Las redes inalámbricas tienen a su favor la flexibilidad que permite a los usuarios acceder a las mismas donde y cuando deseen, adquiriendo especial protagonismo la conexión a aplicaciones corporativas al mejorar la interacción empleado-empresa, consiguiendo que los trabajadores estén menos ligados al centro de trabajo y facilitando un mejor uso de los recursos disponibles. Sin embargo, esta tecnología conlleva riesgos que pueden afectar a la autenticación de los usuarios, así como a la integridad y confidencialidad de la información que transportan este tipo de redes, si no se toman las medidas adecuadas. Afortunadamente contamos en la actualidad con un amplio abanico de métodos de seguridad que limitan el acceso fraudulento a dichas redes, entre ellos destacamos en este reportaje el RADIUS —*Remote Authentication Dial-In User Service*—, orientado al acceso a redes móviles.

Radius: Mecanismo de seguridad en accesos desde movilidad

Alfonso Miñarro López,
Ingeniero Técnico de Telecomunicación (UPM).
Telefónica España

El germen de lo que hoy es el protocolo RADIUS se remonta al año 1991 cuando Merit Network, organización dependiente de la Universidad de Michigan, especificó en una RFI —*Request For Information*— los requisitos para reemplazar sus servidores *«dial-In»* propietarios por otros estandarizados, a la que respondió Livingston Enterprises (adquirida más tarde por Lucent Technologies) con la descripción de un Servidor Radius. En 1997 se convertiría en estándar mediante la publicación por parte del IETF —*Internet Engineering Task Force*— de las RFCs —*Request For Comments*— 2058 y 2059.

El protocolo Radius se ha aplicado en redes inalámbricas y les ha proporcionado mayor robustez y control de seguridad

En sus inicios debido a las soluciones tecnológicas del momento, se concibió para controlar de forma centralizada el acceso remoto de usuarios cuya conexión se realizaba mediante modems. A medida que se ha ido produciendo el desarrollo tecnológico, el protocolo RADIUS se ha implementando con éxito en escenarios de redes inalámbricas, ofreciéndoles la robustez y control necesarios en lo que a seguridad se refiere.

La implementación del protocolo RADIUS se divide en tres funciones: Autenticación, Autorización y Auditoría, formando parte de los protocolos conocidos con el término de «triple A».

La Figura 1 presenta estas funciones, mediante las cuales se pretende dar respuesta a preguntas como: ¿Quién eres?, ¿Qué tienes permitido hacer? y ¿Qué hiciste? antes, durante y después del acceso a la red respectivamente.

Basado en un modelo Cliente/Servidor, el cliente solicita al servidor los recursos o servicios que éste necesita, interviniendo en el proceso diferentes actores:

Este protocolo combina los procesos de autenticación y auditoría mediante el flujo de mensajes entre el cliente y el servidor Radius

— *El Cliente RADIUS:* El papel de cliente RADIUS lo representa el servidor de acceso a la red, o NAS —*Network Access Server*—, que proporciona el acceso a los recursos de la red a los usuarios finales.

— *El Servidor RADIUS:* De forma centralizada y segura se encarga de gestionar la información más sensible como las contraseñas y los perfiles de usuario, de disponer los recursos necesarios para gestionar el direccionamiento IP asociado a las sesiones de usuario establecidas, así como estadísticas relativas al número de éstas con la finalidad de poder generar los registros de CDR —*Call Data Record*— que permitan la facturación por los servicios prestados a los usuarios.

— *El protocolo:* La información AAA intercambiada entre el Cliente y el Servidor RADIUS se realiza mediante paquetes RADIUS encapsulados sobre el protocolo de transporte UDP —*User Datagram Protocol*— utilizando en la actualidad los puerto 1812 para la autenticación y 1813 para el *accounting*.

— *El método de Autenticación:* El Servidor Radius es capaz de soportar diferentes métodos de autenticación, entre los que destacan: PAP —*Password Authentication Protocol*—, CHAP —*Challenge Handshake Auhtentication Protocol*— o EAP —*Extensible Authentication Protocol*—.

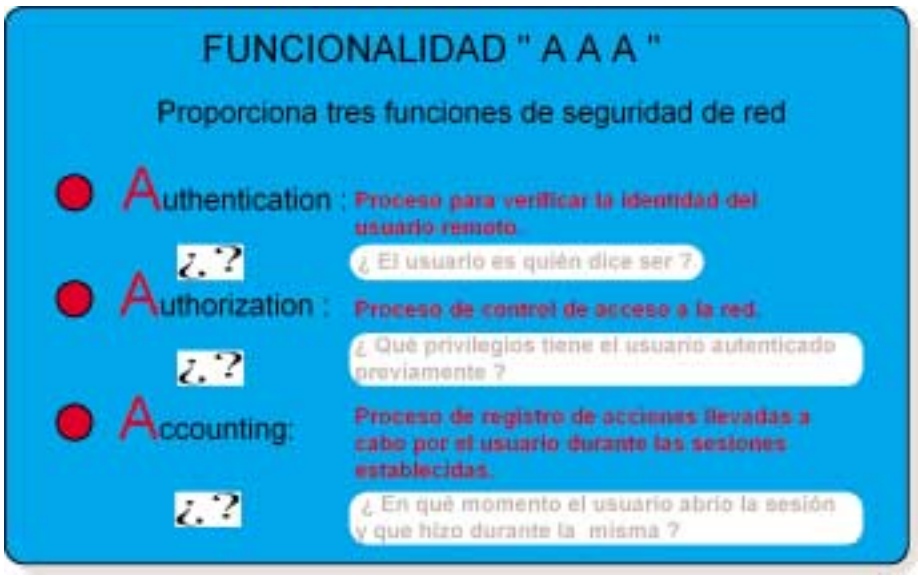

Figura 1: Claves de la arquitectura AAA (Authentication, Authorization, Accounting).

INTERCAMBIO DE MENSAJES RADIUS

Este protocolo combina los procesos de autenticación, autorización y auditoría mediante el flujo de mensajes entre el Cliente y el Servidor RADIUS que se puede observar en la Figura 2.

FASES DE AUTENTICACIÓN Y AUTORIZACIÓN

1. El usuario que desea tener acceso a la red, envía al Cliente Radius tanto su nombre de usuario como su clave de acceso empleando un protocolo de autenticación a nivel de enlace PPP —*Point to Point Protocol*—.

2. Una vez que el Cliente Radius ha obtenido los datos del usuario final, envía mediante un paquete *'Access-Request'* las credenciales de usuario, información de parámetros de conexión y la identificación del cliente Radius por la que está recibiendo la petición de acceso.

3. Cuando esta petición llega al Servidor Radius, éste verifica la información recibida en el paquete anterior (información del usuario, así como el secreto compartido entre el Servidor y el Cliente), pudiendo suceder:

3.a) Que el Servidor Radius decline la petición anterior, ya sea porque el usuario no sea válido o el servicio que solicita no le sea permitido, devolviendo el Servidor Radius al Cliente Radius un paquete *'Access-Reject'*, con la posterior desconexión del usuario.

3.b) Que las comprobaciones efectuadas por el Servidor Radius sean satisfactorias, devolviendo al cliente Radius un paquete *'Access-Accept'*, facilitando información extra como por ejemplo una dirección IP asignada, para el establecimiento de la sesión y dando lugar a la fase de *Accounting*.

FASE DE AUDITORÍA

4. Una vez que se completa con éxito la fase de autenticación, comienza la

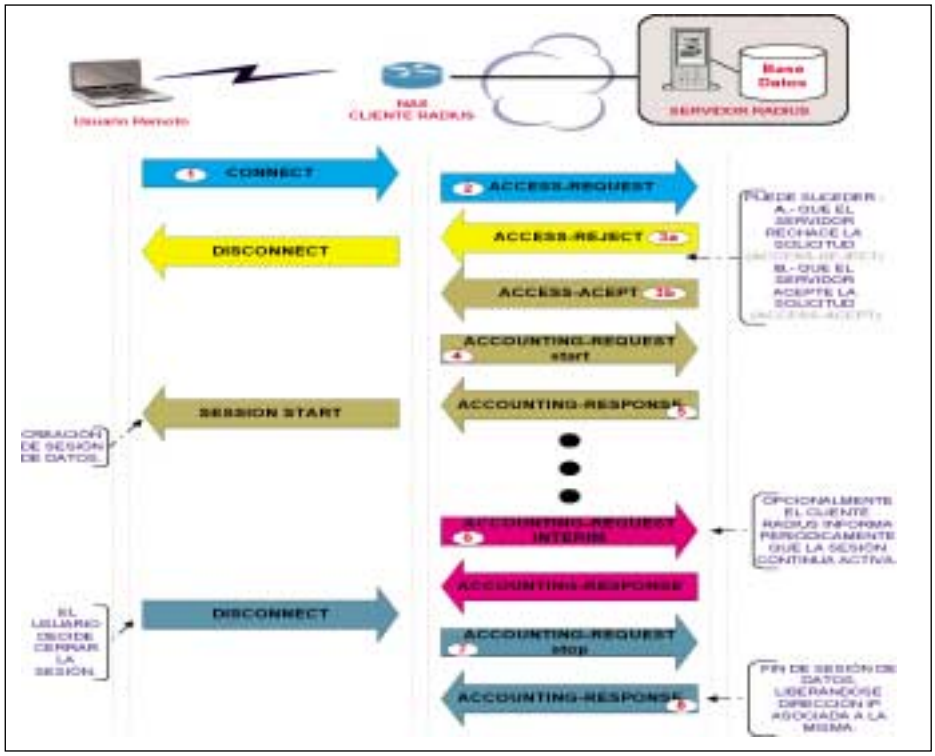

Figura 2: Diagrama de mensajes RADIUS para el establecimiento de una sesión.

fase de *Accounting* con el envío de un paquete *'Accounting-request (start)'* por parte del Cliente Radius hacia el Servidor Radius para indicar que el usuario se encuentra «logeado» en la red.

5. El servidor Radius contesta a éste con otro mensaje *'Accounting-response'* y desde ese momento el usuario está accediendo a los recursos solicitados en la fase anterior.

6. De forma periódica el Cliente Radius informa por medio del mensaje *'Accounting-Request (Interim)'* que la sesión establecida previamente continua activa y por tanto la dirección IP facilitada sigue en uso. Este mensaje será contestado por el Servidor Radius con un paquete *'Accounting-Response'*. Esta pareja de mensajes se repetirá en función de la duración de la sesión y de la periodicidad con que se envíen los mismos.

7. Una vez que el usuario desea finalizar la sesión establecida, el Cliente Radius envía un paquete de *'Accounting-Request (Stop)'*.

8. Por último el Servidor Radius responde con un paquete *'Accounting-Response'*, liberándose la dirección IP anteriormente asignada, no sin antes proceder por parte del Servidor Radius a guardar la información relativa a la sesión que acaba de finalizar:

— Identificación del usuario.

— Hora de inicio y final de la sesión del usuario.

— Duración de la conexión.

— Total de paquetes transferidos durante la sesión, tanto transmitidos como recibidos.

— La causa de la finalización de la sesión.

SERVICIOS DE DATOS EN MOVILIDAD

Entre los posibles servicios de datos que puede prestar un operador de red móvil podemos distinguir los siguientes:

— Servicio WAP —*Wireless Application Protocol*—.

— Servicio MMS, que permite el envío/recepción de mensajería multimedia.

— Acceso a Internet.

— Servicio Intranet, que ofrece el acceso a redes corporativas.

— Servicio M2M, que garantiza la comunicación con sistemas de control y telemedida.

— Servicio a otros operadores como por ejemplo los Operadores Móviles Virtuales que proliferan últimamente.

— Servicio PTT —*Push To Talk*—, que proporciona un método de comunicación en tiempo real entre un grupo de usuarios.

Para ofrecer estos servicios se necesita:

1.- Definir en los GGSN —*Gateway GPRS Support Node*— una serie de APNs —*Access Point Name*— que podemos clasificar en:

— *APN GENÉRICO:* Se denominan de este modo, a los APN que facilitan el acceso a los servicios de Internet, WAP, MMS al segmento residencial, no requiriendo provisión individual para cada usuario.

— *APN CORPORATIVO:* Los APN de corporaciones se definen para un grupo cerrado de usuarios permitiéndoles el acceso a la Intranet de la corporación que contrata el servicio.

— *APN OPERADORES:* Estos APN permiten a otros operadores de telecomunicaciones, normalmente OMVs apoyarse en otro operador para ofrecer servicios de datos a sus clientes.

2.- Realizar la provisión del direccionamiento IP en los siguientes elementos de red: el GGSN como equipo donde se crean los contextos en base a esas direcciones IP, el Servidor Radius como gestor de la asignación de direcciones IP y los equipos de transmisión como controladores del enrutamiento del tráfico a través de la red de datos.

Dentro del direccionamiento IP conviene distinguir tres entidades jerárquicas:

— *POOL:* Conjunto de direcciones IP asociadas a un determinado servicio y a un GGSN en particular.

— *RANGO:* Subconjunto de direcciones IP consecutivas dentro de un pool.

— *SESIÓN:* Asignación de una dirección IP concreta por parte del Servidor RADIUS, durante el tiempo que dura la conexión del cliente.

En función del tipo de servicio solicitado, se asigna direccionamiento IP público o privado, por ejemplo para acceso a Internet se emplean direcciones públicas por ser más aconsejable su uso para la libre navegación, mientras que para el acceso a WAP se define di-

TABLA 1: DIRECCIONAMIENTO IP

CLASES DE DIRECCIONANIENTO IP MÁS DESTACADAS
Definidas en la RFC 1166 "Internet Numbers"
Asignadas por ICANN (Internet Corporation for Assigned Names & Numbers)

Clase	Rango	Máscara de Red	Direcciones Privadas
A	1.0.0.0 hasta 127.0.0.0	255.0.0.0	10.0.0.0 a 10.255.255.255
B	128.0.0.0 hasta 191.255.0.0	255.255.0.0	172.16.0.0 a 172.31.255.255
C	192.0.0.0 hasta 223.255.255.0	255.255.255.0	192.168.0.0 a 192.268.255.255

reccionamiento IP privado (más abundante que el público). En el caso de las corporaciones se emplea direccionamiento IP privado en casi la totalidad de los casos.

La Tabla 1 representa las tres clases de direccionamiento IP más destacadas, definidas por el IETF en la RFC 1166 y asignadas por el organismo Internacional ICANN.

SOLUCIÓN RADIUS EN REDES MÓVILES

Sin duda, la introducción de la solución RADIUS como responsable del control de acceso y gestión de sesiones mediante conexiones por GPRS/UMT, aporta a los operadores de redes móviles la tranquilidad de ofrecer a sus clientes un servicio de datos robusto al proporcionar un servicio de autenticación y autorización fiable.

La Figura 3 se muestra la arquitectura típica de la solución Radius incluida en el Núcleo de Red de Paquetes de un operador de red móvil, principalmente porque en los GGSN reside la funcionalidad del Cliente Radius.

En función de la mayor o menor redundancia y/o reparto de carga entre los Servidores Radius de la que queramos dotar esta solución, se incorporaran más o menos elementos, pero básicamente el Hardware de la solución RADIUS la forman una serie de frontales Radius, que actúan como servidores para los GGSNs y una Base de Datos encargada de gestionar la asignación del direccionamiento IP a las sesiones establecidas por los usuarios.

La Base de Datos se subdivide en varias entidades funcionales, donde destacan el gestor de direcciones IP para la reserva/asignación/liberación de la dirección IP y el gestor de sesiones para el registro de la información de la sesión.

La comunicación entre el plano de servicios y la Base de Datos se realiza por medio del interfaz LDAP —*LightWeight Directoty Access Protocol*— con el fin de que los servicios realicen consultas de las sesiones de usuario, como por ejemplo, ¿qué MSISDN es el que está usando determinada IP con la finalidad de proceder al cobro de los recursos empleados?

TRAYECTO GGSN – SERVIDOR RADIUS: MODO DE ASIGNACIÓN DE IPS

En la Figura 3, se distinguen varios tramos de transporte IP por los que transcurre la comunicación desde que un usuario desea hacer uso de un servicio de datos determinado hasta que finalmente lo disfruta. Para el caso que nos ocupa nos interesa centraremos en el tramo GGSN-Radius y en el proceso de asignación de Ips.

Previa consulta al HLR por parte del SGSN para verificar si el usuario tiene permitido el acceso al servicio de datos, el GGSN debe crear un contexto PDP —*Packet Data Protocol*—, siendo necesario para ello la solicitud al Servidor RADIUS de una dirección IP, que emplea el terminal del usuario durante el intercambio de paquetes con la red externa.

La Figura 4 representa el proceso de autenticación y de solicitud de dirección IP, donde se distinguen dos fases:

FASE CAP: En la que se produce la autorización y se obtiene información de las características de tarificación asociadas al usuario mediante consulta del Servidor Radius al Servidor de Identificación de Usuarios.

FASE SAP: En esta fase se producen las funciones de autenticación y *accounting*, solicitando el Servidor RADIUS a la Base de Datos la asignación de una dirección IP disponible.

El proceso de asignación de IP se caracteriza por el siguiente ciclo de vida:

— Dirección *IP reservada*: En el proceso de Autenticación y mediante el mensaje de *'Access Request'* se procede a la reserva de una IP.

— Dirección *IP asignada*: la IP reservada previamente se confirma con la llegada del mensaje *'Accounting-request (start)'* al Servidor RADIUS por parte del GGSN, dándose comienzo a una sesión.

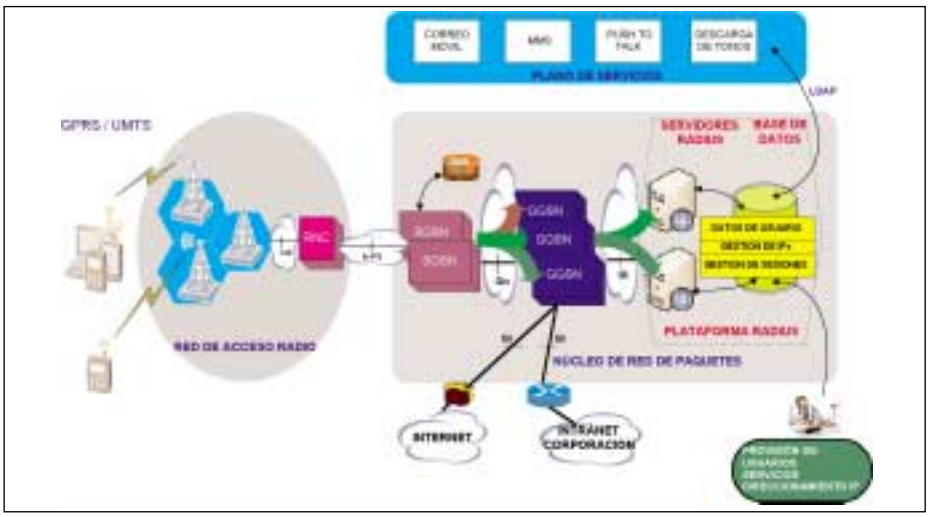

Figura 3: Topología de la Solución Radius en una red Móvil.

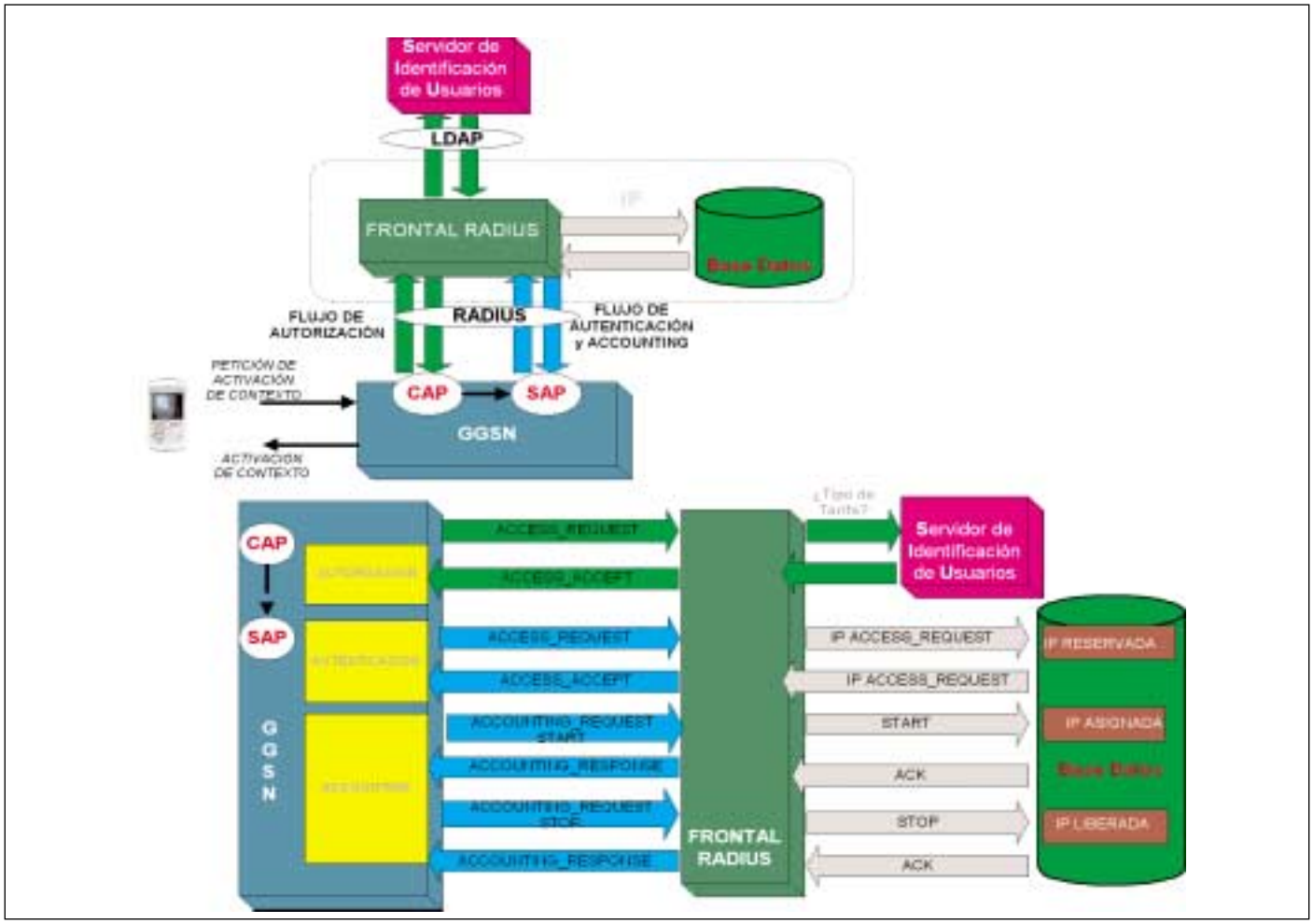

Figura 4: Autenticación y Asignación de IPs.

— Dirección *IP liberada*: Cuando llega el mensaje *'Accounting-request (stop)'* al Servidor Radius por parte del GGSN, procediéndose a finalizar la sesión, quedando la IP disponible para uso futuro.

RADIUS EN ENTORNOS CORPORATIVOS

Si bien, el operador móvil deberá proporcionar un APN específico para cada una de las empresas que contraten el servicio, el GGSN que lo tiene provisionado será el encargado de realizar una petición de autenticación, autorización y *accounting* contra el servidor Radius del operador, siendo posible varias alternativas:

— Que la empresa NO disponga de Servidor Radius en su red:

En este caso la autenticación del usuario se realiza en el propio Servidor Radius del operador móvil y es lo que se conoce como AUTENTICACIÓN BÁSICA.

— Que la empresa SI disponga de Servidor Radius:

Aprovechando que el Servidor Radius del operador puede actuar como Servidor Proxy hacia el Servidor Radius de la corporación, será este último el que realizará la autenticación de sus usuarios, dando lugar a una AUTENTICACIÓN DELEGADA.

Al ser abierto, este protocolo proporciona ventajas, como la posibilidad de soportar diferentes esquemas de autenticación

CONCLUSIONES

En la introducción comentaba que, tecnológicamente las redes inalámbricas aportan beneficios importantes en términos de movilidad y flexibilidad, sin olvidar que la seguridad en este tipo de entornos es fundamental, debido al aumento de dispositivos móviles y a la proliferación de las actividades que esto conlleva.

El hecho de que el protocolo RADIUS sea abierto, proporciona ventajas, en cuanto a que puede soportar diferentes esquemas de autenticación, además de estar ampliamente extendido debido a la cantidad de productos que implementan este protocolo.

Tabla 2: Evolución de las normas sobre RADIUS

RFC	TÍTULO	FECHA PUBLICACIÓN	ESTADO
2058	Remote Authentication Dial In User Service (RADIUS)	01/1997	Obsoleta por RFC2138
2059	RADIUS Accounting	01/1997	Obsoleta por RFC2139
2138	Remote Authentication Dial In User Service (RADIUS)	04/1997	Obsoleta por RFC2865
2139	RADIUS Accounting	04/1997	Obsoleta por RFC2866
2548	Microsoft Vendor-specific RADIUS Attributes	03/1999	Informativa
2618	RADIUS Authentication Client MIB	06/1999	Obsoleta por RFC4668
2619	RADIUS Authentication Server MIB	06/1999	Obsoleta por RFC4669
2620	RADIUS Accounting Client MIB	06/1999	Obsoleta por RFC4670
2621	RADIUS Accounting Server MIB	06/1999	Obsoleta por RFC4671
2809	Implementation of L2TP Compulsory Tunneling via RADIUS	04/2000	Informativa
2865	Remote Authentication Dial In User Service (RADIUS)	06/2000	Propuesta como estándar (Actualizada con RFC2868, RFC3575, RFC5080)
2866	RADIUS Accounting	06/2000	Informativa (Actualizada con RFC2867, RFC5080)
2867	RADIUS Accounting Modifications for Tunnel Protocol Support	06/2000	Informativa (Actualiza la RFC2866)
2868	RADIUS Attributes for Tunnel Protocol Support	06/2000	Informativa (Actualiza la RFC2865)
2869	RADIUS Extensions	06/2000	Informativa (Actualizada con RFC3579, RFC5080)
2882	Network Access Servers Requirements: Extended RADIUS Practices	07/2000	Informativa
3162	RADIUS and IPv6	08/2001	Propuesta como estándar
3539	Authentication, Authorization, and Accounting (AAA) Transport Profile	06/2003	Propuesta como estándar
3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)	07/2003	Propuesta como estándar Actualiza la RFC2865
3576	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	07/2003	Obsoleta por RFC5176
3579	RADIUS Support For Extensible Authentication Protocol (EAP)	09/2003	Informativa (Actualiza la RFC2869; Actualizada con RFC5080)
3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	09/2003	Informativa
4590	RADIUS Extension for Digest Authentication	07/2006	Obsoleta por RFC5090
4668	RADIUS Authentication Client MIB for IPv6	08/2006	Propuesta como estándar
4669	RADIUS Authentication Server MIB for IPv6	08/2006	Propuesta como estándar
4670	RADIUS Accounting Client MIB for IPv6	08/2006	Propuesta como estándar
4671	RADIUS Accounting Server MIB for IPv6	08/2006	Informativa
4672	RADIUS Dynamic Authorization Client MIB	09/2006	Informativa
4673	RADIUS Dynamic Authorization Server MIB	09/2006	Informativa
4675	RADIUS Attributes for Virtual LAN and Priority Support	09/2006	Propuesta como estándar
4818	RADIUS Delegated-IPv6-Prefix Attribute	04/2007	Propuesta como estándar
4849	RADIUS Filter Rule Attribute	04/2007	Propuesta como estándar
5080	Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes	12/2007	Propuesta como estándar
5090	RADIUS Extension for Digest Authentication	02/2008	Propuesta como estándar
5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	01/2008	Informativa (Actualiza la RFC3576)
5607	Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management	07/2009	Propuesta como estándar
5608	Remote Authentication Dial-In User Service (RADIUS) usage for Simple Network Management Protocol (SNMT) transport Protocol	08/2009	Propuesta como estándar

El protocolo RADIUS se creó en su momento para cubrir unas necesidades que se limitaban a ofrecer mecanismos de identificación y acceso de los usuarios por medio de la comprobación de su identidad, el control de los servicios que usaban y el mantenimiento posterior de una contabilidad de uso y aunque en la actualidad surgen otro tipo de requerimientos como el control de sesiones y errores, la continuidad de RADIUS parece estar asegurada, al abrirse nuevas líneas de investigación por parte del grupo de trabajo del IETF conocido como RADEXT —*RADIUS EXTensions*—, entre las que destaca la implementación de RadSec, o Radius seguro sobre la capa de transporte TCP que sustituye UDP.

El estado actual de dichos trabajos de investigación han permitido hasta este momento elaborar la versión 5 del borrador de una futura norma que lleva por nombre *TLS encryption for RADIUS over TCP (RadSec).*

PARA SABER MÁS

Para la elaboración del trabajo que habéis tenido oportunidad de leer, y que deseo haya sido de vuestro agrado, se ha consultado la siguiente documentación:

— *http://www.ietf.org/* Para acceso a consulta de RFCs.

— *http://www.cisco.com/ipj* The Internet Protocol Journal.

Volume 10, number 1 March 2007

Volume 10, number 2 June 2007

— *RADIUS Securing Public Access to Private Resources.* Autor: Jonathan Hassell. 10/2002. Editorial: O´Reilly.

— *Servicios Avanzados de Telecomunicación*. Autor: Mª Carmen España Boquera. Año 2003. Editorial: Díaz Santos.

— *AAA and network security for mobile access.* Autores: Madjid Nakhjiry & Mahsa Nakhjiri. 09/2005. Editorial: John Wiley and Son.

— *Cisco GGSN Release 8.0 Configuration Guide.* 04/2008.

ANEXO

Se podría pensar que los más de 12 años transcurridos desde la publicación de las primeras normas relacionadas con RADIUS, es tiempo más que suficiente para que dicho protocolo estuviese obsoleto. La tabla 2 quiere demostrar todo lo contrario presentando su continua evolución a través de las distintas normas publicadas hasta el momento, haciéndolo un protocolo con vigencia.