Remote Authentication Dial-In User Service (RADIUS)

Inhalt

[Was ist RADIUS? 2](#_Toc370568458)

[Funktionsweise 2](#_Toc370568459)

[Authentifizierung und Autorisierung 3](#_Toc370568460)

[Accounting 3](#_Toc370568461)

[Proxyfunktionalität und Sicherheit 4](#_Toc370568462)

# Was ist RADIUS?

RADIUS ist ein Client-Server Protokoll zur Authentifizierung (Identifizierung, wer), Autorisierung (Dienste, was) und zum Accounting (Umfang, wie viel), also ein Triple-A System, für Einwahlverbindungen in ein Computernetz. Aufgrund seiner weiten Verbreitung und seinem weiten Support wird RADIUS sehr oft von ISPs benutzt um deren Verbindungen zu managen.

Es läuft auf dem Application Layer des ISO/OSI-Referenzmodells und benutzt UDP zur Übertragung. Alle Komponenten die den Zugriff auf das Netzwerk kontrollieren (VPN-Server, Netzwerkswitch, NAS, etc.) beinhalten einen RADIUS Client als Komponente welche mit dem RADIUS-Server kommuniziert.

RADIUS wird hauptsächlich dazu verwendet um Roaming zwischen ISPs zu erleichtern.

RADIUS benutzt standardmäßig den UDP Port 1812 für die Authentifizierung und den UDP Port 1813 für das Accounting. Alternativ werden die Ports 1645 und 1646 benutzt.

# Funktionsweise

Der Grundbaustein von RADIUS ist ein zentraler RADIUS-Server, an den sich die Clients im physikalischen oder virtuellen (VPN) Netzwerk, zur Authentifizierung wenden. Der Server übernimmt hierbei die komplette Überprüfung von Benutzername und Passwort. Außerdem stellt der RADIUS-Server diverse Parameter für die Verbindung zum Client bereit. Diese Daten werden vom Server direkt aus Konfigurationsdateien und/oder aus einer Datenbank ausgelesen. Es kann auch sein dass der RADIUS-Server diese Informationen erst von anderen Servern anfragen muss.

Durch diese Funktionsweise können mit einem RADIUS-Server die kompletten Einstellungen von allen Benutzern zentral verwaltet werden. Dazu gehören Up- und Downloadspeed, maximale Anzahl der B-Kanäle bei ISDN oder auch Parameter wie IP- oder Routing-Parameter.

Der große Vorteil von RADIUS ist, dass der Benutzer nur einmalig zu registrieren ist und dann zentral Verwaltet werden kann und von überall innerhalb des Netzwerkes verfügbar ist.

Kombiniert man DHCP und PPP kann man sich in RADIUS-Systemen automatisch einwählen.

# Authentifizierung und Autorisierung

Zuerst fragt der RADIUS-Client mittels RADIUS: Access-Request beim RADIUS-Server an. Der Server kann dann auf 3 verschiedene Arten reagieren.

* Access-Reject
  + Hierbei wird dem Benutzer der Zugriff auf alle Netzwerkressourcen verwehrt. Der Grund dafür können eine fehlgeschlagene „proof of identification“ oder ein unbekannter/inaktiver Account sein.
* Access-Challenge
  + Bei einer Access-Challenge verlangt der RADIUS-Server weitere Informationen vom User, etwa ein sekundäres Passwort, ein PIN-Code, eine Smartcard oder ähnliches.

Access-Challenge wird auch benutzt wenn die Verbindung zwischen RADIUS-Client und RADIUS-Server getunnelt ist.

* Access-Accept
  + Der Zugriff ist bestätigt. Sobald der User authentifiziert ist überprüft der RADIUS-Server regelmäßig ob der User autorisiert ist die Services im Netzwerk zu benutzen welche er anfragt. Diese Informationen sind in einer lokalen Datenbank gespeichert oder können in einer externen Ressource wie ein LDAP oder Active Directory Verzeichnis gespeichert sein.

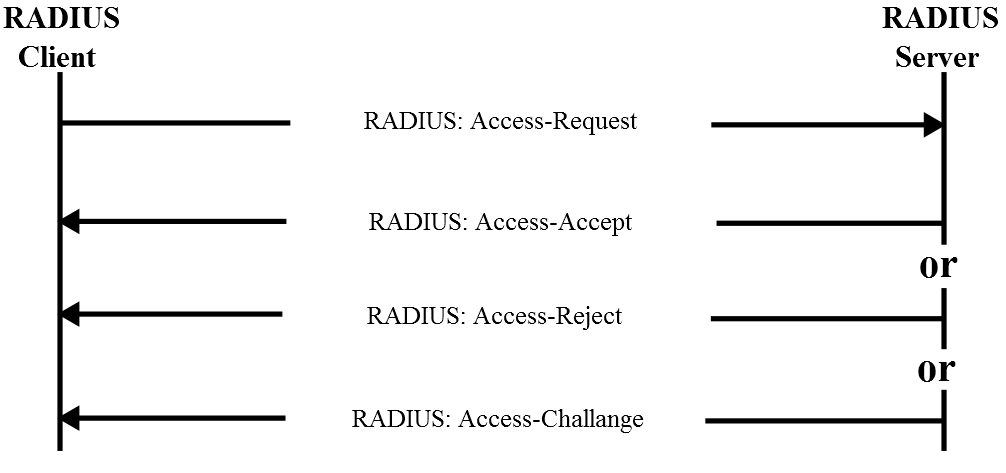


Abbildung So sieht der Verbindungsaufbau von RADIUS-Client zu RADIUS-Server aus.

# Accounting

Das Accounting für RADIUS ist in RFC 2866 detailliert beschrieben und definiert.

Sobald dem User der Netzwerkzugriff erlaubt wurde, schickt der NAS dem RADIUS-Server einen Accounting Start Request. Der RADIUS-Server antwortet sobald er durch den Accounting Start die Useridentifikation, Netzwerkadresse, point of attachment und deine eindeutige Session-ID bekommen hat.

Danach schickt der NAS ein Accounting Interim Update um den RADIUS-Server auf dem neuesten Stand der Session zu halten. Diese Updates beinhalten meistens die Dauer der aktuellen Session sowie den Datenverbrauch.

Wenn der User den Netzwerkzugriff beendet, schickt der NAS ein Accounting Stop an den RADIUS-Server mit den finalen Informationen über die Sitzung. Diese Infos beinhalten unter anderem die übertragenen Pakete, die übertragenen Daten, den Grund für den Disconnect, etc.

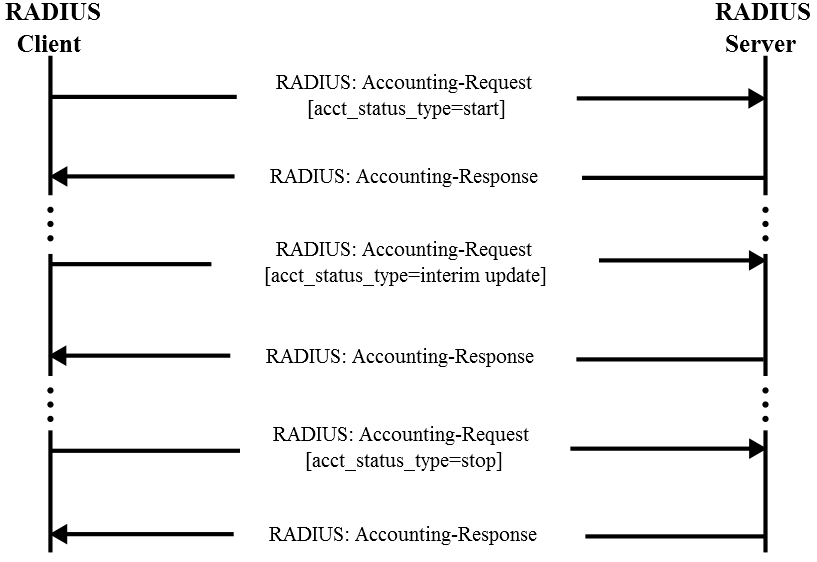


Abbildung Accounting-Informationen werden ausgetauscht.

# Proxyfunktionalität und Sicherheit

Wenn ein RADIUS-Server eine AAA-Anfrage mit einem Realm (Prefix/Postfix, Server) erhält, durchsucht der RADIUS-Server eine Tabelle mit konfigurierten Realms. Wenn der Realm bekannt ist, wird die Anfrage über eben diesen Realm vermittelt (Proxy).

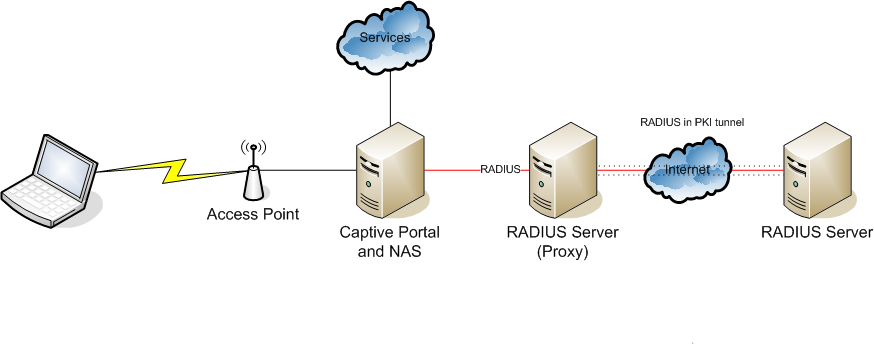


Abbildung Eine Anfrage über einen RADIUS-Server als Proxy.

Wenn man einen RADIUS-Server für Roaming benutzt treten diverse Sicherheitsbedenken auf. Deshalb bauen die meisten Roamingpartner zwischen ihren RADIUS-Servern eine sichere Verbindung (Tunneling) auf, um so zu verhindern, dass sensible Informationen wie Username und Password auszulesen sind.

Das RADIUS-Protokoll überträgt Passwörter nicht im Klartext zwischen dem NAS und dme RADIUS-Server. Stattdessen wird ein „shared secret“ in Verbindung mit einem MD5-Hash benutzt, um so das „shared secret“ zu verschlüsseln/obfuscaten. Diese Implementierung von Sicherheitsmaßnahmen ist nicht darauf ausgelegt sehr stark zu sein und die Userdaten zu schätzen da meistens zusätzliche Sicherheitsmaßnahmen wie IPsec benutzt werden um den Traffic zwischen RADIUS-Server und NAS zu schützen.