远程认证拨号用户服务（RADIUS）

Remote Authentication Dial In User Service，远程用户拨号认证系统

[ri'məut]adj.远程的

Authentication:身份验证

备忘录状态

本文档描述了一种 Internet 社区的 Internet 标准跟踪协议，它需要进一步进行讨论和建议以得到改进。请参考最新版的“Internet 正式协议标准”(STD1)来获得本协议的标准化程度和状态。本备忘录可以不受限制地传播。

IESG 说明

本协议已经被广泛实现和使用，经验表明当本协议在一个大范围的系统中使用会降低性能和丢失数据。部分原因是协议中没有提供拥塞控制的机制。读者可以发现阅读本文对跟踪 IETF 组织的 AAA 工作组的工作进程有很大的帮助，AAA 工作组可能会开发一个能够更好的解决扩展性和拥塞控制问题的成功的协议。

摘要

本文描述了一个**传输认证、授权和配置信息的协议**。这些信息在**想要认证链路**的**网络接入服务器**（Network Access Server）和共享的**认证服务器务器**之间传递。

实现说明

本备忘录记录了 RADIUS 协议，RADIUS 协议的早期版本使用的 **UDP 端口**是 1645，由于和"datametrics"服务冲突，官方为 RADIUS 协议分配了一个**新的端口号 1812**。

目录

1. 简介

本文档废弃了 RFC 2138 [1]。它与 RFC 2138 之间的差别可以在附录"更新记录"中找到。

要经营为众多的用户提供的串口线路和 modem 池，这会带来巨大的管理支持方面的需求。由于 modem 池是通向外部的链路，因此它对安全、认证、计费都提出了很高的要求。可以通过维护一个用户数据库来实现该需求，该数据库包含了认证（验证用户的名字和密码）以及为用户提供的服务类型的详细的配置信息（如 SLIP、PPP、telnet 和 rlogin 等）。

RADIUS 协议的主要特性如下：

客户/服务器模式

网络接入服务器(NAS)是 RADIUS 的客户端。客户端负责将用户信息传递给指定的 RADIUS 服务器，然后处理 RADIUS 服务器的回应。

RADIUS 服务器负责接收用户的连接请求，认证该用户，然后给客户端返回能够给用户提供服务的所有必要的配置信息。

RADIUS 服务器可以作为其它 RADIUS 服务器或者其他类型的认证服务器的代理客户端。

网络安全

客户端与 RADIUS 服务器之间的交互是通过**共享密钥来进行相互认证的**，共享密钥不会通过网络传送。另外，为了减少在不安全的网络中侦听到用户密码的可能性，在客户端和 RADIUS 服务器之间传送的密码都是加密的。

弹性的认证机制

RADIUS 服务器能够支持多种认证用户的方式，如果用户提供了用户名和用户　密码的明文，RADIUS 协议能够支持 PPP **PAP** 或者 **CHAP**、**UNIX login** 以及其它的认证方式。

协议扩充性

所有的交互报文由多个不同长度的 Attribute-Length-Value 三元组组成，新属性值的加入不会破坏到协议的原有实现。

1.1. 描述文档的约定

本文中的关键词"MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", 以及"OPTIONAL"的参见 BCP 14 [2]中的描述。这些关键词意义与其是否大写无关。

如果一种实现没有满足本协议中的一个或者多个 MUST 或者 MUST NOT 要求，**那么该实现和本协议是不兼容的**；如果一个实现满足了本协议中所有的 MUST、MUST NOT、SHOULD 和 SHOULD NOT 要求，那么该实现和本协议是**无条件兼容**；如果该实现满足本协议所有的 MUST 和 MUST NOT 要求，但没有满足所有的 SHOULD 和 SHOULD NOT 要求，那么该实现和本协议是有条件兼容。

不支持某个特定服务的 NAS 一定不要（MUST NOT）支持该服务的 RADIUS 属性，例如：不能提供 ARAP 服务的 NAS 一定不要（MUST NOT）支持 ARAP 服务的 RADIUS 属性，**对于授权不支持的服务的接入成功回应报文，NAS 必须将之做为接入拒绝回应报文一样处理。**

1.2. 术语

本文使用了以下的术语：

服务　　NAS 为拨入用户提供的某种服务，如：PPP 或者 Telnet。

会话　　NAS 为拨入用户提供的每一个服务都会建立一个会话。第一次开始提供服务做为会话的开始，服务终止做为会话的结束。如果 NAS 支持的话，一个用户可以有多个并行或者串行的会话。

静默丢弃

应用程序不对包进行任何处理就**直接丢弃**。应用程序**应该（SHOULD）**有提供记录错误的能力，其中包括被静默丢弃的包的内容，而且应用程序应该（SHOULD）在一个统计计数器中记录下该事件。

2. 操作

当一个客户端被配置成采用 RADIUS 协议时，客户端的任何用户提交认证信息给客户端。当用户想输入他们的用户名和密码时，客户端可以给出定制化的登陆提示信息。或者，用户可以使用一种如 PPP 协议的链路协议，这些协议有能够携带这些信息的认证报文。

一旦客户端获得这些信息，可能会选择使用 RADIUS 协议进行认证，为了这样做，客户端生成一个包含用户名，用户密码，客户端的 ID 号，以及用户接入的端口号 ID 属性的接入请求报文。当提供用户密码时，用户密码都被用 MD5 算法隐藏起来。

通过网络将接入请求报文提交给 RADIUS 服务器，**如果在一定长的时间内没有回应，请求报文将被重复发送几次**。如果主服务器一旦宕机(即：死机)或者不可达，客户端也可将请求报文转发给备用的一个或者多个服务器。在多次重试都发现主服务器失败，备用服务器可以被启用，当然也可以使用循环（round-robin）的方式。

重试和放弃算法是目前正在研究的一个课题，在本文中就不再赘述了。

一旦 RADIUS 服务器接收到请求报文，服务器将验证发送请求报文的客户端的有效性，一个在 RADIUS 服务器中没有共享密钥的客户端请求必须（MUST）被**静默丢弃**。如果客户端是有效的，RADIUS 从用户数据库中查找是否有和请求匹配的用户。数据库中的用户记录中包含了一系列必须满足的允许接入用户的要求。这些要求始终包含密码，但也可能包含用户允许被接入的特定客户端和端口号。

RADIUS 服务器为了满足请求也**可以（MAY）**向其他服务器发起请求。在这种情况
下，它是做为客户端的。

如果有任何 Proxy-State 属性在接入请求报文中出现，这些属性必须（MUST）原封不动地按顺序拷贝到回应报文中。其它属性可以被置于 Proxy-State 属性的前面，后面，甚至中间。

如果任一条件没有被满足，RADIUS 服务器将发送接入拒绝回应报文以表明用户的请求是无效的。如果需要的话，服务器可以（MAY）在接入拒绝回应报文中包含一个文本信息，这个信息可以（MAY）被客户端显示给用户。除了 Proxy-State 属性外，其它属性不能出现在接入拒绝回应报文中。

如果所有的条件都被满足，而 **RADIUS 服务器想要发送一个用户必须（must）回应的挑战，RADIUS 服务器将发送一个**接入挑战报文，该报文可以（MAY）包含一条客户端显示给用户的文本信息，这个信息提示用户对挑战做出回应。该报文也可以（MAY）包含一个 State 属性。

如果客户端接收到一个接入挑战报文，并且支持挑战/回应认证方式，如果有的话，客户端可以给用户提示文本信息，提示用户回应。然后客户端使用新的请求 ID 重新提交最初的接入请求报文，并且携带上被回应替换的 User-Password 属性（被加密的），并且包含从接入挑战报文中获得的 State 属性，如果有的话，State 属性在请求报文中只应该（SHOULD）**出现零次或者 1 次。**对于新的接入请求报文，服务器可能回应接入成功回应报文，接入拒绝回应报文或者接入挑战报文。

如果所有的条件都满足，一系列的用户配置信息将被放入到接入成功回应报文中，这些值包含了服务类型（如：SLIP，PPP 或者 Login User）和提供服务所有必需的值。对于 SLIP 和 PPP 服务来说，可能包含 IP 地址，子网掩码，MTU，想要的压缩算法，想要的报文过滤标识符。对于字符模式的用户，可能包含想要的协议和主机。

2.1. 挑战/回应

在挑战/回应认证方式下，给用户下发一个不可预测的数字，挑战用户加密该数字，然后传回结果，能够被认证的用户往往配备了特别的设备，如能够很容易计算出正确回应的智能卡或软件。不能被认证的用户，往往缺乏合适的设备或者软件，并且也缺少必要的密钥而不能仿造出设备或者软件，而只能靠猜测来回应。

接入挑战报文通常携带有一个需要显示给用户的挑战字符串，该挑战字符串包含在 Reply-Message 属性中，如一个永远不可能重复的数字。通常，该数字是从外部服务器获得，这个服务器知道认证用户的认证类型，因此可以根据合适的基数和长度选择一个随机或者不可重复伪随机数。

然后用户将这个挑战字输入到能够计算出回应的设备（或者软件）中，然后将计算出的回应传到客户端中，客户端将之通过第二个接入请求报文转发给 RADIUS 服务器，如果该回应和服务器想要的回应相匹配，RADIUS 服务器就返回一个接入成功回应报文，否则，就返回一个接入拒绝回应报文。

例如：NAS 给 RADIUS 服务器发送了一个携带 NAS-Identifier，NAS-Port，User-Name 和 User-Password（可能只是一个固定字符串"challenge"或者不携）属性的**接入请求报文**，服务器回应一个携带 State 和 Reply-Message 属性的**接入挑战报文**，Reply-Message 属性包含字符串"Challenge 12345678, enter your response at the prompt"，这个字符串由 NAS 上显示，NAS 接收到回应，向服务器发送一个新的携带 NAS-Identifier，NAS-Port，User-Name，User-Password（正是用户输入的用户密码，已经被加密）以及被接入挑战报文带来的 State 属性的接入请求报文，服务器判断回应是否和想要的回应相匹配，然后返回接入成功回应报文或者接入拒绝回应报文。或者甚至再发送一个接入挑战报文。

2.2. 使用 PAP 和 CHAP 互操作

对于 **PAP 认证方式**，NAS 获得 PAP ID 和密码，然后将它们做为接入请求报文中的 User-Name 和 User-Password 属性发送出去。NAS 可以（MAY）包含值为 Framed-User 的 Service-Type 属性和值为 PPP 的 Framed-Protocol 属性，以提示 RADIUS 服务器用户需要 PPP 服务。

对于 CHAP 认证方式，NAS 生成一个随机挑战字（16 个字节比较合适）并发送给用户，用户回应一个携带 CHAP ID 和 CHAP 用户名的 CHAP 回应。NAS 然后向 RADIUS 服务器发送一个接入请求报文，该请求报文将 **CHAP 用户名做为 User-Name 属性，CHAP ID 和 CHAP 回应做为 CHAP-Password 属性。随机挑战字可以包含在 CHAP-Challenge 属性中，或者如果是 16 个字节长度的话，它可以放在接入请求报文的 Request Authenticator 域中**。NAS 可以（MAY）包含值为 Framed-User 的 Service-Type 属性和值为 PPP 的 Framed-Protocol 属性，以提示 RADIUS 服务器用户需要 PPP 服务。

RADIUS 根据 User-Name 属性查找到用户密码，对 CHAP ID 字节，密码和 CHAP 挑战字（如果 CHAP-Challenge 属性存在，从该属性取值，否则从 Request Authenticator 域取值）进行 MD5 加密获得挑战字，然后将加密结果和 CHAP-Password 属性比较，如果匹配，服务器发送回接入成功回应报文，否则发送回接入拒绝回应报文。

如果 RADIUS 服务器不能完成请求的认证过程，必须（MUST）返回接入拒绝回应报文，例如：CHAP 认证方式需要用户的密码在服务端是可以明文存放的，因为它需要加密 CHAP 挑战字然后同 CHAP 回应比较，如果在服务端不能获取明文的用户密码，服务器必须（MUST）给客户端发送接入拒绝回应报文。

2.3. 代理

在代理 RADIUS 下，一个 RADIUS 服务器从 RADIUS 客户端（如 NAS）接到一个认证（或计费）请求时，将该请求转发给远程 RADIUS 服务器，接收到远程服务器的回应以后，然后将该回应发送回客户端。代理机制反映了本地管理策略的变化。代理 RADIUS 的常用的用途是漫游，漫游允许两个或者更多的管理实体允许彼此的用户在另一个实体网络中拨号登陆。

NAS 向"转发服务器"发送 RADIUS 接入请求报文，该服务器将报文转发到"远程服务器"，远程服务器发送回应报文（接入成功回应报文，接入拒绝回应报文或者接入挑战报文）给转发服务器，转发服务再将报文发送回 NAS。为方便 RADIUS 代理操作，User-Name 属性可以（MAY）包含一个网络接入标识[8]。哪个远程服务器将接收到转发的报文应该（SHOULD）取决于认证"域"的选择，认证域可以（MAY）是网络接入标识（一个命名的域）的一个部分。做为另一选择，哪个服务器将接收到转发的报文也可以（MAY）取决于转发服务器的配置，例如 Called-Station-Id 属性（一个数字化的域）。

一个 RADIUS 服务器既可以做转发服务器，也可以做远程服务器，对于其中一些域，它做为转发服务器，对另外一些域，它做为远程服务器。一个转发服务器可以做为任意个数的远程服务器的转发器，一个远程服务器可以有任意个数的转发服务器给它转发报文，也可以为任意个数的域提供认证。一个转发服务器可以将报文转发给另一个转发服务器，形成一个代理链，但是需要小心避免形成循环转发。

下面场景阐述了 NAS、转发服务器以及远程服务器之间的代理通讯机制：

1. NAS 发送接入请求报文给转发服务器。

2.转发服务器将接入请求报文转发给远程服务器。

3.远程服务器回应接入成功回应报文，接入拒绝回应报文或者接入挑战报文给转发服务器，例如，回应接入成功回应报文。

4.转发服务器将接入成功回应报文发送回 NAS。

转发服务器必须（MUST）将已经在报文中的 Proxy-State 属性做不透明处理（不需要理解它们）。它的操作必须不能（MUST NOT）依赖于由前一个服务器增加的 Proxy-State 属性的内容。

如果从客户端接收到的请求报文中有任何 Proxy-State 属性，转发服务器在回应给客户端时必须（MUST）包含这些 Proxy-State 属性，当转发接入请求报文时，转发服务器可以（MAY）在请求报文中包含 Proxy-State 属性，或者也可以（MAY）在转发请求报文时删除它们，如果转发服务器在转发接入请求报文时删除了 Proxy-State 属性，那么在回应给客户端之前必须（MUST）重新携带这些 Proxy-State 属性。

现在我们阐述以下每一步骤的细节：

1. NAS 发送接入请求报文给转发服务器，如果存在 User-Password 属性的话，转发服务器使用已经知道的该 NAS 的共享密钥解密它，如果报文中有 CHAP-Password 属性但没有 CHAP-Challenge 属性，转发服务器必须（MUST）不能修改 Request Authenticator 域，或者将之拷贝到 CHAP-Challenge 属性中。

'' 转发服务器可以（MAY）增加一个 Proxy-State 属性到报文中（一定不能（MUST NOT）超过一个），如果要增加 Proxy-State 属性，增加的 Proxy-State 属性必须（MUST）出现所有其它 Proxy-State 属性的最后面。转发服务器一定不能（MUST NOT）改动任何已经存在于报文中的 Proxy-State 属性（可以（may）选择不转发它们，但一定不能（MUST NOT）修改它们的内容）。转发服务器一定不要（MUST NOT）改动任何相同类型的属性顺序，包括 Proxy-State 属性。

2. 如果 User-Password 属性存在的话，转发服务器需要使用远程服务器的共享密钥加密 User-Password 属性，如果必要的话，重新设置 Identifier 域，然后将接入请求报文转发到远程服务器。

3. 远程服务器（如果是最终的目的地）使用 User-Password，CHAP-Password 属性，或者使用其他将来扩展的认证方式验证用户。然后回应接入成功回应报文，接入拒绝回应报文或者接入挑战报文给转发服务器。例如，回应一个接入成功回应报文。远程服务器必须（MUST）按顺序将所有的 Proxy-State 属性（只有 Proxy-State 属性）从接入请求报文中拷贝到回应报文中，而且不能改动它们。

4. 转发服务器使用远程服务器的共享密钥验证 Response Authenticator 域，如果验证失败就静默丢弃该报文，如果报文验证被通过，转发服务器移去最后一个 Proxy-State 属性（如果转发服务器曾经增加过该属性），使用和 NAS 共享密钥生成 Response Authenticator 域，恢复和 NAS 的原始请求报文匹配的 Identifier 域，然后将接入成功回应报文发送回 NAS。

为了强制使用本地策略，转发服务器可能（MAY）需要修改属性，该策略已经超出本文说明的范围，但以下的限制需要说明，转发服务器一定不能（MUST not）改动已经在报文中存在的 Proxy-State，State 或者 Class 属性。

转发服务器的实现应该（should）认真考虑哪个 Service-Type 属性值可以接 受，必须（must）认真考虑在被代理的接入请求报文中的 Service-Type， NAS-Prompt 或者 Administrative 属性的影响，转发服务器的实现也可以（may）提供机制阻止这些属性或者其它的服务类型或者其它的属性转发，但该机制超出了本文说明的范围。

2.4. 为什么使用 UDP?

一个经常被问到的问题是为什么使用 UDP 而不是 TCP 做为传输协议，选择 UDP 是基于以下严格的技术理由：

有许多观点必须（must）要理解，RADIUS 是一个基于有几个有趣的特性的协议的交互过程：

1. 如果请求的主认证服务器失败了，备服务器必须（must）能够被找到。

为了满足该需求，在传输层之上必须（must）保存一份请求的拷贝以可以选择发送。这意味也需要一个重传定时器。

2. 这个特殊协议的定时需求和 TCP 提供的定时机制有明显的不同。

举一个极端的例子，RADIUS 不需要数据丢失的检测，用户愿意为认证完成等待几秒钟。强悍的 TCP 的重传（基于平均的回环时间）是不需要的，既然 TCP 重传太耗时间。

另一个极端的例子，用户不会愿意为认证等待上几分钟，因此 TCP 的可靠传输机制在两分钟后是没有用的，更快的启用备用服务器允许用户在（不耐烦而）放弃之前就获得接入。

3. 本协议的无状态的特性简化了 UDP 的使用

客户端和服务器存在还是不存在，系统被重启。这些都不会产生超时机制和 TCP 连接丢失的检测问题，而通常都需要写大量代码处理这些异常事件。UDP 则完全消除了这些特殊处理。（每一个客户端和服务器能够只打开一次 UDP 传输并且让网络中的所有类型的失败事件通过。）

4. UDP 简化了服务器的实现

在最早的 RADIUS 实现中，服务器是单线程的，这意味着，同时只可以接收，处理然后返回一个请求。后来发现后台的想要做到实时（1 秒或者多秒）处理是难以实现的，当每一分钟都有成百的用户需要认证的时候，服务端的请求队列会被填满。请求到回应之间的时间会增长到用户无法忍受的地步（当在数据库中查询或者 DNS 耗费了 30 秒或者更多的秒时，这种情况会变得更加严重）。一种最明显的解决方案就是服务器支持多线程，多线程这一点对于 UDP 来说实现起来很简单，每个请求都有单独的处理线程，处理线程能够使用 UDP 报文直接回应给客户端 NAS。

这当然不是万能药，众所周知，使用 UDP 协议时，需要做一件已经内置到 TCP 协议中的事：我们必须人工管理到同一服务器的重传定时器。尽管使用 TCP 协议不需要对定时器有相同的关注。在本协议中这一缺点相对于使用 UDP 的优势来说只是一个小的代价。

如果没有 TCP 协议，我们可能仍然在用锡罐传递信息，但对于本协议，UDP 是更好的选择。

2.5. 重传提示

如果 RADIUS 服务器和备用 RADIUS 服务器使用相同的共享密钥，那么转发给备用 RADIUS 服务器的报文可以使用相同的 ID 和 Request Authenticator 域，因为属性的内容没有改变。如果您想往备用服务器发送的报文使用新的 Request Authenticator 域，您也可以改变。

如果您改变了 User-Password 属性（或者任何其它的属性）的内容，您需要一个新的 Request Authenticator 域，当然因此需要一个新的 ID。

如果 NAS 向相同的服务器重传 RADIUS 请求报文，这些属性都没有变化，您必须（MUST）使用相同的 Request Authenticator 和 ID 域，使用相同的源端口号。如果有任何属性变化了，您必须（MUST）使用一个新的 Request Authenticator 和 ID 域。

对于所有的服务器，NAS 可以（MAY）使用相同的 ID，或者可以（MAY）对于每个服务器使用独立的 ID 序列。这要看具体的实现。如果 NAS 需要为请求报文使用超过 256 个 ID，则 NAS 可以（MAY）使用其它端口号发送请求，这样每个源端口号都可以保持一个 ID 序列。这样，对于一个服务器，同时可以有 1600 万请求报文。

2.6. 被证明是有害的心跳

一些实现采用发送测试 RADIUS 请求报文的方式检查服务器是否有效。强烈质疑这种方式，它增加了负载而且不能提供任何额外的有用的信息，既然 RADIUS 请求报文包含在一个数据包，在这个时间段，你可以发送一个 ping 报，但您只发送了一个 RADIUS 请求报文，获得了一个表明 RADIUS 服务器是有效的回应，但是如果您没有 RADIUS 请求需要发送，那么服务器是有效的还是无效的根本不是一个问题，因为您根本就没有用它。

如果你想监控您的 RADIUS 服务器，请使用 SNMP 协议，这是 SNMP 的工作。

3. 报文格式

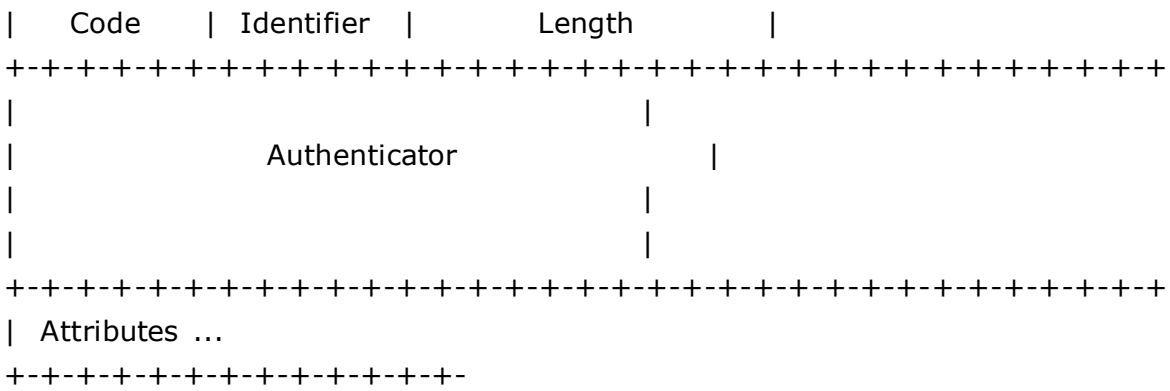
准确地讲，RADIUS 报文是封装在 UDP 报文的数据域[4]中的，它的 UDP 目的端口号是 1812（十进制数）。

当产生一个回应的时候，源端口和目的端口互换。

本文定义了 RADIUS 协议。早期的 RADIUS 计费协议使用 UDP 端口 1645，由于它和著名的"datametrics"服务相冲突。官方为 RADIUS 计费协议重新分配的端口号是 1812。

RADIUS 报文格式如下所示。各个域的数据是从左向右传输的。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



3.1 代码

Code 域占位一个字节，它用来标识 RADIUS 报文类型。当收到的报文的代码域非法时，该报文将会被静默丢弃。

RADIUS 计费报文 Code 域（十进制）分配如下：

1	接入请求报文
2	接入成功回应报文
3	接入拒绝回应报文
4	计费请求报文
5	计费回应报文
11	接入挑战报文
12	服务器状态报文（试验）
13	客户端状态报文（试验）
255	保留

代码 4 和 5 在 RADIUS 计费文档[5]中说明，代码 12 和 13 为可能的使用预留，但本文不做进一步讨论。

3.2 标识符

Identifier 域占位一个字节，用于匹配请求和回应报文。如果在一个很短的时间内接收到相同的源 IP 地址、源 UDP 端口号和相同的 Identifier 域的请求报文，RADIUS 服务器就可以认为是重复的请求报文。

3.3 长度

长度域占位两个字节。它包含了报文中的 Code 域，Identifier 域，Length 域，Authenticator 域和属性域的总长度。在长度域限定的范围之外的字节必须（MUST）作为填充字节，在接收到时不予处理。如果包的实际长度小于长度域中给出的值，该包必须（MUST）被静默丢弃。报文的最小长度是 20，最大长度是 4096。

3.4 认证字

Authenticator 域占位 16 个字节。最重要的字节先传输。该域的值用来鉴别服务器的回应报文，并且用在用户密码的隐藏算法中。

3.4.1 请求认证字

在接入请求报文中，认证字的值是一个占位 16 个字节随机数，称作请求认证字。该值在共享密钥（客户端和服务器的共享密钥）的生命周期中应该（SHOULD）是不可预测的和唯一的。否则在同一密钥下，重复的请求报文将使攻击者能够使用以前截获的回应报文回应。既然可以想像得到在不同的地理区域可以（MAY）使用相同的共享密钥认证。那么，请求认证字域应该（SHOULD）在全球范围内唯一。

在接入请求报文中的 Request Authenticator 域的值也应该（SHOULD）是不可预测的，以免攻击者可以欺骗服务器，让服务器响应一个预计的挑战值，然后用该响应冒充服务器欺骗后续的接入请求。

尽管 RADIUS 协议没有能力阻止通过实时的主动搭线攻击窃听认证会话，然而生成唯一的和不可预知请求报文就能够防范大多数的主动攻击。

NAS 和 RADIUS 服务器共享一个密钥，该共享密钥被加在请求认证字域后面，然后对之使用 MD5 算法生成一个 16 字节的摘要，将该摘要和用户输入的密钥进行异或，然后将异或结果放入接入请求报文的 User-Password 属性中，请参考属性章节中关于 User-Password 属性的条目以了解更详细的信息。

3.4.2 回应认证字

在接入成功回应报文，接入拒绝回应报文和接入挑战报文中的认证字域的值称作回应认证字。包含对如下字段组成的字节流的 MD5 加密的摘要信息：从代码域开始，包含标识符域，长度域，接入请求报文中的请求认证字域和回应报文中的属性，然后后面加上共享密钥。

即 ResponseAuth=MD5(Code+ID+Length+RequestAuth+Attributes+Secret)，这里+表示连接。

3.5 管理提示

共享密钥（在客户端和 RADIUS 服务器之间的共享密钥）的长度应该（SHOULD）至少大到不可能猜测的程度。推荐的共享密钥应该至少 16 个字节。这样才会有总够大的密钥范围以阻止穷举攻击。密钥必须不能（MUST NOT）是空的，因为这样报文很容易被伪造。

RADIUS 服务器必须（MUST）根据 RADIUS 的 UDP 报文的源 IP 地址决定使用那个共享密钥，因此，RADIUS 请求才可以被代理。

当使用转发代理时，代理必须（must）能够在报文通过的每个方向上更改报文。当代理转发请求报文时，代理可以（MAY）增加 Proxy-State 属性，当代理转发回应报文时，代理必须（MUST）移除它增加的 Proxy-State 属性（如果它曾经增加过）。**Proxy-State** 属性总是在其它的 Proxy-State 属性后增加或者移除，没有其它关于该属性在属性列表中位置的要求。由于是基于整个报文内容鉴别接入成功回应报文和接入拒绝回应报文的，Proxy-State 属性的变化会使得原来的签名无效，因此代理不得不重新签名。

RADIUS 代理实现的进一步的详细信息超出了本文描述的范围。

4. 报文类型

RADIUS 报文类型由在报文中第一个字节中的代码域决定。

4.1. 接入请求报文

描述

接入请求报文被发送给 RADIUS 服务器，报文携带了决定是否允许用户接入指定 NAS 的信息，还包含该用户需要使用的服务的信息。一个 RADIUS 实现想要认证用户，那么必须（MUST）发送一个代码域值置为 1 的 RADIUS 报文。

一旦从一个有效的客户端接受到接入请求报文，必须（MUST）要有一个合适的回应报文被发送回。

一个接入请求报文应该（SHOULD）包含 User-Name 属性，它必须包含 NAS-IP-Address 或者 NAS-Identifier 属性（或者两者都包含）。

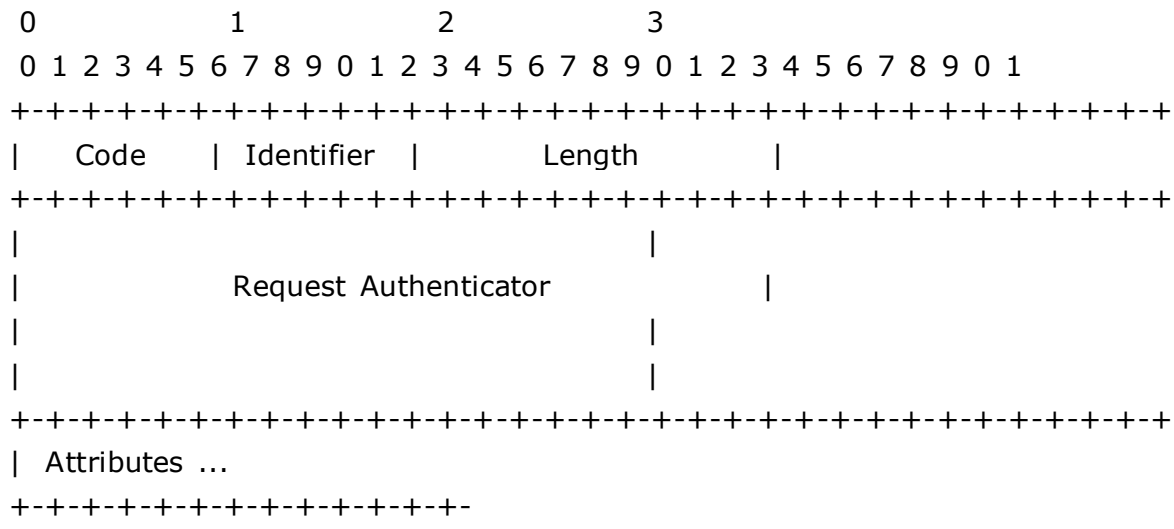
一个接入请求报文必须（MUST）包含 User-Password，CHAP-Password 或者 State 属性。**一个接入请求报文必须不能（MUST NOT）同时包含 User-Password 和 CHAP-Password 属性**。如果将来的扩展允许携带其它类型的认证信息，扩展的属性可以替代接入请求报文中的 User-Password 和 CHAP-Password 属性。

一个接入请求报文应该（SHOULD）包含 NAS-Port 或者 NAS-Port-Type 属性，或者两者都包含，除非被请求的接入类型不涉及端口或者 NAS 不区分端口。

一个接入请求报文可以（MAY）包含额外的属性做为对服务器的提示，但服务器不需要一定处理该提示。

当 User-Password 属性存在时，会采用基于 MD5 [3]算法的方法将该属性值隐藏起来。

接入请求报文格式如下所示。各个域是自左向右传输的。



代码

1 代表接入请求报文

标识符

当属性域的内容变化时，或者接收到前一个请求的有效回应时，Identifier 域必须（MUST）改变。当报文重发时，Identifier 域必须（MUST）保持不变。

请求认证字

每当使用新的标识符域时，请求认证字域的值必须（MUST）改变。

属性

属性域的长度是变化的，包含了请求服务类型所需要的属性列表，也包含了任何想要的可选属性。

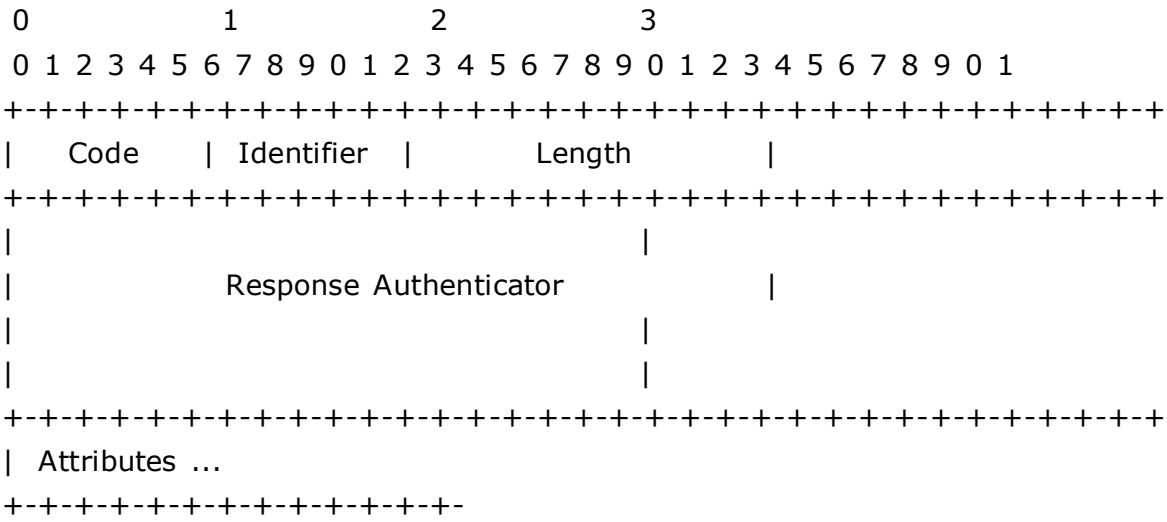
4.2. 接入成功回应报文

描述

接入成功回应报文是由 RADIUS 服务器发送的，提供了开始给用户提供服务的特定的配置信息。如果接收到的接入请求报文的所有属性都是可以接受的，那么 RADIUS 实现必须（MUST）发送一个代码域值为 2 的报文（接入成功回应报文）。

客户端接收到接入成功回应报文后，标识符域应该和一个等待回应的接入请求报文的相应域匹配。回应认证字域必须（MUST）包含对等待回应的接入请求报文的正确回应，无效的报文将被静默丢弃。

接入成功回应报文格式如下所示。各个域是自左向右传输的。



代码

2 代表接入成功回应报文

标识符

标识符域是对引起这次回应的接入请求报文的标识符域的一个拷贝。

回应认证字

回应认证字的值根据接入请求报文计算得来，已经在前面描述过了。

属性

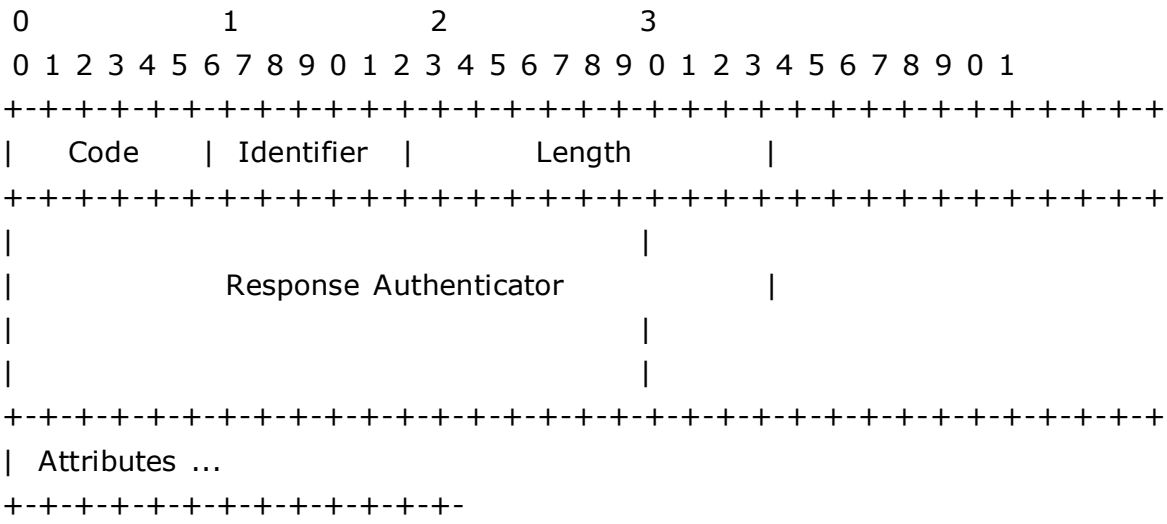
Attributes 域的长度是变化的，其中包含了零个或者多个属性。

4.3. 接入拒绝回应报文

描述

如果接收到的任何属性不可接受，RADIUS 服务必须（MUST）发送一个代码域值为 3 的报文（接入拒绝回应报文）。该报文包含一个或者多个 Reply-Message 属性，该属性包含了一个文本消息，它可以（MAY）由 NAS 显示给用户。

接入拒绝回应报文格式如下所示。各个域是自左向右传输的。



代码

3 代表接入拒绝回应报文

标识符

标识符域是对引起这次回应的接入请求报文的标识符域的一个拷贝。

回应认证字

回应认证字域的值根据接入请求报文计算得来，已经在前面描述过了。

属性

属性域的长度是变化的，其中包含了零个或者多个属性。

4.4. 接入挑战报文

描述

如果 RADIUS 服务器想要给用户发送一个挑战，要求用户回应，那么 RADIUS 服务器必须（MUST）回应一个代码域值为 11 的报文（接入挑战报文）。

属性域中可以（MAY）有一个或者多个 Reply-Message 属性，可以（MAY）有一个或者 0 个 State 属性，Vendor-Specific，Idle-Timeout，Session-Timeout 和 Proxy-State 属性也可以（MAY）包含。本文中不允许接入挑战报文包含其它任何属性。

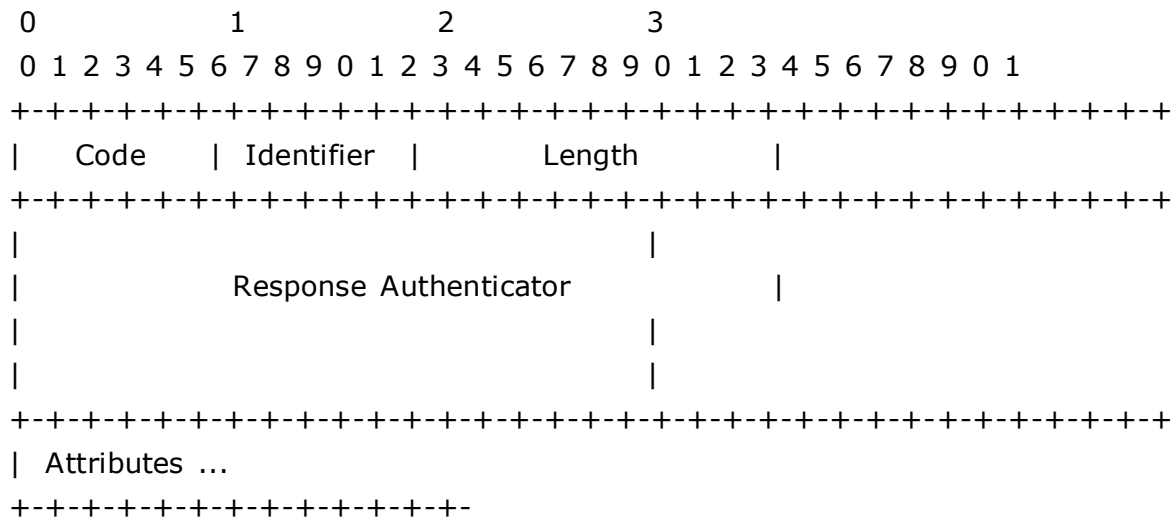
客户端接收到接入挑战报文后，标识符域应该和一个等待回应的接入请求报文的标识符域匹配。另外，回应认证字域必须（MUST）包含对等待回应的接入请求报文的正确回应，无效的报文将被静默丢弃。

如果 NAS 不支持挑战/回应认证方式，NAS 必须（MUST）将接入挑战报文做为接入拒绝回应报文对待。

如果 NAS 支持挑战/回应认证方式，接收到一个有效的接入挑战报文表示应该（SHOULD）发送一个新的接入请求报文了。如果有文本消息，NAS 可以（MAY）显示给用户，并等待用户回应，然后 NAS 发送原来的接入请求报文，该报文携带了新的请求 ID，新的请求认证字，User-Password 属性被用户的回应替换（加密的），也包含了接入挑战报文中的 State 属性（如果有的话），但只能有 0 个或者 1 个 State 属性包含在接入请求报文中。

（支持 PAP 认证方式的 NAS 可以（MAY）转发 Reply-Message 属性给拨号客户端然后接受一个 PAP 回应，好像是用户输入的回应一样）。如果 NAS 不支持这种方式，NAS 必须（MUST）将接入挑战报文做为接入拒绝回应报文对待。

接入挑战报文格式如下所示。各个域是自左向右传输的。



代码

11 代表接入挑战报文

标识符

标识符域是对引起这次回应的接入请求报文的标识符域的一个拷贝。

回应认证字

回应认证字域的值根据接入请求报文计算得来，已经在前面描述过了。

属性

Attributes 域的长度是变化的，其中包含了零个或者多个属性。

5. 属性

RADISU 属性携带了特定的认证和授权信息以及请求和回应报文的配置细节。

由 RADIUS 报文的长度域来决定属性列表在何处结束。

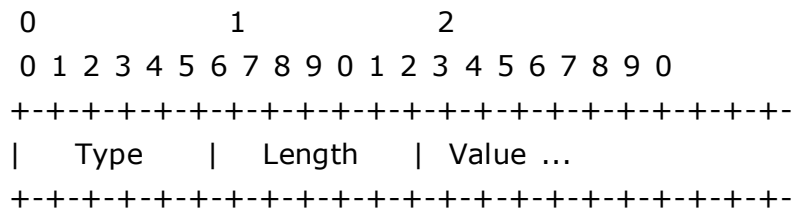
有些属性可以（MAY）被多次包含，这通常有特别的目的，这种情况都会在每个属性的描述中特别指出。在属性章节的最后提供了一个汇总表。

如果相同类型的属性多次出现，任何代理都必须（MUST）保持相同类型的属性的次序。不同类型的属性的次序不需要保持，RADIUS 服务器或者客户端必须（MUST）不能依赖于不同类型的属性的次序。RADIUS 服务器和客户端必须（MUST）不能要求相同类型的属性相连。

哪种类型的报文可以包含哪些属性，这些限制性描述只适用于本文定义的报文类型，即接入请求报文，接入成功回应报文，接入拒绝回应报文和接入挑战报文（代码域值为 1、2、3 和 11）。其它文档定义的其它报文类型也可以使用本文描述的属性。哪些属性可以包含在计费请求和计费回应报文（代码域值为 4 和 5）中，请参见 RADIUS 计费协议文档[5]。

同样地，这里只说明了哪些属性可以包含在本文定义的报文类型中，将来的备忘录定义了新的属性应该（should）要说明这些新的属性可以包含在哪些报文类型中。

属性域的格式如下所示。是自左向右传输的。



属性列表

类型域占位一个字节。到目前为止，在最新的“Assigned Number” RFC [6]中给出了 RADIUS Type 的值的详细描述。值 192-223 是保留给实验用的，值 224-240 是保留给特定实现用的，值 241-255 是预留的，而且不应该（should not）使用它们。

RADIUS 服务器和 RADIUS 客户端可以（MAY）忽略它不认识的属性类型。

本文中涉及到以下的属性 Type 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 (unassigned)
18 Reply-Message
19 Callback-Number
20 Callback-Id
21 (unassigned)
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
37 Framed-AppleTalk-Link
38 Framed-AppleTalk-Network
39 Framed-AppleTalk-Zone
40-59 (reserved for accounting)
60 CHAP-Challenge
61 NAS-Port-Type
62 Port-Limit
63 Login-LAT-Port

长度

长度（Length）域占位一个字节，表示包括 Type、Length、Value 域在内的属性的长度。如果接受到的接入请求报文中的属性长度无效，则应该（SHOULD）发送一个接入拒绝回应报文。如果接收到的接入成功回应报文，接入拒绝回应报文和接入挑战报文有无效长度的属性，必须将之做为接入拒绝回应报文处理，或者直接静默丢弃。

值

值域占位零个或者更多字节，它包含了属性信息的详细描述。值域的格式和长度是由属性的类型和长度决定的。

需要指出的是，在 RADIUS 中没有任何类型的属性值是以 NUL（十六进制的 0x00）结束的。譬如，“text”和“string"类型的属性值是不能以 NUL 结束。由于属性具有长度域，因而不必使用结束符。“text”类型的属性值包含 UTF-8 编码的 10646 [7]字符，而“string”类型的属性值含有 8 位二进制数据。服务器和客户端必须（MUST）能够处理嵌入的 null。使用 C 语言实现的 RADIUS 在处理字符串时需要注意不能使用 strcpy()函数。

值域有五种数据类型。注意：**类型“text”是类型“string"的一个子集**。

text　1-253 个字节，包含 UTF-8 编码的 10646 [7]字符。长度为零的 text 类型的属性必须不能（MUST NOT）被发送，而应该将整个属性忽略。

string　1-253 个字节，包含二进制数据（值从 0 到 255，十进制）。长度为零的 string 类型的属性必须不能（MUST NOT）发送，而应该将整个属性忽略。

address　32 位的数值，最重要的字节优先传输。

integer　32 位的无符号数，最重要的字节优先传输。

time　32 位的无符号数，最重要的字节优先。从格林威治时间 1970 年 1 月 1 日 0 时 0 分 0 秒时起的秒数。标准的属性是不使用该数据类型的，在这里提到该数据类型主要是有可能在将来的属性中使用。

5.1. User-Name（用户名）

描述

该属性表示被认证的用户的名称，如果能够得到的话，该属性必须（MUST）在接入请求报文中发送。

该属性可以（MAY）包含在接入成功回应报文中，在这种情况下，客户端应该（SHOULD）在该会话的所有的计费请求报文中使用接入成功回应报文中返回的用户名称。如果接入成功回应报文中包含值为 Rlogin 的 Service-Type 属性和 User-Name 属性，NAS 可以（MAY）使用返回的 User-Name 执行 Rlogin 功能。

User-Name 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
0               1               2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

1 代表 User-Name

长度

>= 3

字符串

字符串域占位 1 个或者多个字节，NAS 可以（may）限制 User-Name 属性的最大长度，但推荐（recommended）至少应该能够处理 63 个字节。

用户名的格式可以（MAY）是如下几种格式之一：

文本　　最好包含 UTF-8 编码的 10646 [7]字符。

网络接入标识（NAI）
网路接入标识在 RFC 2486 [8]描述。

识别名
ASN.1 格式的名称用在公共密钥认证体系

5.2. User-Password

描述

该属性表示用户用来认证的用户密码，或者是用户在收到接入挑战报文后用户的输入。它只出现在接入请求报文中。

在传输的过程中，密码是隐藏起来的，首先，将密码用 null（\0）填充到 16 的整数倍个字节长，然后对在请求认证字后面加上共享密钥的字节流进行 MD5 加密生成 hash 值，将该 hash 值和密码的第一个 16 字节进行异或，然后将结果放入 User-Password 属性的第一个 16 字节中。

如果密码长度超过 16 个字符，则对第一个异或值后面加上共享密钥的字节流进行 MD5 加密生成 hash 值。该 hash 值和密码的第二个 16 个字节进行异或，然后将异或值放入 User-Password 属性的第二个 16 字节中。

如果必要，重复这个操作，每一个异或值后面加上共享密钥产生下一个 hash 值，然后和密码下一段的 16 字节进行异或。密码最长不能超过 128 个字符。

这个方法引用自 Kaufman, Perlman 和 Speciner 合写的《网络安全》一书，在第 109 到第 110 页。该方法的一个更加精确的解释如下：

共享密钥为 S，伪随机数 Request Authenticator 为 RA，将密码拆分成多个 16 个字节的块 p1，p2，等等。最后一块用 null（\0）填充满 16 个字节，密码块为 c(1)，c(2)，等等。中间值为 b1，b2，等等。

```
b1 = MD5(S + RA)      c(1) = p1 xor b1
b2 = MD5(S + c(1))    c(2) = p2 xor b2
     .                .
     .                .
     .                .
bi = MD5(S + c(i-1))  c(i) = pi xor bi
```

User-Password 属性字符串为 c(1)+c(2)+...c(i)，+表示连接。

一旦接收到报文，逆向处理就能得到密码明文。

User-Password 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0             1             2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|    Type     |    Length     |  String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

类型

2 代表用户密码

长度

至少 18 字节，但不能超过 130 个字节

字符串

本字符串占位 16 到 128（包含）个字节。

5.3. CHAP-Password

描述

该属性表示 PPP 挑战握手认证协议（CHAP）的用户回应的挑战值，它只出现在接入请求报文中。

如果报文中有 CHAP-Challenge 属性（60）的话，CHAP 挑战值会在该属性中，否则应该在请求认证字域中。

CHAP-Password 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
0             1             2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  CHAP Ident   |  String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

3 代表 CHAP 密码

长度

19

CHAP 标识

该域占位一个字节，包含了用户的 CHAP 回应的 CHAP 标识。

字符串

该字符串占位 16 个字节，包含了用户的 CHAP 回应。

5.4. NAS-IP-Address

描述

本属性表示要求认证用户的 NAS 的 IP 地址，应该（SHOULD）在 RADIUS 服务器范围内唯一地标识 NAS。NAS-IP-Address 属性只出现在接入请求报文中，接入请求报文中必须包含 NAS-IP-Address 或者 NAS-Identifier 属性。

需要注意的是，一定不能（MUST NOT）使用 NAS-IP-Address 属性查询用来认证请求报文的共享密钥。必须（MUST）使用接入请求报文的源 IP 地址查询共享密钥。

NAS-IP-Address 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0            1            2            3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |         Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       Address (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

4 代表 NAS IP 地址

长度

6

地址

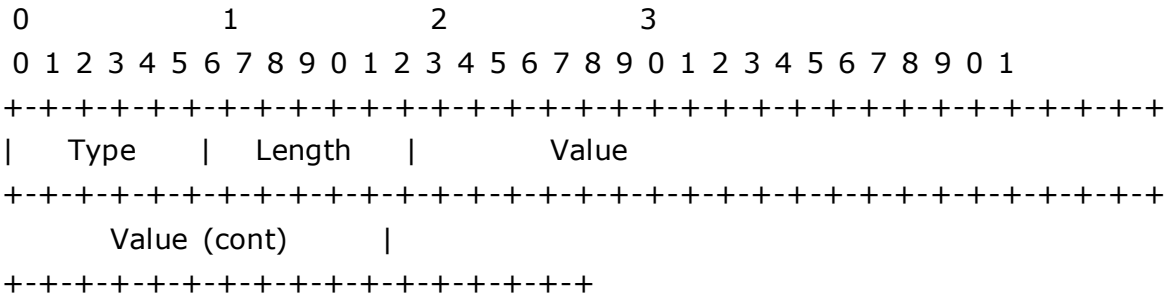
地址域占位 4 个字节。

5.5. NAS-Port

描述

该属性表示认证用户的 NAS 的物理端口号，它只出现在接入请求报文中，需要注意的是，该端口是物理意义上的 NAS 端口，而不是 TCP 或者 UDP 意义上的端口号。如果 NAS 区分端口的话，NAS-Port 或者 NAS-Port-Type 属性（61），或者两者都应该（SHOULD）出现在接入请求报文中。

NAS-Port 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

5 代表 NAS 端口号

长度

6

值

值域占位 4 个字节。

5.6. Service-Type

描述

该属性表示用户请求的服务类型，或者 NAS 准备提供的服务类型，它可以（MAY）出现在接入请求报文或者接入成功回应报文中。NAS 不需要实现所有的服务类型。如果接收到不知道或者不支持的服务类型，则必须（MUST）像接收到接入拒绝回应报文一样处理。

Service-Type 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type     |    Length     |           Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       Value (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

6 代表服务类型

长度

6

值

值域占位 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

如下定义了使用在接入成功回应报文中的服务类型，当服务类型使用在接入请求报文中时，它们可以（MAY）被认为是在提示 RADIUS 服务器，NAS 有理由相信用户喜欢指定的服务类型，但服务器不需要重视该提示。

Login 用户应该（should）被连接到主机上。

Framed 应该（should）为用户启用 Framed 协议，如 PPP 或者 SLIP 协议。

Callback Login 用户应该被断开连接后回调，然后连接到主机上。

Callback Framed 用户应该被断开后回调，然后应该（should）为用户启用 Framed 协议，如 PPP 或者 SLIP 协议。

Outbound 用户应该（should）被授权访问（外出）设备。

Administrative 用户应该（should）被授权访问有管理 NAS 权限的接口，该接口可以执行特权命令。

NAS Prompt 应该提供给用户一个 NAS 上的命令行提示信息，该 NAS 上不能执行特权命令。

Authenticate Only 只需要认证，在接入成功回应报文中不需要返回授权信息（典型用法是代理服务器，而不是 NAS 本身）。

Callback NAS Prompt 用户应该被断开后回调，然后提供给用户一个 NAS 上的命令行提示信息，该 NAS 上不能执行特权命令。

Call Check 由 NAS 用在接入请求报文中，表示接收到一个调用，RADIUS 服务器应该返回一个接入成功回应报文来应答该调用，或者返回一个接入拒绝回应报文以拒绝该调用。典型的是基于 Called-Station-Id 或者 Calling-Station-Id 属性。推荐（recommended）接入请求报文使用 Calling-Station-Id 属性的值做为 User-Name 属性的值。

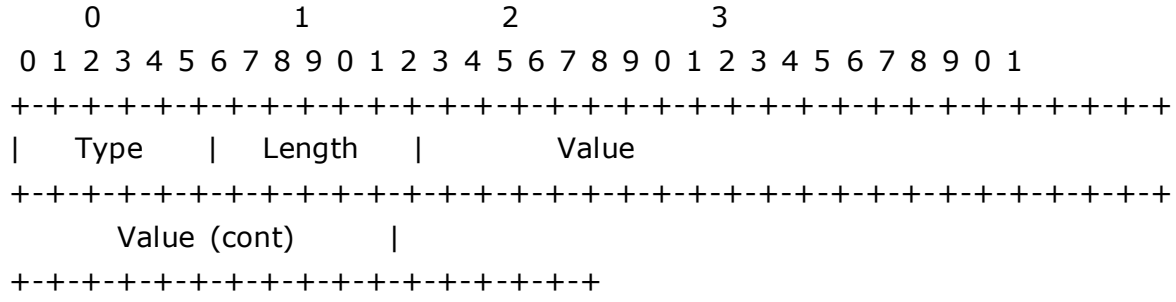
Callback Administrative 用户应该（should）被断开后回调，然后用户被授权访问有管理 NAS 权限的接口，该接口可以执行特权命令。

5.7. Framed-Protocol

描述

（该属性表示 framing 使用 framed 接入）。它可以（MAY）用在接入请求报文和接入拒绝回应报文中。

Framed-Protocol 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

7 代表 Framed-Protocol.

长度

6

值

值域占位 4 个字节。

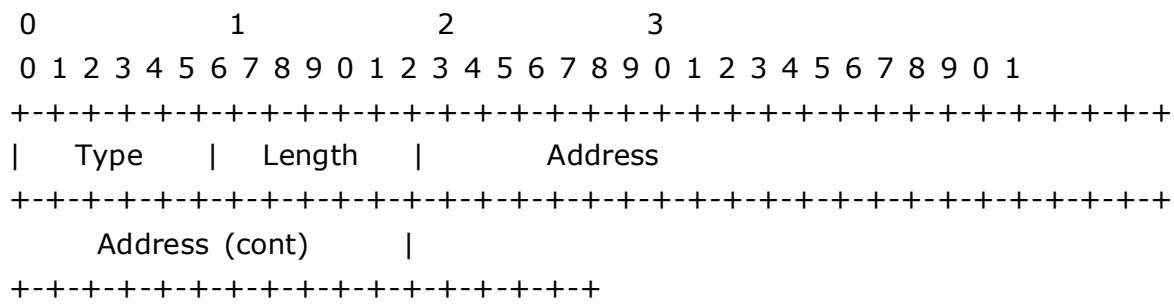
1 PPP
2 SLIP
3 AppleTalk Remote Access Protocol (ARAP)
4 Gandalf proprietary SingleLink/MultiLink protocol
5 Xylogics proprietary IPX/SLIP
6 X.75 Synchronous

5.8. Framed-IP-Address

描述

该属性表示配置给用户的 IP 地址，它可以（MAY）使用在接入成功回应报文中，它可以（MAY）由 NAS 使用在接入请求报文中以提示服务器更愿意使用该 IP 地址做为用户的 IP 地址，但是服务器不需要重视该提示。

Framed-IP-Address 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

8 代表用户 IP 地址

长度

6

地址

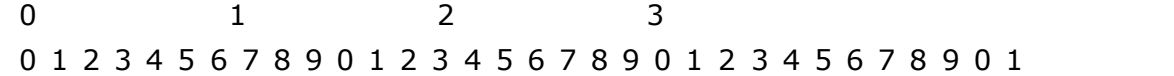
地址域占位 4 个字节。值 0xFFFFFFFF 表示 NAS 应该（should）允许用户选择一个地址（即协商地址），值 0xFFFFFFFE 表示 NAS 应该（should）为用户选择一个地址（即从 NAS 的地址池中分配地址）。其它有效值表示 NAS 应该（should）使用该值做为用户的 IP 地址。

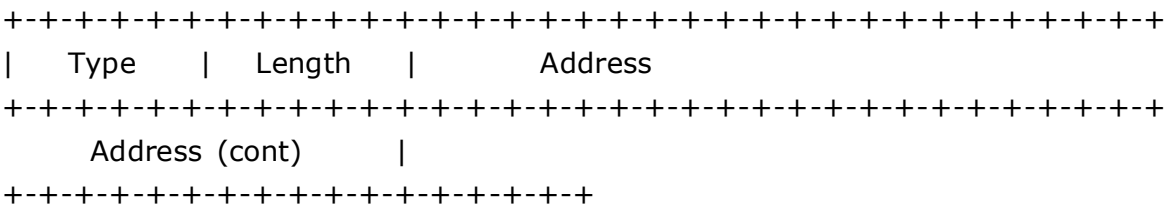
5.9. Framed-IP-Netmask

描述

当用户是一个网络上的路由器时，该属性表示配置给用户的 IP 地址掩码。它可以（MAY）使用在接入成功回应报文。它可以（MAY）由 NAS 使用在接入请求报文中以提示服务器更愿意使用该 IP 地址掩码，但是服务器不需要重视该提示。

Framed-IP-Netmask 属性的格式如下所示。各个域是按照自左向右的顺序传输的。





类型

9 代表用户 IP 地址掩码

长度

6

地址

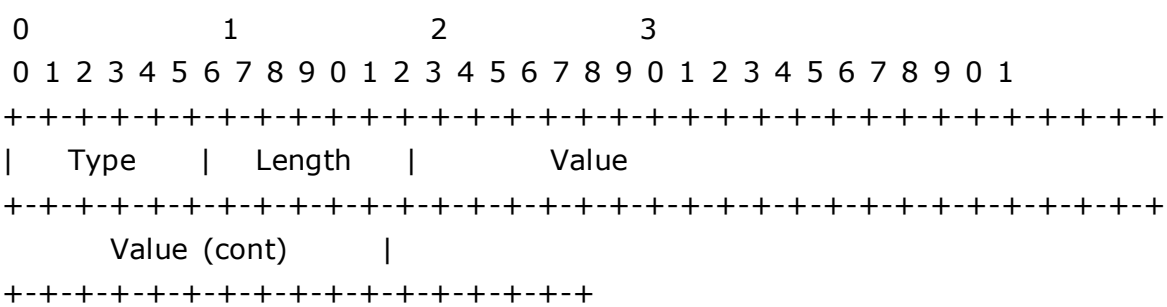
地址域占位 4 个字节，该值指定了用户的 IP 地址掩码。

5.10. Framed-Routing

描述

当用户是一个网络上的路由器时，该属性表示了用户的路由方法，它只使用在接入成功回应报文。

Framed-Routing 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

10 代表 Framed-Routing.

长度

6

值

值域占位 4 个字节

0 None
1 Send routing packets
2 Listen for routing packets
3 Send and Listen

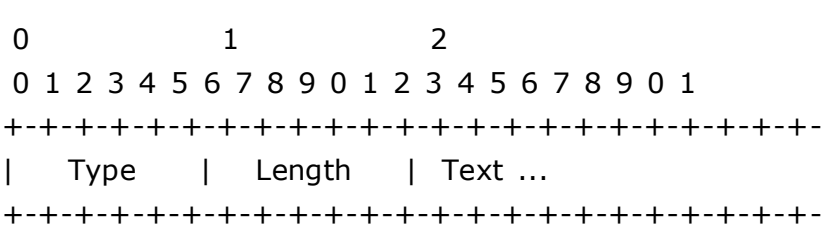
5.11. Filter-Id

描述

该属性表示用户的过滤列表的名称，接入成功回应报文中可以（MAY）包含 0 个或多个 Filter-Id 属性。

使用名称标识过滤列表允许过滤使用在不同的 NAS 上而不用考虑过滤列表的实现细节。

Filter-Id 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

11 代表 Filter-Id.

长度

>= 3

文本

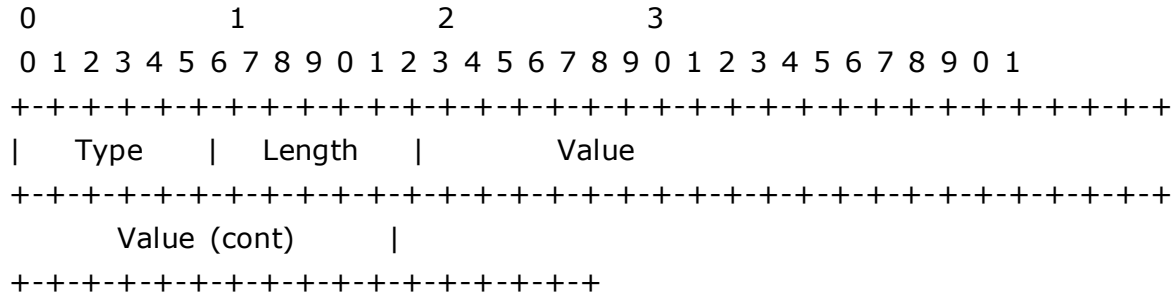
文本域占位 1 个或多个字节，它的内容是独立于实现的，它有意使用人类可读的形式，并且一定不能（MUST NOT）影响协议的操作，推荐（recommended）该消息包含 UTF-8 编码的 10646 [7]字符。

5.12. Framed-MTU

描述

当不能使用其它协商方式（如 PPP）时，该属性表示用户的最大传输单位，它可以（MAY）由 NAS 使用在接入请求报文中以提示服务器更愿意使用该值，但是服务器不需要重视该提示。

Framed-MTU 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

12 代表 Framed-MTU.

长度

6

值

值域占位 4 个字节，它的取值范围从 64 到 65535。

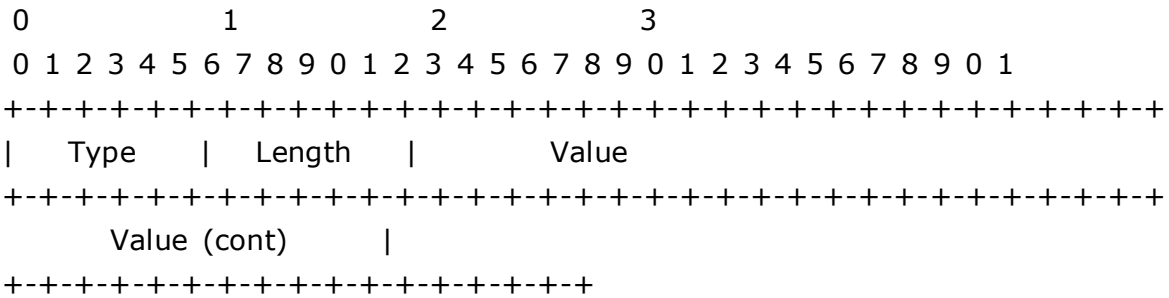
5.13. Framed-Compression

描述

该属性表示链路使用的压缩协议，它可以（MAY）使用在接入成功回应报文，它可以（MAY）由 NAS 使用在接入请求报文中以提示服务器更愿意使用该压缩算法，但是服务器不需要重视该提示。

可以（MAY）发送多个压缩协议属性，NAS 的职责是为的相应链路流量选择合适的压缩协议。

Framed-Compression 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

13 代表 Framed-Compression.

长度

6

值

值域占位 4 个字节

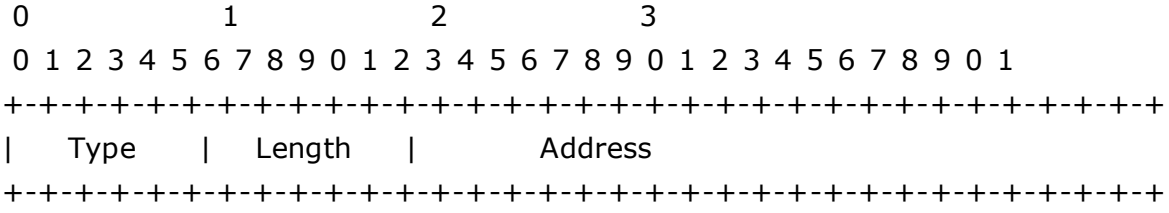
0 None
1 VJ TCP/IP header compression [10]
2 IPX header compression
3 Stac-LZS compression

5.14. Login-IP-Host

描述

当 Login-Service 属性存在时，该属性表示用户连接的系统，它可以（MAY）使用在接入成功回应报文中，它可以（MAY）由 NAS 使用在接入请求报文中以提示服务器更愿意使用该主机，但是服务器不需要重视该提示。

Login-IP-Host 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



```
      Address (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

14 代表 Login-IP-Host.

长度

6

地址

地址域占位 4 个字节，值 0xFFFFFFFF 表示 NAS 应该（SHOULD）允许用户选择地址，值 0 表示 NAS 应该（SHOULD）选择一个用户连接的主机，其它值表示 NAS 应该（SHOULD）将用户连接到该 IP 地址上。

5.15. Login-Service

描述

该属性表示用来连接用户到登录主机的服务，它只能使用在接入成功回应报文中。

Login-Service 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0             1             2             3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type     |    Length     |          Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       Value (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

15 代表 Login-Service.

长度

6

值

值域占位 4 个字节。

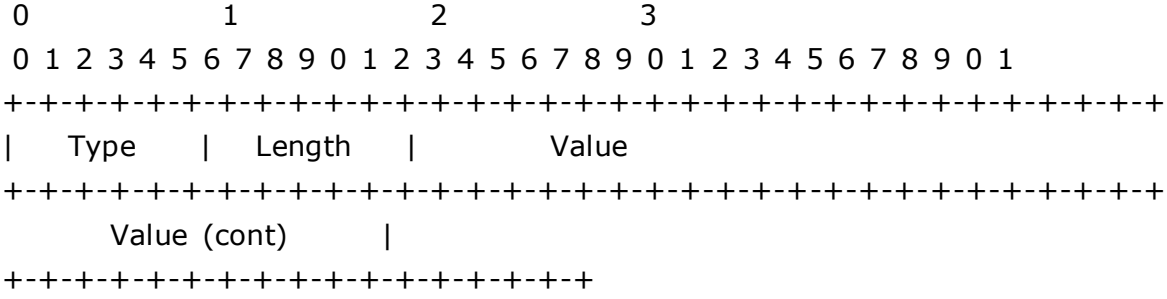
0 Telnet
1 Rlogin
2 TCP Clear
3 PortMaster (proprietary)
4 LAT
5 X25-PAD
6 X25-T3POS
8 TCP Clear Quiet (suppresses any NAS-generated connect string)

5.16. Login-TCP-Port

描述

当 Login-Service 属性也存在时，该属性表示连接到用户的 TCP 端口号，它只在接入成功回应报文中使用。

Login-TCP-Port 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

16 代表 Login-TCP-Port.

长度

6

值

值域占位 4 个字节，取值范围从 0 到 65535。

5.17. （未被分配）

描述

属性类型 17 还未被分配

5.18. Reply-Message

描述

该属性表示可以（MAY）显示给用户的文本信息。

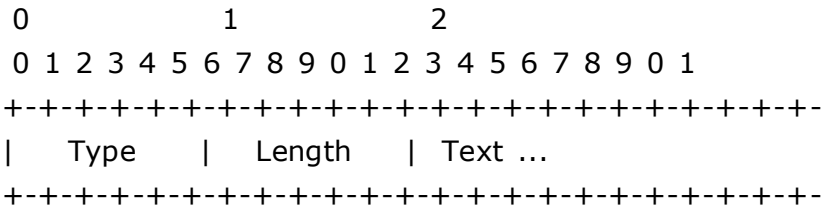
当使用在接入成功回应报文中，它表示成功消息。

当使用在接入拒绝回应报文中，它表示失败消息，它可以（MAY）表示在用户尝试另一个接入请求之前给用户的对话框提示消息。

当使用在接入挑战报文中，它可以（MAY）表示一个提示用户回应的对话框消息。

如果有任何提示信息需要显示，可以（MAY）包含多个 Reply-Message 属性。
它们必须（MUST）按照报文中出现的顺序显示给用户。

Reply-Message 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

18 代表 Reply-Message.

长度

>= 3

文本

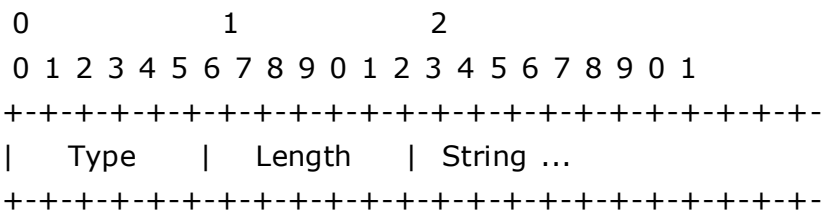
文本域占位 1 个或多个字节，它的内容是独立于实现的，它有意使用人类可读的形式，并且一定不能（MUST NOT）影响协议的操作，推荐（recommended）该消息包含 UTF-8 编码的 10646 [7]字符。

5.19. Callback-Number

描述

该属性表示用来回调的拨号字符串，它可以（MAY）使用在接入请求报文中，它可以（MAY）由 NAS 使用在接入请求报文中以提示服务器需要一个回调服务，但是服务器不需要重视该提示。

Callback-Number 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

19 代表 Callback-Number.

长度

>= 3

字符串

字符串域占位 1 个或者多个字节，该信息的实际格式由位置或者应用程序决定，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

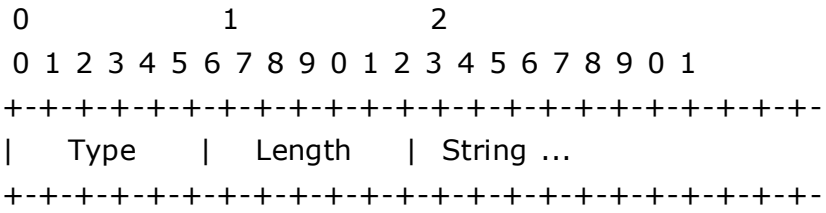
该域允许的用法的定义超出了本规范的讨论范围。

5.20. Callback-Id

描述

该属性表示调用场所的名字，由 NAS 解释，它可以（MAY）使用在接入成功回应报文。

Callback-Id 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

20 代表 Callback-Id.

长度

>= 3

字符串

字符串域占位 1 个或者多个字节，该信息的实际格式由位置或者应用程序决定，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

该域允许的用法的定义超出了本规范的讨论范围。

5.21. （未分配）

描述

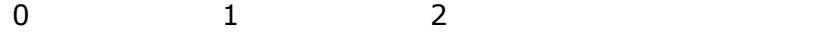
属性类型 21 还未被分配

5.22. Framed-Route

描述

该属性提供 NAS 上用户配置的路由信息，它用在接入请求报文并且可以出现多次。

Framed-Route 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|    Type     |    Length     | Text ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```


类型

22 代表 Framed-Route.

长度

>= 3

文本

文本域占位 1 个或多个字节，它的内容是独立于实现的，它有意使用人类可读的形式，并且一定不能（MUST NOT）影响协议的操作，推荐（recommended）该消息包含 UTF-8 编码的 10646 [7]字符。

对于 IP 路由，它应该（SHOULD）包含了点分十进制的目的地址前缀，后面加上"/"字符，然后再加上标识使用前缀的多少高位的长度，后面跟一个空格，一个点分十进制格式的网关地址，一个空格，一个或者多个被空格分割的矩阵。例如："192.168.1.0/24 192.168.1.1 1 2 -1 3 400"。长度可以（may）被忽略。在这种情况下，A 类地址缺省为 8 位，B 类地址缺省为 16 位，C 类地址缺省为 24 位。例如："192.168.1.0 192.168.1.1 1"。

当网关地址为"0.0.0.0"时，应该（SHOULD）将用户的 IP 地址做为网关地址。

5.23. Framed-IPX-Network

描述

该属性表示用户的 IPX 网络号，它用在接入成功回应报文。

Framed-IPX-Network 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0                   1                   2                   3
```

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type     |    Length     |           Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        Value (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

23 代表 Framed-IPX-Network.

长度

6

值

值域占位 4 个字节，值 0xFFFFFFFE 表示 NAS 应该为用户选择一个 IPX（即从 NAS 拥有的一个或者多个 IPX 网络的池中分配），其它值表示用户链路应该使用该 IPX 网络。

5.24 State

描述

该属性用在服务器发往客户端的接入挑战报文中。如果接入挑战报文中有该属性的话，客户端回应挑战时，向服务器发送的新的接入请求报文必须（MUST）不修改属性的值。

该属性用在由服务器发送往客户端的接入成功回应报文中，该接入成功回应报文也包含值为"RADIUS-Request"的 Termination-Action 属性，在当前会话中断时，如果 NAS 履行了 Termination-Action 属性指定的动作，发送了一个新的接入请求报文。那么，必须在该接入请求报文中包含没有改动过的 State 属性。

在这两个用法中，客户端必须不能（MUST NOT）在本地解析该属性。报文中 必须（must）只能有 0 个或者 1 个 State 属性。State 属性的使用方法是独立于实现的。

State 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0             1             2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type     |    Length     |  String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

24 代表 State.

长度

>= 3

字符串

字符串域占位 1 个或者多个字节，该信息的实际格式由位置或者应用程序决定，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

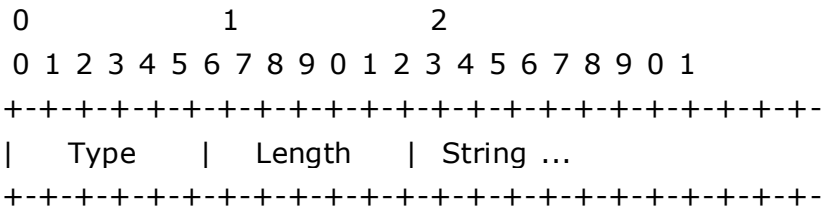
该域允许的用法的定义超出了本规范的讨论范围。

5.25. Class

描述

该属性用在服务器发往客户端的接入成功回应报文中，如果计费服务器支持 的话，它应该（SHOULD）做为计费请求报文的一部分不做修改的发送给计费服务器。客户端必须不能（MUST NOT）解析该属性。

Class 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

25 代表 Class.

长度

>= 3

字符串

字符串域占位 1 个或者多个字节，该信息的实际格式由位置或者应用程序决定，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

该域允许的用法的定义超出了本规范的讨论范围。

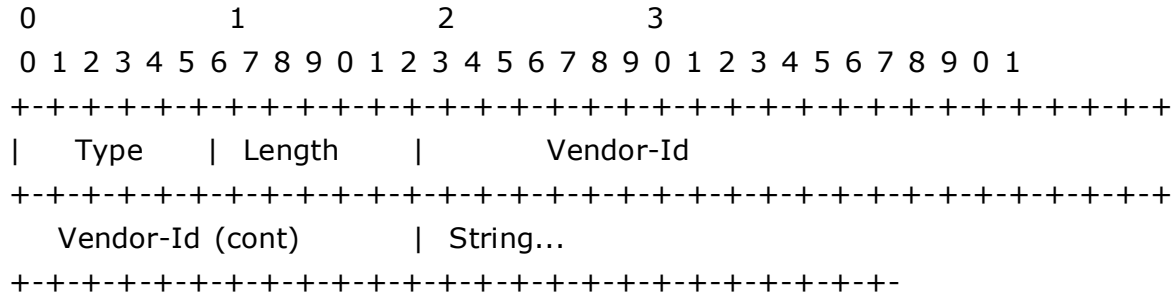
5.26. Vendor-Specific

描述

该属性允许厂商支持他们的扩展属性，这些属性不是为了通用的用途，它必 须不能（MUST not）影响 RADIUS 协议的操作。

如果服务器不能解析由客户端发送的厂商私有信息，服务器必须（MUST）忽　　略该属性（但可以指出来），如果客户端没有接收到它想要的厂商私有信息，它应该（SHOULD）试图在没有该属性的情况下继续操作，尽管它们可能在一个被削弱的模式下工作（指出这种情况）。

Vendor-Specific 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

26 代表 Vendor-Specific.

长度

>= 7

厂商 ID

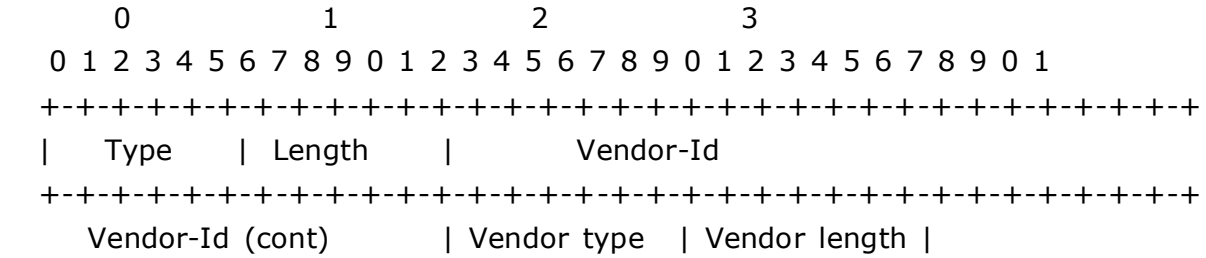
表示为网络字节序，高位字节是 0，低位的三个字节是厂商的 SMI 网络管理私有企业代码，被定义在 RFC“Assigned Numbers” [6]。

字符串

字符串域占位 1 个或者多个字节，该信息的实际格式由位置或者应用程序决定，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

该域允许的用法的定义超出了本规范的讨论范围。

它应该（SHOULD）以厂商类型/厂商长度/值的顺序编码。如下所示，自定义属性域依赖于各个厂商对该属性的定义。一个 Vendor-Specific 属性编码的例子使用如下方法：



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Attribute-Specific...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

多个子属性可以（MAY）编码在一个 Vendor-Specific 属性中，尽管它们不是必须要这样做。

5.27. Session-Timeout

描述

该属性设置了提供给用户的服务的最大秒数，即在会话中断之前，或者提示之前，用户可以使用服务的最大秒数。该属性用在服务器发送到客户端的接入成功回应报文或者接入挑战报文中。

Session-Timeout 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0             1             2             3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |          Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        Value (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

27 代表 Session-Timeout.

长度

6

值

值域占位 4 个字节，包含了一个 32 位的无符号整数，表示用户保持的 NAS 连接的最大秒数。

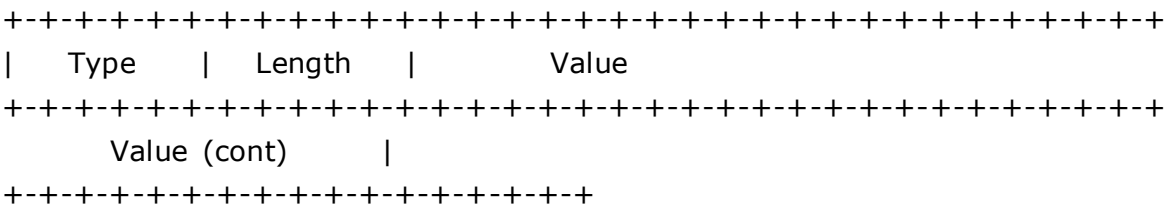
5.28. Idle-Timeout

描述

该属性设置了提供给用户最大的连接闲置持续的最大秒数，即在会话中断之前，或者提示之前，用户的连接可以持续闲置的最大秒数。该属性用在服务器发送到客户端的接入成功回应报文或者接入挑战报文中。

Idle-Timeout 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0             1             2             3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```



类型

28 代表 Idle-Timeout.

长度

6

值

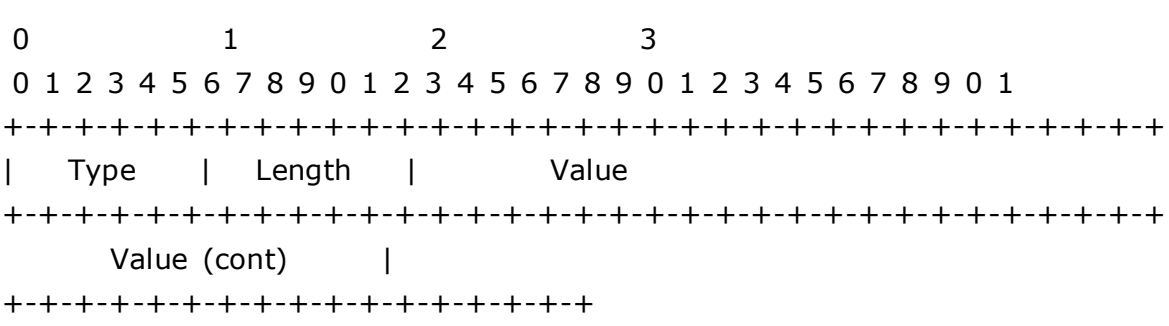
值域占位 4 个字节，包含了一个 32 位的无符号整数，如果用户连接持续闲置时间超过该值，该连接将被 NAS 断开。

5.29. Termination-Action

描述

该属性表示当服务结束时 NAS 应该做何动作，它只用在接入成功回应报文中。

Termination-Action 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

29 代表 Termination-Action.

长度

6

值

值域占位 4 个字节

0 Default
1 RADIUS-Request

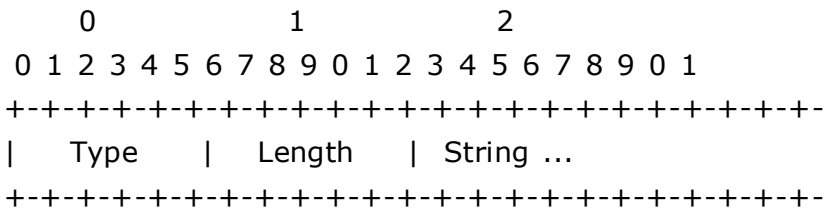
如果该值设为 RADIUS-Request，在服务中断之前，NAS 可以（MAY）向 RADIUS 服务器发送一个新的接入请求报文，如果有 State 属性的话，应该包含 State 属性。

5.30. Called-Station-Id

描述

该属性允许 NAS 在接入请求报文中包含用户呼叫的电话号码，使用拨号标识服务（DNIS）或者类似的技术。需要说明的是，和呼叫进来的电话号码不同，它只用在接入请求报文中。

Called-Station-Id 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

30 代表 Called-Station-Id.

长度

>= 3

字符串

字符串占位 1 个或者多个字节，包含了用户呼叫的电话号码。

该信息的实际格式由位置或者应用程序决定，推荐（recommended）包含 UTF-8 编码的 10646 [7]字符，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

该域允许的用法的定义超出了本规范的讨论范围。

5.31. Calling-Station-Id

描述

该属性允许 NAS 在接入请求报文中包含主叫的电话号码，使用拨号标识服务（DNIS）(Automatic Number Identification (ANI))或者类似的技术。它只用在接入请求报文中。

Calling-Station-Id 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0             1             2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|    Type     |    Length     |  String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

类型

31 代表 Calling-Station-Id.

长度

>= 3

字符串

字符串占位 1 个或者多个字节，包含了主叫号码。

该信息的实际格式由位置或者应用程序决定，推荐（recommended）包含 UTF-8 编码的 10646 [7]字符，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

该域允许的用法的定义超出了本规范的讨论范围。

5.32. NAS-Identifier

描述

该属性包含了一个标识发起接入请求报文的 NAS 的字符串，它只用在接入请求报文中，NAS-IP-Address 或者 NAS-Identifier 属性必须（MUST）有一个出现在接入请求报文中。

需要注意的是，NAS-Identifier 属性必须不能（MUST NOT）用来选择鉴别请求报文的共享密钥，必须（MUST）使用接入请求报文的源 IP 地址查询共享密钥。

NAS-Identifier 属性的格式如下所示。各个域是按照自左向右的顺序传输的。

```
 0             1             2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|    Type     |    Length     |  String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

类型

32 代表 NAS-Identifier.

长度

>= 3

字符串

字符串域占位 1 个或者多个字节，应该在一个 RADIUS 服务器范围内唯一标识 NAS。例如，完全的有效的域名适合做为 NAS-Identifier 属性。

该信息的实际格式由位置或者应用程序决定，推荐（recommended）包含 UTF-8 编码的 10646 [7]字符，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

该域允许的用法的定义超出了本规范的讨论范围。

5.33. Proxy-State

描述

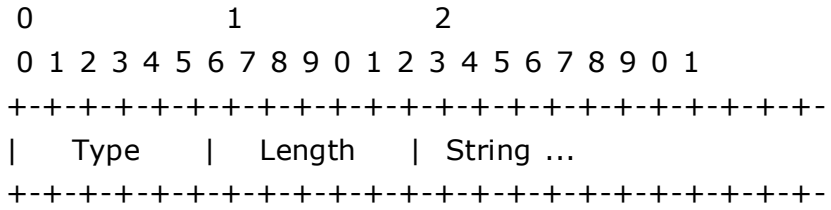
当转发一个接入请求报文时，该属性由代理服务器发往另一个服务器，该属 性必须在接入成功回应报文，接入拒绝回应报文和接入挑战报文中不做修改地返回。当代理服务器接收到一个请求的回应报文时，在转发该回应报文给 NAS 之前，它必须（MUST）移除由它自己增加上的 Proxy-State 属性（即报文中最后一个 Proxy-State 属性）。

如果转发报文时，在报文中增加了一个 Proxy-State 属性，则 Proxy-State 属性必须（MUST）加到所有已存在的 Proxy-State 属性之后。

除了由当前服务器增加的 Proxy-State 属性外，其它 Proxy-State 属性的内容应该（should）做为不透明的字节对待（不需要理解它们），必须不能（MUST NOT）影响协议的操作。

Proxy-State 属性的使用方法是独立于实现的，它的功能的描述超出了本规范描述的范围。

Proxy-State 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

33 代表 Proxy-State.

长度

>= 3

字符串

字符串域占位 1 个或者多个字节，该信息的实际格式由位置或者应用程序决定，一个可靠的实现应该（SHOULD）将该域做为普通的字节对待。

该域允许的用法的定义超出了本规范的讨论范围。

5.34. Login-LAT-Service

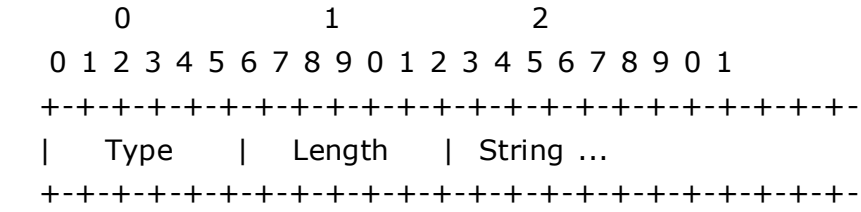
Description

This Attribute indicates the system with which the user is to be connected by LAT. It MAY be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

Administrators use the service attribute when dealing with clustered systems, such as a VAX or Alpha cluster. In such an environment several different time sharing hosts share the same resources (disks, printers, etc.), and administrators often configure each to offer access (service) to each of the shared resources. In this case, each host in the cluster advertises its services through LAT broadcasts.

Sophisticated users often know which service providers (machines) are faster and tend to use a node name when initiating a LAT connection. Alternately, some administrators want particular users to use certain machines as a primitive form of load balancing (although LAT knows how to do load balancing itself).

A summary of the Login-LAT-Service Attribute format is shown below. The fields are transmitted from left to right.



Type

34 for Login-LAT-Service.

Length

>= 3

String

The String field is one or more octets, and contains the identity of the LAT service to use. The LAT Architecture allows this string to contain $ (dollar), - (hyphen), . (period), _ (underscore), numerics, upper and lower case alphabetics, and the ISO Latin-1 character set extension [11]. All LAT string comparisons are case insensitive.

5.35. Login-LAT-Node

Description

This Attribute indicates the Node with which the user is to be automatically connected by LAT. It MAY be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

A summary of the Login-LAT-Node Attribute format is shown below. The fields are transmitted from left to right.

```
     0             1             2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|    Type     |    Length     | String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type

35 for Login-LAT-Node.

Length

>= 3

String

The String field is one or more octets, and contains the identity of the LAT Node to connect the user to. The LAT Architecture allows this string to contain $ (dollar), - (hyphen), . (period), _ (underscore), numerics, upper and lower case alphabetics, and the ISO Latin-1 character set extension. All LAT string comparisons are case insensitive.

5.36. Login-LAT-Group

Description

This Attribute contains a string identifying the LAT group codes which this user is authorized to use. It MAY be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

LAT supports 256 different group codes, which LAT uses as a form of access rights. LAT encodes the group codes as a 256 bit bitmap.

Administrators can assign one or more of the group code bits at the LAT service provider; it will only accept LAT connections that have these group codes set in the bit map. The administrators assign a bitmap of authorized group codes to each user; LAT gets these from the operating system, and uses these in its requests to the service providers.

A summary of the Login-LAT-Group Attribute format is shown below. The fields are transmitted from left to right.

```
     0             1             2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

```
|     Type      |    Length     | String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type

36 for Login-LAT-Group.

Length

34

String

The String field is a 32 octet bit map, most significant octet first. A robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

5.37. Framed-AppleTalk-Link

Description

This Attribute indicates the AppleTalk network number which should be used for the serial link to the user, which is another AppleTalk router. It is only used in Access-Accept packets. It is never used when the user is not another router.

A summary of the Framed-AppleTalk-Link Attribute format is shown below. The fields are transmitted from left to right.

```
     0             1             2             3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |          Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        Value (cont)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

37 for Framed-AppleTalk-Link.

Length

6

Value

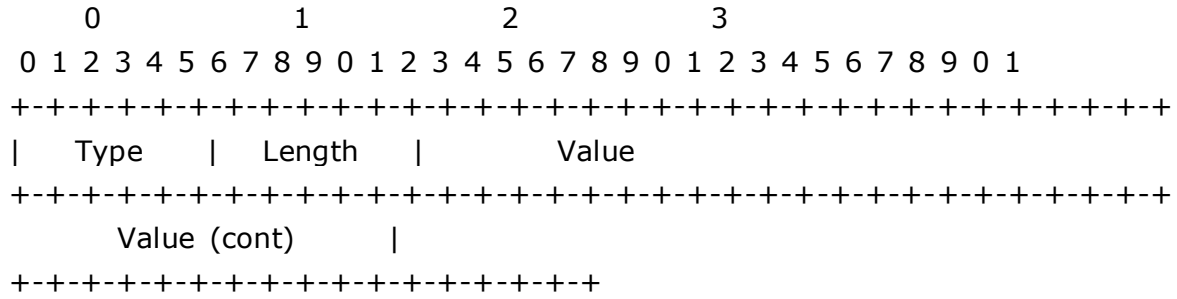
The Value field is four octets. Despite the size of the field, values range from 0 to 65535. The special value of 0 indicates that this is an unnumbered serial link. A value of 1-65535 means that the serial line between the NAS and the user should be assigned that value as an AppleTalk network number.

5.38. Framed-AppleTalk-Network

Description

This Attribute indicates the AppleTalk Network number which the NAS should probe to allocate an AppleTalk node for the user. It is only used in Access-Accept packets. It is never used when the user is another router. Multiple instances of this Attribute indicate that the NAS may probe using any of the network numbers specified.

A summary of the Framed-AppleTalk-Network Attribute format is shown below. The fields are transmitted from left to right.



Type

38 for Framed-AppleTalk-Network.

Length

6

Value

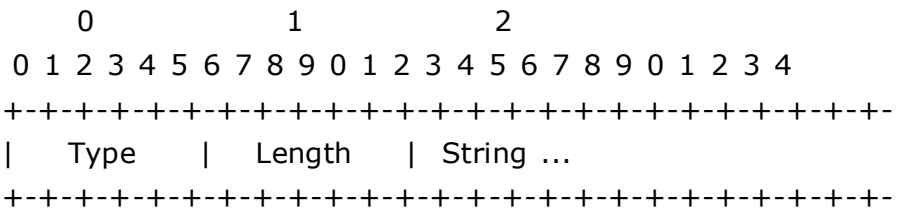
The Value field is four octets. Despite the size of the field, values range from 0 to 65535. The special value 0 indicates that the NAS should assign a network for the user, using its default cable range. A value between 1 and 65535 (inclusive) indicates the AppleTalk Network the NAS should probe to find an address for the user.

5.39. Framed-AppleTalk-Zone

Description

This Attribute indicates the AppleTalk Default Zone to be used for this user. It is only used in Access-Accept packets. Multiple instances of this attribute in the same packet are not allowed.

A summary of the Framed-AppleTalk-Zone Attribute format is shown below. The fields are transmitted from left to right.



Type

39 for Framed-AppleTalk-Zone.

Length

>= 3

String

The name of the Default AppleTalk Zone to be used for this user. A robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

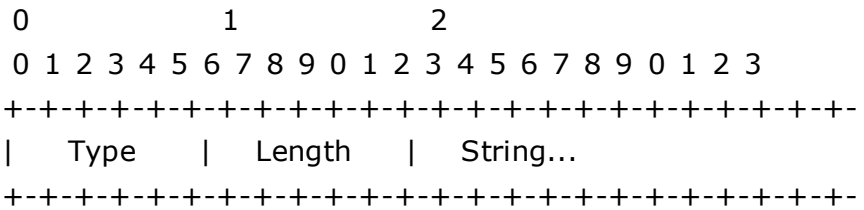
5.40. CHAP-Challenge

描述

当用户使用了 PPP 挑战握手认证协议（CHAP）时，该属性包含了由 NAS 发送的 CHAP 挑战，它只用在接入请求报文中。

如果 CHAP 挑战值为 16 个字节长，它可以（MAY）不使用该属性，而是放入**请求认证字域**中。

CHAP-Challenge 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

60 代表 CHAP-Challenge.

长度

>= 7

字符串

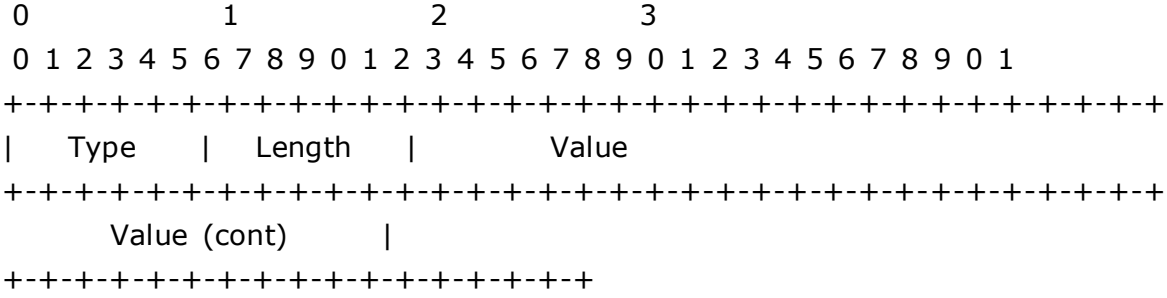
字符串域包含了 CHAP 挑战值。

5.41. NAS-Port-Type

描述

该属性表示了用户认证的 NAS 的物理端口的类型，它可以用来代替 NAS-Port 属性，或者独立存在。它只用在接入请求报文中，如果 NAS 区分它的端口的话，NAS-Port 或者 NAS-Port-Type 属性（或者两者都）应该（SHOULD）包含在接入请求报文中。

NAS-Port-Type 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



类型

61 代表 NAS-Port-Type.

长度

6

值

值域占位 4 个字节，值“Virtual”指的是经由某些传输协议到 NAS 上的连接，而不是经过物理端口的连接。例如：一个用户 telnet 到一个 NAS，做为一个 Outbound-User 认证，接入请求报文可以包含值为“Virtual”的 NAS-Port-Type 属性，以提示服务器用户使用的不是物理端口。

0 Async
1 Sync
2 ISDN Sync
3 ISDN Async V.120
4 ISDN Async V.110
5 Virtual
6 PIAFS
7 HDLC Clear Channel
8 X.25
9 X.75
10 G.3 Fax
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 Ethernet
16 xDSL - Digital Subscriber Line of unknown type
17 Cable
18 Wireless - Other
19 Wireless - IEEE 802.11

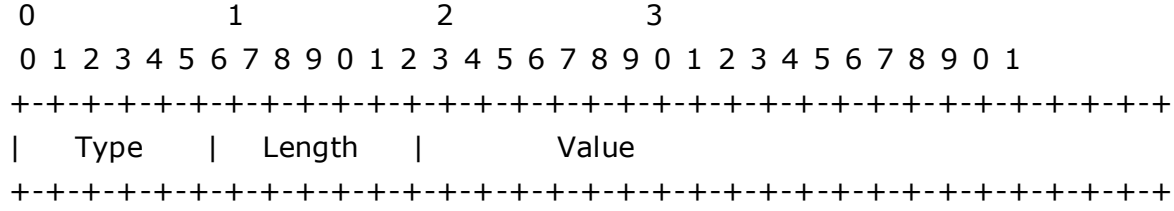
PIAFS 是一种通常使用在日本的无线 ISDN 形式，支持 PHS（Personal Handyphone System）网路接入论坛标准（PIAFS）。

5.42. Port-Limit

描述

该属性设置了 NAS 提供给用户的端口的最大数量,该属性可以在接入成功回应报文中由服务器发送给客户端，它用来关联多链路 PPP 协议[12]或者类似协议。它也可以（MAY）由 NAS 发送往服务器，以提示服务器想要使用多少个端口，但是服务器不需要重视该提示。

NAS-Port-Type 属性的格式如下所示。各个域是按照自左向右的顺序传输的。



```
        Value (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

类型

62 代表 Port-Limit.

长度

6

值

值域占位 4 个字节，包含了一个 32 位的无符号整数，表示允许连接到 NAS 的最大端口数量。

5.43. Login-LAT-Port

Description

This Attribute indicates the Port with which the user is to be connected by LAT. It MAY be used in Access-Accept packets, but only when LAT is specified as the Login-Service. It MAY be used in an Access-Request packet as a hint to the server, but the server is not required to honor the hint.

A summary of the Login-LAT-Port Attribute format is shown below. The fields are transmitted from left to right.

```
     0             1             2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type     |    Length     | String ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

63 for Login-LAT-Port.

Length

>= 3

String

The String field is one or more octets, and contains the identity of the LAT port to use. The LAT Architecture allows this string to contain $ (dollar), - (hyphen), . (period), _ (underscore), numerics, upper and lower case alphabetics, and the ISO Latin-1

character set extension. All LAT string comparisons are case insensitive.

5.44. 属性与报文对应关系

下表列出了哪个属性可以出现在哪种类型的报文中，以及可以出现几次：

Request	Accept	Reject	Challenge	#	Attribute
0-1	0-1	0	0	1	User-Name
0-1	0	0	0	2	User-Password [注 1]
0-1	0	0	0	3	CHAP-Password [注 1]
0-1	0	0	0	4	NAS-IP-Address [注 2]
0-1	0	0	0	5	NAS-Port
0-1	0-1	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	0-1	0	0	10	Framed-Routing
0	0+	0	0	11	Filter-Id
0-1	0-1	0	0	12	Framed-MTU
0+	0+	0	0	13	Framed-Compression
0+	0+	0	0	14	Login-IP-Host
0	0-1	0	0	15	Login-Service
0	0-1	0	0	16	Login-TCP-Port
0	0+	0+	0+	18	Reply-Message
0-1	0-1	0	0	19	Callback-Number
0	0-1	0	0	20	Callback-Id
0	0+	0	0	22	Framed-Route
0	0-1	0	0	23	Framed-IPX-Network
0-1	0-1	0	0-1	24	State [注 1]
0	0+	0	0	25	Class
0+	0+	0	0+	26	Vendor-Specific
0	0-1	0	0-1	27	Session-Timeout
0	0-1	0	0-1	28	Idle-Timeout
0	0-1	0	0	29	Termination-Action
0-1	0	0	0	30	Called-Station-Id
0-1	0	0	0	31	Calling-Station-Id
0-1	0	0	0	32	NAS-Identifier [注 2]
0+	0+	0+	0+	33	Proxy-State
0-1	0-1	0	0	34	Login-LAT-Service
0-1	0-1	0	0	35	Login-LAT-Node
0-1	0-1	0	0	36	Login-LAT-Group
0	0-1	0	0	37	Framed-AppleTalk-Link
0	0+	0	0	38	Framed-AppleTalk-Network

0	0-1	0	0	39	Framed-AppleTalk-Zone
0-1	0	0	0	60	CHAP-Challenge
0-1	0	0	0	61	NAS-Port-Type
0-1	0-1	0	0	62	Port-Limit
0-1	0-1	0	0	63	Login-LAT-Port
Request	Accept	Reject	Challenge	#	Attribute

[注 1] 接入请求报文必须（MUST）包含 User-Password，CHAP-Password 或者 State 属性之一。接入请求报文中必须不能（MUST NOT）同时包含 User-Password 和 CHAP-Password 属性。如果将来的扩展允许携带其它类型的认证信息，扩展的属性可以替代接入请求报文中的 User-Password 和 CHAP-Password 属性。

[注 2] 接入请求报文必须（MUST）包含 NAS-IP-Address 或者 NAS-Identifier 属性，或者两者都包含。

下表说明上表字段的涵义：

0	该属性必须不能（MUST NOT）出现在该类型报文中。
0+	0 个或者多个该属性的实例可以（MAY）出现在该类型报文中。
0-1	0 个或者 1 个该属性的实例可以（MAY）出现在该类型报文中。
1	该属性必须且只能有（MUST）一个实例出现在该类型的报文中。

6. IANA 事项

本节提供了 IANA 关于和 RADIUS 协议相关的值的注册的指导。参考了 BCP 26 [13]。

在 RADIUS 中有三个需要注册的名称空间：报文类型代码，属性类型和属性值（对于某些属性）。

RADIUS 不想有意定义为通用的网路接入服务器管理协议，不应该（should not）分配和认证，授权和计费信息无关的属性。

6.1. 术语定义

下列使用的术语定义在 BCP 26 中：“名称空间”，“分配值”，“注册”。

下列使用的策略定义在 BCP 26 中：“私有用途”，“先来先得”，“专家检视”，“要求规范化”，“IETF 一致同意”，“标准协议化活动”。

6.2. 推荐的注册策略

注册需求应该（should）参考一下“指定专家”的意见，IESG 相关领域主席应该任命“指定专家”。

对于需要“专家检视”的注册需求，应该（should）请教一下 ietf-radius 邮件列表的专家。

报文类型代码域值取值范围为 1 到 254，其中 1-5，11-13 已经被分配出去了。由于新的报文类型会对互操作性有很大的影响。新的报文类型代码需要标准动作，应该从 14 开始分配。

属性类型取值范围为 1 到 255，是 RADIS 中最缺乏的资源。因此分配时必须（must）非常小心。属性值 1-53，55，60-88，90-91 已经被分配出去了，17 和 21 用来重用。由专家检视后，属性 17，21，54，56-59，89，92-191 可以（may）被分配并要求规范化。属性类型块（为了特定的目的一次超过 3 个）的分配应该（should）需要 IETF 一致同意。推荐（recommended）17 和 21 属性只在其它所有属性用尽后再使用。

需要注意的是，RADIUS 协议定义了厂商扩展机制（26 号属性），应该鼓励使用厂商扩展属性，而不是分配全局属性类型。否则对只有一个厂商的 RADIUS 协议实现的特定功能而分配全局属性类型，对互操作性是没有好处的。

像上面属性章节规定的：

属性类型值 192-223 是保留给实验用的，值 224-240 是保留给特定实现用的，值 241-255 是预留的，而且不应该（should not）使用它们。

因此属性值 192-240 考虑用于私有用途，值 241-255 需要标准协议化活动。

在 RADIUS 协议中的某些属性（如：NAS-Port-Type 属性）根据不同的涵义定义了一系列的值，每个属性可以有 40 亿个值。向列表中增加新值由 IANA 基于先来先得原则分配。

7. 举例

下面举了几个例子来说明报文流和典型属性的用法。这些例子无意穷举各种情况，其它的情况是可能出现的。例子中给出的报文是网络字节序的十六进制数据，使用的共享密钥为“xyzzy5461”。

7.1. 用户 telnet 到特定主机

IP 地址为 192.168.1.16 的 NAS 发送一个接入请求 UDP 报文给 RADIUS 服务器。表示一个名为 nemo 的用户在端口 3 使用密码“arctangent”登录。

请求认证字是一个 NAS 生成的 16 个字节的随机数。

User-Password 属性是占位 16 个字节的密码，末尾使用 null 填充满。然后再和 MD5（共享密码|请求认证字）异或。

```
   01 00 00 38 0f 40 3f 94 73 97 80 57 bd 83 d5 cb
98 f4 22 7a 01 06 6e 65 6d 6f 02 12 0d be 70 8d
93 d4 13 ce 31 96 e4 3f 78 2a 0a ee 04 06 c0 a8
01 10 05 06 00 00 00 03
```

```
    1 Code = Access-Request (1)
 1 ID = 0
```

```
 2 Length = 56
16 Request Authenticator

     Attributes:
 6  User-Name = "nemo"
18  User-Password
 6  NAS-IP-Address = 192.168.1.16
 6  NAS-Port = 3
```

RADIUS 服务器认证 nemo 用户，然后给 NAS 发送接入成功回应 UDP 报文，告诉 NAS 将 nemo 用户 telnet 到主机 192.168.1.3。

回应认证字是一个 16 字节的 MD5 校验码，对代码域（2），标识符域（0），长度域（38），上面的请求认证字，回应报文中的属性域以及共享密钥进行 MD5 加密生成回应认证字。

```
 02 00 00 26 86 fe 22 0e 76 24 ba 2a 10 05 f6 bf
9b 55 e0 b2 06 06 00 00 00 01 0f 06 00 00 00 00
0e 06 c0 a8 01 03

      1 Code = Access-Accept (2)
 1 ID = 0 (same as in Access-Request)
 2 Length = 38
16 Response Authenticator

     Attributes:
 6  Service-Type (6) = Login (1)
 6  Login-Service (15) = Telnet (0)
 6  Login-IP-Host (14) = 192.168.1.3
```

7.2. 用户使用 CHAP 认证

IP 地址为 192.168.1.16 的 NAS 发送接入请求 UDP 报文给 RADIUS 服务器，表示一个 flopsy 用户使用 PPP 协议在端口 20 使用 CHAP 认证方式登录。NAS 发送了 Service-Type 和 Framed-Protocol 属性，以提示 RADIUS 服务器该用户想使用 PPP 协议，尽管 NAS 不需要这样做。

请求认证字是一个 NAS 生成的 16 个字节的随机数，它也用来表示 CHAP 挑战字。

CHAP-Password 属性由 1 个字节的 CHAP ID（本例中为 22）以及后面的 16 个字节的 CHAP 回应组成。

```
01 01 00 47 2a ee 86 f0 8d 0d 55 96 9c a5 97 8e
0d 33 67 a2 01 08 66 6c 6f 70 73 79 03 13 16 e9
75 57 c3 16 18 58 95 f2 93 ff 63 44 07 72 75 04
06 c0 a8 01 10 05 06 00 00 00 14 06 06 00 00 00
02 07 06 00 00 00 01
```

```
 1 Code = 1     (Access-Request)
 1 ID = 1
 2 Length = 71
16 Request Authenticator

 Attributes:
 8  User-Name (1) = "flopsy"
19  CHAP-Password (3)
 6  NAS-IP-Address (4) = 192.168.1.16
 6  NAS-Port (5) = 20
 6  Service-Type (6) = Framed (2)
 6  Framed-Protocol (7) = PPP (1)
```

RADIUS 服务器认证 flopsy 用户，然后给 NAS 发送接入成功回应 UDP 报文，告诉 NAS 开始 PPP 服务，并且为用户从动态地址池中分配一个 IP 地址。

回应认证字是一个 16 字节的 MD5 校验码，对代码域（2），标识符域（1），长度域（56），上面的请求认证字，回应报文的属性域以及共享密钥进行 MD5 加密生成回应认证字。

```
02 01 00 38 15 ef bc 7d ab 26 cf a3 dc 34 d9 c0
3c 86 01 a4 06 06 00 00 00 02 07 06 00 00 00 01
08 06 ff ff ff fe 0a 06 00 00 00 02 0d 06 00 00
00 01 0c 06 00 00 05 dc

 1 Code = Access-Accept (2)
 1 ID = 1 (same as in Access-Request)
 2 Length = 56
16 Response Authenticator

     Attributes:
 6  Service-Type (6) = Framed (2)
 6  Framed-Protocol (7) = PPP (1)
 6  Framed-IP-Address (8) = 255.255.255.254
 6  Framed-Routing (10) = None (0)
 6  Framed-Compression (13) = VJ TCP/IP Header Compression (1)
 6  Framed-MTU (12) = 1500
```

7.3. 使用挑战回应卡认证

IP 地址为 192.168.1.16 的 NAS 发送一个接入请求 UDP 报文给 RADIUS 服务器，表示一个 mopsy 用户要在端口 7 登录，在本例中，假定用户输入密码“challenge”。
在本例中，由智能卡生成的挑战和回应分别是“32769430”和“99101462”。

请求认证字是一个由 NAS 生成的 16 个字节的随机数。

User-Password 属性是占位 16 个字节的密码，在本例中，密码为“challenge”，后面使用 null 填充满 16 个字节。然后再和 MD5（共享密码|请求认证字）异或。

```
01 02 00 39 f3 a4 7a 1f 6a 6d 76 71 0b 94 7a b9
30 41 a0 39 01 07 6d 6f 70 73 79 02 12 33 65 75
73 77 82 89 b5 70 88 5e 15 08 48 25 c5 04 06 c0
a8 01 10 05 06 00 00 00 07

 1 Code = Access-Request (1)
 1 ID = 2
 2 Length = 57
16 Request Authenticator

    Attributes:
 7 User-Name (1) = "mopsy"
18 User-Password (2)
 6  NAS-IP-Address (4) = 192.168.1.16
 6  NAS-Port (5) = 7
```

RADIUS 服务器决定挑战 mopsy 用户，需要发送回一个挑战字符串并等待回应，因此 RADIUS 服务器发送了一个接入挑战 UDP 报文给 NAS。

回应认证字是一个 16 字节的 MD5 校验码，对代码域（11），标识符域（2），长度域（78），上面的请求认证字，回应报文的属性域以及共享密钥进行 MD5 加密生成回应认证字。

Reply-Message 属性值为“Challenge 32769430. Enter response at prompt.”。

State 属性是一个随着用户的回应返回的神奇的 cookie，在本例中是一个 8 个字节的数据（33 32 37 36 39 34 33 30，十六进制）。

```
    0b 02 00 4e 36 f3 c8 76 4a e8 c7 11 57 40 3c 0c
71 ff 9c 45 12 30 43 68 61 6c 6c 65 6e 67 65 20
33 32 37 36 39 34 33 30 2e 20 20 45 6e 74 65 72
20 72 65 73 70 6f 6e 73 65 20 61 74 20 70 72 6f
6d 70 74 2e 18 0a 33 32 37 36 39 34 33 30

    1 Code = Access-Challenge (11)
 1 ID = 2 (same as in Access-Request)
 2 Length = 78
16 Response Authenticator

    Attributes:
48  Reply-Message (18)
10  State (24)
```

用户输入回应后，NAS 发送一个新的携带该回应的接入请求报文，其中包括 State 属性。

请求认证字是一个新的 16 字节随机数。

User-Password 属性是用户回应的 16 字节字符串，在本例中为“99101462”，后面用 null 填满 16 个字节，然后和 MD5（共享密钥|请求认证字）异或。

State 属性是接入挑战报文中的神奇 cookie，没有做修改。

```
01 03 00 43 b1 22 55 6d 42 8a 13 d0 d6 25 38 07
c4 57 ec f0 01 07 6d 6f 70 73 79 02 12 69 2c 1f
20 5f c0 81 b9 19 b9 51 95 f5 61 a5 81 04 06 c0
a8 01 10 05 06 00 00 00 07 18 10 33 32 37 36 39
34 33 30

     1 Code = Access-Request (1)
 1 ID = 3 (Note that this changes.)
 2 Length = 67
16 Request Authenticator

    Attributes:
 7  User-Name = "mopsy"
18  User-Password
 6  NAS-IP-Address (4) = 192.168.1.16
 6  NAS-Port (5) = 7
10  State (24)
```

回应是不正确的（为了举例之便），所以 RADIUS 服务器告诉 NAS 拒绝了试图的登录。

回应认证字是一个 16 字节的 MD5 校验码，对代码域（11），标识符域（3），长度域（20），上面的请求认证字，回应报文的属性域以及共享密钥进行 MD5 加密生成回应认证字。

```
03 03 00 14 a4 2f 4f ca 45 91 6c 4e 09 c8 34 0f
9e 74 6a a0

     1 Code = Access-Reject (3)
 1 ID = 3 (same as in Access-Request)
 2 Length = 20
16 Response Authenticator

    Attributes:
  (none, although a Reply-Message could be sent)
```

8. 安全事项

安全问题是本文的主题。

实践上，在每个 RADIUS 服务器中，都有一个联系用户名和认证信息（密钥）的数据库，不希望一个指定的命名用户使用多种方式认证。这样使得用户易受攻击，它可以从安全方法中协商一个最弱的安全方法。相反，每个命名用户应该（should）使用一种认证方式认证。如果一个用户需要在不同的环境下使用不同的认证方式，应该（SHOULD）使用不同的用户名，每一个用户名标识一种认证方式。

密码和其它的密钥应该（should）存储在各自的终端，对这些终端的访问应该尽可能地限制。理想的情况下，密钥应该（should）只允许执行认证功能的进程访问。

密钥应该（should）限制处理密钥条目的数量而分布式的机制，理想情况下，未授权的人不应该知道密钥。可以使用 SNMP 安全协议做到这一点，但是这种机制超出了本文的范围。

其它的分发机制当前正在进行研究和试验，SNMP 安全文档[14]也一个关于网路协议安全威胁的精彩观点.

在 5.2 节秒数的 User-Password 属性加密机制还没有在公开的文献中发表有足够数量的密码分析文章，在 IETF 社区的一些人认为这种方法可能没有提供对在 RADIUS 协议中传输密码的足够的安全保护[15]。用户应该（should）评估他们的威胁环境，考虑是否应该应用其它额外的安全机制。

9. 更改记录

下列是对 RFC 2138 做的修改：

字符串应该（should）使用 UTF-8 编码代替 US-ASCII 编码，一个字符占位 8 位。

整数和日期定义为 32 位无符号值。

修改了能够包含在接入挑战报文中属性列表，和属性表保持了一致。

User-Name 属性中提到了网络接入标识。

User-Name 属性现在可以（may）在接入成功回应报文中返回，这样可以在计费和 Rlogin 时使用返回的 User-Name 属性值。

为 Service-Type，Login-Service，Framed-Protocol，Framed-Compression 和 NAS-Port-Type 属性增添了新值。

NAS-Port 现在能够使用所有的 32 位。

样例现在包含了报文的 16 进制描述。

在判断报文重复时，UDP 源端口必须（must）做为条件之一用来匹配请求标识符。

在厂商定制属性中允许定义多个子属性。

接入请求报文中现在需要包含 NAS-IP-Address 或者 NAS-Identifier 属性（或者可以包含两者）。

在操作章节增加了说明，进一步说明了代理，重传和心跳。

如果相同类型的多个属性同时出现，任何代理都必须（MUST）保留相同类型的属性顺序。

进一步阐述了 Proxy-State 属性。

进一步阐明了属性必须不能（must not）依赖于在报文中的位置，只要相同类型的属性保持顺序即可。

增加了 IANA 事项章节。

在"操作"章节下修改了"代理"小节。

Framed-MTU 属性现在能够做为提示在接入请求报文中发送。

修改和安全注意事项

文本字符串指明做为字符串的子集，阐述了 UTF-8 的用法。

10. 参考文献

[1] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March, 1997.

[3] Rivest, R. and S. Dusse, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[4] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[5] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[6] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC1700, October 1994.

[7] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC2279, January 1998.

[8] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC2486, January 1999.

[9] Kaufman, C., Perlman, R., and Speciner, M., "Network Security: Private Communications in a Public World", Prentice Hall, March 1995, ISBN 0-13-061466-1.

[10] Jacobson, V., "Compressing TCP/IP headers for low-speed seriallinks", RFC 1144, February 1990.

[11] ISO 8859. International Standard -- Information Processing --8-bit Single-Byte Coded Graphic Character Sets -- Part 1: Latin Alphabet No. 1, ISO 8859-1:1987.

[12] Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T.Coradetti, "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

[13] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANAConsiderations Section in RFCs", BCP 26, RFC 2434, October 1998.

[14] Galvin, J., McCloghrie, K. and J. Davin, "SNMP Security Protocols", RFC 1352, July 1992.

[15] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes Vol.2 No. 2, Summer 1996.

11. Acknowledgements

RADIUS was originally developed by Steve Willens of Livingston Enterprises for their PortMaster series of Network Access Servers.