¿Cómo el RADIUS trabaja?

Contenido

Introducción

El Protocolo de servicio de usuario de acceso telefónico de autenticación remota (RADIUS) fue desarrollado por Livingston Enterprises, Inc., como un protocolo de autenticación del servidor de acceso y de contabilidad. La especificación RADIUS RFC 2865 sustituye a la RFC 2138. El estándar de contabilidad RADIUS RFC 2866 sustituye al RFC 2139.

prerrequisitos

Requisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

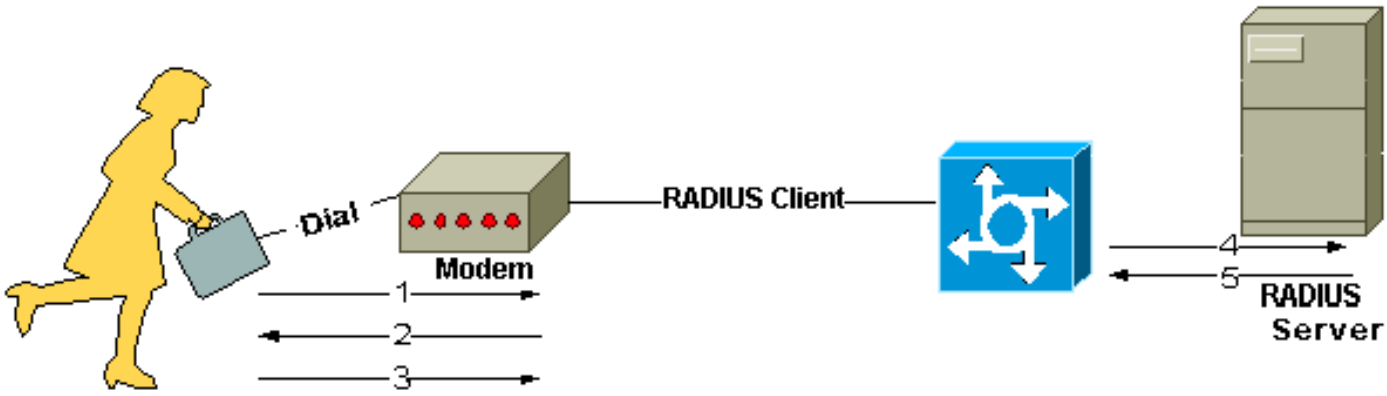
Antecedentes

La comunicación entre un servidor de acceso de red (NAS) y el servidor RADIUS se basa en el protocolo de datagrama de usuario (UPD). Generalmente, el protocolo RADIUS se considera un Servicio sin conexión. Los problemas relacionados con la disponibilidad de los servidores, la

retransmisión y los tiempos de espera son tratados por los dispositivos activados por RADIUS en lugar del protocolo de transmisión.

El RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un NAS y el servidor de RADIUS es generalmente un proceso de daemon que se ejecuta en UNIX o una máquina del Windows NT. El cliente pasa la información del usuario a los servidores RADIUS designados y a los actos en la respuesta se vuelve que. Los servidores de RADIUS reciben las peticiones de conexión del usuario, autentican al usuario, y después devuelven la información de la configuración necesaria para que el cliente entregue el servicio al usuario. Un servidor RADIUS puede funcionar como cliente proxy para otros servidores RADIUS u otro tipo de servidores de autenticación.

Esta figura muestra la interacción entre un usuario de marcación de entrada y el servidor y cliente RADIUS.



1. El usuario inicia la autenticación PPP al NAS.
2. NAS le pedirá que ingrese el nombre de usuario y la contraseña (en caso de Protocolo de autenticación de contraseña [PAP]) o la integración (en caso de Protocolo de confirmación de aceptación de la contraseña [CHAP]).
3. Contestaciones del usuario.
4. El cliente RADIUS envía el nombre de usuario y la contraseña encriptada al servidor de RADIUS.
5. El servidor RADIUS responde con Aceptar, Rechazar o Impugnar.
6. El cliente RADIUS actúa dependiendo de los servicios y de los parámetros de servicios agrupados con Aceptar o Rechazar.

Autenticación y autorización

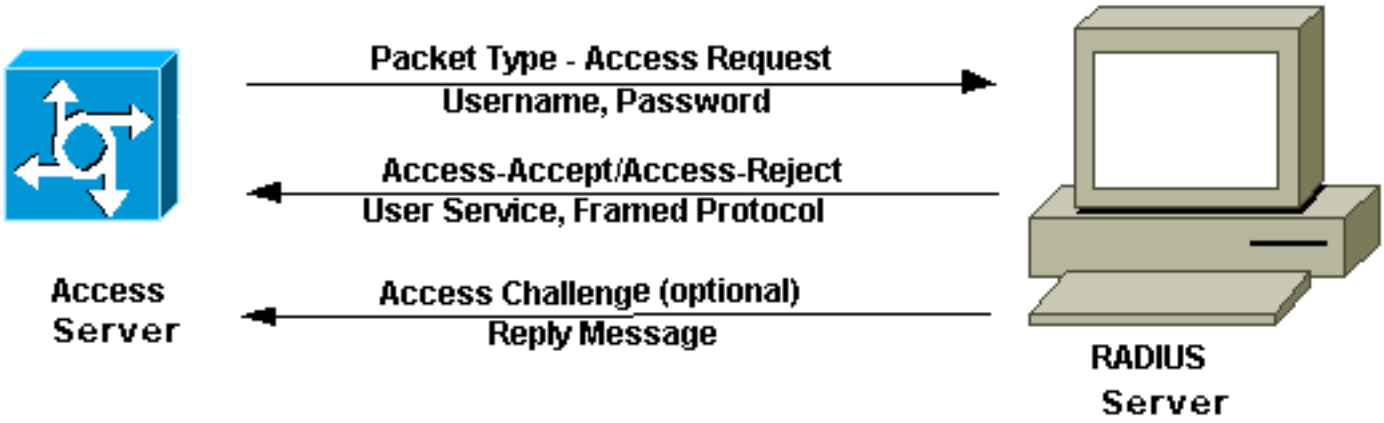
El servidor RADIUS puede soportar varios métodos para autenticar un usuario. Cuando se proporciona el nombre de usuario y la contraseña original dados por el usuario, puede soportar el login PPP, PAP o de la GRIETA, de UNIX, y otros mecanismos de autenticación.

Comúnmente, el ingreso de un usuario al sistema consiste en un pedido (Solicitud de acceso) desde el NAS hacia el servidor RADIUS y de una correspondiente respuesta (Aceptación de acceso o Rechazo de acceso) desde el servidor. El paquete access-request contiene el nombre de usuario, la contraseña encriptada, la dirección IP NAS, y el puerto. El Early Deployment del RADIUS fue hecho usando el número del puerto 1645 UDP, que está en conflicto con el servicio del “datametrics”. Debido a este conflicto, el RFC 2865 asignó oficialmente el número del puerto 1812 para el RADIUS. La mayoría de los dispositivos de Cisco y de las aplicaciones ofrecen el soporte para cualquier números del conjunto de puertos. El formato del pedido proporciona

asimismo información sobre el tipo de sesión que el usuario desea iniciar. Por ejemplo, si la interrogación se presenta en el modo de carácter, la inferencia es “tipo de servicio = EXEC-usuario,” pero si la petición se presenta en el PPP en modo de paquete, la inferencia es “tipo de servicio = Usuario entramado” y el “tipo de Framed =PPP.”

Cuando el servidor de RADIUS recibe el pedido de acceso del NAS, busca una base de datos para el nombre de usuario enumerado. Si el nombre de usuario no existe en la base de datos, se carga un perfil predeterminado o el servidor RADIUS inmediatamente envía un mensaje Access-Reject (acceso denegado). Este mensaje de acceso rechazado puede estar acompañado de un mensaje de texto que indique el motivo del rechazo.

En RADIUS, la autenticación y la autorización están unidas. Si se encuentra el nombre de usuario y la contraseña es correcta, el servidor RADIUS devuelve una respuesta de Acceso-Aceptar e incluye una lista de pares de atributo-valor que describe los parámetros que deben usarse en esta sesión. Los parámetros comunes incluyen el tipo de servicio (shell o entramado), el tipo de protocolo, la dirección IP para asignar el usuario (estática o dinámica), la lista de acceso a aplicar o una ruta estática para instalar en la tabla de ruteo de NAS. La información de configuración en el servidor RADIUS define qué se instalará en el NAS. La siguiente figura ilustra la secuencia de autenticación y autorización de RADIUS.



Contabilidad

La funciones de contabilidad del protocolo RADIUS pueden emplearse independientemente de la autenticación o autorización de RADIUS. Las funciones de contabilidad de RADIUS permiten que los datos sean enviados al inicio y al final de las sesiones, indicando la cantidad de recursos (por ejemplo, tiempo, paquetes, bytes y otros) utilizados durante la sesión. Un Proveedor de servicios de Internet (ISP) puede usar RADIUS para el control de acceso y un software de contabilidad para satisfacer necesidades especiales de seguridad y facturación. El puerto de contabilidad para el RADIUS para la mayoría de los dispositivos de Cisco es 1646, pero puede también ser 1813 (debido al cambio en los puertos como se especifica en el RFC 2139).

Las transacciones entre el cliente y el servidor RADIUS son autenticadas mediante el uso de un secreto compartido, que nunca se envía por la red. Además, las contraseñas del usuario se envían cifradas entre el cliente y el servidor de RADIUS para eliminar la posibilidad que alguien snooping en una red insegura podría determinar una contraseña de usuario.

Información Relacionada

- Página de soporte de la tecnología de RADIUS

- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems