RADIUS

.: Seguridad en Sistemas de Información :.

Por: Pablo Dafonte Iglesias

Carlos Pallardó Ávila

Índice básico:

1. Como nació RADIUS

1.1. Historia

Desde que en 1979 los ingenieros de IBM en Suiza realizaron los primeros experimentos de WLAN usando rayos infrarrojos para conectar un par de ordenadores, la tecnología ha progresado considerablemente. Pero el mayor auge en el mundo de las conexiones entre computadores se ha producido en los últimos años gracias a la aparición de Internet. Actualmente este auge aumentó más si cabe debido a la existencia de protocolos de comunicación estándar que definen la conexión vía radio entre los distintos nodos de una red WLAN. Estos estándares han permitido la disponibilidad en el mercado de Tarjetas Interfaz de Red (NIC) inalámbricas de muy bajo precio y fácilmente implementables en todo tipo de dispositivos (PC portátil, PDA, AP ..), así como de "chipsets" embebidos en portátiles con lo que la seguridad en el mundo de las conexiones inalámbricas pasó de no tener ninguna importancia a ser de gran relevancia en muy poco tiempo.

Para responder a este problema surgieron varias soluciones, una de ellas es Radius. Fue especificado originalmente en una RFI por Merit Network en 1991 para hacer un control de acceso por dial para NSFnet. A continuación Livingston Enterprises respondió al RFI con una descripción del servidor RADIUS. Merit Network ganó el contrato para Livingston Enterprises para que él pusiese RADIUS a la serie PortMaster de sus Servidores de Acceso a la Red (NAS). Más tarde, en 1997, se publicó como RFC 2058 y RFC 2059 (aunque las versiones actuales de estos RFC son la 2865 y la 2866). Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto.

Radius se creó siguiendo un modelo cliente/servidor que pretendía ofrecer seguridad en las redes. Para ello se incorporaron muchos mecanismos de autenticación flexibles. Además de esto se pretendía que este protocolo fuera extensible para que se pudieran añadir más atributos para dar más información sin que esto corrompiera el funcionamiento del mismo.

1.2. Motivaciones

Según se publicó en varias revistas on-line y en muchos periódicos de diversos países el mayor robo de datos de la Historia ocurrió por vía inalámbrica. Según informa el periódico *20minutos*:

> " (…)Los intrusos utilizaron una antena wi-fi y un ordenador portátil para hacerse con los datos de acceso de algunos empleados a los servidores centrales, lo que les permitió luego acceder a la base central de datos de la cadena TJX, a la que pertenece el comercio espiado. Esta gran cadena comercial, valorada en 17.400 millones de dólares, utilizaba WEP para cifrar sus comunicaciones wireless en 2005, pese a que desde 2001 no se consideraba a ese protocolo seguro y desde 2003 se recomendaba el uso del más seguro WPA.
>
> Se estima que los intrusos han podido acceder a los datos de entre 50 y 200 millones de tarjetas de crédito (que figuraban en los registros de cuatro años de actividad), además de números de licencia de conducir, números de seguridad social e identificaciones militares de casi medio millón de clientes.(…)"

De hecho el montante total de dinero que supuso este gran robo aún no ha podido ser fijado y se estima que llevará años de duras investigaciones determinar, si es que se logra este montante.

Aunque en las redes de cableado telefónico resulta más complicado realizar intrusiones el tema de la seguridad también es muy relevante. Unido a ello las empresas de telefonía que empezaron a ofrecer servicios de transmisión de datos también necesitaban un producto que además de autenticar a los usuarios pudiera autorizarles para acceder a todo o a parte de lo que la red podía ofrecer. Por último también se tuvo en cuenta en los orígenes de RADIUS que para estas empresas podría resultar más que interesante que el mismo producto que autenticara y autorizara fuera capaz de realizar informes de horas de uso, fechas de inicio y de fin y cualquier otro dato que se pudiera controlar de los diferentes usuarios que trataran de identificarse contra este servicio para, con todo estos datos, poder facturar en consecuencia.

2. Que es exactamente RADIUS

2.1. AAA

Antes de hablar de Radius en sí mismo resulta conveniente introducir el marco AAA. Este entorno implica una serie de conceptos básicos de los que se encarga el protocolo que vamos a estudiar. AAA son las siglas de Authentication, Authorization y Accounting (Autenticación, Autorización y Contabilidad), los tres aspectos de los que se ocupa la arquitectura:

2.1.1. Autenticación

Es el proceso de verificar si la identidad de una persona o una máquina es el que dice que es. Busca establecer una relación de confianza entre los interlocutores. Cuando hablamos de autenticar usuarios el primer ejemplo que se nos viene a la cabeza es el del nombre de usuario y la contraseña, aunque esto se puedo complicar mucho más si se desea. Infraestructuras tan completas como los certificados digitales son soluciones más actuales y complejas al problema de la autenticación.

2.1.2. Autorización

Este aspecto involucra la utilización de reglas y plantillas para decidir si un usuario previamente autenticado goza de privilegios suficientes para acceder o no a cierto recurso. Por ejemplo, en un entorno UNIX podríamos autorizar el uso de cierto fichero a un usuario con los permisos que determinan si puede leer, escribir o incluso ejecutarlo si el fichero así lo permite.

2.1.3. Cuentas

En el entorno de la arquitectura AAA se encuentran las cuentas de usuario. Éstas miden y documentan los recursos que un usuario utiliza durante su acceso, al mismo

tiempo guardan datos sobre cuando y como se realiza este acceso. Por ejemplo, en un sistema UNIX es frecuente limitar a sus usuarios el número de procesos que pueden ejecutar concurrentemente, la cantidad de CPU a utilizar o cualquier otro parámetro que se desee limitar.

2.2. ¿Qué es RADIUS?

Es un sistema de autenticación y contabilidad empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del proveedor siempre que ésta sea la adecuada.

RADIUS (Remote Authentication Dial In User Service) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Básicamente es un software de dominio público que identifica usuarios que acceden de forma remota a un servidor, permitiendo asignarles direcciones de red de forma dinámica. Cuando se habla de RADIUS hay dos partes diferenciadas, la del Centro de Servicio de la corporación/empresa y la del proveedor. Cuando un usuario accede con un login y password genéricos (invitado/empresa) el servidor RADIUS le asigna una dirección IP reservada, por eso no puede 'salir' a Internet. Sin embargo, si el usuario accede con su login concreto (pepe@xxxx.es/xxxxxx) el servidor hace una consulta al servidor de la base de datos del proveedor correspondiente, que identifica si ese usuario es suyo, y si lo es selecciona una dirección IP libre del rango de direcciones registradas Internet suyo (y por tanto validas para 'salir'), y le dice al Radius que tiene CSIV que le asigne esa dirección IP al usuario que acaba de realizar la llamada.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

Existen diferentes implementaciones que desarrollan este sistema y cada una ofrece distintas características y funcionalidades. Posteriormente mencionaremos algunas de las más conocidas y utilizadas. Sin embargo pese a la gran variedad, todas ellas tienen ciertas funciones comunes. Principalmente permiten tener el control total de como se trata cada llamada y de lo que guardamos, de dar una serie de IPs (lo que se llama pool de IPs) a cada grupo de llamadas dependiendo de cualquier factor, como por ejemplo, a que número han llamado, el número desde el que han llamado, el tipo de usuario (por ejemplo, con el realm, es decir, lo que ponemos después de la @), la máquina que ha respondido a la llamada, y cualquier tipo de control que se desee realizar.

Otra funcionalidad que todas, o casi todas, las implementaciones ofrecen es un sistema de monitorización de la actividad que analiza todos los datos de las distintas llamadas (tiempo de la llamada, hora de inicio, hora de fin,…). Incluida en esta monitorización también están las posibilidades de generar estadísticas del flujo de información que pasa a través del Radius.

Una de las pegas de la mayoría de las implementaciones y el punto fuerte de aquellas de mayor prestigio (y de pago) es que para configurarlas hay que hacerlo a través de ficheros de texto o, como mucho, a través de web. Sin embargo los radius más caros incluyen en el precio la configuración, el soporte y, en los mejores casos, formación para que alguien de la propia corporación pueda configurarlo por si mismo a través de una amigable GUI.

Todo lo referente a la utilización de Radius, se refleja en los siguientes RFC´s:

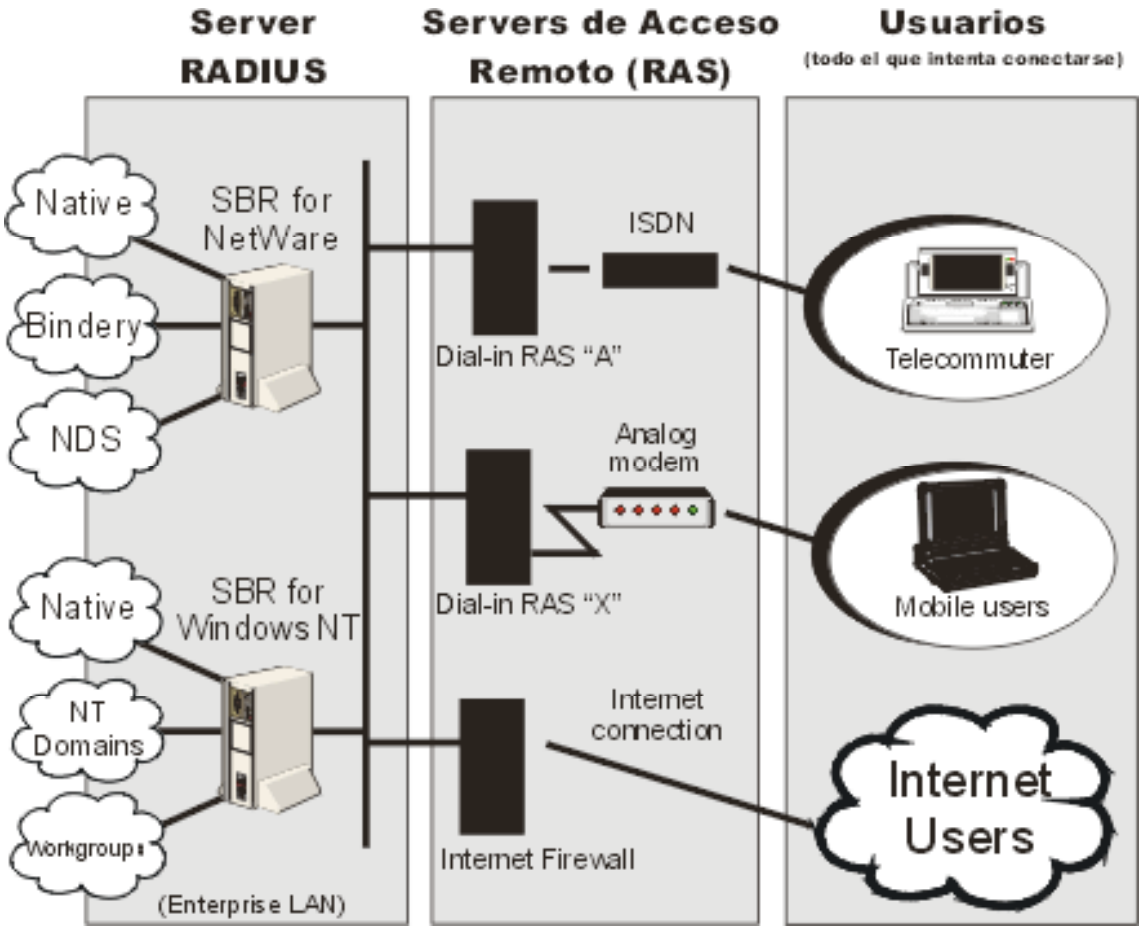
+ Remote Authentication Dial In User Service (RADIUS). RFC 2865 Junio 2000
RADIUS Accounting. RFC 2866. Junio 2000
+ RADIUS Accounting Modifications for Tunnel Protocol Support. RFC 2867. Junio 2000
+ RADIUS Attributes for Tunnel Protocol Support. RFC 2868. Junio 2000
+ RADIUS extensions. RFC 2869. Junio 2000

2.2.1. ACCESO REMOTO A TRAVÉS DE SERVER RADIUS

Existe la necesidad de proveer de modo centralizado de la funcionalidad de Autenticación, de Autorización y de Auditoria, Informes, de todo acceso remoto o intento de acceso a la red. Estas tres funcionalidades se conocen como AAA. El estándar RADIUS ha sido aceptado y está soportado por las empresas líderes en acceso remoto y firewalls.

El puerto utilizado por el sistema Radius para establecer sus conexiones es el 1812 UDP. Los paquetes RADIUS se transportan usando el protocolo UDP (no orientado a conexión y recepción no garantizada), por lo que si la respuesta no llega en un tiempo determinado, se pueden producir retransmisiones; es decir, se reenviará la petición al servidor.

2.2.2. COMPONENTES DEL ENTORNO RADIUS



Cada usuario es un cliente del RAS.

Cada RAS es a la vez servidor para el usuario y cliente para RADIUS.

2.2.3. SERVIDOR DE ACCESO REMOTO (RAS)

Este servidor es la vía de comunicación entre Radius y aquellos usuarios o servidores que desean conectarse a la red que éste verifica. Tanto si se trata de usuarios que se encuentran en la propia corporación vía cable, como si es por vía inalámbrica o si se trata de usuarios que quieren conectarse desde fuera (Internet) RAS es quien se encarga de enrutar las peticiones de todos estos usuarios hacia Radius. Sin embargo será Radius el que dé los privilegios para que el usuario que acceda pueda acceder a la Intranet, a parte de Internet, a todo o a lo que se decida.

El servidor de acceso remoto es el dispositivo encargado de recibir las llamadas SLIP o PPP, autenticar cada usuario según le confirme el servidor Radius y dar el acceso a la red que éste le haya indicado que tiene el cliente que solicita conectarse. También puede generar conexiones directas a la red a través del firewall, autenticando cada usuario vía RADIUS Server y concediéndole acceso a la red con derechos específicos. Otra de sus características es que soporta peticiones avanzadas de otro RAS mediante la utilidad "Proxy RADIUS".

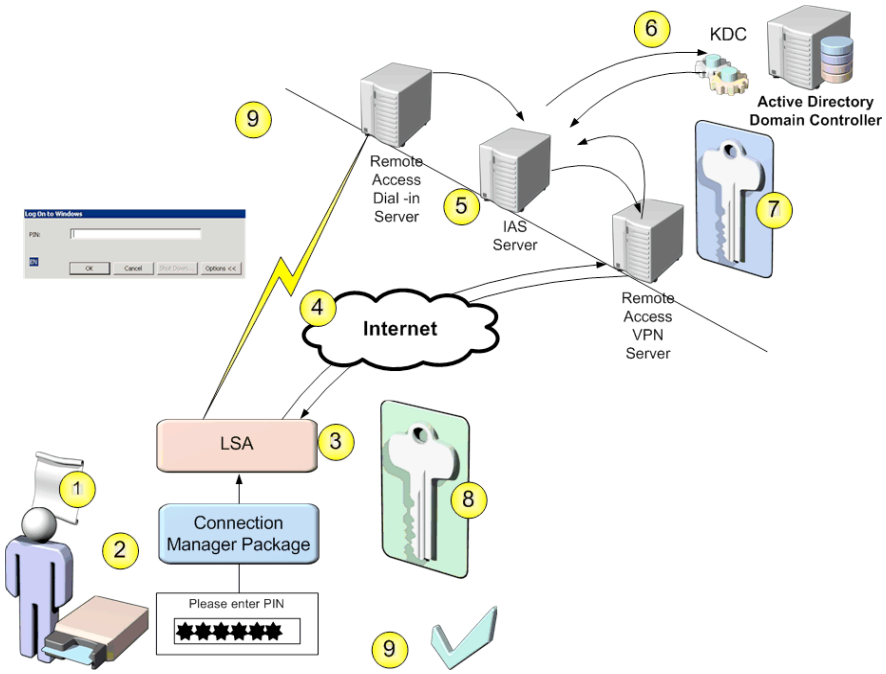
Los estándares RAS soportados por RADIUS son, entre otros, los siguientes: Ascend MAX, Bay Networks, Shina, Telebit NetBlazer, Robotics y Firewalls

2.2.4. PROCESO DE AUTENTICACIÓN

Los pasos que tiene que seguir un usuario para demostrar su identidad a través de este acceso son los siguientes:

1. El usuario llama al RAS y le comunica nombre de usuario y password, iniciando las negociaciones PPP.

2. En esta etapa RAS actúa sólo como intermediario, pasando la información de autenticación al RADIUS Server.
3. Si RADIUS puede autenticar al usuario emite una respuesta de aceptación, junto con la información requerida por el RAS para dar vía libre a la conexión (IP, NetWare Network number). Si no puede autenticar al usuario, le envía una notificación con el motivo.
4. Con la información remitida por RADIUS, RAS completa la negociación PPP, permitiendo la conexión a la red o denegando el acceso.



2.2.5. ATRIBUTOS. PERFILES DE USUARIO

En el proceso de autenticación se intercambia también otro tipo de información muy útil para las conexiones: el listado de atributos. Este listado define los distintos perfiles de usuario que se han incluido en el servidor Radius. Cada uno de estos perfiles se caracteriza por dos tipos de atributos, que son los que se muestran a continuación:

- CHECK-LIST: Son los requerimientos para la conexión que RAS debe enviar a RADIUS. Si no se cumplen el RADIUS puede rechazar el acceso aunque el usuario

sí pueda ser autenticado. Por ejemplo: imaginemos que sólo ciertos usuarios pueden utilizar conexiones ISDN y que uno de los usuarios que si puede utilizar otros servicios pide este.

- RETURN-LIST: Estos son los atributos que RADIUS devuelve al RAS una vez que ha confirmado la autenticación. Aquí se definen parámetros adicionales que el RAS podría incluir en la conexión, normalmente en las negociaciones PPP. Un ejemplo de esto podría ser cuando se asigna a determinados usuarios una dirección IP específica o cuando se desea establecer un tiempo límite permitido de conexión para cierto tipo de usuarios.

También hay que tener en cuenta los DICTIONARY FILES. Estos son ficheros que establecen los valores de los atributos tanto para Check-List como para Return-List y son aquellos que se deben modificar en caso de que se deseen añadir nuevos perfiles de usuario.

Según el protocolo RFC-2865, que es aquel en el que está definido el protocolo, señala exactamente que los atributos específicos son los siguientes:

1 User-Name
2 User-Password
3 CHAP-Password
4 NAS-IP-Address
5 NAS-Port
6 Service-Type
7 Framed-Protocol
8 Framed-IP-Address
9 Framed-IP-Netmask
10 Framed-Routing
11 Filter-Id
12 Framed-MTU
13 Framed-Compression
14 Login-IP-Host
15 Login-Service
16 Login-TCP-Port
17 (unassigned)
18 Reply-Message
19 Callback-Number
20 Callback-Id
21 (unassigned)
22 Framed-Route
23 Framed-IPX-Network
24 State
25 Class
26 Vendor-Specific
27 Session-Timeout
28 Idle-Timeout
29 Termination-Action
30 Called-Station-Id

31 Calling-Station-Id
32 NAS-Identifier
33 Proxy-State
34 Login-LAT-Service
35 Login-LAT-Node
36 Login-LAT-Group
37 Framed-AppleTalk-Link
38 Framed-AppleTalk-Network
39 Framed-AppleTalk-Zone
40 – 59 (reserved for accounting)
60 CHAP-Challenge
61 NAS-Port-Type
62 Port-Limit
63 Login-LAT-Port

Además dentro de este "Request For Comments" (el documento con la propuesta oficial de cómo funcionará el protocolo RADIUS) se especifican detalladamente cual es el significado de todos estos atributos, que información se puede incluir en cada uno de ellos o donde se pueden situar otros comentarios que se podrían incluir si así se considerara oportuno. Añadido a esto incorpora el funcionamiento exacto del protocolo y como se realiza la comunicación a través de él.

2.2.6. ACCOUNTING

Además de todo esto una característica muy importante del estándar RADIUS es la utilidad que tiene para obtener todo tipo de estadísticas e informes sobre los accesos remotos e intentos de acceso a la red. Esta funcionalidad permite conocer, entre otras cosas la hora de inicio de la conexión, la hora de desconexión de ésta o el listado de usuarios conectados en cada momento.

2.3. Usos de Radius

Como ya se ha hablado a lo largo de este trabajo, RADIUS es un protocolo Standard de la industria que implementa autenticación, autorización y contabilización para conexión a servidores. En el pasado, los servidores de acceso eran típicamente servidores tipo "network acces server" (NAS) que mediante una conexión discada (Telefónica), o de un tipo red privada virtual (VPN), daban servicios de Internet a quien los solicitara. Hoy por hoy, los requerimientos han cambiado, y los usos para el protocolo RADIUS están cambiando a puntos de acceso inalámbrico (AP), switches

Ethernet y otro tipo de equipos de red que requieren autenticar y autorizar sus conexiones.

Y como no podía ser menos, la extensión de tecnologías de voz sobre IP no podía quedar sin autenticar, autorizar y contabilizar. Para ello qué mejor que tirar de protocolos ya probados y manejar servidores RADIUS para ello.

2.3.1. Conexión por línea conmutada

Algunas de las circunstancias en donde, tradicionalmente se usa este protocolo es en conexiones Dial-up (esta es la típica conexión que tuvimos todos a través del teléfono, 56K). Para los proveedores de red de telefonía que ofrecen acceso a datos a través de ella Radius resulta de gran ayuda por lo que, como ya se ha comentado, el servidor controla los momentos de acceso y desconexión de los clientes por lo que puede facturar gracias a los datos que le proporciona.

2.3.2. Redes wireless

Otro de los usos típicos es en redes wireless en combinación con el estándar 802.1.X que estudiaremos más tarde ya que es el ámbito en el que, actualmente, más se está usando.

En todas las redes inalámbricas basadas en 802.1.X es obligatorio implementar alguna de las soluciones RADIUS por lo que grandes empresas del sector como Microsoft y Cisco ofrecen soluciones de este tipo.

2.3.3. VoIP

VoIP, al tratarse de un protocolo de voz aprovechando la red de datos, crea dos grupos de necesidades: las heredadas de las redes de datos convencionales en temas de

control de acceso y seguridad, y las heredadas de los servicios de voz tradicionales, relacionados con la tarificación y autenticación de usuarios.

Para ello, asociados a los servicios de datos, se deberá incluir servicios de AAA. Una forma de resolver esto es incluir servicios RADIUS asociados a los servicios de voz sobre IP.

3. Implementaciones

El Servidor Radius admite tanto clientes *hardware* (servidores de túneles, por ejemplo), como clientes *software* (otro servidor Radius) por separado o simultáneamente. También puede actuar en modo Proxy -reenviando las peticiones a otro servidor Radius de acuerdo con diversos criterios.

3.1. Hardware

Normalmente se implementa en equipos como routers, switchers y puntos de acceso wireless.

La implementación del protocolo RADIUS en hardware, se reduce a autenticaciones simples, como sería el de controlar el acceso a una persona desde la consola del propio componente hardware, evitando que personas que no sean administradores de esa maquina, puedan trabajar con ella a través de la conexión de consola que incluyen algunos de estos equipos (equipos ya de cierta potencia y precio).

El uso de RADIUS en hardware, como se puede ver está muy limitado: pocos usuarios, sólo se podrá mantener la información de un número muy escaso de usuarios; problemas de escalabilidad, ya que para tener la misma información en varios equipos, se tendrá que replicar; tiene un fin muy concreto, como es el de acceder directamente al componente hardware para su configuración o monitorización). La autenticación de un número considerable de usuarios, se realizará de forma software sustentada sobre ficheros o bases de datos.

3.2. Software

Como ya se ha adelantado en el punto anterior, la autenticación de un gran número de usuarios, a partir de este protocolo, se realizará de forma software y

sustentado sobre ficheros o una base de datos con la información de logins, contraseñas e información acerca de permisos de acceso a zonas.

Esta es la única opción factible para montar un sistema de autenticación mediante el protocolo RADIUS, en cuanto a autenticación de usuarios finales se refiere. La idea es crear una relación de la información básica de los usuarios, para el tema de la autenticación de un usuario en el sistema. La información básica está formada por login, password y permisos de acceso; no nos interesa nada más para este protocolo.

Se generarán ficheros de logs, o entradas en tablas de una base de datos, para mantener la información de contabilidad relacionada con las conexiones realizadas por los usuarios.

Para hacer esto se recurre a dos métodos:

1. Para sistemas pequeños (menos de 50 usuarios), los datos se pueden mantener en ficheros a los que accederá el servidor RADIUS.
2. Para sistemas medianos o grandes, lo mejor será tratar esos datos dentro de una serie de tablas en una base de datos sobre la que se confrontará el servidor de RADIUS.

Algunos ejemplos de software dedicado a la implementación de este protocolo son los que se muestran a continuación:

- IAS - Internet Authentication Service, incluido en Microsoft Windows Server 2003.

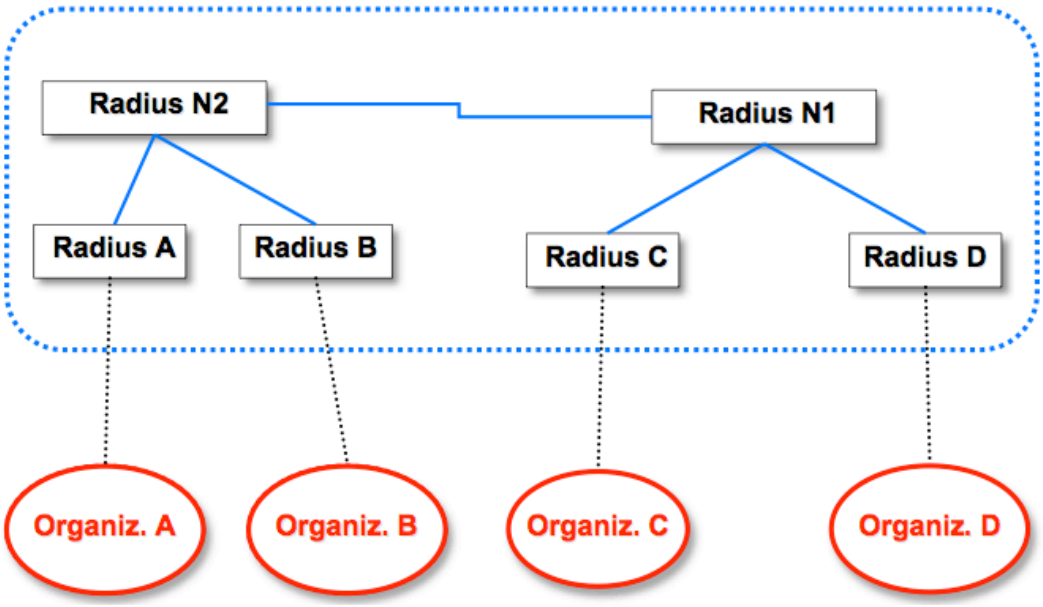
El resto de soluciones son software libre.

- Ascend RADIUS es un port de FreeBSD. Para más información, remitimos a la web del proyecto FreeBSD: http://www.freebsd.org/ .
- Cistron RADIUS. Web del proyecto http://www.radius.cistron.nl/ .
- FreeRADIUS. Web del proyecto http://www.freeradius.org/ .
- FreeRADIUS Client http://www.freeradius.org/.
- Gnu RADIUS. Web del proyecto http://www.gnu.org/software/radius/ .
- XTRADIUS. Dónde conseguirlo: http://sourceforge.net/projects/xtradius/ y para Debian http://packages.debian.org/stable/net/xtradius/ .

4. Redes de confianza

En algunas redes de gran ámbito, nacional o incluso internacional, se está implantando la idea de crear redes de servidores Radius virtuales que validarían a un cliente se encuentre donde se encuentre. Para ello se utilizarán las ideas de confianza entre servidores de modo que.

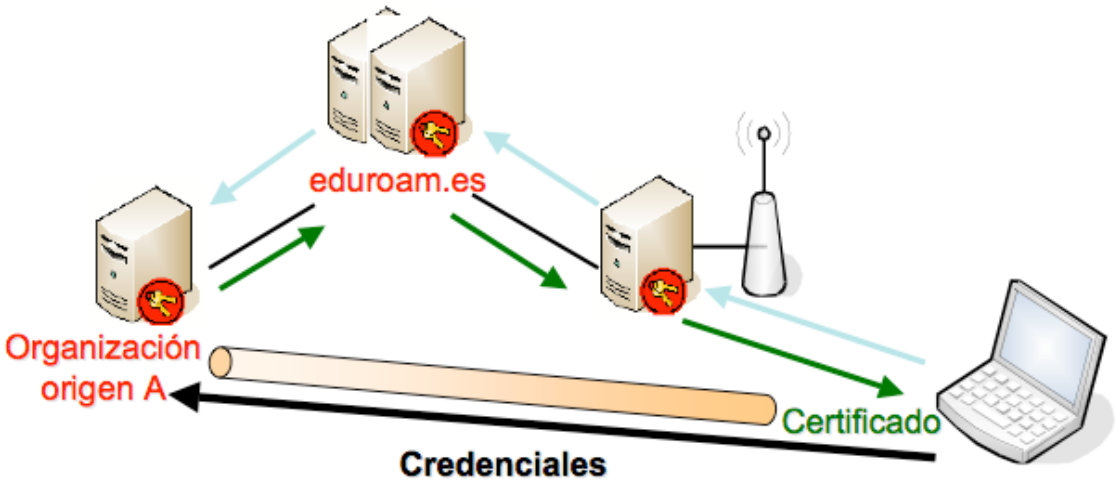
La idea consiste en que ciertos servidores Radius dependan de otros de manera que con que uno de ellos tenga los datos sobre determinado usuario este ya quede validado para toda la red aunque no acceda directamente a la localización del Radius que tiene dichos datos.



Para explicar esta idea con más detalle utilicemos como ejemplo la red de conexión para universitarios Erasmus. A nivel europeo se ha creado una red inalámbrica, eduroam, que se puede encontrar en la universidad de la Coruña (y en muchas más universidades europeas, sobre todo en España y Portugal. Con esta red se pretende conectar a los alumnos que se encuentran en una universidad distinta a la suya por motivos de becas (Erasmus, Seneca), con la red y los datos de su propia universidad de origen.

Imaginemos una alumna Holandesa que estudie Magisterio en la "BREDA UNIVERSITY OF PROFESSIONAL EDUCATION" y venga a La Coruña en el último año porque además de las asignaturas que le faltan también quiere aprender Castellano y Gallego. Cuando comienza los tramites para el traslado esta joven se dará de alta en el servidor Radius de su Universidad, la cual pertenece a la red Dutch NREN (similar a la red IRIS de España).

Cuando esta alumna llega a la UDC tratara de conectarse a la red eduroam con sus datos. Tras esperar unos instantes podrá utilizar el acceso a la red que proporciona la universidad y podrá realizar todas sus prácticas de 5º de carrera sin mayor problema. Para que esta aceptación se haya producido sus datos han tenido que seguir el camino siguiente: UDC → CESGA → RED Iris → SurfNet → Dutch NREN → BEUPE.



Su petición viajará por todos estos servidores y, como el último de ellos autenticará y autorizará a dicha alumna por confianza el resto de servidores también aceptarán y darán acceso a la red de la universidad a través de su infraestructura.

Con esta solución se consigue dar servicio sólo a usuarios autorizados de forma totalmente segura. Otra gran ventaja de esta solución, además de la gran escalabilidad que ofrece, es que no carga de gestión al centro que se visita ya que la conexión se enruta con la red a la que realmente pertenece. Por último resulta relativamente fácil de usar para los usuarios que llegan como extranjeros a una institución y agradecen

cualquier facilidad de contacto con lo que ya conocen. Además también resulta de gran utilidad a las propias organizaciones que lo utilizan porque pueden usar la potencialidad de Radius de contabilidad para realizar un seguimiento en caso de usos sospechosos o irregulares.

5. Estándar 802.1X

802.1X es un estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.

Este estándar se emplea en wireless añadiendo un Servidor de Autenticación a la transmisión de información, así cualquier host que desee conectarse a la WLAN deberá autenticarse a través de este servidor que, en caso que se produzca de manera satisfactoria habilitará un puerto de conexión que le permitirá al host acceder a los servicios de la WLAN. También proporciona la posibilidad de distribuir claves WEP, además del control de autenticación.

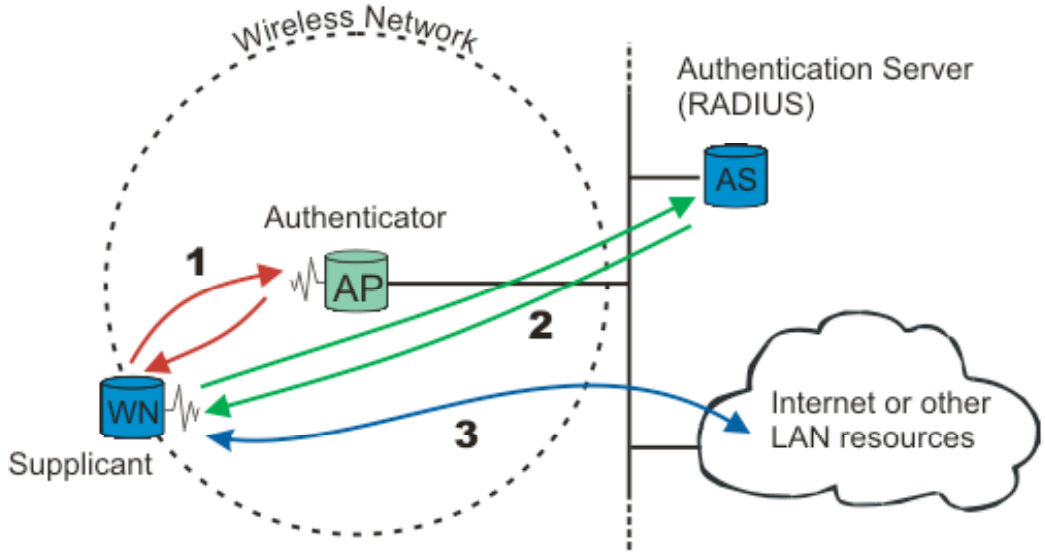
El protocolo 802.1x ofrece un marco en el que se lleva a cabo un proceso de autentificación del usuario, así como un proceso de variación dinámica de claves, todo ello ajustado a un protocolo, denominado EAP (Extensible Authentication Protocol). Mediante este procedimiento, todo usuario que esté empleando la red se encuentra autentificado y con una clave única, que se va modificando de manera automática y que es negociada por el servidor y el cliente de manera transparente para el usuario. El servicio soporta múltiples procesos de autenticación tales como Kerberos, certificados públicos, claves de una vez y el protocolo que estamos estudiando: RADIUS.

Para entender cómo funciona el protocolo 802.1x sigamos el siguiente esquema.

- El cliente, que quiere conectarse a la red, manda un mensaje de inicio de EAP que da lugar al proceso de autentificación. Para explicar todo esto más claramente vamos a seguir un ejemplo: imaginemos que un empleado necesita entrar en un recinto militar, esa persona banco pediría acceso al soldado que vigila la entrada (en nuestro caso RADIUS).
- El punto de acceso a la red respondería con una solicitud de autentificación EAP. En nuestro ejemplo, el soldado respondería solicitando el nombre y el apellido de la persona que quiere entrar, así como su huella digital. Además, antes de

preguntarle, el soldado le diría una contraseña al usuario, para que éste sepa que realmente es un soldado cualificado.

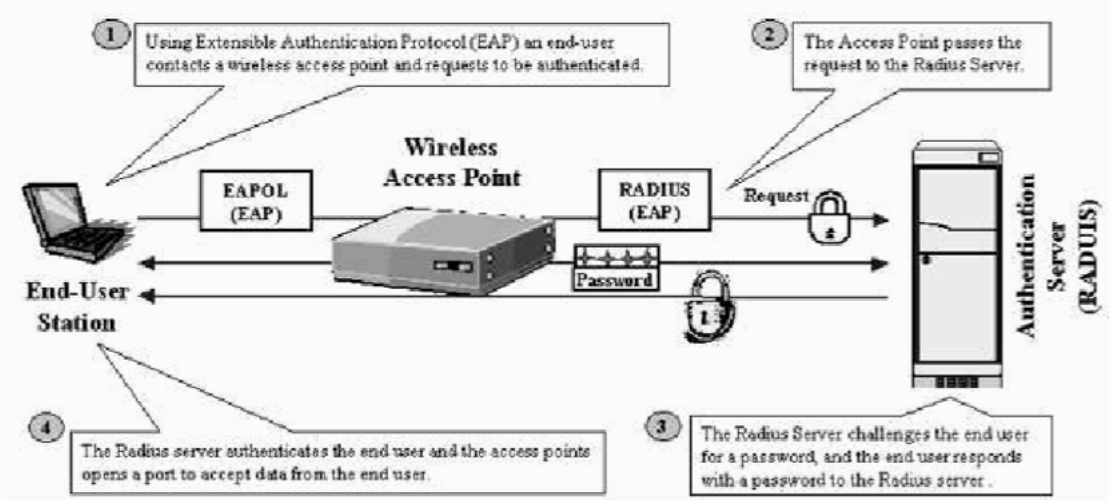
- El cliente responde al punto de acceso con un mensaje EAP que contendrá los datos de autentificación. Nuestro cliente le daría el nombre y los apellidos al soldado además de su huella digital.
- El servidor de autentificación verifica los datos suministrados por el cliente mediante algoritmos, y otorga acceso a la red en caso de validarse. En nuestro caso, el sistema del recinto militar verificaría la huella digital, y el soldado validaría que se correspondiese con el cliente.
- El punto de acceso suministra un mensaje EAP de aceptación o rechazo, dejando que el cliente se conecte o rechazándolo. Nuestro soldado le abrirá la puerta o no, en función de la verificación al cliente.
- Una vez autentificado, el servidor acepta al cliente, por lo que el punto de acceso establecerá el puerto del cliente en un estado autorizado. Nuestro usuario estará dentro de las instalaciones militares.



De esta manera, el protocolo 802.1x provee una manera efectiva de autentificar, se implementen o no claves de autentificación WEP. De todas formas, la mayoría de las instalaciones 802.1x otorgan cambios automáticos de claves de encriptación usadas solo para la sesión con el cliente, no dejando el tiempo necesario para que ningún programa de capturas de tramas sea capaz de obtener la clave.

El uso del protocolo 802.1x está en proceso de convertirse en un estándar. De hecho Windows XP® y Windows Vista implementan 802.1x de manera nativa, aunque necesita algún servidor Windows Server en la red. Por su parte MAC OS X también implementa todo el protocolo desde la versión 10.3. En cuanto a Linux actualmente se está trabajando en el proyecto conocido como Open1X que trabaja en un programa Xsupplicant que soportará este protocolo.

Aunque 802.1x no es específico para wireless proporciona mejoras para el control de acceso en WLAN's, por eso fabricantes como CISCO han diseñado protocolos propios empleando las funcionalidades que proporciona 802.1x en los niveles superiores a la capa MAC. (Otros fabricantes como Linksys han seguido sus pasos y mediante un sencillo proceso de configuración es posible usar estos protocolos).



6. Futuro

6.1. Deficiencias de Radius

Al tratarse de un protocolo con bastantes años a sus espaldas tiene severas deficiencias que lo hacen cada día más reemplazable. Utiliza MD5 como algoritmo de dispersión para almacenar contraseñas, algoritmo que por otra parte se ha demostrado inseguro hace apenas unos meses. Tiene graves problemas de escalabilidad, admitidos ya en su propia RFC. Al estar basado en UDP y no implementar el concepto de conexión, no permite llevar ningún tipo de control sobre el uso de un servicio una vez el usuario ha sido autenticado.

Adicionalmente, Radius es un protocolo salto a salto, lo que quiere decir que cada servidor Radius en la cadena de autenticación tiene acceso a los datos de autenticación del usuario. Este modelo de seguridad puede parecer suficiente cuando se utilizan escenarios simples en los que no existe el concepto de roaming, pero la realidad es que por lo general las cadenas de autenticación son largas e implican diversos servidores de distintas empresas. En estas circunstancias, el modelo salto a salto es claramente inseguro.

6.2. Posibles alternativas

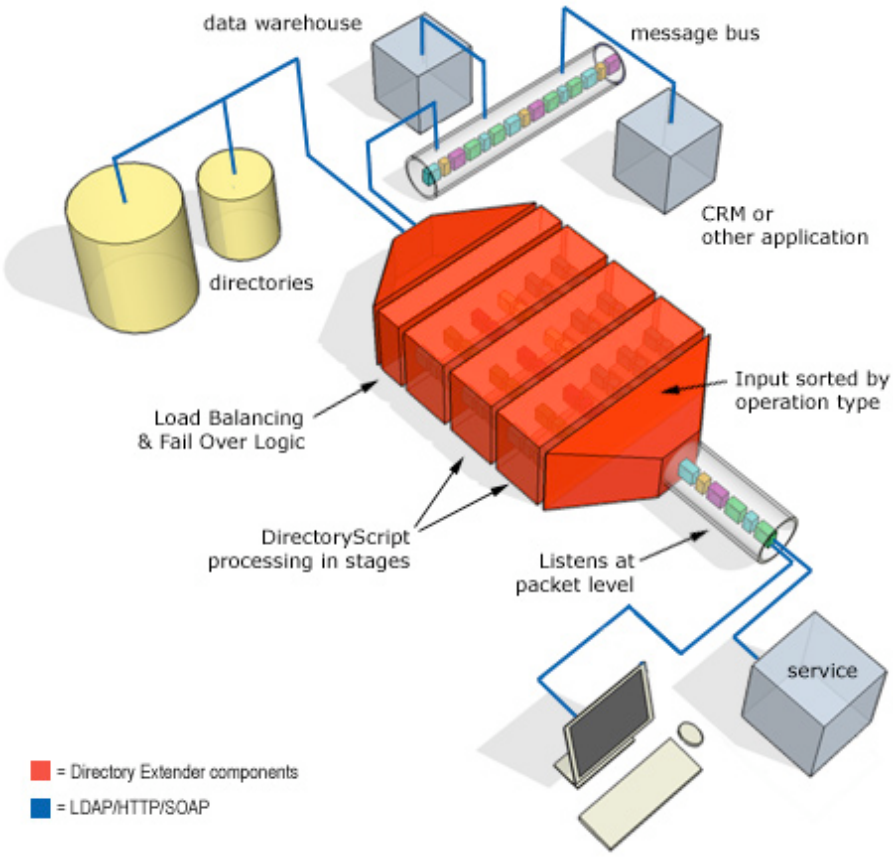
DIAMETER

DIAMETER es un protocolo de red para la autentificación, autorización y control (AAA) para aplicaciones tales como acceso de red o movilidad IP. El concepto básico es proporcionar un protocolo base que pueda ser extendido para proporcionar servicios AAA a nuevas tecnologías de acceso. Diameter está diseñado para trabajar en local y con roaming de AAA.

El nombre es un juego de palabras respecto al protocolo RADIUS, su predecesor

(un diámetro es el doble del radio). Diameter no es directamente compatible hacia atrás, pero proporciona un método de actualización desde RADIUS. Las principales diferencias son:

1. Usa protocolos de transportes fiables (TCP o SCTP, no UDP).
2. Usa seguridad a nivel de transporte (IPSEC o TLS).
3. Tiene compatibilidad transicional con RADIUS.
4. Tiene un espacio de direcciones mayor para AVPs (*Attribute Value Pairs*, pares atributo-valor) e identificadores (32 bits en lugar de 8).
5. Es un protocolo peer-to-peer en lugar de cliente-servidor: admite mensajes iniciados por el servidor.
6. Pueden usarse modelos con y sin estado.
7. Tiene descubrimiento dinámico de peers (usando DNS SRV y NAPTR)
8. Tiene negociación de capacidades.
9. Admite ACKs en el nivel de aplicación, definiendo métodos de fallo y máquinas de estado (RFC 3539).
10. Tiene notificación de errors.
11. Tiene mejor compatibilidad con roaming.
12. Es más fácil de extender, pudiendo definirse nuevos comandos y atributos.
13. Incluye una implementación básica de sesiones y control de usuario.


data warehouse
message bus
CRM or
other application
directories
Input sorted by
operation type
Load Balancing
& Fail Over Logic
DirectoryScript
processing in stages
Listens at
packet level
service
= Directory Extender components
= LDAP/HTTP/SOAP

7. Conclusiones

El protocolo RADIUS es un protocolo con un uso muy específico y especializado, como se ha visto a lo largo de este trabajo. Su extendido uso se debe a la veteranía del protocolo y al buen rendimiento que ha dado hasta el momento, aunque presente ciertas limitaciones (vistas en un punto anterior de este texto), que provocan que se esté sustituyendo paulatinamente.

8. Bibliografía

Información básica:

http://www.virusprot.com/Amzsolup.html

http://en.wikipedia.org/wiki/RADIUS

http://es.wikipedia.org/wiki/RADIUS

http://blackspiral.org/docs/pfc/itis/node12.html

definición del protocolo Radius:

http://tools.ietf.org/html/rfc2865

Donde se usa radius:

http://es.wikipedia.org/wiki/Conexi%C3%B3n_por_l%C3%ADnea_conmutada

Un pdf con un poco de historia sobre WLANS:

www.fundacionauna.com/areas/26_estudios/pdf/3.pdf

ppt de Radius en red europea iris:

www.rediris.es/moviris/recursos/presentaciones/Red%20de%20Servidores%20**Radius**.ppt

www.rediris.es/cert/doc/reuniones/fs2006/archivo/SanSebastian2006.pdf

Opinión de Radiator con breves explicaciones del funcionamiento general:

http://www.ciao.es/Radiator__Opinion_629062

Radiator:

http://www.open.com.au/radiator/index.html

Microsoft:

http://www.microsoft.com/latam/technet/articulos/wireless/pgch05.mspx

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/9ecf38e5-3200-490d-83d8-2c624da94d8b.mspx?mfr=true

http://www.microsoft.com/spain/technet/recursos/articulos/2008.aspx

Radius sin hardware:

http://www.wi-fiplanet.com/news/article.php/3089211

Definiciones (tanto de 802.1X como de Radius)

http://www.virusprot.com/Glosarioc.html

802.1X:

www.rediris.es/moviris/recursos/presentaciones/Infraestructura%20de%20RedIRIS.ppt

http://www.laflecha.net/articulos/wireless/redes_inalambricas/

http://www.networkworld.com/research/2002/0506whatisit.html

http://en.wikipedia.org/wiki/802.1x

DIAMETER

http://es.wikipedia.org/wiki/DIAMETER

http://en.wikipedia.org/wiki/DIAMETER

http://www.opendiameter.org/