Untersuchen der Funktionsweise von RADIUS

Inhalt

Einleitung

In diesem Dokument wird beschrieben, was ein RADIUS-Server ist und wie er funktioniert.

Voraussetzungen

Anforderungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Das RADIUS-Protokoll (Remote Authentication Dial-In User Service) wurde von Livingston Enterprises, Inc., als Authentifizierungs- und Kontoführungsprotokoll für Zugriffsserver entwickelt. Die RADIUS-Spezifikation RFC 2865 ersetzt RFC 2138. Der RADIUS-Rechnungslegungsstandard

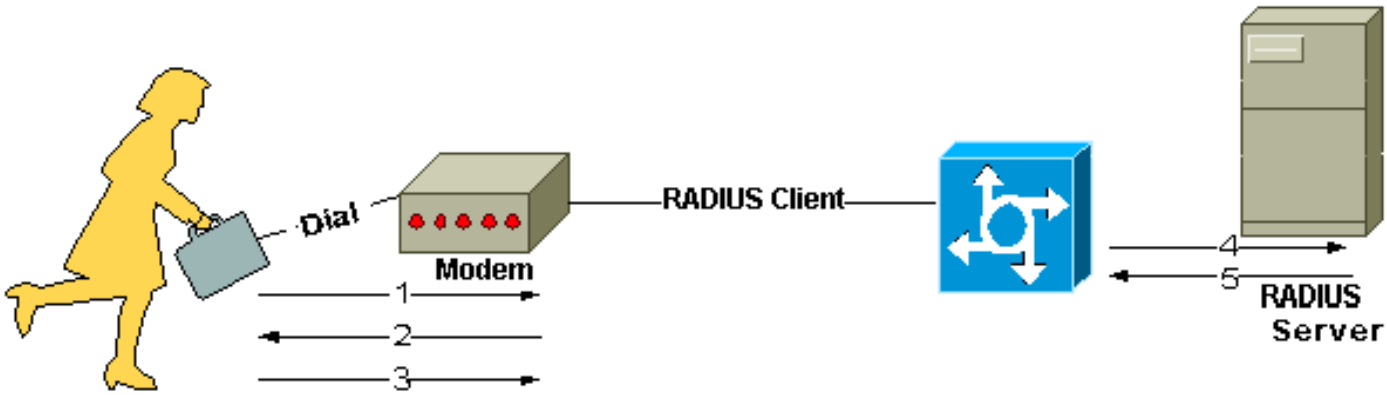
RFC 2866 ersetzt RFC 2139.

Die Kommunikation zwischen einem Netzwerkzugriffsserver (NAS) und einem RADIUS-Server basiert auf dem User Datagram Protocol (UDP). Im Allgemeinen wird das RADIUS-Protokoll als verbindungsloser Dienst betrachtet. Probleme im Zusammenhang mit der Serververfügbarkeit, der erneuten Übertragung und Zeitüberschreitungen werden von den RADIUS-fähigen Geräten und nicht vom Übertragungsprotokoll behandelt.

RADIUS ist ein Client/Server-Protokoll

Der RADIUS-Client ist in der Regel ein NAS, und der RADIUS-Server ist in der Regel ein Daemon-Prozess, der auf einem UNIX- oder Windows NT-System ausgeführt wird. Der Client leitet Benutzerinformationen an festgelegte RADIUS-Server weiter und reagiert entsprechend der zurückgegebenen Antwort. RADIUS-Server empfangen Benutzerverbindungsanforderungen, authentifizieren den Benutzer und geben dann die erforderlichen Konfigurationsinformationen zurück, damit der Client dem Benutzer den Dienst bereitstellen kann. Ein RADIUS-Server kann als Proxyclient für andere RADIUS-Server oder andere Authentifizierungsserver fungieren.

Diese Abbildung zeigt die Interaktion zwischen einem Einwählbenutzer und dem RADIUS-Client und -Server.



Interaktion zwischen Einwahlbenutzer und RADIUS-Client und -Server

1. Der Benutzer initiiert die PPP-Authentifizierung am NAS.
2. NAS fordert Benutzername und Kennwort (wenn Password Authentication Protocol [PAP]) oder Abfrage (wenn Challenge Handshake Authentication Protocol [CHAP]) an.
3. Der Benutzer antwortet.
4. Der RADIUS-Client sendet Benutzernamen und verschlüsseltes Kennwort an den RADIUS-Server.
5. Der RADIUS-Server antwortet mit "Accept", "Reject" oder "Challenge".
6. Der RADIUS-Client reagiert auf Services und Dienstparameter, die mit "Annehmen" oder "Ablehnen" gebündelt sind.

Authentifizierung und Autorisierung

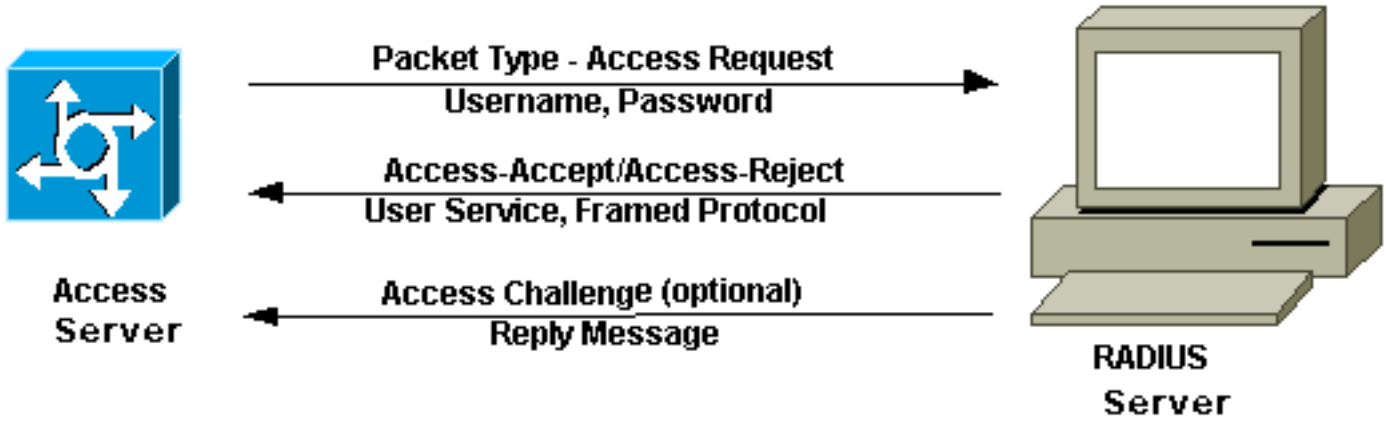
Der RADIUS-Server kann verschiedene Methoden zur Benutzerauthentifizierung unterstützen. Wenn der Benutzername und das ursprüngliche Kennwort vom Benutzer bereitgestellt werden, kann dies PPP, PAP oder CHAP, UNIX-Anmeldung und andere Authentifizierungsmechanismen unterstützen.

In der Regel besteht eine Benutzeranmeldung aus einer Abfrage (Access-Request) vom NAS zum

RADIUS-Server und einer entsprechenden Antwort (Access-Accept oder Access-Reject) vom Server. Das Access-Request-Paket enthält den Benutzernamen, das verschlüsselte Kennwort, die NAS-IP-Adresse und den Port. Die frühe Bereitstellung von RADIUS erfolgte über den UDP-Port 1645, was in Konflikt mit dem Dienst "Data Metrics" (Datenmetriken) stand. Aufgrund dieses Konflikts wurde RFC 2865 der offiziellen Port-Nummer 1812 für RADIUS zugewiesen. Die meisten Geräte und Anwendungen von Cisco unterstützen beide Port-Nummern. Das Format der Anforderung enthält auch Informationen über den Sitzungstyp, den der Benutzer initiieren möchte. Wenn die Abfrage z. B. im Zeichenmodus dargestellt wird, lautet die Schlussfolgerung "Service-Type = Exec-User". Wenn die Anforderung jedoch im PPP-Paketmodus dargestellt wird, lautet die Schlussfolgerung "Service Type = Framed User" und "Framed Type = PPP".

Wenn der RADIUS-Server die Access-Request vom NAS empfängt, sucht er in einer Datenbank nach dem aufgeführten Benutzernamen. Wenn der Benutzername nicht in der Datenbank vorhanden ist, wird entweder ein Standardprofil geladen, oder der RADIUS-Server sendet sofort eine Access-Reject-Nachricht. Dieser Access-Reject-Nachricht kann eine Textnachricht beigefügt werden, die den Grund für die Ablehnung angibt.

In RADIUS sind Authentifizierung und Autorisierung miteinander gekoppelt. Wenn der Benutzername gefunden wurde und das Kennwort korrekt ist, gibt der RADIUS-Server eine Access-Accept-Antwort zurück, die eine Liste von Attribut-Wert-Paaren enthält, die die für diese Sitzung zu verwendenden Parameter beschreiben. Zu den typischen Parametern gehören der Servicetyp (Shell oder Frame), der Protokolltyp, die IP-Adresse für die Zuweisung des Benutzers (statisch oder dynamisch), die anzuwendende Zugriffsliste oder eine statische Route für die Installation in der NAS-Routing-Tabelle. Die Konfigurationsinformationen im RADIUS-Server legen fest, was auf dem NAS installiert werden kann. Die folgende Abbildung zeigt die RADIUS-Authentifizierungs- und -Autorisierungssequenz.



RADIUS-Authentifizierungs- und -Autorisierungssequenz

Buchhaltung

Die Accounting-Funktionen des RADIUS-Protokolls können unabhängig von der RADIUS-Authentifizierung oder -Autorisierung verwendet werden. Die RADIUS-Abrechnungsfunktionen ermöglichen das Senden von Daten zu Beginn und am Ende einer Sitzung. Damit wird die Menge der während der Sitzung verwendeten Ressourcen (z. B. Zeit, Pakete, Bytes usw.) angegeben. Ein Internetdienstanbieter (ISP) kann RADIUS-Zugriffskontroll- und -Abrechnungssoftware verwenden, um spezielle Sicherheits- und Abrechnungsanforderungen zu erfüllen. Der Accounting-Port für RADIUS für die meisten Cisco Geräte ist 1646, kann aber auch 1813 sein (aufgrund der in RFC 2139 festgelegten Portänderung).

Transaktionen zwischen dem Client und dem RADIUS-Server werden mithilfe eines gemeinsamen

geheimen Schlüssels authentifiziert, der nie über das Netzwerk gesendet wird. Darüber hinaus werden Benutzerkennwörter verschlüsselt zwischen dem Client und dem RADIUS-Server gesendet, um die Möglichkeit zu vermeiden, dass jemand, der in einem unsicheren Netzwerk schnüffelt, ein Benutzerkennwort ermitteln kann.

Zugehörige Informationen

- Authentifizierungsprotokolle
- Request For Comments (RFCs)
- Technischer Support – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.