Universidad de las Ciencias Informáticas

Facultad 2


# Protocolo Diameter para los procedimientos de la AAA (Authentication, Authorization y Accounting)

Trabajo de Diploma para optar por el título de

Ingeniero en Ciencias Informáticas

Autores: Yaima Gómez Chirino

Randy Soto Naranjo

Tutores: Ing. Manuel Cheong Gómez

Ing. Alberto Arce Martínez

Ciudad de la Habana, junio 2009

# Declaración de Auditoría

*Por este medio declaramos que somos los únicos autores de este trabajo y autorizamos a la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.*

*Para que así conste firmo la presente a los ____ días del mes de ___ del año 2009.*

| | |
|---|---|
| _____ | _____ |
| Firma del Autor | Firma del Autor |
| **(Yaima Gómez Chirino)** | **(Randy Soto Naranjo)** |
| _____ | _____ |
| Firma del Tutor | Firma del Tutor |
| **(Ing. Manuel Cheong Gómez)** | **(Ing. Alberto Arce Martínez)** |

# Agradecimientos

*A mis padres (Elia Esther y Calixto) por siempre estar ahí cuando los he necesitado en los buenos y malos momentos dándome su apoyo y amor. Por haberme hecho la mujer que hoy soy, porque a nadie más que a ellos les debo todo esto. Por ser los mejores padres del mundo. Los quiero con todo mi corazón….*

*A mi pequeña (Daima) que siempre está a mi lado dándome su cariño, que es la alegría de mi vida. Eres la hermana más linda del mundo. Te quiero mucho….*

*A mi hermano (Carlos Manuel) porque fue mi guía desde que era pequeña, por su preocupación y amor, y porque eres el médico más bueno del mundo. Gracias por todo, te quiero con la vida….*

*A (Orleysis) por todo su amor y comprensión, por hacerme sentir tan feliz e importante, por tantos consejos y por tanto amor. Te amo mucho mucho……*

*A mis abuelos (Papín y mami Elia) por su amor y preocupación en todos estos años. Los quiero mucho….*

*A mis tías, mi tío y mis primos por su preocupación y cariño.*

*A (Noilsa, Yusy y Mairelis) que a pesar de la distancia no han cambiado en nada y siguen siendo tan buenas amigas como antes. Gracias por su amistad….*

*A mis amigas (Clairet, Lisy y Carmen) que han sido mi familia en estos cinco años…*

*A mi compañero de tesis (Randy) que fue un buen colega y un buen amigo. Gracias por ayudarme a cumplir mi sueño.*

*A mis tutores, al profesor Orlando y a Marleodys e Ivanierk por su ayuda.*

*A todos mis compañeros en estos cinco años de universidad.*

*A todos Muchas Gracias.*

*Yaima*

*A mis padres (Ramón Soto y Mayra M. Naranjo Castro) por haberme guiado por todo este turbulento camino por enseñarme a levantarme cada vez que tropecé por tanto aliento que me dieron, Uds. fueron siempre mi mayor guía y mi inspiración a llegar donde estoy los quiero mucho.....*
*A mi hermana (Yenni) que tanto la quiero.*

*A mi abuela (Irene) por toda su ayuda y comprensión.*

*A mis familiares le agradezco mucho en especial a mi tía Mirian Naranjo Castro la cual a estado siempre a mi lado apoyándome en todo lo que le fue posible.*
*A Susel por todo su apoyo, amor y cariño que ella me ha sabido dar.... te quiero.*

*A mis amigos de todos estos años en especial a (Ivanier, Marleodys, Fabio, Juan Carlos, Héctor, Edel, Frank, Daniel, Andrés, José A, José R, Aimel, Aleida, Lisbet) a todos ustedes muchas gracia por ser tan buenos conmigo, a mis compañeros que siempre estuvieron a mi lado cuando los nesesite gracias también.*
*A aquellos que no fueron tan amigos, me hicieron mejor personas por sus criticas que siempre las tuve presentes, y me ayudaron ha ver el mundo de otra manera, que excite la bondad pero tan bien esta cargada de gente como Uds. que se encargan de hacerle imposible la vida al de al lado gracias.....*
*A mi compañera de tesis (Yaima) que fue una buena colega y una buena amiga.*

*A Orlando Agramonte sin ti mi hermano estaría en cero todavía, tu sabes lo que te digo.....*

*A mi tutores Manuel Cheong y Aberto Arce gracias por su ayuda.*

*Al tribunal en general gracias por ser justo conmigo.*

*Randy*

# Dedicatoria

*A mi mamá Elia Esther, a mi papá Calixto, a mis hermanos*
*y a todos mis seres queridos por ayudarme a ser mejor cada día……*

*Yaima*

*A mis padres (Ramón y Mayra), a mi hermana*
*y a todos mis seres queridos….*

*Randy*

# Resumen

La Universidad de las Ciencias Informáticas (UCI) es una institución que carece de seguridad y confiabilidad en su red inalámbrica, lo que provocaría que cualquier persona pueda conectarse a la red sin autorización. Dirigiendo la investigación a sentar las bases en el estudio de un protocolo que resuelva los problemas de seguridad actualmente existentes en la red inalámbrica de la UCI. En el presente trabajo se llevó a cabo una investigación del protocolo Diameter, en él se darán a conocer sus principales características, funciones y mejoras sobre sus antecesores. También se investigó aspectos relacionados con la infraestructura de red inalámbrica que existe hasta el momento en la Universidad de las Ciencias Informáticas y a partir de las necesidades y deficiencias de esta se toma este protocolo como objeto de estudio. Es importante señalar que el estudio del protocolo Diameter se llevó aparejado conjuntamente con el protocolo AAA (Autenticación, Autorización y Contabilización) debido a las funciones que brinda conjuntamente con Diameter, de él se detallan sus principales características.

Se pretende que este proyecto sirva de soporte bibliográfico a la hora de utilizar el protocolo Diameter en la infraestructura de red inalámbrica existente en la universidad.

Palabras claves: red inalámbrica, seguridad, protocolo, Diameter, AAA.

# Indice

# Introducción

En los últimos años se ha visto como el empleo de la nuevas tecnologías de comunicación han pasado a ser parte de la vida cotidiana. A medida que el tiempo ha pasado las redes de ordenadores han dejado de ser un medio de comunicación para un segmento específico de la población para ser utilizadas por la mayoría de los ciudadanos, empresas e instituciones de aprendizaje, utilizándose para distintas actividades que varían desde el comercio electrónico hasta el control logístico en diversas compañías. El auge del uso de las redes de comunicación ha tenido múltiples consecuencias, pudiendo destacar entre ellas el aumento e importancia de la información que fluye por estas redes, siendo desplazado el término redes de ordenadores por el de redes de comunicación.

Esta expansión de las redes de comunicación ha llevado aparejado el incremento de la información, por lo cual se ha hecho habitual utilizarla para indefinidas operaciones tan comunes como llevar a cabo transacciones administrativas por ejemplo bancarias, comunicación en tiempo real con personas de todo el mundo e incluso descargar distintos tipos de archivos para el trabajo o simplemente para el entretenimiento personal. En la mayoría de los casos encontramos que esta información requiere algún tipo de protección en su tránsito por las diferentes redes ya sea mediante servicios de confidencialidad y de autenticación; además el aumento en el uso de las redes de comunicación ha traído consigo un incremento en el tipo de dispositivos y protocolos de comunicación para lograr el desarrollo de una comunicación segura donde el uso de los protocolos es una parte fundamental ya que son un conjunto de normas o reglas que permiten el intercambio de información entre dos dispositivos de un mismo nivel. Estos ayudan no sólo a la comunicación, sino que permiten entre varias cosas la corrección de errores. (1)

Existen muchos protocolos los cuales facilitan la comunicación básica, pero cada uno tiene diferentes propósitos y realiza distintas tareas como es el caso de los protocolos de seguridad donde se puede destacar el protocolo AAA (2) en el que sus principales funciones son Autenticación, Autorización y Contabilización que incluye los tres servicios que debe tener todo sistema seguro.

La autenticación es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.

La autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.

El servicio accounting es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, de planeamiento de capacidad, auditoría. Estas AAA se combinan a veces con auditoría convirtiéndose en AAAA.

Las tecnologías, y como caso particular las redes, pueden considerarse como herramientas para fortalecer los vínculos internos y externos entre personas de todo el mundo y facilitar su acceso a herramientas e información, así como para abrir espacios de trabajo e intercambio. Las redes inalámbricas, y en especial tecnologías como Wi-Fi, cuentan con características que facilitan esta posibilidad. Estas redes han alcanzado un gran auge en todo el mundo, desde el 2005 en Europa los puntos de conexión públicos superan a los 90000 y se encuentran ubicados en aeropuertos, hoteles, biblioteca, restaurantes o cafés. Este crecimiento no ha venido aparejado de igual manera en todos los países, en los subdesarrollados las redes inalámbricas tienen un nivel prematuro aunque se han venido fomentando proyectos como es el caso del TRICALCAR (Tejiendo Redes Inalámbricas Comunitarias en América Latina y el Caribe) el cual pretende que el desarrollo de estas redes sirva para ampliar la conectividad a comunidades rurales y urbano marginales que no han podido aprovechar aún de los beneficios de las TIC(Tecnología de la Información y las Comunicaciones).En Cuba debido al embargo económico que existe, la puesta en práctica de las redes inalámbricas solamente se ha venido observando en la telefonía móvil donde las empresas rectoras de estos sistemas son ETECSA , CUBATEL y la UCI(Universidad de las Ciencias Informáticas).En la actualidad se esta llevando a cabo un estudio a fondo para la implementación de estas tecnologías con la ayuda de nuestra hermana República Bolivariana de Venezuela a partir del proyecto del Cable Submarino Venezuela – Cuba.

La Universidad de las Ciencias Informáticas (UCI) es una institución que cuenta con una gran cantidad de usuarios que necesitan tener una infraestructura de red inalámbrica segura, de alta velocidad, de gran potencia y que soporte un elevado número de usuarios conectados simultáneamente. Actualmente la configuración que tiene no satisface estas necesidades ya que no se puede hablar de una red inalámbrica sino de puntos de acceso que iluminan áreas específicas de la universidad como es el rectorado y algunos proyectos productivos en los docentes. Estos puntos de acceso no están bien configurados por lo que no cumplen con las buenas prácticas que se proponen a nivel internacional para garantizar la seguridad en este tipo de infraestructura, lo que traería aparejado que cualquier persona pueda conectarse a la red sin autorización.

Debido a la gran importancia que tiene la seguridad en cualquier sistema de red se ha decidido plantear la **siguiente problemática**: ¿Cómo lograr la seguridad en una infraestructura de red inalámbrica?

El **objeto de estudio** del presente trabajo es el protocolo Diameter sobre los procedimientos de la AAA para lograr la seguridad requerida en la red inalámbrica. Reconociendo además como **campo de acción** dicho protocolo para redes inalámbricas en la Universidad de la Ciencias Informáticas (UCI).

Para guiar la investigación y tomando en cuenta lo analizado hasta el momento se decide trabajar sobre la base de la siguiente **idea a defender:** lograr mejoras en la infraestructura de la red inalámbrica de la UCI a partir de la utilización del protocolo Diameter sobre los procedimientos de la AAA.

El **objetivo general** de la investigación es: el estudio del protocolo Diameter sobre los procedimientos de la AAA para lograr la seguridad en la red inalámbrica en la UCI (Universidad de las Ciencias Informáticas).

Del objetivo general se derivan los siguientes **objetivos específicos**:

1. Identificar los problemas de seguridad reales de la red inalámbrica en la UCI.
2. Describir el funcionamiento del protocolo Diameter sobre los procedimientos de la AAA.
3. Mejoras de Diameter que permiten utilizarlo como mecanismos para asegurar los accesos a la red inalámbrica de la UCI.

### Tareas de la investigación:

1- Realizar un estudio acerca de los distintos protocolos de comunicación.

2- Realizar un estudio de las Redes Inalámbricas.
3- Realizar un estudio acerca del funcionamiento de los procedimientos de la AAA.
4- Realizar un estudio acerca de todo lo relacionado con el protocolo Diameter a partir de los procedimientos de la AAA.

Para la realización de estos objetivos se emplearon los métodos siguientes:
**Métodos Teóricos:** Permiten estudiar las características del objeto de investigación que no son observables directamente.

**- Histórico-Lógico:** Los métodos históricos analizan la trayectoria completa del fenómeno, revela las etapas principales de su desenvolvimiento y las conexiones históricas fundamentales. Los métodos lógicos se basan en el estudio histórico del fenómeno, ponen de manifiesto la lógica interna de su desarrollo, de su teoría y hallan el conocimiento mas profundo de su esencia.

**- Análisis y Síntesis:** El análisis permite la división mental del fenómeno en sus múltiples relaciones y componentes para facilitar su estudio y la síntesis establece mentalmente la unión entre las partes previamente analizadas, posibilita descubrir sus características generales y las relaciones esenciales entre ellas.

**Métodos empíricos:** Estos métodos nos permiten extraer de los fenómenos analizados las informaciones que se necesitan sobre ellos a través de observaciones, del uso de técnicas opináticas y la propia experimentación.

**-Observación:** Registro visual de lo que ocurre en una situación real, en un fenómeno determinado, clasificando y consignando los hechos y acontecimientos pertinentes de acuerdo con algún esquema previsto.

**-Entrevista:** Es una conversación planificada para obtener información. Su uso constituye un medio para el conocimiento cualitativo de los fenómenos o sobre características personales del entrevistado y puede influir en determinados aspectos de la conducta humana por lo que es importante una buena comunicación.

El presente trabajo de diploma consta de cuatro partes fundamentales: resumen, introducción, desarrollo y conclusiones. El desarrollo esta estructurado en 3 capítulos:

**Capítulo 1:** Fundamentación Teórica. En este capítulo se hace un análisis de la actualidad internacional y nacional sobre el tema de las redes inalámbricas así como el tema de los protocolos enfatizando en Diameter, además se abordan las principales definiciones que se tienen en cuenta durante todo el trabajo.

**Capítulo 2:** En este capítulo se describirán las características específicas y generales del protocolo Diameter con el objetivo de sirva de soporte bibliográfico a la hora de utilizar dicho protocolo, se abordara también acerca de sus servicios y aplicaciones.

**Capítulo 3:** En este capítulo se listarán algunas de las mejoras de Diameter a partir de una comparación de este con sus antecesores.

Para finalizar se presentan las conclusiones, recomendaciones, referencias bibliográficas, bibliografía y glosario de términos.

# Capítulo 1: Fundamentación Teórica

## 1.1 Introducción

En este capítulo se abordará acerca de los principales conceptos y términos estudiados en la investigación, dirigiéndonos al objetivo central que es el protocolo Diameter y sus aspectos relevantes para que sirva de base este estudio para garantizar la seguridad en la red inalámbrica de la universidad. Este protocolo será analizado a partir de sus antecesores el protocolo TACACS+, Radius y de su protocolo base AAA. Se detallarán también los antecedentes y actualidad tanto nacionales como internacionales del mismo.

## 1.2 Introducción a la temática. Redes inalámbricas

### 1.2.1 Un poco de historia

El primer protocolo de seguridad inalámbrica reconocido por IEEE (del inglés: Institute of Electrical and Electronics Engineers, es una sociedad profesional de ingenieros eléctricos y científicos informáticos) fue el WEP (del inglés: Wired Equivalent Privacy, algoritmo de seguridad para brindar protección a las redes inalámbricas). Permitía la utilización de claves encriptadas de 40 bits según el algoritmo de encriptación RC4 (3) (del inglés: Rivest Cipher 4, es un algoritmo de encriptación que se usa en algunos protocolos para proteger el tráfico de internet) y asignaba a cada máquina cliente una clave por sesión. Pero desde que en el verano de 2001 fuera hackeado empezó a considerarse como el Talón de Aquiles de la cadena de seguridad inalámbrica. Combinando WEP con el protocolo de autenticación 802.1X las cosas mejoraron algo, dado que en este esquema, el cliente WEP estaba obligado a solicitar acceso a la red utilizando EAP (del inglés: Extensible Authentication Protocol (EAP) es una autenticación framework usada habitualmente en redes WLAN) (4), tal como establece 802.1X.

Sin embargo, esta solución no resultó suficiente puesto que sólo cubría las carencias de WEP en el ámbito de la autenticación, dejando sin resolver la otra incógnita de cualquier ecuación de seguridad WLAN (del inglés: Wireless Local Area Network, es un sistema de comunicación de datos inalámbricos flexible) (la encriptación). Esta fue la razón por la que los fabricantes se pusieron manos a la obra en el desarrollo de WPA (del inglés: Wi-Fi Protected Access (WPA) es un estándar abierto internacional para

aplicaciones que utilizan las comunicaciones inalámbricas), que elevaba la potencia de la encriptación mediante la aplicación de la técnica TKIP (del inglés: Temporal Key Integration Protocol (TKIP) para mejorar el cifrado de datos inalámbricos) (5). Con este protocolo, la clave utilizada por cada cliente cambia en varias ocasiones durante cada sesión. Aparte de TKIP, la sustitución de RC4 por el algoritmo más fuerte AES (6) (del inglés: Advanced Encryption Standard, es un esquema de cifrado de bloques), desarrollado para el ejército estadounidense por el National Institute of Standards, aportaba una ventaja más a las prestaciones de seguridad ideadas para WPA.

Pero finalmente WPA se quedó sin AES (del inglés: Advanced Encryption Standard) debido a la impaciencia de los fabricantes ante la alta demanda de productos WLAN con mayores niveles de seguridad que los proporcionados por WEP. En consecuencia, la mayoría comenzó la comercialización de productos WPA sólo con TKIP.TKIP fue básicamente ideado como un parche para WEP y compartía con él muchas características, incluido el motor de encriptación y el algoritmo RC4. Su principal ventaja es que las claves utilizadas tienen un carácter temporal, pudiendo cambiar incluso para cada paquete dentro de una misma sesión. Así mismo, las claves son de mayor longitud, siempre de 128 bits. Por lo que, resultan más difíciles de violar que las utilizadas en el modelo WEP con RC4. A pesar de que TKIP (con WPA) constituyó probablemente en su momento la mejor solución disponible, nunca pudo deshacerse de los problemas que arrastró desde su mismo diseño. El protocolo debía operar sobre el hardware entonces existente, por tanto, no puede introducir encriptación avanzada, si antes dicho hardware no se actualiza con más potencia informática. Luego se creó el 802.11i una evolución de las tecnologías anteriores, fundamentalmente de WPA (Wi-Fi Protected Access), implementado ya hace tiempo por la industria, hasta el punto de que el nuevo estándar todavía se conoce también como WPA2 (Wi-fi Protected Access 2, es un sistema para proteger las redes inalámbricas). El estándar 802.11i elimina muchas de las debilidades de sus predecesores tanto en lo que autenticación de usuarios como a robustez de los métodos de encriptación. Y lo consigue en el primer caso gracias a su capacidad para trabajar en colaboración con 802.1X, y en el segundo, mediante la incorporación de encriptación AES. Aparte de incrementar de manera más que significativa la seguridad de los entornos WLAN, también reduce considerablemente la complejidad y el tiempo de roaming de los usuarios de un punto de acceso a otro.

Con estas ventajas, uno de los avances más importantes y de mayor valor para el mercado fue la movilización de las comunicaciones de datos mediante la utilización de tecnología inalámbrica como el Bluetooth, el protocolo 802.11 o Wi-Fi[2] y el uso de terminales móviles que soportan este tipo de tecnologías (GSM(del inglés: Global System for Mobile Communications, es el principal estándar para la

telefonía móvil digital)/GPRS(del inglés: General Packet Radio Service, extensión de GSM para la transmisión de datos) /UMTS(del inglés: Universal Mobile Telecomunications System, diseñada para introducir más usuarios a la red)/HSPA(del inglés: High Speed Packet Access, es un conjunto de protocolos que mejoran el ancho de banda sobre UMTS)).

### 1.2.2 Actualidad

La tendencia del uso de tecnologías inalámbricas y de dispositivos móviles es creciente. Las mejoras producidas en los anchos de banda, las coberturas territoriales y la facilidad de uso han permitido desarrollar nuevas aplicaciones y servicios en este entorno.

Durante los últimos años, las tecnologías inalámbricas se han ido consolidando como una de las tendencias claves de la industria, teniendo especial incidencia en favorecer la conectividad y la movilidad, dos objetivos muy demandados en la actualidad por todo tipo de usuarios.

Así como las redes inalámbricas de área local (WLAN) o Wi-Fi han ido ganando terreno tanto a nivel de hogar como de empresas, las redes WiMax (del inglés: Worldwide Interoperability for Microwave Access (WiMax) es una norma de transmisión de datos usando ondas de radio) se han ido posicionando como uno de los nuevos estándares con más futuro para masificar el acceso a internet, desatando una amplia expectativa mundial.

En el proceso de avance de las redes inalámbricas ha tenido mucho que ver la estandarización, que busca hacer compatibles los sistemas de múltiples proveedores y fabricantes. En el caso de Wi-Fi, por ejemplo, la IEEE desarrolló un grupo de especificaciones conocida como el estándar 802.11. Dicho estándar incluye el 802.11b (el más popular con 11Mbps, con un rango de alrededor de 100 metros), el 802.11a (con 54 Mbps y un rango un poco menor al anterior) y el 802.11g (que combina la velocidad de “a” y “b”). Actualmente la última generación de este estándar es el 802.11n el cual es superior a los anteriores mencionados, lo que muestra un gran avance para la tecnología inalámbrica. Este se dice que es superior debido a que tiene un mejor rendimiento, mayor alcance y una fiabilidad superior, para tener una idea este aumenta su rendimiento hasta 2.5 veces y tiene el doble de alcance en comparación con el anterior estándar el 802.11b.

En la medida que se han ido homologando los estándares, WiMax se ha ido perfilando como el próximo paso en la ruta hacia el mundo “de las redes inalámbricas”, extendiendo el acceso a banda ancha inalámbrica a nuevos lugares y distancias más largas. En efecto, desde sus inicios, la promesa de

WiMax fue ofrecer una solución a lo que algunos denominan el problema de la “última milla”, es decir, superar los costos y tiempos asociados a dotar de líneas de acceso a empresas o personas en nuevos puntos de las ciudades y regiones.

### ¿Qué es WiMax?

WiMax es una novedosa tecnología estándar de conexión a banda ancha a través de ondas de radio con mayor alcance y confiabilidad que las alternativas actuales. No sólo promete resolver los problemas de la “última milla”, sino convertirse también en una opción de conectividad móvil, con aplicaciones tanto para el hogar como para las empresas.

En términos más precisos, WiMax se conoce hoy como un estándar de transmisión inalámbrica de datos (el 802.16d) diseñado para ser utilizado en Redes de Área Metropolitana MAN (del inglés: Metropolitan Área Network, es una red de alta velocidad) que proporciona accesos en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología portátil LMDS (del inglés: Local Multipoint Distribution Service, es una tecnología de conexión vía radio inalámbrica).

Se espera que el estándar WiMax provea una solución “carrier class” que pueda escalar para soportar miles de usuarios en una misma estación base y proveer servicios de diferentes niveles. Esto permitiría que un sector de la estación base pueda brindar un rango suficiente de datos para soportar simultáneamente más de 60 negocios con conectividad tipo T1 (es el servicio de línea digital normalizado) y cientos de hogares con conectividad de tipo DSL (del inglés: Digital Subscriber Line, es una tecnología que asume los datos digitales).

### 1.2.3 Redes inalámbricas

En la actualidad con el objetivo de ganar en movilidad a la hora de trabajar desde cualquier lugar en que un usuario se encuentre, se están implementando en muchos lugares el uso de las redes inalámbricas. Las tecnologías de comunicación inalámbrica nos libran de la necesidad de utilizar los dispositivos atándolos a cables, con la comodidad que ello proporciona. Hoy en día casi todos los equipos con capacidad computacional parecen tener conectividad inalámbrica de algún tipo, sea Wi-Fi o Bluetooth. Incluso algunos teléfonos móviles de última generación proporcionan conectividad Wi-Fi para poder hacer llamadas y navegar por internet cuando estamos en la oficina o en casa sin tener que recurrir a GPRS o UMTS con sus costosas tarifas.

Las redes inalámbricas son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. Con una red cableada, un dispositivo tiene que estar en un punto fijo para mantenerse conectado y formar parte de ella. Con un dispositivo inalámbrico, sin embargo, al usuario le basta con estar dentro del radio de cobertura de la red para mantenerse conectado.

Las comunicaciones inalámbricas se caracterizan por poder transmitir información (voz o datos) sin necesidad de estar conectadas físicamente a ningún dispositivo intermedio o receptor (como es el caso de una conexión por cable). Existen al menos dos tipos de medios por los que se pueden propagar, ondas de luz o radio, y varios elementos que influyen en la calidad de la transmisión (las frecuencias, la calidad de las señales y las interferencias).

### 1.2.4 Principales problemas de seguridad inalámbrica.

Aparte de los problemas de seguridad que atañen también a las redes convencionales de cable, las redes inalámbricas presentan inconvenientes adicionales debidos a su propia naturaleza inmaterial. Dado que cualquiera puede interceptar los paquetes que se transmiten a través del espectro electromagnético. Es necesario cifrarlos de alguna manera para que los posibles espías no puedan interpretar su significado. El cifrado es la primera vertiente de la seguridad que debemos tener en cuenta de manera especial.

Con la configuración por defecto de la mayoría de los puntos de acceso, cualquiera puede intentar conectarse a la red si se encuentra dentro de su alcance y tiene un dispositivo adecuado. Por ello es especialmente importante conseguir un método fiable de autenticación o restricción de acceso que asegure que sólo los dispositivos o usuarios que se deseen serán capaces de conectarse a la red sin cables.

Aparte de los accesos no autorizados a la información, una red mal protegida puede hacer que los equipos sean utilizados para ataques distribuidos. Por lo que alguien pudiera estar usándolos para atacar a otras redes o servidores. A todos los efectos es como si fuéramos nosotros los que realizamos los ataques por lo que puede tener repercusiones legales.

Otra cuestión importante en la autenticación de los puntos de acceso, es que existen ataques realizados a la inversa, es decir, somos nosotros los que nos conectamos a un punto de acceso el cual está suplantando a otro auténtico, de modo que todo nuestro tráfico es analizado por el atacante obteniendo

acceso a la información. Por ello es tan importante que se autentique a los usuarios como a los servidores de entrada.

Como se ha observado para lograr la seguridad de una infraestructura de red inalámbrica es necesario mencionar y tratar los protocolos de comunicación para un mejor entendimiento del tema.

## 1.3 Protocolos

Los protocolos son reglas y procedimientos para la comunicación. El término protocolo se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

Se puede definir un protocolo como el conjunto de normas que regulan la comunicación (establecimiento, mantenimiento y cancelación) entre los distintos componentes de una red informática. Existen dos tipos de protocolos: protocolos de bajo nivel y protocolos de red. Los protocolos de bajo nivel controlan la forma en que las señales se transmiten por el cable o medio físico. Los protocolos de red organizan la información (controles y datos) para su transmisión por el medio físico a través de los protocolos de bajo nivel. (7)

Algunos protocolos sólo trabajan en ciertos niveles OSI (del inglés: Open Systems Interconection). El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red NIC (del inglés: Network Interface Card, permite la conexión entre diferentes aparatos conectados entre si) y salgan al cable de la red.

Los protocolos también pueden trabajar juntos en una jerarquía o conjunto de protocolos. Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos se corresponden con los niveles del modelo OSI. Por ejemplo, el nivel de aplicación del protocolo TCP/IP (Transmission Control Protocol / Internet Protocol) se corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

### 1.3.1 Protocolos en una arquitectura multinivel

En una red, tienen que trabajar juntos varios protocolos. Al trabajar juntos, aseguran que los datos se preparan correctamente, se transfieran al destino correspondiente y se reciban de forma apropiada.

El trabajo de los distintos protocolos tiene que estar coordinado de forma que no se produzcan conflictos o se realicen tareas incompletas. Los resultados de esta coordinación se conocen como trabajo en niveles. (8)

### Jerarquía de protocolos

Una jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía especifica un protocolo diferente para la gestión de una función o de un subsistema del proceso de comunicación. Cada nivel tiene su propio conjunto de reglas. Los protocolos definen las reglas para cada nivel en el modelo OSI:

| | |
|---|---|
| Nivel de Aplicación | Inicia o acepta una petición |
| Nivel de Presentación | Añade información de formato, presentación y cifrado al paquete de datos |
| Nivel de sesión | Añade información del flujo de tráfico para determinar cuándo se envía el paquete |
| Nivel de Transporte | Añade información para el control de errores |
| Nivel de red | Se añade información de dirección y secuencia al paquete |
| Nivel de enlace de datos | Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física |
| Nivel físico | El paquete se envía como una secuencia de bits |

**Fig1.1 Estructura de niveles del modelo OSI.**

Los niveles inferiores en el modelo OSI especifican cómo pueden conectar los fabricantes sus productos a los productos de otros fabricantes, por ejemplo, utilizando NIC de varios fabricantes en la misma LAN

(del inglés: Local Area Network, es la interconexión de varios ordenadores y periféricos). Cuando se utilizan los mismos protocolos, pueden enviar y recibir datos entre sí. Los niveles superiores especifican las reglas para dirigir las sesiones de comunicación (el tiempo en el que dos equipos mantienen una conexión) y la interpretación de aplicaciones. A medida que aumenta el nivel de la jerarquía, aumenta la sofisticación de las tareas asociadas a los protocolos.

El proceso por el cual se conectan los protocolos entre sí y con la NIC se conoce como: proceso de ligadura (binding process), el cual permite una gran flexibilidad a la hora de configurar una red. Se pueden mezclar y combinar los protocolos y las NIC según las necesidades. Por ejemplo, se pueden ligar dos jerarquías de protocolos a una NIC, como intercambio de paquetes entre redes e intercambio de paquetes en secuencia IPX/SPX (del inglés: Internet Work Packet Exchange/Sequenced Packet Exchange, es una familia de protocolos de red). Si hay más de una NIC en el equipo, cada jerarquía de protocolos puede estar en una NIC o en ambas.

El orden de ligadura determina la secuencia en la que el sistema operativo ejecuta el protocolo. Cuando se ligan varios protocolos a una NIC, el orden de ligadura es la secuencia en que se utilizarán los protocolos para intentar una comunicación correcta. Normalmente, el proceso de ligadura se inicia cuando se instala o se inicia el sistema operativo o el protocolo. Por ejemplo, si el primer protocolo ligado es TCP/IP, el sistema operativo de red intentará la conexión con TCP/IP antes de utilizar otro protocolo. Si falla esta conexión, el equipo tratará de realizar una conexión utilizando el siguiente protocolo en el orden de ligadura.

El proceso de ligadura consiste en asociar más de una jerarquía de protocolos a la NIC. Las jerarquías de protocolos tienen que estar ligadas o asociadas con los componentes en un orden para que los datos puedan moverse adecuadamente por la jerarquía durante la ejecución. Por ejemplo, se puede ligar TCP/IP al nivel de sesión del sistema básico de entrada/salida en red (NetBIOS), así como al controlador de la NIC. El controlador de la NIC también está ligado a la NIC.

### Capa de transporte del modelo OSI

Dentro de las 7 capas del modelo OSI es en la de transporte donde se encuentran los protocolos a tratar en esta investigación. Pues esta capa es la responsable de establecer y mantener una comunicación entre dos hosts. El nivel de transporte proporciona notificación de la recepción, control de flujo y secuenciación de paquetes. También gestiona las retransmisiones de paquetes. El nivel de transporte puede utilizar los protocolos TCP o el Protocolo de Datagramas de Usuario (UDP, es un

protocolo del nivel de transporte basado en el intercambio de datagramas) en función de los requerimientos de la transmisión.

### Propiedades típicas de los protocolos

- Detección de la conexión física sobre la que se realiza la conexión (cableada o sin cables)
- Pasos necesarios para comenzar a comunicarse (Handshaking)
- Negociación de las características de la conexión.
- Cómo se inicia y cómo termina un mensaje.
- Formato de los mensajes.
- Qué hacer con los mensajes erróneos o corruptos (corrección de errores)
- Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
- Terminación de la sesión de conexión.
- Estrategias para asegurar la seguridad (autenticación, cifrado).
- Como se construye una red física
- Como los computadores se conectan a la red

Una vez tratadas las características generales de los protocolos sería necesario entrar en especificaciones respecto a la seguridad, ya que es un aspecto relevante en la presente investigación.

## 1.4 Seguridad

Los primeros elementos de la técnica seguridad informática a nivel mundial pueden encontrarse hacia los años 60, donde las motivaciones de la guerra con la crisis de los misiles y el alto potencial de investigación que generan las universidades en ese momento, establecen el sustrato necesario para que se desarrollen las necesidades de protección y control, registro y surgimiento, aniquilación y supervivencia que orientan en ese momento la política internacional.

Durante las décadas del 70 y 80 se promueven múltiples iniciativas para fortalecer el tema de seguridad informática particularmente orientado por el área técnica. Instituciones como la IEEE establecen líneas de acción sobre el tema, fundando grupos de investigación, realizando conferencias internacionales y publicaciones que poco a poco formaron los primero profesionales en seguridad informática.

La seguridad informática enfrenta durante la década de los 90 un nuevo desafío: seguridad distribuida. Mientras en las décadas anteriores el detalle de la seguridad giraba entorno al aseguramiento de características de software generalmente para uso local o personal, los profesionales de la seguridad informática debían ahora pensar tanto en la seguridad local como en la seguridad de la interacción con un tercero. Técnicas como las de control de paquetes de comunicaciones, cortafuegos, detección de intrusos, redes privadas virtuales, criptografía asimétrica, filtros de correo, entre otras recibieron gran acogida por la industria, generando variedad de productos y conceptos que son utilizados por las diferentes organizaciones privadas, públicas y militares.

Se puede definir Seguridad Informática como un conjunto de métodos y herramientas destinados a proteger los bienes informáticos de una institución.

En un sistema informático se deben asegurar: (9)

**Reconocimiento:** cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.

**Integridad:** un sistema íntegro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.

**Aislamiento:** Los datos utilizados por un usuario deben ser independientes de los de otro físico y lógicamente (usando técnicas de ocultación y/o compartimiento) también se debe lograr independencia entre los datos accesibles y los considerados críticos.

**Auditabilidad:** procedimiento utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones del sistema. Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección.

**Controlabilidad:** todos los sistemas y subsistemas deben estar bajo control permanente.

**Recuperabilidad:** en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.

**Administración y Custodia:** la vigilancia permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.

En busca de una mejor seguridad disímiles investigadores y desarrolladores se han encargado de fortalecer los medios de seguridad en la informática por lo cual surgen los protocolos de seguridad que se verán de forma general haciendo énfasis en el protocolo AAA que es el problema que nos acomete.

## 1.5 Protocolos de seguridad

Un escenario típico consiste en un número de actores principales, tales como individuos, compañías, computadoras, lectores de tarjetas magnéticas, los cuales se comunican usando una variedad de canales (teléfono, correo electrónico, radio) o dispositivos físicos (tarjetas bancarias, pasajes).Un protocolo de seguridad define las reglas que gobiernan estas comunicaciones, diseñadas para que el sistema pueda soportar ataques de carácter malicioso. Protegerse contra todos los ataques posibles es generalmente muy costoso, por lo cual los protocolos son diseñados bajo ciertas premisas con respecto a los riesgos a los cuales el sistema está expuesto. De las premisas consideradas básicas para obtener sistemas de comunicación seguros, se encuentran: confidencialidad, integridad, autenticación, disponibilidad y no repudio.

**Confidencialidad:** Característica que asegura que la información en tránsito, es difícil para aquellas partes no autorizadas. El método más habitual de conseguir este objetivo es a través de algoritmos de cifrado, bien sea de clave secreta o pública. La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas ¨pinchadas¨ la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información esta físicamente almacenada.

**Integridad:** La integridad asegura que los datos no han sido modificados en tránsito y que, por tanto, llegan al destinatario exactamente igual que fueron enviados. Nótese que la información ha podido ser capturada y/o examinada: solo podemos estar seguros de que no ha sido alterada. La forma más habitual de asegurar la integridad es utilizando firmas digitales o funciones hash con clave.

**Autenticación:** La autenticación hace referencia a la capacidad de asegurar el origen y destino de la información, evitando suplantaciones. Es un término que suele equipararse al de identificación, aunque este último es más usual para referirse a personas físicas. Los mecanismos habituales para conseguir identificación son los biométricos, mientras que para la autenticación de información se utilizan firmas digitales.

**No repudio:** ofrece protección a un usuario frente a otro usuario que niegue posteriormente que en realidad se realizó cierta comunicación (como por ejemplo que una tienda niegue haber recibido el pago por parte de un cliente que realmente lo ha efectuado). Es un concepto muy ligado a la autenticación. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

**Disponibilidad:** la disponibilidad de la información se refiere a la seguridad de que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su perdida o bloqueo, bien sea por ataque engañoso, mala operación accidental o situaciones casuales o de fuerza mayor.

Una vez vistas las premisas que rigen a los protocolos de seguridad solo quedaría ver en específico el protocolo a tratar en la investigación.

### 1.5.1 Protocolo de seguridad AAA

Cuando uno escucha las siglas AAA es posible que vengan a la mente la lucha libre o un tamaño de baterías; sin embargo, en el ambiente de seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (del inglés: Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

**Autenticación:** Es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, ó los números de teléfono, en la identificación de llamadas. Viene al

caso mencionar que los protocolos de autenticación digital modernos permiten demostrar la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red.

**Autorización:** Se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son, pero sin estar limitado a: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

**Contabilización:** Se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes (del inglés "batch accounting") consiste en la grabación de los datos de consumo para su entrega en algún momento posterior. La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

Las propuestas de los protocolos y sistemas AAA son desarrollados por el grupo de trabajo AAA de la IETF (del inglés: Internet Engineering Task Force, encargados de definir los RFC donde se encuentran definidos los principales protocolos de internet). Existe otro grupo dentro de la IETF, llamado el grupo de investigación de arquitectura AAA, el cual es responsable de desarrollar una arquitectura general AAA.

El marco de trabajo AAA consiste en tres componentes fundamentales: el servidor AAA, los módulos específicos a las aplicaciones (ASM) y un repositorio.

El servidor AAA cuenta con reglas para evaluar una petición y tomar decisiones relacionadas con autenticación y autorización. El usuario envía una petición al servidor; esta petición debe estar formateada de tal modo que el servidor no tenga que interpretar ninguna información específica a

alguna aplicación para tomar una decisión. El servidor verifica la petición, determina qué tipo de autorización es requerida, toma una política del repositorio y realiza una de las dos siguientes acciones:

- Redirecciona la petición al módulo específico de la aplicación, para evaluación.
- Hace una decisión basado en el repositorio de políticas y eventos.

Todos los eventos son almacenados en el repositorio de políticas y eventos. Este repositorio puede ser usado para evaluar futuras peticiones y accesar información de auditoría específica de un usuario.

AAA es una propiedad que todo sistema seguro debe contemplar; sin embargo, no es el caso. Mucha gente piensa en AAA sólo para conexiones y accesos remotos. Con todo, es posible implementarla a nivel local. De hecho, sistemas operativos como Unix y Windows poseen los elementos necesarios para implementar estas características. Es deber de cada administrador configurar los sistemas de manera que cuenten con las tres A.

Los sistemas de seguridad AAA definen esencialmente una plataforma que coordina las tres disciplinas individuales a través de tecnologías de red variadas. La Autenticación se refiere a validar la identidad de los usuarios para permitirles o no el acceso a la red. La Autorización define qué derechos y servicios tiene el usuario final una vez que su acceso ha sido aceptado. Por último el Registro de los usuarios permite mantener la información de los servicios que han sido utilizados por el usuario final, para propósitos tales como la facturación, auditoría y planes de capacitación.

En la figura 1.2 se muestran los componentes de una solución AAA. El servidor AAA está incorporado a la red y sirve como depósito central para distribuir y guardar la información AAA. El dispositivo que actúa como punto de entrada a la red es típicamente un NAS (pueden ser también ruteadores, servidores o quizás otro host) que efectúa las funciones de un cliente AAA. El proceso AAA puede resumirse de la siguiente manera:

El usuario final se conecta al dispositivo de entrada y solicita acceso a la red. El punto de Acceso (cliente AAA), solicita y reenvía las credenciales del usuario al servidor AAA. El servidor procesa los datos y responde al cliente AAA si acepta o rechaza la petición y adjunta otros datos relevantes. El cliente notifica al usuario final que su acceso ha sido aceptado o no para recursos específicos.

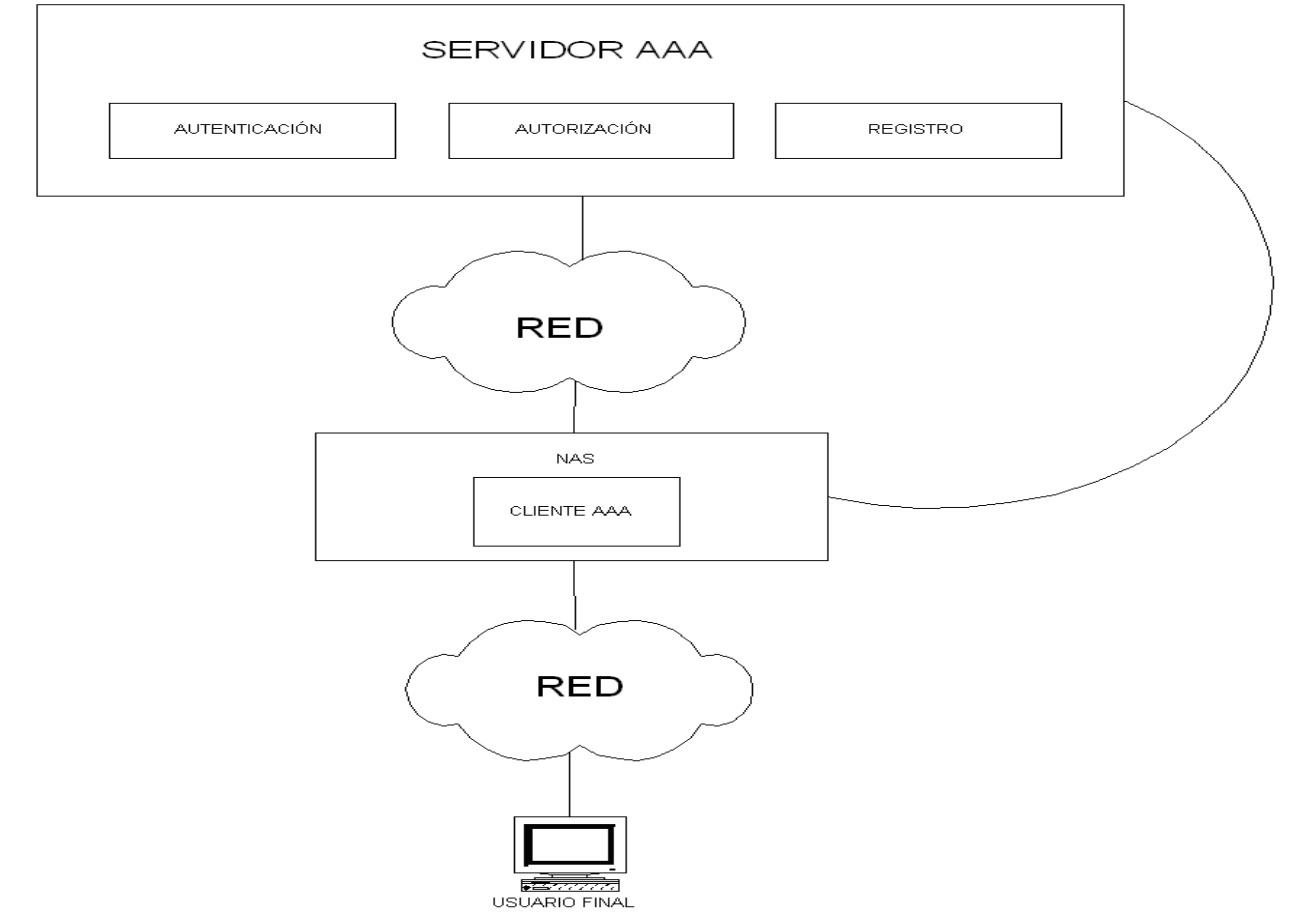


**Figura 1.2: Solución AAA**

La idea del grupo de trabajo de la AAA fue definir un protocolo que implementara autenticación, autorización y auditoría y que fuese lo suficientemente genérico para ser usado en una gran variedad de aplicaciones. Actualmente se usan protocolos independientes para implementar las AAA.

Los únicos protocolos que proporcionan los tres servicios de la AAA de forma completa e integral son TACACS+, RADIUS, y DIAMETER.

## 1.6 Protocolo TACACS+, Radius y Diameter.

### 1.6.1 Protocolo TACACS+

El protocolo **TACACS+ (del inglés: Terminal Access Controller Access Control System**, descrito en la **RFC 1492**) es un protocolo de autenticación remota que se usa para gestionar el acceso (proporciona servicios separados de autenticación, autorización y registro) a servidores y dispositivos de comunicaciones. TACACS+ está basado en TACACS, pero, a pesar de su nombre, es un protocolo completamente nuevo e incompatible con las versiones anteriores de TACACS.

TACACS+ es un protocolo cliente/servidor; el cliente de TACACS+ es típicamente un RAS (del inglés: Remote Access Services, se refiere a cualquier combinación de hardware y software para permitir el acceso remoto a las herramientas o la información que residen en una red), y el servidor de TACACS+ normalmente es un proceso daemon que corre en algún UNIX o servidor Microsoft Windows. Una característica fundamental de TACACS+ es la separación que hace de autenticación, autorización, y contabilidad. TACACS+ usa TCP para su transporte. El daemon del servidor usualmente escucha en el puerto 49, el puerto asignado para el login de TACACS.

### La Autenticación de TACACS+

TACACS+ permite que el contenido del intercambio de autenticación sea de longitud arbitraria y por tanto pudiera usar mecanismos de autenticación diferentes a los originales del protocolo tales como PPP, CHAP, EAP, token chap, y Kerberos). La autenticación no es obligatoria; es una opción configurada en sitio. Algunos sitios no lo requieren en absoluto; otros sólo lo requieren con toda la seguridad para el acceso a servicios. La autenticación de TACACS+ tiene tres tipos de paquete:

- START que siempre se envía por el cliente inicialmente
- CONTINUE que siempre se envía por el cliente l
- REPLY que siempre se envía por el servidor

La autenticación empieza con el cliente que envía un mensaje de START al servidor. El mensaje describe el tipo de autenticación a ser usada (por ejemplo, CHAP, contraseña de clear text simple, PAP), y puede contener el nombre de usuario y algunos datos de la autenticación. El paquete de

START sólo se envía como el primer mensaje en una sesión de autenticación TACACS+, o como el paquete que sigue inmediatamente después de un reinicio.

Un reinicio puede pedirse por el servidor en un paquete de REPLY. Un paquete de START siempre tiene un número de secuencia igual a 1. En la contestación a un paquete de START, el servidor envía un REPLY. El mensaje de REPLY indica si la autenticación está terminada, o si debe continuar. Si el REPLY indica que esa autenticación debe continuar, el mensaje también indica que la nueva información se necesita. El cliente consigue esa información y la responde con un mensaje CONTINUE. Este proceso se repite hasta que toda la información para la autenticación se recoge, y el proceso de autenticación concluye.

### Autorización TACACS+

Autorización es la acción de determinar lo que se le permite hacer a cada usuario Generalmente autenticación precede a autorización, pero no obligatoriamente no se requiere ese orden. Un requerimiento de autorización puede indicar que el usuario no esta autenticado (es decir, nosotros no sabemos quién es el usuario). En este caso, es al agente de autorización quien le compete determinar si a un usuario no autenticado se le permite acceso a los servicios en cuestión.

Cuando la autenticación se completa (si la autenticación se usa), el cliente puede empezar el proceso de autorización, si la autorización se requiere. Una sesión de la autorización se define como un solo par de mensajes: un mensaje de REQUEST seguido por un RESPONSE El mensaje REQUEST de autorización contiene un juego fijo de campos que describen y procesan la autenticidad del usuario, y un juego no constante de argumentos que describen los servicios y opciones para la autorización que se pide. Aquí son algunos ejemplos de cuando la autorización se realizaría.

Cuando un usuario hace login y quiere iniciar un shell; cuando un usuario empieza PPP y quiere usar IP encima de PPP con una dirección de IP particular. En los servidores TACACS+ un daemon podrían responder a estas demandas permitiendo el servicio, o poniendo una restricción de tiempo en el login al shell, o requiriendo listas de acceso IP en la conexión del PPP.

## Contabilidad TACACS+

La contabilidad es típicamente la tercera acción después de la autenticación y autorización. La contabilidad es la acción de grabar lo que un usuario está haciendo o ha hecho. Esta en TACACS+ puede servir a dos propósitos:

- Puede usarse para responder por el pago de los servicios que usó, como en un ambiente de facturación.
- Puede usarse como una herramienta de intervención para los servicios de seguridad. Es decir como una herramienta de detección de uso no correcto o violatorio de la normas del servicio.

Con este fin, TACACS+ soporta tres tipos de registros de contabilidad:

- Los registros START que indican que un servicio está a punto de empezar.
- Los registros STOP que indican que un servicio simplemente ha terminado.
- Los registros UPDATE son avisos del intermedio que indican que un servicio todavía está realizándose.

Los registros TACACS+ de contabilidad contienen toda la información usada en los archivos de la autorización y también contienen la información de contabilidad específica como tiempos de inicio y parada (cuando es apropiado) y la información del uso del mismo.

## Transacciones TACACS+

Las transacciones entre el cliente de TACACS+ y el servidor de TACACS+ se autentican a través del uso de una contraseña secreta compartida que nunca se envía sobre la red. Típicamente, la contraseña secreta se configura en ambas entidades. TACACS+ encripta todo el tráfico entre el cliente de TACACS+ y el servidor daemon TACACS+. La Figura 1.3 muestra la interacción entre un usuario dial, el cliente de TACACS+ y servidor.

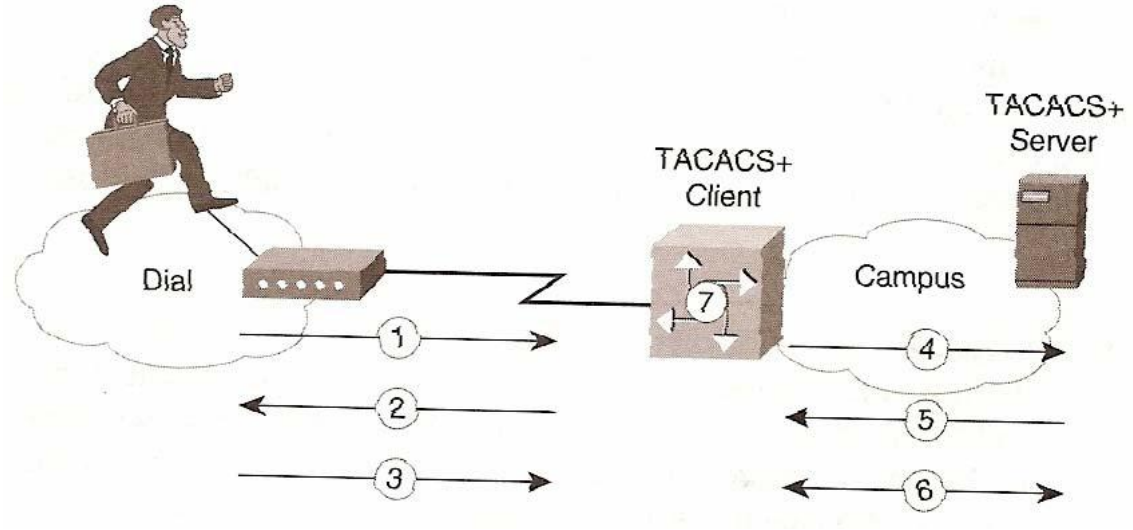


**Figure 1.3: Un intercambio TACACS+**

El usuario inicia una autenticación sobre PPP al RAS.

El RAS le pide al usuario nombre de usuario y contraseña.

El usuario replica con su contraseña y nombre de usuario.

EL cliente TACACS+ que generalmente es el mismo RAS envía en un paquete encriptado con la información del usuario al servidor TACACS+.

EL SCA TACACS+ responde con la autenticación o la negación.

EL servidor TACACS+ y el RAS intercambian mensajes de autorización. Si la autorización fue positiva el RAS deja entrar al usuario.

### 1.6.2 Protocolo Radius y Diameter

El protocolo de servicio de usuario de acceso telefónico de autenticación remota Radius (del inglés: Remote Authentication Dial-In User Service) desarrollado por Livingston Enterprise y publicado en 1997 como los RFC 2058 (10) y 2059 (11), fue diseñado para proporcionar AAA entre un NAS (12) (del inglés: Network Access Server, es un mediador entre los mensajes entrantes y salientes desde y hacia el servidor) y un servidor Radius. El mismo utiliza una sola base de datos, donde se encuentra almacenada toda la información de autenticación. El NAS actúa como un cliente y pasa la información del usuario al servidor Radius, el cual es responsable de procesar las peticiones de los clientes, autenticar al usuario y configurar al cliente para proporcionar el servicio al usuario. Es ampliamente utilizado y se implementa para administrar el acceso a los servicios de red. Este protocolo define una

norma para el intercambio de información entre un dispositivo de acceso a la red y un servidor de autenticación, autorización y contabilidad (AAA) para realizar operaciones de autenticación, autorización y contabilidad. Un servidor AAA Radius puede administrar los perfiles de usuario para la autenticación (comprobar el nombre de usuario y la contraseña), información de configuración que especifica el tipo de servicio que se va a proporcionar y las directivas que se van a aplicar que pueden restringir el acceso de los usuarios. El protocolo Radius proporciona únicamente el marco para el intercambio de autenticación y se puede utilizar con numerosos métodos de autenticación.

### Principales características de Radius

- - Modelo cliente / servidor

Un servidor de acceso a la red NAS funciona como un cliente de Radius. El cliente es responsable de pasar la información a los usuarios designados, a los servidores Radius y, a continuación, actuar sobre la respuesta que se devuelve. Los servidores Radius son responsables de la recepción de las solicitudes del usuario, la autenticación del usuario y, a continuación, devolver toda la información de configuración necesaria para entregar servicio al usuario. Un servidor Radius puede actuar como un cliente proxy a otros servidores Radius u otros tipos de servidores de autenticación.

- Red de seguridad

Las comunicaciones entre el cliente y el servidor Radius son autenticadas a través de la utilización de un secreto compartido, que nunca es enviado a través de la red. Además, las contraseñas se envían cifradas entre el cliente y el servidor Radius, para eliminar las posibilidades de que alguien que husmee pueda determinar la contraseña de un usuario y anular la seguridad de red.

- Mecanismos de autenticación flexibles

El servidor Radius puede apoyar una variedad de métodos para autenticar un usuario. Cuando se realiza la conexión con un ISP (del inglés: Internet Service Provider, es una empresa dedicada a conectara internet a los usuarios) mediante módem, DSL, cables módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS sobre el protocolo PPP (Point-to-Point Protocol, es un protocolo que permite establecer una comunicación a nivel de enlace entre dos computadoras), quien redirige la petición a un servidor Radius sobre el protocolo Radius. El servidor Radius comprueba que la

información es correcta utilizando esquemas de autenticación como PAP (Pastor Authentication Protocol o Protocolo de Autenticación de Clave de acceso es un protocolo de autenticación), CHAP (Challenge-Handshake Authentication Protocol, es un protocolo de autenticación por desafío mutuo) o EAP (Extensible Authentication Protocol). Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP (del inglés: Layer 2 Tunneling Protocol, es un protocolo creado para corregir las deficiencias de los protocolos PPTP y L2F) (13).

Con la emergencia de nuevas tecnologías y aplicaciones como las redes inalámbricas e IPs móviles, los requisitos para la autenticación y autorización han aumentado grandemente, y los mecanismos de mando de acceso son más complejos. El protocolo existente (Radius) puede ser insuficiente para cubrir con estos nuevos requisitos ya que presenta problemas de cofidenciabilidad, seguridad e infraestructura. Aquí es donde el protocolo Diameter entra en la obra. El protocolo ofrece servicios de autenticación, autorización y contabilidad (AAA) basándose en el protocolo Radius. Proporciona la misma funcionalidad que Radius, pero con mejoras en las deficiencias de su antecesor. Diameter está diseñado para trabajar tanto de una manera local como en un estado de alerta, sondeo y captura, que en inglés se le denomina roaming de AAA, que le permite ofrecer servicios sumamente móviles, dinámicos, flexibles y versátiles.

Es importante destacar que un nodo Diameter puede actuar como Servidor para ciertas peticiones, y como Agente para otras. Los agentes Diameter se introdujeron para añadir flexibilidad a la arquitectura.

Diameter no es directamente compatible hacia atrás, pero proporciona un método de actualización desde Radius. Las principales diferencias son: (14)

- Usa protocolos de transportes fiables (TCP o SCTP, no UDP).
- Usa seguridad a nivel de transporte (IPSEC o TLS).
- Tiene compatibilidad transaccional con RADIUS.
- Tiene un espacio de direcciones mayor para AVPs (del inglés: Atribute Value Pairs, pares atributo-valor) e identificadores (32 bits en lugar de 8).
- Es un protocolo peer-to-peer en lugar de cliente-servidor: admite mensajes iniciados por el servidor.
- Tiene descubrimiento dinámico de peers (usando DNS SRV y NAPTR)
- Tiene negociación de capacidades

- Admite ACKs en el nivel de aplicación, definiendo métodos de fallo y máquinas de estado (RFC 3539)
- Tiene notificación de errores.
- Tiene mejor compatibilidad con roaming.
- Es más fácil de extender, pudiendo definirse nuevos comandos y atributos.
- Incluye una implementación básica de sesiones y control de usuarios.

Estos dos protocolos se encuentran desarrollados en gran parte de Latinoamérica en distintos servicio de telefonía y dispositivos para el control de la seguridad de las redes, muchas empresas ofrecen productos que permiten la implantación de estos protocolos entre ellos se encuentra router Cisco SN 5428 el cual incluye servicios de red inteligente tales como seguridad avanzada, redes LAN virtuales y QoS(del inglés: Management Server, es una medida de desempeño para un sistema de transmisión) para ayudar a volver más escalable, seguras y manejables las redes de almacenamiento. Al solucionar la seguridad y escalabilidad, el Cisco SN 5428 incluye soporte para mediciones familiares y ampliamente conocidas basadas en IP, tales como autenticación RADIUS y TACACS+, listas de control de acceso y redes LAN virtuales. En la Universidad Autónoma Indígena de México se desarrolló el estudio de la estructuración de una red WI-FI con el fin de las mejoras de la información en el entorno académico el protocolo analizado y posteriormente utilizado fue Radius dadas las políticas de seguridad que brinda el mismo.

Cuba no se ha quedado exento del desarrollo de proyectos que incluyan al protocolo Radius tal es el caso del Sistema Integrado de Contabilidad y Configuración (SICC), concebido y elaborado por el Departamento de Telemática del Instituto Superior “José Antonio Echeverría” (ISPJAE). Sin embargo no pasa lo mismo con el protocolo Diameter este se encuentra en un estado muy embrionario todavía en el país, aunque es de interés de muchos su estudio ya que es una versión superior al protocolo Radius. Carece de implementación en la isla, pero esto no quiere decir que no lo hayan propuesto para desarrollar algún proyecto en el cual se puede incluir el de “Arquitectura para la gestión de ancho de banda basada en usuarios y destino del tráfico”, desarrollado en la Facultad de Ingeniería Eléctrica, Instituto Superior Politécnico José Antonio Echeverría, Cujae, Ciudad de La Habana, Cuba. Donde se proponía este protocolo para intercambiar la información de políticas entre el Punto de decisión de políticas (PDP (del inglés: (Policy Decisión Point), es el responsable de obtener las políticas de las bases de datos de políticas) y Puntos de ejecución de políticas (PEP (del inglés: Policy Enforcement Point), es una entidad donde las políticas son aplicadas).

## 1.7 Conclusiones

Teniendo en cuenta que para la fundamentación de este proyecto no se cuenta con antecedentes de la temática, se ha logrado definir conceptos que delimitan el proyecto investigativo y sirven de apoyo. Además se trataron características generales de la problemática a resolver.

# Capítulo 2: Protocolo Diameter

## 2.1 Introducción

En esta sección se definen la mayoría de los elementos básicos para la construcción del protocolo Diameter así como el conjunto de mensajes, características y atributos de la estructura. Se señalarán definiciones entre las operaciones de campo, los distintos tipos de agentes que interactúan en la transformación, transporte y enrutamiento de mensajes.

## 2.2 Bases de especificación del protocolo Diameter

En las bases del protocolo Diameter se define el concepto de solicitudes donde una solicitud del protocolo Diameter no es más que los servicios, protocolos y procedimientos que serán utilizados por los servidores proxy y el propio protocolo, ejemplo de esto es el IP móvil donde las solicitudes y funcionalidades tienen como base al protocolo Diameter, teniendo como precedente la utilización de NAS con el propósito de autenticación y autorización, la cual se considera una aplicación de este protocolo; este incluye la autorización de solicitud de mensajes que son específicos de cada aplicación como sería la solicitud de autorización de un usuario al servidor; no necesita ofrecer ningún tipo de detalle sobre el procedimiento de esta mensajería aunque si se definen los métodos y los mensajes y la razón es que se requiere esta definición para lograr el monitoreo en el protocolo Diameter.

### 2.2.1 Especificaciones de seguridad

El protocolo Diameter cuenta con mecanismos de seguridad de extremo a extremo, en la capa de transporte se utiliza como protocolo de seguridad TLS(del inglés: Transport Layer Security, es un protocolo criptográfico que proporciona un canal de comunicación seguro) y en la capa de red IPSec (del inglés: Internet Protocol Security, es un protocolo que brinda seguridad de transmisión de información)que garantiza la seguridad de los mensajes entre dos nodos, aunque es importante señalar que solo es necesario proteger datos específicos, esto se evidencia en el momento que se tiene señalización de una propiedad extranjera a través de servidores proxy donde este sería un intermediario.

### 2.2.2 Perfil de transporte de Diameter

Al ser diseñado Diameter a partir del protocolo Radius los diseñadores se empeñaron en aumentar la fiabilidad en la mensajería teniendo en cuenta sobre la base dos bloques que resuelven este problema y el protocolo AAA en el perfil de transporte haciendo a un lado la conexión UDP e incorporando TCP o SCTP (del inglés: Stream Control Transmission Protocol, es una alternativa a los protocolos TCP y UDP). De manera general se puede decir que Diameter contiene el uso de un protocolo de transporte fiable que está respaldado en la base de la pirámide del protocolo como se muestra en la figura 2.1.

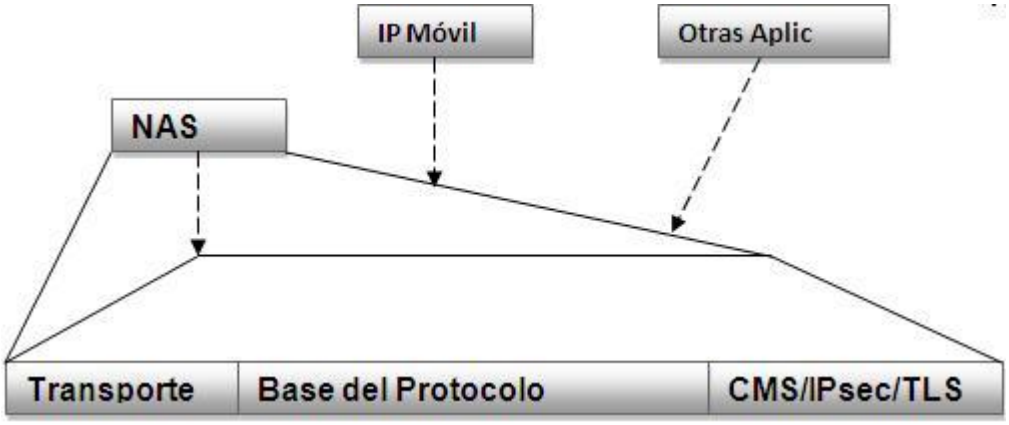


**Figura 2.1 Especificaciones de la interdependencia del protocolo Diameter.**

### 2.2.3 Aplicaciones NAS en el protocolo Diameter

Siendo NAS una aplicación del protocolo Diameter el cual se define en una solicitud separada, pero debido a la naturaleza central de los servidores AAA y su interrelación con el NAS como dispositivo de borde los servidores AAA se encargan de las aplicaciones y los servicios a través de NAS.

Los procedimientos y las solicitudes a través de un NAS son fundamentales para la funcionalidad de otras aplicaciones sobre el protocolo Diameter lo cual hace aún más difícil la implementación, comprensión y relación dentro de este protocolo.

### 2.2.4 Aplicaciones del protocolo Diameter

Las especificaciones de la base del protocolo Diameter solo describen el apoyo de la contabilidad, mientras que otros protocolos y servicios que utilizan servidores Diameter son considerados como

solicitudes de Diameter. No todos los nodos Diameter desplegados en una infraestructura prestarán apoyo a todas las aplicaciones Diameter, por lo tanto cuando dos nodos Diameter interactúan con los demás a través de una aplicación cada nodo tiene que asegurarse que los otros no admitan dicha solicitud, la característica llamada capacidad de negociación asegura que esto no ocurra.

Para facilitar la capacidad de negociación entre las aplicaciones del protocolo Diameter cada uno tiene asignado un identificador único de solicitud de modo que una vez aprobada la solicitud se pueden aprobar las aplicaciones que soporta un nodo en particular. A continuación se verá una breve reseña de alguna de estas aplicaciones:

- Contabilidad: es la única aplicación que se encuentra enmarcada específicamente en la base del protocolo Diameter.
- Aplicación de control de crédito: debido a la popularidad recientemente adquirida de la utilización de las tarjetas de prepago de celulares es una de las prácticas de la infraestructura AAA que más auge ha tomado, ejemplo de los servicios solicitados a través de ella son los siguientes: servicio de mensajería y servicio de descarga, los cuales se encuentran controlados por la sección de iniciación del protocolo (SIP)(del inglés: Session Initiation Protocol) (15).El proveedor de servicios debe ser capaz de determinar si permite la cobertura de cada uno de los servicios solicitados antes de la iniciación del servicio y poner fin al servicio una vez que el crédito se haya agotado. La aplicación de control de crédito proporciona métodos en tiempo real que permite controlar muchos servicios ofrecidos por las redes celulares para los usuarios finales. Esta aplicación define la interacción entre la entidad, la prestación del servicio y el llamado crédito de control del servidor, actualmente este tipo de aplicación se sigue desarrollando.
- Aplicación NAS: esta aplicación describe la iteración de los servidores Diameter con los servidores de acceso a la red (NAS) para la autenticación y otros procedimientos. La aplicación NASREQ permite a la NAS hacer peticiones y apoyar una variedad de mecanismos de autenticación como PAP, CHAP y EAP, esta es una de las aplicaciones que permite compatibilidad con el protocolo antecesor Radius.
- IP móvil: si bien la movilidad ip facilita el transporte y enrutamiento de datos para la comunicación hacia y desde un móvil de acogida, también facilita la verificación de la identidad y

mecanismos para la autorización final de anfitriones. Este tiene definido un número de claves de seguridad y mecanismos de gestión que se ven facilitadas por el protocolo AAA. Diameter cierra una brecha bastante completa para móviles de IPv4(es la versión 4 del protocolo IP), esta aplicación además permite la movilidad entre ámbitos administrativos.

- EAP: es otra aplicación de Diameter que define los procedimientos para la ejecución e intercambio de mensajes entre el protocolo Diameter y los servidores NAS.

### 2.2.5 Funciones de los tipos de nodos Diameter

Antes de adentrarse en la descripción detallada del protocolo Diameter es necesario conocer las entidades y funciones que se encuentran en una infraestructura del protocolo Diameter (16). Con el fin de asegurarse de la fiabilidad, seguridad y el comportamiento de enrutamiento en dicho protocolo ya que se encuentran involucrados en la base de las funciones que desempeña en la mensajería:

- Nodo: es un host de proceso que implementa el protocolo Diameter.
- Peer: es un nodo de Diameter que tiene una directa relación con otro nodo a través de la capa de transporte de Diameter.
- Cliente: dispositivo en el borde de la red que realiza el control de acceso, ejemplo de ello son: NASES, IP móvil o agentes extranjeros.

  Se debe tener en cuenta que el usuario final que desee tener acceso a la red no es el cliente y el mismo no participa en la señalización.

- Servidor Diameter: es un dispositivo que maneja las solicitudes de AAA para un determinado momento.
- Agente: es un nodo que proporciona un agente transmisor, proxy, redirecciona o traduce los servicios.
- Agente transmisor: está relacionado o interviene en el enrutamiento de mensajes basado en los atributos y tablas de enrutamiento. Los agentes transmisores no generan ningunas decisiones de política ya que no examinan todos los casos de incumplimiento de ruta dentro de los atributos de

los mensajes, por esa razón estos agentes necesitan comprender la semántica de los atributos relacionados con el enrutamiento. Un transmisor nunca origina un mensaje pero es capaz de manejar cualquier aplicación o tipo de mensaje.

- Agente proxy: Los agentes proxy pueden ser vistos como agentes transmisores que además pueden crear reglas de decisión. Ellos pueden rastrear varios estados en el dispositivo NAS para propósitos de aprovisionamiento de recursos. Los proxy típicamente no responden a las peticiones de los clientes pero pueden originar mensajes de rechazos en caso que las políticas sean violadas.

- Los agentes de redireccionamiento no se sientan en los caminos de remisión y no alteran ningún atributo de los mensajes. Por lo tanto ellos no reenvían cualquier mensaje, como hacen los agentes de trasmisión, pero refiere al cliente a un servidor redireccionando los mensajes de acuerdo a la configuración. Ellos son capaces de manejar cualquier tipo de mensaje pero pueden ser configurados para redireccionar solamente cierto tipo de mensaje.

- Los agentes de traslado realizan un protocolo de traslación entre Diameter y otros protocolos AAA, tales como Radius. Ellos son considerados especialmente para la compatibilidad con Radius.

- Un corredor es más un término de negocio que un término técnico y por lo tanto dependiente del modelo de negocio puede adoptar diferentes roles: transmisores, proxy o agente de redireccionamiento pero no actúa como un servidor.

## 2.3 Mensajes del protocolo Diameter

Los mensajes del protocolo Diameter se utilizan para el transporte de información de las aplicaciones AAA. La información está contenida dentro de un mensaje que es típicamente un atributo donde el formato es AVP por esta razón dichos atributos son a menudo denominados AVPS (del inglés: Atribute Virtual Protocol). En el protocolo Diameter no se puede utilizar la terminología “tipos de mensaje” por lo que se puede decir que solo existen solicitudes y respuestas, en este protocolo se debe hablar de comandos los cuales distinguen a través de un código la función específica a realizar de un mensaje,

donde la resección de este mensaje está definido por el comando, el código y los atributos incluidos en el mensaje.

**Formato de mensaje Diameter**

| 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 | |
|---|---|
| Versión | Longitud de códigos |
| Bandera | Comando de códigos |
| ID de la aplicación | |
| Identificador de ruta a ruta | |
| Identificador de extremo a extremo | |
| AVPs…. | |

**Tabla 2.1 Cabecera y formato de mensajes de Diameter**

Como se muestra en la tabla los mensajes consisten de una norma de cabecera y una serie de AVPS.

1. En el campo de versión viene el número de la versión del protocolo.

2. En el campo de la bandera hasta el momento se especifican solo cuatro banderas:

- R significa una solicitud, muestra si el mensaje es una petición o es una respuesta.
- P define si es emitido por un servidor a través de un proxy, redirigido o debe ser procesado.
- E significa un error, para mostrar si el mensaje contiene errores del protocolo o de semántica.
- T para mostrar si un mensaje fue retransmitido después de un vínculo, conmutación por errores o se utiliza para ayudar a la eliminación de mensajes publicados.

3. El campo comando de códigos indica el comando asociado con los mensajes tales como: abortar solicitud del período de secciones o contabilidad y respuesta. Cada mensaje debe contener un

código de mando con el fin de que el receptor pueda determinar que medida debe tomar para cada mensaje.

4. El campo aplicación ID contiene una identidad única que se utiliza para contabilizar.
5. El campo identificador de ruta a ruta contiene un identificador que se utilice para que coincide la solicitud y la respuesta.
6. Otro campo es el identificador de extremo a extremo es un identificador usado para la detección del mensaje duplicado. El identificador de un mensaje de respuesta debe coincidir con el identificador del mensaje de solicitud. En caso de ser una comunicación local dichos identificadores deben permanecer durante al menos cuatro minutos.
7. El campo AVPs se utiliza para detectar mensajes duplicados.

### 2.3.1 Valor –Atributo Pair (AVP)

La información en el protocolo Diameter es transportada en el formato de atributos pares (atributo-valor) normalmente conocido como AVPs. El AVP presenta de 0 a 255 códigos hacia atrás lo cual le permite tener una compatibilidad con el protocolo antecesor Radius. Sería importante explicar la estructura de la AVP que se muestra en la siguiente tabla:

| 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 |
|---|
| Código AVP |
| Bandera(VMPRRRRR) \| Longitud AVP |
| ID vendor (opcional) |
| Datos de los Atributos |

**Tabla 2.2 Formato AVP de Diameter.**

1. **Banderas:**

- ”el bit M”: el cual es obligatorio, su propósito es indicar si necesita apoyo para atribuir o procesar un mensaje. Si un nodo recibe un bit M y no se reconoce su valor se debe rechazar dicho mensaje.

- “el bit P”: este bit indica la necesidad de encriptar el mensaje de un extremo a otro, de aparecer este bit el mensaje no debe ser enviado a menos que exista una seguridad cifrada entre el iniciador y el destinatario del mensaje.
- “RRRRR”: indica la existencia de 5 bit reservados en el campo de las banderas.

### Ejemplos de especificaciones AVPS

La base del protocolo Diameter y sus aplicaciones definen un gran número de AVPs.

- Host-Origen AVP: este atributo está contenido en el punto final del origen de los mensajes, no puede ser modificado por ninguno de los agentes, está presente en todos los mensajes, es conocido como identidad de Diameter, puede contener más de una dirección si está interactuando con más de un host.

- Origen-Dominio AVP: este atributo incluye el dominio del mensaje iniciado que está presente en todos los mensajes y no debe ser modificado por ningún agente.

- Host-Destino AVP: se usa principalmente para enviar un mensaje del usuario al servidor o de un servidor de origen a solicitudes de destinos fijas por ejemplo:

- Cuando el mecanismo de seguridad que se utiliza son preestablecidos es decir la clave de la sección se comparte entre la fuente y el destino final del mensaje.
- Cuando el intercambio de autenticación abarca múltiples mensajes de ida y vuelta.
- Para mensajes de inicio del servidor (como por ejemplo el pedido de aborto de una sección) que debe llegar a un cliente específico.

- Dominio-Destino AVP: contiene el dominio al cual el mensaje va dirigido. Este atributo no puede estar presente en el mensaje de respuesta, el AVP mencionado se utiliza para la toma de decisiones de enrutamiento del mensaje.

- AVPs Routing: se utiliza para fines de enrutamiento, este tipo de atributo no deben ser protegido de extremo a extremo debido a la necesidad de ser procesado.

- Códigos Resultados AVP: indica si una solicitud se ha completado con éxito o no, todos los mensajes de respuesta deben incluir un código de resultados. Los códigos de error proporcionan

información sobre el tipo de problema durante la transmisión de la solicitud, se clasifican en diferentes clases tales como roles de protocolo, transitorios o fracasos permanentes.

## 2.4 Conceptos de Transporte y Enrutamiento del protocolo Diameter.

Los diseñadores del protocolo Diameter definieron con mucho cuidado la comunicación no solo para permitir operaciones entre varios dominios sino también para fijar la fiabilidad tomando experiencia del protocolo anterior Radius.

### 2.4.1 Concepto de transporte en el protocolo Diameter

Es importante señalar que la comunicación por parte del cliente esta basada en TCP (17) o SCTP (18) mientras que los servidores soportan TCP y SCTP, para lograr un mejor entendimiento ya que sería bastante complejo explicar lo que nos proporciona la comunicación TCP/SCTP como es la conmutación por error, el control de la congestión y la interfaz de múltiples mecanismos se tratarán por separado, aquí solamente entraremos en especificación de dos importantes conceptos del transporte del protocolo Diameter “la sesión y la conexión”.

- Sesión: es un concepto lógico en la capa de aplicación que se establece de un extremo a otro entre un dispositivo y un servidor, una sesión es procesada por alguna de las dos partes (dispositivo o servidor) y por lo tanto se identifica mediante un id de sesión AVP. (19)
- La conexión es por otra parte un concepto del nivel de transporte que se establece entre dos dispositivos que envían y reciben mensajes. (19)

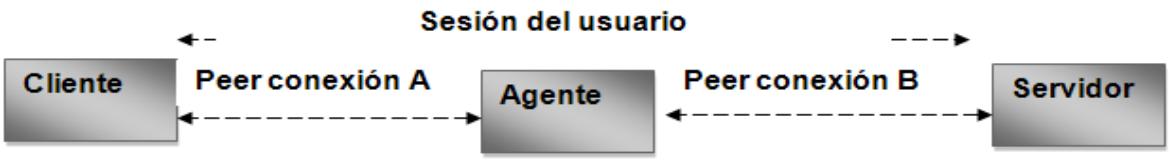


**Figura 2.2 Conexión de sesión en Diameter**

Es importante señalar que la conexión y el período de sesión no podrán tener relaciones directas de uno a uno. Por ejemplo una solicitud de autenticación de usuario crea un único período de sesión mientras

que los datos para este período de sesión pueden ser multiplexados con los datos de muchos otros períodos de sesión cuando se está llevando a cabo más de una conexión. Por otro lado el uso de TCP o SCTP en cada tramo permite la detención y reparación para fallos a nivel local (Hop By Hop) y los proxy intermediarios. Los paquetes perdidos son retransmitidos y pueden buscar rutas por salto más cortas.

### 2.4.2 Concepto de enrutamiento del protocolo Diameter

Diameter tiene definida muy clara la ruta hacia otros nodos la cual se basa en sus principales conceptos y herramientas. Para un mejor entendimiento se explicarán las herramientas que utiliza para el envío de mensajes.

- **Tabla de Pares**: se utiliza para la transmisión de mensajes. Cada nodo Diameter contiene una tabla de pares que contiene información de la identidad de los pares, contiene la información del estado del nodo si es configurado estáticamente o dinámicamente y la fecha de caducidad para la entrada de estos pares en la tabla.

- **Dominio basado en la tabla de enrutamiento**: el agente Diameter consulta el dominio de la tabla de enrutamiento con el fin de reenviar el mensaje hacia el próximo destino o la “AAA-hop “ apropiado que pueden residir en otro dominio. El mismo contiene los siguientes campos:

  - **Nombre del campo de dominio:** es similar a la red en el prefijo de enrutamiento ip y es el principal cable para la búsqueda.

  - **Identificador del campo de aplicación:** es similar al identificador de host de enrutamiento ip en el sentido que es la clave secundaria la que define la búsqueda. Una misma entrada puede tener diferentes destinos en función del tipo de la aplicación en el período de sesión. En este caso el servidor destino debe de haber anunciado el apoyo a esa solicitud.

  - **Acción de localización:** este campo indica si un mensaje es para ser procesado a nivel local, trasmitido al siguiente servidor hop o redirigirse al remitente.
  - **Identificador de servidor:** al tener identificados uno o más servidores permite que el mensaje sea enrutado por los distintos servidores, para esto debe existir en el nodo Diameter la tabla de pares que identifique los servidores.

### 2.4.3 Enrutamiento y reenvío de mensajes en el protocolo Diameter

Si un nodo Diameter es el destino final de una solicitud se debe procesar el mensaje a nivel local, aunque se debe consultar la tabla de pares, esta tabla incluye todos los host con los que el nodo puede comunicarse directamente. Los mensajes pueden ser transmitidos por otro agente pero estos deben incluir la información del destino en el interior del AVP y especificar en el AVPs el tipo de aplicación. Un ejemplo de esto es la autentificación-aplicación-ID, acción-aplicación-ID o proveedor- especificación – aplicación – ID, las solicitudes se dirigen hacia su destino final utilizando una combinación de destino y de destino-host (parecida a la combinación que se utiliza para identificar un host en una dirección IP).
Para una mejor comprensión se detallaron algunos conceptos importantes de esta sección.

- ❖ Cuando la solicitud no es emitida por un servidor proxy debe contener una indicación que diga que es para el consumo local, una muestra de esto es cuando una solicitud de destino incluye un host AVP que contiene la identidad de un anfitrión local, otra muestra un poco menos evidente es cuando dicha solicitud contiene una indicación de un host de destino AVP que no esté presente en el dominio AVP pero este incluye un host donde el servidor esté configurado para ser local.

- ❖ Las peticiones deben ser enviadas a un nodo específico, pero pueden ser procesadas por cualquier servidor que este en el dominio, solo que estas deben estar contenidas en el dominio de destino y no en el dominio del host.

- ❖ Las peticiones deben ser enviadas a un servidor central en específico donde en un determinado ámbito contenga el host de destino y el dominio AVPs.

## 2.5 Capacidad de negociación.

La función básica de Diameter se define como un procedimiento de capacidad de intercambio el cual permite que los pares estén consientes de la capacidad de soportar varias funcionalidades y aplicaciones con que cuentan cada una. La capacidad de intercambio es también utilizada para negociar sobre la base de un conjunto común de funcionalidades para la aplicación de Diameter, cuando ambos nodos soportan una aplicación específica. Los 2 pares deben llevar a cabo un intercambio de capacidad de negociación antes de poner a funcionar la conexión. La negociación no es

más que un par enviando un pedido de intercambio de capacidades, al cual responde el otro par con una respuesta de intercambio de capacidades.

Cuando se manda el mensaje relacionado al intercambio de capacidad, cada par indica el soporte que le da a cada aplicación dada publicando identificadores relevantes de la aplicación. Por Ej.: las aplicaciones que soporta NASREQ(es una aplicación que proporciona los servicios de la AAA) incluyen un valor de 1- en las de Autorización-Aplicación-ID o Acción – Aplicación - ID AVP de los comandos de pedidos y respuestas del intercambio de capacidades. Una vez que el par que recibe el mensaje de pedido de otro par, él examina las aplicaciones que lo soportan y si encuentran alguna aplicación común del mismo para que reciba, él almacenará en la memoria temporal la información que es soportada por las aplicaciones del par junto a la identidad del par. Esto optimiza las interacciones futuras entre estos 2 pares así como evita que cada par envíe comandos relacionados a las aplicaciones que estos no soportan. Si el par que recibe no encuentra ninguna aplicación común entre él y el par que envía el mensaje, el que recibe devolverá una respuesta de intercambio de capacidad con un código de resultado AVP establecido como Aplicación no compatible para Diameter y desconecta la capa de transporte.

El mecanismo de intercambio de capacidad también sirve como un vehículo que asegura la seguridad de la sesión de Diameter cuando el que recibe no tiene ningún mecanismo de seguridad compatible con el que envía, el que recibe devuelve una respuesta con el código de resultado AVP de Seguridad no compatible para Diameter y puede cerrar la conexión.

Como la sesión de Diameter deberá ser enrutada a través de múltiples nodos y agentes hasta llegar al par del destino, la sesión tendrá que ser enrutada solamente a través de aquellos nodos que hayan publicado la capacidad de soporte de la aplicación requerida por la sesión si hay o no un nodo que permita recibir y responder al pedido desde un par desconocido es un asunto de política de la red y el nodo puede descartar cualquier transacción que dependa de los pares desconocidos en caso que falle un transporte.

## 2.6 Requerimiento de seguridad

La dependencia tradicional de Radius de seguridad de extremo a extremo basada en el intercambio de secreto ha creado muchos problemas para las aplicaciones modernas sobre los procedimientos del protocolo AAA. Radius no ofrece una protección integral de una forma simétrica (en los diferentes

mecanismos de pedido y respuesta) este tema con el procedimiento de seguridad de Radius es especialmente severo cuando se trata de ocultar atributos o la red necesita tratar con clientes móviles o direcciones de ip dinámicas. Algunas especificaciones han tratado de proveer una para el uso de IPSec para Radius. Todavía los detalles del uso de IPSec para ofrecer servicios de seguridad para aplicaciones específicas de Radius no están bien definidos.

Una vez más Diameter se va por encima y trata de superar las desventajas presentadas por Radius.

- Diameter comienza por enviar soporte de seguridad para ambos clientes aplicando IPSec a través NAS hacia los servidores. Envía soporte aplicando TLS por los servidores Diameter mientras que deja el soporte de TLS para clientes como son NAS y agentes de movilidad como por ejemplo AF (Agente Foráneo, un agente foráneo almacena información sobre cada nodo móvil visitado en su red), o opcional.

- Una razón para facilitar los requerimientos de soporte de TLS para NAS y dispositivos de borde es relajar la necesidad de PKI (del inglés: Public Key Infrastructure, permite la ejecución con garantía de operaciones criptográficas) de estos dispositivos de forma tal que IPSec pueda ser utilizado para el tráfico por los bordes o tráfico intra dominio. Por otra parte se recomienda que el tráfico dentro del dominio sea protegido por TLS.

- Aún cuando IPSec o TLS puedan ofrecer protección de seguridad. Como se ve arriba los mensajes de Diameter deben estar protegidos de un extremo a otro, ej.: Cuando la confiabilidad de un mensaje se ve comprometido al pasar por intermediarios. Al contrario ocurre en Radius.

### 2.6.1 El uso de IPSec y TLS por Diameter.

El protocolo Diameter necesita de la seguridad en el nivel de transporte (a través de IPSec o TLS) por cada conexión. La conexión deberá extenderse solamente entre dos intermediarios de Diameter (por ejemplo: un cliente a un transmisor, un agente a otro agente y así).La especificación básica de Diameter asume que los mensajes de él son seguros por usar tanto IPSec como TLS. Cuando en IPSec no se usa solamente la capacidad de intercambio entre dos nodos de Diameter puede ser hecha sin TLS. Los dos pares indican el soporte para TLS a cada uno a través del uso de banda-seguridad-id AVP (con un valor de TLS) el par necesita comenzar el contacto TLS siguiendo la capacidad de intercambio de mensaje. Si el contacto TLS falla a este punto la conexión entre dos pares debe ser cerrada.

Todas las implementaciones de Diameter deben soportar el modo de transporte IPSec con algoritmos de encriptación y autenticación para proveer autenticación y confidencialidad por paquetes. También deben soportar mecanismos IPSec y mecanismos que identifican la replicación de ip, además Diameter envía el uso de intercambio de códigos de internet (IKE del inglés: Internet Key Exchange, es un protocolo usado para establecer una Asociación de Seguridad) para la autenticación del par, la administración del código y la negociación de asociaciones de IPSec en todas las implementaciones Diameter. Sin embargo Diameter disminuye los requerimientos de soporte de todas las autenticaciones IKE y solamente requiere el uso de secretos precompartidos por la autenticación IKE ,mientras deja el soporte de autenticación-base –certificación como una opción para implementadores, un tema que se desprende con el uso de certificaciones con IPSec e IKE es que como el uso de identificadores de puerto está prohibido en la fase uno de IKE, como no es posible únicamente configurar los autorices de autentificación de raíz (CAs) para cada aplicación individualmente. Esto implica un error en el uso de certificados para proveer seguridad basada en IPSec de los mensajes de Diameter: La misma política debe ser utilizada para todas las aplicaciones. La razón es la siguiente, como la autenticación ocurre solamente dentro de la fase 1 de IKE entre el cliente y el servidor usualmente nos es posible definir y separar los esquemas de autorización para cada aplicación durante el establecimiento IPSec SA (Asociación de Seguridad), el cual ocurre después en la fase 2.

Cuando se usa TLS, el nodo de Diameter que inicia la conexión actúa como el cliente TLS, mientras que el nodo de Diameter(el otro) que acepta la conexión actúa como servidor los pares de Diameter que implementan TLS para asegurar sus conexiones necesitan autenticarse plenamente como parte de la sesión TLS. Para soportar una autenticación mutua de TLS el par que actúa como servidor debe ser capaz de pedir un certificado al par que actúa como cliente, el cliente debe suministrar el certificado. Otra vez el tema que se desprende del uso del certificado es que ambos pares necesitan confiar la raíz CA que a expedido estos certificados. Aún cuando TLS es mucho más flexible que IPSec al configurar la raíz CA (es la entidad certificadora dentro de una infraestructura PKI), todavía es posible que diferentes CA sean utilizados para generar certificados por diferentes usos de Diameter.

Finalmente las especificaciones recomiendan que un par de Diameter implemente el mismo mecanismo de seguridad (IPSec o TLS) a través de toda su conexión par a par para evitar inconsistencias, redundancias o aprovisionamiento de seguridad inadecuado.

### 2.6.2 Modo de autorización: Impacto de la Seguridad sobre la Autorización y la contabilidad.

Como parte de la seguridad del nivel de transmisión de cada conexión, no solamente están los 2 pares de Diameter a cada lado de la conexión (extremo AAA) y requirieron autenticarse cada uno sino que también necesita autorizar la conexión y la sesión por Ej.:

El mero hecho de que un par sea autenticado exitosamente no quiere decir que este autorizado como un servidor Diameter que soporte las aplicaciones que están publicadas. Lo que se muestra a continuación también es requerido.

- Autorización de funcionalidad, antes de iniciar una conexión un par debe chequear que sus pares están autorizados para actuar en sus roles. Antes de poner a funcionar una conexión se llevan a cabo chequeos de autorización en cada conexión a lo largo del recorrido. Esto incluye la capacidad de negociación para determinar que las aplicaciones son soportadas por cada servidor. Esto es asegurar que los mensajes relacionados a una sesión son enrrutados a lo largo del recorrido que solamente incluye nodos autorizados que han dado a conocer que soportan la aplicación requerida por esta sesión.

- El servidor central, priorizado para autorizar una sesión debe asegurar que la ruta que debe atravesar un pedido debe ser autorizada. Ej.: El pedido ha pasado por dominios seguros. Esto se complementa al chequear la ruta física al examinar AVP Registro-Ruta. Un mensaje de error Diameter-Autorización-Rechazo si la ruta atravesada no es aceptable.

- Mensaje de contabilidad, están también atados a la autorización antes mencionada. Un servidor central puede querer crear una política para aceptar solamente pedido de contabilidad por sesiones para lo cual las respuestas de autorización específicas han sido creadas por el servidor.

- Los agentes locales de Diameter necesitan chequear el registro de ruteo incluido en la respuesta de autorización que vienen del servidor central. Esto significa asegurar que la ruta tomada por

los mensajes es aceptable. Cuando se reenvía una respuesta de autorización más adelante del recorrido, un agente local acepta el riesgo implícito en autorizar la sesión. La misma responsabilidad está implícita en crear un pedido de contabilidad que se corresponda con una respuesta de autorización.

## 2.7 Detalles de la aplicación

Como se mencionó anteriormente, la mayoría de las aplicaciones Diameter están definidas en diferentes documentos excepto la aplicación de la contabilidad que se describe junto con las especificaciones de Diameter [Diameter 3588]. Proveemos una visión general de varias aplicaciones.

### Ejemplo de intercambio de mensajes de contabilidad.

En contraste con Radius, los métodos de contabilidad están especificados dentro de la especificación de Diameter. Aún cuando el mensaje para la contabilidad en la especificación de Diameter es corto, el grupo de trabajo IETF AAA ha dedicado esfuerzos en proveer más seguimiento en la administración, en la contabilidad y sus atributos produciendo otras dos RFC [ACCMGM 2975] y [ACCATT 2924].

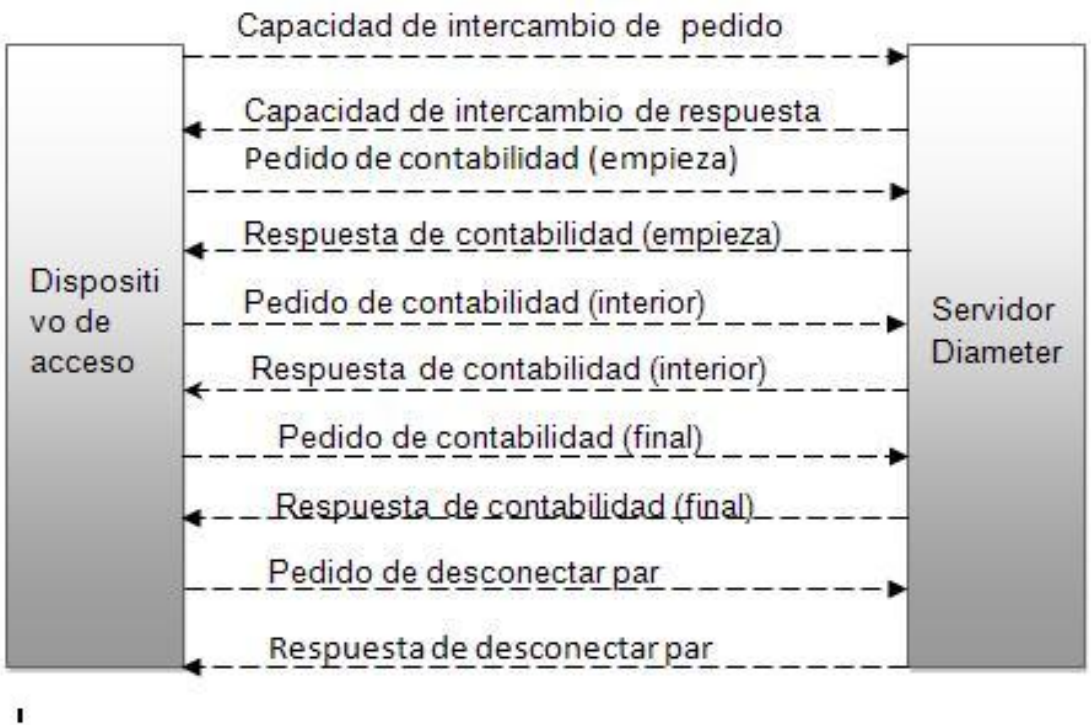


**Figura 2.3 Ejemplo de solicitud de cambio de la contabilidad de Diameter**

La figura 2.3 muestra un ejemplo de intercambio de mensaje para la aplicación de contabilidad los nombres de los mensajes se auto explican, el mensaje de intercambio de capacidad está incluido para asegurar que los dos nodos soportan a plenitud la aplicación de contabilidad.

### 2.7.1 Autenticación del protocolo Diameter NASREQ

Las redes modernas descansan en tres mecanismo de autenticación donde un NAS al margen de una red interactúa con una terminal de un servidor AAA a través de un protocolo AAA para tener control de acceso, también vimos que las interacciones de los servidores AAA NAS para tener control de acceso y autenticación estaban centralizados en el diseño de Radius y sus mensajes ya que Radius estaba diseñado como un protocolo cliente-servidor.

Al contrario de Radius, Diameter es un protocolo peer to peer con algo más que autenticación y contabilidad, la aplicación NAS de Diameter describe la interacción entre el NAS y el servidor que no está totalmente estandarizado todavía y se encuentra en estos momentos en un borrador de internet (NASREQDR). Las autenticaciones modernas están basadas principalmente en EAP. Esto significa que

la aplicación EAP de Diameter (DIAEAPR) también será implementada con la aplicación NAS para desarrollar una autenticación EAP con un servidor Diameter a través de un NAS.

Otro elemento invaluable en la aplicación NAS de Diameter es las consideraciones relacionadas con Radius. Diameter fue diseñado para servir eventualmente como un sucesor de Radius y los diseñadores estaban completamente consientes de las grandes deficiencias de Radius, la coexistencia con Radius era considerado especialmente importante para los NASES. Esto junto con las razones históricas (NAS fue probablemente diseñado entre las primeras aplicaciones de Diameter) que llevaron a la aplicación NAS a emplear gran cantidad de su ancho de banda para definir los roles y requerimientos de lo que se conocía como agente de traslación.

La adición de materiales sobre las iteraciones de Radius al NAS de Diameter hace de esta aplicación algo único en comparación con otras aplicaciones de Diameter como por ej. IP-móvil, el cual solamente define la funcionalidad de la aplicación.

#### 2.7.1.1 Comandos introducidos por NASREQ

Ahora necesitamos familiarizarnos con los más importantes comandos utilizados en NAS. La aplicación NAS define un número de comandos que se relacionan mayormente con la autenticación y la autorización. Se supone que como el protocolo Diameter especifica mensajes de contabilidad, la aplicación NAS se centra en los comandos de autorización y de autenticación. Por lo que se piensa que esta suposición se confirma sobre el hecho que NAS define un comando de pedido y de respuesta AA que tienen que ver con las dos primeras A de AAA: Autenticación y Autorización.

- Comando de pedido AA (AAR) (código 265) Es enviado por un NAS para pedir Autenticación y o Autorización para un determinado usuario. En el mensaje de pedido de “R” bit dentro del campo de las banderas de comandos se sitúa para indicar un pedido. Todos los pedidos tienen que incluir información que identifique la fuente de la llamada. Esto podría incluir la relación usuario nombre, identificador de puerto NAS y otros. Para los pedidos de autenticación la relación usuario nombre y la autenticación AVPs se necesita que esté presente. Para los pedidos de Autorización: La información sobre la estación que llama y a la que se llama está incluida. Las especificaciones incluyen una lista detallada AVPs relacionada a autorización, autenticación y otros AVPs llevados a cabo por este comando, entre los AVPs importantes llevados a cabo por

AAR están, NAS-ID, NAS-Dirección-IP, NAS-Puerto, Tipo de pedido de autenticación, Usuario-Contraseña, CHAP-Autenticación, CHAP-Reto.

- Comando de repuesta AA (AAA)(código 265). Es enviado en respuesta al mensaje de pedido AA y puede incluir la autorización AVPs relacionada si la autorización fue pedida y procesada satisfactoriamente. Este mensaje deberá llevar un mensaje de texto a través de un mensaje AVP de respuesta, el "R" bit dentro del campo de banderas está claro.

- Re autenticación, comando de pedido de re autenticación (RAR)(código 258).Ya está definido por el protocolo Diameter pero se menciona aquí para completar la discusión sobre NAS. La aplicación NAS permite al servidor iniciar una Re autenticación y o Re autorización para una sesión.

- Respuesta de re autenticación comando de respuesta de re autenticación (RAA)(código 258). Es también definida por el protocolo Diameter y se envía como respuesta a un pedido de re autenticación y debe incluir AVP resultado-código.

#### 2.7.1.2 NASREQ AVPs.

Diameter reserva los códigos APV de 0 a 255 para la compatibilidad con Radius. La aplicación NAS asigna los valores 363-366 y 406 del código AVP del código de espacio definido en Diameter. Los valores de 363-366 y 406 son asignado para dar soporte a los mecanismos de contabilidad que relacionan a un NAS mientras los valores 401 son para el NAS reglas de filtro y túnel. Los valores 403-405 son asignados al algoritmo CHAP, CHAP-ID y respuestas AVPs CHAP. Note que el desafío CHAP AVP es el mismo que el atributo desafío CHAP (60) definido por Radius. También debería notarse que los intervalos del código valor mencionados anteriormente no son excluyentes a una aplicación NAS. La aplicación IP-móvil usa algunos de estos valores de código pero no hay conflicto de uso entre la aplicación NAS y el IP-móvil.

Aparte de los nuevos códigos AVP introducidos recientemente, el documento NAS utiliza un gran número de AVPs que ya se definieron en el protocolo Diameter pero agrupar estos AVPs en varios grupos de los cuales uno de los más importantes son la sesión NAS de AVPs, Autenticación NAS de AVPs, Autorización NAS de AVPs, Contabilidad NAS de AVPs, Túnel NAS de AVPs y otros AVPs para

la autorización del uso de varios tipos de redes como por ejemplo IP, hipervínculos enmarcados y no enmarcados, IPX.

Para dar algunos ejemplos sobre aplicaciones NAS de AVPs describimos algunas AVPs relacionadas a autenticación PAP y CHAP.

- AVP usuario-contraseña: Lleva la contraseña de autenticación del usuario por mecanismo de autenticación de contraseña o la entrada que el usuario da en mecanismos multirondas de autenticación. La contraseña puede ser una contraseña permanente o parcial debido a la accesibilidad de las contraseñas permanentes los mensajes Diameter que llevan estas contraseñas tienen que ser protegidos por un mecanismo de seguridad de extremo a extremo como por ejemplo el SMS (del inglés: Short Message Service, es un servicio disponible en el empleo de teléfonos móviles para el envío de mensajes cortos) cuando transita por proxy no confiables. En estos casos la protección Hop by Hop que da IPSec o TLS no es suficiente.

- Reintento de contraseña AVPs: Cuando ocurre una falla de autenticación el servidor reenvía un mensaje de respuesta AA indicando la falla y al mismo tiempo puede incluir un AVP de reintento de contraseña indicando el número de intentos de autenticación que un usuario puede llevar a cabo.

- AVP autenticación CHAP: Se usa para llevar a cabo la información necesaria para ejecutar un desafío basado en una autenticación PPP. AVP autenticación CHAP es un grupo AVP que significa que pueden ser incluidos otros AVP como por ejemplo, algoritmo CHAP AVP, identificador CHAP AVP, respuesta CHAP AVPs. El algoritmo CHAP AVP incluye un identificador que indica que el algoritmo debía ser usado para computar una respuesta al desafío, mientras que la identidad CHAP AVP incluye un identificador que se usa para calcular la respuesta. Hasta ahora en MD5 (del inglés: Message-Digest Algorithm 5, es un algoritmo de reducción criptográfico), que está estandarizado como un algoritmo CHAP. El AVP repuesta CHAP incluye los datos de autenticación calculados por el usuario en respuesta al desafío.

- Desafío CHAP: Incluye el desafío que fue enviado por el NAS al par CHAP. Note que este AVP no está definido como parte del grupo dentro de la autenticación CHAP AVP. Si la autenticación CHAP AVP se incluye en un mensaje el desafío CHAP AVP tiene que ser incluido también.

### 2.7.1.3 Mensajería NAS

Un ejemplo del intercambio de mensaje NAS servidor se muestra en la figura 2.4. Nótese que el intercambio de mensaje entre el NAS y el usuario no está considerado como un intercambio de mensaje de Diameter y solamente está incluido por exhaustividad.

Como se puede observar el ejemplo del concepto es más bien simple:

- A la llegada de una nueva llamada, un servicio de pedido o un pedido de re autenticación del usuario el NAS crea un mensaje de pedido de AA de Diameter (AAR) incluyendo la identidad del usuario, la información de pedido del usuario y otra información relacionada con la llamada y envía el mensaje a un servidor.

- El servidor procesa el pedido y devuelve un mensaje de respuesta AA de Diameter que incluye la información de la autorización o un AVP código-resultado indicando una falla. Alternativamente el servidor debe indicar que otras rondas de intercambio son requeridas para completar el proceso de autenticación. Note que Diameter también permite pedidos de solo autorización los cuales no incluye ningún dato relacionado con autenticación. Permitir esta opción debía sin embargo incluir serios riesgos de seguridad si no está diseñada adecuadamente. Aún cuando la correspondencia de funcionalidad no existe en Radius la travesía de dichos pedidos a través de los agentes de traslación puede conducir a una falla en el completamiento del intercambio cliente servidor en cuanto a pedidos de solo autorización.

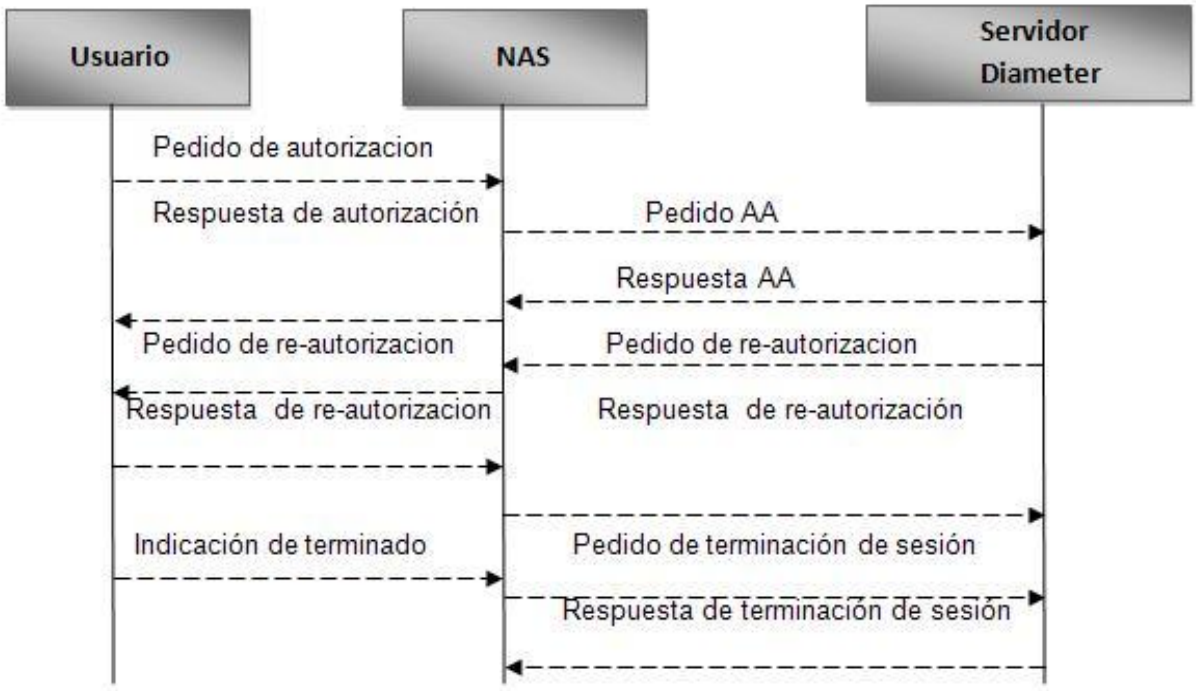


**Figura 2.4 Mensajes NAS para aplicaciones Diameter**

- Cuando el intercambio de autenticación o autorización se completa exitosamente la aplicación NAS empieza un contexto de sesión. Si la contabilidad será implementada, un mensaje de contabilidad será enviado para registrar el comienzo de la nueva sesión. En dependencia de la política de red el fallo al establecer los procedimiento de contabilidad para la sesión puede ser un fallo para establecer la sesión el servidor Diameter informa al NAS sobre el tiempo máximo permitido antes de la próxima re autorización o re autenticación usando AVP de autorización de tiempo límite.

- La sesión empieza y la aplicación NAS empieza la sesión de contexto si se pide la contabilidad la aplicación necesita enviar un mensaje de contabilidad. El NAS debe intentar la re autenticación o la re autorización antes de que termine el período de autorización. Aunque los servidores típicamente implementan un período de gracia antes que libere todo el estado de información que tiene que ver con el usuario, el servidor debe emitir un aviso de pedido de re autorización re autenticación no solicitada antes de que espire el período de autorización para evitar la terminación del servicio.

- Cuando el usuario indica al NAS que necesita terminar una sesión existente, el NAS emite un período de terminación de sesión (STR) al servidor Diameter. Cuando los procedimientos de contabilidad son implementados la terminación de la sesión necesita ser comunicada al servidor.

- Al recibir y procesar un pedido de terminación de sesión válido el servidor Diameter responde con una respuesta, determinación de sesión RSTA, incluyendo un AVP código-resultado. Cuando se termina la sesión el servidor liberará todos los recursos que están atados a la sesión ID para la sesión cerrada. También todos lo servidores proxy en la cadenas de proxy liberarán cualquier recurso relacionado.

## 2.8 Aplicación móvil IP

Al discutir sobre el registro del móvil IP, discutimos el uso del servidor AAA en la autenticación de la señalización de mensajes de móvil IP al servidor AAA FA y HA (un agente local almacena información sobre el nodo móvil cuya dirección permanente es la red del agente), sin embargo también mencionamos que el móvil IP solo discute las autenticaciones del registro de pedido y respuesta y la distribución principal desde el servidor AAA al dispositivo móvil. Ellos no describen como el mismo material clave es distribuido a los agentes de móvil IP. Esas especificaciones simplemente afirman que las interacciones entre servidores AAA y agentes móviles (FA y HA) son manejadas por protocolos AAA. IETF AAA WWG ha estado trabajando en proveer especificaciones para el uso de Diameter para llevar a cabo la autenticación inicial y la distribución principal requerida por las señalizaciones IP por mucho más tiempo [DIAMIPDR]. La especificación no solo provee detalles de la autenticación sino también autorización y contabilidad por ejemplo esto no solo ayuda a especificar como la FA autentica un nodo móvil que esta visitando la red foránea sino también como el FA informa el dominio al que pertenece el nodo móvil sobre los recursos que el NM consume en la red foránea. Debe notarse sin embargo que esta especificación solo se aplica al IPv4 y no al IPv6 (es una nueva versión de IP después de IPv4).

## 2.9 Soporte EAP

EAP provee un marco para dar autenticación y servicios de control de acceso para muchos tipos diferentes de multimedia. También se mencionó que las señalizaciones EAP entre el servidor AAA y el

NAS es llevada a cabo por un protocolo AAA. Se describió brevemente la encapsulación de mensajes EAP dentro de Diameter y los atributos de Diameter utilizados para este propósito.

Los detalles del soporte de Diameter para EAP se proveen en la aplicación EAP de Diameter [DIAEAPDR].
La aplicación EAP de Diameter tiene que ver con la autenticación y el transporte de mensaje relacionado a la autenticación entre NAS y servidores AAA, está estrechamente ligado a la aplicación NASREQ. Esto se refiere a que para un agente Diameter que soporte la aplicación EAP debe también soportar la aplicación NASREQ. Un agente Diameter puede establecer su soporte de EAP para que el cliente y NAS sepan si pueden comprometerse en un intercambio EAP. Cuando un servidor no puede soportar EAP debe permitir al NAS negociar otros mecanismos de autenticación como PAP o CHAP con el fin usuario dispositivo.
El modelo para transportar EAP sobre Diameter es muy similar al de Radius.

- Los mensajes EAP que van desde el NAS hacia el servidor AAA son llevado dentro de mensajes de pedido de Diameter. El mensaje EAP por si solo es llevado como un EAP-payload-AVP.

- Los mensajes EAP desde el servidor AAA al NAS son llevados en un mensaje de respuesta EAP. El mensaje EAP es llevado por si solo en un EAP-payload-AVP. El código resultado puede ser utilizado para indicar información adicional al NAS por ejemplo en el comienzo de un una conversación EAP al recibir el primer mensaje de pedido desde el NAS el servidor Diameter puede enviar un DIAMETER-MULTI-ROUND-AUTH dentro del código resultado AVP para indicar al NAS que se esperan más mensajes de pedido que tienen que ver con el procedimiento de autenticación que se está llevando a cabo.

Aunque frecuentemente el servidor EAP se adjunta colocado con los servidores Diameter, como el EAP y el Diameter son todavía mecanismos separados, la interacción requiere algunas consideraciones.

- El EAP se comunica entre el EAP (FIN-USUARIO-DISPOSITIVO) y el servidor EAP, más que con el NAS. Por otra parte el NAS se comunica con el Diameter y puede no entender ningunos de los mensajes EAP excepto el éxito de EAP y el fracaso y actuar solo como un puente para el resto de los mensajes.

- El resultado del proceso de autenticación es típicamente convenido directamente al par EAP a través de los mensajes de éxito o fallo de EAP mientras que el resultado del proceso de autorización de acceso se le asigna al NAS a través de código resultado AVP en la respuesta de Diameter. Si los dos procesos presentan conflicto, por ejemplo, un mensaje de éxito de EAP se envía al par junto con el mensaje de Diameter conjuntamente con el NAS que transporta una falla código resultado AVP el par puede creer que tienen derecho a acceder a la red mientras que el NAS no puede autorizar ningún acceso al par, el conflicto puede pasar si hay proxy Diameter en el camino de su propias decisiones de autorización.

- Muchas redes de accesos surgidas hoy, se esfuerzan en proteger la identidad del usuario permitiendo que el usuario no mande su identidad actual en un pedido EAP que inicia y está desprotegido. En otros tiempos solamente el mensaje EAP y no el mensaje Diameter puede llevar la identidad del usuario. Un NAS que no tiene la capacidad de entender las señalizaciones EAP puede no estar informado sobre la verdadera identidad del par. Debe tenerse mucho cuidado para que en algún punto algunas partes de las identidades del par interactúen con el NAS y así el NAS pueda autorizar al par para acceder y contabilizar sus recursos.

- Frecuentemente la información sensible de primera mano puede necesitar ser transportada en mensajes EAP. Los estándar de Diameter aún no proveen especificaciones en protección de seguridad extremo a extremo (SMS DIAMETER nunca fue estandarizado) y solamente provee una guía de IPSec o TLS para aprovisionar la seguridad de extremo a extremo. Por esta razón debe tenerse mucho cuidado para protegerse la confidencialidad de claves sensibles en tránsito.

## 2.10 Conclusiones

En este capítulo se abordó y profundizó sobre las características del protocolo Diameter, con el objetivo de ver a través de dichas características las mejoras que tiene este protocolo así como su forma de utilización.

# Capítulo 3: Diameter como solución óptima

## 3.1 Introducción

Ahora que se completó el intento de describir las principales características y funcionalidades del protocolo Diameter a través del curso de su evolución se tratará de proveer en este capítulo una comparación entre él y sus antecesores, en el cual se proporcionarán algunas observaciones acerca de por qué el protocolo Diameter fue objeto de la investigación.

## 3.2 Comparativa TACACS+ y Radius

TACACS+ es un protocolo propiedad de CISCO, que sustituye los protocolos TACACS y XTACACS, que sólo proporcionaban autenticación. Cisco añadió seguridad al estándar y la posibilidad de dividir el servidor AAA en tres servidores por separado. Debido a que es propiedad de Cisco, el estándar está perdiendo popularidad entre los proveedores.

El protocolo TACACS+ es un protocolo cliente servidor AAA al igual que Radius y ofrece muchos de los servicios que presta el servidor RADIUS con diferencias tan solo de forma y no de fondo como son:

- TACACS+ usa TCP a diferencia de RADIUS que utiliza UDP.
- RADIUS combina tanto la autenticación como la autorización a diferencia de TACACS+ que lo hace por separado.

Los protocolos AAA como TACACS + y RADIUS fueron desplegados para proporcionar acceso telefónico (PPP) y la terminal de acceso al servidor. Con el tiempo, con el crecimiento de la Internet y la introducción de nuevas tecnologías de acceso, incluidos los inalámbricos, DSL, Mobile IP y Ethernet, router y servidores de acceso a la red (NAS) han aumentado en complejidad y densidad, poniendo nuevas demandas sobre los protocolos de AAA.

El protocolo Diameter, normalizado por el grupo de trabajo de la IETF Autenticación, Autorización y Contabilidad, es el sucesor del protocolo de Radius y fue desarrollado para superar varias limitaciones de su antecesor.

## 3.3 Ventajas de Diameter sobre Radius

En la siguiente subsección se dan una lista de mejoras que Diameter tiene como un protocolo AAA sobre las que ofrece RADIUS.

### 3.3.1 Conmutación por Error

La conmutación por error se define como un proceso de envío de todos los pedidos pendientes de un agente a otro agente una vez que una falla transportada con el primer agente es detectada. Para que esto sea posible se requiere que los nodos hayan acordado el soporte de la falla poniendo una bandera en los mensajes de Diameter.

Radius no define un mecanismo estándar de conmutación por errores y como resultado una conducta de conmutación por errores puede diferir entre las implementaciones de Radius, él tiene que estar apoyado por otro tipo de servidor que acepte conmutación por error, ya que los clientes que se vayan a conectar a él no sabrían si el servidor está disponible o no. Por otra parte Diameter es más confiable para transportar fallas y para proveer una conducta bien definida de conmutación de errores. Diameter soporta aplicaciones de capas de conocimientos y mecanismos específicos de alertas que detectan la falta de actividad. De manera general se puede decir que Diameter brinda posibilidades para la conmutación por error al contrario de Radius demostrándose así una de las características por las cuales Diameter es superior a su antecesor.

### 3.3.2 Mensaje de inicio del servidor

El soporte de los mensajes de inicio del servidor es solamente opcional en Radius [RAD3576] y esto hace que se dificulte implementar opciones tales como desconexiones no solicitadas o re autenticación o re autorizaciones en demandas a través de un despliegue heterogéneo. En el protocolo Diameter el soporte de mensajes de inicio de servidor es obligatorio.

### 3.3.3 Transporte confiable

Al usar UDP como un transporte y carecer de retransmisión en Radius hace que la confiabilidad sea pobre para la contabilidad: la pérdida de paquetes puede traducirse directamente en pérdida de recurso. Diameter tiene mecanismo de transporte más confiable (TCP y SCTP).

Aunque UDP es una conexión mucho mas rápida que TCP esta no permite la comprobación de los datos ni la retransmisión de aquellos que se queden en el camino, lo cual hace una desventaja en la conexión de Radius, mientras que una vez más Diameter se va por encima de este erradicando este error ya que utiliza TCP y SCTP que aunque sean un poco más lentos no existe la pérdida de datos que es el aspecto más importante.

### 3.3.4 Capacidad de negociación

El cliente y el servidor no tienen ninguna forma de indicar su apoyo a diversos atributos entre ellos y Radius no soporta mensajes de error. Esto significa que la capacidad de realizar descubrimiento y la negociación para un acuerdo de servicio puede ser muy difícil con Radius. La capacidad de negociación de Diameter incluye soporte para manejo de errores, así como la forma de indicar el apoyo de pares atributo-valor (a través de la bandera u obligatoria).

Para lograr el soporte de errores en Radius sería necesario tener otro servidor que respalde esta debilidad de Radius lo cual hace mucho más difícil su configuración y despliegue. Aunque se puede destacar que existen versiones de servidores Radius de código abierto en las cuales se pude configurar esta debilidad, tal es el caso de Free Radius.

### 3.3.5 Parámetros de seguridad y audibilidad

Radius define una capa de aplicación de protección de la integridad (autenticación de mensajes), esquema que solo se requiere para el acceso de los paquetes de respuestas. La autenticación está basada en compartir secretos pero la confianza solo está establecida entre las rutas vecinas y no de extremo a extremo. Proxy maliciosos entre clientes y servidores pueden modificar atributos e incluso la cabeza del mensaje sin ser detectados. No hay soporte de confidencialidad por paquete solo atributos que se pueden esconder. El protocolo de contabilidad de Radius tiene parámetros de re ejecución de

protección. El soporte de IPSec no se requiere en Radius. El uso de IPSec solo se define cuando Radius se usa con IPv6. Aún entonces el uso de IKE limita la usabilidad de IPSec para varias aplicaciones, también no tener la posibilidades de establecer un certificado de jerarquía hace del uso de Radius una aplicación itinerante muy difícil, donde la relaciones de confianzas inter dominios AAA se necesitan.

Por otra parte Diameter define ambos niveles de transmisión de seguridad y seguridad de extremo a extremo y requiere soporte obligatorio de IPSec y soporte opcional TLS en los clientes. Sin embargo la seguridad de los datos de un objeto no es obligatoria en Diameter

### 3.3.6 Soporte de DIAMETER para agentes e inter dominios itinerantes

El protocolo Radius no provee soporte para agentes y proxy claramente, como esta conducta no se define él varía ascendentemente entre las implementaciones e interoperabilidad de problemas. Aún cuando el concepto de cadena de Radius vía servidores inter medios se define debido a la carencia explicita de soporte para proxy y datos de objetos y transmisión de nivel de seguridad, el movimiento basado en Radius es vulnerable a ataques de fraude y como resultado puede causar problemas a gran escala en el despliegue.

Diameter define error de agentes y proxy y sus conductas explícitamente. Al proveer soporte explícito para inter dominios itinerantes, ruteo de mensajes y seguridad de capas de transmisión, Diameter sobre dirige las limitaciones de Radius.

Aunque la tecnología de este nuevo esquema como son los agentes lleva algunos años en ejecución todavía se puede considerar que es embrionario ya que algunos aspectos fundamentales como es la seguridad no se encuentran satisfactoriamente desarrollados y como Radius no proporciona una seguridad de extremo a extremo quedan expuestos estos agentes a cualquier tipo de ataques, no ocurriendo esto en Diameter.

### 3.3.7 Configuración y descubrimientos de pares

Las implementaciones de Radius requieren el nombre o la dirección de los servidores o los clientes para ser configuradas manualmente así como los correspondientes secretos compartidos. Esto incide en una gran carga administrativa y propicia la tentación de usar los secretos compartidos de Radius para muchos clientes (NAS) y puede resultar en grandes vulnerabilidades de seguridad.

A través del DNS (del inglés: Domain Name System, es una base de datos que almacena información asociada a nombres de dominio) Diameter posibilita un descubrimiento de pares dinámicos, la derivación de claves dinámicas de sesiones es posible mediante la transmisión de niveles de seguridad, ya que el DNS proporciona algunas ventajas como son:

- Desaparece la carga excesiva en la red y en los host.
- No hay duplicidad de nombres: el problema se elimina debido a la existencia de dominios controlados por un único administrador. Puede haber nombres iguales pero en dominio diferentes.
- Consistencia de la información: la información que esta distribuida es actualizada automáticamente sin la intervención de ningún administrador.

### 3.3.8 Compatibilidad con Radius

Aunque Diameter no comparte un formato de mensaje con Radius, se ha gastado un considerable esfuerzo para permitir la compatibilidad con su antecesor a fin de que los dos protocolos puedan ser desplegados en la misma red. No obstante, se espera que las traducciones tengan lugar a través de pasarelas que permiten la comunicación entre dispositivos y legado de Radius con los agentes Diameter.

### 3.3.9 Problemas con la utilización de Diámetro

Debido a que las bases del protocolo Diameter (RFC) no llevan tanto tiempo en divulgación para el uso de los usuarios muchas compañías se han opuesto a trabajar con Diameter por lo que el despliegue ha sido lento ya que muchos clientes no dieron su paso adelante, además algunos vendedores afirman que Diameter será utilizado solo por los usuarios de IPv6.

Debido a que Diameter en sus requisitos utiliza TCP y SCTP apoyado por los agentes y servidores del mismo sobrecargan la red y los enlaces, ya en este protocolo no tienen las características de peso ligero como es UDP la cual fue sustituida por el complicado TCP y SCTP para el período de sesiones y las cuestiones de aplicaciones de él.

Existe un gran despliegue sobre el protocolo Radius y de Diameter solo un buen plan de emigración que incluye el despliegue de agentes para la traducción y la coexistencia de Radius y Diameter, lo cual no será una migración sencilla.

### 3.3.10 Iteraciones Diameter-Radius (traducción agentes)

Diameter y Radius como se mencionó anteriormente puede que tengan que coexistir dentro de los límites del mismo operador de la administración durante un largo período de emigración. Por esto en el proceso de diseño de Diameter se centró una gran cantidad de esfuerzo en la prestación de servicios para la coexistencia de estos dos protocolos. Un ejemplo de estos esfuerzos es que se garantizó que el espacio del atributo Radius esté incluido dentro del espacio del atributo Diameter para eliminar la necesidad de atribuir la conversación entre Radius y Diameter. Sin embargo Diameter crea un subconjunto de las características y los mensajes de Radius, por esa razón coexisten Diameter y Radius.

Debido a su enfoque en materia de autenticación y autorización, la aplicación Diameter – NAS es la especificación con más similitud a Radius. Por esta razón esta aplicación es la primera que se describe en la especificación de interoperabilidad entre las implementaciones Diameter y Radius. Esta interoperabilidad se prevee a través de una arquitectura que consta de distintos sistemas de Radius y Diameter a través de un traducción de agentes en su frontera.

Dado que la funcionalidad de Diameter es superior a la de Radius y hay muchas diferencias entre estos puede haber muchas variantes y aplicaciones para los agentes encargados de la traducción. También debido a las simultáneas normalizaciones Radius-Diameter, varios mensajes de Radius pueden ser manejados de diferentes maneras por los diferentes agentes de traducción a lo largo del proceso, mientras que ninguno de los agentes de traducción puede tener acceso a la completa y exacta información del estado de la sesión.

La aplicación Diameter – NAS describe muchos requisitos y procedimientos de conversación Diameter de Radius –Agente de traducción. No se entrará en detalles exactos sobre como ocurre la traducción de un mensaje, un atributo o AVP o un servicio como la seguridad se lleva a cabo en todos los casos. Se destacarán algunas cuestiones importantes de consideración en la traducción:

- Radius: mecanismo de seguridad de Hop by Hop, mientras que Diameter puede aplicar seguridad de extremo a extremo.los agentes de Diameter tendrán que descifrar los mensajes y atributos de Radius y asegurar la información de manera específica como se plantea en el protocolo Diameter. Por ejemplo cuando el agente recibe una traducción Radius el mensaje debe incluir el atributo contraseña de un usuario encriptadas por Radius la cual debe estar compartida para establecer el enlace, el agente debe descifrar la contraseña de Radius y remitirá la información dentro de la contraseña en un mensaje de Diameter que está protegido por mecanismos de seguridad de este protocolo. Al autenticar el valor de un mensaje-Radius que incluye mensaje para autenticar un atributo (definido por [RATEXT2869]) debe ser verificada por el agente de traducción, pero no incluida en el mensaje creado por el agente Diameter.

- Radius no apoya la arquitectura peer to peer, ni la arquitectura de un mensaje iniciado por el servidor, mientras que Diameter define un gran número de códigos de comandos que se pueden usar tanto en la solicitud y mensajes de una respuesta de manera peer to peer. Cuando las negociaciones involucran múltiples rondas de intercambio de mensajes Radius ofrece acceso a petición del cliente y al servidor de acceso de desafío para los mensajes del servidor al cliente. El agente de traducción debe crear los mensajes de solicitud de acceso basado en los comandos de Diameter.

- Los servidores Radius son errantes mientras que los nodos de Diameter mantienen su estado, los agentes Diameter pueden tener una imagen encubierta de manera general de extremo a extremo en el período de sesiones.

- AVPs – Diameter definen el nombre de dominio completo (FQDN (Fully Qualified Domain Name, es un nombre que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo)), mientras que Radius no los define. Los agentes de traducción

deben cambiar el formato de la información de acuerdo con el sistema para el mensaje que se esta remitiendo. Un buen ejemplo de esto es la conversión de Radius –NAS –Atributo en la dirección de ip de origen Diameter huésped AVP en el formato FQDN.

- Diameter se apoya en los grupos AVPs. Cuando el agente recibe la traducción atributo Radius o de los atributos Radius(es decir tanto de uno como de varios) tendrá que ser parte de un grupo de AVP, que el agente deberá extraer el correspondiente atributo Radius para construir el grupo AVP – Diameter. Ejemplo es la manipulación de intercambio de CHAP. El atributo CHAP-Contraseña de Radius incluye la respuesta de los datos del atributo, además incluye CHAP-ID en la cabeza de los atributos. Al contrario de esto Diameter define un grupo de Autentificación - CHAP-AVP que incluye CHAP- respuesta y CHAP-IDENT, como sub-AVPs. Esta conversión tiene que ser realizada por los agentes de traducción.

En resumen los agentes de traducción son los responsables de actuar en las pasarelas de interoperabilidad entre Radius y Diameter. El problema es: Diameter no especifica los detalles de la operación de estos agentes, por lo tanto la aplicación de Diameter para esto no puede ser llevado por si solo hacia atrás para corresponder con Radius de manera plug -and –play.

El protocolo TACACS+ es más seguro que Radius debido a la conexión TCP, pero este tiene mejor accounting y una mejor interfaz de programación. En algunos puntos estos protocolos son superiores en características y funcionalidades unos respecto al otro, desde diferentes puntos de vista uno puede ser superior al otro pero lo que si queda claro es que ninguno de los dos ha logrado ser tan completo como el protocolo Diameter que erradica las debilidades de ambos protocolos.

## 3.4 Conclusiones

Como se muestra en esta comparación el protocolo Diameter no solamente por ser el más actual es el que nos brinda mayor factibilidad para la seguridad de una red inalámbrica, sino por todas las principales características que ha ido incorporando y mejorando de sus antecesores. Ya en el se muestra una mayor robustez respecto a la seguridad y contabilidad de la red. Actualmente la utilización de este protocolo no se encuentra tan difundida ya que muchos de sus componentes son cambiantes debido a que se encuentran en desarrollo actualmente.

# Conclusiones Generales

- Concluida la investigación del protocolo Diameter sobre los procedimientos de la AAA, se logró la comprensión de las funciones que brinda este protocolo para la red inalámbrica dando cumplimiento a los objetivos de este trabajo.
- Con lo anteriormente explicado e investigado se ha llegado a la conclusión que la implementación de Diameter permitirá proveer de servicios más seguros y confiables en las redes inalámbricas logrando tener total control de la actividad que se esté realizando en la misma a través de la contabilidad, con todas estas características y funcionalidades que brindaría Diameter se lograría obtener mejoras en la red inalámbrica.
- Una vez realizado el estudio de las características del protocolo Diameter conjuntamente con el protocolo AAA así como de la red inalámbrica de la universidad, se llegó a la conclusión que este protocolo sería el idóneo para garantizar la seguridad de una red inalámbrica debido a todas las características y funcionalidades que brindan los mismos en cuanto a seguridad, confiabilidad, accesibilidad y administración. Todo esto queda respaldado por lo anteriormente expuesto.
- Se logró observar que aunque existan protocolos que también se pueden utilizar para garantizar la seguridad en la red inalámbrica de la UCI, Diameter erradica las principales dificultades de dichos protocolos.

Concluido este trabajo de diploma y desarrollado los temas que en él se expone, se logró de modo general una mayor comprensión de los beneficios que trae consigo la utilización del protocolo Diameter sobre los procedimientos de la AAA.

# Recomendaciones

- Siendo el protocolo Diameter totalmente nuevo y muchas de sus características y funcionalidades todavía se encuentran en desarrollo se recomienda que se continúe la investigación del mismo ya que pueden existir cambios y actualizaciones que no estarían comprendidas en la presente investigación.

- Se recomienda que se adquiera la tecnología necesaria para poner en prueba este protocolo en un medio real y así quede respaldada la presente investigación.

- Se debe tener en cuenta la presente investigación a la hora de escoger un protocolo efectivo para desplegar la red inalámbrica en la universidad de las ciencias informáticas (UCI).

# Referencias Bibliográfica


1. [En línea] (http://fmc.axarnet.es/redes/tema_06.htm)
2. [En línea] http://ieee.com/AAA.com.
3. [En línea] http:// www.wisdom.weizmann.ac.i1/itsik/RC4/Papers/Mantin1.zip/.
4. [En línea] http://tools.ietf.org/html/rfc2284"
5. [En línea] http://tools.ietf.org/html/rfc2716"
6. [En línea] http://tools.ietf.org/html/rfc3602"
7. [En línea] (wwwgobiernodecanarias.org/educación/conocernos_mejor/pagina/protocol1.htm)
8. [En línea] (fmc.axarnet.es/redes/tema6.htm)
9. [En línea] http://www.wikipedia.org/wiki/Seguridad Informatica/.
10. [En línea] http://tools.ietf.org/html/rfc2058"
11. [En línea] http://tools.ietf.org/html/rfc2059"
12. [En línea] http://tools.ietf.org/html/rfc2881"
13. [En línea] http://tools.ietf.org/html/rfc2661"
14. Radius. [En línea] 2009. .http://www.wikipedia.org/wiki/Radius/.
15. [En línea] www.faqs.org/rfcs/rfc3261.html - 616k .
16. [En línea] www.faqs.org/rfcs/rfc3588.
17. [En línea] www.faqs.org/rfcs/rfc793.
18. [En línea] www.faqs.org/rfcs/rfc2960.
19. **JohnWiley.** *AAA and Network Security for Mobile Access.* USA : s.n., 2005. 318.

# Bibliografía


1. Cuba se lanza a la telefonia IP y la television digital. s.l. : Diario de la Juventud Cubana, 03 30, 2009.
2. Diameter. [Online] http://wikipedia.org/wiki/Diameter.
3. Diameter y Radius para permitir interoperabilidad. Liu, Yan.
4. Especial seguridad en entornos inalambricos. Forado, Raymond. 2005.
5. [En línea] (http://fmc.axarnet.es/redes/tema_06.htm)
6. [En línea] http://ieee.com/AAA.com.
7. Forado, Raymond. Seguridad en redes Wimax. [Online] 2008. http://www.bormart.es.
8. http://www.normes-internet.com
9. Institute of Electrical and Electronic Engineers. [Online] http://www.ieee.org/.
10. **Izquierdo, Antonio.** Metodologia para la validacion y evaluacion remota de implementaciones de protocolos de seguridad.Aplicacion a la arquitectura IPSec. Madrid : Universidad Carlos III, 2006.
11. **John&Sons.** AAA and network Security for Mobile Access. EEUU : Motorola, 2005. 318.
12. Protocolo AAA. [Online] “http://www.wikipedia.org/wiki/Protocolo AAA/”.
13. Protocolo de comunicaciones . [Online] http://www.wikipwdia.org/wiki/protocolo de comunicacion.
14. Protocolo de seguridad en redes inalambricas. Madrid : Universidad Carlos III.
15. Radius. [Online] 2009. http://www.wikipedia.org/wiki/Radius/.
16. Security Portal. Security Portal. [Online] 2006. http://www.joomla.org/.

# Glosario de términos

A continuación se presenta por orden alfabético algunos de los términos utilizados en la realización de este documento y que puedan crear confusión en la comprensión del mismo.

**AAA:** En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting en inglés). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

**ACKs:** ACKNOWLEDGEMENT (ACK) (en español acuse de recibo), en comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes ha llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente".

**AES:** Advanced Encryption Standard (AES), también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Se espera que sea usado en el mundo entero y analizado exhaustivamente, como fue el caso de su predecesor, el Data Encryption Standard (DES).

**Ancho de banda**: En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

**Bluetooth**: La tecnología inalámbrica Bluetooth es una tecnología de ondas de radio de corto alcance (2.4 giga hertzios de frecuencia) cuyo objetivo es el simplificar las comunicaciones entre dispositivos informáticos, como ordenadores móviles, teléfonos móviles, otros dispositivos de mano y entre estos dispositivos e Internet. También pretende simplificar la sincronización de datos entre los dispositivos y otros ordenadores.

**Carrier class:** en telecomunicaciones, un "Carrier Grade" o "clase transportista" se refiere a un sistema o un componente de hardware o software que es muy fiable, muy probado y demostrado en sus

capacidades. Portador de grado, sus sistemas son probados y fabricados para cumplir o superar los "cinco nueves" normas de alta disponibilidad, y dar muy rápido a través de recuperación de fallos de redundancia (normalmente menos de 50 milisegundos).

**CAs:** La CA es la entidad certificadora dentro de una infraestructura PKI. De ella salen todos los otros certificados.

**CHAP:** es un protocolo de autenticación por desafío mutuo (CHAP, en inglés: Challenge Handshake Authentication Protocol).Es un método de autentificación remota o inalámbrica. Diversos proveedores de servicios emplean CHAP. Por ejemplo, para autentificar a un usuario frente a un ISP.CHAP es un método de autentificación usado por servidores accesibles vía PPP. CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa en un secreto compartido (como una contraseña).

**Conmutación:** La conmutación es una técnica que sirve para hacer un uso eficiente de los enlaces físicos en una red de computadoras. Si no existiese una técnica de conmutación en la comunicación entre dos nodos, se tendría que enlazar en forma de malla. Una ventaja adicional de la conmutación de paquetes, (además de la seguridad de transmisión de datos) es que como se parte en paquetes el mensaje, éste se está ensamblando de una manera más rápida en el nodo destino.

**Daemon:** es un programa de ordenador que se ejecuta en segundo plano, hay varios daemon.

**DNS:** El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

**DNS SRV** : RR de DNS que especifica la ubicación del servidor (s) para un protocolo específico. El servidor SRV RR permite a los administradores utilizar varios servidores de un solo dominio, de pasar de los servidores de acogida para acoger con poco ruido, y al designar algunos host como servidores primarios para un servicio y otros como las copias de seguridad.

**DSL:** (siglas de Digital Subscriber Line, "línea de suscripción digital") es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica básica o conmutada

**EAP: (Extensible Authentication Protocol)** es una autenticación framework usada habitualmente en redes WLAN Point-to-Point-Protocol. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es mas frecuente su uso.

**FA:** almacena información sobre cada nodo móvil visitado en su red. Los agentes externos también cuidan la dirección que está siendo usada por el móvil IP.

**FQDN:** (Fully Qualified Domain Name) es un nombre que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo. Por ejemplo, dada la computadora llamada «serv1» y el nombre de dominio «bar.com», el FQDN será «serv1.bar.com», a su vez un FQDN asociado a serv1 podría ser «post.serv1.bar.com».

**GSM:** Global System for Mobile communications o Sistema Global para las Comunicaciones Móviles. Principal estándar para la telefonía móvil digital. Se dice que la telefonía analógica pertenecía a la primera generación, siendo GSM de 2G.

**GPRS:** General Packet Radio Service o Servicio General de Paquetes por Radio. Esta tecnología es la extensión de GSM para la transmisión de datos (se cambió de la conmutación de circuitos en GSM a la conmutación de paquetes en GPRS). Sólo necesita modificaciones en el software de las estaciones de radio para lograrlo. Se considera que está situada entre GSM y UMTS.

**HA:** almacena la información sobre el nodo móvil cuya dirección permanente es la de la red del agente.

**HSPA:** High Speed Packet Access o Alta Velocidad de acceso de Paquetes. Esta tecnología es también conocida como HSDPA (High Speed Down-Link Packet Access) correspondiente a 3.5G el y 3.5 plus o 3.75 al HSUPA (High Speed up-link Packet Access). Conjunto de protocolos que mejoran el ancho de banda sobre UMTS, pero mucho más rápido que ésta.

**Host o terminal**: Aparato capaz de realizar operaciones de diálogo con un servidor. También se le llama cliente. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc.

**Hop by Hop:** es el principio de controlar el flujo de datos en una red. Con el transporte hop-by-hop, los trozos de datos se transmiten de nodo a nodo en un almacenamiento y forma de reenvío.

**IEEE:** Electronics and Electrical Engineers. Una sociedad profesional de ingenieros eléctricos y científicos informáticos que subvencionan una serie de grupos de estándares técnicos.

**IETF:** Internet Engineering Task Force, en español Grupo de Trabajo en Ingeniería de Internet, es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad.

**IKE:** Internet ley Exchange (IKE) es un protocolo usado para establecer una Asociación de Seguridad (SA) en el protocolo IPSec. Supone una alternativa al intercambio manual de claves. Su objetivo es la negociación de una Asociación de Seguridad para IPSEC. Permite, además, especificar el tiempo de vida de la sesión IPSEC, autenticación dinámica de otras máquinas, etc.

**Interoperabilidad:** Capacidad de los sistemas de tecnologías de la información y las comunicaciones (TIC), y de los procesos empresariales a los que apoyan, de intercambiar datos y posibilitar la puesta en común de información y conocimientos.

**IP**: El Protocolo de Internet (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

**IPv4:** es la versión 4 del Protocolo IP (Internet Protocol) versión anterior de ipv6. Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

**IPv6:** El protocolo IPv6 es una nueva versión de IP (Internet Protocol), diseñada para reemplazar a la versión 4 (IPv4) RFC 791, IPv6 es la segunda versión del Protocolo de Internet que se ha adoptado para uso general. También hubo un IPv5, pero no fue un sucesor de IPv4; mejor dicho, fue un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio.

**IPSec:** Internet Protocol Security. Protocolo que brinda seguridad de transmisión de información sensible a través de redes públicas, tales como Internet.

**ISP:** Un proveedor de servicios de Internet (o ISP, por la sigla en idioma inglés de Internet Service Provider) es una empresa dedicada a conectar a Internet a los usuarios, o las distintas redes que tengan, y a dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrece servicios relacionados, como alojamiento web o registro de dominios, entre otros.

**IPX/SPX:** (del inglés Internetwork Packet Exchange/Sequenced Packet Exchange), Protocolo Novell o simplemente IPX es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red NetWare. El protocolo Intercambio de Paquetes Entre Redes (IPX) es la implementación del protocolo IDP (Internet Datagram Protocol) de Xerox. Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino.

**LAN:** Una red de área local, red local o LAN (del inglés Local Area Network) es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

**LMDS:** El Sistema de Distribución Local Multipunto o LMDS (del inglés Local Multipoint Distribution Service) es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a internet, comunicaciones de datos en redes privadas, y video bajo demanda.

**L2TP:** (Layer 2 Tunneling Protocol) fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado

**MAN:** (Metropolitan Area Network o MAN, en inglés) es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como una excelente

alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

**MD5:** En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

**Modelo OSI**: Modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection).

**NAPTR**: de inglés: Naming Authority Pointer: es un Nuevo tipo de registro DNS.

**NAS:** tiene la responsabilidad de servir como puente o mediador entre los mensajes entrantes y salientes desde y hacia el servidor, es decir, se encarga de retransmitir las solicitudes de conexión, autenticación de usuarios y en general toda la información necesaria para el usuario.

**NASREQ:** es una aplicación de Diameter que proporciona los servicios de la AAA para marcar en los usuarios de productos fitosanitarios y es la próxima generación de reemplazo para el protocolo de Radius.

**NIC:** tarjeta de red permite la comunicación entre diferentes aparatos conectados entre si y también permite compartir recursos entre dos o más equipos (discos duros, CD-ROM, impresoras, etc.). A las tarjetas de red también se les llama adaptador de red o NIC (Network Interface Card, Tarjeta de Interfaz de Red en español).

**Nodo**: Punto de intersección o unión de varios elementos que confluyen en el mismo lugar. En una red de ordenadores cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

**PAP:** son las siglas de Password Authentication Protocol un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet. PAP es un subprotocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o password en ASCII

sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

**PDP:** (Policy Decisión Point, PDP): es el responsable de obtener las políticas de las bases de datos de políticas y generar las decisiones acordes con las peticiones de los PEP. La información intercambiada entre el PEP y el PDP se realiza utilizando COPS (Common Object Policy Service Protocol).

**PEP:** (Policy Enforcement Point, PEP): es una entidad donde las políticas son aplicadas.

**PKI:** Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas. El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública. La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

**PPP:** Point to Point Protocol. Protocolo de punto a punto, que se utiliza para la conexión de ordenadores al Internet a través de líneas de teléfono. El protocolo PPP permite establecer una comunicación a nivel de enlace entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA). Además del simple transporte de datos, PPP facilita dos funciones importantes:

- Autenticación. Generalmente mediante una clave de acceso.
- Asignación dinámica de IP. Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones. Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

**QoS:** Quality Of Service. Calidad de servicio. Medida de desempeño para un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

**RAS: Servicios de acceso remoto (RAS)** se refiere a cualquier combinación de hardware y software para permitir el acceso remoto a las herramientas o la información que normalmente residen en una red de dispositivos de TI. Acuñado originalmente por Microsoft para referirse a su incorporada en NT herramientas de acceso remoto, RAS es un servicio proporcionado por Windows NT que permite a la mayoría de los servicios que estarán disponibles en una red para tener acceso a más de un modem de enlace. El servicio incluye soporte para acceso telefónico y de inicio de sesión.

**RC4:(Stream Cipher 4)** es el sistema de cifrado de flujo más utilizado y se usa en algunos de los protocolos más populares como TLS para proteger el trafico de internet y WEP para añadir seguridad en las redes inalámbricas. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común. El RC4 tiene una clave de 2048 bits, lo que hace que el algoritmo sea rápido y seguro. Crea bytes aleatorios a partir de la clave y hace la operación XOR byte a byte con el archivo a cifrar.

**RFC**: Documento Request For Comments (abreviado como RFC), que se traduce como "petición de comentarios", es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet , que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

**Roaming:** (en español itinerancia) es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra. Roaming es una palabra del idioma inglés que significa vagar o rondar. El término más adecuado en castellano es "itinerancia".
El concepto de roaming o itinerancia, cuando es utilizado en las redes Wi-Fi, significa que el dispositivo Wi-Fi cliente puede desplazarse e ir registrándose en diferentes bases o puntos de acceso.
En telefonía móvil, la itinerancia (el roaming) es la capacidad de hacer y recibir llamadas en redes móviles fuera del área de servicio local de su compañía; es decir, dentro de la zona de servicio de otra empresa del mismo país, o bien durante una estancia en otro país diferente, con la red de una empresa extranjera.

**SCTP:** Stream Control Transmission Protocol (SCTP) es un protocolo de comunicación de capa de transporte que fue definido por el grupo SIGTRAN de IETF en el año 2000. El protocolo está especificado en la RFC 2960, y la RFC 3286 brinda una introducción al mismo. SCTP es una alternativa a los protocolos de transporte TCP y UDP pues provee confiabilidad, control de flujo y secuenciación como TCP. Sin embargo, SCTP opcionalmente permite el envío de mensajes fuera de orden y a diferencia de TCP, SCTP es un protocolo orientado al mensaje (similar al envío de datagramas UDP).

Las ventajas de SCTP son:

- Capacidad de Multihoming, en la cual uno (o dos) de los extremos de una asociación (conexión) pueden tener más de una dirección IP. Esto permite reaccionar en forma transparente ante fallos en la red.
- Entrega de los datos en trozos que forman parte de flujos independientes y paralelos eliminando así el problema de head of the line blocking que sufre TCP
- Es capaz de seleccionar y monitorizar caminos, seleccionando un camino "primario" y verificando constantemente la conectividad de cada uno de los caminos alternativos.
- Mecanismos de validación y asentimiento como protección ante ataques por inundación, proveyendo notificación de trozos de datos duplicados o perdidos.

**SMS:** El servicio de mensajes cortos o SMS (Short Message Service) es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos (también conocidos como mensajes de texto, o más coloquialmente, textos o mensajitos) entre teléfonos móviles, teléfonos fijos y otros dispositivos de mano. SMS fue diseñado originariamente como parte del estándar de telefonía móvil digital GSM, pero en la actualidad está disponible en una amplia variedad de redes, incluyendo las redes 3G.

**T1**: Dentro de las líneas alquiladas T1 es el servicio de línea digital normalizado. Se originó de una necesidad de más ancho de banda que el originado por redes de conmutación de paquetes como X.25. ! Velocidad de trasmisión de 1,544Mbps. ! Las líneas T1 pueden transportar voz y datos mediante el uso de dispositivos multiplexores! Puede proporcionar 24 canales de voz o datos en un ancho de banda de 64Kbps (T1 fraccional) de los cuales el cliente puede elegir el nº de canales que le conviene alquilar. ! Una de las desventajas más señalables de T1 es que el ancho de banda es fijado, lo cual no se acomoda a las ráfagas de tráfico de las LAN-s.

**TCP:** Protocolo de Control de Transmisión (Transmission Control Protocol) es uno de los protocolos fundamentales en Internet. Utilizado dentro de una red de datos compuesta por ordenadores para crear conexiones entre ellos a través de las cuales enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través de los puertos.

**TKIP**: (Temporal Key Integrity Protocol) es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente.

**TLS: Transport Layer Security**. Protocolo de comunicación de datos desarrollado para transmitir documentos privados a través del Internet. Es un protocolo criptográfico que proporciona un canal de comunicación seguro por una red, comúnmente Internet.

**UDP: User Datagram Protocol (UDP)** es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

**UMTS:** Universal Mobile Telecomunications System o Sistema Móvil de Telecomunicaciones Universal. Esta tecnología usa multiplexión por división en frecuencia por los móviles de tercera generación, sucesores de GSM, diseñada para introducir más usuarios a la red (mejora en eficiencia) y obtener una alta tasa de envío de datos a dispositivos móviles.

**WAP** (del inglés: Wireless Application Protocol; Estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas).

**WPA2:** (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA.WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de

"migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

**WEP: (Wired Equivalent Privacy, Privacidad Equivalente al Cable)** es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.
**Wi-Fi:** es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables.

**WiMax:** son las siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas). Es una norma de transmisión de datos usando ondas de radio. Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local. que permite la recepción de datos por microondas y retransmisión por ondas de radio. El protocolo que caracteriza esta tecnología es el IEEE 802.16. Se presenta como muy adecuada para dar servicios de banda ancha en zonas donde el despliegue de cobre, cable o fibra por la baja densidad de población presenta unos costes por usuario muy elevados (zonas rurales).

**WLAN**: (en inglés Wireless Local Area Network) es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

**802.1x**: estándar de autenticación se usa para gestionar el proceso de autenticación en protocolos de comunicaciones, así como la gestión y reparto de claves de cifrado. El 802.1x no es exclusivo de redes inalámbricas.

**802.11i**: nuevo estándar de seguridad inalámbrica. Estándar de seguridad para WLAN, combina el uso de 802.1x y protocolos de cifrado TKIP/CCMP que ofrece autenticación de usuario (no de dispositivo), confiabilidad e integridad de los datos WPA2 (Wi-Fi Protected Access 2).