Examine cómo funciona RADIUS

Contenido

Introducción

Este documento describe qué es un servidor RADIUS y cómo funciona.

Prerequisites

Requirements

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.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco.](#)

Antecedentes

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

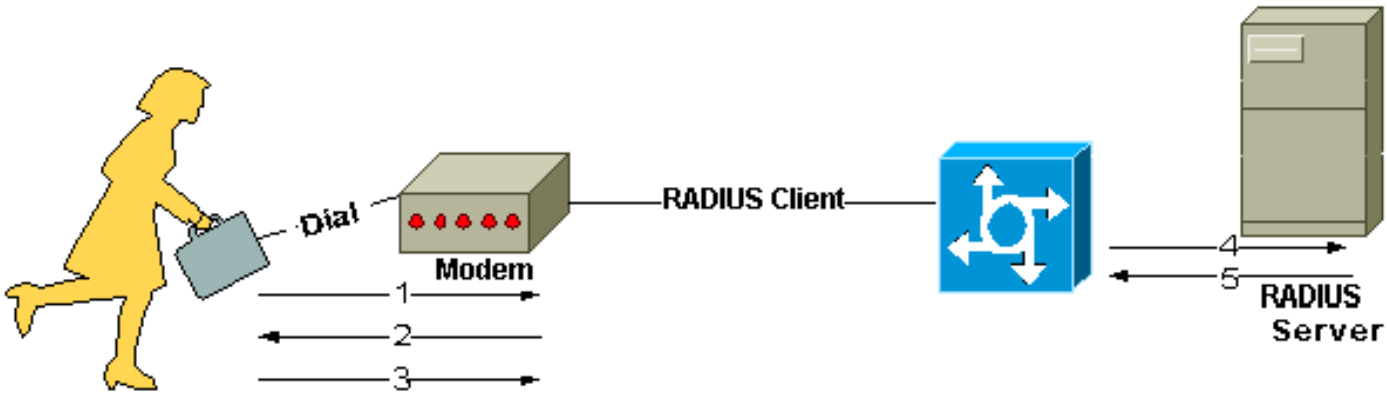
estándar de contabilidad RADIUS RFC 2866 sustituye al RFC 2139.

La comunicación entre un servidor de acceso de red (NAS) y el servidor RADIUS se basa en el protocolo de datagrama de usuario (UPD). Por lo general, 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.

RADIUS es un protocolo entre cliente y servidor

El cliente RADIUS suele ser un NAS y el servidor RADIUS suele ser un proceso demonio que se ejecuta en una máquina UNIX o Windows NT. El cliente pasa la información del usuario a los servidores RADIUS designados y actúa en la respuesta devuelta. Los servidores RADIUS reciben las solicitudes de conexión del usuario, autentican al usuario y devuelven la información de configuración necesaria para que el cliente pueda prestarle 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.



Interacción entre el usuario de acceso telefónico y el cliente y servidor RADIUS

1. El usuario inicia la autenticación PPP en el 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. El usuario responde.
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.

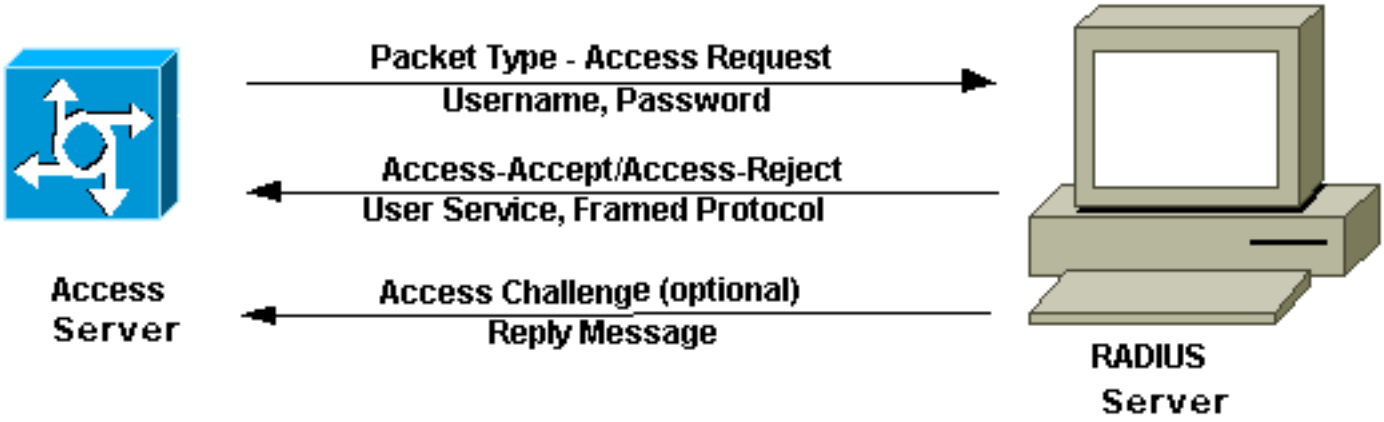
Autenticación y autorización

El servidor RADIUS puede soportar varios métodos para autenticar un usuario. Cuando se le proporciona el nombre de usuario y la contraseña original aportados por el mismo, puede admitir PPP, PAP o CHAP, el inicio de sesión 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 de solicitud de acceso contiene el nombre de usuario, la contraseña cifrada, la dirección IP de NAS y el puerto. La implementación temprana de RADIUS se realizó con el puerto UDP número 1645, que entra en conflicto con el servicio de "métricas de datos". Debido a este conflicto, RFC 2865 asignó oficialmente el número de Puerto 1812 para RADIUS. La mayoría de los dispositivos y aplicaciones de Cisco ofrecen soporte para un conjunto de números de puerto. El formato del pedido proporciona asimismo información sobre el tipo de sesión que el usuario desea iniciar. Por ejemplo, si la pregunta se presenta en modo carácter, la inferencia es “"Service-Type = Exec-User," pero si la respuesta se presenta en modo paquete PPP, la inferencia es “Service Type = Framed User” y “Framed Type= PPP.”

Cuando el servidor RADIUS recibe la solicitud de acceso del NAS, busca en una base de datos el nombre de usuario indicado. Si el nombre de usuario no existe en la base de datos, se carga un perfil predeterminado o el servidor RADIUS envía inmediatamente un mensaje de rechazo de acceso. Este mensaje de rechazo de acceso puede ir acompañado de un mensaje de texto que indique el motivo de la denegación.

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 aceptación de acceso, que incluye una lista de pares atributo-valor que describen los parámetros que se utilizarán para 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 lo que se puede instalar en el NAS. La siguiente figura ilustra la secuencia de autenticación y autorización de RADIUS.



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 contabilización de RADIUS permiten el envío de datos al inicio y al final de las sesiones, lo que indica la cantidad de recursos (como tiempo, paquetes, bytes, etc.) utilizados durante la sesión. Un proveedor de servicios de Internet (ISP) puede utilizar el software de control de acceso RADIUS y de contabilidad para satisfacer necesidades especiales de seguridad y facturación. El puerto de cuenta para RADIUS para la mayoría de los dispositivos Cisco es 1646, pero también puede ser 1813 (debido al cambio en los puertos, como se especifica en 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 de usuario se envían cifradas entre el cliente y el servidor RADIUS para eliminar la posibilidad de que alguien que está indagando en una red no segura pueda determinar una contraseña de usuario.

Información Relacionada

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).