中将所有的 Proxy-State 属性返回, 并且顺序不变。AAA-Proxy 收到响应报文后, 如果之前在请求报文中加入了 Proxy-State 属性, 则必须将自己增加的 (最后一个) Proxy-State 属性从响应报文中拆离。

(5) 各级 AAA-Proxy 在没有收到上级的响应前不能向下级 AAA-Proxy (或 BNAS) 回 Access-Accept 报文, 但可以根据自己的策略响应 Access-Reject 报文, 如某 AAA-Proxy 定义, 在某时间段不处理漫游业务, 对这种情况 Proxy 应该立即给下级 AAA-Proxy (或 BNAS) 回送 Access-Reject 报文。

对于认证类报文的重发机制, 由 BNAS 来保证, BNAS 采用定时重发机制, 在规定时间内没有收到响应报文, 重新发送该报文, 发送达到最大重发次数后, 仍然没有收到响应报文, BNAS 认为认证失败。

## 8.2 计费类报文漫游处理

对于计费类报文也采取立即转发方式 (即 Forward Mode), 如图 6 所示, 图 6 中的序号表示报文发送的时间顺序。

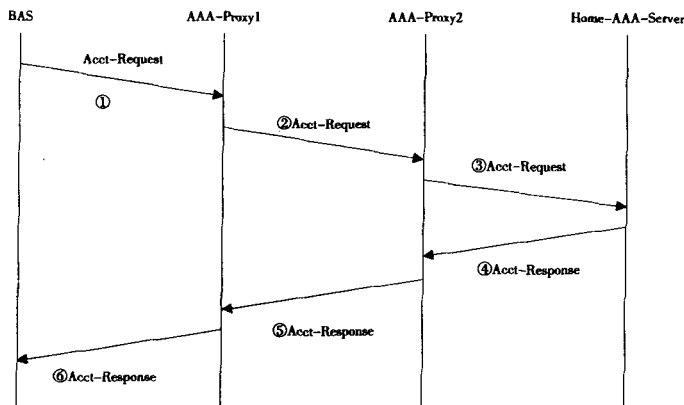


图 6 计费漫游示意图

对图 6 中的流程说明如下:

(1) 各级 AAA-Proxy 在收到下级 AAA-Proxy (或 BNAS) 的请求报文时, 首先根据下级 AAA-Proxy (或 BNAS) 和自己之间的共享密钥对报文进行合法性检验, 若合法性检验失败, 则丢弃报文 (Silent Discard), 否则执行以下流程。

(2) 根据自己和上级 AAA-Proxy (或 HOME-AAA-Server) 之间的共享密钥重新加密请求报文并转发。

(3) AAA-Proxy 可以根据需要在请求报文中增加 Proxy-State 属性, 如果原来的报文中存在 Proxy-State 属性则增加的 Proxy-State 属性必须放在所有的 Proxy-State 属性之后。下级 AAA-Proxy 必须原封不动的转发 Proxy-State 属性。HOME-AAA-Server 必须在对应的响应报文中将所有的 Proxy-State 属性返回, 并且顺序不变。AAA-Proxy 收到响应报文后, 如果之前在请求报文中加入了 Proxy-State 属性, 则必须将自己增加的 (最后一个) Proxy-State 属性从响应报文中拆离。

(4) 报文转发时应根据报文在本 AAA-Proxy 上的驻留时间, 修改报文中 Acct-Delay-Time 属性内容。

(5) 对于计费类报文的重发机制, 也由 BNAS 来保证, BNAS 采用定时重发机制, 在规定时间内没有收到响应报文, 重新发送该报文, 发送达到最大重发次数后, 仍然没有收到响应报文, BNAS 认为计费失败。

附录 A  
(规范性附录)  
VPDN 的业务流程

VPDN 用户接入消息序列如图 A.1 所示。

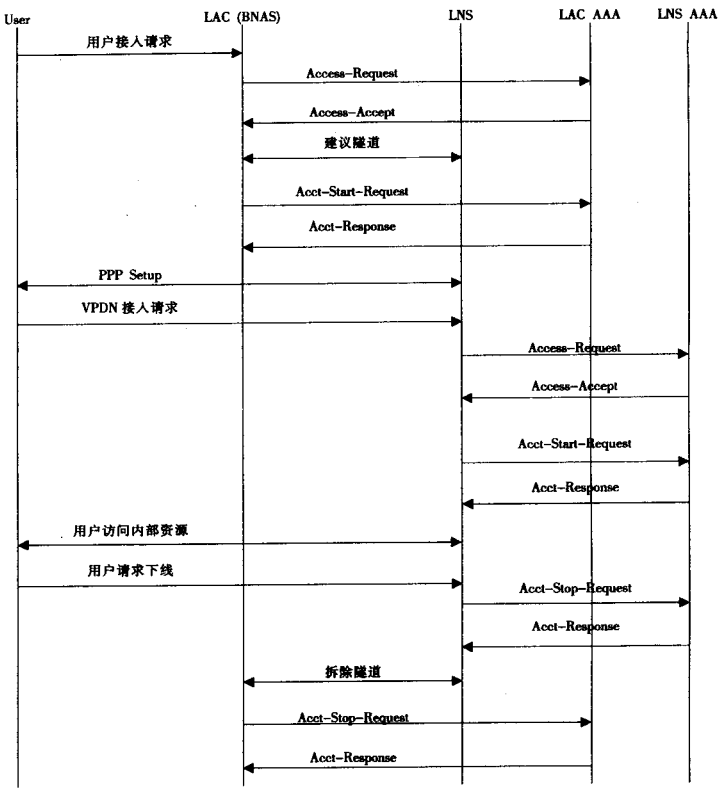


图 A.1 VPDN 用户接入消息序列