ICS 33 040 40
L 78

YD

中华人民共和国通信行业标准

YD/T 1615-2007

公众IP网络安全要求 ——基于远端接入用户验证服务协议（RADIUS）的访问控制

Security Requirements for Public IP Based Network

——RADIUS Protocol for Access Control

2007-04-16 发布　　2007-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“公众IP网络安全”系列标准之一。该系列标准预计的结构及名称如下：

1. 公众IP网络安全要求——安全框架；
2. 公众IP网络安全要求——基于数字证书的访问控制；
3. 公众IP网络安全要求——基于远端接入用户验证服务协议（RADIUS）的访问控制；
4. 公众IP网络安全要求——基于Diameter的访问控制。

本标准在制定过程中参考了IETF RFC 2865、RFC2866、RFC2689、RFC3162等。

本标准由中国标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院

中国电信集团公司

本标准主要起草人：刘　述　唐永丽　彭　俊　魏　亮　毕立波　武　静　陈　通　张　雄

公众 IP 网络安全要求
——基于远端接入用户验证服务协议（RADIUS）的访问控制

1 范围

本标准规定了基于 RADIUS 协议的访问控制要求，包括 RADIUS 服务器的结构、作用及在网络中的位置，RADIUS 认证与计费消息的格式与属性，以及 RADIUS 认证计费过程、RADIUS 的安全机制。

本标准适用于公众 IP 网络的接入系统。

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 1466-2006　　IP 安全协议（IPSec）技术要求

YD/T 1614-2007　　公众 IP 网络安全要求——基于数字证书的访问控制

3 定义和缩略语

3.1 定义

下列定义适用于本标准。

- 计费

收集资源使用信息的动作，以用于能力规划、审核、营业额或成本分配。

- 计费记录

一条计费记录表述了一个用户在整个会话过程中资源消费的总结。计费服务器可以通过处理中间计费事件或从若干为同一用户服务的设备上收集的计费事件来完成计费记录的创建。

- 认证

核实某个实体（客体）身份的动作。

- 授权

决定一个提出请求的实体（客体）是否被允许访问资源（主体）的动作。

- 代理

除了转发请求和响应，代理还制定与资源使用和配置相关的策略决定。该工作通常通过跟踪接入服务器设备的状态来完成。代理在收到服务器响应之前一般不会响应客户请求。当策略被违反时，它可以生成拒绝（Reject）消息。因此，代理必须理解通过它们的消息的语义，而且不一定支持所有的应用。

- 中间计费

中间计费消息提供一个用户会话过程中资源使用的快照。如果因设备重启动或者其他网络故障，使得会话总结消息或会话记录无法被接收的情况下，它通常用于用户会话的分段记账。

- 多会话（Multi-session）

一个多会话表现为若干会话的一个逻辑链接。多会话通过使用Acct-Multi-Session-Id来辨识。多会话的一个举例可以是一个多链路PPP束。该PPP束的每一个分支都是一个会话，而整个PPP束则是一个多会话。

- 网络接入标识符

网络接入标识符或NAI，在Diameter协议中用来摘录某个用户的身份和域（realm）的信息。身份用来在认证和/或授权过程中标识该用户，而域（realm）则用于消息的路由。

- 域

NAI中紧跟在“@”字符后面的字符串。NAI域名必须是惟一的，并且遵从DNS命名空间的管理。在RADIUS中，域名不必遵从DNS命名方式，可以独立。

- 会话状态

通过跟踪所有经过授权的活动会话，状态代理保留会话状态信息。每个经过授权的会话都与某特殊的业务绑定，其状态为活动，一直到被通知改变为其他状态或到期。

- 子会话

子会话表示一个提供给已有会话的独特的业务（例如Qos或数据特性）。这些业务可以同时（例如在同一会话过程中同时传送语音和数据）或连续发生。会话中的这些改变通过Accounting-Sub-Session-Id来表征。

- RADIUS服务器

RADIUS服务器指支持RADIUS协议，对用户进行计费与认证的服务器，通常由运营商提供与维护。

- RADIUS客户端

RADIUS客户端指支持RADIUS协议，对于用户进行接入，并把用户的认证信息转发至RADIUS服务器，对用户身份进行认证的设备。

3.2 缩略语

下列缩略语适用于本标准。

AAA	Authentication，Authorization and Accounting	认证授权和计费
ADSL	Asymmetrical Digital Subscriber Loop	非对称式数据用户线
AVP	Attribute Value Pairs	属性值对
CHAP	Challenge Handshack Authentication Protocol	握手认证协议
CMS	Cryptographic Message Syntax	密码消息语法
EAP	Extensible Authentication Protocol	可扩展认证协议
EAPOL	EAP over LAN，	局域网上传送EAP协议
HDLC	High-Level Data Link Control	高层数据链路控制
HTTP	Hyper Text Transmission Protocol	超文本传输协议
IP	Internet Protocol	互联网协议
LAN	Local Area Network	局域网
LAT	Local Area Transport	局域传送协议
LCP	Link Control Protocol	链路控制协议

MTU	Maximum Transmission Unit	最大传输单元
NAI	Network Access Identifier	网络接入标识
NAS	Network Access Server	网络接入服务器
OTP	One Time Password	一次性密码
PAP	Password Authentication Protocol	密码认证协议
PPP	Point to Point Protocol	点对点协议
RADIUS	Remote Authentication Dial-In User Service	远端拨入用户验证服务
RAS	Registration，Admissin and Status	注册允许和状态协议
SCTP	Stream Control Transmission Protocol	流控制传输协议
SLIP	Serial Line IP	串行IP
SMI	Structure of Management Information	管理信息结构
SNMP	Simple Network Management Protocol	简单网管协议
TACACS	Terminal Access Controller Access Control System	终端接入控制者接入控制系统协议
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
UDP	User Datagram Protocol	用户数据报协议

4 RADIUS 服务器结构作用及在网络中的位置

4.1 RADIUS 服务器的结构

RADIUS 服务器应可以对用户进行认证、处理与用户及应用相关的授权并收集计费信息。RADIUS 服务器应与一特定的应用模块有接口，这个应用模块用于管理授权过程所需的资源。RADIUS 系统的组成部分可能会分布在不同的管理域中。

4.1.1 RADIUS 服务器体系中的组成部分

授权规则的评估：授权过程的第一个步骤是为用户或代表用户利益的实体产生一个请求并发向 RADIUS 服务器。RADIUS 服务器有一套规则来检验这些请求，并做出相应的授权决定。RADIUS 服务器应有一套基于规则的引擎，它可以理解请求中的一般信息，不过它不会知道任何具体的应用信息，除非这些信息是可以用布尔值或数值来表述的。

应用专用模块：RADIUS 服务器最终会与应用专用模块进行交互。对于业务提供者，业务专用模块用于管理资源并配置服务设备来提供授权服务。它可能也参与授权的决策，因为它具有针对业务的信息。业务专用模块是 RADIUS 服务器一个分离的体系组成部分，它必须是可被寻址的，因此应在全球命名空间中。

授权事件记录：为了审计，RADIUS 服务器必须具有某种形式的数据库，用来存储有时间戳的事件。这个数据库可以说明曾颁发的授权。

策略库：这是一个包含可用的服务与资源数据库，授权的决策就对根据这些进行的，另外进行决策所需的各种策略也应在此数据库中。在此，对于服务与资源的命名空间也非常重要，它们必须是从别的 RADIUS 服务器上可以寻址的。

请求前转：RADIUS 可分布多个管理域的本质，使 RADIUS 服务器间必须有一种机制，使消息可以

进行前转。两 RADIUS 服务器间的通信协议应为端到端的。

4.1.2 RADIUS 服务器的模型

RADIUS 服务器应可以处理 AAA 请求，对其中的内容进行检查，判断应授予什么样的权限，从库中检索策略规则，运行各种本地的功能，并从下列可选项中择其一进行进一步地处理 AAA 请求的每一个成份：

（1）让连接的应用专用模块对某一成分进行评估；

（2）在授权事件记录或策略库中查找回应的结果；

（3）把成份前转到其他 AAA 服务器上进行评估。

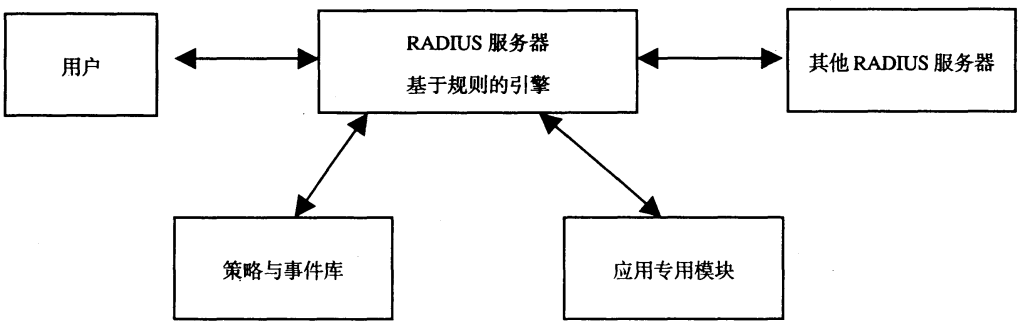


图 1 RADIUS 服务器与其相关部分的关系

图 1 显示了连接各个体系组成部分的 RADIUS 服务器，在这个模型里，用户与其他 AAA 服务与 RADIUS 服务器发送请求以获得授权，请求消息采用 RADIUS 协议。RADIUS 服务器与应用专用模块及策略库、事件记录库相连接，它们之间的协议不在本标准的范围内。

4.2 RADIUS 服务器的作用

基于RADIUS的AAA服务器，目前广泛用于通常用于AAA服务器应能够对网络接入客户进行认证、处理与用户及应用相关的授权并收集计费信息。一个AAA服务器通常会为一个或多个网络接入设备提供AAA服务。

- 认证（Authentication）

认证过程是执行AAA任务的第一步，用来判别正在接入的用户的身份；基于RADIUS协议的AAA服务器能够支持多种认证机制，例如PAP和CHAP。

- 授权（Authorization）

授权过程用来授予已经通过认证的用户可以拥有的网络及业务使用权限（例如，分配一个IP地址给用户）。

- 计费（Accounting）

计费过程对于商用IP网络是非常重要的，它可以实现对允许接入业务的用户记录各种与业务使用费用相关的信息，包括业务使用起止时间、数据流量、该用户使用的网络资源等。

除了以上三个基本功能外，基于RADIUS的AAA服务器还应具有以下功能：

—— 支持采用加密等技术手段保证客户端与服务器之间的通信安全，基于 RADIUS 协议的情况下，仅需要保证逐跳（hop-by-hop）安全。

—— 支持简单网管协议（SNMP），可选。

4.3 RADIUS 服务器在网络中的位置

RADIUS服务器从所处的网络位置以及承担的功能从逻辑上可以分为代理服务器和普通服务器。AAA系统的组成部分可能会分布在不同的管理域中。通常情况下，基于RADIUS的AAA客户端一般会安装在用户接入设备上，通过网络与基于RADIUS的AAA服务器通信。同时，基于RADIUS的AAA服务器还可以作为另一个基于RADIUS的AAA服务器或其他认证服务器的代理客户端，这时该AAA服务器被称作代理AAA服务器。

4.3.1 本地域用户完成 AAA 过程的网络配置

图2给出了使用基于RADIUS协议的AAA服务器进行用户接入认证和授权的一个典型配置。此时申请接入服务的用户属于本地域，因此可以直接通过本地所属的AAA服务器完成AAA过程。

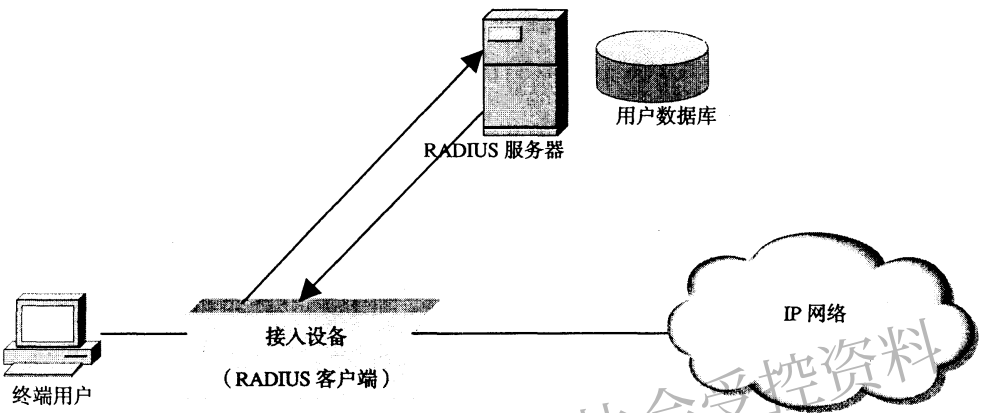


图 2 本地域用户完成 AAA 过程的网络配置

终端用户接入一个支持RADIUS客户端服务的接入设备。接入设备从终端用户得到所需的接入认证用户信息(用户名／密码、主叫号码等)。接入设备随后使用UDP/IP转发加密过的接入请求给基于RADIUS的AAA服务器。消息中可能还包含类似接入设备端口号ID以及IP地址一类的属性。

基于RADIUS的AAA服务器随后检查用户认证信息的属性是否与自己数据库中存储的信息匹配。如果不匹配，服务器则返回拒绝接入的消息给接入设备，该消息中可以可选携带指明失败原因的文本信息。接入设备则会通知终端用户认证失败。如果匹配，服务器则返回允许接入的消息给接入设备，该消息中将附带完成连接所需要的任何附加配置信息，例如一个分配给终端用户的IP地址或者一个限制特定协议类型的过滤器，如Telnet或HTTP。

4.3.2 漫游到外地的用户完成 AAA 过程的网络配置

在IP商用网络中，RADIUS系统通常会根据网络本身的结构以及运营商的运营策略进行配置，可能存在多种不同的情况，例如，全网采用统一的RADIUS服务器进行用户访问控制；或者网内各域拥有自己的RADIUS服务器负责本域内的用户认证计费。如果IP商用网络采用了RADIUS服务器分布式设置的方式，并且执行用户归属地认证的运营策略，则需要服务器支持代理的功能。

图3 给出了漫游用户通过RADIUS系统进行归属地认证的网络配置。这时，漫游地的RADIUS服务器承担代理服务器的角色。漫游用户接入当地支持客户端服务的接入设备。接入设备从终端用户得到所需的接入认证用户信息（用户名／密码、主叫号码等），随后使用UDP/IP转发加密过的接入请求给漫游地RADIUS服务器。消息中可能还包含类似接入设备端口号ID以及IP地址一类的属性。

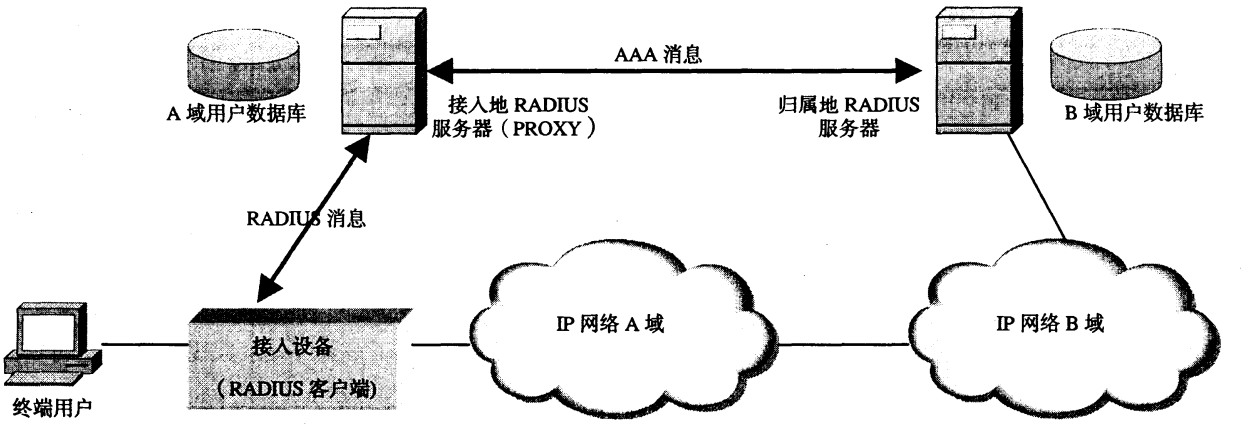


图 3　漫游用户完成 AAA 过程的网络配置

漫游地的RADIUS服务器根据用户的接入信息应能够判断该用户是否为漫游用户，如果是，则本地RADIUS服务器向该用户归属地的RADIUS服务器发送接入请求。归属地RADIUS服务器接收到该请求后，检查用户认证信息的属性是否与自己数据库中存储的信息匹配。如果不匹配，服务器则返回拒绝接入的消息给漫游地RADIUS服务器，该消息中可以携带可选的指明失败原因的文本信息。如果匹配，服务器则返回允许接入的消息给接入设备，该消息中将附带完成连接所需要的任何附加配置信息，例如一个分配给终端用户的IP地址或者一个限制特定协议类型的过滤器，如Telnet或HTTP。归属地RADIUS服务器接收到认证请求的响应（成功／失败），均会向接入设备发送相应的应答，接入设备应根据应答，通知终端用户是否可以接入。

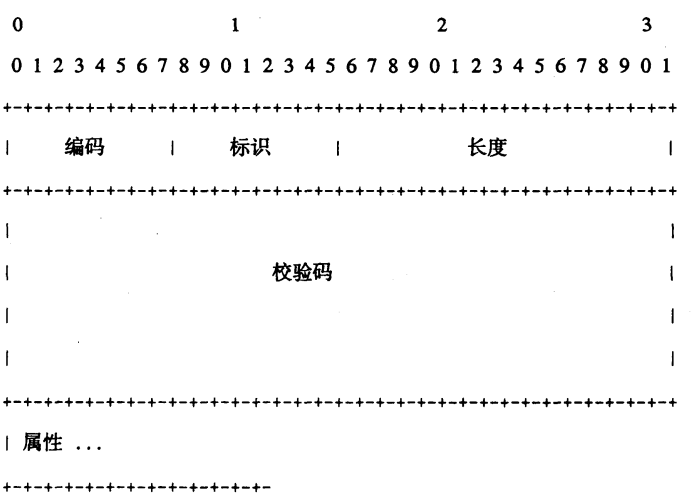
5　消息的格式与属性

5.1　认证消息的格式与属性

5.1.1　认证消息的格式

将RADIUS数据包封装到UDP数据字段，此时UDP目的端口字段应该是1812（十进制）。生成应答消息的时候，调换源和目的端口。

RADIUS数据格式如下图所示。这些字段按照从左到右的顺序传输。



编码（code）字段：编码字段是一个字节，说明了RADIUS数据包的类型。如果接收到的数据包的编码字段无效，就直接丢弃。

RADIUS编码（十进制）的分配如下所示：

1 Access-Request
2 Access-Accept
3 Access-Reject
4 Accounting-Request
5 Accounting-Response
11 Access-Challenge（接入口令）
12 Status-Server （试验性）
13 Status-Client （试验性）
255 保留的

编码12和13留作未来可能的使用情况，在本标准没有过多讨论。

标识符（Identifier）字段：标识符字段是一个字节，用于匹配申请和应答。RADIUS服务器可以检测到较短时间内具有相同的客户源IP地址、源UDP端口以及标识符的重复申请。

长度字段：长度字段是2个字节。它说明了包括编码、标识符、长度、校验码以及属性字段在内的数据包长度。接收端必须把超出了长度字段范围的字节看作是填充字节并忽略它们。如果数据包比长度字段声明的长度短，则丢弃该数据包。数据包的最短长度是20字节，最长是4096字节。

校验码（Authenticator）字段

校验码字段：校验码字段是16字节。首先发送最高有效位。这个值用来验证来自RADIUS服务器的应答，它用在口令的隐藏算法中。

请求消息的校验字段：在接入请求消息中，校验字段值是请求校验的16字节的随机数字。在口令（在客户和RADIUS服务器之间共享的口令）存在的时间内这个值应该不可预知而且惟一的，因为一个重复的申请值和同样的口令会让入侵者用在前面截取的应答消息来应答。因为希望通过相同的口令来验证在不同地域的服务器，因此请消息校验字段应该具有全局以及暂时惟一值。

Access-Request消息包的请求消息校验值应该是不可预测的，以免攻击者欺骗服务器来应答一个预知的未来的请求，然后用这个应答伪装成未来接入请求的服务器。

虽然RADIUS等协议不能通过实时的方式来保护经过认证的会话不受窃听的攻击，但是生成一个惟一的不可预测的请求可以防止大量的攻击通过认证。

接入服务器和RADIUS服务器共享一个密钥。这个密钥后跟着请求消息校验字段，经过一个单向的MD5计算中形成一个数字摘要，然后这个值和用户输入的口令进行异或操作，异或的结果放置到Access-Request消息包的用户口令属性字段中。详细的描述请参见属性一节中有关用户口令的部分。

应答消息的校验字段：将接入请求、接入拒绝和Access-Challenge数据包中的Authenticator字段值称作应答Authenticator，该值包括一个通过一组字节计算出来单向MD5杂散，这些字节包括RADIUS数据包，这个数据包以编码字节开始，包括标识符、长度，以及来自接入请求的请求校验字段，然后就是应答属性，以及共享的口令。也就是说，ResponseAuth=MD5（Code+ID+Length +RequestAuth+Attributes+Secret），此处+号标识连接在一起。

如果采用转发代理，在数据包通过的时候，代理必须能够改变数据包——当代理转发请求的时候，代理可以在请求上加入一个代理状态属性，如果它在请求上加入了代理状态属性，在它转发应答的时候，它必须去掉这个属性。代理状态通常加入/去掉在其他任何代理状态的后面，但是并没有规定它们在属性

列表中的位置。因为是在整个数据包内容的基础上对接入接受以及接入拒绝进行验证，去掉代理状态属性会导致数据包中的签名无效，因此代理必须重新签署该属性。

5.1.2 认证消息类型

RADIUS数据包类型由数据包的第一个字节中的编码字段来决定。

5.1.2.1 Accept-Request

Access-Request消息包发送给RADIUS服务器，它用来携带决定一个用户是否可以接入一个特定的接入服务器的信息以及来自用户的任何特别的业务请求。

在从一个有效的客户接收到接入请求的时候，必须发送一个适当的应答消息。

接入请求应该包含用户名字属性。它必须包含接入服务器IP地址属性或者接入服务器标识符属性(或者两者都包括)。

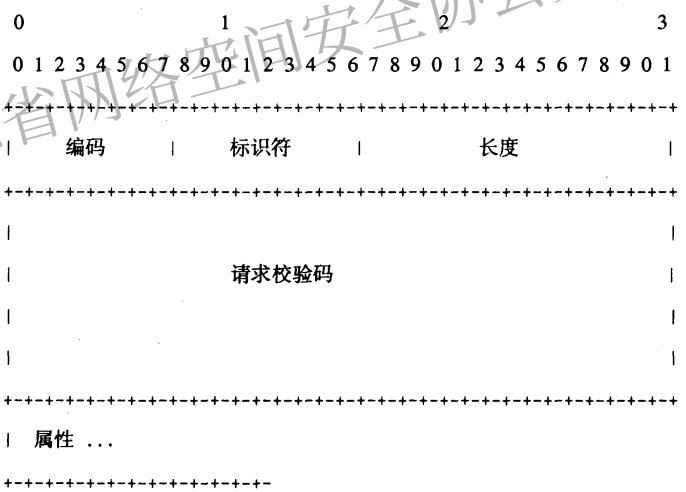
接入请求必须包含用户口令或者CHAP口令或者状态(STATE)。接入请求不能同时包含用户口令和CHAP口令。如果将来的扩展版本允许传送其他形式的认证信息，在接入请求中可以包含用于这些认证信息的属性而无需包含用户口令或者CHAP口令。

接入请求应该包含接入服务器端口或者接入服务器端口类型属性或者两者都包括，除非请求的接入类型不包括端口或者接入服务器不区分端口信息。

接入请求还可以包含附加的属性，作为给服务器的一个指示，但是不要求服务器接受这个指示。

当出现用户口令的时候，口令采用一种基于RSA消息摘要算法MD5的算法来隐藏它。

接入请求格式的如下图所示。这些字段按照从左到右的方向传输。



编码：接入请求的编码值为1。

标识符：当属性字段的内容发生变化而且接收到了一个对前一个请求的有效应答的时候，必须改变标识符字段。为了重传的需要，标识符必须保持不变。

请求校验码：当采用新的标识符的时候，必须改变请求校验值。

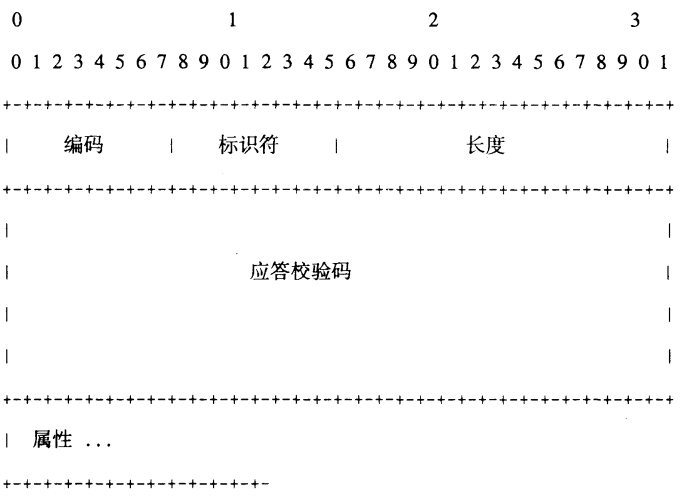
属性：属性字段长度是可变的，包含了业务类型需要的属性列表，以及任何需要的可选的属性。

5.1.2.2 Access-Accept

RADIUS服务器发送Access-Accept消息，这些数据包提供了为用户传送业务所需要的特定的配置信息。如果接入请求中所有的属性值都是可接受的，那么RADIUS必须传送编码值为2的数据包(接入接受)。

一旦接收到了access-accept，标识符字段与待处理的接入请求匹配。应答校验值字段必须包含对待处理的接入请求的正确应答。丢弃无效的数据包。

Access-Accept消息格式如下图所示。这些字段按照从左到右的顺序传送。



编码：Access-Accept 的编码值是2。

标识符：标识符字段复制了引起Access-Accept的接入请求的标识符字段。

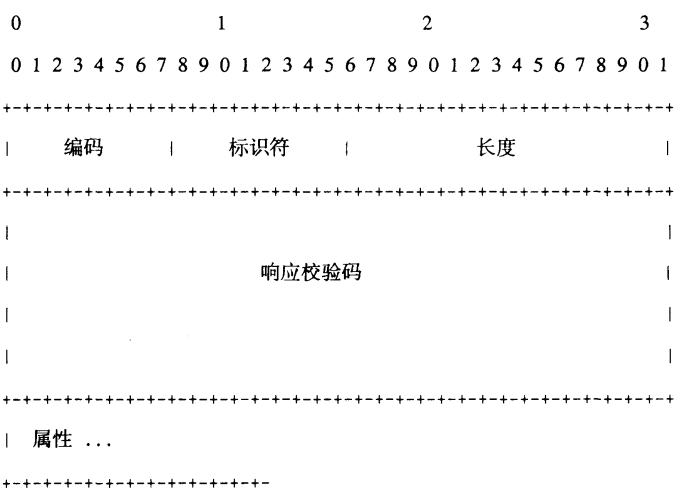
应答校验码：应答校验值是从前面描述过的接入请求值计算出来的。

属性：属性字段的长度是可变的，而且包含了0个或者多个属性的一个列表。

5.1.2.3 Access-Reject

如果任何接收到的属性值都不可接受，那么RADIUS服务器必须发送一个编码字段为3的数据包（access-reject）。它可能包括一个或者多个应答消息属性，在该属性中有一个接入服务器可能显示给用户的文本消息。

Access-Reject数据包的格式如下图所示。这些字段按照从左到右的顺序发送。



编码：Access-Reject的编码值是3。

标识符：标识符字段复制了引起Access-reject的接入请求的标识符字段。

应答校验符：应答校验符值和前面描述的一样，通过对接入请求值的计算而得到。

属性：该属性字段的长度可变，它包含了0个或者多个属性的一个列表。

5.1.2.4 Access-Challenge

如果RADIUS服务器希望发送给用户一个需要应答的质询消息，RADIUS服务器必须通过发送一个编码字段为11（Access-Challenge）的数据包来应答接入请求。

该属性字段可以具有一个或者多个应答消息属性和一个状态属性（state），或者什么都没有。也可以包括厂商特有的空闲超时、会话超时以及代理状态属性。在Access-Challenge中不能再包含任何其他的在本文档中定义的属性。

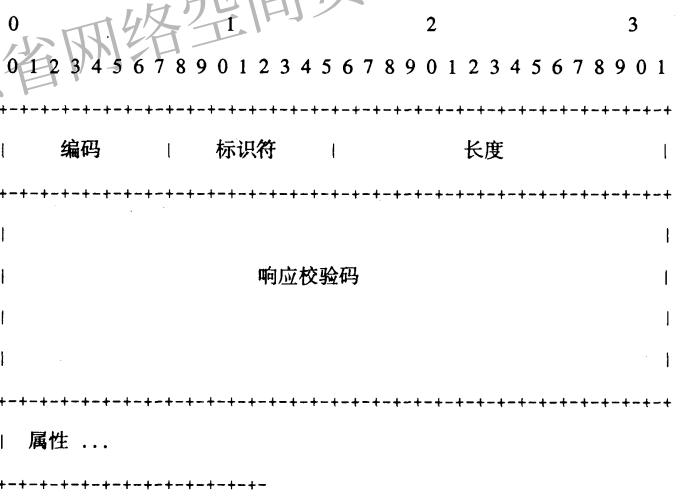
在收到一个Access-Challenge后，将标识符字段和未决的接入请求进行匹配。除此以外，应答Authenticator字段必须包含对未决的接入请求的正确的应答。丢弃无效的数据包。

如果接入服务器不支持质询/响应，它必须把Access-Challenge看作是接收到了一个access-reject数据包。

如果接入服务器支持质询/响应，那么接收到一个有效的access-challenge就意味着应该发送一个新的接入请求。如果可能的话，接入服务器可以向用户显示文本消息，并且提示用户给出应答。然后它发送它最初的接入请求，该申请具有一个新的申请ID和申请校验码，用户的应答（加密）代替了用户的口令属性，同时还包括来自Access-Challenge的任何一个状态（STATE）属性。在接入请求中最多只能包括一个状态属性的实例。

支持PAP的接入服务器可以将应答消息转发给拨号客户并且接受一个PAP应答，它可以把这个应答看作是用户输入的应答。如果接入服务器不支持上述做法，它必须把接受到的Access-Challenge看作是接收到一个access-reject数据包。

Access-Challenge数据包的格式如下图所示。这些字段按照从左到右的顺序发送。



编码：Access-Challenge的编码值为11。

标识符：标识符字段复制了引起Access-challenge接入请求的标识符字段。

应答校验字段：应答校验字段值和前面描述的一样，通过对接入请求值的计算而得到。

属性：该属性字段的长度可变，它包含0个或者多个属性的一个列表。

5.1.3 属性

RADIUS属性携带特定的验证、授权信息以及用于申请和应答的配置信息。

RADIUS数据包的长度来指示属性列表的结束。

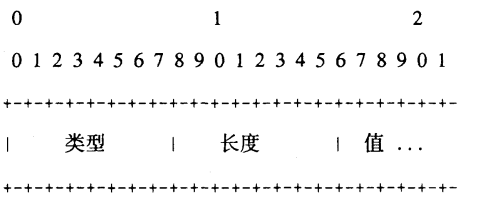
有些属性可能会包含多次，这样做的结果是一些属性所特有的，在对每个属性的描述有对此有规定。

如果出现了具有同样类型的多个属性，任何一个代理都要保持同样类型属性的顺序。不要求保持不同类型的属性的顺序。一个RADIUS服务器或者客户不能对不同类型的属性的顺序有任何依赖性。

对一个属性的描述限制了可以包含该属性的数据包类别，这个规定只是用于在本文档中定义的数据包类型，它们分别是Access-Request、Access-Accept、Access-Rejec和Access-Challenge（编码分别为1、2、3和11）。其他文档定义的其他的数据包类型也许也可以使用此处定义的属性。

和此处定义的数据包类型需要声明只有特定的属性可以在这些数据包中使用一样，将来定义的新属性也应该指示这些属性可以用在哪些数据包类型中。

属性格式如下图所示。这些字段按照从左到右的顺序发送。



类型（Type）：类型字段是一个字节。192~223留作实验用，224~240用作特殊的执行情况，241~255保留，不应该使用这些值。

一个RADIUS服务器可以忽略未知类型的属性。

一个RADIUS客户可以忽略未知类型的属性。

本标准涉及到了下面的属性值：

1 User-Name
2 User-Password
3 CHAP-Password
4 NAS-IP-Address
5 NAS-Port
6 Service-Type
7 Framed-Protocol
8 Framed-IP-Address
9 Framed-IP-Netmask
10 Framed-Routing
11 Filter-Id
12 Framed-MTU
13 Framed-Compression
14 Login-IP-Host
15 Login-Service
16 Login-TCP-Port
17 （未分配）
18 Reply-Message
19 Callback-Number
20 Callback-Id

21	（未分配）
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	Vendor-Specific
27	Session-Timeout
28	Idle-Timeout
29	Termination-Action
30	Called-Station-Id
31	Calling-Station-Id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
40~59	（为计费保留）
60	CHAP-Challenge
61	NAS-Port-Type
62	Port-Limit
63	Login-LAT-Port
79	EAP-Message
80	Message-Authenticator
85	Acct-Interim-Interval

长度：长度字段是一个字节，它表示了包括类型、长度以及属性值字段的这个属性的长度。如果ACCESS-REQUEST 中收到的属性中的长度字段无效，那么应该发送一个 ACCESS-REJECT 消息。如果接收到的 Access-Accept，Access-Reject 或者 Access-Challenge 数据包中属性中的长度字段无效，那么这个数据包可以作为 ACCESS-REJECT 或者直接丢弃。

数值（Value）：数值字段是 0 或者多个字节，它包含属性所特有的信息。数值字段的格式和长度是由类型和长度字段来决定的。

值字段的格式是 5 种数据类型中的一种。注意类型“文本（text）”是“字符串（string）”的一个子集。

文本：1~253 个字节包含 UTF-8 编码的 10646 个字符。不能发送长度为 0 的文本；相反应该忽略整个属性。

字符串：1~253 字节包含二进制数据（包含 0 和 255 的十进制数，包括 0 和 255）。不能发送长度为 0 的字符串；相反应该忽略整个属性。

地址：32 比特值，最高有效位在前面。

整数：32 比特无符号值，最高有效位在前面。

时间：32 比特无符号数，最高有效为在前面——从 1970 年 1 月 1 日 00:00:00 UTC 开始计秒。标准

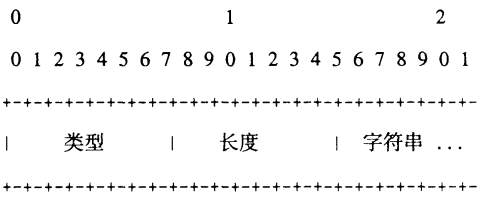
的属性不使用这种数据类型，在此描述它是为了在将来的属性中使用。

5.1.3.1 User-Name

本属性说明了将要验证的用户的名字。如果可用的话，它必须在 Access-Request 消息包中发送。

它可以在 Access-Accept 消息中发送，但是客户应该把在 Access-Accept 消息中返回的名字用在所有的该会话的计费申请数据包中。如果 access-accept 包括 Rlogin 的业务类型和用户名属性，接入服务器在执行 Rlogin 功能的时候，可以使用返回的用户名。

用户名属性格式如下所示。这些字段按照从左到右的顺序发送。



类型：用户名的类型值为 1。

长度：≥3

字符串：字符串字段是一个或者多个字节。接入服务器可能会限制用户名的长度，但是建议至少应该具有可以处理 63 字节的字符串的能力。

用户名的格式可以使下面几种模式的一种：

文本：只包括 UTF-8 编码的 10646 个字符；

网络接入标识符；

明确的名字（Distinguished name）：一个 ASN.1 形式的名字，用在公共密钥验证系统中。

5.1.3.2 User-Password

这个属性指出将要验证的用户口令，或者是在 access-challenge 后面的用户输入。它只用在 Access-Request 消息包。

在传输过程中，口令是隐藏的。在口令的最后填充 0 成为 16 字节的倍数。过共享的口令和它后面的申请校验码字节计算出一个单向的 MD5 杂散。这个值和口令最前面的 16 个字节进行异或操作，然后把它放置在用户口令属性的字符串字段的前 16 个字节内。

如果口令长于 16 个字符，那么需要执行第二次单向 MD5 杂散的计算，这个摘要是通过共享的密码和放在它后面的第一次或操作的结果来计算得到的。这个杂散和口令的第二个 16 个字节进行或操作，然后将结果放置在用户口令属性的字符串的第二个 16 字节处。

如果需要的话，还可以重复这个操作，通过每个或操作的结果和共享的口令来生成下一个杂散，该杂散和口令的下一个 16 字节或，但是杂散不能超过 128 个字符。

将共享的口令称作 S，伪随机 128 比特的申请校验码为 RA。将口令分成 16 字节为一组的字段 P1、P2 等。将最后的不足 16 字节部分填充 0 到 16 字节。将密码组称作 c（1），c（2）等。中间的值称作 b1、b2 等。

$$b1 = MD5(S + RA) \qquad c(1) = p1 \text{ xor } b1$$

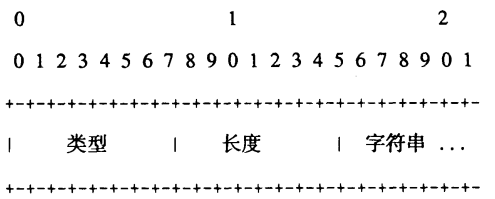
$$b2 = MD5(S + c(1)) \qquad c(2) = p2 \text{ xor } b2$$

$$bi = MD5(S + c(i-1)) \qquad c(i) = pi \text{ xor } bi$$

字符串包含 c（1）+c（2）+...+c（i），此处“+”代表结合在一起。

在接收端，进行逆过程来生成最初的口令。

用户口令属性的格式如下所示。这些字段按照从左到右的顺序发送。



类型：用户口令的类型为 2。

长度：至少为 18 字节但是不能长于 130 字节。

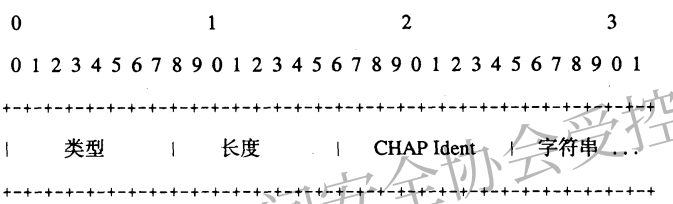
字符串：字符串字段的长度在 16 到 128 字节之间，包括 16 和 128 字节。

5.1.3.3 CHAP-Password

这个属性给出了 PPP CHAP 用户在应答 challenge 时的应答值。它只用在 Access-Request 消息包中。

如果数据包中存在 CHAP-challenge 属性，在该属性（60）中可以找到 CHAP challenge 值，否则在申请校验码字段中可以找到 CHAP challenge 值。

CHAP 口令属性格式如下所示。这些字段按照从左到右的顺序发送。



类型：CHAP 口令的类型是 3。

长度：19

CHAP 标识符：这个字段是 1 个字节，包括来自用户 CHAP 应答消息的 CHAP 标识符。

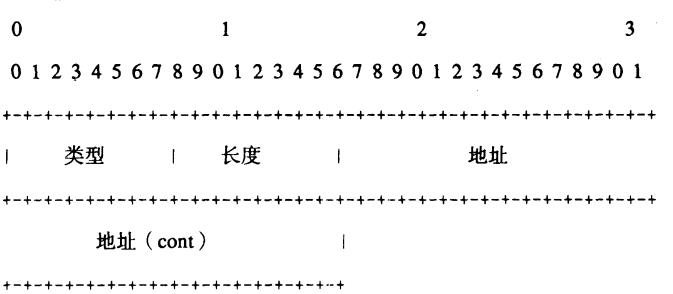
字符串：字符串字段是 16 字节，包含来自用户的 CHAP 应答消息。

5.1.3.4 NAS-IP-Address

该属性给出了验证申请用户的标识 IP 地址，在 RADIUS 服务器范围内，它对接入服务器应该是惟一的。NAS-IP 地址只用在 Access-Request 消息包中。在 Access-Request 消息包中必须出现 NAS-IP 地址或者接入服务器标识符。

注意不能用 NAS-IP 地址来选择验证申请的共享口令。必须利用 Access-Request 消息包中的源 IP 地址来选择共享口令。

NAS-IP 地址属性的格式如下所示。这些字段按照从左到右的方式发送。



类型：NAS-IP 地址的类型是 4。

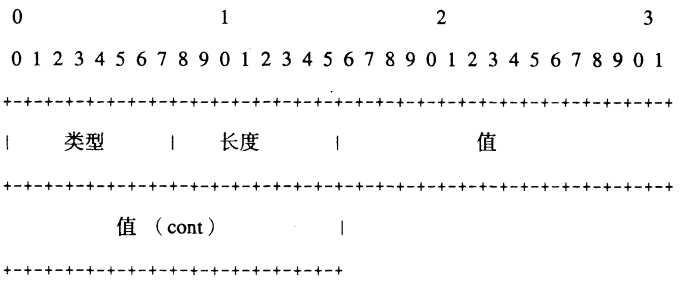
长度：6

地址：地址字段是4个字节。

5.1.3.5 NAS-Port

该属性字段给出了正在验证用户的接入服务器物理端口号。它只用在 Access-Request 消息包里。注意此处“端口”是指接入服务器上的物理连接，而不是通常意义上的 TCP 或者 UDP 端口号。如果接入服务器区分不同的端口，那么接入服务器端口或者接入服务器端口类型（61）或者两个一起应该出现在 Access-Request 消息包中。

接入服务器端口格式如下图所示。这些字段按照从左到右的方式发送。



类型：接入服务器端口的类型为5。

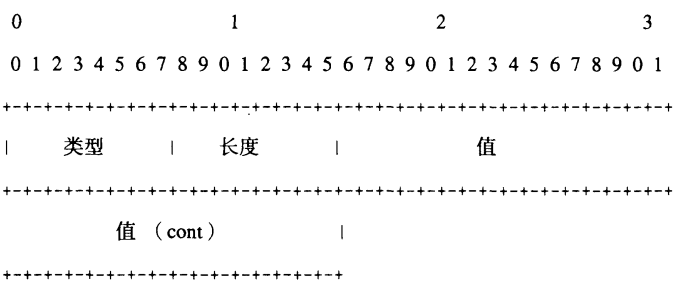
长度：6

值：这个值字段应该是4个字节。

5.1.3.6 Service-Type

这个属性指出了用户申请的业务类型，或者提供给用户的业务类型。它可以用在接入请求以及 Access-Accept 消息中。并不要求接入服务器要执行所有的业务类型，而且接入服务器必须把未知的后者不支持的业务类型当作是收到了 access-reject 消息。

业务类型属性的格式如下图所示。



类型：业务类型的类型值是6。

长度：6

值：值字段是4个字节。

1	Login
2	Framed
3	Callback Login
4	Callback Framed
5	Outbound
6	Administrative
7	NAS Prompt
8	Authenticate Only

9 Callback NAS Prompt

10 Call Check

11 Callback Administrative

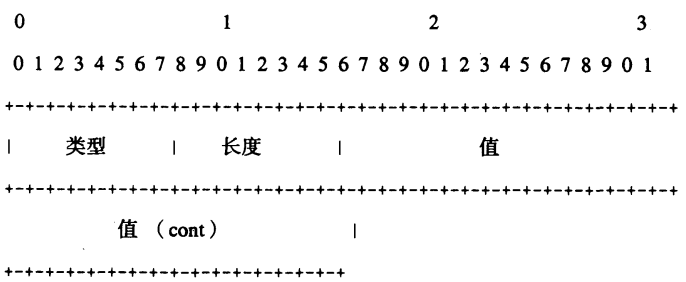
在 access-accept 中业务类型的定义如下。用在接入请求里的时候，可能将它们看作是对 RADIUS 服务器的一个提示，也就是说接入服务器有理由相信用户希望使用给出的业务类型，但是不要求服务器接受这个提示。

Login	用户应该和主机互连
Framed	应该为用户启用成帧的协议例如 PPP 或者 SLIP
Callback Login	用户断开连接并且回呼，然后再与主机互连
Callback Framed	用户断开连接然后回呼，于是为用户开启成帧协议例如 PPP 或者 SLIP
Outbound	同意用户访问外部（outgoing）设备
Administrative	通过特权命令，应该允许用户接入到接入服务器的管理接口
NAS Prompt	在接入服务器上应该为用户提供一个命令提示符，在命令符后面输入非特权命令
Authenticate Only	申请只验证，不需要在 Access-Accept（典型地是用在代理服务器上，而不是用在接入服务器本身上）中返回授权信息
Callback NAS Prompt	断开用户并且回呼，然后在接入服务器上提供一个命令提示符，在命令符后面输入非特权命令
Call Check	接入服务器用在 Access-Request 消息包中说明收到了一个呼叫，RADIUS 服务器应该根据 called-station-id 或者 Calling-Station-Id 属性消息发送回一个 access-accept 消息来应答这个呼叫，或者发送一个 access-reject 来拒绝这个呼叫。建议这样的接入请求把 Calling-Station-Id 的值作为用户名的值
Callback Administrative	断开用户后回呼它，然后同意它接入到接入服务器的管理接口，通过它执行特权命名

5.1.3.7 Framed-Protocol

该属性说明了成帧接入要采用的成帧技术。它可以用在Access-Request和Access-Accept消息中。

Framed-protocol属性的格式如下图所示。这些字节按照从左到右的顺序发送。



类型：Framed-Protocol的类型值为7。

长度：6

值：值字段是4个字节。

1 PPP

2 SLIP

3 AppleTalk Remote Access Protocol （ARAP）

4 Gandalf 所有的 SingleLink/MultiLink 协议

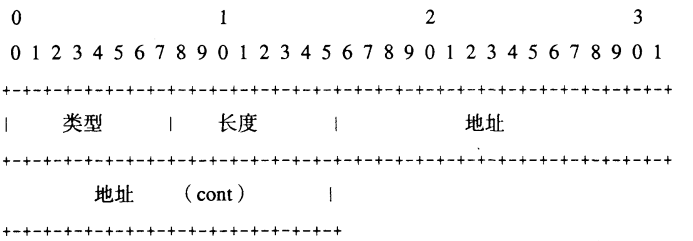
5 Xylogics 所有的 IPX/SLIP

6 同步 X.75

5.1.3.8 Framed-IP-Address

这个属性说明了用户将要被配置的地址。它可以用在Access-Accept消息中。它可以用在接入请求中做为接入服务器给服务器的一个提示，也就是说接入服务器希望选择这个地址，但是并不要求服务器要接受这个提示。

Framed-IP-Address属性的格式如下图所示。该字段按照从左到右的顺序发送。



类型：Framed-IP-Address 的类型值是 8。

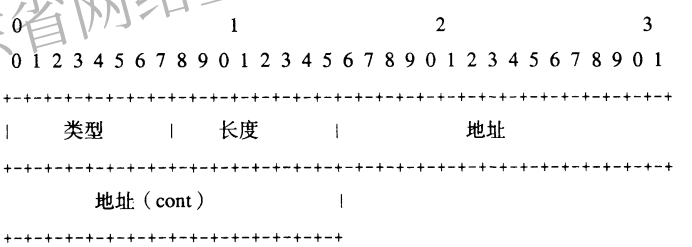
长度：6

地址：地址字段是 4 个字节。0xFFFFFFFF 说明接入服务器应该允许用户选择地址（例如，通过协商的方式）。0xFFFFFFFE 说明接入服务器应该为用户选择一个地址（例如，为用户分配一个接入服务器所拥有的地址池中的一个地址）。其他有效的地址值说明接入服务器应该使用这些值作为用户的 IP 地址。

5.1.3.9 Framed-IP-Netmask

当用户是到网络的一个路由器时，该属性给出了需要为用户配置的 IP 网络掩码（netmask）。它可以用在 Access-Accept 消息中。它用在 Access-Request 消息包中作为接入服务器给服务器的一个提示，接入服务器提示它希望使用该网络掩码，但是并不要求服务器接受这个提示。

Framed-IP-Netmask 属性格式如下图所示。这些字段按照从左到右的顺序发送。



类型：Framed-IP-Netmask 的类型值为 9。

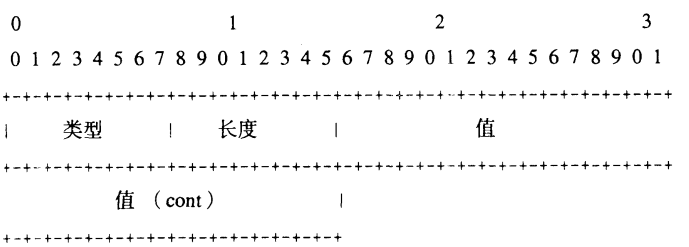
长度：6

地址：地址字段是 4 个字节，它说明用户的 IP 网络掩码。

5.1.3.10 Framed-Routing

当用户是到网络的一个路由器时，该属性说明了用户采用的路由方式。它只用在 Access-Accept 消息中。

Framed-Routing 属性的格式如下图所示。这些字段按照从左到右的方式发送。



类型：Framed-Routing 的类型值是 10。

长度：6

值：值字段是 4 个字节。

0	None
1	发送路由数据包
2	监听路由数据包
3	发送和监听

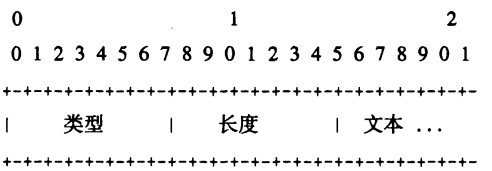
5.1.3.11 Filter-Id

描述

这个属性说明了用户过滤器表的名字。在 Access-Accept 消息中可以发送 0 个或者多个过滤器 id 属性。

用名字来表示一个过滤器使得过滤器可以用在不同的接入服务器上，而无需考虑过滤器列表的详细情况。

过滤器标识属性的格式如下所示。这些字段按照从左到右的方式发送。



类型：过滤器标识的类型值为 11。

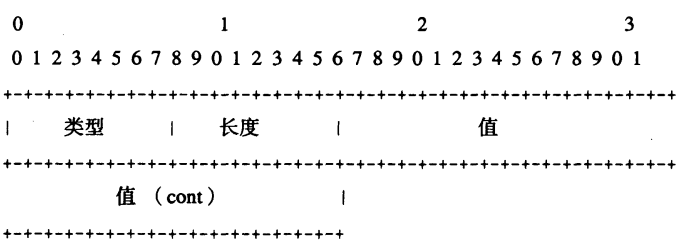
长度：≥3

文本：文本字段是 1 个或者多个字节，它的内容和执行的操作有关。它将要做成可读而且不能影响协议的操作。建议消息包含 UTF-8 编码的 10646 个字符。

5.1.3.12 Framed-MTU

当无法通过其他方式（例如 PPP）协商最大传输单元时，利用这个属性给出了为用户配置的最大传输单元。它可以用在 Access-Accept 消息中。它也可以用在接入请求中，此时接入服务器通过它来提示服务器，它希望使用这个值，但是并不要求服务器接受这个提示。

Framed-MTU 属性的格式如下图所示。这些字节按照从左到右的方式发送。



类型：Framed-MTU 的类型值为 12。

长度：6

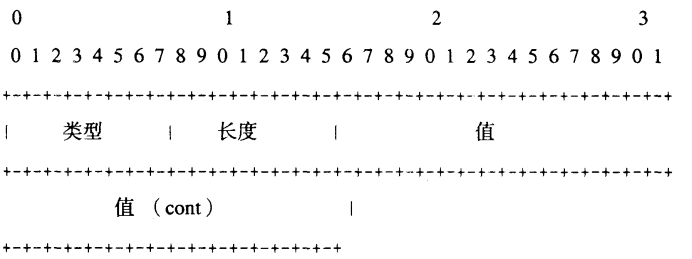
值：值字段为 4 个字节。不管该字段的大小，该值的范围是从 64 到 65535。

5.1.3.13 Framed-Compression

该属性给出了链路使用的压缩协议。它可以用在 Access-Accept 消息中。它也可以用在 Access-Request 消息包中，作为接入服务器给服务器的一个提示，也就是说接入服务器希望使用这种压缩协议，但是并不强制接入服务器接受这个提示。

可以发送多个压缩协议。接入服务器负责为相应的链路流量选择合适的压缩协议。

Framed-Compression 属性的格式如下所示，这些字节按照从左到右的方式发送。



类型：Framed-Compression 的类型值是 13。

长度：6

值：值字段是 4 个字节。

0 None

1 VJ TCP/IP 包头压缩[10]

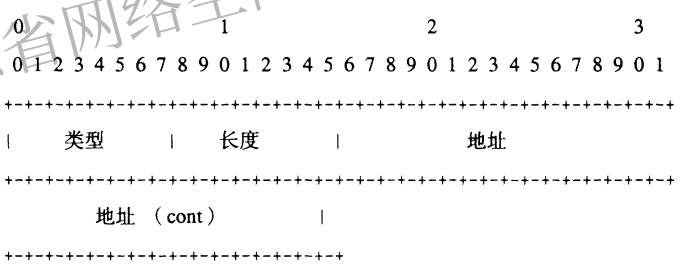
2 IPX 包头压缩

3 Stac-LZS 压缩

5.1.3.14 Login-IP-Host

当包含了 Login-Service 属性的时候，该属性给出了连接用户的系统。它可以用在 Access-Accept 消息中。它也可以用在 Access-Request 消息包中作为给服务器的一个提示，它提示接入服务器希望使用这个主机，但是并不要求服务器接受这个提示。

Login-IP-Host 属性格式如下图所示。这些按照从左到右的方式发送。



类型：Login-IP-Host 的类型值为 14。

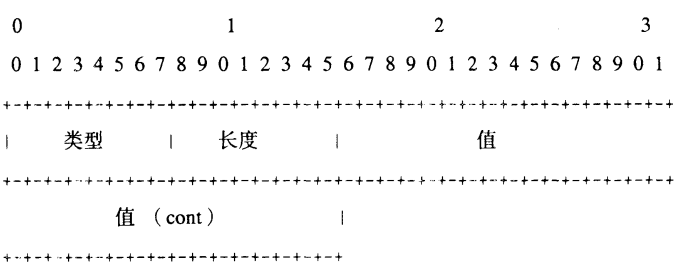
长度：6

地址：地址字段是 4 个字节。0xFFFFFFFF 说明接入服务器应该允许用户选择一个地址。0 代表接入服务器应该选择一个连接用户的主机。其他值说明了接入服务器应该将用户连接到的地址。

5.1.3.15 Login-Service

该属性说明了用户连接到登陆主机将使用的的服务。它只用在 Access-Accept 消息中。

Login-Service 属性的格式如下所示。这些字段按照从左到右的方式发送。



类型：Login-Service 的类型值是 15。

长度：6

值：值字段是 4 个字节。

0 Telnet

1 Rlogin

2 TCP Clear

3 PortMaster （专用的）

4 LAT

5 X25-PAD

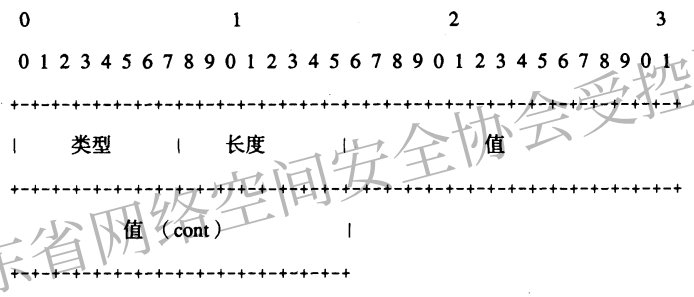
6 X25-T3POS

8 TCP Clear Quiet

5.1.3.16 Login-TCP-Port

当出现了 Login-Service 属性的时候，该属性指示了连接用户的 TCP 端口。它只用在 Access-Accept 消息中。

Login-TCP-Port 属性的格式如下图所示。这些按照从左到右的方式传送。



类型：Login-TCP-Port 的类型值是 16。

长度：6

值：值字段是 4 个字节。该值的范围是从 0-65535。

5.1.3.17 Reply-Message

该属性说明了可以显示给用户的文本内容。

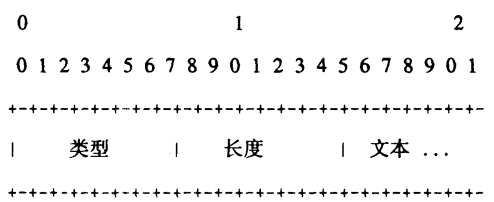
当用在 Access-Accept 消息中的时候，它是一个成功消息。

用在 access-reject 中，它是一个失败的消息。在用户试图发送另外一个接入请求之前，它可以作为一个对话消息来提示用户。

如果用在 Access-Challenge 数据包中，它作为一个对话消息来提示用户做出应答。

可以包含多个应答消息，如果所有的消息都可以显示，那么应该按照它们在数据包中的顺序来显示它们。

应答消息属性格式如下所示。这些按照从左到右的顺序发送。



类型：应答消息的类型值为 18。

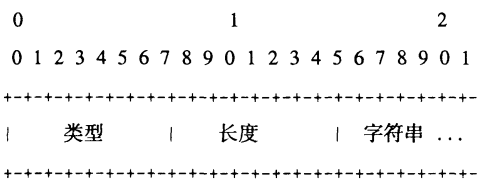
长度：≥3

文本：文本字段是 1 个或者多个字节，而且它们的内容与执行情况有关。它们试图做成可读的，但是不能影响协议的操作。建议消息包含 UTF-8 编码的 10646 字符。

5.1.3.18 Callback-Number

该属性给出了用于回呼的一个字符串。它可以用在 Access-Accept 消息中。它也可以用在 Access-Request 消息包中作为给服务器的一个提示，它提示服务器用户希望使用回呼业务，但是不要求服务器接受这个提示。

回呼号码属性的格式如下图所示。这些字节按照从左到右的方式发送。



类型：回呼号码的类型值是 19。

长度：≥3

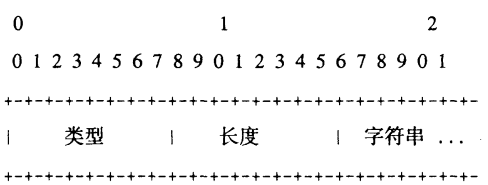
字符串：字符串字段是 1 个或者多个字节。该消息的实际格式是站点或者应用所特有的，一个强壮的执行应该把这个字段看作是普通的字节。

对这个字节的使用范围的规定不在本标准的范围内。

5.1.3.19 Callback-Id

这个属性给出了将要接受回呼地方的名字，由接入服务器负责解释。它可以用在 Access-Accept 消息中。

Callback-Id 属性格式如下图所示。它们按照从左到右的方式发送。



类型：Callback-Id 的类型值是 20。

长度：≥3

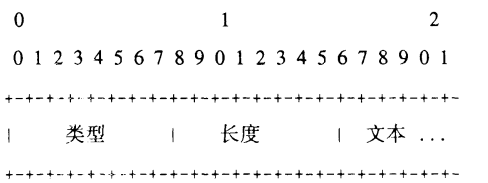
字符串：字符串字段是 1 个或者多个字节。信息的实际格式是站点或者应用所特有的，一个强壮的应用应该把这个字段看作是普通字节。

对这个字节的使用范围的规定不在本标准的范围内。

5.1.3.20 Framed-Route

该属性给出了接入服务器将要为用户配置的路由信息。它用在 Access-Accept 消息中而且可以多次出现。

Framed-Route 属性格式如下图所示。这些字节按照从左到右的顺序发送。



类型：Framed-Route 的类型值是 22。

长度：≥3

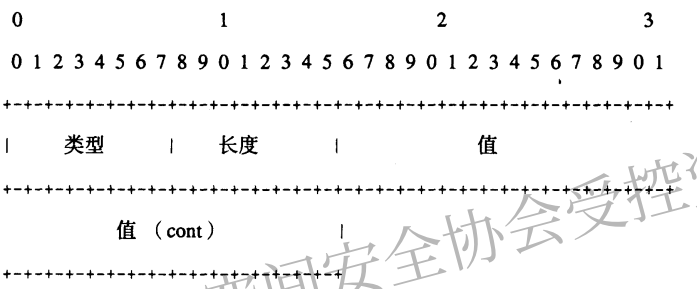
文本：文本字段是 1 个或者多个字节，它的内容与应用有关。它试图做成可读的而且不能影响协议的操作。建议该消息包含 UTF-8 编码的 10646 字符.对于 IP 路由，它应该包含一个以 4 个点隔开的 4 位十进制地址，可以选择性地加上一个/以及一个十进制的长度说明符，从而说明使用了前缀的高位比特位的数量。然后加一个空格，接下来是以 4 个点隔开的 4 位十进制网关地址，空格，然后是一个或者多个由空格分开的衡量指标。例如，“192.168.1.0/24 192.168.1.1 1 2 -1 3 400”。可以省略长度指示符，在这种情况下，类别 A 前缀的缺省值是 8 比特，类别 B 前缀的缺省值是 16 比特，类别 C 前缀的缺省值是 24 比特。例如，“192.168.1.0 192.168.1.1 1”。

当将网关地址定义为“0.0.0.0”时，应该把用户的 IP 地址作为网关地址。

5.1.3.21 Framed-IPX-Network

本属性说明了将要为用户配置的 IPX 网络号。它用在 Access-Accept 消息中。

Framed-IPX-Network 属性格式如下图所示。这些字段按照从左到右的顺序发送。



类型：Framed-IPX-Network 的类型值是 23。

长度：6

值：值字段是 4 个字节。0xFFFFFFFE 指示接入服务器应该为用户选择一个 IPX 网络（例如，从接入服务器控制的具有一个或者多个 IPX 网络的网络池中分配）。其他的值应该用作到达用户的链路的 IPX 网络。

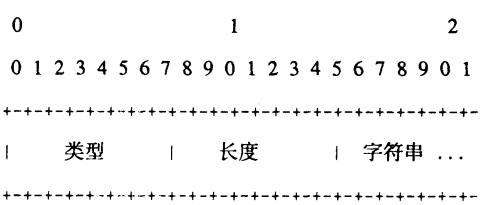
5.1.3.22 State

该属性可以由服务器在 access-challenge 数据包中发送给客户，如果用户需要应答，那么必须不加改动地通过新的接入请求应答数据包从客户发送给服务器。

该属性也可以由服务器通过 access-accept 发送给客户，在该数据包中还包含了一个带有 RAIDUS 申请值的 Termination-Action 属性。如果接入服务器通过发送一个新的接入请求来终止当前的会话从而执行 Termination-Action 属性，那么在接入请求中一定要包括未加改动的状态属性。

不管采用何种使用方式，客户不能在本地翻译该属性。一个数据包只能含有一个或者不包含状态属性。状态属性的使用与执行情况无关。

状态属性的格式如下图所示，这些字段按照从左到右的方式发送。



类型：状态属性的类型值是 24

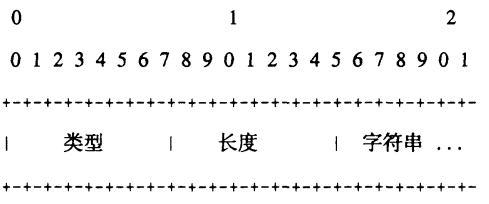
长度：≥3

字符串：字符串字节是 1 个或者多个字节。该信息的实际格式是站点或者应用特有的，一个强壮的执行情况应该把该字节看作是普通的字节。

5.1.3.23 Class

该属性由服务器通过 access-accept 发送给客户，如果支持计费功能，那么客户应该把该属性作为计费申请数据包的一部分，不加修改地发送给计费服务器。客户不能在本地翻译该属性。

类别属性的格式如下图所示。这些字段按照从左到右的方式发送。



类型：类别的类型值是 25。

长度：≥3

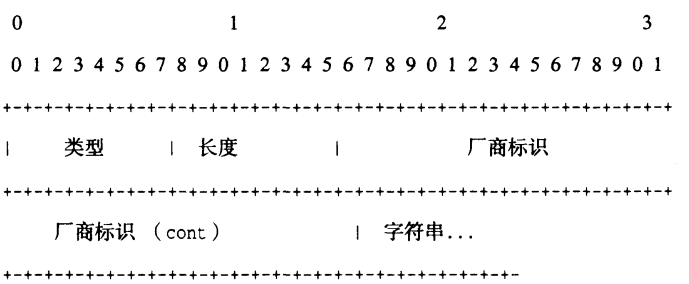
字符串：字符串字段时一个或者多个字节。这些信息的实际格式是站点或者应用所特有的，而且一个强壮的执行情况应该把这个字段看作是普通的字节。

5.1.3.24 Vendor-Specific

这个属性让设备厂商可以支持他们自己的非通用的扩展的属性。但它不能影响 RADIUS 协议的运行。

没有配备可以翻译客户发送过来的厂商特有信息的功能的服务器必须忽略这些信息（即使这些是报告信息）。没有收到期望的厂商特有信息的客户应该试着在没有这些信息的情况下执行它，虽然它可能是通过一种降级的模式来执行这些操作（并且报告它们正在执行这些动作）。

厂商特有属性的格式如下图所示。它们是按照从左到右的顺序发送。



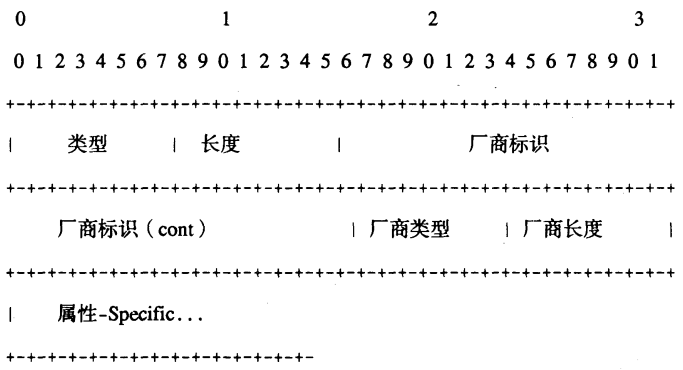
类型：厂商特有属性值为 26。

长度：≥7

厂商 ID：高位字节是 0，低位的 3 个字节是符合网络字节顺序的厂商的 SMI 网络管理专用企业编码，它的定义参见 RFC 的“分配号码”。

字符串：字符串字段是 1 个或者多个字节。该信息的实际格式是站点或者应用所特有的，一个强壮的执行情况应该把这个字段看作是普通的字节。

应该将它编码成厂商类型/厂商长度/值字段等一个序列，如下图所示。特有属性字段与厂商对属性的定义有关。下图给出了一个采用这个方法对厂商特有属性编码的例子。

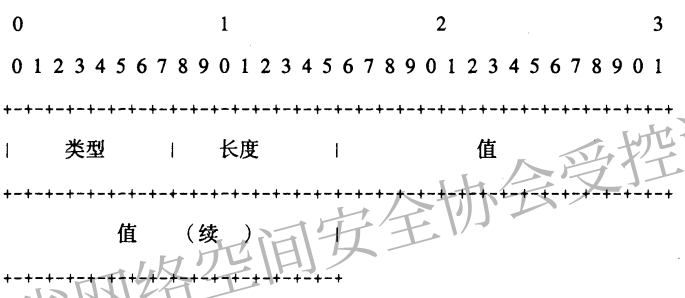


可以把多个子属性编码到一个单一的厂商特有属性中，但不是必须这样做。

5.1.3.25 Session-Timeout

该属性设置了在会话或者提示终止之前可以提供给用户的最大秒数。服务器可以通过 access-accept 或者 access-challenge 来把这个属性发送给客户。

会话超时属性格式如下图所示。这些字段按照从左到右的顺序发送。



类型：会话超时的类型值是 27。

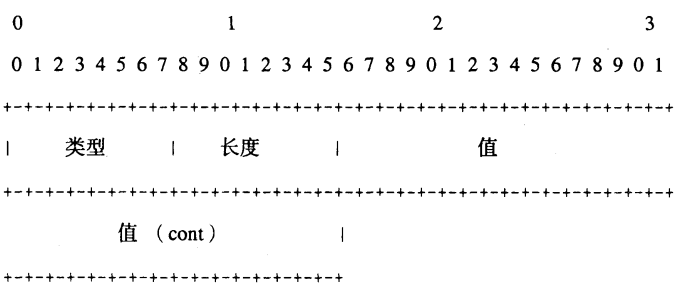
长度：6

值：该字段是 4 个字节，包含一个 32 比特无符号整数，说明了允许用户连接到接入服务器的最长的秒数。

5.1.3.26 Idle-Timeout

该属性设置了在终止会话或者提示之前，用户可以保持空闲连接的最大连续秒数。服务器可以通过 Access-Accept 或者 Access-Challenge 将这个属性发送给客户。

空闲超时属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：空闲超时的类型值是 28。

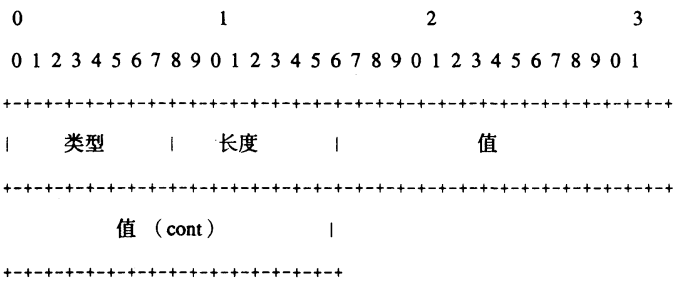
长度：6

值：这个字段是 4 个字节，包含一个 32 比特无符号整数，说明在接入服务器中断用户的连接之前，用户连接可以保持空闲的连续秒数。

5.1.3.27 Termination-Action

这个属性描述当规定的业务完成以后，接入服务器应该采取的动作。它只用在 access-accept 消息包中。

终止行为属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：终止行为的类型值 29。

长度：6

值：值字段是 4 个字节。

0 缺省值

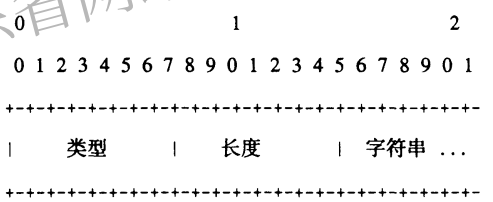
1 RADIUS 申请

如果值字段设置为 RADIUS 申请，在终止规定的业务后，接入服务器可能会向 RADIUS 服务器发送一个新的接入请求消息，该消息包括任何存在的状态属性。

5.1.3.28 Called-Station-Id

这个属性让接入服务器在 Access-Request 消息包中发送被叫用户的电话号码，采用的是拨号标识或者相似的技术。注意，这个号码可能和呼叫近来的号码不同。它只用在 Access-Request 消息包中。

Called-Station-Id 属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：Called-Station-Id 的类型值是 30。

长度：≥3

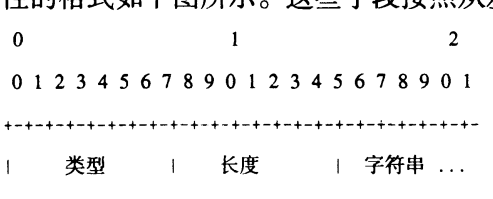
字符串：字符串字段是 1 个或者多个字节，包含了接入呼叫用户的电话号码。

该信息的实际格式是站点或者应用所特有的。建议采用 UTF-8 编码的 10646 字符，但是一个强壮的执行情况应该把这个字段看作是普通的字节。

5.1.3.29 Calling-Station-Id

这个属性允许接入服务器在 Access-Request 消息包中发送呼叫用户的电话号码，采用自动号码标识或者相似的技术。它只用在 Access-Request 消息包中。

Calling-Station-Id 属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：Calling-Station-Id 的类型值是 31。

长度：≥3

字符串：字符串是一个或者多个字节，包含呼叫用户的电话号码。

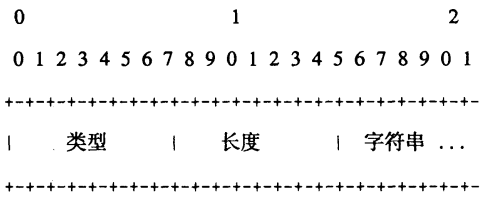
该信息的实际格式是站点或者应用所特有的。建议采用 UTF-8 编码的 10646 字符，但是一个强壮的执行情况应该把这个字段看作是普通的字节。

5.1.3.30 NAS-Identifier

这个属性包含一个标识发起接入请求的接入服务器的字符串。它只用在 Access-Request 消息包中。NAS-IP-Address 或者 NAS-Identifier 必须出现在 Access-Request 消息包中。

注意不能用 NAS-Identifier 来选择用于验证申请的共享口令。必须用 Access-Request 消息包的源 IP 地址来选择共享口令。

NAS-Identifier 属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：NAS-Identifier 的类型值是 32。

长度：≥3

字符串：字符串字段是一个或者多个字节，并且在 RADIUS 服务器范围内，对接入服务器应该是惟一的。例如，一个完全合格的域名应该适合作为一个接入服务器标识。

该信息的实际格式是站点或者应用所特有的，而且一个强壮的执行情况应该把这个字段看作是普通的字节。

5.1.3.31 Proxy-State

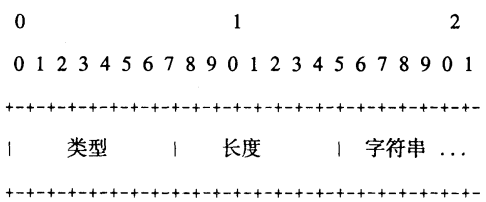
当代理服务器向另外一个服务器转发接入请求的时候，会发送这个属性并且必须在 Access-Accept、Access-Reject 或者 Access-Challenge 中不加改变地返回。当代理服务器收到了关于它的申请的应答，在把这个应答转发给接入服务器之前，它必须要去掉它自己的代理状态属性（数据包中最后一个代理状态）。

在转发数据包的时候，如果为数据包加入了一个代理属性，那么这个代理属性应该放在任何一个现有代理属性的后面。

除了由当前服务器加入的代理属性，应该认为其他已经存在的代理属性的内容是不透明的字节并且不能影响协议的操作。

对代理属性的使用和执行情况有关。对它的功能的描述不在本标准范围内。

代理状态属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：代理状态的类型值是 33。

长度：≥3

字符串：字符串字节是一个或者多个字节。该信息的实际格式是站点或者应用所特有的，一个强壮的执行情况应该把这些字段看作普通字节。

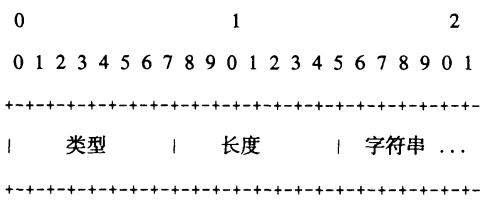
5.1.3.32 Login-LAT-Service

这个属性说明了通过 LAT 与用户相连的系统。只有将 LAT 定义为 Login-service 时，才可以把该属性用在 Access-Accept 消息中。它可以用在 Access-Request 消息包中作为给服务器的一个提示，但是并不要求服务器接受这个提示。

管理者在处理簇系统的时候会使用业务属性，例如 VAX 或者 Alpha 簇。在那种环境下，几个不同时间共享的主机共享同样的资源（磁盘、打印机等），而且管理者通常为每个主机进行配置从而为每个可访问的共享资源提供连接。在这种情况下，簇中的每个主机都通过 LAT 广播来公布它自己的业务。

精明的用户通常知道哪个业务供应商（机器）更快一些而且在发起一个 LAT 连接的时候希望使用一个节点名字。可选择地是，一些管理者希望特定的用户使用某些机器，把这种做法作为平衡负载的一种简单的方式（尽管 LAT 自己知道如何平衡负载）。

Login-LAT-Service 属性的格式如下图所示。这些字节按照从左到右的方式发送。



类型：Login-LAT-Service 的类型值是 34。

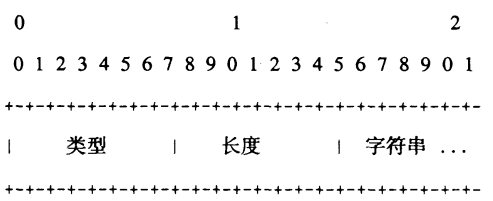
长度：≥3

字符串：字符串字节是一个或者多个字节，并且包含使用的 LAT 业务的身份。LAT 结构使这个字符串包含$（美元符号），-（横线），.（点），_（下划线），数字，大小写字母以及 ISO Latin-1 字符扩展集[11]。所有 LAT 字符串的对比与大小写无关。

5.1.3.33 Login-LAT-Node

这个属性给出了 LAT 将用户自动连接到的节点。只有 LAT 被定义为 Login 业务，它才可以用在 Access-Accept 消息中。它也可以用在 Access-Request 消息包中，作为给服务器的一个提示，但是并不要求服务器接受这个提示。

Login-LAT-Node 的属性格式如下图所示。这些字段按照从左到右的顺序发送。



类型：Login-LAT-Node 的类型值为 35。

长度：≥3

字符串：字符串字段时一个或者多个字节，包含将用户与相应节点连接起来的 LAT 的身份。LAT 结构使这个字符串包含$（美元符号），-（横线），.（点），_（下划线），数字，大小写字母以及 ISO Latin-1 字符扩展集[11]。所有 LAT 字符串的对比与大小写无关。

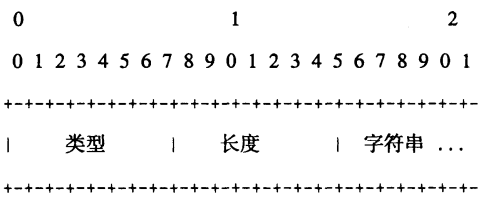
5.1.3.34 Login-LAT-Group

这个属性包含了一个字符串，该字符串确定了用户得到授权可以使用的 LAT 组编码。只有 LAT 被定义为 Login 业务时，它才可以用在 Access-Accept 消息中。它可以用在 Access-Request 消息包中，作为给服务器的一个提示，但是不要求服务器接受这个提示。

LAT 支持 256 个不同的组编码，LAT 使用它们作为接入权力的一种形式。LAT 将组编码编成为一个 256 比特的位图。

LAT 业务供应商可以分配给管理者一个或者多个组编码；它只接受在位图中具有这些组编码的 LAT 连接。管理者为每个用户分配一个授权组编码的位图；LAT 从操作系统中获得这些编码，并且把它们用在提交给业务供应商的申请中。

Login-LAT-Group 属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：Login-LAT-Group 的类型值是 36。

长度：34

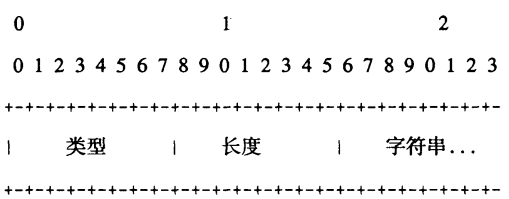
字符串：字符串字节是 32 字节的位图，最高有效位字节在前面。一个强壮的执行情况应该把这些字段看作是普通的字节。

5.1.3.35 CHAP-Challenge

这个属性包含了接入服务器发送给 PPP CHAP 用户的 CHAP 口令（Challenge）。它只用在 Access-Request 消息包中。

如果 CHAP 口令值是 16 字节，可能会把它放置在 Request Authenticator 字段而不再放在本属性中。

CHAP-Challenge 属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：CHAP-Challenge 的类型值是 60。

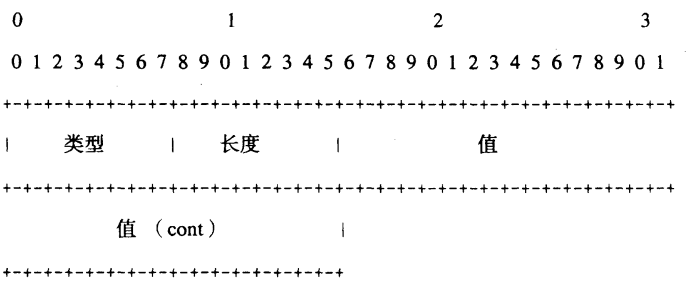
长度：≥7

字符串：字符串字段包含 CHAP 口令。

5.1.3.36 NAS-Port-Type

该属性给出了接入服务器用来验证用户的物理端口类型。它可以代替或者补充 NAS-Port 属性。它只用在 Access-Request 消息包中。如果接入服务器的端口有区别，那么在 Access-Request 消息包中应该出现 NAS-Port 或者 NAS-Port-Type 或者两者同时出现。

NAS-Port-Type 属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：NAS-Port-Type 的类型值是 61。

长度：6

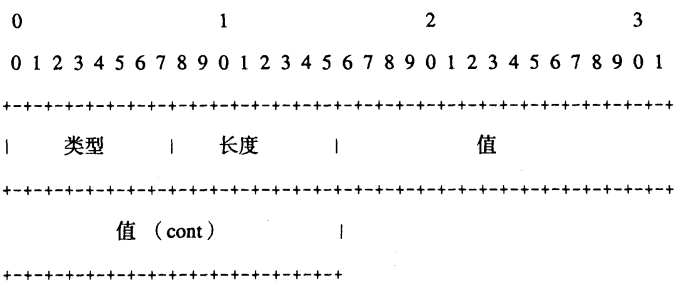
值：值字段是 4 个字节。“虚拟”是指到接入服务器的一条不是通过物理端口而是通过某种传输协议形成的连接。例如，如果一个用户作为流出用户 Telnet 到一个接入服务器来验证自己，接入请求可能会包括 NAS-Port-Type 为虚拟的属性，从而作为给 RADIUS 服务器的一个提示，提示用户不在物理端口上。

0	Async
1	Sync
2	ISDN Sync
3	ISDN Async V.120
4	ISDN Async V.110
5	虚拟
6	PIAFS
7	HDLC 非信道化线路
8	X.25
9	X.75
10	G.3 Fax
11	SDSL
12	ADSL-CAP
13	ADSL-DMT
14	IDSL
15	以太网
16	xDSL
17	有线电视线路
18	无线
19	无线 - IEEE 802.11

5.1.3.37 Port-Limit

这个属性设置了接入服务器可以提供给用户的最大的端口数。服务器可以在 Access-Accept 消息中把这个属性发送给客户。它有意和多链路 PPP[12]结合起来使用或者是类似的用法。接入服务器也可以把它发送给服务器作为一个提示，提示需要使用多个端口，但是不要求服务器接受这个提示。

端口限制属性格式如下图所示。这个字段按照从左到右的顺序发送。



类型：端口限制的类型值为62。

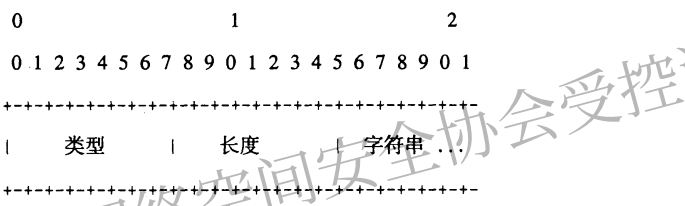
长度：6

值：值字段是4个字节，包含一个32比特无符号整数，给出了用户允许连接到接入服务器上的最多的端口数。

5.1.3.38 Login-LAT-Port

本属性给出了LAT将用户与之连接起来的端口。只有当将LAT定义为Login业务的时候，它才可以用在Access-Accept消息中。它可以用在Access-Request消息中作为给服务器的一个提示，但是不要求服务器接受这个提示。

Login-LAT-Port属性的格式如下图所示。这些字段按照从左到右的顺序发送。



类型：Login-LAT-Port的类型值是63。

长度：≥3

字符串：字符串字段是一个或者多个字节，而且包含了将要使用的LAT端口的身份。LAT结构允许这个字符串包含$（美元），-（连字符），.（点），_（下划线），数字，大小写字母以及ISO Latin-1字符扩展集。所有的LAT字符串对比与大小写无关。

5.1.3.39 EAP-Message

这个属性封装了扩展接入协议（EAP）的包。可以允许NAS通过EAP方式对拨入用户进行认证，而不必理解EAP协议。

NAS把收到的EAP消息放到一个或多个EAP属性中，并作为Access-Request消息的一部分前转给RADIUS服务器。RADIUS服务器可以返回Access-Challenge、Access-Accept、Access-Reject消息。

RADIUS服务器收到了EAP消息，如果不能理解，应返回Accept-Reject消息。

NAS把用户发来的EAP消息放到一个或多个EAP-Message属性里并在一个Access-Request消息里前转给RADIUS服务器，如果有多个EAP-Message属性，它们必须连续放置于Access-Request或Access-Challenge消息中。Access-Accept与Access-Reject消息只能有一个EAP-Message属性，来承载EAP-Success或EAP-Failure消息。

EAP会使用多种认证的方式，包括强加密的方式。为了防止攻击者暗中破坏RADIUS/EAP，RADIUS/EAP提供保护机制是非常必要的，其强度至少与采用的EAP认证方式相同。

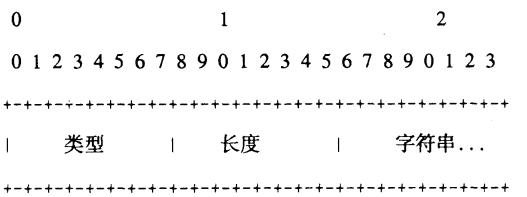
因此Message-Authenticator属性必须用于保护所有包括EAP-Message属性的Access-Request、

Access-Challenge、Access-Accept 与 Access-Reject 消息。

包含有 EAP-Message 属性的 Access-Request 消息如果没有 Message-Authenticator 属性，应被 RADIUS 服务器丢弃，支持 EAP-Message 的 RADIUS 服务器必须计算 Message-Authenticator 的值，如果与收到的值不一致则把这个消息丢弃。不支持 EAP-Message 的 RADIUS 服务器，如果收到有 EAP-Message 属性的消息，必须返回 Access-Reject 消息。如果 RADIUS 服务器收到的 Access-Request 消息里有不可识别的 EAP-Message 属性，应返回一个 Access-Reject 属性。

Access-Challenge、Access-Accept、Access-Reject 消息如果包含有 EAP-Message 属性却没有 Message-Authenticator 属性，应被 NAS 丢弃。NAS 如果支持 EAP-Message 属性必须计算 Message-Authenticator 的值。如果与收到的值不匹配，应把消息丢弃。

EAP-Message 属性格式如下图所示。



类型：EAP-Message 的类型为 79

长度：≥3

字符串：字符串域里包括了 EAP 的包。如果多个 EAP-Message 属性在一个消息中，它们的应连续放置，这样可以允许长于 253 字节的 EAP 消息以 RADIUS 承载。

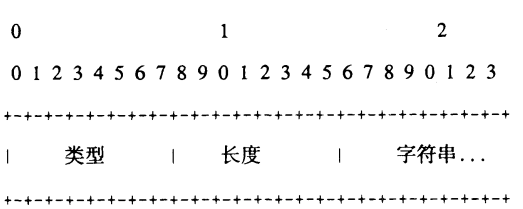
5.1.3.40 Message-Authenticator

该属性可能用于 Access-Request 消息的签名，以防止使用 CHAP，PAP 或 EAP 等认证方式时内容被窜改。它可能用于任一个 Access-Request 消息中。它必须在所有包括了 EAP-Message 的 Access-Request、Access-Accept、Accept-Reject 与 Access-Challenge 消息中。

一个 RADIUS 服务器收到了有 Message-Authenticator 属性的 Access-Request 消息必须计算正确的 Message-Authenticator 的值，如果这个值与发送的不一致，这个消息应被丢弃。

RADIUS 客户端如果收到带有 Message-Authenticator 属性的 Access-Accept、Access-Reject、Access-Challenge 消息后必须计算的 Message-Authenticator 的值，如果与发送的不一致，应把这个消息丢弃。

这个消息的格式如下图所示。



类型：Message-Authenticator 的值为 80

长度：18

字符串：当 Message-Authenticator 出现在一个 Access-Request 消息中，它是整个 Access-Request 消息 HMAC-MD5 的校验值，包括类型、标识、长度与校验码，用共享密钥作为密钥。加密算法如下：

Message-Authenticator = HMAC-MD5 （类型，标识，长度，请求校验码，各属性）。

当计算这个值时，Message-Authenticator 的值当作 16 个字节的 0 进行计算。

对于 Access-Challenge、Access-Accept、Access-Reject 消息，Message-Authenticator 计算如下，使用 Access-Request 中的校验码。

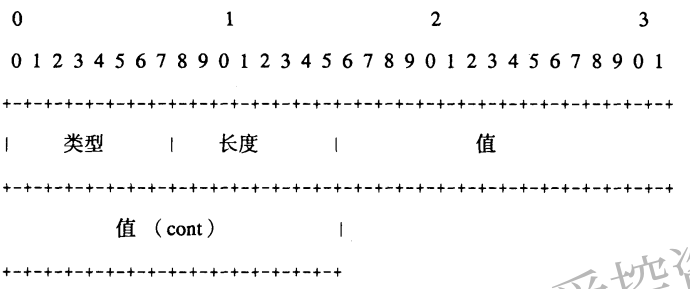
Message-Authenticator = HMAC-MD5 （类型，标识，长度，请求校验码，各属性）。

当计算校验码时，Message-Authenticator 的值当作 16 个字节的 0 进行计算。

当有 User-Password 属性时，这个属性并不需要，不过对于其他类型的认证，该属性可以很好地防止攻击。

5.1.3.41 Acct-Interim-Interval

这个属性表示一个会话中，每个中间更新消息相隔的秒数。这个值只会出现在 Access-Accept 消息中。这个消息的格式如下图所示。



类型：Acct-Interim-Interval 的值为 85。

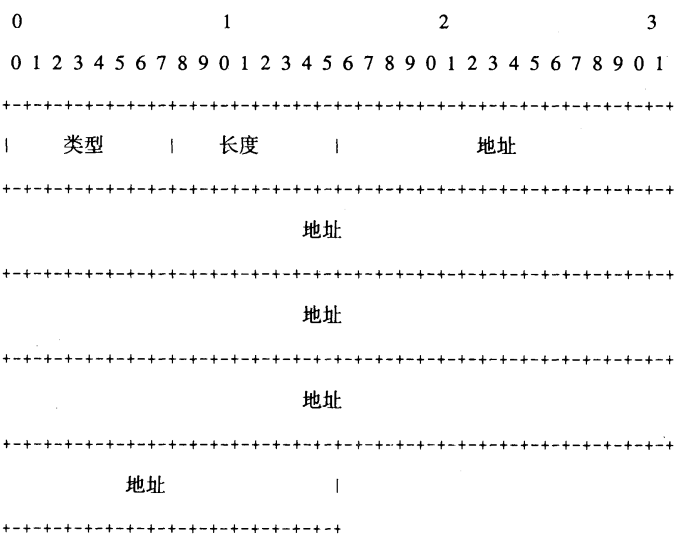
长度：6

值：这个值包含有 NAS 为这个会话发送的每个中间更新间隔的秒数，这个值必须不能小于 60。这个值应小于 600。其对网络流量的影响应仔细考虑。

5.1.3.42 NAS-IPv6-Address

该属性表明发起用户认证的 NAS 的 IPv6 地址，该属性在 RADIUS 服务器的作用泛围内应是惟一的。NAS-IPv6-Address 应只用于 Access-Request 包中。NAS-IPv6-Address 与/或 NAS-IP-Address 应出现于一个 Access-Request 消息中，但是如果两个属性均未出现的话，NAS-Identifier 必须在这个消息中。

NAS-IPv6-Address 属性格式如下图所示。



类型：NAS-IPv6-Address 为 95。

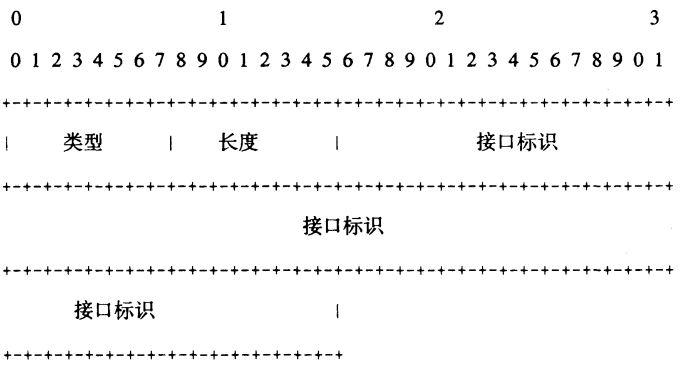
长度：18

地址：地址域是 16 字节

5.1.3.43 Framed-Interface-Id

该属性表示为用户所配置的 IPv6 接口的标识，它可能用于 Access-Accept 消息中。如果 Interface-Identifier IPv6CP 选项成功进行协商，这个属性必须在 Access-Request 消息中，向服务器提示，NAS 更倾向于使用这个值，在服务器端推荐，但不要求接受这个提示。

Framed-Interface-Id 属性格式如下图所示。



类型：Framed-Interface-Id 为 96。

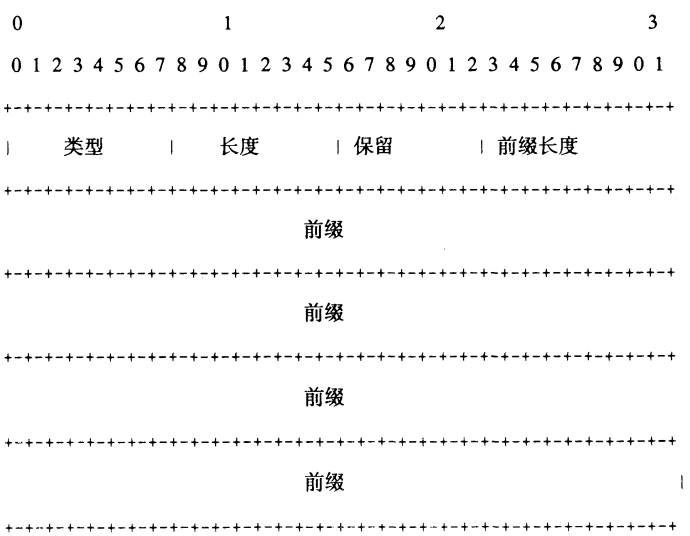
长度 ：10

接口标识：这个值域为 8 个位组。

5.1.3.44 Framed-IPv6-Prefix

该属性表明为用于用户配置的 IPv6 前缀（与相应的路由）。它可能用于 Access-Accept 消息中，并可以多次出现。它也可能用户 Access-Request 消息中，做为对服务器的一种提示，NAS 希望使用这个前缀。但服务器并不要求接受这个提示。服务器会认为 NAS 了解到相应前缀的路由，因此，服务器并不需要对于同一个前缀发送 Framed-IPv6-Route 属性。

Framed-IPv6-Prefix 属性如下图所示。



类型：Framed-IPv6-Prefix 为 97

长度：最少为 4 字节，不能长于 20 字节。

保留：这个值域必须保留，一般设为0。

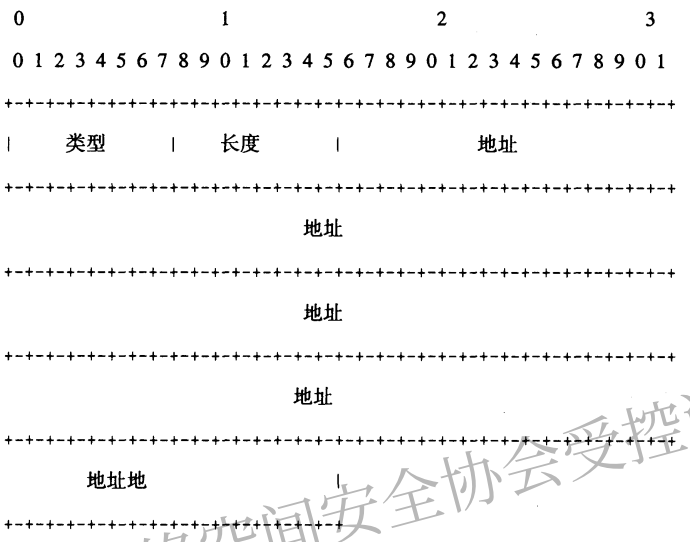
前缀长度：这个前缀长度以比特位表示，最小为0，最大为128。

前缀：前缀域最大为16个8位组长，前缀长度之外的比特位必须为0。

5.1.3.45 Login-IPv6-Host

该属性表明当Login-Service属性存在时，连接用户的系统标识， 它可能用于Access-Accept消息中。它可能用于Access-Request消息中，提示服务器，NAS希望使用这个主机，但服务器并不要求接受这个提示。

Login-IPv6-Host消息的格式如下图所示。



类型：Login-IPv6-Host为98

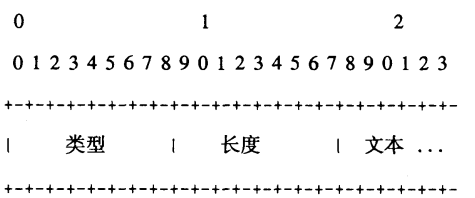
长度：18

地址：地址域为16个8位组。0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF表明NAS不允许用户选择一个地址或设备名进行连接。值0表示NAS选择一个主机连接用户。其他的值表明NAS连接用户的地址。

5.1.3.46 Framed-IPv6-Route

该属性提供了为用户配置的路由信息。它用于Access-Accept消息中可多次出现。

Framed-IPv6-Route属性的格式如下图所示。



类型：Framed-IPv6-Route为99。

长度：≥3

文本：文本域为一个或多个8位组，内容与应用相关，这个值域不能以NUL（十六进制 0x00）结束，它应便于阅读但不能影响协议的操作。

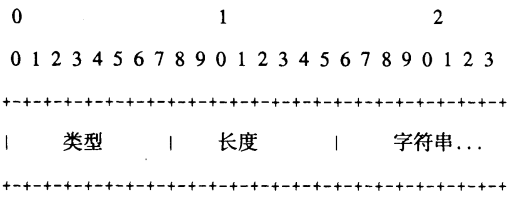
对于IPv6路由，它应包括目标的前缀，后面可跟一个斜线与10进制表示的掩码长度。然后为一空格，一个网关的地址，空格，一个或多个路由的量度（用十进制编码），每个量度用空格分开。比如“2000:0:0:106::/64 2000::106:a00:20ff:fe99:a998 1”。

当网关的地址为未指定的IPv6地址，用户的IPv6地址应当做网关的地址。未指定的地址可表示为“2000:0:0:106::/64 :: 1”。

5.1.3.47 Framed-IPv6-Pool

该属性包含有分配的地址池的名称。地址池用于给用户分配一个IPv6的前缀。如果NAS不支持多个前缀池，应忽略这个属性。

Framed-IPv6-Pool属性的格式如下所示。



类型：Framed-IPv6-Pool为100

长度：≥3

字符串：字符串域包括了分配给NAS的IPv6前缀池的名称。该域不能以NUL（0x00）结束。

5.2 计费消息的格式与属性

5.2.1 计费消息的格式

计费消息的格式同第 5.1.1 节中的“认证消息的格式”。

5.2.2 计费消息类型

RADIUS 数据包类型由数据包中第一个字节的代码字段决定。

5.2.2.1 Accounting-Request

Accounting-Request 数据包负责承载由客户端(一般为网络接入服务器或接入服务器代理)向 RADIUS 计费服务器传送的基于用户业务计费的信息。客户端传送的 Accounting-Request 数据包代码字段设置为 4。

服务器根据记录计费数据包的情况决定是否回复 Accounting-Response 数据包。服务器成功记录计费数据包，向客户端传送 Accounting-Response 数据包，服务器未成功记录计费数据包，不向客户端传送 Accounting-Response 数据包。

除了 User-Password、CHAP-Password、Reply-Message、State 四个属性外，在 RADIUS Access-Request 和 Access-Accept 消息中有效的属性在 Accounting-Request 数据包中同样有效。RADIUS Accounting-Request 数据包中必须包括 NAS-IP-Address 和 NAS-Identifier 属性。如果请求的业务未包括端口号或接入服务器不区分业务端口号，那么可以不包括 NAS-Port 或 NAS-Port-Type 属性。

如果 Accounting-Request 数据包包括 Framed-IP-Address 属性，那么该属性必须包括用户的 IP 地址。如果 Access-Accept 使用具有特殊值的 Framed-IP-Address 属性告知接入服务器为用户分派或协商 IP 地址，那么 Accounting-Request 数据包必须包含已分派或已协商的 IP 地址。

Accounting-Request 数据包格式如第 5.1.1 节中图所示。

代码：使用 4 表示 Accounting-Request 数据包。

标识符：传输，标识符必须保持与以前相一致，不作任何改动。如果 Accounting-Request 数据包中的属性包含 Acct-Delay-Time 属性，那么在对数据包重传时，更新 Acct-Delay-Time 数值，同时改变属性字段的内容，请求新标识符和请求认证符。

请求校验符：Accounting-Request 数据包的请求认证符包括一个根据“请求校验符”中描述的方法计

算出的 16 字节 MD5 杂散值。

属性：属性字段长度可变，包括一个属性列表。

5.2.2.2 Accounting-Response

Accounting-Response 数据包是 RADIUS 计费服务器向客户端发送的确认消息，说明已经接收并且成功记录了 Accounting-Request 消息。如果成功记录 Accounting-Request 数据包，RADIUS 计费服务器必须向客户端发送代码字段为 5 的 Accounting-Response 数据包。客户端接收到 Accounting-Response 数据包，首先将消息中的标识符字段与未处理的 Accounting-Request 数据包进行匹配。响应认证符 Response Authenticator 字段必须包括对未处理的 Accounting-Request 数据包的正确响应。无效数据包会被悄悄丢弃。RADIUS 计费响应消息不要求包含属性。对 Accounting-Request 数据包格式总结如下，字段是按照从左到右的顺序传送的。

代码：使用 5 表示 Accounting-Response 数据包。

标识符：标识符字段复制 Accounting-Request 消息中的标识符字段。

响应校验符：Accounting-Response 的响应认证符包括根据“响应校验符”中描述的方法计算出的一个 16 字节 MD5 杂散值。

属性：属性字段长度可变，包括一系列 0 或多个属性。

5.2.3 属性

请求消息和响应消息使用 RADIUS 属性传递指定的认证、授权、计费详细信息。某些特定的属性可以出现在多个属性描述中。使用 RADIUS 数据包长度指出属性列表的结束处。属性格式总结如下。属性字段按照由左向右的顺序传送。

类型：类型字段长度为一个字节。数值 192~223 为进行实验预留，数值 224~240 为特定实现机制预留，数值 241~255 为今后使用预留，目前不使用。

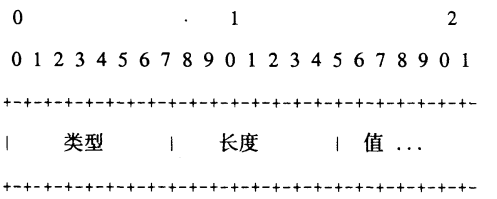
40 Acct-Status-Type
41 Acct-Delay-Time
42 Acct-Input-Octets
43 Acct-Output-Octets
44 Acct-Session-Id
45 Acct-Authentic
46 Acct-Session-Time
47 Acct-Input-Packets
48 Acct-Output-Packets
49 Acct-Terminate-Cause
50 Acct-Multi-Session-Id
51 Acct-Link-Count
52 Acct-Input-Gigawords
53 Acct-Output-Gigawords
55 Event-Timestamp

5.2.3.1 Acct-Status-Type

这个属性用于指示 Accounting-Request 是否对用户业务的起始处和结束处进行标记。

客户端可以使用这个属性标记计费开始 Accounting-on 及计费结束 Accounting-off。

Acct-Status-Type 属性格式如下图所示。按照从左至右的顺序传送这个字段。



类型：使用 40 表示 Acct-Status-Type。

长度：6

数值：数值字段长度为 4 字节。

1 Start

2 Stop

3 Interim-Update

7 Accounting-On

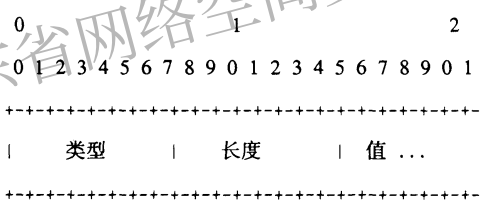
8 Accounting-Off

5.2.3.2 Acct-Delay-Time

这个属性指示出客户端开始尝试发送记录的时间与服务器上出现 Accounting-Request 消息的准确时间的时间差，忽略网络传送时间。

注：Acct-Delay-Time 属性的变更会导致标识符随之改变。

Acct-Delay-Time 属性格式如下图所示。这个字段按照由左至右的顺序传送。



类型：使用 41 表示 Acct-Delay-Time。

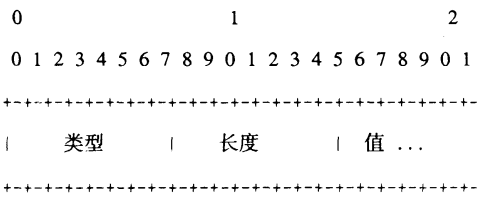
长度：6

数值：数值字段为 4 字节长度。

5.2.3.3 Acct-Input-Octets

这个属性用于记录接收提供业务端口发送的字节数，并且只能出现在将 Acct-Status-Type 设置为 Stop 的 Accounting-Request 数据包记录中。

Acct-Input-Octets 属性格式如下图所示。这个字段按照从左至右的顺序传送。



类型：使用 42 表示 Acct-Input-Octets。

长度：6

数值：数值字段为 4 字节。

5.2.3.4 Acct-Output-Octets

这个属性用于记录传送业务的端口已经发送的字节数，并且只能出现在将 Acct-Status-Type 设置为 Stop 的 Accounting-Request 数据包记录中。

Acct-Output-Octests 属性格式与 5.2.3.3 相同。这个字段按照从左至右的顺序传送。

类型：使用 43 表示 Acct-Output-Octets。

长度：6

数值：数值字段为 4 字节。

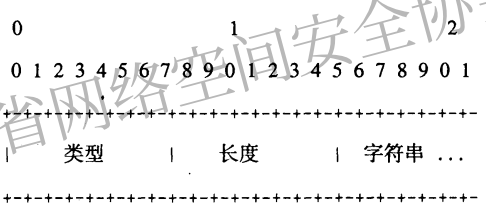
5.2.3.5 Acct-Session-Id

这个属性是一个惟一 Accounting ID，利用这个属性可以在 log 文件中与开始记录和停止记录进行匹配。对于已有会话的开始记录与停止记录必须使用相同的 Acct-Session-Id。Acct-Session-Id 对 Accounting-Request 数据包而言是必选的，对 Access-Request 数据包而言是可选的。在一个会话过程中，如果 Access-Request 数据包选用 Acct-Session-Id，那么在 Accounting-Request 数据包中的网络接入服务器必须使用相同的 Acct-Session-Id。

Acct-Session-Id 应包括使用 UTF-8 编码的 10646 字符。

例如，一种实现机制使用高 8 位为 16 进制数的字符串，每一次重新启动的时候前两位数字递增。在重启动次数达到 2^24-1 次后，下面六位数字从第一位用户登录开始从 0 计数。也可能使用其他类型的编码字符。

Acct-Session-Id 属性格式如下图所示。



类型：使用 44 表示 Acct-Session-Id。

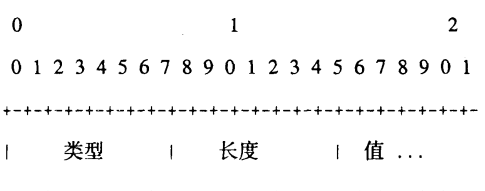
长度：≥3

字符串：字符串字段应为使用 UTF-8 编码的 10646 字符的字符。

5.2.3.6 Acct-Authentic

这个属性可以包括在 Accounting-Request 数据包中，用于指示用户如何通过 RADIUS 协议、接入服务器以及其他远程认证协议的认证。如果向用户传递的业务未经过认证，用户侧不能生成计费记录。

Acct-Authentic 属性格式如下图所示。这个字段按照从左至右的顺序传送。



类型：使用 45 表示 Acct-Authentic。

长度：6

数值：数值字段是 4 字节。

1 RADIUS

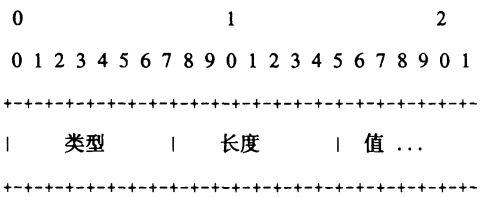
2 Local

3 Remote

5.2.3.7 Acct-Session-Time

这个属性用于指示用户接收业务已经用去的时间，它只能出现在将 Acct-Status-Type 设置为 Stop 的 Accounting-Request 记录中。

Acct-Session-Time 属性格式如下图所示。这个字段按照从左至右的顺序传送。



类型：使用 46 表示 Acct-Session-Time。

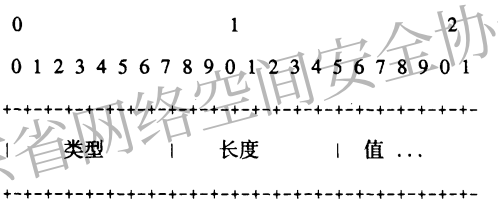
长度：6

数值：数值字段为 4 字节。

5.2.3.8 Acct-Input-Packets

这个属性用于指示从提供业务的端口接收到的数据包数目，这个端口向已经成帧的用户提供业务。该属性仅能出现在 Acct-Status-Type 设置为 Stop 的 Accounting-Request 记录中。

Acct-Input-packets 属性格式如下图所示。这个字段按照从左至右的顺序传送。



类型：使用 47 表示 Acct-Input-Packets。

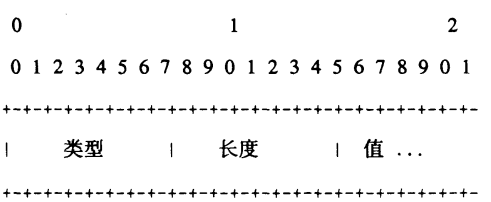
长度：6

数值：数值字段为 4 字节。

5.2.3.9 Acct-Output-Packets

这个属性用于指示向成帧的用户端口发送了多少业务数据包，只能出现在将 Acct-Status-Type 设置为停止的 Accounting-Request 记录中。

Acct-Output-Packets 属性格式如下图所示。这个字段按照从左至右的顺序传送。



类型：使用 48 表示 Acct-Output-Packets。

长度：6

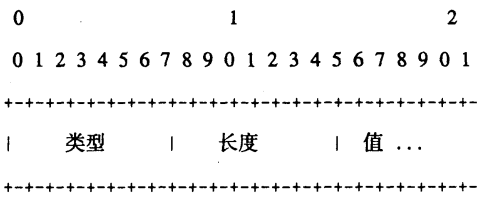
数值：数值字段为 4 字节。

5.2.3.10 Acct-Terminate-Cause

这个属性用于指示会话如何中断，仅能出现在 Acct-Status-Type 设置为 Stop 的 Accounting-Request 记

录中。

Acct-Terminate-Cause 属性格式如下所示。字段按从左至右的顺序传送。



类型：使用 49 表示 Acct-Terminate-Cause。

长度：6

数值：数值字段为 4 字节，包括一个规定了会话中断原因的整型。

1 用户请求：用户请求业务中断，例如：LCP 中断或用户登出。

2 丢失承载：端口丢弃 DCD。

3 丢失业务：不能再提供业务。例如：用户到主机的连接被中断。

4 空闲超时：空闲定时器超时。

5 会话超时：最大会话长度定时器超时。

6 管理复位：管理员复位端口或会话。

7 管理重启：管理员结束接入服务器相关业务，例如重启接入服务器。

8 端口错误：接入服务器检测到要求结束会话的端口出现一个错误。

9 接入服务器错误：接入服务器检测到要求结束会话的端口出现几个错误。

10 接入服务器请求：接入服务器为非错误原因结束会话。

11 接入服务器重启：接入服务器为非管理原因重启结束会话。

12 不需要的端口：资源到达低线以下时，接入服务器结束当前会话。

13 优先选择的端口：为了将端口分配给更高优先权用户使用，接入服务器结束当前会话。

14 暂停的端口：接入服务器为暂缓虚拟会话结束当前会话。

15 业务不可达：接入服务器不能提供被请求的业务。

16 回呼：接入服务器中断当前会话，完成新会话的回呼。

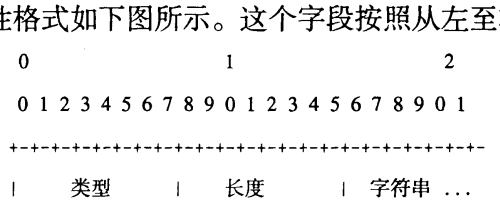
17 用户错误：用户输入错误，导致会话中断。

18 主机请求：登陆主机正常中断会话。

5.2.3.11 Acct-Multi-Session-Id

这个属性是一个惟一的计费 ID，可以使 log 文件中的多条相关会话链接在一起。链接到一起的每一个会话都会得到一个惟一的 Acct-Session-Id，但是它们的 Acct-Multi-Session-Id 都相同。强烈建议 Acct-Multi-Session-Id 包括 UTF-8 编码的 10646 字符。

Acct-Session-Id 属性格式如下图所示。这个字段按照从左至右的顺序传送。



类型：使用 50 表示 Acct-Multi-Session-Id。

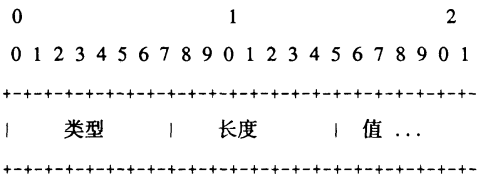
长度：≥3。

字符串：字符串字段应该包括使用 UTF-8 编码的 10646 字符。

5.2.3.12 Acct-Link-Count

这个属性用于给出生成计费记录时给定的多链路会话中的链路数。接入服务器可以在可能包括多链路的任何 Accounting-Request 数据包中包括 Acct-Link-Count 属性。

Acct-Link-Count 属性格式如下图所示。这个字段按照从左至右的顺序传送。



类型：使用 51 表示 Acct-Link-Count。

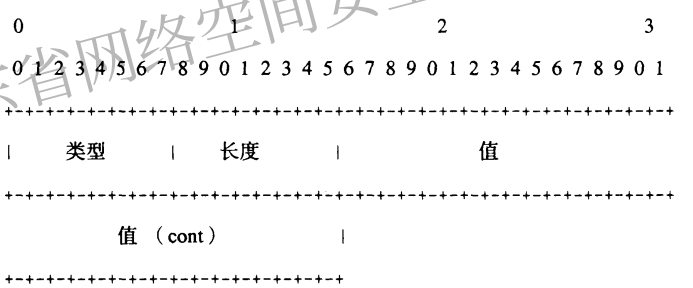
长度：6

数值：数值字段为 4 字节，包括多链路会话中的链路数。

数值可以告知计费服务器何时记录下所有给定多链路会话的记录。当接收到的 Acct-Status-Type 值为 Stop 的 Accounting-Request 数目和相同的 Acct-Multi-Session-Id 和惟一的 Acct-Session-Id 等于 Accounting-Request 中 Acct-Link-Count 的最大值，接收到对多链路会话的停止 Accounting-Request。

5.2.3.13 Acct-Input-Gigaword

这个属性表示 Acct-Input-Octets 从服务开始，完成了多少次以 2^32 为模的循环计数，只能出现在 Acct-Status-Type 属性为 Stop 或 Interim-Update 的 Accounting-Request 消息中。格式如下图所示。



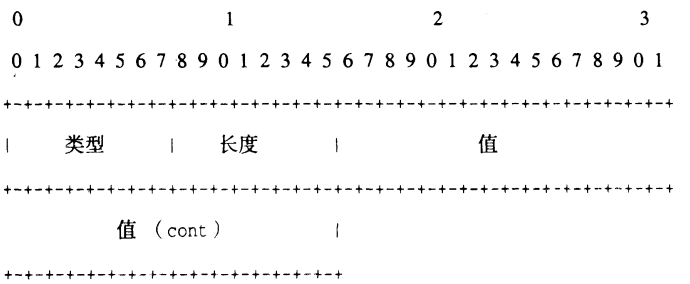
类型：Acct-Input-Gigawords 的值为 52

长度：6

值：值域为 4 个字节。

5.2.3.14 Acct-Output-Gigawords

这个属性表示 Acct-Output-Octets 从服务开始，完成了多少次 2^32 为模的循环计数，只能出现在 Acct-Status-Type 属性为 Stop 或 Interim-Update 的 Accounting-Request 消息中。格式如下图所示。



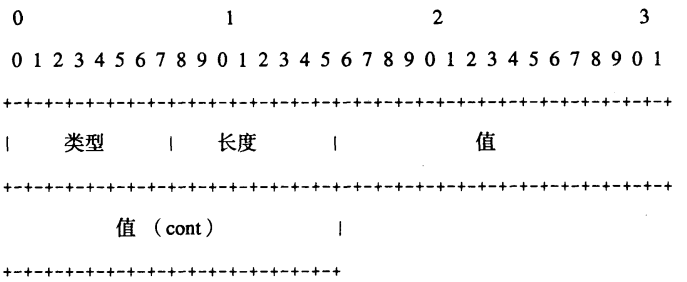
类型：Acct-Output-Gigawords 的值为 53。

长度：6

值：值域为4个字节。

5.2.3.15 Event-Timestamp

这个属性包含在Accounting-Request消息中，来记录事件在NAS上发生的时间。从1970年00:00 UTC起始，以秒计。其格式如下图所示。



类型：Event-Timestamp的类型为55。

长度：6

值：值为4个字节，无符号类型，从1970年00:00 UTC起始，以秒计

6 RADIUS认证、计费过程

6.1 用户的认证

用户认证可分为本地用户认证和异地用户认证，认证过程如图4所示。

（1）用户启动认证首先要向接入服务器传送个人标识，及确认个人标识真实的相关信息，个人标识也可由用户设备自动发送。

（2）接入服务器收到用户标识后向认证服务器发送用户标识，与其他相关信息后，把这些信息构成一个RADIUS的请求消息向本地接入服务器发送。

（3）接入服务器收到相关用户信息后，首先判断用户是否为本地用户，如果用户为本地用户则根据用户提供的信息判断用户是否合法；如果用户非本地用户，则把用户的相关信息转发到用户开户地所在认证服务器上进行认证。

（4）根据本地或远程认识服务器返回的判断结果，认证服务器向合法用户授权，允许接入，拒绝非法的用户请求。

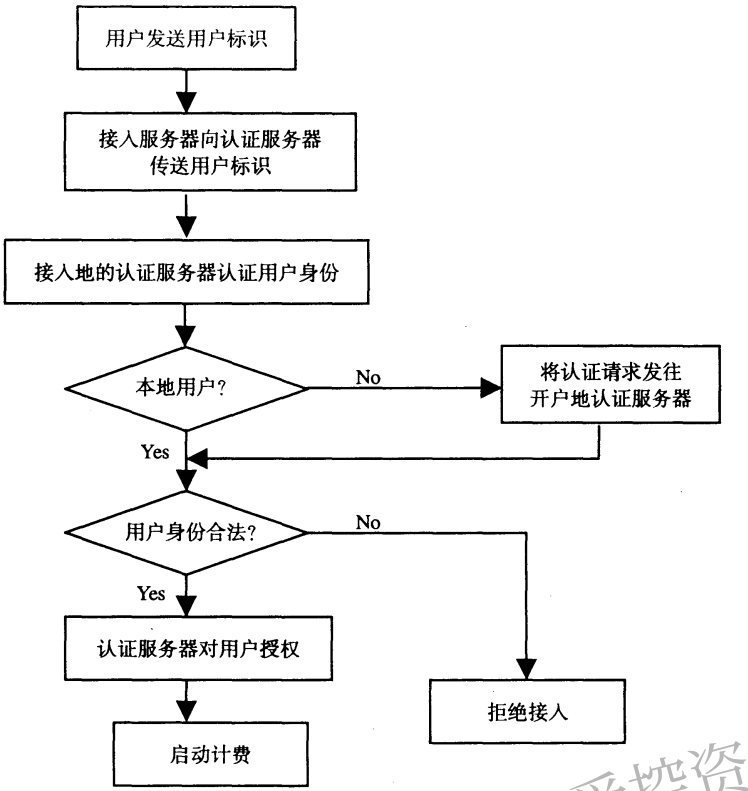


图 4　用户认证流程

6.2　计费过程

RADIUS 协议启动计费过程与结束计费过程如图 5 和图 6 所示。

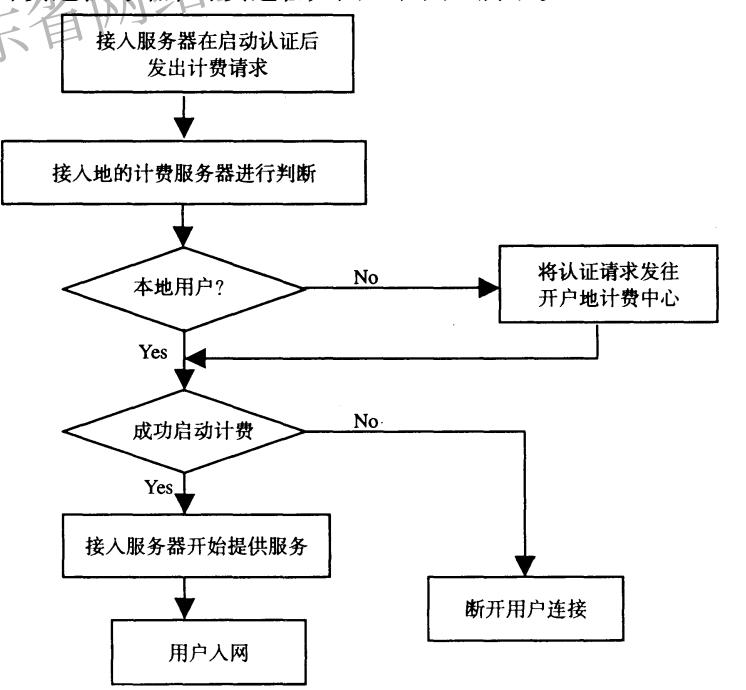


图 5　启动用户计费流程

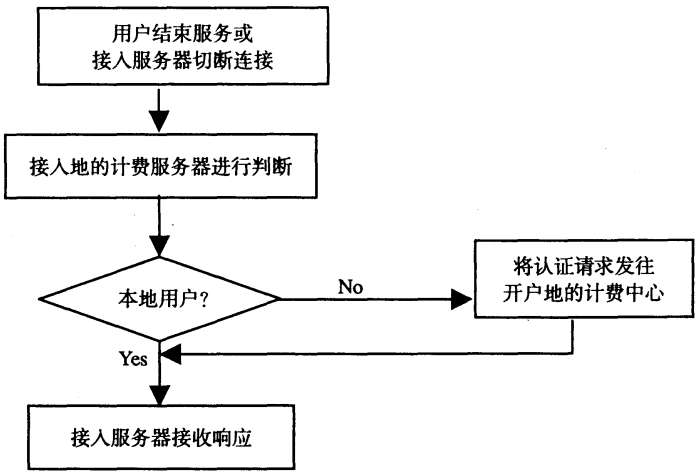


图 6　结束用户计费流程

启动计费过程：

（1）接入服务器在完成用户认证向计费服务器发送一个 RADIUS 计费请求，启动计费。

（2）计费服务器对被计费的对象进行鉴别，如果是本地用户就在本地计费服务器上进行计费，如果不是则判断用户开户地所在的计费服务器，把用户的计费请求转发到相应的计费服务器上。

（3）计费服务器向用户发送计费响应，或转发远程计费服务器的响应。如果用户的计费进程成功启动，接入服务器允许用户接入，否则断开用户的连接。

结束计费过程：

（1）用户主动结束服务或接入服务器检测到任何异常断开用户连接均会触发接入服务器向计费服务器发送计费请求，结束用户计费。

（2）计费服务器对被计费的对象进行鉴别，如果是本地用户就在本地计费服务器上进行计费，如果不是则判断用户开户地所在的计费服务器，把用户的计费请求转发到相应的计费服务器上。

（3）计费服务器向用户发送计费响应，或转发远程计费服务器的响应。

6.3　接入服务器与 RADIUS 服务器间的信息流程

6.3.1　接入服务器与 RADIUS 服务器间认证时的信息流程

接入服务器与 Radius 服务器间认证时的信息流程如图 7 所示。

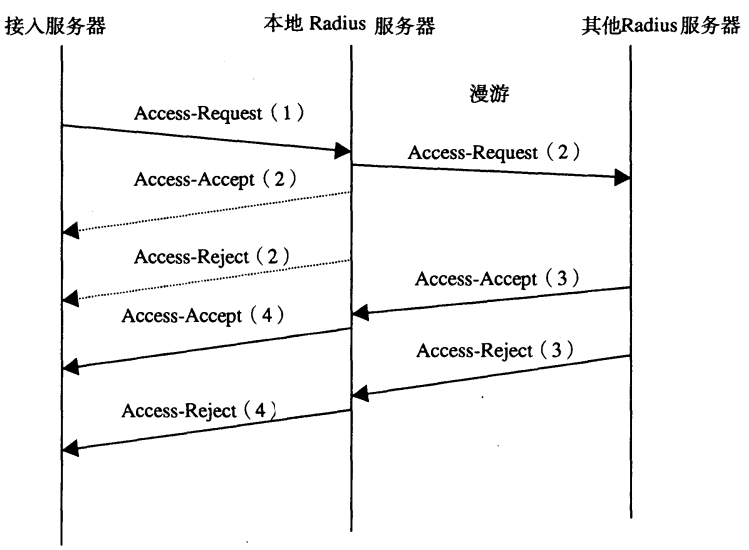


图 7　NAS 与 Radius 服务器间用户认证的信息流程

（1）接入服务器用“接入请求”（Access-Request）消息将用户主叫号码，用户名和密码送到Radius服务器，如果是卡号用户，将用户卡号，密码等发送到Radius服务器。

（2）本地认证中心进行用户认证，如通过，向接入服务器回送“接入认可”（Access-Accept）消息；否则，回送“接入拒绝”（Access-Reject）消息。对于漫游用户，在本地Radius服务器无法进行接入认证的时候，还需要向开户地的Radius服务器发出“接入请求”（Access-Request）请求进行漫游认证。

（3）开户地认证中心进行用户认证，如通过，向用户接入地认证中心回送“接入认可”（Access-Accept）消息；否则，回送“接入拒绝”（Access-Reject）消息。

（4）接入服务器收到本地Radius服务器转发用户开户地认证中心的“接入认可”或“接入拒绝”消息后，允许用户接入或拒绝用户接入。

6.3.2 接入服务器与 RADIUS 服务器间传递 EAP 信息的流程

接入服务器使用 EAP 时，用户可使用 PPP 接入也可通过 802.1x 启动 EAP 的对话。在使用 EAP 时，NAS 与 RADIUS 服务器的流程如图 8 所示。该流程中使用的认证方式为 OTP。

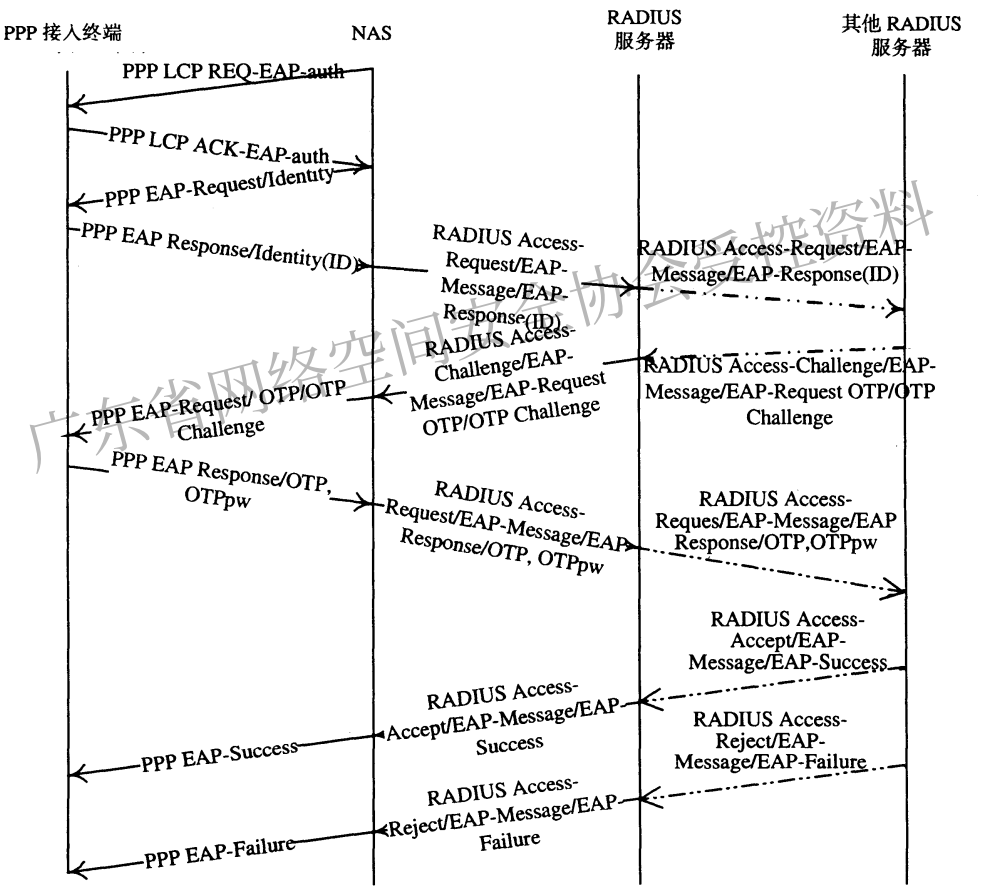


图 8　NAS 与 RADIUS 服务器间传递 EAP 信息的流程(PPP)

首先由 NAS 发起 EAP 的认证过程，并向终端用户发送 EAP-Request 请求用户的标识，用户返回标识后，NAS 把用户的标识用 EAP-Message 属性封装向 RADIUS 服务器发送 Access-Request 消息，如果这个用户是漫游的用户，RADIUS 服务器则转发给用户归属的服务器。如果 RADIUS 服务器要求使用 OTP 方式进行认证，则用 EAP-Message 封装 EAP-Request/OTP/OTP Challenge 消息请求用户进行认证。NAS 向用户发送 PPP EAP Request/OTP/OTP Challenge 消息，如果用户支持 OTP 认证方式，则返回 PPP EAP Response/OTP，OPTpw 作为应答。NAS 用 EAP-Message 把用户的 EAP 消息进行封装，构成 Access-Request 消息发送给 RADIUS 服务器，如果用户是漫游的用户，RADIUS 服务器则把消息转发给

相应的 RADIUS 服务器，否则根据认证的结果，用 EAP-Message 封装 EAP-Success 或 EAP-Failure 消息，通过 Access-Accept 或 Access-Reject 消息返回给 NAS，NAS 根据 RADIUS 服务器的结果允许或拒绝用户接入。

如果 NAS 采用 IEEE 802.1x 方式接入，流程如图 9 所示。

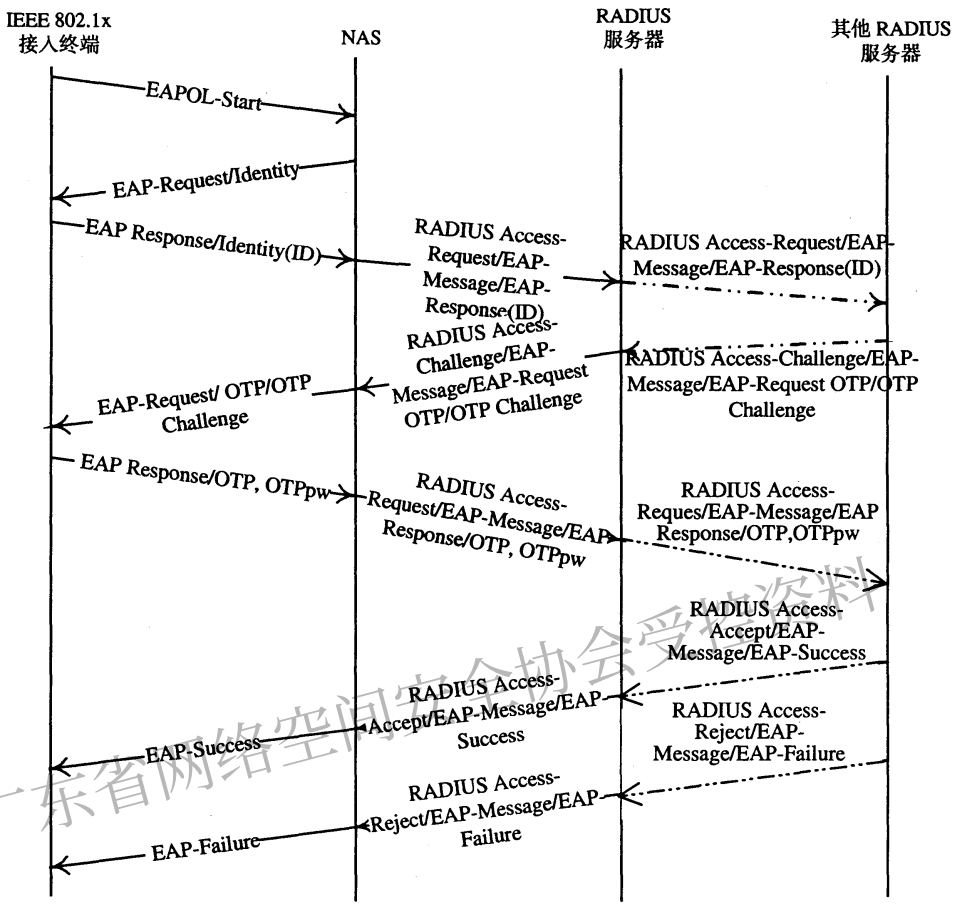


图 9　NAS 与 RADIUS 服务器间的流程（EAPOL）

IEEE 802.1x 的流程与 PPP EAP 的流程基本一致，但是 802.1x 使用的是 EAPOL（EAP over LAN）进行认证消息的传递，故不需要 PPP 的协商，终端可发出 EAPOL-start 消息请求开始 EAP 的认证过程。

6.3.3　接入服务器与 Radius 服务器间启动与结束计费信息的流程

接入服务器与 Radius 服务器间的启动与结束计费信息的流程如图 10 所示。

启动计费时：

（1）启动计费时，接入服务器用“计费请求”（Accounting-Request）消息将计费信息发向本地Radius计费中心。

（2）本地计费中心检测被计费的用户，如果是本地用户，本地计费中心向其发送“计费响应”（Accounting-Response）消息表示成功启动计费，如果是漫游用户则向漫游用户的开户地计费中心发送“计费请求”（Accounting-Request）消息。

（3）用户开户地的计费中心收到用户接入地的请求消息后，向用户接入地的计费服务器发送“计费响应”（Accounting-Response）消息表示成功启动用户计费。

（4）用户接入地的计费服务器收到用户开户地的响应后转发给接入服务器。

（5）如果Radius服务器在规定时间内没有应答，接入服务器认为计费没有成功，则切断用户接入。

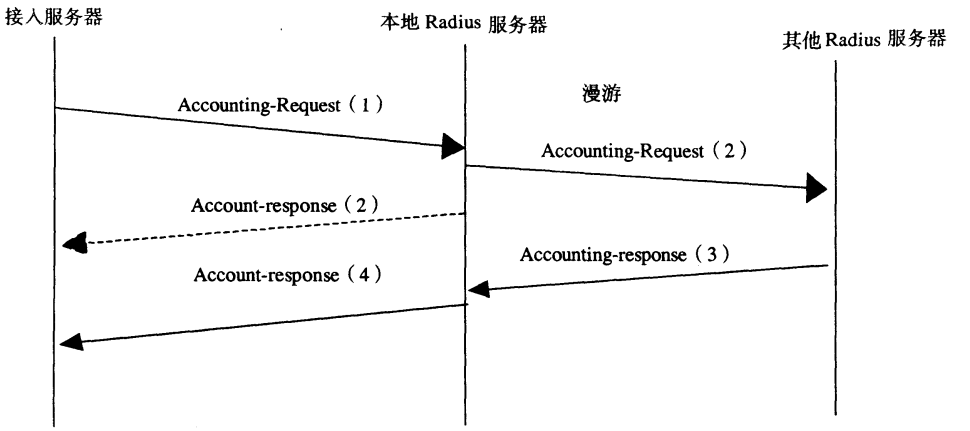


图 10　接入服务器与 Radius 服务器间启动与结束计费信息的流程

在结束计费时：

（1）用户断线或接入服务器切断连接时，接入服务器用“计费请求”（Accounting-Request）消息将计费信息发向本地Radius计费中心。

（2）本地计费中心检测被计费的用户，如果是本地用户，本地计费中心向其发送“计费响应”（Accounting-Response）消息表示成功结束用户计费，如果是漫游用户则向漫游用户的开户地计费中心发送“计费请求”（Accounting-Request）消息。

（3）用户开户地的计费中心收到用户接入地的请求消息后，向用户接入地的计费服务器发送“计费响应”（Accounting-Response）消息表示成功结束用户计费。

（4）用户接入地的计费服务器收到用户开户地的响应后转发给接入服务器。接入服务器根据实际情况判断是否进行进一步处理。

7　RADIUS 的安全机制

RADIUS客户端与服务器端传送消息时，消息通过二者间的共享密钥与MD5算法来确定通信双方的身份。此共享密钥应定期进行维护。

如果RADIUS客户端与服务器间传送的消息非常敏感时还应考虑采用进一步的手段对消息进行鉴别与加密。

7.1　对等端间密钥的管理

RADIUS实体间的共享密钥应定期进行维护与更换。在更换共享密钥时，可先在两实体间同时进行人工的设置，也可通过系统进行密钥的自动更换，但进行自动更新时，必须使用可靠的方式（如数字证书）保证密钥交换时的密钥不会外泄，并确认双方的身份。

当使用证书的更换共享密钥时，需要配置信任的根证书授权机构（CA）。在更新加密密钥时，RADIUS实体用CA颁布的证书来进行认证，并用经CA确认的公钥对共享密钥进行加密并进行传送。CA与证书的使用见YD/T 1614-2007《公众IP网络安全要求——基于数字证书的访问控制》。

7.2　IPsec 的使用

在使用非空密码和认证算法以提供数据包的认证、完整性保护和机密性的传输方式中，RADIUS服务器与客户间，RADIUS服务器与服务器间可以通过IPSec ESP对传送的RADIUS消息报文进行加密。

IPsec使用应符合YD/T 1466-2006《IP安全协议（IPSec）技术要求》中的规定。

中 华 人 民 共 和 国

通 信 行 业 标 准

公众 IP 网络安全要求

——基于远端接入用户验证服务协议（RADIUS）的访问控制

YD/T 1615-2007

*

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

北京新瑞铭印刷有限公司

*

开本：880 × 1230　1/16　　2007 年 6 月第 1 版

印张：3.5　　2007 年 6 月北京第 1 次印刷

字数：102 千字

ISBN 978 - 7 - 115 - 1409/07 - 72

定价：25 元

本书如有印装质量问题，请与本社联系　电话：(010)67114922