Protocolos de control de acceso RADIUS.

Introducción.

El desarrollo tecnológico actual facilita el acceso a los servicios en cualquier momento y desde cualquier dispositivo conectado a cualquier red de redes. En este sentido las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada, pero en cualquier caso no se puede obviar la seguridad de las mismas, pues sin ella sería muy difícil garantizar la calidad de los servicios.

La seguridad incluye varios aspectos, todos importantes. Uno de ellos es controlar quiénes acceden a la red (Authentication), a qué servicios tienen acceso (Authorization) y por qué tiempo hacen uso del mismo (Accounting). En esta dirección, los protocolos de seguridad más usados para el control de acceso a redes son: RADIUS, TACACS+ y DIAMETER.

RADIUS (Remote Authentication Dial-In User Server) desarrollado originalmente por Livingston Enterprises en 1991 y publicado posteriormente en las RFC 2138 y 2139, actualmente está definido en la RFC 2865 (Autenticación y Autorización) y en la 2866 (Contabilización).

Es un protocolo para el control de acceso a la red, implementado en dispositivos como routers, switch y servidores, provee autenticación centralizada, autorización y manejo o contabilización de cuentas (AAA). Es un sistema de seguridad distribuido que garantiza el acceso remoto a redes y servicios de la red contra el acceso no autorizado [1].

RADIUS consta de tres componentes: un protocolo con un formato de trama que utiliza el protocolo de datagramas de usuario (UDP), un servidor y un cliente [2].

Principales características [2] [3]:

- Funciona bajo el modelo cliente-servidor, pues requieren de un cliente RADIUS, que puede ser un NAS, que interactúe con los servidores RADIUS. Los clientes transmiten a los servidores información del usuario, generalmente sus credenciales como nombre y contraseña. Los servidores se encargan de recibir las solicitudes de conexión de usuarios, autenticar al usuario y brindarle toda la información de configuración necesaria al cliente RADIUS para que pueda ofrecerle al usuario el servicio deseado.

- Ofrece nivel limitado de seguridad en la red ya que aunque las comunicaciones entre el cliente y el servidor son validadas mediante un secreto compartido que no se envía por la red, solo se encripta la clave del usuario en los paquetes de solicitudes de acceso desde el cliente al servidor, utilizando el método de encriptación MD5. El resto del paquete no está encriptado pudiendo ser objeto de captura el nombre de usuario, servicios autorizados y la contabilización de estos.

- Los servidores RADIUS soportan varios esquemas de autenticación de usuario como: EAP (Extensible Authentication Protocol), PAP (Password Authentication Protocol) y CHAP

(Challenge Handshake Authentication Protocol) y soportan varios orígenes de información como: una base de datos del sistema (/etc/passwd), o una base de datos interna (del propio servidor RADIUS), mecanismos PAM y otros como Active Directory, LDAP y Kerberos.

• Es un protocolo de la capa de aplicación que utiliza UDP como transporte. Los puertos oficialmente definidos por la IANA (Internet Assigned Numbers Authority) son el 1812 para la autenticación y el 1813 para la contabilización, pero están los puertos 1645 y 1646 no oficiales pero ampliamente usados en implementaciones de servidores y clientes RADIUS.

• Capacidad para el manejo de sesiones, notificando inicio/cierre de conexión, lo que permite que al usuario se le pueda determinar su consumo y facturar en consecuencia; esta constituye una de las características fundamentales de este protocolo.

Cuando un usuario o equipo envía una solicitud a un servidor de acceso a la red (NAS) para obtener acceso a un recurso de red particular, envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere al dispositivo NAS a través de los protocolos de la capa de enlace, por ejemplo PPP quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS solicitando el acceso a la red. El servidor RADIUS comprueba que la información es correcta utilizando algunos de los esquemas de autenticación mencionados anteriormente (esto dependen del propio servidor RADIUS).

El servidor entonces devuelve una de las tres respuestas siguientes [3] [5]:

1. Acceso aceptado: el usuario tiene acceso. Una vez que el usuario se ha autenticado, el servidor RADIUS le asigna los recursos de red como dirección IP y otros parámetros y a menudo comprobará que el usuario está autorizado a utilizar el servicio de red solicitado.

2. Reto de acceso: se solicita información adicional de usuario como PIN, una contraseña secundaria o, simplemente se emplean diálogos de autenticación entre el usuario y el Server RADIUS por medio del uso de túneles seguros entre ellos, de manera que las credenciales de acceso están ocultas para el servidor de acceso a la red.

3. Acceso rechazado: se le rechaza el acceso al usuario por diferentes razones, entre ellas que la cuenta del usuario esté desactivada o sea desconocida, o al proporcionar una prueba no válida de identificación.

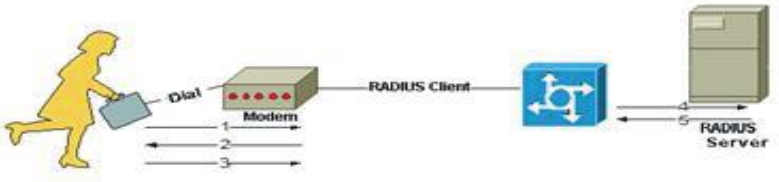
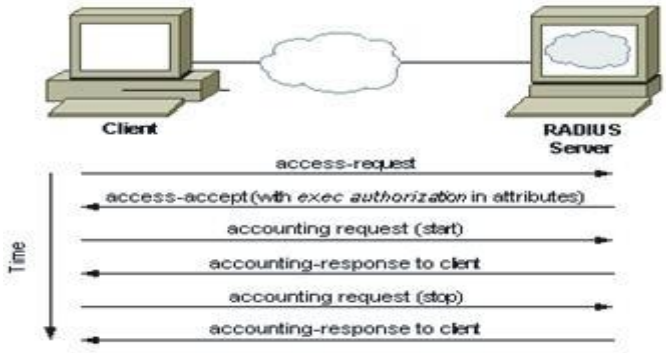


Fig. 1 Interacción entre el usuario, cliente y servidor RADIUS [4]

Una vez garantizado el acceso a la red y a sus recursos, se podrá transmitir información y comienza un proceso de contabilización de uso de los servicios asignados al usuario. En este proceso se registran datos del usuario como: identificación del usuario, dirección IP, punto de conexión y un identificador de sesión único. Estos datos son actualizados periódicamente

mientras está activa la sesión. De igual manera se procede cuando se termina la misma. Este proceso está enfocado mayormente a la facturación del usuario por el uso del servicio, aunque los datos recopilados pueden ser empleados para fines estadísticos.



2: RADIUS Message Flow [2]

Un mensaje RADIUS consta de una cabecera con sus atributos, como muestra la figura 3, cada uno de los cuales especifica un pedazo de información acerca del intento de conexión. Los paquetes RADIUS tienen la siguiente estructura [3] [6]:

• Code (Código): 8 bits para definir el tipo de paquete. Existen 9 códigos para 9 tipos de paquetes.

• Identifier (Identificador): 1 octeto para relacionar una respuesta RADIUS con la solicitud correspondiente.

• Length. Longitud del paquete: 16 bits para la longitud total del paquete, incluyendo los campos desde el código hasta los atributos opcionales.

• Authenticator (Verificador): 32 bits para autenticar la respuesta del servidor RADIUS y para encriptar la clave.

• Attributes (Atributos): Este campo transporta datos en la solicitud y respuesta para la autenticación, autorización y contabilización. El campo longitud del paquete sirve para determinar cuál es el final de los atributos.

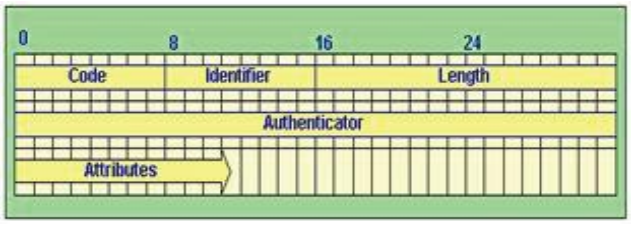


Fig. 3: Formato de un paquete RADIUS

A pesar del esfuerzo de RADIUS por mantenerse como un estándar, la arquitectura Autenticación, Autorización y Contabilidad (AAA) que ofrecía éste no cubría los requerimientos de las nuevas tecnologías, propiciando el desarrollo de un nuevo protocolo con nuevas

características, diseñado para la escalabilidad de acuerdo al crecimiento de las redes: TACACS+ cuya arquitectura complementa de forma independiente la arquitectura AAA. [2]

TACACS+ está basado en el protocolo TACACS (Terminal Acces Controller Access Control System) utilizado para el control de acceso mediante autenticación y autorización, definido desde 1997 por el IETF (Interner Engineering Task Force) en un borrador no publicado draft-grant-tacacs 02.txt [7].

TACACS+ evoluciona los protocolos anteriores, incluyendo nuevas características de seguridad en sus paquetes; mientras que RADIUS combina la autenticación y autorización en un perfil de usuario, TACACS+ separa estas acciones [2].

TACACS+ es también un protocolo propietario de Cisco que funciona bajo el modelo cliente-servidor y emplea el protocolo TCP para el transporte, puerto 49, lo que lo hace más confiable frente a RADIUS. A diferencia del protocolo RADIUS, este implementa encriptación no sólo en las credenciales sino también en los datos, utilizando también un secreto compartido mediante el algoritmo de encriptación MD5 [2].

La secuencia del proceso de autenticación, autorización y contabilización mediante el protocolo TACACS+, se detalla en la figura 4.

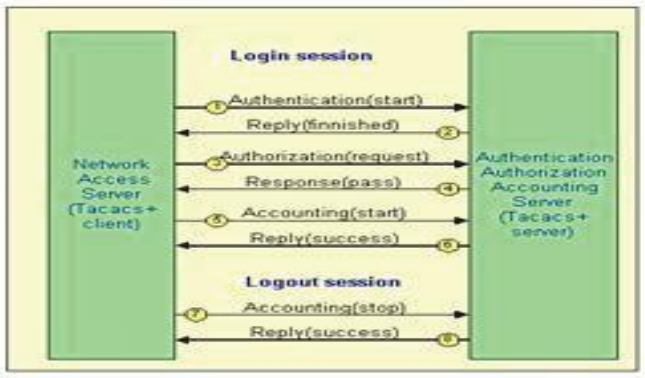


Fig. 4: TACACS+ Message Flow [7]

Los mensajes que se intercambian entre un cliente y un servidor TACACS+, tienen el formato siguiente [7]:

- Version (Versión): 1 octeto para indicar el número de versión

- Type (Tipo): 8 bits para indicar un tipo de mensaje dependiendo de la acción: autenticación autorización o contabilización

- Seq_no (Número de secuencia): 1 octeto para indicar el número de secuencia de paquetes de la sesión actual

- Flags (Banderas): 1 octeto para indicar si hay o no datos encriptados después del campo longitud

- Session_id (identificador de sesión): 4 octetos para identificar la sesión en cada paquete de respuesta del servidor

- Length (Longitud): Longitud del paquete

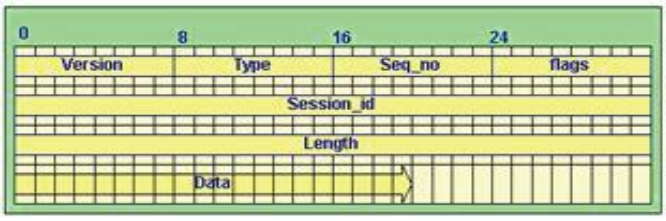


Fig. 5: Formato de un paquete TACACS+

Debido a el crecimiento de Internet y la introducción de nuevas tecnologías de acceso, incluidas las inalámbricas, DSL, Mobile IP y Ethernet, routers y servidores de acceso de red cuya complejidad y densidad demandan nuevas exigencias en los protocolos AAA, como por ejemplo manejar políticas para varios servicios, incapaz cubrirlas con RADIUS y TACACS+ es que surge DIAMETER, considerado por algunos el sucesor de RADIUS [8].

Desarrollado en 1998 y definido por la IETF desde el 2003 en la RFC 3588 en la que se definen una serie de parámetros mínimos para un protocolo AAA, aunque existen otras RFC que definen parámetros del protocolo sobre IP4, IP6, 3GGP, SIP, QoS. DIAMETER usa los protocolos TCP o SCTP para el transporte por el puerto 3868 y emplea seguridad mediante el uso de TLS o IPSEC.

Este protocolo proporciona autenticación, autorización y contabilidad, para aplicaciones de acceso a la red o de movilidad IP (roaming), también extiende su uso para situaciones de roaming, es decir está diseñado para trabajar localmente como en estado de alerta, sondeo y captura con la finalidad de ofrecer servicios dinámicos [9]. Una de las principales características de este protocolo es su flexibilidad y extensión mediante la adición de nuevos comandos y atributos, por ejemplo para el uso del EAP, lo que facilita entrega confiable de los pares atributos-valores (AVPs), capacidad de negociación, notificación de errores, posibilidad de expansión al poder agregar nuevos comandos y AVPs y servicios básicos de aplicaciones como por ejemplo manejo de sesiones y contabilidad [5].

Las AVPs constituyen lo más importante de este protocolo, se usan para enviar información, algunas son empleadas para el funcionamiento propio de DIAMETER y otras para transmitir los datos de las aplicaciones que usan DIAMETER.

Dado que DIAMETER no es un protocolo completo en sí mismo, sino que requiere de extensiones específicas para cada aplicación referentes a la tecnología o arquitectura de acceso a la red; el mismo sólo provee requisitos mínimos para ser protocolo AAA, por tanto para su implementación es necesario garantizar la interoperabilidad, esto significa que todos los nodos deben estar preparados para recibir mensajes DIAMETER y evitar el bloqueo, lo que significa que todos los nodos DIAMETER deberían usar SCTP [5].

Los mensajes DIAMETER están formados por una cabecera DIAMETER y un número variable de pares Atributos-Valores (AVPs), teniendo los paquetes la siguiente estructura [9]:

En la cabecera AVP se especifican algunos parámetros como: la compatibilidad con RADIUS, si el paquete es un acuse de recibo y contiene códigos de comandos, se especifican números de secuencias para corresponder las solicitudes con las respuestas y se indican próximo envío y próximo recibido.

Los comandos AVP definen o especifican, entre otros parámetros, los comandos DIAMETER usados e indican si el AVP está encriptado usando encriptación hop-by-hop y especifican si se requiere soporte AVP.

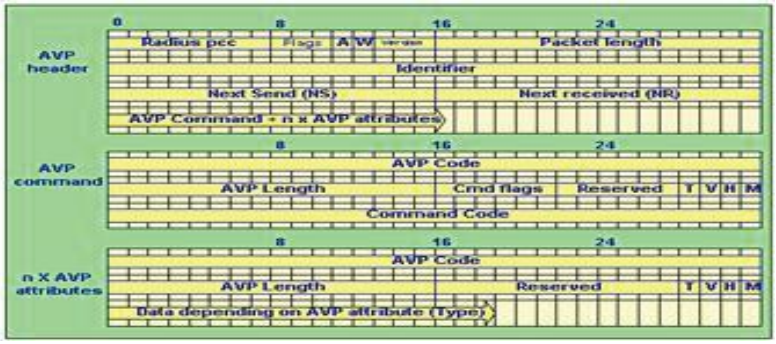


Fig. 6: Formato de un paquete DIAMETER [9]

El flujo de mensajes con DIAMETER se inicia con la estabilización de la conexión. Después el iniciador envía un mensaje de Solicitud e Intercambio de Capacidades (CER), la otra parte envía un mensaje de respuesta de intercambio de capacidades (CEA), posteriormente puede negociarse si se desea TLS, esto es opcional y la conexión está lista para el intercambio de mensajes de aplicación. Si no han ocurrido intercambios de mensajes por un tiempo, uno de los dos enviará una solicitud de dispositivo “perro guardián” (DWR) y el otro deberá responder con una respuesta al dispositivo “perro guardián” (DWA). La comunicación puede terminarse por cualquiera de las partes enviando una solicitud de desconexión (DPR) y la otra parte debe responder a la solicitud (DPA). Con esto ya queda desconectada la conexión.

Fig. 7: Flujo de mensajes DIAMETER

Algunas de las diferencias entre estos protocolos se reflejan en la Tabla 1 [2]

Tabla 1 Comparativa entre RADIUS, TACACS+ y DIAMETER

Parámetros	RADIUS	TACACS+	DIAMETER
Protocolo de transporte	UDP	TCP	TCP o SCTP con TLS o IPSEC
Tipo de protocolo	Cliente / servidor		Peer to Peer
Tipo de mensaje	Solicitud / Respuesta del cliente al servidor		Solicitud / Repuesta de una parte a otra
Encriptación de paquetes	Solo la contraseña en las respuestas al acceso. Otra información esta vulnerable a ser capturada	Todo el cuerpo del paquete excepto la cabecera estándar	Todo el cuerpo del paquete
Algoritmo de encriptación	Secreto compartido con MD5		Secreto compartido con HMAC-MD5
Autenticación y Autorización	Combinado en un mismo perfil de usuario. Los paquetes de acceso aceptado generados por el servidor para el cliente contiene información de autorización	Independientes. Empleo de arquitectura AAA permitiendo separar en servidores diferentes las soluciones AAA	Independientes
Soporte Multiprotocolo	Limitado, no soporta los protocolos: (ARA) - Protocolo de Control de Tramas NetBIOS. - (NASI) - Conexiones X.25 con PAD	Si	
Administración de Routers	No muy útil para la gestión ya que el usuario no tiene el control del comando	Proporciona dos métodos de control de autorización de los comandos: por usuarios o por grupos	Ofrece soporte para los comandos específicos del vendedor
Notificación de errores	No	Si	

Algunos productos que emplean estos protocolos se relacionan a continuación:

TACACS+:

Advanced TACACS+ server (demos), CiscoSecure (CISCO), RADIATER Radius server (Open System Consultans Pty. Lts.), Shiva Access Manager (Shiva), TrustMe Authentication Server (RACAL)

RADIUS:

NTX Access (Internet Transaction Services), DTC Radius ver. 2.03 (Digital Technologies Corporation), RADIATOR Radius server (Open System Consultans Pty. Lts.), Authentication, Authorization and Accounting Server (Merit), Cistron Radius Server (Cistron), RadiusNT (IEA Software, Inc), Radtac Manager Server 4.2.1 (Media Online Italia s.r.l.), RADIUS-VMS (DLS Internet services, Inc.), Internet Authentication Service (Microsoft)

Conclusiones.

No es menos cierto que la seguridad de las redes tiene una importancia incuestionable, conocer quiénes y cómo acceden a nuestras redes es la base de una jerarquía de seguridad, pero paralelo a ello es de vital importancia auditar y contabilizar el uso de los servicios que se brindan, no sólo desde el punto de vista económico, sino también para una acción preventiva y/o investigativa. El empleo de los protocolos AAA permite el control de la red desde tecnologías de acceso. La elección de uno u otro depende de las necesidades e interés del negocio. Cada uno ofrece ventajas y desventajas según sus propias características. Por ejemplo DIAMETER es empleado básicamente para aplicaciones IMS (Subsistema de Multimedia IP) en aplicaciones 3GPP y aplicaciones móviles sobre Ipv4. Por otro lado para emplear RADIUS se recomienda agregar o incorporar protección adicional como empleo de túneles IPsec.

REFERENCIAS

1. HASSELL, JONATHAN: "Securing Public Access to Private Resources", disponible en: http://oreilly.com/catalog/9780596003227/

2. Cisco - TACACS+ and RADIUS Comparison p.2-5, disponible en: www.cisco.com/application/pdf/paws/13838/10.pdf

3. RFC 2138 - Remote Authentication Dial In User Service (RADIUS), disponible en: http://www.faqs.org/rfcs/rfc2138.html

4. How Does RADIUS Work?, disponible en: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml

5. Capitulo 6 Perspectiva de la Interconexión p.8-9, disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/mayoral_p_e/capitulo6.pdf

6. "The Internet NG Project RADIUS ", disponible en: http://ing.ctit.utwente.nl/WU5/D5.1/Technology/radius/

7. "The Internet NG Project - TACACS+ -", disponible en: http://ing.ctit.utwente.nl/WU5/D5.1/Technology/tacacs+/

8. CUEVAS, ANTONIO. GARCÍA, CARLOS. MORENO, JOSÉ IGNACIO. SOTO, IGNACIO: "Los pilares de las redes 4G: QoS, AAA y Movilidad", disponible en: http://www.it.uc3m.es/cgarcia/articulos/telecomi+d_redes4g.pdf

9. "The Internet NG Project DIAMETER -, disponible en: http://ing.ctit.utwente.nl/WU5/D5.1/Technology/diameter/

10. http://en.wikipedia.org/wiki/Diameter_protocol