检查RADIUS的工作方式

目录

简介

本文档介绍RADIUS服务器及其工作原理。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

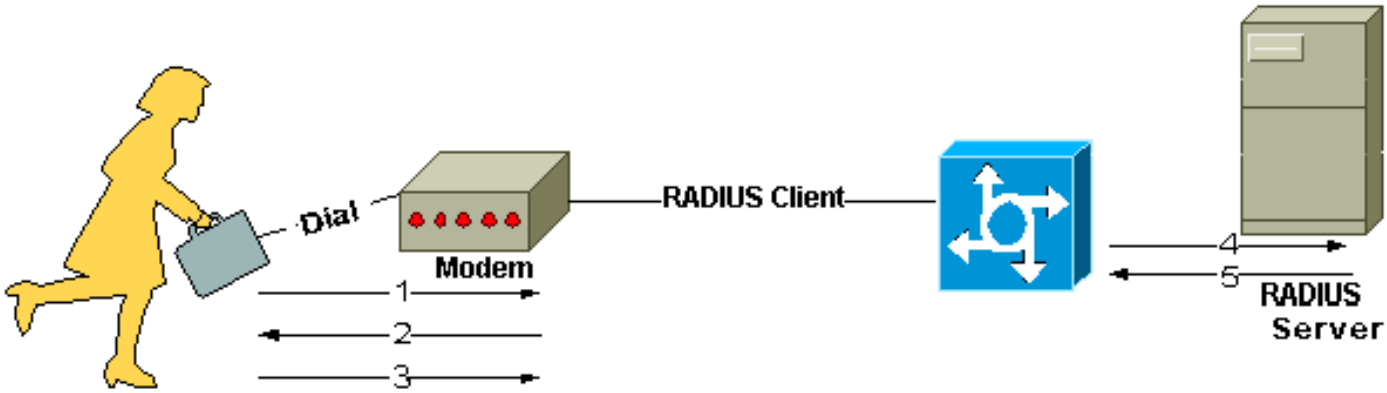
远程身份验证拨入用户服务 (RADIUS) 协议由 Livingston Enterprises, Inc. 开发，用作接入服务器身份验证和记帐协议。RADIUS 规范 RFC 2865 淘汰了 RFC 2138。RADIUS 记帐标准 RFC 2866 淘汰了 RFC 2139。

网络接入服务器 (NAS) 和 RADIUS 服务器之间的通信基于用户数据报协议 (UDP)。通常，RADIUS 协议被视为无连接服务。与服务器可用性、重新传输和超时相关的问题由启用了 RADIUS 的设备而不是传输协议来处理。

RADIUS是客户端/服务器协议

RADIUS客户端通常是NAS，而RADIUS服务器通常是在UNIX或Windows NT计算机上运行的守护进程。客户端将用户信息传递到指定的RADIUS服务器，并对返回的响应执行操作。RADIUS 服务器收到用户连接请求，对用户进行身份验证，然后返回客户端向用户提供服务所必需的配置信息。RADIUS 服务器可用作其他 RADIUS 服务器或其他类型身份验证服务器的代理客户端。

此图显示拨入用户和 RADIUS 客户端和服务器之间的交互。



拨入用户与RADIUS客户端和服务器之间的交互

1. 用户启动对 NAS 的 PPP 身份验证。
2. NAS 提示输入用户名和口令（如果使用口令身份验证协议 [PAP]）或质询（如果使用质询握手身份验证协议 [CHAP]）。
3. 用户回复。
4. RADIUS 客户端将用户名和加密口令发送到 RADIUS 服务器。
5. RADIUS 服务器以 Accept、Reject 或 Challenge 做出响应。
6. RADIUS 客户端对与 Accept 或 Reject 绑定的服务和服务参数进行操作。

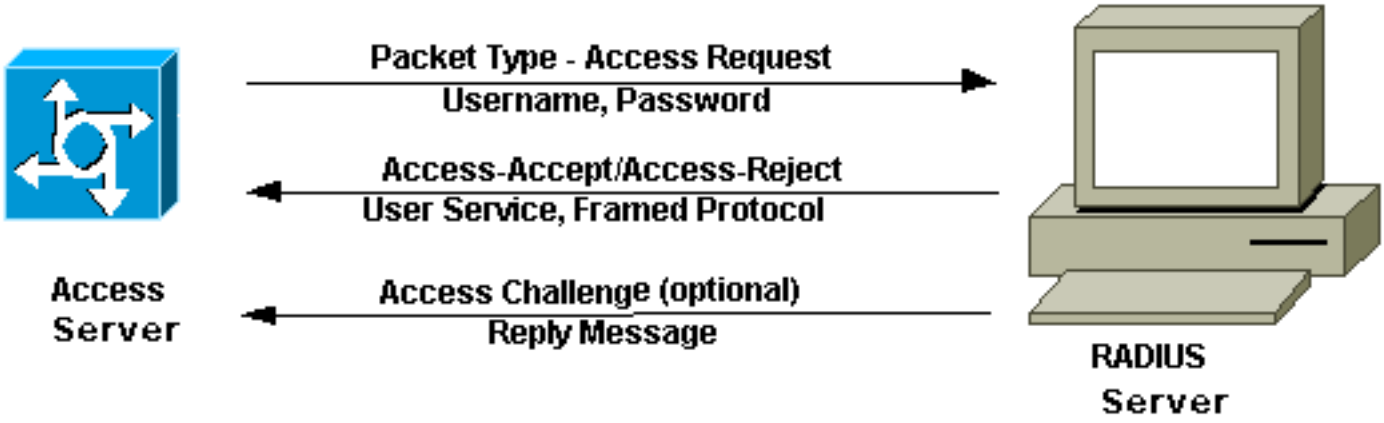
认证 和 授权

RADIUS 服务器可以支持多种对用户进行身份验证的方法。向其提供用户指定的用户名和原始口令时，它可以支持 PPP、PAP 或 CHAP、UNIX 登录及其他身份验证机制。

通常，用户登录包含从 NAS 到 RADIUS 服务器的查询 (Access-Request) 和来自服务器的对应响应（Access-Accept 或 Access-Reject）。Access-Request 数据包包含用户名、加密口令、NAS IP 地址和端口。RADIUS的早期部署使用UDP端口号1645完成，该端口号与“数据度量”服务冲突。由于此冲突，RFC 2865 为 RADIUS 正式指定了端口号 1812。大多数 Cisco 设备和应用程序提供对其中任何一个端口号设置的支持。请求的格式还提供了有关用户希望启动的会话类型的信息。例如，如果以字符模式提供查询，则推断为“服务类型 = Exec 用户”，但如果以 PPP 数据包模式提供请求，则推断为“服务类型 = 成帧用户”和“成帧类型 = PPP”。

当 RADIUS 服务器收到来自 NAS 的 Access-Request 消息时，它会在数据库中搜索列出的用户名。如果数据库中不存在该用户名，则加载默认配置文件，或RADIUS服务器立即发送Access-Reject消息。此Access-Reject消息可随附指示拒绝原因的文本消息。

在 RADIUS 中，身份验证和授权结合在一起。如果找到用户名且密码正确，则RADIUS服务器会返回Access-Accept响应，其中包括描述要用于此会话的参数的属性 — 值对列表。典型的参数包括服务类型（shell 或成帧）、协议类型、要分配给用户的 IP 地址（静态或动态）、要应用的访问列表，或要在 NAS 路由表中安装的静态路由。RADIUS服务器中的配置信息定义可在NAS上安装的设备。下图说明了RADIUS身份验证和授权顺序。



RADIUS身份验证和授权序列

记账

RADIUS 协议的记帐功能可独立于 RADIUS 身份验证或授权使用。RADIUS记账功能允许在会话开始和结束时发送数据，这表示会话期间使用的资源量（例如时间、数据包、字节等）。Internet服务提供商(ISP)可以使用RADIUS访问控制和记帐软件来满足特殊的安全和计费需求。对于大多数 Cisco 设备，用于 RADIUS 的记帐端口是 1646，但也可以是 1813（由于 RFC 2139 中指定的端口更改）。

客户端和 RADIUS 服务器之间的事务通过使用从未在网络上发送的共享密钥进行身份验证。此外，用户密码会在客户端和RADIUS服务器之间加密发送，以消除在不安全网络上侦听的人确定用户密码的可能性。

相关信息

- **身份验证协议**
- **请求注解 (RFC)**
- **技术支持 - Cisco Systems**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。