INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

SEMINARIO DE TITULACION
"SEGURIDAD DE LA INFORMACIÓN"

TESINA

"IMPLEMENTACIÓN DE UN SERVIDOR RADIUS"

QUE PRESENTAN PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

EFRAÍN CEJA GARCÍA.

Asesores:

DR. GABRIEL SANCHEZ PÉREZ.

ING. ARTURO DE LA CRUZ TELLEZ.

VIGENCIA: DES/ESIME-CUL-2008/23/3/10

México, D.F. Octubre 2012

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

POR LA OPCIÓN DE TITULACIÓN SEMINARIO EN SEGURIDAD DE LA INFORMACIÓN

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN.

DEBERÁN DESARROLLAR:

CEJA GARCÍA EFRAÍN.

"IMPLEMENTACIÓN DE UN SERVIDOR RADIUS."

INTRODUCCIÓN.

LA IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA ACCESO A USUARIOS POR MEDIO DE UN SERVIDOR BASADO EN RADIUS, EN UNA RED LOCAL EN LA CUAL SOLO MEDIANTE AUTENTICACIÓN SE PUEDE ACCEDER DE MANERA SEGURA A LA RED, EN BASE A LOS PROTOCOLOS PAP Y CHAP LA AUTENTICACIÓN DE LOS USUARIOS SERA CONFIABLE.

CAPITULADO

I. INTRODUCCIÓN AL SERVIDOR.
II. FORMATO DE ENVÍO DE PAQUETES.
III. IMPLEMENTACIÓN.

México D.F. Octubre 2012

VIGENCIA: DES/ESIME-CUL-2008/23/3/10

DR. GABRIEL SÁNCHEZ PÉREZ
Coordinador del Seminario.

ING. ARTURO DE LA CRUZ TELLEZ
Asesor del Seminario.

DR. JOSÉ VELAZQUEZ LOPEZ
Jefe de la Carrera de I.C.

Agradecimientos.

Agradezco a Dios.

Agradezco a Jesús mi salvador porque sin Él nunca hubiera terminado la carrera, pues en los momentos más difíciles y en mis angustias, solo recordarle me hizo ponerme en pie. “Él vive y yo gracias a Él”.

Agradezco a mi Madre.

Quién mas me podría ayudar mi único amparo y mi fortaleza durante toda mi vida. Madre y aun Más, quien como tu que me cargaste por nueve meses y nunca me reprochaste nada.

Agradezco a mi Padre.

Porque siempre estas en mis sueños, para ti este gran esfuerzo.
Te agradezco, por tu visión y tu valentía, Gracias Papá.

Agradezco a mi Familia.

Sin su apoyo nunca hubiera logrado nada y por la memoria de los que fallecieron; Gracias por su apoyo y su amor incondicional, por que aun en sus últimos días me indicaron el camino y guardaron mi vida, para siempre, ¡Gloria a Cristo! por que ahora están en su presencia.

Agradezco a mis amigos.

Porque estuvieron conmigo y en las buenas y en las malas. Gracias por alentarme, les recordare con siempre con cariño.

La libertad de un individuo termina,

Cuando empieza la libertad de otros individuos.

ÍNDICE

Introducción. Pag. 1.

Planteamiento del Problema. Pag. 2.

Objetivo. Pag. 2.

Objetivos Específicos. Pag. 3.

Justificación. Pag. 4.

Capítulo 1 Introducción al Servidor.

1.1 Introducción a RADIUS. Pag. 5.

1.2 ¿Qué es RADIUS?. Pag. 5.

1.3 El Protocolo RADIUS. Pag. 6.

1.4 Proxy RADIUS. Pag. 7.

1.5 Modelo Cliente Servidor RADIUS. Pag. 9.

1.6 Red de Seguridad RADIUS. Pag. 9.

1.7 Sesión RADIUS. Pag. 9.

1.8 Desechamiento RADIUS. Pag. 10.

1.9 Autenticación. Pag. 10.

1.10 Autorización. Pag. 11.

1.11 Arqueo. Pag. 12.

1.12 Métodos de Autenticación. Pag. 14.

1.13 Funcionamiento del RADIUS. Pag. 18.

1.14 Respuesta por Desafío CHAP. Pag. 19.

1.15 Funcionamiento con los Protocolos PAP y CHAP. Pag. 20.

1.16 Funcionamiento de la comunicación en los servidores RADIUS. Pag. 22.

1.17 Retransmisión. Pag. 24.

Capítulo 2 Formato de Envío de Paquetes.

2.1 Encapsulado. Pag. 26.

2.2 Códigos. Pag. 27.

2.3 Identificador. Pag. 27.

2.4 Longitud. Pag. 27.

2.5 Autenticador. Pag. 28.

2.6 Respuesta de Autentificación (Response Authentication). Pag. 29.

2.7 Petición de Acceso (Access Request). Pag. 30.

2.8 Aceptación de Acceso (Access Accept). Pag. 32.

2.9 Denegación de Acceso (Access Reject). Pag. 33.

2.10 Desafío de Acceso (Access Challenge). Pag. 34.

2.11 Atributos de Radius. Pag. 36.

2.12 Tipos de Formatos. Pag. 37.

2.13 Nombre de Usuario. Pag. 39.

2.14 Password de Usuario. Pag. 41.

2.15 Password de CHAP. Pag. 42.

2.16 Dirección IP Del NAS. Pag. 43.

2.17 Puerto del NAS. Pag. 44.

Capítulo 3 Implementación.

3.1 RADIUS Multiplataforma. Pag. 45.

3.2 Microsoft IAS. Pag. 46.

3.3 Configurando el Servidor. Pag. 47.

3.4 Instalando el Servidor IAS. Pag. 50.

3.5 Configuración de Puertos en el IAS. Pag. 52.

3.6 Active Directory. Pag. 55.

3.7 Protocolo de Seguridad. Pag. 57.

3.8 Pruebas de Funcionamiento. Pag. 59.

3.9 Software de prueba. Pag. 61.

3.10 Prueba de Implementación del Cliente RADIUS en Wi-Fi. Pag. 62.

Conclusiones. Pag. 65.

Glosario. Pag. 66.

Referencias. Pag. 68.

ÍNDICE DE TABLAS

Tabla 1.1 Formato de paquetes de datos de RADIUS. Pag. 26

Tabla 1.2 Formato de paquetes de datos de Access-Request. Pag. 32.

Tabla 1.3 Formato de paquetes de datos de Access-Accept. Pag. 33.

Tabla 1.4 Formato de paquetes de datos de Access-Reject. Pag. 34.

Tabla 1.5 Formato de paquetes de datos de Access-Challenge. Pag. 36.

Tabla 1.6 Formato de atributos de RADIUS. Pag. 37.

Tabla 1.7 Formato de atributos de Nombre de Usuario. Pag. 40.

Tabla 1.8 Formato de atributos de Password de Usuario. Pag. 42.

Tabla 1.9 Formato de atributos de Password de CHAP. Pag. 43.

Tabla 1.10 Formato de atributos de IP del NAS. Pag. 43.

Tabla 1.11 Formato de atributos del puerto del NAS Pag. 44.

ÍNDICE DE FIGURAS

Figura 1.1 Administre su Servidor. Pag. 47.

Figura 1.2 Configuración Típica. Pag. 48.

Figura 1.3 Nombre de Dominio. Pag. 48.

Figura 1.4 Propiedades de la Configuración. Pag. 49.

Figura 1.5 Servidor Configurado. Pag. 49.

Figura 1.6 Servicios de Red. Pag. 50.

Figura 1.7 IAS. Pag. 51.

Figura 1.8 Instalación del IAS. Pag. 51.

Figura 1.9 Finalización de la Instalación del IAS. Pag. 52.

Figura 1.10 Registro del Servidor. Pag. 53.

Figura 1.11 Asignación de Puertos. Pag. 53.

Figura 1.12 Nombre del Cliente RADIUS. Pag. 54.

Figura 1.13 Asignación del Cliente Compartido. Pag. 55.

Figura 1.14 Registro del Servidor en Active Directory. Pag. 56.

Figura 1.15 Propiedades del Registro de Active Directory. Pag. 57.

Figura 1.16 Selección de Información para la Carga. Pag. 57.

Figura 1.17 Tipo de Autenticación. Pag. 58.

Figura 1.18 Métodos de Autenticación. Pag. 58.

Figura 1.19 Creación de Usuarios Cliente. Pag. 59.

Figura 1.20 Nombre/Dominio de Usuarios Cliente. Pag. 60.

Figura 1.21 Password. Pag. 60.

Figura 1.22 Configuración Completada. Pag. 61.

Figura 1.23 Access – Accept. Pag. 62.

Figura 1.24 Conexión a Red Inalámbrica. Pag. 63.

Figura 1.25 Configuración de Seguridad. Pag. 63.

Figura 1.26 Conexión a Red Inalámbrica Exitosa. Pag. 64.

INTRODUCCIÓN.

Dentro del uso de tecnología y medios tecnológicos que la carrera en Computación permite utilizar esta el uso de hardware y software para la seguridad informática , como lo son las cámaras IP, los lectores de huellas dactilares, así como los protocolos de envío y transferencia de información, se plantea en esta tesina el uso de esta tecnología para la seguridad de la información y en especifico para autenticación de usuarios de una red domestica, que bien puede ser implementada para un café internet y contar con un negocio propio, o para la implementación de un circuito cerrado con cámaras IP.

Para el objetivo que se desea alcanzar se implementara un servidor de autenticación basado en RADIUS (Remote Authentication Dial in User Server), el cual garantiza una conexión segura con los clientes así como un envío de paquetes de datos confiable con los algoritmos de encriptación que ofrece su sistema de cifrado de datos y además de contar con un sistema de identificación con Password o PAP (Password Authentication Protocol).

Su conexión puede ser monitoreada así como se puede contabilizar el tiempo de conexión o sesión, este servidor puede ser encontrado de manera libre en FreeRadius.org o bien puede ser habilitada en un Windows Server bajo el Nombre de IAS (Internet Authentication Server).

PLANTEAMIENTO DEL PROBLEMA.

El tema de esta tesina es la implementación de un sistema de seguridad informática para una red local y solo mediante autenticación se puede acceder de manera segura a la red, desde un punto de vista mas especifico el usuario será autentificado mediante un password y la computadora cliente con el protocolo CHAP (Challenge Handshake Authentication Server) el cual es un protocolo de autenticación por desafío el cual mediante el envío de un texto codificado puede garantizar la interacción con el cliente al servidor.

Se establece entonces como tecnología el servidor Radius el cual ofrece las características necesarias para la seguridad de la conectividad entre el cliente y el servidor.

OBJETIVO.

El objetivo de esta tesina es el poder implementar una red local para autenticar personas y equipos clientes de manera segura; Contar con protocolos de seguridad confiables para poder crear una red que bien podría servir como café internet y tener un negocio propio con herramientas gratuitas o de bajo costo y generar ingresos económicos.

Conocer la tecnología que ofrece la herramienta Radius para poder explotar sus beneficios como servidor de autenticación.

OBJETIVOS ESPECIFICOS.

Autenticación

Es necesario autorizar a los suplicantes para poder concederles el acceso a la red. El cliente debe comunicarse con el NAS (Network Access Server) y este debe de traducir y encaminar los paquetes de datos hacia el servidor y solo si cumple con las características que el servidor tiene en la configuración, concederá el acceso.

Autorización

La autorización debe de permitir el acceso a ciertos servicios que están especificados en el servidor así como los tiempos de sesión.

El primer paso a observar es que el servidor tiene que consultar con la base de datos o el sistema de directorios para confirmar la información proporcionada por el suplicante, y solo así conceder los servicios, y atributos durante la sesión.

JUSTIFICACIÓN.

Radius es una tecnología segura y que puede encontrarse de manera gratuita en FreRadius.org, o bien en el sistema operativo Windows 2003, en ambos caso la seguridad es la misma y su confiabilidad no varia, ya que esta basado en los estándares 2865 y 2866 los cuales describen el funcionamiento del servidor.

El servidor Radius utiliza los protocolos PPP (Point to Point Protocol) para establecimiento de canal seguro punto a punto, el protocolo PAP (Password Authentication Protocol) para autenticación de usuarios mediante password y el protocolo CHAP (Challenge Hand-Shake Access Protocol) de saludo por desafío para establecer una comunicación segura, ya que se basa en el esquema de compartimiento de secreto que es una cadena de datos que es cifrada mediante el algoritmo de cifrado MD5, y así realizar un envío de paquetes seguro.

CAPITULO 1: INTRODUCCION AL SERVIDOR.

1.1 Introducción a RADIUS.

RADIUS son las siglas de Remote Authentication Dial-Up Server, que significa Servidor de Autenticación Remota para sistemas de marcado telefónico a redes.

1.2 ¿Qué es RADIUS?

El RADIUS es un protocolo que cumple con todas las norma del estándar de Autenticación, autorización y arqueo. Esto se debe a que el desarrollo de RADIUS es anterior de AAA y que libremente presto sus códigos y conocimientos al grupo de trabajo que comenzó a diseñarlas bases de AAA. Las personas que formaron los grupos de diseño de RADIUS y AAA fueron en muchos casos las mismas.

AAA son las siglas en ingles de Authentication + Authorization + Accounting, que en castellano se traduce como Autenticación + Autorización + Arqueo. Los tres conceptos nos permiten crear un sistema de gestión completa de usuarios que controle todos los aspectos relativos a su identificación, gestión de recursos o servicios permitidos para su uso y gestión de reportes y estadísticas para el control de su autorización.

Antes de la existencia de este estándar, la autenticación era un proceso independiente al igual que la autorización y el arqueo, para acceder a un servicio concreto, dependiendo del fabricante y del servicio, que había que configurar manualmente en cada uno de los equipos de acceso de los protocolos y las bases de datos de autenticación necesarias. El hecho de estandarizar este proceso facilito la vida de muchos administradores de redes que tenían que hacer grandes

esfuerzos para unificar y administrar sus sistemas. En los primeros años de implementación de internet ya comenzó a ser una importantísima necesidad el encontrar un sistema o protocolo para que los ISP (Internet service Providers) pudieran facilitar y garantizar la entrada a sus clientes

Si agrupamos muchos de estos sistemas basados en autenticación podríamos crear un único tipo de identificación para autenticarnos de forma idéntica en cualquier de los servicios en los que nos hubiéramos previamente registrado. Esto simplificaría la labor del usuario, evitando mantener diferentes tipos de credenciales para todos los sistemas. Pero para que esto no resulte demasiado arriesgado para el usuario debe de tener una gran confianza en las entidades que gestionan sus credenciales y además debe poder tener el control completo sobre la revocación o retirada en cualquier momento.

1.3 El Protocolo RADIUS.

Es un servicio que se ejecuta e una de las múltiples plataformas que permite (Unix GNU/Linux, Windows, Solaris…) y que permanece de forma pasiva a la escucha de solicitudes de autenticación hasta que estas se producen. Para esto utiliza el protocolo UDP y permanece a la escucha en los puertos 1812 o 1645 para la autenticación y 1813 o 1646 para el arqueo. Pero tras la publicación de la RFC 2865 se utiliza por acuerdo 1812 y 1813.

RADIUS esta basado en un modelo cliente-servidor, ya que escucha y espera de forma pasiva las solicitudes de sus clientes a las que responderá de forma

inmediata. En este modelo el cliente es el responsable del envío y de la correcta recepción de las solicitudes de acceso y es el servidor RADIUS el responsable de verificar las credenciales del usuario y de ser correctas, de enviar al NAS (Network Access Server) los parámetros de conexión necesarios para prestar el servicio.

El motivo por el cual RADIUS justifica el uso de UDP (User Datagram Protocol) sobre TCP (Transmission Control Protocol) en su RFC (Request for Comments) es por el aprovechamiento de la normativa del protocolo UDP, que mantiene una copia del paquete de solicitud sobre la capa de transporte a fin de poder recuperarlo para renviarlo, si fuera necesario, a otro servidor RADIUS si la primera no estuviera disponible. De esta manera se simplifica el diseño del protocolo, evitando tener que hacerse cargo del control de llegada de estos paquetes a su destino. Para aprovechar esta simplicidad se utiliza la característica de UDP (User Datagram Protocol) de ser “Stateless” o “Conectionless”. Las retransmisiones se pueden hacer mas rápidamente hacia otros servidores, ya que el puerto no quedara colapsado por el control de la conexión, evitándose las esperas innecesarias en el protocolo TCP (Transfer Control Protocol).

El servidor RADIUS puede actuar como servidor Proxy, canalizando las solicitudes de un cliente hacia otro servidor de autenticación RADIUS, o de otro tipo.

1.4 Proxy RADIUS.

Un servidor Proxy es un servidor que mantiene una memoria cache donde se pueden almacenar direccionamientos para otros servidores, el propósito de los

servidores Proxy es incrementar la disponibilidad y las prestaciones de servicio, reduciendo la carga en redes de área amplia y en servidores web.

Los servidores también pueden acceder a otros servidores a través de los cortafuegos.

Con el Proxy RADIUS un servidor RADIUS recibe una petición del Cliente RADIUS, y renvía la petición a un servidor remoto recibe la respuesta del servidor remoto y la envía al Cliente RADIUS, probablemente con modificaciones en cuanto políticas de la localidad en la que este ubicada el servidor remoto. Una de las utilidades del RADIUS remoto es el Roaming, el Roaming permite a los usuarios contar con la posibilidad de accesar a sus servicios conectándose a distintos servidores de la red.

El NAS (Network Access Server) envía la Petición de acceso al servidor RADIUS remoto el cual reenvia la petición a otro servidor remoto el cual contesta con Access Reject, Access Accept o Access Challenge al servidor remoto y este a su vez manda la respuesta al NAS (Network Access Server). El atributo del nombre de usuario debe tener un identificador de acceso a red para las operaciones del RADIUS Server.

La elección del Servidor que recibirá las peticiones esta basada en su “Realm”(Dominio) autentificación, así también de manera alterna el criterio de los servidores que recibirán la petición reenviada esta dada por los criterios de configuración de recepción, como lo es la Called Station-ID, identificación de la estación requisitada.

El servidor RADIUS puede funcionar como servidor remoto también así como servidor de reenvió de paquetes para otros Dominios, un servidor requisitado

puede funcionar como requisitador para cualquier numero de servidores remotos, un servidor puede recibir las peticiones de cualquier numero de servidores y puede proporcionar autentificación para cualquier numero de dominios. Un servidor requisitado puede requisitar a otros servidores para formar una cadena de Proxy, sin embargo se debe tomar precauciones para evitar problemas de retardos.

1.5 Modelo Cliente Servidor RADIUS.

El cliente es capas de pasar información de los usuarios al servidor RADIUS y luego actuar sobre la respuesta que se recibe.

Los servidores RADIUS se encargan de recibir las peticiones de conexión, y a continuación autentificarlos. El servidor RADIUS puede funcionar como un servidor Proxy para otros servidores.

1.6 Red de seguridad RADIUS.

El trafico seguro que el servidor RADIUS proporciona se dan mediante la implementación de un secreto compartido que no es enviado a través de la red con lo cual se evita el riesgo de que alguien pudiera tener acceso mediante la obtención contraseña de usuario.

1.7 Sesión RADIUS.

Cada servicio proporcionado a los usuarios registrados es considerado una sesión considerando como inicio de esta, el punto donde el servicio es primeramente proporcionado, y el fin de sesión como el punto donde el servicio termina, un

usuario puede tener múltiples sesiones si el NAS (Network Access Server) lo soporta.

1.8 Desechamiento RADIUS.

El Servidor RADIUS puede desechar paquetes de información sin necesidad de un procesamiento, la implementación realiza un descaramiento de paquetes que se consideren de error y lo anexa a un listado de los errores.

1.9 Autenticación.

La autenticación es la base del estándar de Radius, debe de dar un respuesta inequívoca a la pregunta, ¿Quién pretende acceder a los servicios que presta la red? Los primeros sistemas basados en autenticación utilizan una estructura simple de nombre de usuario y contraseña en texto plano, basando todo el sistema en estos dos datos que podrían ser interpretados o robados por una persona. Con el tiempo este sistema fue mejorando mediante el acceso por desafío, en el cual no hay intercambio de contraseñas durante el transporte de la autenticación, sino la encriptación de mensajes por una misma clave y un mismo algoritmo, evitando el transporte de la contraseña, posteriormente se implantan otros métodos como el acceso por equipos telefónicos con identificador, el generador de contraseñas portátil, tarjetas de acceso, sistemas biométricos etc. Hasta llegar a la actualidad, a un sistema basado en certificados.

La autenticación no consiste únicamente en la identificación de personas, sino también de equipos que acceden a una red. Además se pueden autenticar otro tipo de características como las profesiones, los estados civiles, etc. También se

puede gestionar la autenticidad de algún equipo mediante la dirección MAC de la tarjeta de red NIC (Network Interface Controller), de un Router de entrada o de un equipo.

Durante el proceso de autenticación el suplicante habla con el NAS (Network Access Server) y este es quien traduce y encamina los paquetes hacia el servidor de autenticación. De esta manera no existe un camino abierto entre el suplicante y el servidor de autenticación con lo que se garantiza bastante la seguridad del servidor de autenticación contra ataques directos, ya que un atacante tendría que estar en el interior de su infraestructura.

En la fase de autenticación se produce un mensaje inicial de solicitud de acceso desde el NAS (Network Access Server) al servidor de autenticación en forma de:

Access - Request (Solicitud de Acceso). El suplicante envía el nombre de usuario y la contraseña cifrada, si procede hacia el NAS (Network Access Server) este envía entonces al servidor de autenticación el mensaje de Access-Request solicitando además el puerto de acceso para el suplicante.

1.10 Autorización.

La autorización permite acceder al solicitante acceder a ciertos servicios o bien la autorización es el acto de confiar un derecho a un solicitante.

Tras el traspaso de credenciales para la autenticación se produce la consulta del servidor de autenticación a la base de datos de usuario centrándose en la información del usuario que solicita acceso. En los registros relacionados con este usuario, se podrá consultar todo tipo de derechos y deberes relacionados con el.

De esta manera el servidor conocerá detalles como: si el solicitante esta autorizado a acceder a la red en este momento, si le debe asignar una dirección IP correcta, si habrá que configurarle parámetros específicos para su conexión, si deberá concederle un ancho de banda determinado, si debe solicitar otro tipo de credenciales, o simplemente si deberá denegar su acceso. Todas estas reglas son definidas para cada usuario en concreto, para un grupo de usuarios por defecto.

En algunos casos, como en las comunicaciones de dial-up (marcado por Modem) al solicitar el acceso a la red a través de un dispositivo PPP (Point to Point Protocol) o similar, no se produce una solicitud de identidad al suplicante ya que este dato es intrínseco, al puerto de conexión PAE (Post Access Entity) que conoce algún dato como el Caller - Id (Identificador de llamada) o dirección MAC de suplicante.

1.11 Arqueo.

Una vez realizado el proceso de autorización se produce la fase de arqueo o “Accounting”. Esta es iniciada por el Autenticador o NAS (Network Access Server) tras autorizar el acceso al suplicante. El arqueo es la fase estadística y de recolección de datos sobre la conexión. Se produce en forma de contadores o Logs de conexión y se suelen almacenar en bases de datos SQL relacionadas con el usuario o en ficheros tipo L og. Estos datos correctamente manejados y gestionados nos permiten tomar decisiones en cuanto al uso de los recursos por parte de los usuarios, con el fin de denegar conexiones, cambiar los anchos de banda mediante QoS (calidad de Servicio), impedir descargas, etc. La fase de arqueo esta limitada por la capacidad del equipo NAS (Network Access Server) de

registrar información de sesiones. Algunos equipos ni siquiera son capaces de realizar este recuento y de suministrar información alguna de arqueo.

La contabilidad de la conexión permite a los buenos administradores mediante estadística gestionar la futura demanda de crecimiento de sus sistemas para planificar sus ampliaciones. También como debe suceder en los sistemas de seguridad o IDS se deberían generar avisos por intentos reiterados o denegados de conexiones infructuosas para tomar decisiones basadas en la seguridad, si bien la mayor parte de los equipos y servidores no proveen este tipo de información.

Una de las principales motivaciones del arqueo es la economía. Mediante ella se podrá facturar a los usuarios los servicios prestados, bien sea en forma de tiempo o de flujo de datos .Cuando nos conectemos a Internet mediante conexiones móviles (GPRS, UMTS, 3G, Edge…), se nos suele tarificar este servicio por descarga de datos, si no contratamos tarifa plana. Es en el proceso de arqueo donde se acumula la información de nuestras sesiones para posteriormente tarificarlas. De esa manera, el Accounting es el responsable de proporcionar los datos necesarios para enlazar con un sistema de tarificación adecuado, si se precisa de él.

Durante la fase de arqueo se producen los siguientes mensajes:

- ***Accounting – Request [Start]*** (Solicitud de inicio de arqueo). Es una solicitud de inicio enviada desde el equipo NAS (Network Access Server) al servidor para indicar que ha comenzado la fase de arqueo, y se comienza a registrar los datos de la sesión del usuario.

- ***Accounting - Response [Start]*** (Respuesta de asentimiento al inicio de arqueo). El servidor de autenticación responde a la solicitud inicial, registrando la información de inicio y enviando este paquete al NAS (Network Access Server) para mostrar su conformidad.
- ***Accounting – Request [Stop]*** (Solicitud de final de arqueo). El NAS (Network Access Server) comprueba la desconexión del usuario y envía al servidor un mensaje de final de la fase de arqueo con los siguientes datos de la sesión del usuario:

  Delay time (tiempo de intento de envío de este mensaje).
  Input octets (numero de bytes recibidos por el usuario).
  Output octets (numero de bytes enviados por el usuario).
  Sesión time (duración en segundos de la sesión del usuario).
  Input packets (numero de paquetes recibidos por el usuario).
  Output packets (numero de paquetes enviados por el usuario).
  Reason (motivo de la desconexión de la sesión del usuario).

- ***Accounting – Response [Stop]*** (Respuesta de asentimiento al final de arqueo). El servidor tras almacenar la información anterior, envía al NAS (Network Access Server) su conformidad al final de la fase de arqueo, admitiendo haber recibido correctamente toda la información de la sesión.

1.12 Métodos de Autenticación.

Los métodos de autenticación son paquetes de software o módulos de software sobre los que se basa el proceso de autenticación de usuarios. Estos módulos son

realmente complejas cajas matemáticas encargadas de realizar el cifrado, descifrado y empaquetado de todos los procesos complejos de autenticación. Desde el método nativo de RADIUS que es PAP (Password Authentication Protocol) hasta los más actuales como algunos tipos nuevos de EAP (Extensible Authentication Protocol), la evolución en cuanto a seguridad ha sido notable. Cuando RADIUS recibe una solicitud de acceso, va pasándola por cada uno de los módulos de autenticación que tenga activados en su configuración, hasta que alguno de esos módulos reconozca sus algoritmos o las credenciales del usuario y se encargue de validar la autenticación.

- **PAP** (Password Authentication Protocol o Protocolo de autenticación mediante contraseña). Es el sistema mas sencillo de autenticación se basa simplemente en la transmisión del nombre de usuario y de su contraseña en texto plano.
- **CHAP** (Challenge Handshake Authentication Protocol o protocolo de autenticación por desafío) Es un método de tipo de secreto compartido ya que ambos equipos comparte una el conocimiento de una contraseña. El suplicante o usuario conoce su contraseña en texto plano y el servidor también tiene que conocer la contraseña. En el momento de la autenticación el servidor envía una frase aleatoria (Desafío) para que el suplicante la pase junto con su contraseña con una función MD5 y se la reenvia. Al recibirla el servidor que ya conoce su valor calculado, la compara con su resultado recibido y si es correcto permite la entrada de entrada del suplicante a la red. el desafío se puede repetir en varias ocasiones en la sesión del usuario.

- **MS-CHAPv2** Es la primera versión del protocolo CHAP (Challenge Handshake Authentication Protocol) basado en desafío para sistemas Microsoft .Ya no esta incluida en Windows Vista. La mejora de MS-CHAP sobre CHAP (Challenge Handshake Authentication Protocol) es que ni el servidor ni el cliente deben de almacenar la contraseña de usuario en texto plano, ya que al procesar el desafío por parte del cliente como por parte del servidor ambos utilizan el valor hash de la contraseña y no la contraseña en si.
- **MS-CHAPv2** Es la versión actual de CHAP (Challenge Handshake Authentication Protocol) de Microsoft, que tiene soporte en todos sus SO desde Windows 2000 y que es incompatible con la v1. Permite soporte para cambios de contraseña y mensajes de respuesta con estados.

  En Unix se puede utilizar simplemente los nombres de usuarios y contraseñas existentes en un sistema Unix/Linux que se encuentran almacenados en el directorio /etc de Unix en el fichero passwd o mediante la función shadow.
- **HTTP Digest** es también un protocolo de autenticación por desafío para clientes de servidores web con autenticación RADIUS; para evitar los ataques de repetición usa también frases pre computadas única .También utiliza MD5 como algoritmo aunque maneja otros como SHA-1.
- **EAP-MD5** Es un método simple e inseguro de autenticación que utiliza el algoritmo MD5 para calcular el hash de una contraseña. Este protocolo es fácilmente violable ya que todo el proceso circula en texto plano. Se puede

capturar el Hash y forzarlo off-line, por lo que es vulnerable sino se utiliza algún tipo de tunelamiento de las comunicaciones.

- **EAP-OTC** (One Time Password). Es un método similar a MD5 pero basado en un sistema portátil de generación de claves instantáneas. Las opciones capaces de generar la contraseña de un solo uso son programas de software, llaveros con algoritmos programados, PDA con software apropiado, etc.
- **EAP-GTC** (Generic Token Card). Es un sistema simple para el uso de algunas tarjetas smartcard (criptográficas) sobre protocolo EAP. Requiere que el usuario teclee su PIN para finalizar la autenticación.
- **EAP-MS-CHAP** Es la aplicación de la versión 1 del protocolo CHAP (Challenge Handshake Authentication Protocol) de Microsoft transportado por EAP (Extensible Authentication Protocol), que es la versión Microsoft del sistema de desafío o Challenge de contraseña , Es vulnerable si nó lleva cifrado o tunelamiento de las comunicaciones.
- **EAP-MS-CHAPv2** Version 2 del protocolo MS-CHAP.
- **EAP-SIM** Versión de EAP (Extensible Authentication Protocol) para Authentication de los equipos de telefonía móvil GSM mediante tarjeta SIM, aunque también se puede utilizar como método de autenticación mediante el lector de tarjetas SIM.
- **EAP- AKA** (Authentication and Key Agreement). Autenticación y aceptación de clave. Utilizada en servicios UMTS (Universal Mobile Telecommucations System), se basa en el uso de la criptografía simétrica para canalizar la

autenticación y la distribución de claves de sesión. Proporciona privacidad de usuario y mecanismos de reconexión rápida.

- **EAP- LEAP** Protocolo propietario de Cisco que es muy similar a EAP-MD5 pero utilizando un sistema de rotación dinámica de claves.
- **EAP- FAST** Protocolo propietario de Cisco que pretende sustituir LEAP (Lightweight Extensible Authentication Protocol) por sus vulnerabilidades , tunelando el transporte de la autenticación sin el uso de certificados mediante el sistema PAC que genera en el servidor una clave única por usuario que será distribuida a la creación del usuario de manera manual o automática.
- **Biometría** Se considera ossistemas de seguridad que utilizan las características del cuerpo humano como, la huella dactilar, el iris, la voz, etc.

1.13 Funcionamiento del RADIUS.

Cuando un cliente es configurado para usar RADIUS cualquier usuario del cliente presenta información de identificación, esto es en el Prompt de login, un nombre de usuario y una contraseña, de manera complementaria el usuario proporcionara un enlace de entrada de protocolo con el cual identificara los paquetes de datos como lo es el protocolo PPP (Point to Point Protocol).

El cliente realizara una autentificación utilizando el Servidor RADIUS realizara una petición de acceso “Access Request” el cual contendrá atributos como nombre de

usuario, password, canal de enlace o puerto en donde el usuario esta accesando, cuando el password es ingresado se encripta utilizando el algoritmo de RSA: MD5.

La petición de acceso es enviada al servidor RADIUS si esta no es confirmada se regresa con el tiempo de espera, esta petición es enviada un numero de veces, el cliente puede reenviar esta petición a otros servidores, en la fase en que el primer servidor es inaccesible, un servidor alternativo puede ser utilizado, en el caso que el servidor no esté funcionando.

Una vez que el RADIUS procesa la Petición de enlace, valida el cliente que envió la petición, un cliente que al inscribirse no comparte el secreto es descartado, si el cliente es aceptado el RADIUS busca el usuario en una base de datos para encontrar al usuario que coincida con la petición de acceso cliente “Access Request” , la base de datos contiene información de usuario que permite el poder establecer al conexión con el usuario, así .como lo es el password, pero también contiene especificaciones como lo son el puerto de conexión en el cual se le perimirte al cliente conectarse.

El RADIUS puede realizar una búsqueda de servidores para poder satisfacer una petición del cliente.

Si ninguna condición de conexión se cumple, el Servidor RADIUS envía una señal de rechazo conocida .como “Access Reject”. En el caso de que todos los atributos del “Access Request” se encuentren completados y exista un reconocimiento por parte de el RADIUS, se puede realizar un saludo por desafío en el cual el usuario debe de responder con una saludo, el cliente envía otra petición de acceso

"Access Request" con un ID diferente, con el atributo del Password remplazado con la respuesta del usuario encriptada dependiendo de la respuesta puede contestar con un Petición de acceso "Access Accept", acceso denegado "Access Reject", o bien con Otro desafío.

1.14 Respuesta por Desafío (CHAP).

En una autentificación por Respuesta por Desafío se le da a un usuario un numero al asar a encriptar, el usuario devuelve el mensaje con el numero encriptado.

La autentificación de Respuesta por desafío por lo general contiene un mensaje escrito incluyendo un reto a ser mostrado, como un número aleatorio, que normalmente es un número obtenido por un servidor externo que conoce normalmente el tipo de autentificación que posee el usuario.

El usuario con esto realiza el cálculo de la respuesta, esta es mandada al cliente y este la reenvia al Servidor RADIUS con una segunda Access Request, si la respuesta coincide con la respuesta esperada el servidor RADIUS contesta con un Access Accept.

Ejemplo:

El NAS envía un Access Request al servidor RADIUS con un NA-identificador, NAS port, user-Name, user-Password el cual debe de ser enviado como reto , el servidor responde con otro reto con un mensaje de reto para que uno ingrese una respuesta en el Prompt el NAS manda un nuevo Access Request al servidor con un nuevo ID, con NAS Identificador, NAS Port, User Name, User Password (La

respuesta del usuario encriptada), y el mismo atributo de estado que se recibió con el Access Challenge, el servidor manda de respuesta un Access Accept, o un Access Reject o bien puede responder con otro reto.

1.15 Funcionamiento con los protocolos PAP y CHAP.

Para el PAP el NAS toma el PAP (Password Authentication Protocol) ID y el Password y los envía empaquetados en una petición de acceso al RADIUS Access Request, el NAS (Network Athentication Server) también incluye atributos del tipo de servicio Framed user, Framed Protocol, esto como dato del tipo de servicio que se espera.

Para el CHAP (Challenge Handshake Authentication Protocol) el NAS (Network Authentication Server) genera un reto aleatorio de 16 octetos (preferentemente) al usuario quien responde al reto con un CHAP (Challenge Handshake Authentication Protocol) ID, y un CHAP (Challenge Handshake Authentication Protocol) User Uame, el NAS (Network Authentication Server) manda una petición de acceso al RADIUS Access Request con los atributos mencionados y el CHAP (Challenge Handshake Authentication Protocol) response se encripta como password, el reto aleatorio puede ser enviado en el desafío, o si son 16 octetos puede ser enviado a un autentificador de petición del Access Request Packets, el NAS puede incluir atributos de servicio como lo son el Framed User y Framed Protocol, Service-Type = Framed User, Framed –Protocol=PPP (Point to Point Protocol) , como datos que el servidor debe tomar en cuenta para proporcionar el

servicio requerido. El servidor RADIUS Toma el Password basado en el usuario, encripta el mensaje utilizando el algoritmo MD5 en el octeto del CHAP (Challenge Handshake Authentication Protocol) ID, si el password y el usuario coinciden el RADIUS envía la aceptación de acceso Access Accept. Si el RADIUS no puede identificar la petición, el Servidor envía un Access Reject, por ejemplo si el protocolo CHAP (Challenge Handshake Authentication Protocol) solicita que el usuario tenga su Password en texto normal (Plano) el desafío no se puede realizar, por no poder llevar a cabo la encriptación y compararla con la respuesta del CHAP (Challenge Handshake Authentication Protocol). Si el password no esta disponible para el servidor, entonces se envía una señal de Rechazo Access Reject.

1.16 Funcionamiento de la comunicación en los servidores RADIUS.

- El NAS (Network Access Server) envía un Access Request al servidor Proxy.
- El servidor Proxy en vía la petición a un servidor remoto.
- El servidor remoto regresa una respuesta al servidor Proxy, la respuesta puede ser Access Accept, Access Reject o bien un Access Challenge, para el caso de un Access Accept.
- En contestación el servidor Proxy le contesta un Access Accept al NAS (Network Access Server).

El servidor de reenvió debe de tomar en cuenta atributos del Proxy State que ya hallan pasado, el renvío de los paquetes no depende de los atributos de el Proxy-State adheridos de un Proxy anterior. Si se encuentran algunos atributos en la petición recibida de el cliente el servidor de renvío debe incluir estos atributos en la contestación al cliente, el servidor de renvío debe incluir estos atributos en el Access Request cuando reenvia la petición, o se podrían monitorear estos atributos cuanto el servidor de renvío los omite en la petición, aunque estos se deben de adjuntar al Response (Respuesta) antes de mandarlo al cliente.

El NAS (Network Access Server) envía una petición al servidor de reenvió, el servidor de reenvió desencripta el password de usuario si coincide el secreto que posee el NAS. Si existe algún atributo del CHAP password pero no hay ningún atributo del CHAP (Challenge Handshake Authentication Protocol) - challege, el servidor de renvío debe abandonar el Autentificador de Desafío o copiarla a algún atributo del CHAP (Challenge Handshake Authentication Protocol) challege.

El servidor de reenvió debe adherir algún atributo al paquete (No debe adherir mas de uno), si anexa un estado al Proxy el estado se debe encolar después de los demás estados del Proxy. Los estados del Proxy no deben ser modificados pero puede no enviarlos, el servidor de renvío no debe alterar el orden de los atributos del mismo tipo, incluyendo los estados.

El servidor de renvío encripta los password’s de usuario si presentan el secreto que comparten con el servidor remoto, envía el identificador como Needed, y renvía el Access Request, al servidor remoto.

El servidor remoto verifica que el usuario este utilizando el User-Password y el CHAP-Password, o tal método es reservado como futura extensión, entonces el servidor contesta con un Access Accept, Access Reject, o bien un Access Challenge de regreso al servidor de reenvió en este ejemplo se toma como asentado un Access Accept el servidor de reenvió debe copiar todos los estados del Proxy y solo los estados del Proxy , y enviarlos en orden desde el Access Request hasta el paquete de respuesta sin modificación alguna.

El servidor de reenvió verifica la respuesta con el autentificador de respuesta(Response Authenticator), usando el secreto que comparte con el servidor remoto, si la autentificación con el servidor remoto falla el servidor de reenvió descarta el paquete, si el servidor acepta la verificación como autentica , el servidor de reenvió elimina el ultimo estado del proxy y añade uno, firma la respuesta de autenticación utilizando el secreto que comparte con el NAS (Network Access Server), restablece el identificador para coincidir con la petición original del NAS, y la reenvía en respuesta de aceptación al NAS (Network Access Server) un Access Accept.

Un servidor de reenvió debe modificar los atributos para reforzar la política local, un servidor de reenvió, no debe modificar los estado existentes del Proxy - State, o los atributos de clase en el paquete.

1.17 Retransmisión.

Si el servidor RADIUS y algún Servidor RADIUS alterno comparten el mismo secreto, esta bien retransmitir el paquete de datos a otro servidor RADIUS con el

mismo ID, y el mismo identificador de peticiones, porque el contenido de los atributos no han cambiado. Si se quiere utilizar algún otro identificador de peticiones entonces se debe:

Si usted cambio los atributos de Usuario-Password (o cualquier otro atributo), usted podría necesitar algún otro nuevo identificador de peticiones, así como también otra nueva ID.

Si el NAS (Network Access Server) esta retransmitiendo al RADIUS una petición al mismo servidor pero en un tiempo posterior, y los atributos no han cambiado tiene que utilizar el mismo identificador de petición. Pero si algún atributo cambio entonces debe de usar algún otro identificador de peticiones y un nuevo ID.

El NAS (Network Access Server) puede utilizar el mismo ID en todos los servidores, o bien puede utilizar tramos de la Id por todos los servidores esto mediante una implementación.

CAPITULO 2: FORMATO DE ENVÍO DE PAQUETES.

2.1 Encapsulado.

Exactamente un paquete de datos es encapsulado en el campo de Datos de una UDP, donde el puerto para el envío de paquetes de Datos es el 1812.

Cuando una respuesta es generada, el destino y el destinatario son reservados.

Esto documenta el protocolo de RADIUS, en los principios de la implementación del RADIUS se utilizaba el puerto 1645, sin embargo tenia conflictos el servicio con la data métrica(Tamaño de envió de datos). Entonces el Puerto oficialmente asignado fue el 1812.

El formato de Datos se muestra abajo.

Los campos se transmiten de izquierda a derecha.

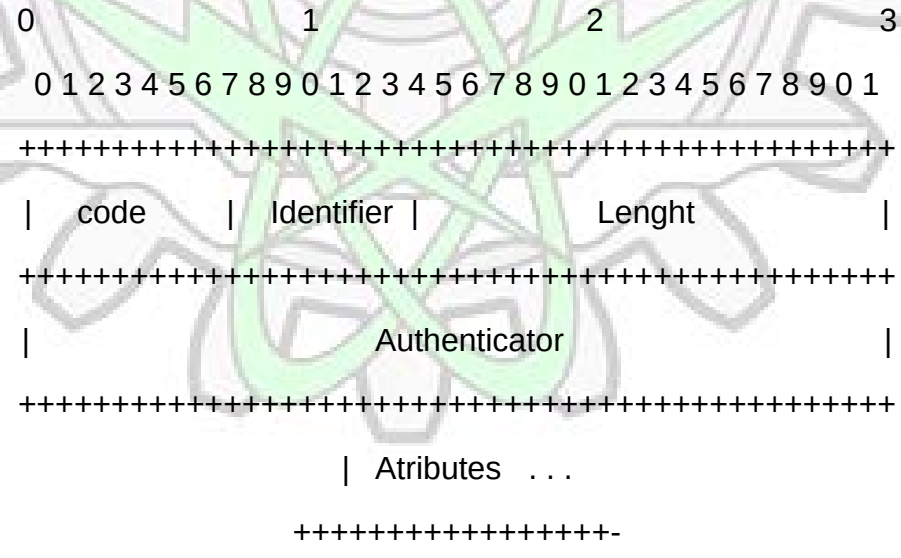

Tabla 1.1 Formato de paquetes de datos de RADIUS.

2.2 Códigos.

El campo de código es de un solo octeto y define el tipo de paquete.

Los códigos de RADIUS son asignados como sigue:

1	Access-Request.
2	Access-Accept.
3	Access-Reject.
4	Accounting-Request.
5	Accounting-Response.
11	Access-Challenge.
12	Status-Server (experimental).
13	Status-Client (experimental).
255	Reserved.

2.3 Identificador.

El campo de identificador es un octeto, y anexa peticiones y repuestas que concuerden, El servidor RADIUS puede duplicar peticiones si tienen el mismo cliente la misma dirección IP, el mismo puerto UDP (User Datagram Protocol) y un identificador con el mimo tiempo.

2.4 Longitud.

La longitud es de dos octetos, e indica la longitud del paquete incluyendo el código, identificador, longitud, autenticador y los campos de atributo. Los

atributos fuera de rango en el octeto de longitud son ignorados, si el paquete que se envía es menor el paquete también se descarta, el tamaño mínimo de longitud de paquete es de 20 y el máximo es de 4096.

2.5 Autenticador.

El campo de autentificación es de 16 octetos, el octeto mas significativo es el primero, este valor es usado para autentificar la respuesta del servidor RADIUS, y es usado para algoritmos de ocultamiento de password.

Petición de Autenticación

En los paquetes de autenticación el tamaño es de 16 octetos de tipo aleatorio, llamada petición de autenticación, el valor debe de ser aleatorio y único durante el periodo de vida de un secreto (el password compartido entre el cliente y el servidor), desde la repetición del valor de petición junto con el secreto permite a los atacantes responder con una respuesta interceptada anteriormente. Desde que se espera que el mismo secreto sea utilizado para identificarse en regiones remotas la petición de autenticación debe de mostrar características únicas globales y temporales.

El valor de la petición de autenticación en el paquete de la petición de acceso debe de ser también impredecible, imaginemos que un atacante engaña a un servidor en una petición, y utiliza la mascara de respuesta como una futura entrada al servidor.

Sin embargo protocolos como el RADIUS son incapaces de defender ante robos o sesiones en tiempo real, la generación de peticiones únicas e impredecibles puede ayudar a prevenir ataques contra la autentificación.

El NAS (Network Access Server) y el servidor RADIUS comparten un secreto. Ese secreto compartido junto con la petición de autentificación se pone en un hash para formar un paquete de envio con encriptación md5, que forman un octeto de 16 bits que es enviado junto con el password ingresado por el usuario.y el resultado adjuntado.

En el atributo de Usuario-Password en el paquete de petición de acceso.se puede observar la entrada de password de usuario en la sección de atributos.

2.6 Respuesta de Autenticación (Response Authentication).

El valor del campo de autentificación en el paquete de aceptación de acceso (Access Accept), denegación de acceso(Access Reject) o el desafío de acceso (Access Challenge), es llamado la respuesta de autentificación, y contiene un arreglo Hash de MD5 en una sola via. que es calculado por medio de la cadena de octetos conformada por: El paquete de RADIUS empezando por el campo de código, incluyendo el identificador, la longitud la petición de autentificación del paquete de la petición de acceso, y los atributos de respuesta, seguido por los atributos de respuesta, seguidos por el secreto compartido, se muestra a continuación la cadena Respuesta de

Autentificación = MD5(Code + Id + Petición de Autentificación + Atributos + Secreto).

El secreto (Password compartido entre el cliente y el servidor RADIUS), debe de ser tan largo e impredecible como cualquier password bien elegido.es preferible que el password sea de 16 octetos. La longitud debe de ser lo suficientemente largo para asegurar la integridad del password contra posibles ataques constantes. Él secreto no puede ser de longitud cero, pues esto podría derivar en olvidar paquetes.

El servidor RADIUS debe de usar la dirección IP del paquete UDP de RADIUS, para decidir que secreto de RADIUS utilizar para que la petición del RADIUS pueda ser enviada a un proxy.

Cuando se esta renviando paquetes a un proxy, el proxy debe de ser capas de alterar los paquetes para cada estado de la trama de envío. Cuando el Proxy renvía cada paquete, debe de remover el atributo de estado, y modificarlo por otro. El estado de proxy siempre se puede realizar esta opción mediante la subscripción de esta en una lista de atributos. Como la respuesta de “Aceptación de petición” y de “Denegación de petición” son autentificados en el contenido del paquete el armado del atributo del estado del proxy invalida la inscripción del paquete, y por este motivo el proxy debe de rescribirlo.

2.7 Petición de Acceso (Access Request).

La petición de Acceso es enviado al servidor RADIUS, y la información enviada es determinada para determinar si el usuario esta habilitado para accesar a algún NAS especifico, y algún servicio en especifico.

Una implementación esperando identificar a un usuario debe de mandar un paquete RADIUS con un campo de código puesto a uno (Access Request).

A pesar de que la petición de acceso provenga de un usuario valido, una respuesta adecuada debe de ser enviada.

Una petición de acceso debe de ser enviada con las siguientes características el atributo de nombre de usuario, debe de tener el atributo de dirección ip del NAS (Network Access Server), y el atributo del identificador de NAS.

La petición de acceso de be de tener un Password de usuario un CHAP (Challenge Handshake Authentication Server) password, es importante notar que la petición de acceso no debe de tener los dos passwords, el de usuario y el de CHAP (Challenge Handshake Authentication Protocol). si futuras extensiones permiten el ingreso de otra información de identificación, el atributo de esta puede ser utilizada en la petición de acceso en lugar del password de usuario o del CHAP (Challenge Handshake Authentication Protocol) password.

Una petición de acceso debe de tener un puerto NAS (Network Access Server), o el atributo del tipo de puerto del NAS (Network Access Server), o los dos amenos que el tipo de acceso no involucre un puerto, o el NAS no haga diferencia en los puertos.

Una petición de acceso debe de contener atributos adicionales para ayudar al servidor, aunque el servidor podría no tenerlos en primer plano.

Cuando un password de usuario es presentado, es ocultado utilizando un algoritmo de encriptación llamado MD5.

El formato de la Petición de Acceso se muestra a continuación. Los campos se transmiten de izquierda a derecha.

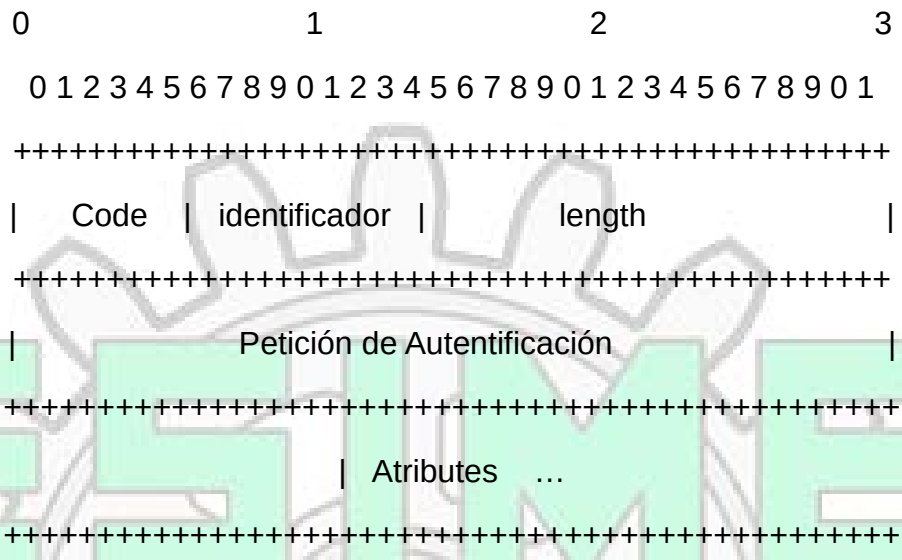

Tabla 1.2 Formato de paquetes de datos de Access-Request.

Código 1 Para Access-Request.

2.8 Aceptación de Acceso (Access Accept).

El paquete de aceptación son enviadas por el servidor RADIUS, y contiene las especificaciones de configuración necesarios para brindar el servicio al usuario. Si todos los atributos recibidos en la petición de acceso son validos entonces la implementación del servidor RADIUS enviara paquetes de de datos con el estado de código puesto en 2 es decir Aceptación de acceso (Access Accept).

En la recepción de la aceptación de acceso, el campo de identificador esta marcado con una petición de acceso pendiente. La repuesta de autenticación debe tener la respuesta correcta para la petición de acceso, delo contrario son desechadas.

Un sumario de la aceptación de acceso es mostrado en la parte inferior. Los campos son transmitidos de izquierda a Derecha.

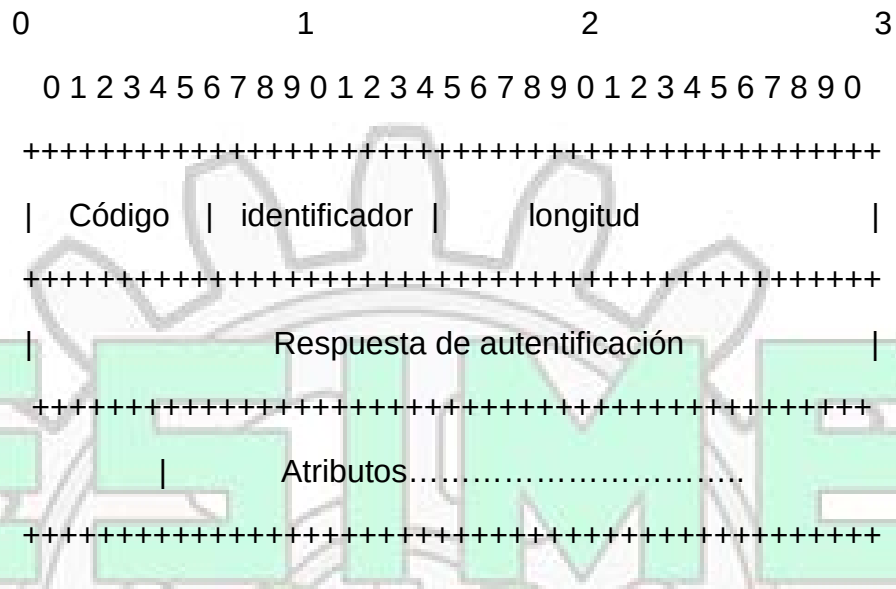

Tabla 1.3 Formato de paquetes de datos de Access-Accept.

Código 2 Para Access Accept.

2.9 Denegación de Acceso (Access Reject.).

Si cualquier atributo recibido no fuera aceptados entonces el servidor RADIUS mandara un paquete con el campo de código puesto a 3 (Denegación de Acceso). Y podría incluir uno o mas mensajes de texto para el NAS (Network Access Server), para poder mostrar al usuario.

Un formato de la Denegación de Acceso se muestra en la parte inferior. Los campos se transmiten de izquierda a derecha.

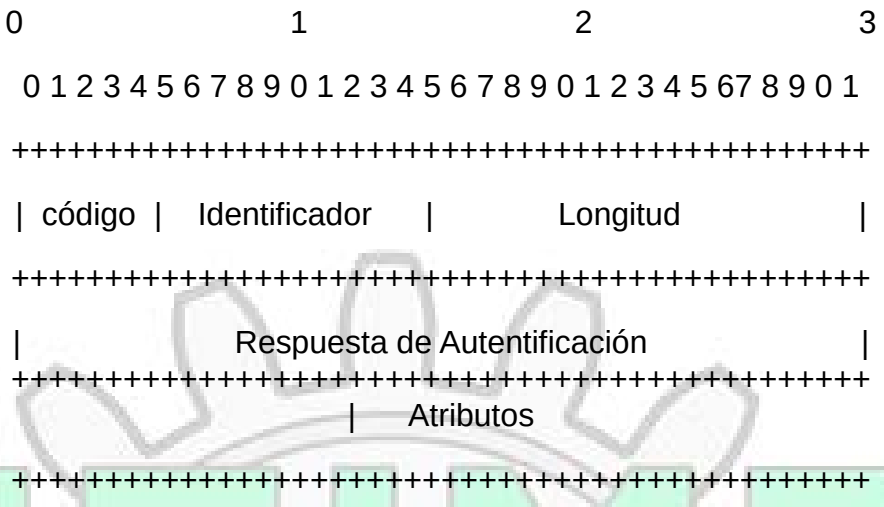

Tabla 1.4 Formato de paquetes de datos de Access-Reject.

Código 3 Para Access Reject.

2.10 Desafío de Acceso (Access Challenge).

Si el servidor RADIUS desea enviar un reto esperando una respuesta, el servidor RADIUS debe de responder una petición de acceso con un paquete con el campo de código puesto a 11 desafíos de acceso (Access Challenge).

El campo de atributo podría tener uno o más atributos de mensajes de respuesta, y podría tener solo un atributo de estado. o ninguno. Vendedor-Especifico, Ideal - Tiempo Fuera, Sesión - Tiempo Fuera y estado de Proxy, los atributos tiene que ser incluidos. Ningún otro atributo es aceptado en el Desafío de acceso.

En la recepción del desafío de acceso el campo del identificador es comparado con una petición de acceso pendiente. Adicionalmente el campo de respuesta de autentificación debe de tener la respuesta correcta para la respuesta de autentificación pendiente. Los paquetes inválidos son rechazados.

Si el NAS (Network Access Server) no soporta una respuesta de Desafío, debe de negociar un acceso por desafío como si se hubiera recibido una denegación de acceso Access Reject. En su lugar.

Si el NAS (Network Access Server), si soporta una Respuesta de Desafío, la recepción de un acceso por desafío indica que una nueva petición de acceso, debe de ser enviada. El NAS (Network Access Server) debe de enviar un mensaje de texto al usuario y espera la respuesta del usuario. Entonces se envía la petición de acceso original con una nueva petición de id, y petición de autentificación, con el atributo del password de usuario en vez de la respuesta de usuario encriptada, incluyendo el atributo de estado del desafío de acceso, solo 0 o 1 puede ser presentado como instancia del atributo de estado que puede ser presentado en la petición de acceso.

Un NAS (Network Access Server) que soporta el protocolo PAP (Password Authentication Protocol) puede reenviar la petición a un cliente entrante de quien acepta la entrada de PAP (Password Authentication Protocol). Si el NAS (Network Authentication Server) no soporta la respuesta debe de enviar un desafío de acceso como si hubiera recibido una denegación de acceso en su lugar

Un sumario del paquete de desafío de acceso se muestra abajo, Los paquetes se a derecha.

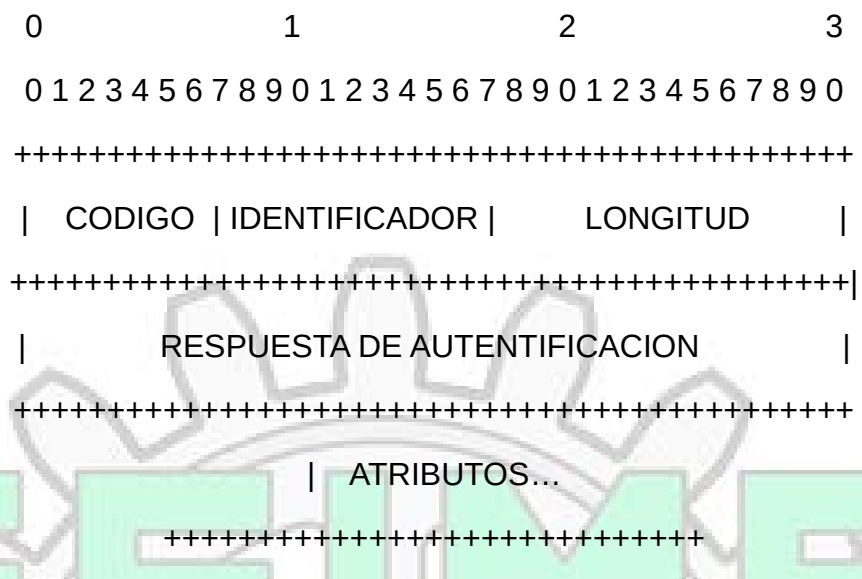

Tabla 1.5 Formato de paquetes de datos de Access-Challenge.

Código 11 Para Access-Challenge.

2.11 Atributos de RADIUS.

Los atributos del RADIUS contienen información específica de autentificación, autorización y detalles de configuración para petición y respuesta.

El final de la lista de atributos se indica por la longitud del paquete del RADIUS.

Algunos atributos se incluyen más e una vez el efecto de este atributo específico es especificado en la descripción de atributos. Si muchos atributos similares son presentados, los atributos deben de ser presentados por el Proxy. El orden de atributos que no tienen un orden, pueden no ser preservados. Un servidor RADIUS o un cliente RADIUS no debe de tener ninguna dependencia al orden de atributos de diferentes tipos, un cliente RADIUS o un Servidor RADIUS no debe de requerir atributos del mismo tipo para ser continuos.

Donde la descripción de atributos limita que tipo de paquete puede ser contenido, aplica a los paquetes llamados petición de acceso, aceptación de acceso, petición de desafío y denegación de acceso (códigos 1,2,3,11), otros documentos. Para determinar que atributo esta permitido en la petición de contabilización y repuesta de contabilización (código 4 y 5) se refiere al documento de RADIUS documento de contabilización.

De la misma forma e tamaño de los paquetes están definidos en su estado y ciertos atributos son permitidos. Futuros memos definen nuevos atributos en los futuros paquetes.

Un sumario del formato de los atributos es presentado abajo, Los campos se envían de izquierda a derecha.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
|  TIPO        |  LONGITUD  |  VALOR…
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Tabla 1.6 Formato de atributos de RADIUS.

2.12 Tipos de Formatos.

El campo de tipo es de un octeto, las actualización del RADIUS son especificadas en el campo de “Numero Asignados” Numero de Referencia [6], valores 192-223 son reservadas para uso experimental, los valores 224-240 son reservadas para usos de implementaciones especificas y los valores 241-255 son reservadas y no deben de usarse.

El servidor RADIUS debe de ignorar cualquier tipo desconocido.

Un cliente RADIUS debe de ignorar cualquier tipo desconocido.

Estas especificaciones conciernen a los siguientes valores:

1 nombre de usuario.

2 password de usuario.

3 CHAP password.

4 NAS IP- Address.

5 Puerto NAS.

6 Tipo de Servicio.

7 Framed Protocol

8 Framed Ip Address.

9 Framed Ip Net-Mask

10 Framed Routing

11 Id de Filtrado

12 Framed - MTU

13 Framed - Compression.

14 Login IP - Host

15 Login Service

16 Login TCP-Port

17 No asignado

18 Mensaje de respuesta

19 Numero de Regreso de Llamada.

20 Id de Regreso de Llamada.

21 no asignado

22 Framed Route

23 Framed - IPX-Network.

24 estado

25 Clase

26 Vendor - Specific

27 Tiempo de sesión terminada

28 Tiempo Idóneo

29 Acción de término

30 Id de estación marcada

31 Id de estación en llamada

32 Identificador del NAS

33 Proxy State

34 Servicio de Login LAT

35 Nodo de Login LAT

36 Grupo de Login LAT

37 Enlace de Framed AppleTalk

38 Red de Framed AppleTalk

39 Zona de Framed AppleTalk

40-59 (Reservado para Contabilización).

60 Desafío CHAP

61 Tipo de puerto NAS

62 Limite de puerto

63 Puerto de Login LAT

2.13 Nombre de Usuario.

Este atributo indica el nombre del usuario a ser identificado.

Debe de ser enviada en la petición de acceso.

Debe de enviar un paquete de aceptación de acceso. En este caso el cliente debe de usar el nombre que se regreso de la aceptación de acceso que se genero de la petición de contabilización para esta sesión. En la aceptación de acceso se incluye el tipo de servicio = Rlogin y el atributo del nombre de usuario. El NAS (Network Access Server) puede usar el nombre de usuario regresado para cuando se emplee la función de RLogin.

Un sumario del formato del atributo de Nombre de usuario es mostrado abajo. Los campos se transmiten de izquierda a derecha.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
|     TIPO      |       LONGITUD      |     CADENA ...
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Tabla 1.7 Formato de atributos de Nombre de Usuario.

Tipo 1 Nombre de Usuario.

Longitud

>=3

El campo de cadena es de uno o más octetos. El NAS (Network Authentication Server) debe de delimitar la longitud máxima del nombre de Usuario. Pero la potencialidad de poder lidiar con un máximo de 63 octetos es recomendada.

El formato del nombre de usuario debe de ser uno de distintas formas:

Consiste solo de 10646 caracteres con codificación UTF-8

Identificador de Acceso a Red.

Identificador De acceso de Red, es un nombre en formato ASN.1 (Abstract Syntax Notation One) y es usado como llave publica en sistemas de autentificación.

2.14 Password de Usuario.

En transmisiones, es password es ocultado, en principio el password es enviado hasta el final con nulos de 16 octetos. Con un arreglo hash de un solo camino sobre un envío de octetos, que consisten de e secreto compartido, seguido del identificador de peticiones, esta repuesta es calculada con una compuerta XOR con el primer segmento de 16 octetos del password y colocados en los primeros 16 octetos del campo de cadena del atributo de Password de Usuario.

Si el Password es mayor a 16 caracteres se calcula un segundo arreglo hash MD5 sobre una cadena de octetos conformados por el secreto compartido, seguido del resultado de la primera operación con el XOR. Ese Arreglo hash es sumado exclusivamente con el segundo arreglo hash de 16 octetos del password es sumado exclusivamente con el password del primer arreglo y es puesto en los siguientes de 16 octetos de la cadena de caracteres del atributo de password e usuario.

Llámese al secreto compartido “S” y al secreto compartido “RA”, se divide el Password el 16 octetos llámese P1, P2 con el ultimo octeto anexado y con nulos enlazados, se le llamara a los textos encriptados c(1), c(2), etc.

B1 = MD5(S + RA) C(1) = P1 XOR B1

B2 = MD5(S + RA) C(2) = P2 XOR B2

. .

B(i) = MD5(S + RA) C(i) = Pi XOR Bi

La cadena va a tener como elementos C1+C2, ….+Ci, donde cada elemento va a ser concatenado por el símbolo +.

De manera contraria el proceso se realiza de manera contraria para poder obtener el password original.

El Password de Usuario es mostrado abajo, Los campos se transmiten de izquierda a derecha.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
|     TIPO      |   LONGITUD    |    CADENA …
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Tabla 1.8 Formato de atributos de Password de Usuario.

Tipo 2 Para Password de usuario, su longitud Debe de ser de almenos 18 caracteres y menor de 130, el campo de cadena debe de ser de una longitud entre 16 y 128 octetos de largo.

2.15 Password de CHAP.

Este atributo indica el valor de la repuesta provista por el PPP (Point to Point Protocol) de un usuario que respondió a una autentificación por desafío solo es usado en los paquetes de petición de acceso.

El valor del desafío de acceso es encontrado en el atributo de CHAP (Challenge Handshake Authentication Protocol.

Un sumario del formato del campo de atributo del CHAP (Challenge Handshake Authentication Protocol) - Password. Se muestra abajo. Los campos son transmitidos de izquierda a derecha.

```
                0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
|    TIPO       |  LONGITUD  | IDENTIFICADOR CHAP | CADENA …
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Tabla 1.9 Formato de atributos de Password de CHAP.

Código 3 Para Password de CHAP.

2.16 Dirección IP del NAS (Network Access Server).

Este atributo indica la dirección ip de identificación del NAS (Network Access Server), que esta requiriendo autentificación del usuario. Y debe de ser. La dirección IP del NAS (Network Access Server) solo es usada en los paquetes de petición de acceso, note que la dirección IP del NAS (Network Access Server) no debe de ser usada para seleccionar el secreto compartido usado para autentificar la petición.

Un formato del atributo de la dirección IP de NAS (Network Access Server) es mostrada abajo, Los campos se transmiten de izquierda a derecha.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1  2 3 4 5 6 7 8 9 0 1
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
     |     TIPO    |  LONGITUD  |          DIRECCION
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
                    DIRECCION             |
+++++++++++++++++++++
```

Tabla 1.10 Formato de atributos de IP del NAS.

Tipo 4 Para la dirección IP del NAS.

2.17 Puerto del NAS (Network Access Server).

Este atributo indica que el numero del puerto físico del NAS (Network Access Server) en el cual identificado el usuario, Esto solo es usado en los paquetes de petición de acceso nótese que se esta refiriendo a puerto en el sentido físico y no en el sentido que podría tener un protocolo en el numero de puerto para un envío de información con UDP o TCP. Cualquier el tipo de puerto de NAS (Network Access Server), deben de presentar en el paquete de petición de acceso, si el NAS (Network Access Server) aprecia a diferencia entre sus puertos.

el formato de los atributos del puerto NAS (Network Access Server) es mostrado abajo, los paquetes se transmiten de izquierda a derecha.

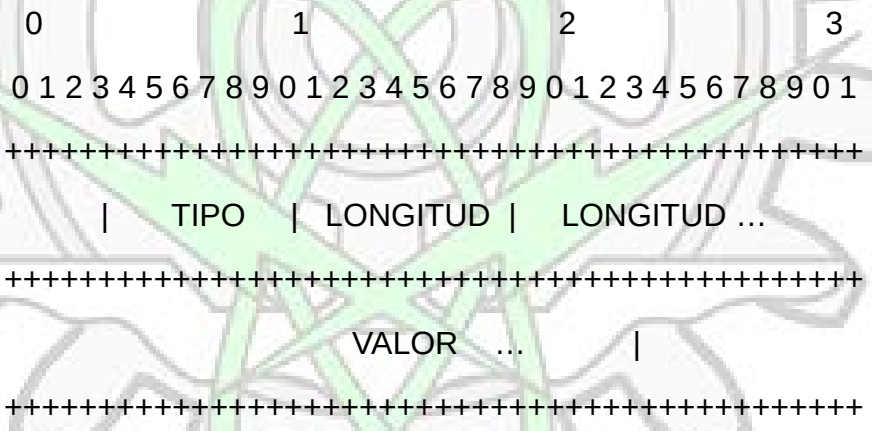

Tabla 1.11 Formato de atributos del puerto del NAS.

TIPO 5 Para puerto NAS.

CAPITULO 3: IMPLEMENTACION.

3.1 Radius Multiplataforma.

Este protocolo fue desarrollado en sistemas Unix y algunos posteriormente trasladados a sistemas basados en Windows. Por tanto los primeros servidores basados en RADIUS fueron compilados para Unix y funcionaron perfectamente para GNU/Linux o sistemas similares.

Con el tiempo muchos servidores como RADIUS han ido emigrando a Windows

En las plataformas basadas en Unix como GNU/Linux podemos encontrar soluciones de tipo OpenSource. El problema que presentan estas implementaciones OpenSource como FreeRadius es la incomodidad en la administración por medio de consolas graficas. Muchos administradores actuales se han formado en cómodos sistemas gráficos de ventanas y evitan cualquier sistema de administración basado en la consola de texto. Aunque el resto de las características que incorporan y la utilidad de los RFC (Request for Comments). En el caso del software OpenSource como FreeRadius el coste por introducción es el coste de consultoría formación e implantación administración y mantenimiento. Para implementación de RADIUS en Windows se utilizara el servidor IAS (Internet Authentication Server) que es un servidor RADIUS robusto y sencillo.

Una razón para implementar Windows es la perfecta sincronía entre los clientes y los servidores mediante la utilización de políticas de grupo, es muy fácil implementar recursos y normas de seguridad es uno de los puntos fuertes.

Active Directory tiene mayor integración en todas las plataformas de escritorio como Windows con lo que si se decide utilizar Active Directory, es mucho mas conveniente utilizar entornos producción sobre Windows.

Active Directory es una implementación propietaria del robusto protocolo LDAP utiliza un esquema de autenticación sobre protocolo Kerberos . se basa en LDAP version3. Se utiliza en combinación con otros protocolos DHCP ,DNS, etc.

Permite formar un sistema de confianzas entre directorios, haciendo que los objetos como usuarios estén disponibles. Cada objeto de directorio posee un identificador único (GUID de Globally Unique Identifier) que facilitan las búsquedas en la base de datos y relaciona los registros.

3.2 Microsoft IAS.

Microsoft Internet Authentication Server, a pesar de su nombre es un servidor RADIUS incluido en las versiones de Windows Server.

IAS cumple la mayor parte de las funciones de un servidor o de un Proxy RADIUS. Como un servidor RADIUS cumple con el RFC 2865 y 2866 Muchos administradores no son conocedores de que Windows incorpore un servidor RADIUS completo en sus versiones Server ya que no es un producto de Microsoft.

Como servidor estándar RADIUS , IAS utiliza de forma predeterminada los puertos 1812 y 1645 para autenticación, y para arqueo 1813 y 1646, para Microsoft los cuatro puertos se mantienen abiertos.

3.3 Configurando el Servidor.

La configuración del servidor se puede realizar de dos maneras de manera manual o de manera asistida en este caso se escogió la forma manual.

Nuestro Primer paso es especificar nuestro dominio que en este caso es Local (“midominio.local”)

Especificamos el dominio de DNS y una vez introducida la dirección de nuestro DNS, se inicia la instalación.

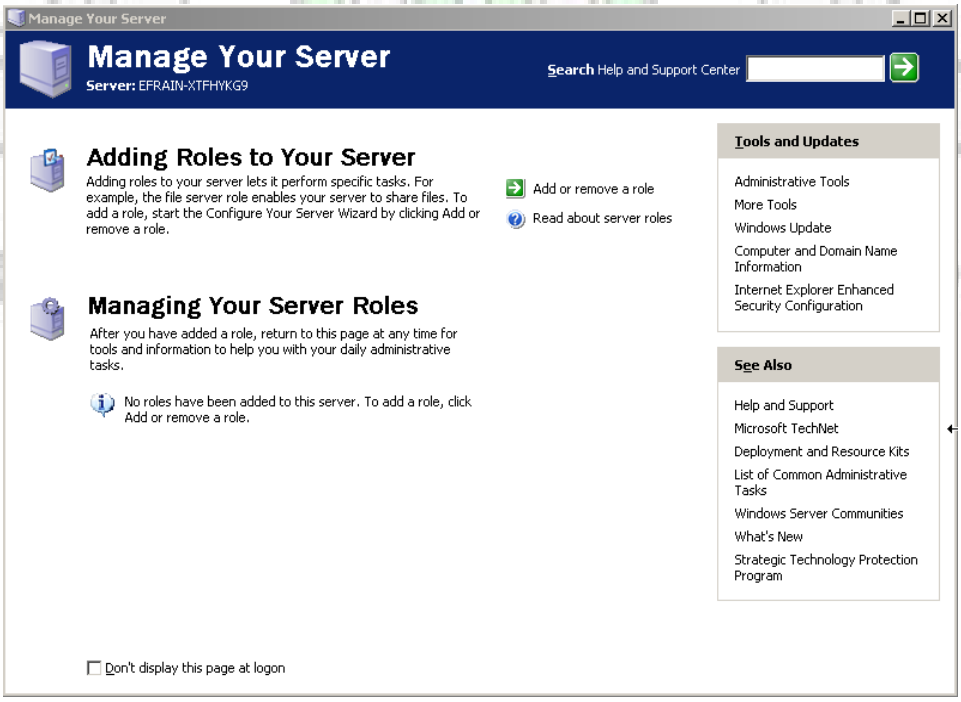

Figura 1.1 Administre su Servidor.

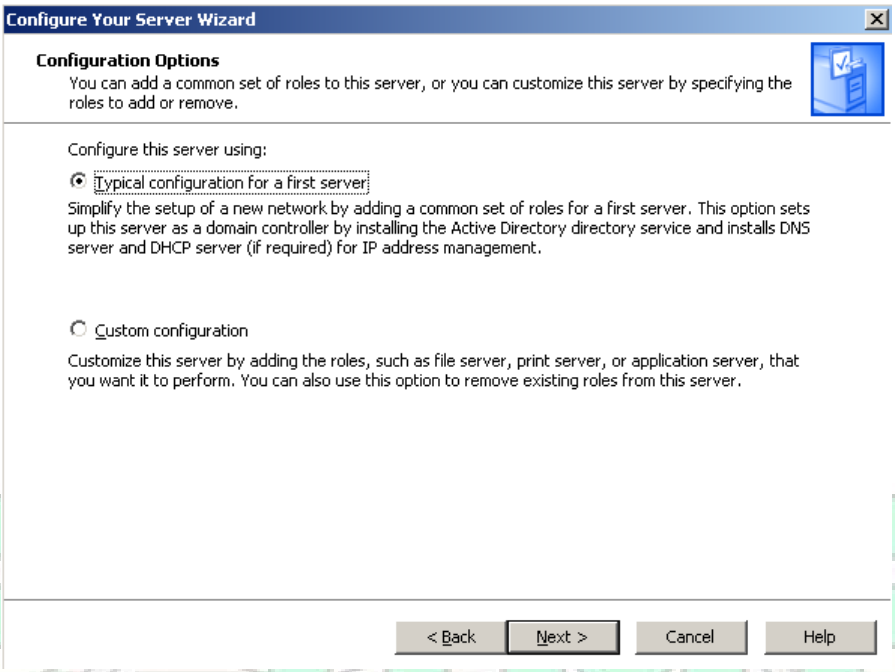

Figura 1.2 Configuración Tipica.

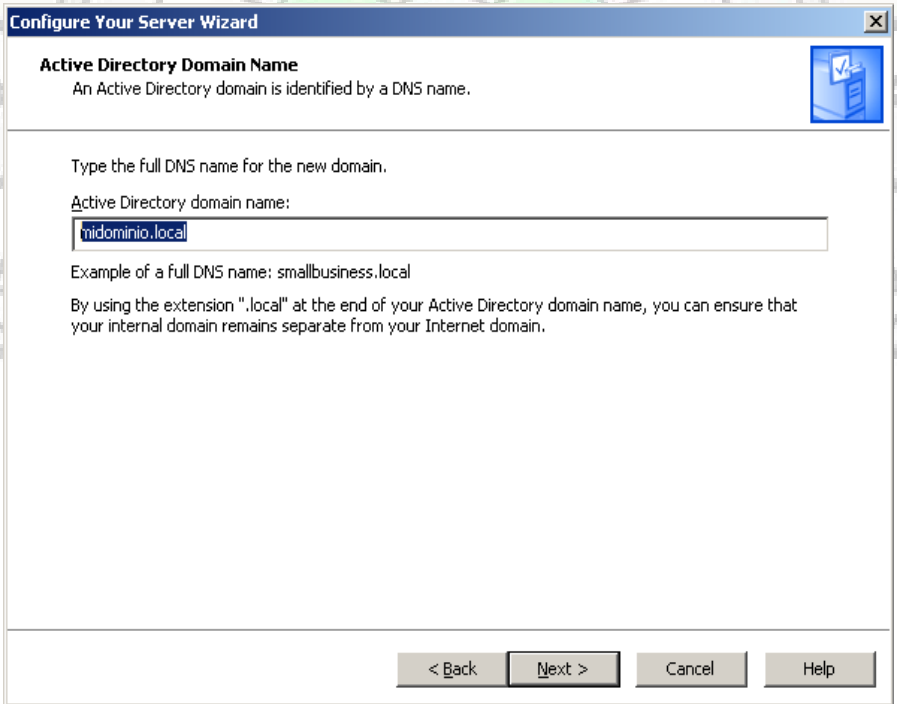

Figura 1.3 Nombre de Dominio.

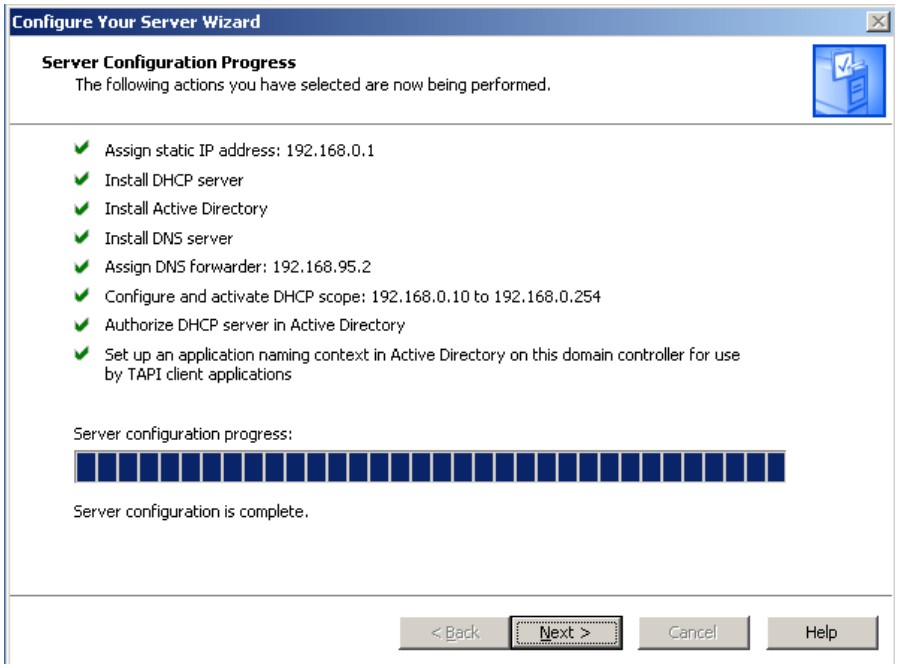

Figura 1.4 Propiedades de la Configuración.

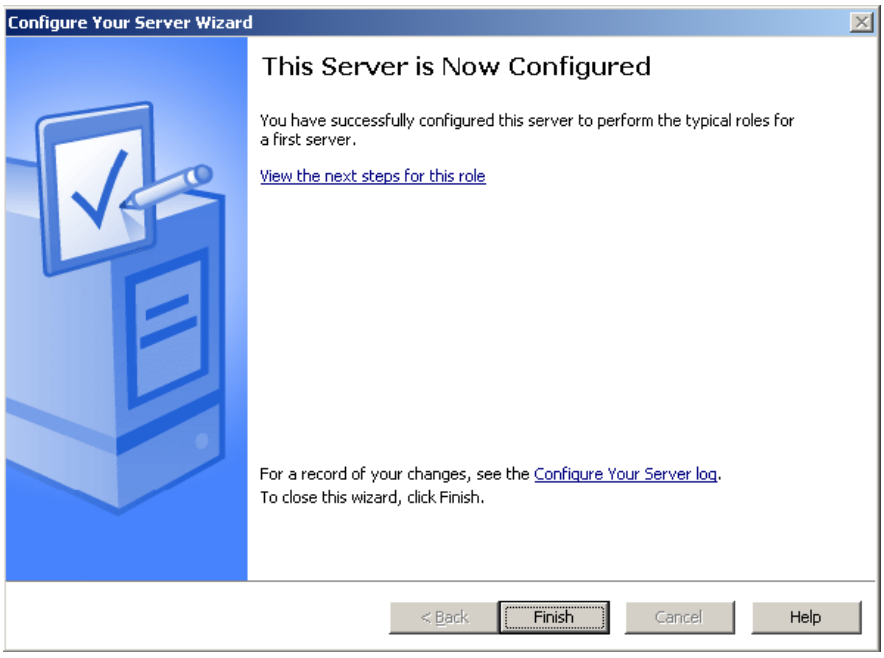

Figura 1.5 Servidor Configurado.

3.4 Instalando el Servidor IAS.

Ahora se inicia la instalación del Servidor IAS (Internet Authentication Server) el Radius de Windows y con ello también iniciamos la configuración de los puertos y la seguridad, para esto abrimos la herramienta de agregar o quitar programas en el panel de control, presionamos en el botón de agregar o quitar componentes de Windows, y seleccionamos Servicios de Red (“Networking Services”).

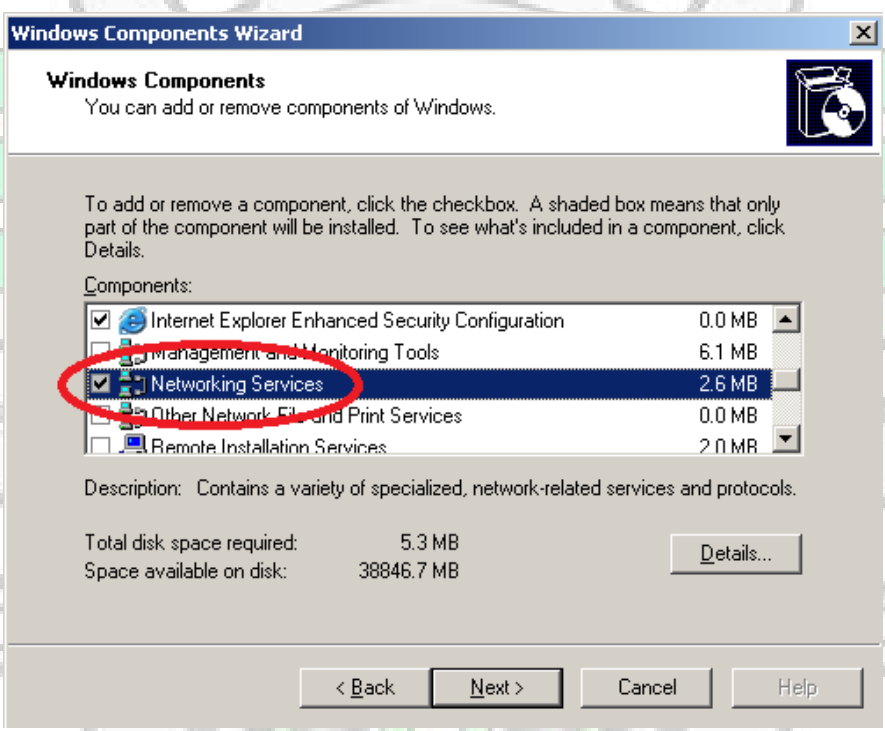

Figura 1.6 Servicios de Red.

Damos click en detalles y seleccionamos el servicio de autenticación de Windows, que es precisamente la instalación del servidor IAS (Internet Authentication Server). Damos Click en detalles y seleccionamos el servicio de autenticación de Windows o IAS (Nuestro Radius).

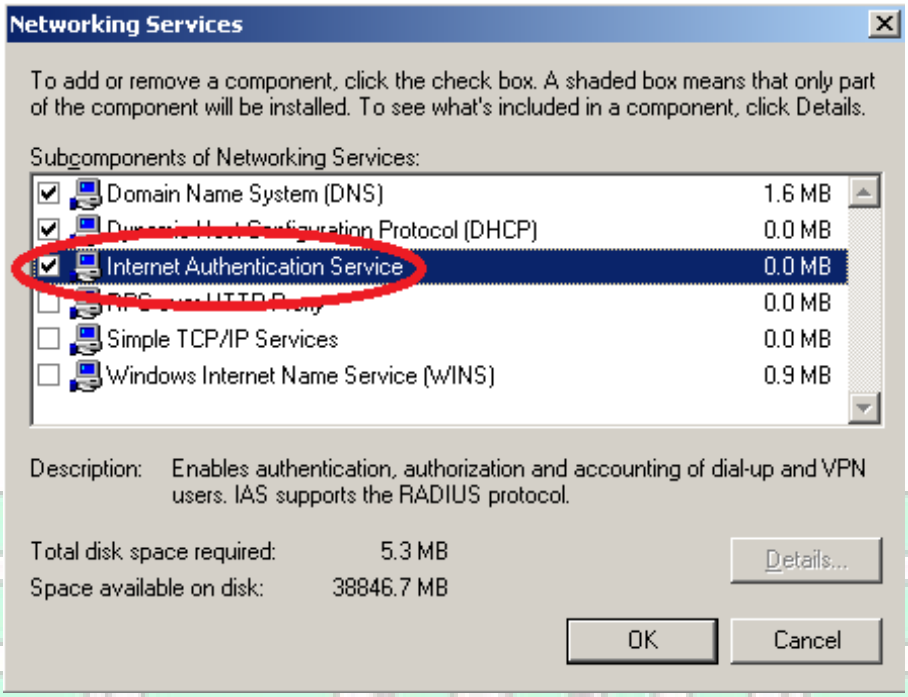

Figura 1.7 IAS.

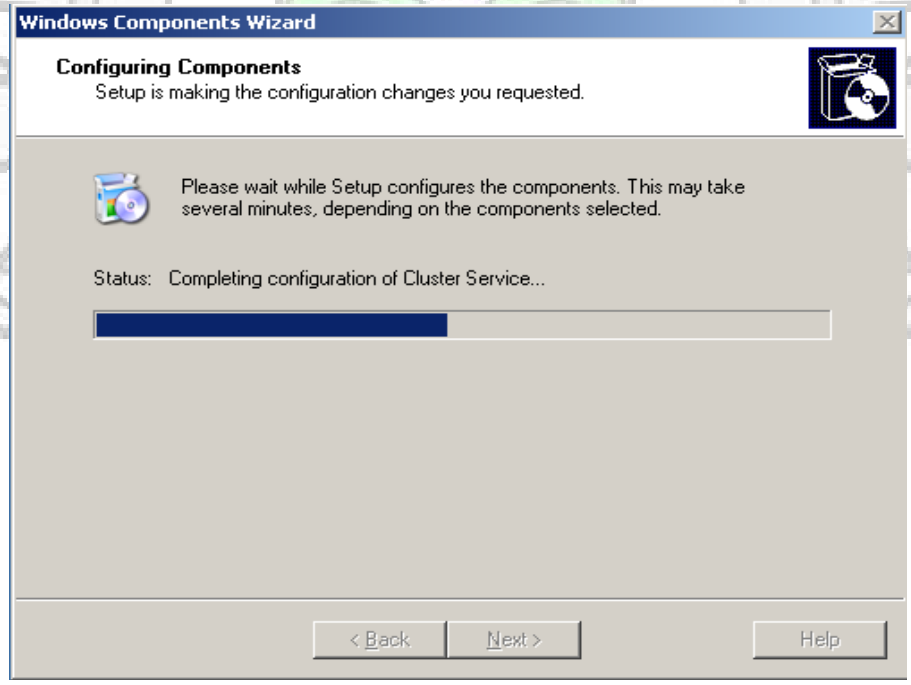

Figura 1.8 Instalación del IAS.

Figura 1.9 Finalización de la instalación del IAS.

Una vez realizada la instalación de nuestro servidor IAS (Internet Authentication Server), es necesario configurar los puertos de conexión en este caso son los puertos 1812,1645, 1813,1646.

3.5 Configuración de Puertos en el IAS.

Para configurar los puertos de conexión de nuestro servidor es decir los puertos estandarizados en los RFCs (Request for Comments) 2865, 2866 que son los 1812, 1813,1845y 1846. Se abre la carpeta de IAS (Internet Authentication Server) en la barra de programas en la opción de Herramientas Administrativas seleccionamos Internet Authentication Service.

Y en la carpeta de Internet Authentication Service (Local), se selecciona con Click derecho del mouse las propiedades y seleccionamos en la ventana emergente los protocolos que vamos a utilizar.

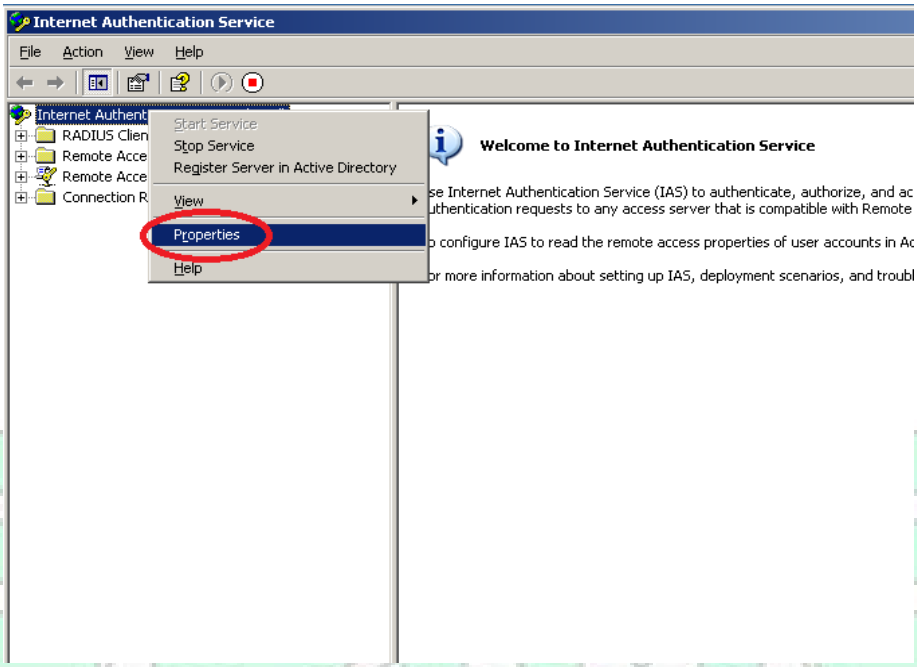

Figura 1.10 Registro del Servidor.

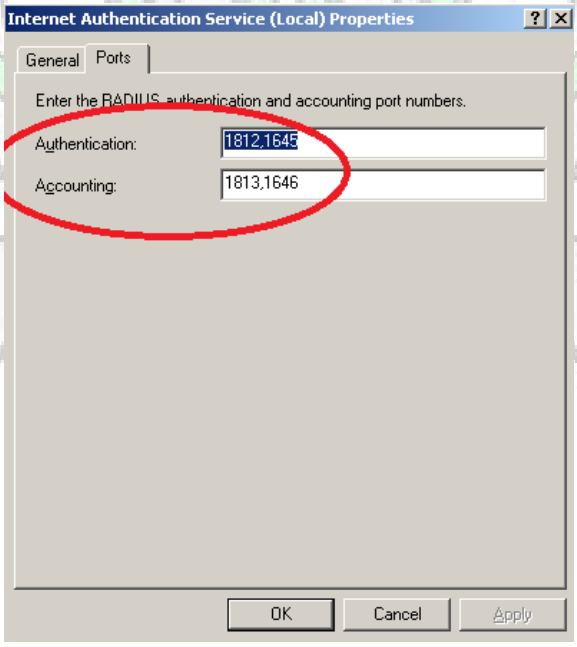

Figura 1.11 Asignación de Puertos.

Para nuestro secreto compartido se va a la carpeta de Radius Client en la misma ventana se selecciona con Click Izquierdo New Radius Client se configura esta opción, se elige un nombre para el cliente y una dirección IP en este caso la misma que se utilizo para dirección fija en nuestro equipo configurada en las propiedades del TCP/IP, y por supuesto se ingresa el secreto compartido tan importante para la comunicación entre el cliente y el servidor Radius.

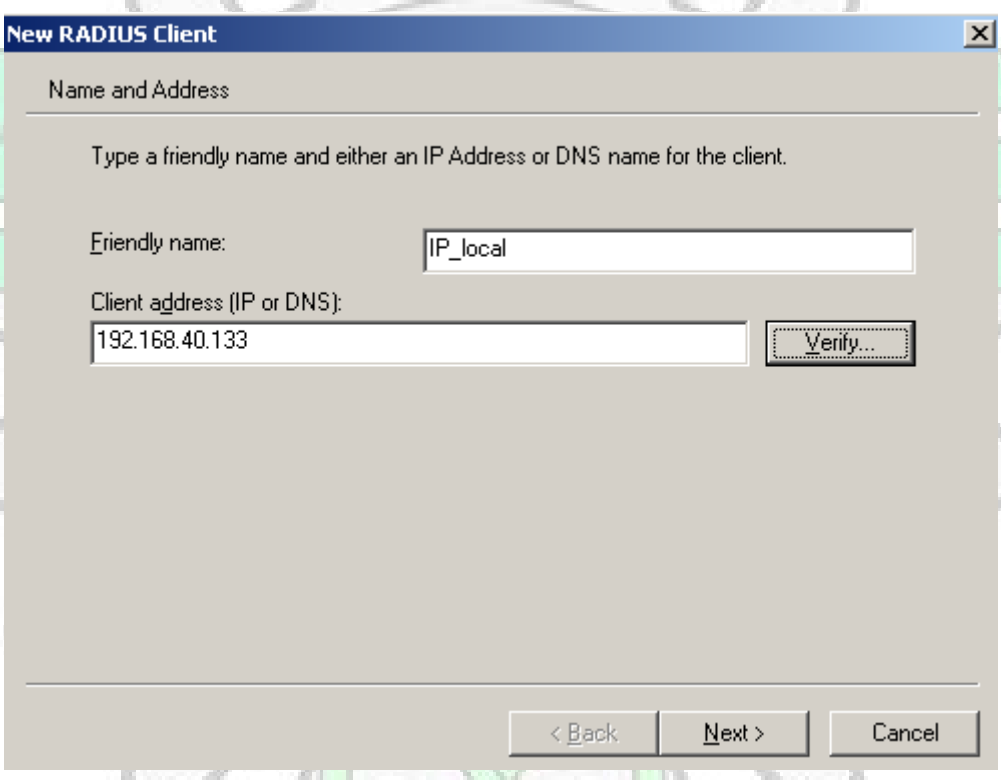

Figura 1.12 Nombre del cliente RADIUS.

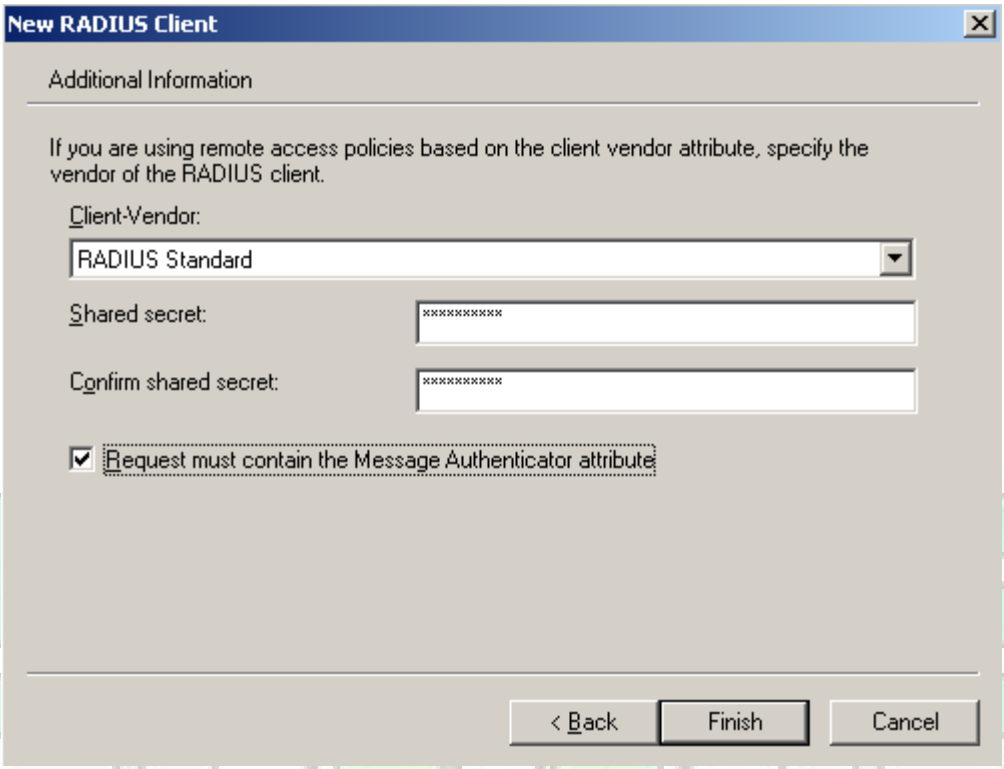

Figura 1.13 Asignación del Cliente Compartido.

Una vez configurado nuestro cliente damos de alta nuestro servidor en Active Directory.

3.6 Active Directory.

Es un servicio de directorio que utiliza una asignación de nombres basada en el estándar de DNS (Domain Name System).

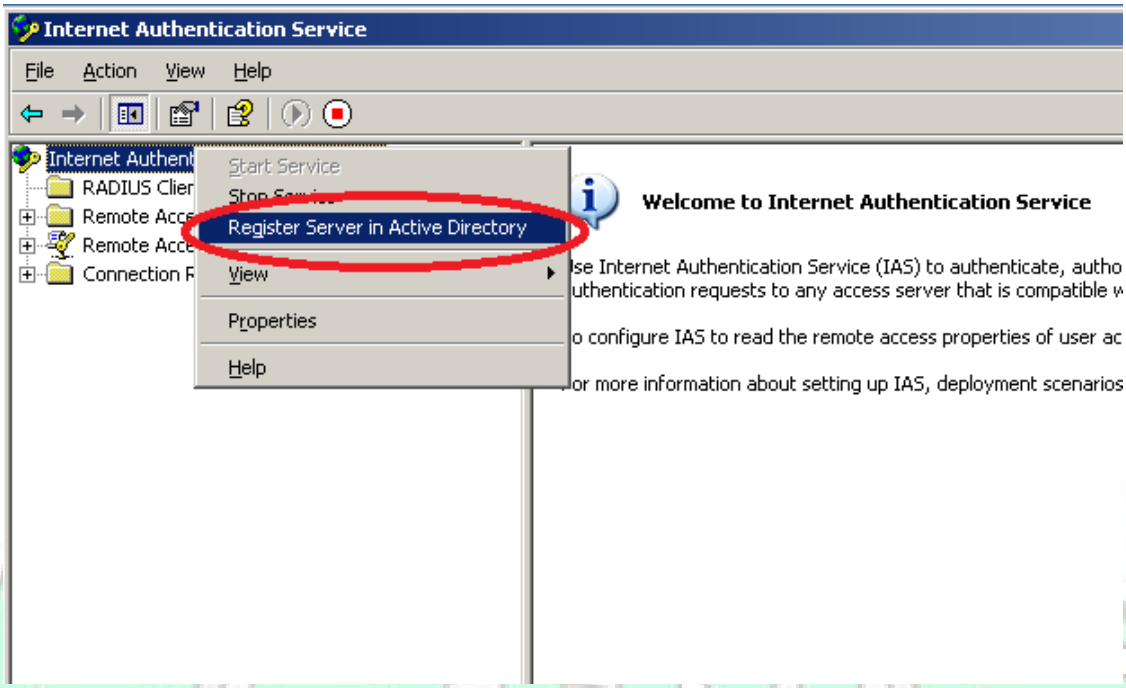

Figura 1.14 Registro del servidor en Active Directory.

En el registro aparecen distintas opciones como el nombre de archivo la ubicación donde se guardara toda la información, también existe la posibilidad de canalizar el arqueo hacia otro programa como se hace en Linux. Cuando seleccionamos sobre el sistema de contabilidad arqueo Accounting veremos que habla sobre el arqueo en documentación de Microsoft en la ayuda veremos que habla de la sobre cuentas lo que puede crear un conflicto en la ventana de configuración seleccionamos el archivo de Archivo local y nos aparecen las siguientes opciones de registro el nombre del archivo con su ruta el formato de registro y la periodicidad para la creación d nuevos ficheros de registros.

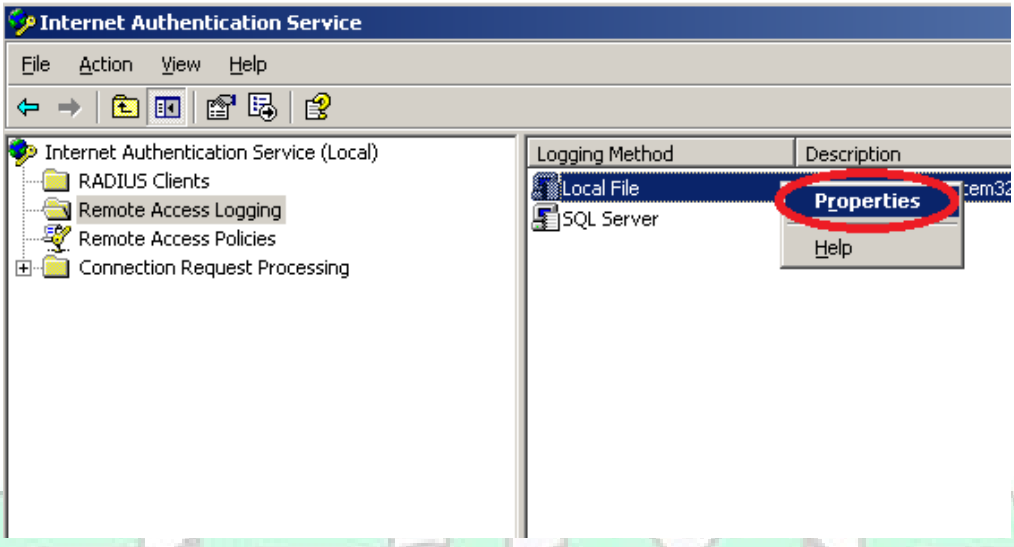

Figura 1.15 Propiedades del Registro de Active Directory.

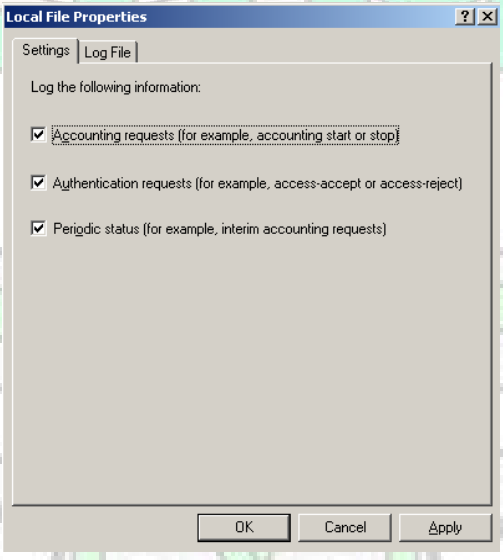

Figura 1.16 Selección de Información para la Carga.

3.7 Protocolos de Seguridad.

En la cuestión de la seguridad vamos a elegir las directivas de acceso y para ello vamos a abrir la carpeta de directivas de acceso remoto y vamos a dar click en Nueva directiva de acceso remoto y en el asistente vamos a seleccionar las

directivas de seguridad que son las siguientes, CHAP, EAP, MS-CHAPv2, MS-CHAPv2 CPW y PAP.

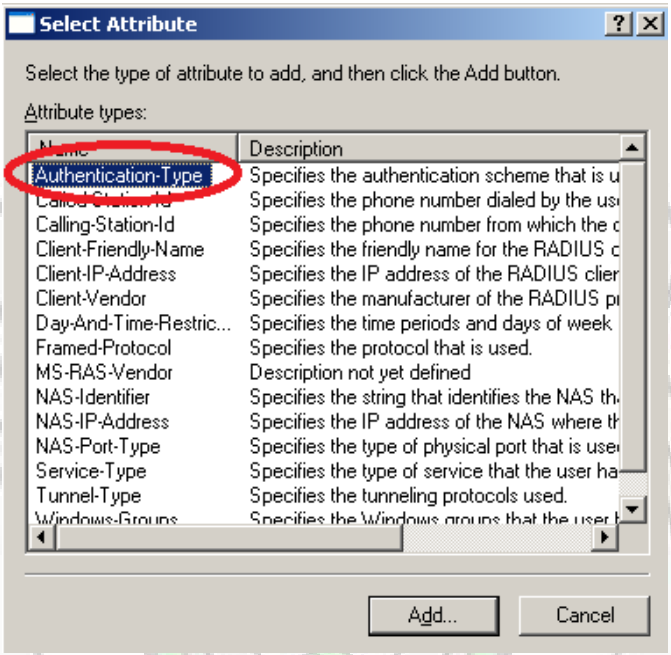

Figura 1.17 Tipo de Autenticación.

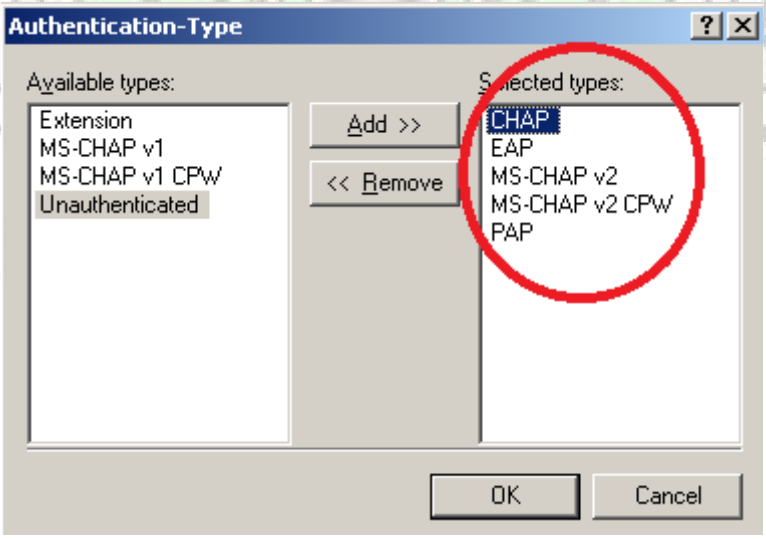

Figura 1.18 Métodos de Autenticación.

3.8 Pruebas de Funcionamiento.

Para poder comprobar que nuestro servidor y la política de seguridad sirven se procederá a hacer un usuario de prueba y se confirmara el acceso a la red con un software de prueba.

Accedemos a herramientas administrativas del menú inicio y buscamos a usuarios y equipos de Active Directory en el desplegado de carpetas seleccionamos Users y en el menú contextual seleccionamos Nuevo – Usuario; Seleccionamos un Nombre una contraseña y por Dominio “dominio.local”.

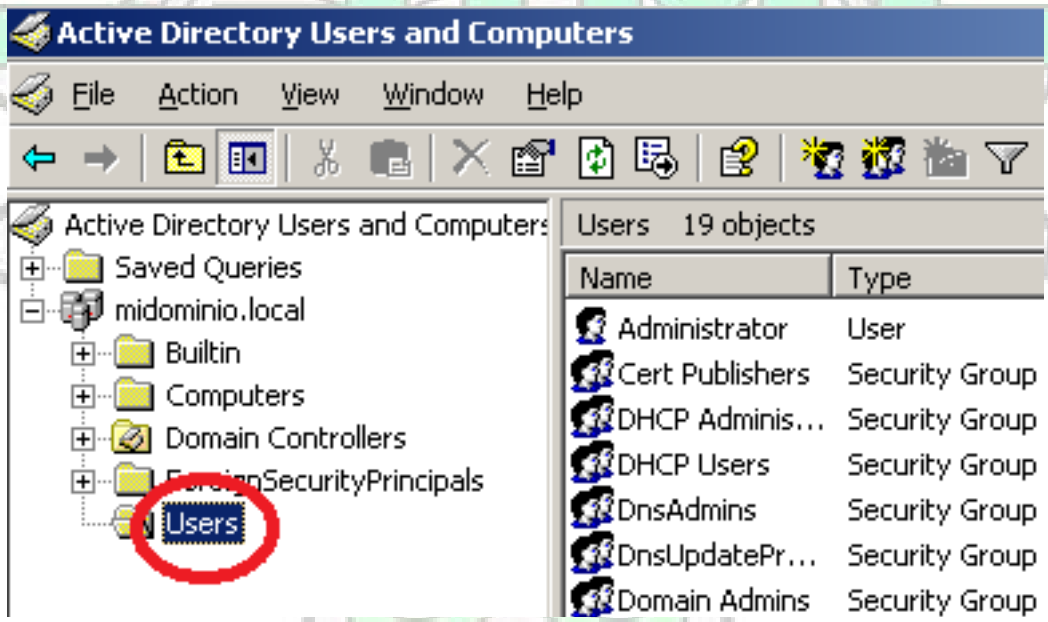

Figura 1.19 Creación de Usuarios Cliente.

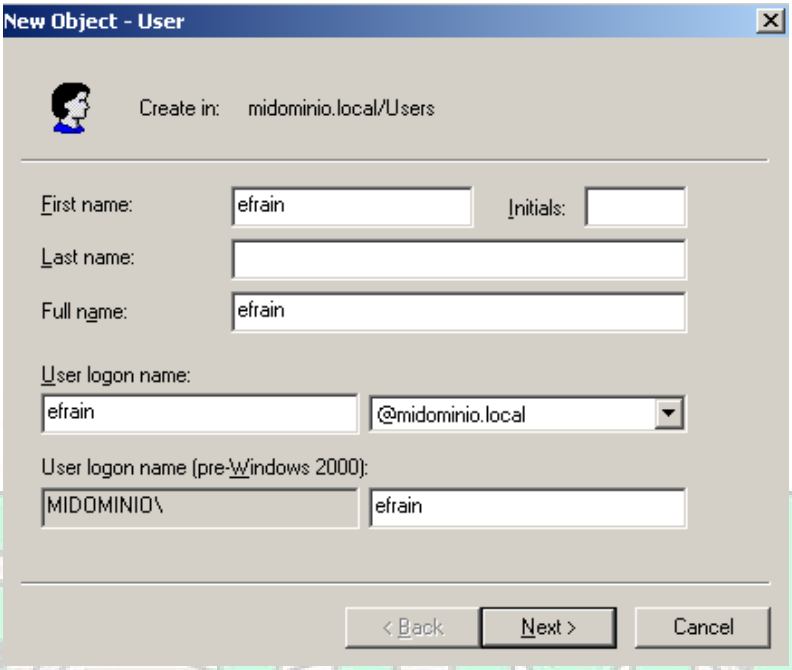

Figura 1.20 Nombre/Dominio de Usuarios Cliente.

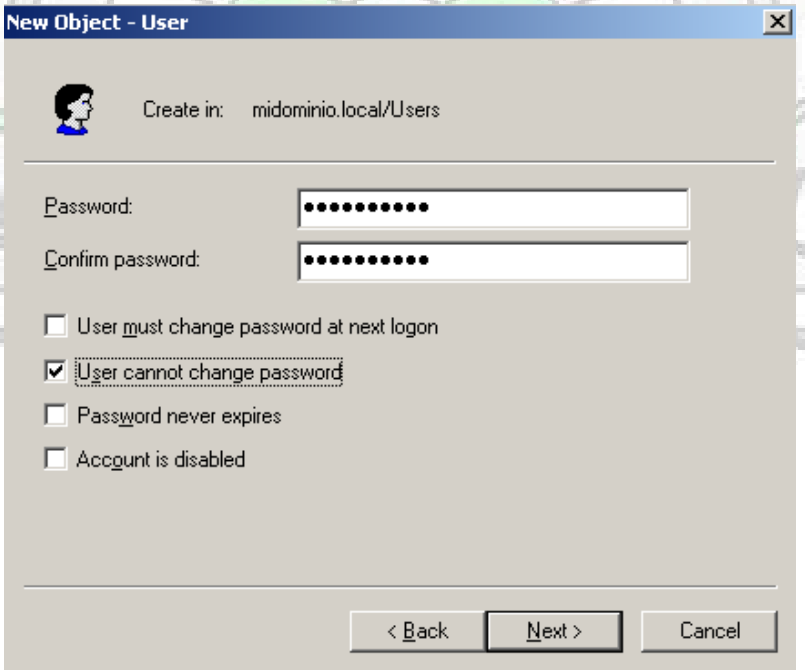

Figura 1.21 Password.

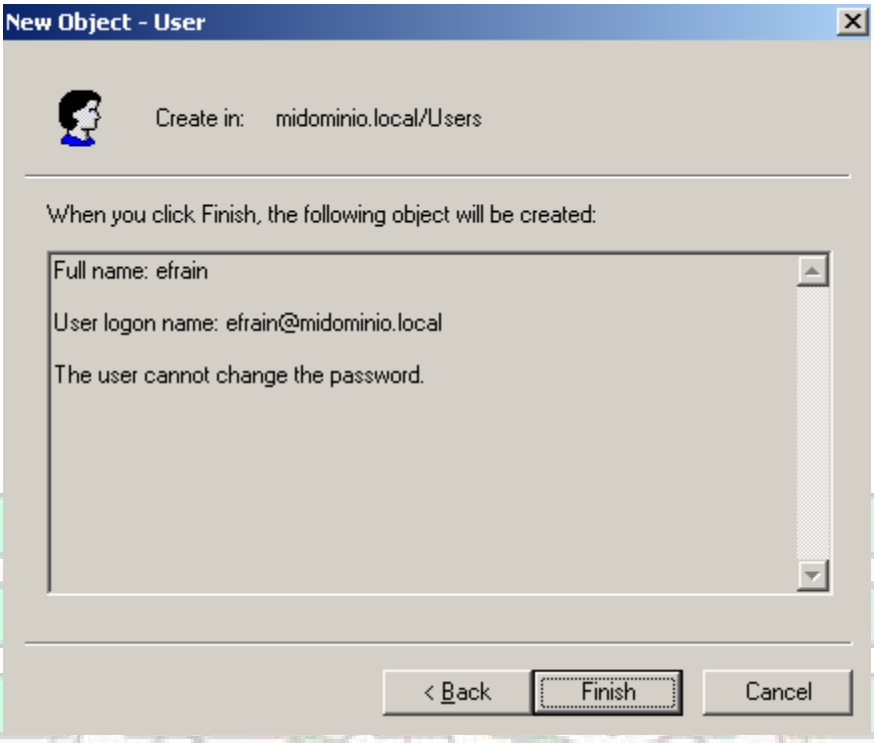

Figura 1.22 Configuración Completada.

3.9 Software de Prueba.

La utilidad es la Utilidad NTRadPing de MasterSoft en su versión 1.5 es muy sencilla de utilizar para realizar solicitudes PAP (Password Authentication Protocol) o CHAP (Challenge Handshake Authentication Protocol), aquí se pueden ingresar datos como la IP del Radius, el Puerto el tiempo de intervalos entre intentos, el numero de intentos, el secreto compartido, el nombre de usuario el password y el tipo de petición o suplica.

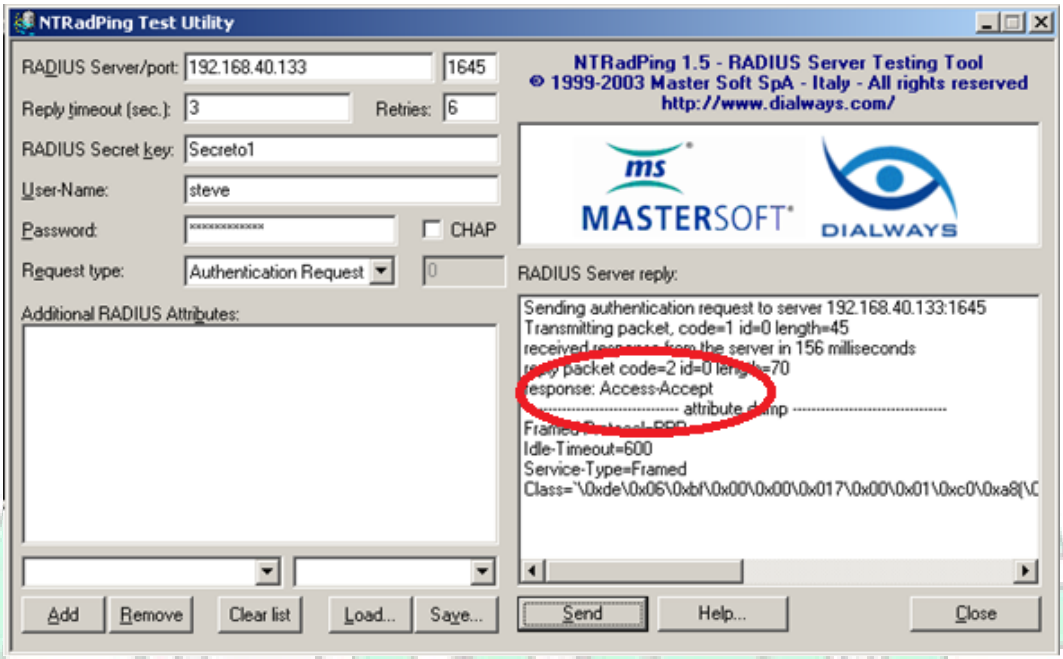

Figura 1.23 Access – Accept.

Prueba exitosa de conexión a red Radius con mensaje de Access Accept.

3.10 Prueba de Implementación del Cliente RADIUS en Wi-Fi.

Se activa el detector de redes inalámbricas de desde un cliente Windows y se detecta en este caso la red de Radius, se deben de configurar las propiedades de la red inalámbrica RADIUS se selecciona el tipo de seguridad de WPA (Wi-Fi Protected Access) desde Propiedades/Seguridad con un cifrado TKIP (Temporal Key Integrity Protocol).

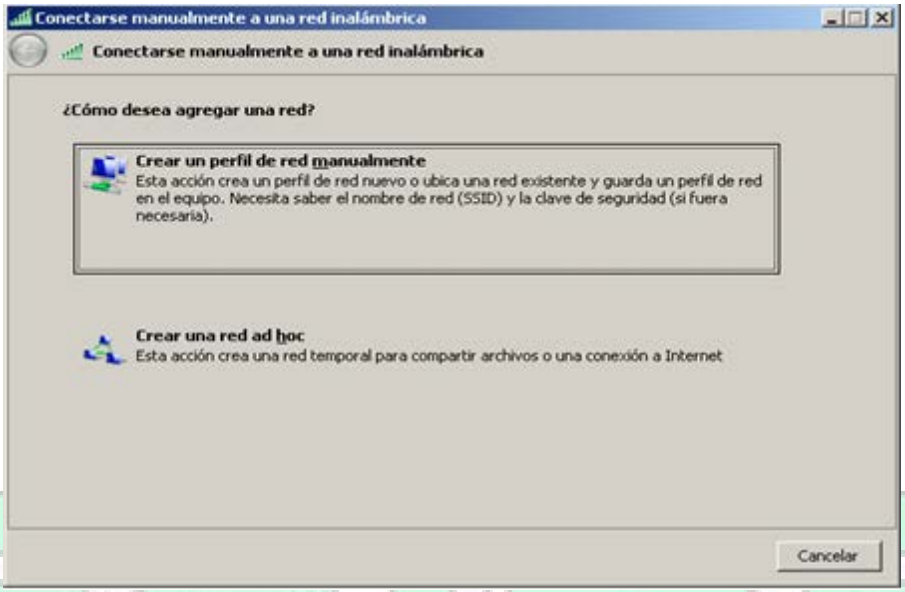

Figura 1.24 Conexión a Red Inalámbrica.

Se elige el método de autenticación PAP en el WPA Enterprise. Y se selecciona la red inalámbrica radius2 se mostrará una ventana en la cual solicite el nombre de usuario y contraseña.

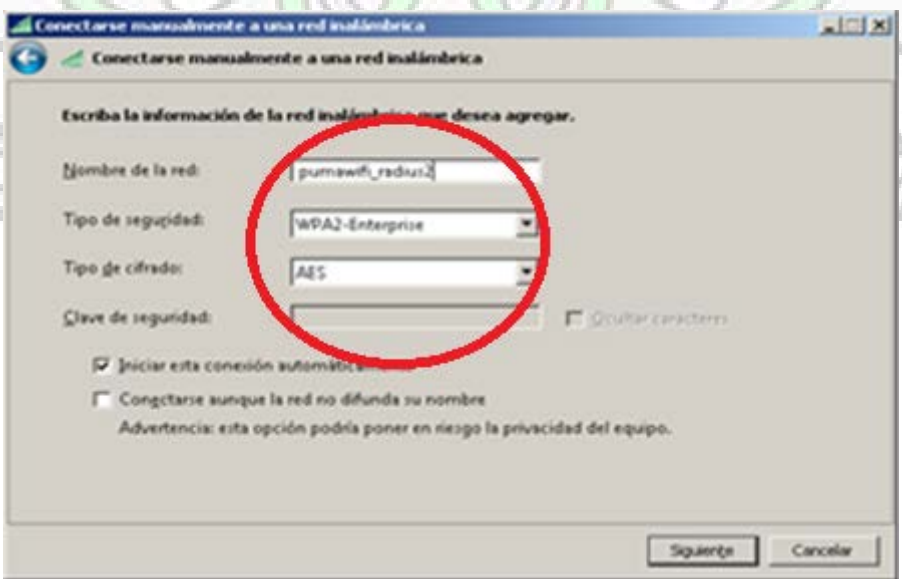

Figura 1.25 Configuración de Seguridad.

Si el usuario se autentifico correctamente se concederá la conexión, en caso contrario se negara el acceso.

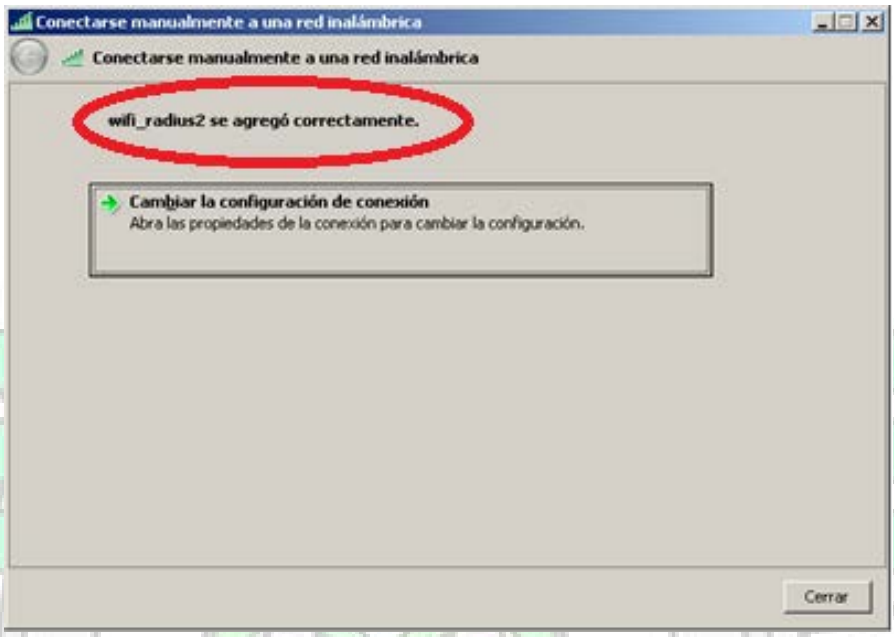

Figura 1.26 Conexión a Red Inalámbrica Exitosa.

Conexión Exitosa a la Red de Radius via Wi - Fi.

CONCLUSIONES

La autentificación es una parte Fundamental en la informática y la seguridad de la información ya que permite la compartición de recursos informáticos de manera confiable , la informática y las tecnologías de la información demandan una mayor asertividad en la identificación de usuarios, es por este motivo que la implementación de este servidor de autenticación es en gran medida una forma de comprender esta necesidad y es por que solo mediante la conjunción de los diversos protocolos de autenticación y envío de mensajes que es posible.

Es en este caso el poder ver y entender de una manera muy fácil el protocolo de autenticación por desafío y compartimiento de secreto, y el protocolo PAP (Password Authentication Protocol) que es uno de los mas necesarios y mas sencillos, entre otras cosas, vimos que un mismo protocolo puede estar dado en mas de una plataforma tecnológica que en este caso el Radius tiene la característica de poderse encontrar en forma gratuita en FreeRadius y En el servidor de Windows como el Internet Authentication Server.

En fin esta poderosísima herramienta nos permite tener una pequeña red en casa que nos puede servir para tener cámara IP conectadas a nuestra RED, o bien incluso hasta un café Internet.

GLOSARIO

CHAP: (Challenge Handshake Authentication Protocol o Protocolo de Desafío Mutuo), Es una actualización de PAP (Password Authentication Protocol), es un método del tipo secreto compartido ya que ambos sistemas comparten una contraseña.

DHCP: (Dynamic Host Configuration Protocol) Es un protocolo que asigna información de configuración a los dispositivos de red tales como una dirección IP.

EAP: (Extensible Authentication Protocol es el Protocolo Extensible de Autentificación), Conjunto de métodos que permiten el envío de información.

IAS: (Microsoft Internet Authentication Server), Es un completo servidor RADIUS incluido en las versiones de Windows Server. IAS cumple la mayor parte de las funciones de un servidor o de un Proxy RADIUS. Como un servidor RADIUS cumple con el RFC 2865 y 2866.

LEAP: (Lightweight Extensible Authentication Protocol es el Protocolo Extensible de Autentificación Ligero), Es un Protocolo de CISCO que utiliza un sistema dinámico de rotación de claves.

MD5: (Message Digest Algorithm), Es un criptografía para envío de información que produce funciones hash (huellas), es un algoritmo de reducción.

NAS: (Network Access Server) Es el servidor de acceso a la red es el que permite la entrada física a la red y tramita la autenticación.

NIC: (Network Interface Controller), Es un dispositivo electrónico que sirve para regular el tráfico de la red e incrementar su potencia ya que provee un acceso físico a tarjetas de expansión.

PAP: (Password Authentication Protocol), Protocolo de autenticación por password es un protocolo que permite la identificación de usuarios mediante un texto personalizado y secreto llamado Password.

PROTOCOLO:	Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.
PROXY:	Programa o dispositivo que realiza una acción en representación de otro, que sirve para permitir el acceso a Internet a todos los equipos de una organización.
RED:	Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.
ROUTER:	Enrutador, Encaminador. Dispositivo hardware y software para interconexión de redes de computadoras.
WPA:	(Wi-Fi Protected Access) es un protocolo de seguridad de red que utiliza la seguridad de las redes Wi-Fi mediante una clave WEP, WAP, Implementa mucho del estándar IEEE 802.11i y en especial del Protocolo de Integridad de Llave Temporal TKIP.

REFERENCIAS

- Manual de Referencia 2865.
- Manual de Referencia 2866.
- AAA Radius 802.1
  Autor: Yago Fernández Hansen, Antonio Ramos Varón, Jean Paul García-Morán.
  Ed. Alfa Omega .
- Windows Server 2003 R2.
  Autor: William R. Stanek.
  Ed. ANAYA.
- Sistemas Distribuidos.
  Autor: George Coulouris, Jean Dollimore, Tim Kindberg.
  Ed. Pearson 3ra Edición.