Onderzoek hoe de RADIUS werkt

Inhoud

Inleiding

Dit document beschrijft wat een RADIUS-server is en hoe deze werkt.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg [Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.](#)

Achtergrondinformatie

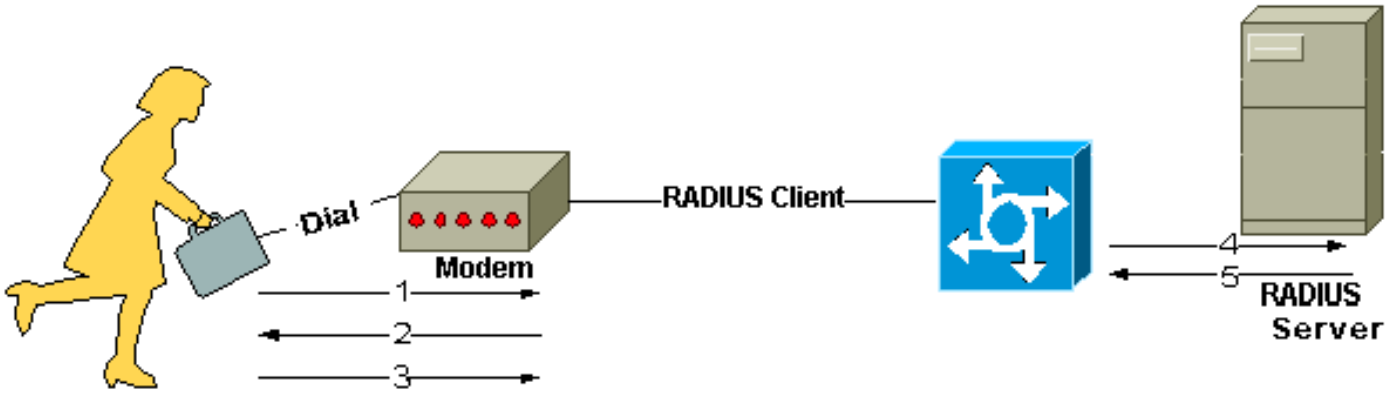
Het RADIUS-protocol (Remote Authentication Dial-In User Service) is door Livingston Enterprises, Inc. ontwikkeld als een protocol voor verificatie en accounting van de toegangsserver. De RADIUS-specificatie [RFC 2865 maakt RFC 2138 overbodig.](#) De RADIUS-accountingstandaard [RFC 2866 maakt RFC 2139 overbodig.](#)

De communicatie tussen een netwerktoegangsserver (NAS) en een RADIUS-server is gebaseerd op het User Datagram Protocol (UDP). Over het algemeen wordt het RADIUS-protocol beschouwd als een service zonder verbindingen. Problemen in verband met de beschikbaarheid van de server, hertransmissies en time-outs worden afgehandeld door de RADIUS-apparaten en niet door het transmissieprotocol.

RADIUS is een client/server-protocol

De RADIUS-client is doorgaans een NAS en de RADIUS-server is meestal een daemon-proces dat op een UNIX- of Windows NT-systeem wordt uitgevoerd. De client geeft gebruikersinformatie door aan aangewezen RADIUS-servers en reageert op de teruggestuurde reactie. RADIUS-servers ontvangen verzoeken voor gebruikersverbindingen, verifiëren de gebruiker en bieden vervolgens de configuratie-informatie die nodig is voor de client om de service aan de gebruiker te leveren. Een RADIUS-server kan als een proxyclient fungeren voor andere RADIUS-servers of andere soorten verificatieservers.

Deze figuur toont de interactie tussen een inbelgebruiker, de RADIUS-client en de server.



Interactie tussen inbelgebruiker en de RADIUS-client en -server

1. De gebruiker initieert PPP-verificatie op de NAS.
2. De NAS vraagt om een gebruikersnaam en wachtwoord (bij Password Authentication Protocol [PAP]) of om een challenge (bij Challenge Handshake Authentication Protocol [CHAP]).
3. De gebruiker reageert.
4. De RADIUS-client stuurt de gebruikersnaam en het versleutelde wachtwoord naar de RADIUS-server.
5. De RADIUS-server reageert met Accept, Reject of Challenge.
6. De RADIUS-client handelt op basis van de services en serviceparameters die met Accept of Reject zijn gebundeld.

Verificatie en autorisatie

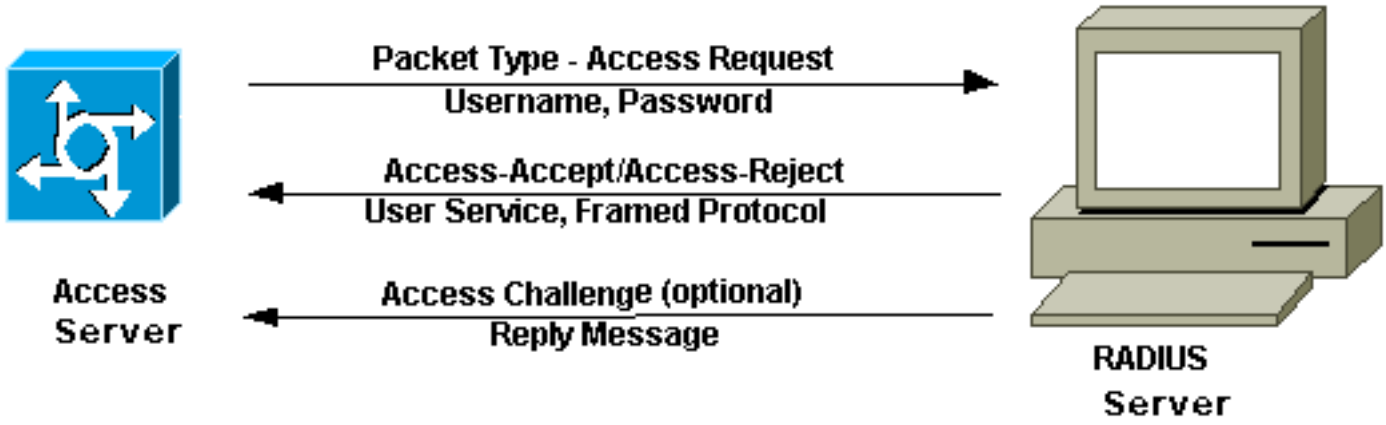
De RADIUS-server ondersteunt een diverse methoden om een gebruiker te verifiëren. Wanneer de gebruiker de gebruikersnaam en het oorspronkelijke wachtwoord opgeeft, kan RADIUS PPP, PAP of CHAP, UNIX-login en andere verificatiemethoden ondersteunen.

Meestal bestaat het inloggen van een gebruiker uit een query (Access-Request) van de NAS naar de RADIUS-server en een respons (Access-Accept of Access-Reject) van de server. Het Access-Request-pakket bevat de gebruikersnaam, het versleutelde wachtwoord en het IP-adres en de

poort van de NAS. De vroege plaatsing van RADIUS werd gedaan met UDP-poortnummer 1645, die met de dienst "gegevensmetriek"strijdig is. Vanwege dit conflict heeft RFC 2865 poortnummer 1812 officieel toegewezen aan RADIUS. De meeste apparaten en toepassingen van Cisco bieden ondersteuning voor beide poortnummers. De indeling van het verzoek geeft ook informatie over het soort sessie dat de gebruiker wil initiëren. Als de query bijvoorbeeld in tekstmodus wordt aangeboden, wordt aangenomen dat 'Service-Type = Exec-User', maar als het verzoek in PPP-pakketmodus wordt aangeboden, wordt aangenomen dat 'Service Type = Framed User' en 'Framed Type = PPP'.

Wanneer de RADIUS-server het Access-Request van de NAS ontvangt, zoekt deze in een database naar de gegeven gebruikersnaam. Als de gebruikersnaam niet in de database bestaat, wordt er een standaardprofiel geladen of stuurt de RADIUS-server onmiddellijk een bericht van toegangsweigering. Dit Access-Reject-bericht kan vergezeld gaan van een tekstbericht dat de reden voor de weigering aangeeft.

Bij RADIUS zijn verificatie en autorisatie gekoppeld. Als de gebruikersnaam wordt gevonden en het wachtwoord juist is, geeft de RADIUS-server een Access-Accept-respons terug, die een lijst met attribuut-waardeparen bevat die de parameters beschrijven die voor deze sessie moeten worden gebruikt. Gangbare parameters omvatten servicetype (shell of framed), protocoltype, IP-adres om toe te wijzen aan de gebruiker (statisch of dynamisch), toe te passen toegangslijst of een statische route om in de routingtabel van de NAS te installeren. De configuratie-informatie in de RADIUS-server bepaalt wat er op de NAS kan worden geïnstalleerd. Het volgende cijfer illustreert de de authentificatie en vergunningsopeenvolging van RADIUS.



RADIUS-verificatie en -autorisatie

Accounting

De accountingfuncties van het RADIUS-protocol kunnen onafhankelijk van RADIUS-verificatie of -autorisatie worden gebruikt. De boekhoudfuncties van RADIUS maken het mogelijk om gegevens te verzenden aan het begin en aan het eind van sessies, wat aangeeft hoeveel bronnen (zoals tijd, pakketten, bytes, enzovoort) tijdens de sessie zijn gebruikt. Een Internet Service Provider (ISP) kan RADIUS-toegangscontrole- en boekhoudingssoftware gebruiken om aan speciale behoeften op het gebied van beveiliging en facturering te voldoen. De accountingpoort voor RADIUS is 1646 op de meeste Cisco-apparaten, maar kan ook 1813 zijn (vanwege de verandering van poorten zoals gespecificeerd in RFC 2139).

De transacties tussen de client en de RADIUS-server worden geverifieerd door middel van een gedeeld geheim dat nooit via het netwerk wordt verzonden. Bovendien worden de gebruikerswachtwoorden verzonden versleuteld tussen de client en de RADIUS-server om de mogelijkheid uit te sluiten dat iemand die op een onveilig netwerk snuffelt een

gebruikerswachtwoord kan bepalen.

Gerelateerde informatie

- Verificatieprotocollen
- Requests for Comments (RFC's)
- Technische ondersteuning – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.