檢查RADIUS的運作方式

目錄

簡介

本檔案將說明RADIUS伺服器的性質及其運作方式。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

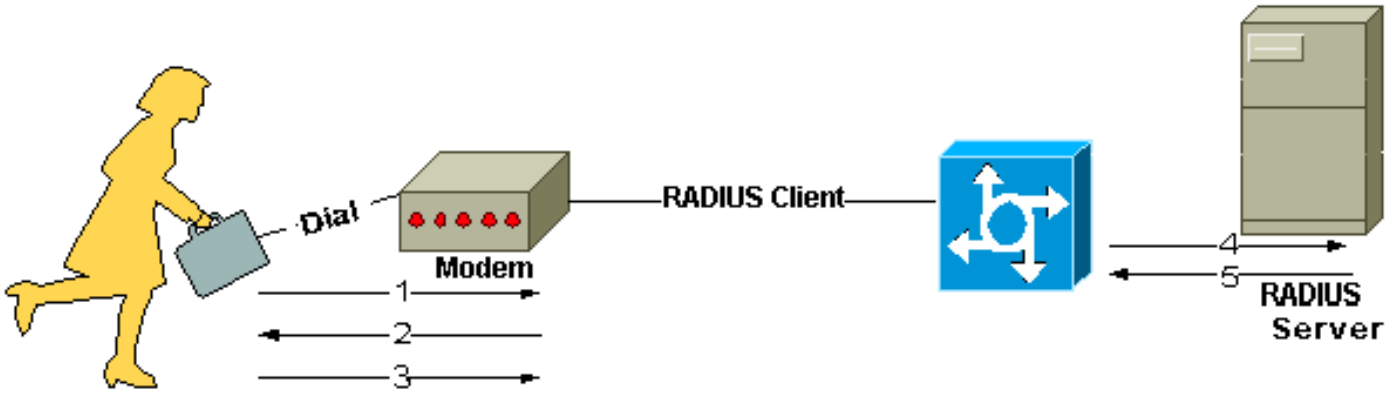
Livingston Enterprises, Inc. 開發了遠端驗證撥入使用者服務 (RADIUS) 通訊協定，以做為存取伺服器驗證和計量的通訊協定。RADIUS 規格 RFC 2865 取代了 RFC 2138。RADIUS 計量標準 RFC 2866 取代了 RFC 2139。

網路訪問伺服器(NAS)和RADIUS伺服器之間的通訊基於使用者資料包協定(UDP)。一般來說，RADIUS通訊協定視為無連線服務。與伺服器可用性、重新傳輸和超時相關的問題由啟用了RADIUS的裝置（而不是傳輸協定）處理。

RADIUS是使用者端/伺服器通訊協定

RADIUS使用者端通常是NAS，而RADIUS伺服器通常是在UNIX或Windows NT機器上執行的守護程式程式。使用者端將使用者資訊傳遞到指定的RADIUS伺服器，並對傳回的回應執行動作。RADIUS伺服器會收到使用者連線要求、驗證使用者，然後傳回使用者端向使用者提供服務所需的組態資訊。RADIUS伺服器可以作為其他RADIUS伺服器或其他型別驗證伺服器的代理使用者端。

下圖顯示撥入使用者與RADIUS使用者端和伺服器之間的互動。



撥入使用者與RADIUS使用者端和伺服器之間的互動

1. 使用者向NAS發起PPP身份驗證。
2. NAS提示輸入使用者名稱和密碼（如果密碼身份驗證協定[PAP]）或質詢（如果質詢握手身份驗證協定[CHAP]）。
3. 使用者應答。
4. RADIUS使用者端將使用者名稱和加密密碼傳送到RADIUS伺服器。
5. RADIUS伺服器使用Accept、Reject或Challenge進行響應。
6. RADIUS使用者端會根據與「接受」或「拒絕」捆綁在一起的服務和服務引數執行操作。

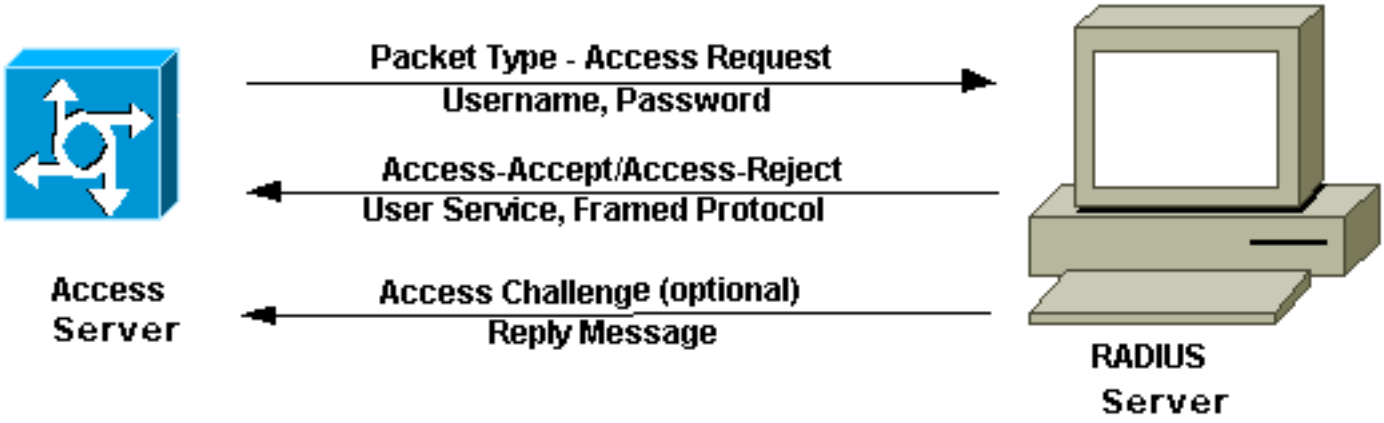
驗證與授權

RADIUS伺服器支援各種驗證使用者的方法。若隨使用者指定的使用者名稱和原始密碼提供，其可支援PPP、PAP或CHAP、UNIX登入和其他驗證機制。

通常，使用者登入包含從NAS到RADIUS伺服器的查詢（訪問請求）和從伺服器發出的相應響應（訪問接受或訪問拒絕）。Access-Request資料包包含使用者名稱、加密密碼、NAS IP地址和埠。RADIUS的早期部署使用UDP埠號1645完成，該埠號與「資料度量」服務衝突。由於此衝突，RFC 2865已正式為RADIUS分配埠號1812。大多數思科裝置和應用支援任一埠號集。請求的格式還提供了有關使用者想要啟動的會話型別的資訊。例如，如果查詢以字元模式顯示，則推理為「Service-Type = Exec-User」，但如果請求以PPP資料包模式顯示，則推理為「Service Type = Framed User」和「Framed Type = PPP」。

當RADIUS伺服器收到來自NAS的存取要求時，它會在資料庫中搜尋列出的使用者名稱。如果資料庫中不存在該使用者名稱，則載入預設配置檔案，或RADIUS伺服器立即傳送訪問拒絕消息。此Access-Reject消息可隨附一條文本消息，指出拒絕的原因。

在RADIUS中，驗證和授權是耦合在一起的。如果找到使用者名稱且密碼正確，則RADIUS伺服器將返回訪問接受響應，該響應包括描述要用於此會話的引數的屬性 — 值對清單。典型的引數包括服務型別（外殼或框架）、協定型別、分配使用者的IP地址（靜態或動態）、要應用的訪問清單，或要在NAS路由表中安裝的靜態路由。RADIUS伺服器中的配置資訊定義了NAS上可以安裝的內容。下圖說明RADIUS身份驗證和授權順序。



RADIUS驗證和授權順序

會計

RADIUS通訊協定的計費功能可獨立於RADIUS驗證或授權使用。RADIUS計費功能允許在會話開始和結束時傳送資料，這表示會話期間使用的資源量（如時間、資料包、位元組等）。Internet服務提供商(ISP)可以使用RADIUS訪問控制和記帳軟體來滿足特定的安全和計費需求。大多數Cisco裝置的RADIUS記帳埠是1646，但也可以是1813(因為RFC 2139中指定的埠更改)。

用戶端和 RADIUS 伺服器之間的交易是透過使用共用金鑰進行驗證，而這個共用金鑰絕不會透過網路傳送。此外，在使用者端和RADIUS伺服器之間傳送使用者密碼時經過加密處理，以消除在不安全網路上窺探的有心人士能確定使用者密碼的可能性。

相關資訊

- **驗證通訊協定**
- **要求建議 (RFC)**
- **技術支援 - Cisco Systems**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。