RADIUS如何工作？

Contents

Introduction

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。

Prerequisites

Requirements

本文档没有任何特定的前提条件。

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

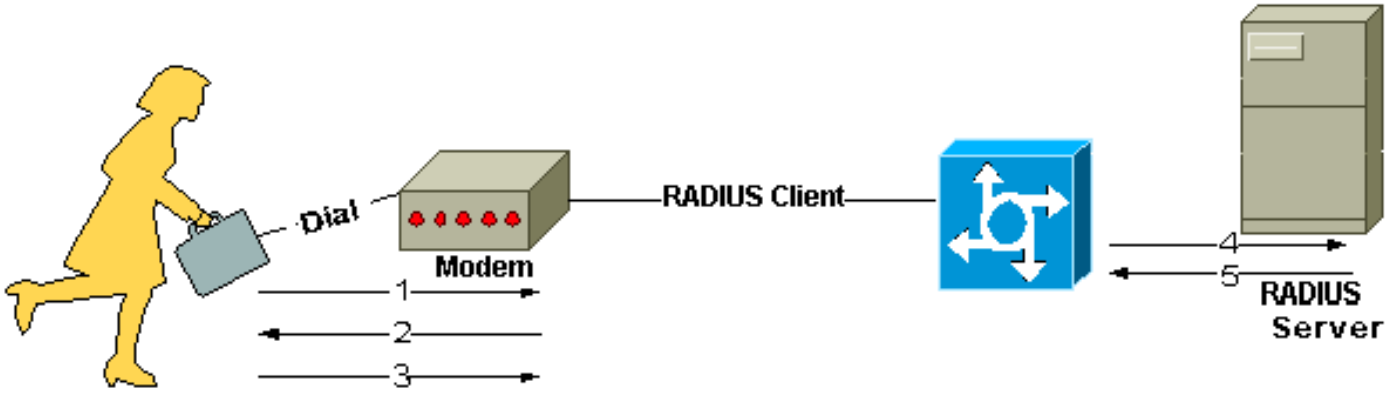
背景信息

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 是一个客户端/服务器协议。RADIUS 客户端通常是 NAS，RADIUS 服务器通常是在 UNIX 或 Windows NT 计算机上运行的后台程序进程。客户端将用户信息传送到指定 RADIUS 服务器并对

返回的响应进行操作。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。



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。

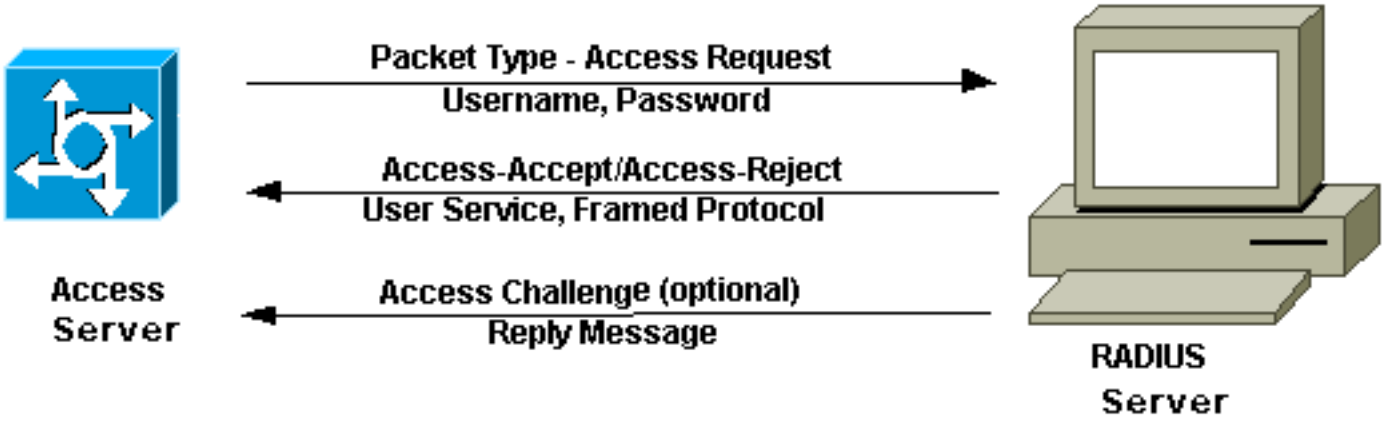
认证和授权

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。早期 RADIUS 部署是使用 UDP 端口号 1645 实施的，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。如果用户名在数据库中不存在，则要么加载默认配置文件，要么 RADIUS 服务器立即发送一条 Access-Reject 消息。此 Access-Reject 消息可能伴随一条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。如果找到用户名且口令正确，则 RADIUS 服务器返回 Access-Accept 响应，其中包括一个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要在 NAS 上安装的程序。下图说明 RADIUS 身份验证和授权序列。



认为

RADIUS 协议的记帐功能可独立于 RADIUS 身份验证或授权使用。RADIUS 记帐功能允许在会话开始和结束时发送用于指示在会话期间使用的资源量（如时间、数据包、字节等）的数据。Internet 服务提供商 (ISP) 可使用 RADIUS 访问控制和记帐软件来满足特殊的安全和计费需要。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，用户口令以加密形式在客户端和 RADIUS 服务器之间发送，以消除在不安全网络上监听的用户能够确定用户口令的可能性。

Related Information

- RADIUS 技术支持页
- 请求注解 (RFC)
- Technical Support - Cisco Systems