Fonctionnement de RADIUS

Table des matières :

1 Introduction

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.

2 Conditions préalables

2.1 Conditions requises

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

2.2 Composants utilisés

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

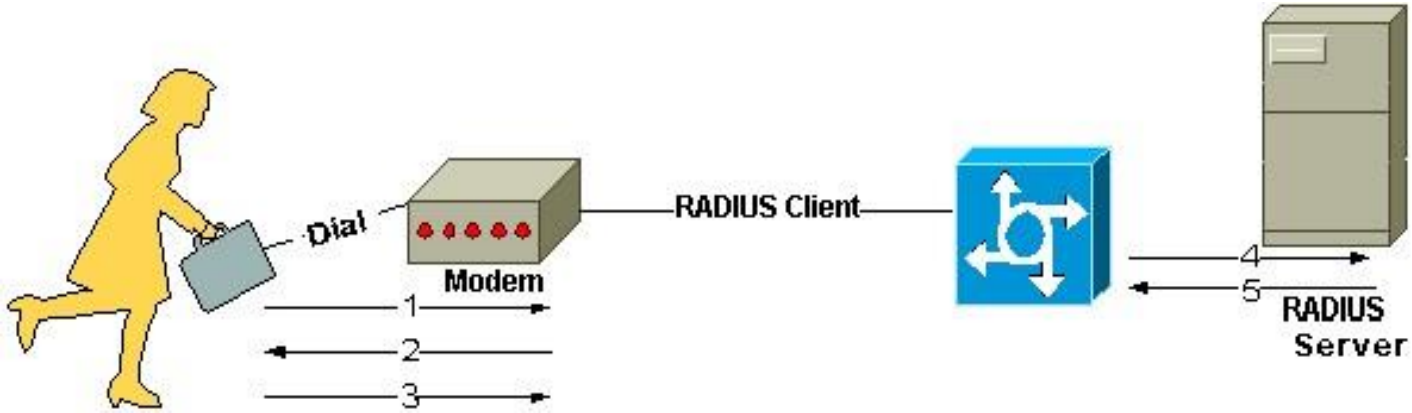
2.3 Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

3 Informations générales

La transmission entre un serveur d'accès à distance (NAS) et un serveur de RADIUS est basée sur le Protocole UDP (User Datagram Protocol). Généralement, le protocole RADIUS est considéré un service sans connexion. Le problème lié à la disponibilité du serveur, la retransmission, et les délais d'attente sont manipulés par les périphériques RADIUS-activés plutôt que le protocole de transmission.
RADIUS est un protocole de client/serveur. Le client RADIUS est typiquement NAS et le serveur de RADIUS est habituellement un processus exécuté de démon sur un ordinateur UNIX ou de Windows NT. Le client passe les serveurs indiqués et les actes de RADIUS des informations utilisateur sur la réponse qui est renvoyée. Les serveurs de RADIUS reçoivent des demandes de connexion utilisateur, authentifient l'utilisateur, et puis renvoient les informations de configuration nécessaires pour que le client fournisse le service à l'utilisateur. Un serveur de RADIUS peut agir en tant que client de proxy à d'autres serveurs de RADIUS ou à d'autres genres de serveurs d'authentification.

Cette figure affiche l'interaction entre un utilisateur en accès entrant et le client RADIUS et le serveur.



1. L'utilisateur initie l'authentification de PPP au NAS.
2. Le NAS incite pour le nom d'utilisateur et mot de passe (si protocole d'identification de mot de passe [PAP]) ou le défi (si authentification Protocol à échanges confirmés [CHAP]).
3. Réponses d'utilisateur.
4. Le client RADIUS envoie le nom d'utilisateur et le mot de passe chiffré au serveur de RADIUS.
5. Le serveur de RADIUS répond avec reçoivent, rejettent, ou contestent.
6. Les actes de client RADIUS sur des services et des paramètres de services ont empaqueté avec reçoivent ou rejettent.

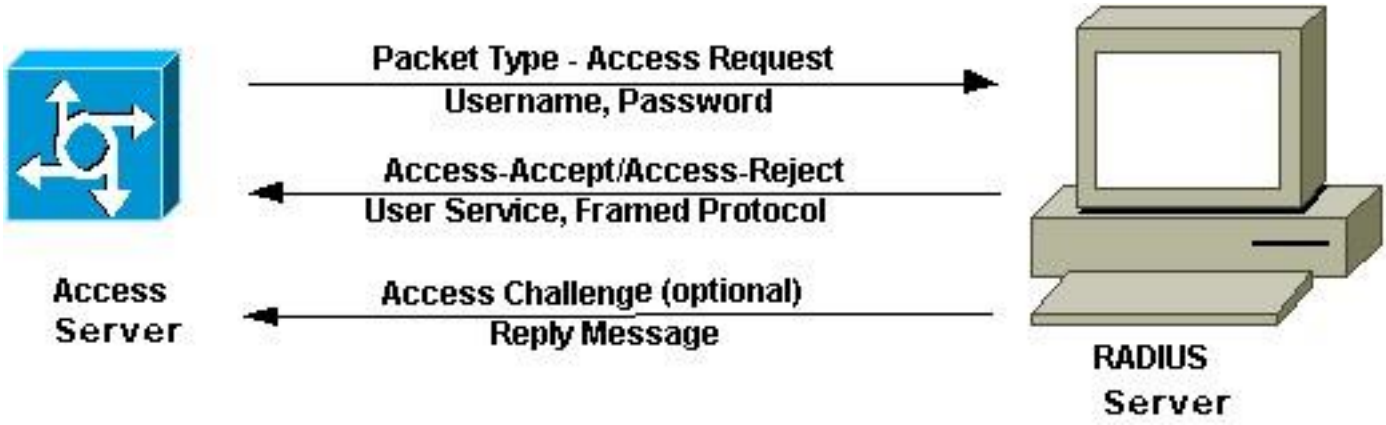
4 Authentification et autorisation

Le serveur de RADIUS peut prendre en charge un grand choix de méthodes pour authentifier un utilisateur. Quand on lui équipe de mot de passe de nom d'utilisateur et d'original donné par l'utilisateur, il peut prendre en charge la procédure de connexion de PPP, PAP ou de CHAP, UNIX, et d'autres mécanismes d'authentification.

Typiquement, une ouverture de session utilisateur se compose d'une requête (Access-demande) du NAS au serveur de RADIUS et à une réponse correspondante (Access-recevez ou Accessanomalie) du serveur. Le paquet de demande d'accès contient le nom d'utilisateur, le mot de passe chiffré, l'adresse IP de NAS, et le port. Le déploiement tôt de RADIUS a été fait utilisant le numéro de port UDP 1645, qui est en conflit avec le service de « datametrics ». En raison de ce conflit, RFC 2865 officiellement assigné le numéro de port 1812 pour RADIUS. La plupart des périphériques et applications de Cisco offrent le soutien de l'un ou l'autre de nombres d'ensemble de ports. Le format de la demande fournit également des informations au sujet du type de session que l'utilisateur veut initier. Par exemple, si la requête est présentée en mode caractère, l'inférence est « type = Exécutif-utilisateur, » mais si la demande est présentée dans le PPP d'exploitation par groupes de bits, l'inférence est « type de service = utilisateur vue » et « type vue
= PPP. »

Quand le serveur de RADIUS reçoit l'Access-demande du NAS, elle recherche une base de données pour le nom d'utilisateur répertorié. Si le nom d'utilisateur n'existe pas dans la base de données, ou un profil par défaut est chargé ou le serveur de RADIUS envoie immédiatement un message d'Access-anomalie. Ce message d'Access-anomalie peut être accompagné d'un message texte indiquant la raison pour le refus.

Dans RADIUS, l'authentification et l'autorisation sont couplées ensemble. Si le nom d'utilisateur est trouvé et le mot de passe est correct, le serveur de RADIUS renvoie une réponse d'Accessrecevoir, y compris une liste de paires de valeurs d'attribut qui décrivent les paramètres à utiliser pour cette session. Les paramètres typiques incluent le type de service (shell ou encadré), le type de protocole, l'adresse IP pour affecter l'utilisateur (statique ou dynamique), la liste d'accès pour s'appliquer, ou une artère statique à installer dans la table de routage de NAS. Les informations de configuration dans le serveur de RADIUS définissent ce qui sera installé sur le NAS. La figure ci-dessous montre l'ordre d'authentification et d'autorisation de RADIUS.



5 Comptabilité

Les fonctionnalités de comptabilisation du protocole RADIUS peuvent être utilisées indépendamment de l'authentification ou de l'autorisation de RADIUS. Les fonctions de traçabilité de RADIUS permettent des données à envoyer au début et à la fin des sessions, indiquant le montant de ressources (telles que le temps, les paquets, les octets, et ainsi de suite) utilisées pendant la session. Un fournisseur de services Internet (ISP) pourrait employer le contrôle d'accès de RADIUS et le logiciel de comptabilité pour répondre aux besoins spéciaux de Sécurité et de facturation. Le port de traçabilité pour RADIUS pour la plupart des périphériques de Cisco est 1646, mais il peut également être 1813 (en raison du changement des ports comme spécifiés 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, des mots de passe utilisateur sont envoyés chiffrés entre le client et le serveur de RADIUS pour éliminer la possibilité que quelqu'un pillant sur un réseau non sécurisé pourrait déterminer un mot de passe d'utilisateur.