

中华人民共和国通信行业标准

YD/T 1340.1-2005

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

Technical requirements of Authentication Authorization Accounting (AAA)
server interface part1: Network Access Server (NAS)

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 报文局性定义 3

 6.3 PADIUS 报文内容 6

7 流程 12

附录 A（规范性附录） VPDN 的业务流程 13

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》

本部分是第一部分。

本部分是以互联网工程任务组（IETF）制定的 RFC 2138、RFC 2139 等标准为基础，结合我国网络实际情况制定的。

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：郑志鹏 杨 崑 方 新 唐小光

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

1 范围

本部分规定了为实现窄带网络接入服务器的认证和计费功能的 AAA 服务器接口的技术要求。
本部分适用于接入窄带网络接入服务器的 AAA 服务器设备。
为简便起见如无特殊说明，本部分中，网络接入服务器特指窄带网络接入服务器。

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。

YD/T 1045-2000	网络接入服务器 (NAS) 技术规范
RFC 2138 (1997)	RADIUS 协议
RFC 2139 (1997)	RADIUS 计费协议
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

网络接入服务器 Network Access Server

网络接入服务器 (Network Access Server, NAS) 是远程访问接入设备，它位于公用电话网/综合业务数字网/公用陆地移动网 (PSTN/ISDN/PLMN) 与 IP 网之间，将拨号用户接入 IP 网，它可以完成远程接入、实现拨号虚拟专网 (VPDN)、构建企业内部 Intranet 等网络应用。

3.2

AAA 服务器 Service/Application Server

提供授权 (Authorization)、认证 (Authentication) 和计费 (Accounting) 功能的服务器。一般采用 RADIUS 协议。

3.3

RADIUS Remote Authentication Dial in User Server

认证 (Authentication) 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

用户 (User) 的信息发送到指定的服务器, 然后根据服务器的不同响应进行处理。RADIUS 服务器通常运行在一台工作站上, 其任务是接收客户发来的请求, 认证用户的权限, 并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 Accounting	认证、授权和计费
NAS	Network Access Server	网络接入服务器

5 RADIUS 报文格式

(1) RADIUS 协议报文的格式定义如图 1 所示。

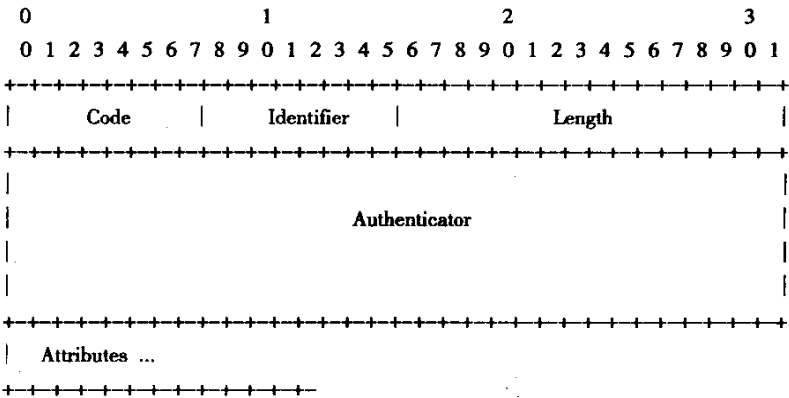


图 1 RADIUS 协议报文的格式定义

- 图 1 中:
- Code: 编号, 表示报文类型。
 - Identifier: 标识符, 用于匹配请求和响应。
 - Length: 长度, 包括 Code、Identifier、Length、Authenticator、Attributes 的长度。
 - Authenticator: 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。

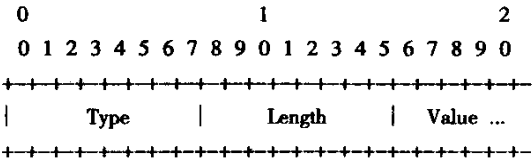


图 2 报文属性的格式定义

- 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。

6 报文和属性定义

NAS 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 号 (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 报文认证通过的回应报文
3	3	M	Access-Reject	对 Access-Request 报文认证失败的回应报文
4	4	M	Acct-Start-Request	计费开始报文
5	5	M	Acct-Start-Response	计费开始响应报文
6	4	M	Acct-Stop-Request	计费结束报文
7	5	M	Acct-Stop-Response	计费结束响应报文
8	4	O	Acct-On-Request	设备计费起始报文
9	5	O	Acct-On-Response	设备计费起始响应报文
10	4	O	Acct-Off-Request	设备计费终止报文
11	5	O	Acct-Off-Response	设备计费终止响应报文
12	4	O	Acct-Update-Request	中间计费实时报文
13	5	O	Acct-Update-Response	中间计费实时响应报文

注：

表 1 中“M”表示必选项，“O”表示可选项。

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-On-Response 是对应的响应报文。

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-Off-Response 是对应的响应报文。

Acct-Update-Request 在一个会话中间（Start 与 Stop 之间）发送，实时上报用户的用量信息，可以减少由于网络或者服务器异常时的计费损失。注意，在中间计费实时报文中的信息是累积的，即报文中的发送分组数量是从会话开始的总的分组数量，而不是从上一个中间计费实时报文以后的分组数量。Acc-Update-Response 是对应的响应报文。

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
2	User-Password	String	PAP 密码
3	CHAP-Password	String	CHAP 密码
4	NAS-IP-Address	Address	NAS IP 地址同 NAS-Identifier 两者必备其一

表 2 (续)

编号	名 称	类 型	描 述
5	NAS-Port	Integer	用户使用的 NAS 物理端口，非 TCP 或者 UDP 端口
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)
7	Framed-Protocol	Integer	帧协议： 1—点对点协议 (PPP)； 2—串行 IP 协议 (SLIP)
8	Framed-IP-Address	Address	用户的 IP 地址。 0xFFFFFFFF 表示用户可以自己定义 IP 地址。 0xFFFFFFFFE 表示 NAS 从本地地址池中为用户分配 IP 地址
11	Filter-ID	String	过滤器名称
12	Framed-MTU	Integer	最大传输单元 (Maximum Transmission Unit)
14	Login-IP-Host	Integer	Login 主机 IP 地址
15	Login-Service	Integer	Login 协议类型： 0—Telnet； 1—远程登录 (Rlogin)； 2—TCP 透传 (TCP Clear)
16	Login-TCP-Port	Integer	Login 使用的 TCP 端口
18	Reply-Message	String	回显信息
19	Callback-Number	String	回呼电话号码
20	Callback-ID	String	回呼的 ID
25	Class	String	在 Access-Accept 报文中由 RADIUS Server 返回，Client 在以后的所有计费报文中使用该属性，并且不能修改该属性内容
26	Vendor-Specific	String	厂商自定义属性
27	Session-Timeout	Integer	最大许可会话时间，以 s 为单位
28	Idle-Timeout	Integer	最大许可空闲时间，以 s 为单位
30	Called-Station-ID	String	接入号码
31	Calling-Station-ID	String	主叫号码
32	NAS-Identifier	String	NAS 标记，同 NAS-IP-Address 两者必备其一
33	Proxy-State	String	代理状态
40	Acct-Status-Type	String	计费报文类别： 1—计费开始 (Start)； 2—计费结束 (Stop)； 3—实时计费 (Interim-Update)； 7—设备计费启动 (Accounting-On)； 8—设备计费终止 (Accounting-Off)

表 2 (续)

编号	名 称	类 型	描 述
41	Acct-Delay-Time	Integer	报文实际发送延迟时间, 以 s 为单位
42	Acct-Input-Octets	Integer	接收字节数
43	Acct-Output-Octets	Integer	发送字节数
44	Acct-Session-ID	Integer	会话标示
45	Acct-Authentic	Integer	认证类型, 在计费报文中提供: 1—RADIUS; 2—本地 (Local); 3—远端 (Remote)
46	Acct-Session-Time	Integer	以 s 为单位
47	Acct-Input-Packets	Integer	接收数据包数
48	Acct-Output-Packets	Integer	发送数据包数
49	Acct-Terminate-Cause	Integer	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—NAS 错误 (NAS Error); 10—NAS 请求 (NAS Request); 11—NAS 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)
50	Acct-Multi-Session-ID	String	在多个相关的连接中使用相同的 Acct-Multi-Session-ID。用于 MP 捆绑中
51	Acct-Link-Count	Integer	通道的数目
60	CHAP-Challenge	String	CHAP 质询
61	NAS-Port-Type	Integer	NAS 用户端口类型: 0—异步 (Async); 1—同步 (Sync); 2—ISDN 同步 (ISDN Sync); 3—ISDN 异步 V.120 (ISDN Async V.120); 4—ISDN 异步 V.110 (ISDN Async V.110)
62	Port-Limit	Integer	最大端口数目

表 2 (续)

编号	名 称	类 型	描 述
64	Tunnel-Type	Integer	隧道协议： 1—点到点隧道协议 (PPTP)； 3—层 2 隧道协议 (L2TP)
65	Tunnel-Medium-Type	Integer	隧道媒体种类： 1—IPv4 (IP version 4)； 2—IPv6
66	Tunnel-Client-Endpoint	String	隧道客户端地址
67	Tunnel-Server-Endpoint	String	隧道服务器地址
68	Acct-Tunnel-Connection	String	隧道连接 ID
69	Tunnel-Password	String	隧道密钥 (密文)

6.3 RADIUS 报文内容

表 3~表 17 中，“M”表示必选项，“O”表示可选项。

6.3.1 Acct-On-Request 报文

Acct-On-Request 报文内容见表 3。

表 3 Acct-On-Request 报文内容

编 号	M/O	值	描 述
4	O	NAS-IP-Address	NAS IP 地址，同 NAS-Identifier 两者必备其一
32	O	NAS-Identifier	NAS 标记，同 NAS-IP-Address 两者必备其一
33	O	Proxy-State	代理状态
40	M	Acct-Status-Type	计费状态 (7-Accounting-On)
44	O	Acct-Session-ID	会话标示

6.3.2 Acct-On-Response

Acct-On-Response 报文内容见表 4。

表 4 Acct-On-Response 报文内容

编 号	M/O	值	描 述
33	O	Proxy-State	代理状态

6.3.3 Acct-Off-Request 报文

Acct-Off-Request 报文内容见表 5。

表 5 Acct-Off-Request 报文内容

编 号	M/O	值	描 述
4	O	NAS-IP-Address	NAS IP 地址，同 NAS-Identifier 两者必备其一
32	O	NAS-Identifier	NAS 标记，同 NAS-IP-Address 两者必备其一

表 5 (续)

编号	M/O	值	描述
33	O	Proxy-State	代理状态
40	M	Acct-Status-Type	计费状态 (8-Accounting-Off)
44	O	Acct-Session-ID	会话标示

6.3.4 Acct-Off-Response

Acct-Off-Response 报文内容见表 6。

表 6 Acct-Off-Response 报文内容

编 号	M/O	值	描 述
33	O	Proxy-State	代理状态

6.3.5 Access-Request

Access-Request 报文内容见表 7。

表 7 Access-Request 报文内容

编 号	M/O	值	说 明
1	M	User-Name	用户名
2	O	User-Password	PAP 密码, 采用 MD5 加密
3	O	CHAP-Password	CHAP 密码
4	O	NAS-IP-Address	NAS IP 地址, 同 NAS-Identifier 两者必备其一
5	M	NAS-Port	用户使用的 NAS 物理端口
6	O	Service-Type	此时返回用户的真正类型。 1—login; 2—Framed
30	M	Called-Station-ID	接入号码
31	M	Calling-Station-ID	主叫号码
32	O	NAS-Identifier	NAS 标记, 同 NAS-IP-Address 两者必备其一
33	O	Proxy-State	代理状态
60	O	CHAP-Challenge	质询, 在 CHAP-Password 存在的条件下存在
61	M	NAS-Port-Type	NAS 用户端口类型

6.3.6 Access-Accept

Access-Accept 报文内容见表 8。

表 8 Access-Accept 报文内容

编 号	M/O	值	描 述
1	O	User-Name	用户名
6	O	Service-Type	此时返回用户的真正类型。 1—login; 2—Framed
11	O	Filter-ID	过滤器
12	O	Framed-MTU	最大传输单元
18	O	Reply-Message	回显信息
25	O	Class	在 Access-Accept 报文中由 RADIUS Server 返回, Client 在以后的所有计费报文中使用该属性, 并且不能修改该属性内容
27	O	Session-Timeout	最大许可上网时间
28	O	Idle-Timeout	许可空闲时间
33	O	Proxy-State	代理状态
62	O	Port-Limit	最大端口数目

在服务类型 Service-Type (属性 6) 为 Framed 时存在以下属性, 见表 9。

表 9 Service-Type 为 Framed 时的属性

编 号	M/O	值	描 述
7	O	Framed-Protocol	帧协议
8	O	Framed-IP-Address	IP 地址
64	O	Tunnel-Type	L2TP 或 PPTP (VPDN 应用)
65	O	Tunnel-Medium-Type	目前只支持 IP 类型, 其他类型认为认证拒绝 (VPDN 应用)
67	O	Tunnel-Server-Endpoint	(VPDN 应用)
69	O	Tunnel-Password	(VPDN 应用)
19	O	Callback-Number	回呼号码 (回呼应用)
20	O	Callback-ID	(回呼应用)

在服务类型 Service-Type (属性 6) 为 login 时必须存在以下属性, 见表 10。

表 10 Service-Type 为 login 时的属性

编 号	M/O	值	描 述
14	M	Login-IP-Host	Login Server 的 IP 地址
15	M	Login-Service	0—Telnet; 1—Rlogin; 2—TCPClear
16	M	Login-TCP-Port	Login 端口

6.3.7 Access-Reject

Access-Reject 报文内容见表 11。

表 11 Access-Reject 报文内容

编 号	M/O	值	描 述
1	O	User-Name	用户名
18	O	Reply-Message	回显消息
33	O	Proxy-State	代理状态

6.3.8 Acct-Start-Request

Acct-Start-Request 报文内容见表 12。

表 12 Acct-Start-Request 报文内容

编 号	M/O	值	描 述
1	M	User-Name	用户名
4	O	NAS-IP-Address	NAS IP 地址，同 NAS-Identifier 两者必备其一
5	O	NAS-Port	NAS 端口
6	M	Service-Type	服务类型
7	O	Framed-Protocol	在 Service-Type=Framed 时存在
8	O	Framed-IP-Address	在 Service-Type=Framed 时存在
25	O	Class	类
30	M	Called-Station-ID	接入号码
31	M	Calling-Station-ID	主叫号码
32	O	NAS-Identifier	NAS 标记，同 NAS-IP-Address 两者必备其一
33	O	Proxy-State	代理状态
40	M	Acct-Status-Type	计费状态（1-计费开始）
41	O	Acct-Delay-Time	发送该报文的时延
44	M	Acct-Session-ID	会话标示
45	O	Acct-Authentic	授权属性
50	O	Acct-Multi-Session-ID	MP 标记（MP 应用）
51	O	Acct-Link-Count	通道的数目（MP 应用）
61	O	NAS-Port-Type	NAS 用户端口类型
64	O	Tunnel-Type	（VPN 应用）

6.3.9 Acct-Start-Response

Acct-Start-Response 报文内容见表 13。

表 13 Acct-Start-Response 报文内容

编 号	M/O	值	描 述
1	O	User-Name	用户名
33	O	Proxy-State	代理状态

6.3.10 Acct-Stop-Request

Acct-Stop-Request 报文内容见表 14。

表 14 Acct-Stop-Request 报文内容

编 号	M/O	值	描 述
1	M	User-Name	用户名
4	O	NAS-IP-Address	NAS IP 地址, 同 NAS-Identifier 两者必备其一
32	O	NAS-Identifier	NAS 标记, 同 NAS-IP-Address 两者必备其一
5	O	NAS-Port	NAS 端口
6	M	Service-Type	服务类型
7	O	Framed-Protocol	在 Service-Type=Framed 时存在
8	O	Framed-IP-Address	在 Service-Type=Framed 时存在
25	O	Class	类
30	M	Called-Station-ID	接入号码
31	M	Calling-Station-ID	主叫号码
33	O	Proxy-State	代理状态
40	M	Acct-Status-Type	计费状态 (2-计费结束)
41	O	Acct-Delay-Time	发送该报文的时延
42	M	Acct-Input-Octets	接收字节数
43	M	Acct-Output-Octets	发送字节数
46	M	Acct-Session-Time	会话时长
47	M	Acct-Input-Packets	接收数据包数
48	M	Acct-Output-Packets	发送数据包数
49	M	Acct-Terminate-Cause	结束原因
44	M	Acct-Session-ID	会话标识
45	O	Acct-Authentic	授权属性
50	O	Acct-Multi-Session-ID	MP information
61	O	NAS-Port-Type	NAS 用户端口类型
64	O	Tunnel-Type	VPN 用户存在

6.3.11 Acct-Stop-Response

Acct-Stop-Response 报文内容见表 15。

表 15 Acct-Stop-Response 报文内容

编 号	M/O	值	描 述
1	O	User-Name	用户名
33	O	Proxy-State	代理状态

6.3.12 Acct-Update-Request

Acct-Update-Request 报文内容见表 16。

表 16 Acct-Update-Request 报文内容

编 号	M/O	值	描 述
1	M	User-Name	用户名
4	O	NAS-IP-Address	NAS IP 地址, 同 NAS-Identifier 两者必备其一
32	O	NAS-Identifier	NAS 标记, 同 NAS-IP-Address 两者必备其一
5	O	NAS-Port	NAS 端口
6	M	Service-Type	服务类型
7	O	Framed-Protocol	在 Service-Type=Framed 时存在
8	O	Framed-IP-Address	在 Service-Type=Framed 时存在
25	O	Class	类
30	M	Called-Station-ID	接入号码
31	M	Calling-Station-ID	主叫号码
33	O	Proxy-State	代理状态
40	M	Acct-Status-Type	计费状态 (3-实时计费)
41	O	Acct-Delay-Time	发送该报文的时延
42	M	Acct-Input-Octets	接收字节数
43	M	Acct-Output-Octets	发送字节数
46	M	Acct-Session-Time	会话时长
47	M	Acct-Input-Packets	接收数据包数
48	M	Acct-Output-Packets	发送数据包数
44	M	Acct-Session-ID	会话标识
45	O	Acct-Authentic	授权属性
50	O	Acct-Multi-Session-ID	MP Information
61	O	NAS-Port-Type	NAS 用户端口类型
64	O	Tunnel-Type	VPN 用户存在

6.3.13 Acct-Update-Response

Acct-Update-Response 报文内容见表 17。

表 17 Acct-Update-Response 报文内容

编 号	M/O	值	描 述
1	O	User-Name	用户名
33	O	Proxy-State	代理状态

7 流程

NAS 的 AAA 认证计费消息流程如图 1 所示。

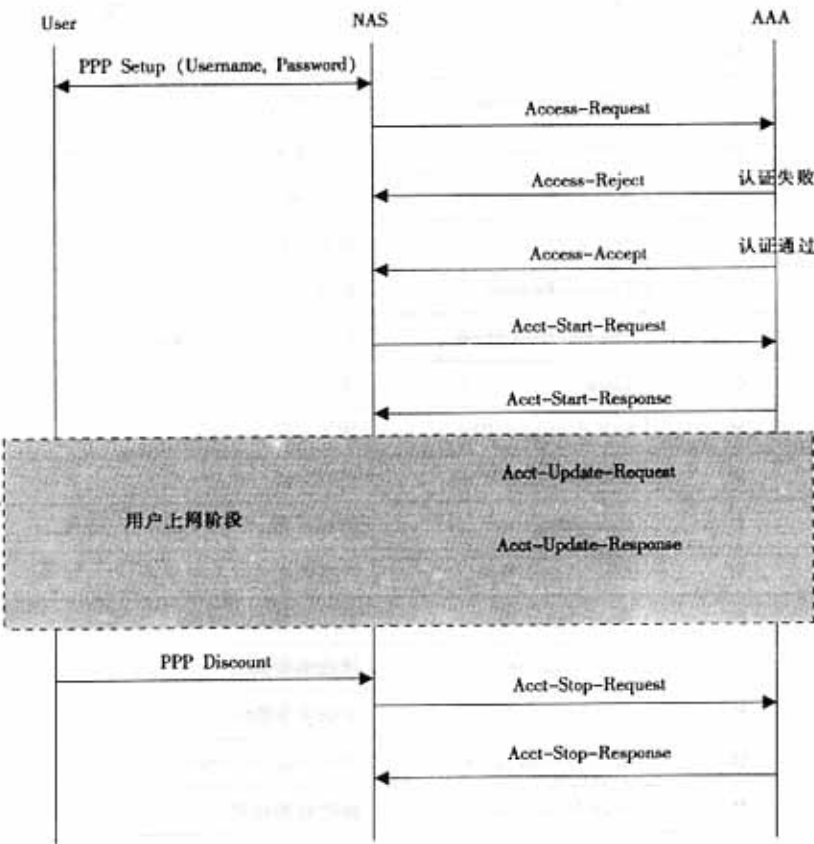


图 1 NAS 的 AAA 认证计费消息流程

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。

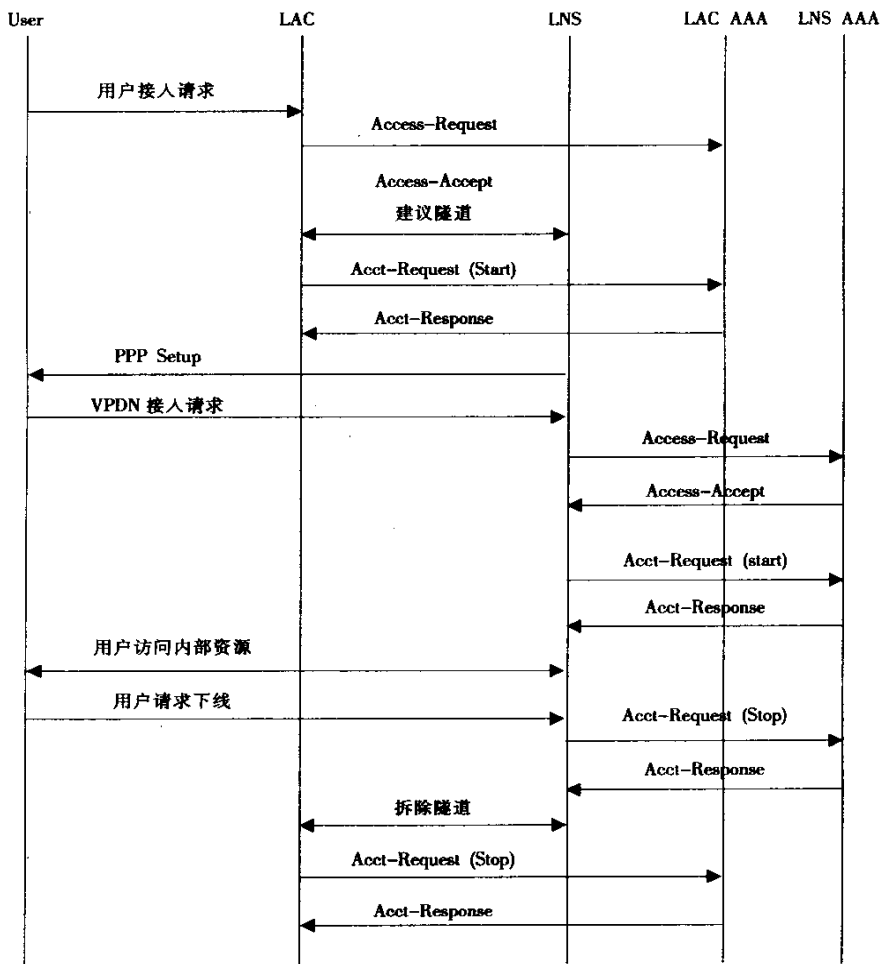


图 A.1 VPDN 用户接入消息序列