Examiner le fonctionnement de RADIUS

Table des matières

Introduction

Ce document décrit ce qu'est un serveur RADIUS et comment il fonctionne.

Conditions préalables

Exigences

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, consultez Conventions relatives aux conseils techniques Cisco.

Informations générales

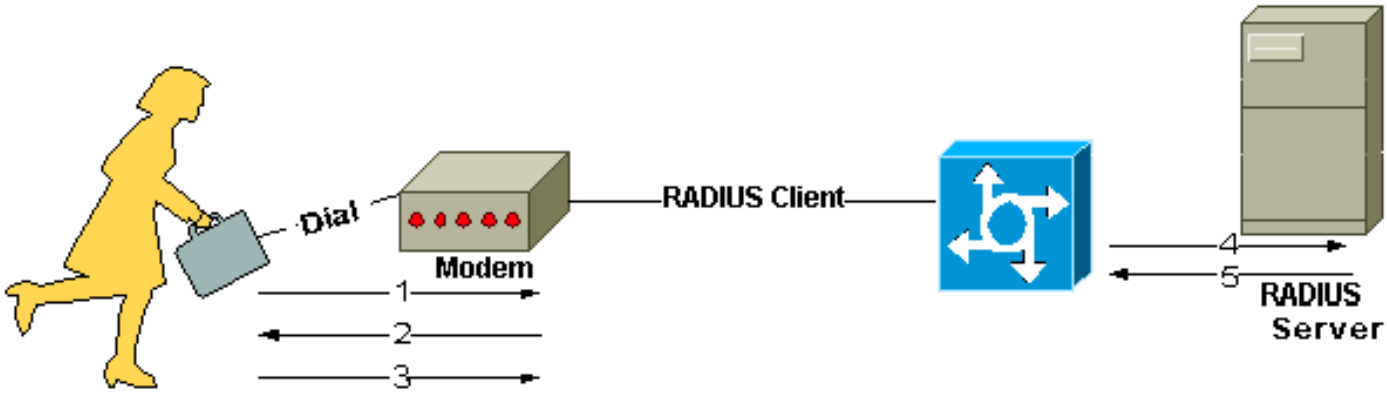
Le protocole de Remote Authentication Dial-In User Service (RADIUS) a été développé par Livingston Enterprises, Inc., comme protocole d'authentification de serveur d'accès et de traçabilité. La spécification RADIUS RFC 2865 rend obsolète la spécification RFC 2138. La norme de comptabilité RADIUS RFC 2866 rend obsolète la spécification RFC 2139.

La communication entre un serveur d'accès réseau (NAS) et un serveur RADIUS se fonde sur le protocole UDP (User Datagram Protocol). En règle générale, le protocole RADIUS est considéré comme un service sans connexion. Les problèmes liés à la disponibilité, à la retransmission et aux délais d'expiration du serveur sont pris en charge par les périphériques RADIUS plutôt que par le protocole de transmission.

RADIUS est un protocole client/serveur

Le client RADIUS est généralement un NAS et le serveur RADIUS est généralement un processus démon qui s'exécute sur une machine UNIX ou Windows NT. Le client transmet les informations utilisateur aux serveurs RADIUS désignés et agit sur la réponse renvoyée. Les serveurs RADIUS reçoivent des demandes de connexion des utilisateurs, authentifient l'utilisateur, puis renvoient les informations de configuration nécessaires pour que le client remette le service à l'utilisateur. Un serveur RADIUS peut faire fonction de client proxy pour d'autres serveurs RADIUS ou pour d'autres types de serveurs d'authentification.

Cette figure illustre l'interaction entre un utilisateur d'accès à distance et le client et le serveur RADIUS.



Interaction entre l'utilisateur d'accès à distance et le client et le serveur RADIUS

1. L'utilisateur lance l'authentification PPP sur le NAS.
2. Le NAS demande le nom d'utilisateur et le mot de passe (si le protocole PAP (Password Authentication Protocol) est adopté) ou lance le défi (si le protocole CHAP d'authentification de négociation par défi [ou Challenge Handshake Authentication Protocol] est adopté).
3. L'utilisateur répond.
4. Le client RADIUS envoie le nom d'utilisateur et le mot de passe chiffré au serveur RADIUS.
5. Le serveur RADIUS répond avec une acceptation, un refus ou un défi.
6. Le client RADIUS agit selon les services et les paramètres de services regroupés avec l'acceptation ou le refus.

Authentification et autorisation

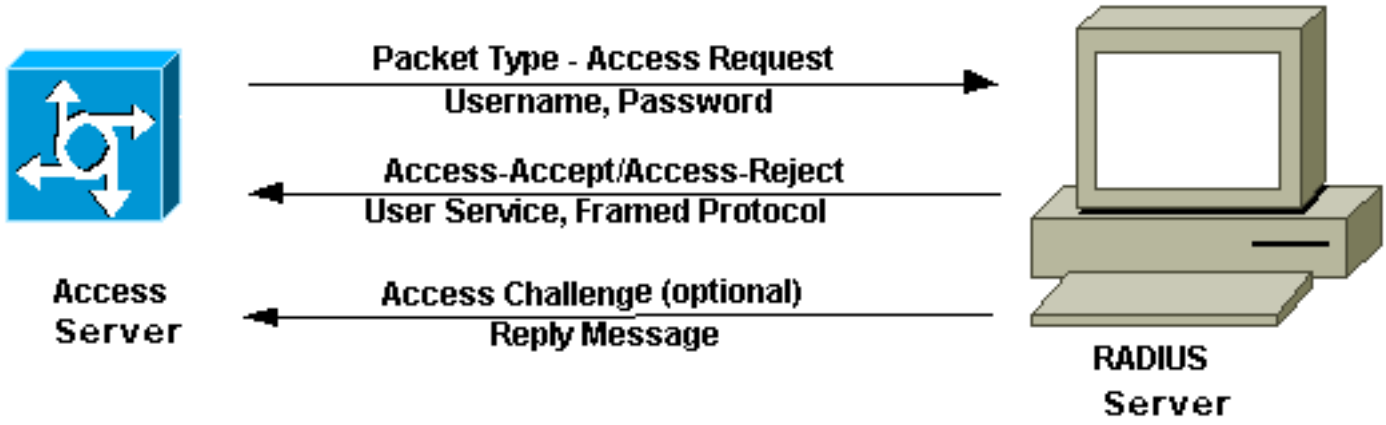
Le serveur RADIUS peut prendre en charge diverses méthodes pour authentifier un utilisateur. Avec le nom d'utilisateur et le mot de passe d'origine de l'utilisateur, il peut prendre en charge les méthodes PPP, PAP ou CHAP, la connexion UNIX et d'autres mécanismes d'authentification.

En règle générale, une connexion utilisateur se compose d'une requête (Access-Request) entre le NAS et le serveur RADIUS, ainsi que d'une réponse correspondante (Access-Accept ou Access-Reject, selon que la demande est acceptée ou refusée) à partir du serveur. Le paquet de requête d'accès Access-Request contient le nom d'utilisateur, le mot de passe chiffré, l'adresse IP du NAS

et le port. Le déploiement précoce de RADIUS a été effectué avec le numéro de port UDP 1645, qui est en conflit avec le service « data metrics ». En raison de ce conflit, le numéro de port 1812 a été attribué officiellement au RFC 2865 pour RADIUS. La plupart des appareils et applications Cisco prennent en charge l'un ou l'autre des ensembles de numéros de port. Le format de la demande fournit également des renseignements sur le type de session que l'utilisateur souhaite lancer. Par exemple, si la requête est présentée en mode caractère, l'inférence est « Service-Type = Exec-User », mais si la requête est présentée en mode de paquet PPP, l'inférence est « Service Type = Framed User » et « Framed Type = PPP ».

Lorsque le serveur RADIUS reçoit la requête d'accès (Access-Request) du NAS, il fait des recherches dans une base de données pour le nom d'utilisateur indiqué. Si le nom d'utilisateur n'existe pas dans la base de données, soit un profil par défaut est chargé, soit le serveur RADIUS envoie immédiatement un message de refus d'accès. Ce message de refus d'accès peut être accompagné d'un message texte indiquant la raison du refus.

Dans RADIUS, l'authentification et l'autorisation sont combinées. Si le nom d'utilisateur est trouvé et que le mot de passe est correct, le serveur RADIUS renvoie une réponse d'acceptation d'accès, qui inclut une liste de paires attribut-valeur décrivant les paramètres à utiliser pour cette session. Les paramètres standard sont le type de service (Shell ou Framed), le type de protocole, l'adresse IP à attribuer à l'utilisateur (statique ou dynamique), la liste d'accès à appliquer ou une route statique à installer dans le tableau de routage du NAS. Les informations de configuration du serveur RADIUS définissent ce qui peut être installé sur le NAS. La figure suivante illustre la séquence d'authentification et d'autorisation RADIUS.



Séquence d'authentification et d'autorisation RADIUS

Gestion de comptes

Les fonctionnalités de gestion du protocole RADIUS peuvent être utilisées indépendamment de l'authentification ou de l'autorisation RADIUS. Les fonctions de comptabilisation RADIUS permettent d'envoyer des données au début et à la fin des sessions, ce qui indique la quantité de ressources (telles que le temps, les paquets, les octets, etc.) utilisées pendant la session. Un fournisseur de services Internet (FAI) peut utiliser le logiciel de comptabilité et de contrôle d'accès RADIUS pour répondre à des besoins spécifiques en matière de sécurité et de facturation. Pour la plupart des périphériques Cisco, le port de gestion pour RADIUS est 1646, mais il peut également s'établir à 1813 (pour les besoins du changement de ports, tel que décrit dans RFC 2139).

Les transactions entre le client et le serveur RADIUS sont authentifiées à l'aide d'un secret partagé, qui n'est jamais envoyé au sein du réseau. En outre, les mots de passe utilisateur sont envoyés chiffrés entre le client et le serveur RADIUS afin d'éliminer la possibilité qu'une personne surveillant un réseau non sécurisé puisse déterminer un mot de passe utilisateur.

Informations connexes

- Protocoles d’authentification
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.