INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

Sistema de Autenticación basado en la norma 802.1X para la red inalámbrica de los anexos de profesores de ESIME Zacatenco

T E S I S

Que para obtener el Título de
Ingeniero en Comunicaciones y Electrónica

Presentan:

José Gerardo Mondragón Legorreta
Luis Uriel Montesinos Flores
Diego Rivas Cortés

Asesores:

M. en C. Fernando Noya Chávez
M. en C. Roberto Galicia Galicia

México, D.F. 2009

Sistema de Autenticación basado en la norma 802.1X para la red inalámbrica de los anexos de profesores de ESIME Zacatenco

Para mi madre quien entrego su vida sin escatimar desde el momento en que fui concebido para que contara con todo lo que me pudiera hacer una persona.

Te AMARE eternamente Luz María Flores Solís

Es ist wahr: Wir lieben das Leben, nicht, weil wir ans Leben, sondern ans Lieben gewöhnt sind.
F. Wilhelm Nietzsche

Agradecimientos

A Dios ya que es quien nos permite seguir adelante si el así lo decide, el que nos dota de todas nuestras cualidades como seres humanos en la vida y el que puede terminar con ella en un suspiro; Gracias por tener poco que pedirte y tanto que agradecerte… A.A.

Mi familia y amigos que siempre han estado para compartir y disfrutar de las alegrías, como para consolar y fortalecer en las tristezas.

Mayra Isabel Vejar Gutiérrez, gracias por todas las palabras que proferiste y todo el tiempo del cual te desprendiste, para contribuir con los elementos más importantes en la realización de este trabajo brindándome tu apoyo y amor.

M. en C. Fernando Noya y M. en C. Roberto Galicia, gracias por el apoyo y orientación que me brindaron para concluir con este trabajo.

Ich verlasse heut' Dein Herz
Verlasse Deine Nähe
Die Zuflucht Deiner Arme
Die Wärme Deiner Haut
Wie Kinder waren wir
Spieler -
Nacht für Nacht
Dem Spiegel treu ergeben
So tanzten wir bis in den Tag
Ich verlasse heut' Dein Herz
Verlasse Deine Liebe
Ich verlasse heut' Dein Herz
Verlasse Deine Liebe
Ich verlasse Deine Tränen
Verlasse was ich hab'
Ich anbefehle heut Dein Herz
Dem Leben - der Freiheit Und der Liebe
So bin ich ruhig -
Da ich Dich liebe!
Im Stillen Laß ich ab von
Dir Der letzte Kuß - im Geist verweht
Was Du denkst
bleibst Du mir schuldig
Was ich fühle das verdanke ich Dir
Ich danke Dir
für all die Liebe
Ich danke Dir in
Ewigkeit
Ich verlasse heut' Dein Herz
Verlasse Deine Liebe
Ich verlasse Dein Herz
Dein Leben
Deine Küsse
Deine Wärme
Deine Nähe
Deine Zärtlichkeit

Tilo Wolf

Objetivo General

Proponer un mecanismo para controlar el acceso de los usuarios, a la red inalámbrica de las salas adjuntas de profesores de ESIME Zacatenco, por medio de un Sistema de Autenticación, fácil de implementar y que ayude a administrar la red, de igual forma será transparente para los usuarios, con la finalidad de eliminar la infiltración de usuarios no autorizados a dicha red, basado en la norma 802.1X.

Objetivos Específicos

- Analizar la problemática de seguridad de la red inalámbrica de ESIME Zacatenco, por no contar con un sistema de autentificación robusto.
- Cumplir con especificaciones de seguridad de la norma 802.1X
- Proponer la implementación de un Sistema de Autentificación basado en Linux, que ayude a la seguridad y eficiencia de la red de los anexos de ESIME Zacatenco.

Introducción

Las comunicaciones inalámbricas tienen sus orígenes en el año 1906 con la creación del tríodo[1], posteriormente muchos años después Motorola da a conocer el teléfono celular, pero el verdadero avance se da con los experimentos que IBM realizo con luz infrarroja, surgen aquí las investigaciones con altas frecuencias y se dan las primeras publicaciones de trabajos LAN (Local Area Network), que fue llamada de esta forma años después.
La forma en cómo se debe de transferir la información de un equipo a otro en este tipo de sistemas, se especifica en el modelo OSI, con esto aseguramos un orden en la transmisión de datos; dicho modelo cuenta con siete capas, en las cuales todos los dispositivos de cómputo y telecomunicaciones son referenciados, las especificaciones de cada una de las capas se mencionarán más adelante.

Con la publicación de la norma 802.11 se da lugar a la tecnología inalámbrica de redes locales, posteriormente se crean a partir de ésta, distintas variantes las cuales representan ciertas mejoras en diferentes aspectos en relación a la original (820.11).

Dentro de la tecnología inalámbrica podemos hablar de las topologías existente, diremos que una topología de red es la forma en la que conectamos los dispositivos en una red, en las redes inalámbricas podremos encontrar dos topologías básicas, de las cuales usaremos la que más convenga para los fines de nuestra red.

La información que viaja dentro de nuestra red es demasiado valiosa, es por ello que se debe utilizar métodos de criptografía, cuya finalidad es garantizar el secreto en la comunicación entre dos equipos, y por otra parte permite asegurar que la información que se envía es auténtica en ambos sentidos, con estos métodos es posible asegurar que el remitente del

[1] Válvula termoiónica de tres electrodos, que tiene la capacidad de controlar con una pequeña tensión una gran corriente. Con lo que se genera el fenómeno llama amplificación.

mensaje es realmente quien dice ser, y que el mensaje original no haya sido modificado en el trayecto del viaje, la seguridad de una red es substancial, debido a que la información que en ocasiones se envía en una red pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc. Las redes inalámbricas son demasiado populares, por lo que es necesario tener conciencia de los problemas relacionados a la seguridad informática, para poder asegurar los recursos de los sistemas informáticos de cualquier red, utilizando los diferentes métodos de seguridad como son el filtrado de direcciones MAC, la clave WEP, clave WPA.

Una parte trascendental dentro de la seguridad informática, es la identificación y verificación de la identidad de usuarios y dispositivos, que tienen permiso de hacer uso de los servicios de una red, tema que debe ser atacado con métodos de autenticación, para la realización de este proyecto el método de autenticación a utilizar, será el determinado por la norma 802.1X, lo cual se explicará en el capítulo dos de este documento.

Justificación

La Escuela Superior de Ingeniería Mecánica y Eléctrica es un plantel del Instituto Politécnico Nacional, que imparte las carreras de Ing. Mecánica, Ing. Eléctrica e Ing. en Comunicaciones y Electrónica, ubicada en Av. Politécnico S/N en la Col. Lindavista D.F. Está compuesta por 5 edificios donde se imparten las carreras y se ubican diferentes áreas administrativas, así como cubículos de profesores.

Nos interesa para este trabajo zonas específicas destinadas para la estancia de profesores, llamadas áreas adjuntas, las cuales están en el primer piso de cada edificio. Divididas en tres salas, con escritorios modulares, acondicionadas con computadoras y servicio de red inalámbrica.

Para realizar las diversas funciones que tiene el docente, la red inalámbrica se ha vuelto una herramienta indispensable, teniendo el inconveniente que la red instalada en estas salas, no tienen ningún sistema que controle los accesos a las terminales, clientes o usuarios para poder hacer uso de ésta. Lo que ocasiona tener muchos usuarios, como son los alumnos que teniendo una computadora portátil fácilmente se pueden conectar a la red inalámbrica, haciendo uso de direcciones IP que no se les ha asignado, creando problemas a los usuarios con direcciones previamente establecidas, saturando la red con tráfico indebido, inclusive muchos usuarios traen software malicioso que perjudica el desempeño de la red inalámbrica, y la información que se transfiere. Además con intrusos que ingresan a la red de profesores, se descarta la garantía de que sus PC´s e información que estas contienen, estén a salvo de ataques.

Por ello se propone un sistema de autentificación para la red inalámbrica de profesores, que sea fácil de administrar, implementar y bajo precio para la ESIME Zacatenco.

Índice

Índice de Figuras

Índice de Tablas

Índice de Ilustraciones

Índice de Gráficas

Estado del Arte

Tras el paso del tiempo, el crecimiento de la tecnología y la necesidad de comunicación entre los seres humanos, ha crecido de manera impresionante, los usuarios necesitan comunicarse estando en cualquier lugar, de ahí el surgimiento de las comunicaciones inalámbricas, el auge en el tema de seguridad informática, y a ello se adjuntan los diferentes problemas que se han presentado por delitos informáticos, y así mismo surge lo que se conoce como autenticación, que no es más que la comprobación de la identidad de algún individuo, y que éste sea quien dice ser.

La autenticación requiere de la utilización de técnicas de criptografía, de tal manera que si es necesaria su implementación dentro de un entorno de red, conlleva la necesidad de un servicio de gestión y distribución de claves, para los algoritmos utilizados por los distintos elementos de la red. Por lo que los nuevos avances en la seguridad Wi-Fi, por parte de Ruckus [1], (Empresa pionera en tecnología Wi-Fi), que consiguió generar automáticamente las claves de cifrado para cada usuario inalámbrico. Gracias a la nueva técnica dinámica de clave pre compartida (PSK Dynamic Pre-Shared Key), que ha eliminado eficazmente la instalación manual tediosa, que requería mucho tiempo de las claves de cifrado, contraseñas o credenciales de usuarios para acceder de forma segura a una red inalámbrica. El modelo dinámico PSK genera de forma dinámica claves seguras, dando seguridad única para cada usuario autenticado, la instalación automática de estas claves de cifrado en los dispositivos de los usuarios finales, se realiza con la mínima intervención de personal de TI.

Con el crecimiento explosivo de las redes Wi-Fi en todo el mundo, las organizaciones han buscado la forma de simplificar la complejidad, y el costo de implementación de la seguridad inalámbrica robusta. Muchas empresas han utilizado una frase de contraseña que debe ser compartida entre muchos usuarios, y manualmente en los dispositivos del cliente. Si esta

"clave pre-compartida" se conoce o roba, debe ser cambiada para todos los usuarios, y volver a introducirla manualmente en cada dispositivo de los clientes.

Una alternativa al enfoque de PSK es un marco de seguridad elaboradas (por ejemplo, 802.1X), que requiere mayor información, tales como los certificados únicos o solicitantes, que se instalarán en cada dispositivo del usuario. Así como también se requiere un alto nivel de conocimientos técnicos, para la implementación del sistema y apoyo técnico permanente para los usuarios. Con Wi-Fi se ha colocado históricamente en dos extremos del espectro de la seguridad, Steve Martin vicepresidente de ingeniería de Ruckus Wireless, dijo: "En un extremo está el enfoque simple que hace la vida más fácil para los administradores de red, pero que crea problemas de seguridad potenciales para las empresas. En el otro extremo es un marco de seguridad muy robusta, pero a menudo abrumadora, tales como 802.1X, que requiere una enorme cantidad de tiempo y esfuerzo para implementar y administrar. Hemos creado lo mejor de ambos mundos con un método de fácil mantenimiento, para proporcionar un alto nivel de seguridad inalámbrica".

Mediante Dynamic PSK, las organizaciones pueden simplificar la administración de seguridad inalámbrica, con la confianza de saber que su red inalámbrica está protegida. Integrar todos los controladores de LAN inalámbrica al Ruckus ZoneDirector (Director de la zona dispositivo de administración creado por Ruckus Wireless), no tiene costo alguno, la tecnología de Dynamic PSK es independiente del dispositivo, y funciona en ordenadores portátiles y dispositivos de mano con Wi-Fi habilitado.

El funcionamiento de PSK inicia cuando un usuario accede a la red inalámbrica, que se autentica a través de un portal cautivo en Ruckus ZoneDirector. Esta información se compara con cualquier servidor de autenticación estándar, tales como Active Directory, RADIUS o una base de datos interna de la ZoneDirector de Ruckus.

Una vez que el usuario se ha autenticado correctamente, la tecnología dinámica PSK genera automáticamente una clave de cifrado única para el dispositivo del usuario. Esta clave se descarga en el cliente y configura automáticamente, junto con la información necesaria de la conexión Wi-Fi. Esto elimina a los usuarios la necesidad de configurar manualmente cualquier cosa y reduce drásticamente la carga de apoyo técnico del personal de TI.

Cada PSK dinámica está vinculada a un dispositivo específico del cliente y tiene una duración configurable. Con Dynamic PSK, el control en la duración de tiempo es válido en incrementos de horas, días, semanas o meses. Una vez que la clave expira, los usuarios deben volver a autenticarse. Si un dispositivo de usuario es robado, otros en la red no se ponen en riesgo. Para los administradores de red, sólo sería necesario eliminar el usuario en peligro de su dispositivo de autenticación o base de datos.

La sencillez que ofrecen estas tecnologías, como Dynamic PSK, realmente cambia el juego para los despliegues inalámbricos, Matthew Crandall, director asociado de Servicios de Información a Johnson College en Pennsylvania, dijo: "Dynamic PSK ha sido una herramienta para ahorrar tiempo notablemente, eliminando la molestia de tener que configurar cada usuario del dispositivo final al mismo tiempo que nos da el estado del arte de la seguridad Wi-Fi". "Al igual que muchas organizaciones, exigen seguridad inalámbrica fuerte, sin que las molestias de gestión asociados a ella se presenten. Dinámica PSK rompe los problemas convencionales que han impedido la aplicación de una arquitectura de seguridad inalámbrica simple y fuerte que es fácilmente escalable ", concluyó Crandall.

[2] Wi-Fi Alliance es una organización de más de 325 compañías que trabajan en colaboración para promover el mercado de Wi-Fi. La organización es responsable por el nivel de éxito de nuestro mercado, cual ha crecido más de 40% por varios años.

América Latina continúa adoptando Wi-Fi como la tecnología preferida para conectar LANs sin alambres. Broadband es un requisito para la penetración de Wi-Fi, y con una penetración de banda ancha alrededor de 24% de la población, hay una gran oportunidad todavía por ser realizada en Latinoamérica. En ciertos casos, usuarios experimentan con Wi-Fi en áreas de

acceso público inicialmente, y continuamos observando la proliferación de servicios de Wi-Fi en áreas públicas. Hay más de 250.000 áreas públicas de Wi-Fi registradas en 130 países, incluyendo miles y miles en Latinoamérica.

La colaboración del desarrollo de Wi-Fi en la integración y el desarrollo del servicio Universal, se ve reflejada ya que el usuario de hoy quiere establecer la mejor conexión posible donde quiera que se encuentre. Con cientos de miles de conexiones públicas de Wi-Fi, e innumerables hogares y negocios que también ofrecen conectividad con Wi-Fi, Wi-Fi es un ingrediente fundamental en la experiencia de conectividad continua.

En los últimos años hemos visto a Wi-Fi siendo incorporado en productos electrónicos, teléfonos móviles, e innumerables categorías de productos que han promovido a Wi-Fi desde el LAN hasta un medio de conectividad continua en aplicaciones que no ha visto límite. Por eso hemos colaborando con otras organizaciones y tecnologías para desarrollar métodos de coexistencia y transferencias que puedan ser transparentes para el usuario. Esto también ha contribuido a que muchos proveedores de servicios telefónicos y de conectividad a la Internet también ofrezcan servicios de Wi-Fi en áreas públicas, en hogares y en empresas.

Wi-Fi Alliance ha desarrollado varios programas para promover la conectividad continua en varias aplicaciones. Por ejemplo, en el año de 2009 se lanzó un programa llamado Voice Over Wi-Fi Personal, el cual establece que productos ofrecen una experiencia excelente de Wi-Fi durante llamadas telefónicas sobre Wi-Fi.

Se tienen programas de calidad de servicio (Wi-Fi Multimedia o WMM) e inteligente uso de poder (WMM Powersave). Estos programas ayudan a mantener una satisfacción al usuario en más y más aplicaciones y productos.

El impacto que Wi-Fi tiene en el desarrollo de las ciudades digitales, es debido a que Wi-Fi se ha establecido también como un ingrediente básico de la ciudad digital. Wi-Fi es una

tecnología que trae la conectividad a las manos del usuario, y hay más de 1.000 ciudades alrededor del mundo que tienen planes o servicios de Wi-Fi establecidos y ofrecidos por estas ciudades para el beneficio público. El acceso usualmente es más común en las áreas más congestionadas, por ejemplo el centro de la ciudad, estaciones de trenes, parques, aeropuertos, y edificios de educación.

También hemos visto a Wi-Fi siendo usado para servicios municipales, como para monitorizar mantenimiento de trenes (ejemplo de Chicago) o para monitorizar consumo de agua y electricidad (ejemplo de Austin).

La industria continúa creciendo sanamente en parte porque Wi-Fi ofrece una forma de establecer una red en forma económica porque no requiere construcción sino mínima infraestructura. Esto es realizado sin sacrificar servicio. Con el advenimiento del programa Wi-Fi CERTIFIED 802.11n draft 2.0, la conexión de Wi-Fi ofrece velocidad, capacidad y distancia que se compara bien con una infraestructura alámbrica. En 2008 estimamos que 50% de todos los productos vendidos en nuestra industria serán basados en esta nueva generación de Wi-Fi.

El desarrollo de WiMax como soporte del Wi-Fi en América Latina, no le quita la popularidad sin duda a Wi-Fi como la conectividad para LAN sin alambres alrededor del mundo. Hay más de 500.000.000 usuarios de Wi-Fi y la industria ha vendido cerca de 1.000.000.000 unidades. Wi-Fi usa conexiones al WAN ofrecidas por otras tecnologías como DSL, cable, etc. La combinación de Wi-Fi y WiMAX será popular en ciertas áreas y circunstancias. Las dos tecnologías son claramente complementarias.

Una de las razones que ha contribuido al éxito de Wi-Fi ha sido que el espectro que usa la tecnología es accesible al público en forma mundial y gratis. La emisión de energía permite que la señal pueda transmitir suficiente datos a distancia adecuada para muchas aplicaciones.

La comunidad de Wi-Fi ha establecido que una industria puede ofrecer soluciones que respetan otras tecnologías usando el mismo espectro, y coexistiendo en el mismo producto. La tecnología también ha innovado continuamente en el área de seguridad.

Hay ciertas oportunidades para continuar promoviendo conectividad y buena experiencia al usuario, por ejemplo Whitespaces, o el área espectral que va a ser desocupada cuando señales de televisión sean digitales.

Para la región en 2015 a nivel tecnología de comunicaciones, es fácil pronosticar que la penetración de banda ancha en el área continuará, y que la penetración de Wi-Fi también acelerará. ABI Research pronostica que la industria de Wi-Fi venderá más de 1.600.000.000 unidades solamente en el año 2013. Es posible que el acceso al Internet por el móvil vaya a ser un modelo popular para el usuario. ABI también pronostica que en 2012 se venderán más de 500.000.000 teléfonos con Wi-Fi.

Capítulo 1 "Comunicación Inalámbrica (Wireless)"

La creación del triodo por Alexander Lee de Forest (1906), dio inicio a una etapa en la creación de las comunicaciones de radio frecuencia, que se presentaron durante el resto del siglo XX [3], como la transmisión de televisión pública (Inglaterra 1927), la creación de la FCC (Federal Communication Comission en 1934, agencia federal de EEUU encargada de regular y administrar las telecomunicaciones, siendo sucesora de la Comisión Federal de Radio que fue establecida tiempo antes 1927), la multiplicación por división temporal se aplica a la telefonía, así como los primeros desarrollos de la telefonía mediante microondas (1950), la primera retransmisión vía satélite (1960), Motorola muestra el teléfono celular a la FCC entre otras aportaciones(1972), hasta que en 1979 IBM experimentó con luz infrarroja, con la finalidad de construir una red local (publicaciones volumen 67 de los Proceeding del Instituto de Ingenieros Eléctricos y Electrónicos "IEEE"), lo que fue considerado como el punto de partida en la línea evolutiva de las redes inalámbricas. A partir de esos momentos, las investigaciones se realizarían en laboratorios, utilizando altas frecuencias, hasta que en 1985 la FCC asigna permisos de operación sin licencia en tres bandas de frecuencia (902 a 928 MHz, 2.400 a 2.483,5 MHz y 5.725 a 5.850 MHz), a dispositivos que utilicen 1 watt o menos, al uso de IMS (Industrial, Scientific and Medical), estas asignaciones llevaron al incremento de actividades en la industria, y la investigación de redes de área local de tipo inalámbrica, que ya se enfocaba al mercado. Publicándose los primeros trabajos de LAN propiamente nombrados seis años más tarde, debido a lo especificado en la norma 802.11, que la transmisión mínima debe de ser de 1 Mbps para considerarse LAN. Dándose poco tiempo después el surgimiento de la Red Inalámbrica de Área Local (WLAN) [4], aunque su introducción al mercado se tardaría algunos años más. El factor que originó un gran empuje al desarrollo de esta clase de red, fue la permanencia de las computadoras portátiles (Adam Osborne) y PDA (Personal Digital Assistant) en el mercado, ya que estos productos portátiles exigían la necesidad de una red sin restricciones de cableado. Pero cumpliendo con

las definiciones de los niveles más bajos del modelo OSI, principalmente de la sub-capa MAC (*Medium Access Control*) [5].

1.1 Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI)

El modelo de Interconexión de Sistemas Abiertos (OSI) fue desarrollado en 1984, por la ISO (International Organization for Standardization / Organización Internacional para la Normalización), este modelo representa un marco teórico o conceptual del cómo se debe transferir información de un sistema a otro, haciendo que exista un orden, entre todos los sistemas y componentes necesarios en la transmisión de datos, con este modelo, todos los dispositivos de cómputo y telecomunicaciones podrán ser referenciados al modelo, para poder llevar a cabo una transferencia de información.

El Modelo OSI se representa mediante 7 Capas o Niveles las cuales se muestran en la Figura. 1.1.

Figura 1. 1 Modelo OSI

Capa 1 Física: Dentro de esta Capa se encuentran todas las características físicas, eléctricas y mecánicas que se encargan del procedimiento y funcionamiento, que lleva a activar, mantener y desactivar el enlace entre 2 sistemas que se están comunicando; en esta capa también se especifica el tipo de conectores, su forma, el número de patas que se van a utilizar, la lógica a utilizar (positiva o negativa), el ancho de bit, la potencia del transmisor, la sensibilidad del receptor, etc.

Las especificaciones de esta capa definen a redes de tipo PAN (Personal Área Network), MAN (Metropolitan Área Network), WAN (Wide Área Network), SAN (Storage Área Network), GAN (Global Área Network). La Unidad de Datos de Protocolo (PDU2) de esta capa, son los bits.

Capa 2 de Enlace de Datos: Esta Capa especifica diferentes características de red y protocolo, proporcionando tránsito confiable de extremo a extremo y para ello utiliza:

- Direccionamiento Físico: Es todo lo contrario de lo que se conoce como direccionamiento lógico o de red, se define por 48 bits siendo los primeros 24 el OUI(Organization User Identifier), y los 24 restantes son designados por el fabricante.
- Topología de Red: Existen dos topologías de red la Física y Lógica.
    - Física: Especifica la forma en la cual estará cableada la red, y el cómo estarán conectados cada uno de los dispositivos que pertenecen a la Red.
    - Lógica: Es la forma en la cual se estará transmitiendo la información por medio de la Red.
- Detección de Errores
- Secuencia de trama

[2] Protocol Data Unit Se utiliza para el intercambio entre unidades parejas, dentro de una capa del modelo OSI. Existen dos clases de PDUs: PDU de datos y PDU de control.

Esta Capa se encuentra dividida en dos subcapas: LLC (IEEE 802.2), MAC (802.3). La PDU en esta capa son las tramas.

Capa 3 de Red: Esta capa realiza la interconexión de dos dispositivos que se están comunicando, y pueden estar ubicados en lugares geográficamente diferentes, así mismo proporciona las rutas más adecuadas para la transmisión, por medio de enrutadores o mejor conocidos como enrutadores, los protocolos como IP (Internet Protocol), IPX(Internet Packet Exchange), Apple Talk basan su funcionamiento en esta capa, y se les conoce como protocolos enrutados (contienen la información del usuario). El PDU de esta capa son los paquetes.

Capa 4 de Transporte: Segmenta la información proveniente de las capas superiores, y la reensambla en una corriente de datos generada a nivel de host receptor. Inicia, controla y termina los circuitos virtuales, los cuales pueden ser permanentes (PVC) o conmutados (SVC). La unidad de datos de protocolo de esta capa, son los segmentos y los protocolos como TCP (Transmisión Control Protocol) y UDP (Used Datagram Protocol), basan su funcionamiento en esta capa, TCP es orientado a la conexión y UDP no se orienta a la conexión. Esto quiere decir que TCP manda la información y necesita un acuse de recibo, para saber que la información fue enviada correctamente y UDP solo envía la información, y no necesita que se le envié ningún paquete con la confirmación de recibo.

Capa 5 de Sesión: Inicia, administra y termina las sesiones entre dos sistemas que se están comunicando, además permite la sincronización de las mismas. La PDU de esta capa son los datos, y protocolos como NFS, Net Bios y Net BEUI basan su funcionamiento en este protocolo.

Capa 6 de Presentación: Esta capa se encarga de representar la información, de manera que todos los equipos que estén conectados a la red, a pesar de tener diferentes representaciones

internas, puedan reconocer la información enviada, en pocas palabras, esta capa cifra, codifica y si es necesario comprime la PDU que son los datos.

Capa 7 Aplicación: Esta capa provee de comunicación a las aplicaciones del usuario, su PDU son los datos y los protocolos que se encuentra en esta capa, por lo regular son aquellos que intercambian datos, como los de correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP).

1.2 Fidelidad Inalámbrica Wi-Fi (802.11)

La IEEE publicó en 1999 la norma 802.11, que dio lugar a la tecnología inalámbrica de redes locales, utilizada para el diseño de redes de datos inalámbricas, la cual está ubicada en la sub-capa MAC de la Capa de Enlace de datos, y a la Capa Física, esta norma define las características a seguir, que garantizan la compatibilidad entre dispositivos, cubriendo las características de una WLAN, para poder ser cerficados por la Wi-Fi Alliance (organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11), quien verifica el cumplimiento de los métodos de acceso, el tipo de modulación, la banda de frecuencia, el ancho de banda, velocidad, VER, etc. especificados por la IEEE.

El estándar 802.11 original, permite un ancho de banda de 1 a 2 Mbps, por lo que se ha modificado para optimizar el ancho de banda (incluyendo los estándares 802.11a, 802.11b y 802.11g "Estándares físicos",) o para especificar componentes de mejor manera, con el fin de garantizar mayor seguridad y compatibilidad [6]. La tabla 1.1 muestra las distintas modificaciones del estándar 802.11 y sus significados:

Nombre del estándar	Nombre / Año	Descripción
802.11a	Wifi5 1999	El estándar 802.11 (llamado WiFi 5) admite un ancho

		de banda superior (el rendimiento total máximo es de 54 Mbps, aunque en la práctica es de 30 Mpbs). El estándar 802.11a provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	Wifi 1999	El estándar 802.11 es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mpbs (6 Mpbs en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	Combinación del 802.11 y el 802.1d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d, que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Internacionalización 2001	El estándar 802.11d es un complemento del estándar 802.11, que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia, según lo que se permite en el país de origen del dispositivo.
802.11e	Mejora de la calidad del servicio 2005	El estándar 802.11e, está destinado a mejorar la calidad del servicio en el nivel de la *capa de enlace de datos*. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión, para permitir mejores transmisiones de audio y vídeo.

802.11f	Itinerancia 2003	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el *protocolo IAPP* que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro, mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como *itinerancia.*
802.11g	2003	El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps, pero de 30 Mpbs en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h	2003	El estándar *802.11h* tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la *h* de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.
802.11i	2004	El estándar *802.11i* está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el *AES* (estándar de cifrado avanzado), y puede cifrar

		transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11Ir		El estándar *802.11r* se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j	2004	El estándar *802.11j* es para la regulación japonesa lo que el 802.11h es para la regulación europea.

Tabla 1. 1 Estándar 802.11

De las modificaciones comerciales de la norma 802.11, son los llamados "estándares físicos" tabla 1.2, que cuentan con modos diferentes de operar, permitiéndoles alcanzar velocidades distintas en la transmisión de datos según sus rangos figura 1.2.

Estándar	Frecuencia	Velocidad	Rango
NO WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2,4 GHz	11 Mbit/s	100 m
WiFi G (802.11b)	2,4 GHz	54 Mbit/s	100 m

Tabla 1. 2 Resumen estándar 802.11

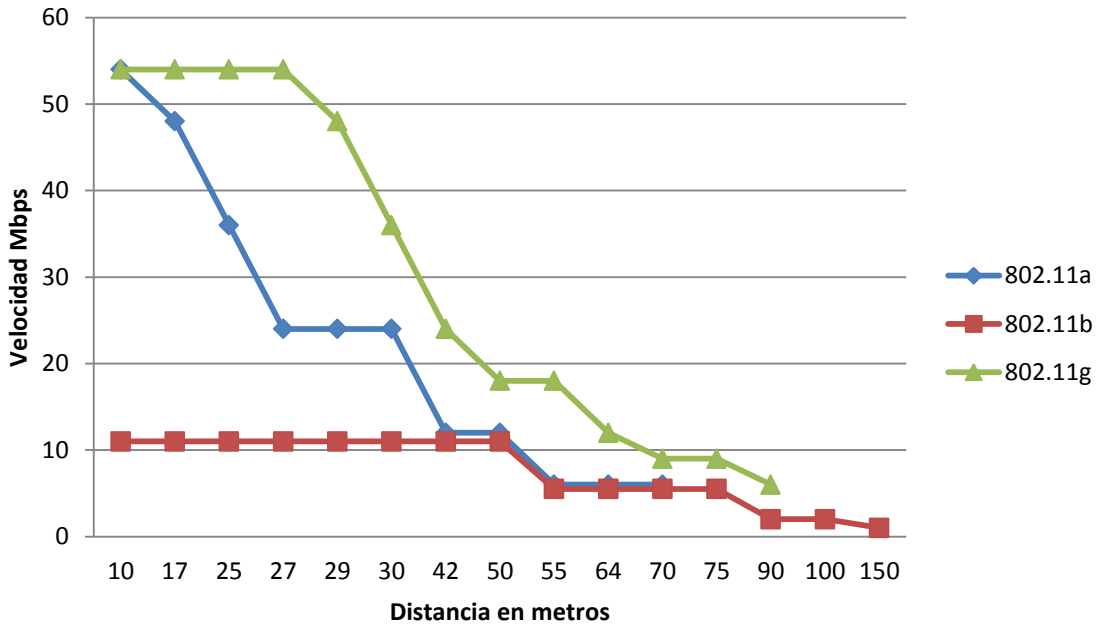


Figura 1. 2 Relación de transmisión de datos con relación al rango de las normas 802.11

1.3 Extensiones de la norma 802.11

Las extensiones más populares de la norma 802.11, son las mencionadas anteriormente en la tabla 1.2 de las que se dará una breve explicación a continuación:

1.3.1 Extensión 802.11a

Este estándar fue introducido al mismo tiempo que el 802.11b, pero la extensión 802.11a es usada con fines empresariales, está es la diferencia entre estas, ya que la 802.11b, se orientó hacia las redes caseras y redes para pequeños negocios. La norma 802.11a tiene un flujo de datos máximo de hasta 54 Mbps en teoría tabla 1.3, cinco veces el de la extensión 11b, en la práctica nos ofrece 22 Mbps y opera a una frecuencia de 5 GHz utilizando 8 canales no superpuestos, basándose en la modulación OFMD (*multiplexación por división de frecuencias ortogonales*), por lo que se produce la incompatibilidad entre dispositivos con

802.11a y 802.11b. Debido a que su costo es elevado, los equipos que trabajan con extensión 11a son menos populares que los de la norma 802.11b, esto es debido a que la banda de 5 GHz está regulada en algunos países.

Velocidad hipotética (en ambientes cerrados)	Rango
54 Mbit/s	10 m
48 Mbit/s	17 m
36 Mbit/s	25 m
24 Mbit/s	30 m
12 Mbit/s	50 m
6 Mbit/s	70 m

Tabla 1. 3 802.11a

1.3.2 Extensión 802.11b

Esta extensión fue introducida en 1999, como actualización del estándar 802.11 los equipos que operaban en esta norma, únicamente nos podían ofrecer una velocidad máxima de conexión de 2 Mbps. La norma 802.11b corrigió este problema, ya que su velocidad máxima de transferencia tiene un límite de 11 Mbps tabla 1.4, ya en la práctica podemos lograr velocidades de 2 a 5 Mbps, esto depende de diferentes factores, tales como: el número de usuarios, la distancia entre el emisor y el receptor, también otro factor importante, son los obstáculos y la interferencia causada por otros dispositivos.

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
11 Mbit/s	50 m	200 m

5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

Tabla 1. 4 802.11b

1.3.3 Extensión 802.11g

Surgió en el año 2003, siendo la evolución de la extensión 802.11b, la velocidad máxima de transferencia que nos ofrece es de 54 Mbps tabla 1.5, pero en la práctica puede ofrecer hasta 22 Mbps, utilizando el rango de frecuencia de 2.4 GHz con modulación OFDM, y al ser compatible con los equipos del estándar 802.11b, es posible que ésta sea reemplazada.

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

Tabla 1. 5 802.11g

1.4 Topologías wireless

Debe de quedar clara la diferencia entre lo que es topología y el modo de funcionamiento de los dispositivos Wi-Fi.

Refiriéndonos a la topología como la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida.

En el mundo Wireless existen dos topologías básicas:

- **Topología Ad-Hoc**. Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red Peer to Peer[3] o de igual a igual representado en la figura 1.3, para lo cual sólo vamos a necesitar el disponer de un SSID[4], igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo, más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí.

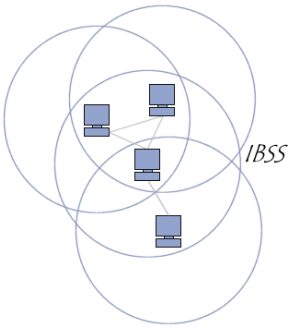


Figura 1. 3 Topología Ad-Hoc

[3] Es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.
[4] Service Set IDentifier, es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

- **Topología Infraestructura**, como se muestra en la figura 1.4 en el cual existe un nodo central (Punto de Acceso WiFi o PA) que sirve de enlace para todos los demás (Tarjetas de Red Wifi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del PA.

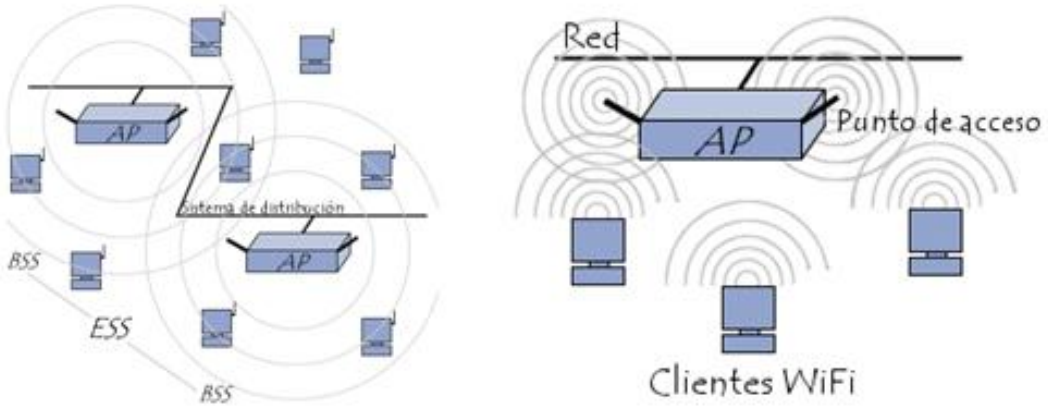


Figura 1. 4 Topología infraestructura

Un caso especial de topología de redes inalámbricas es el de las redes Mesh[5], que se verá más adelante.

Todos los dispositivos, independientemente ya sean Tarjetas de Red (TR) o Puntos de Acceso (PA), tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

[5] Redes acopladas, o redes de malla inalámbricas de infraestructura, para definirlas de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura.

- **Modo Managed**, es el modo en el que la TR se conecta al PA, para que éste último le sirva de "concentrador". La TR sólo se comunica con el PA.

- **Modo Master**. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los dispositivos con TR, si se dispone del firmware apropiado, o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento, nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como PA, realmente TR a los que se les ha añadido cierta funcionalidad extra vía firmware. Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro, y bajo una distribución especial de linux llamada LINUXAP - OPENAP.

Esta afirmación se ve confirmada, al descubrir que muchos PA en realidad lo que tienen en su interior, es una placa de circuitos integrados con un Firmware añadido a un adaptador PCMCIA (Personal Computer Memory Card International Association), en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como TR.

El acceso sin la necesidad de usar cables hace popular a las redes inalámbricas, pero eso genera un problema para la seguridad de este tipo de redes, debido a que cualquier persona con un equipo, que cuente con un dispositivo para conectarse inalámbricamente, que desde el exterior capte la señal del punto de acceso, será capaz de poder ingresar a nuestra red, con la posibilidad de navegar gratis en la Internet, emplear nuestra red como punto de ataque hacia otras redes y no ser detectado, robar información, entre muchas otras cosas

Para poder considerar que una red es segura, debemos tener en cuenta ciertos puntos:

- Las ondas de radio emitidas por nuestro punto de acceso, deben de estar delimitadas lo más exacto posible, de modo que esta señal únicamente sea captada en nuestra área de trabajo, esto es difícil de lograr, pero podemos hacer que sea lo más

aproximado posible, empleando antenas direccionales y configurando correctamente la potencia de transmisión de los puntos de acceso.

- Es necesario tener un mecanismo de autenticación, que permita al usuario verificar que se está conectando a la red correcta, este mecanismo también deberá checar que el usuario está autorizado para acceder a nuestra red.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red, puedan capturar datos mediante escucha pasiva.

Existen varios métodos que nos permiten lograr una configuración segura de una red inalámbrica, cada uno de estos métodos logra un nivel diferente de seguridad, y presenta ciertas ventajas y desventajas.

1.5 Encriptación

1.5.1 Clasificación de los Criptosistemas

Según el tratamiento del mensaje se dividen en:

- Cifrado en bloque (IDEA,AES,RSA*...)64 ó 128 bits.
- Cifrado en flujo (A5,RC4,SEAL...)cifrado bit a bit.

Según el tipo de claves se dividen en:

- Cifrado con clave secreta Sistemas simétricos
- Cifrado en clave pública sistemas asimétricos

(Sistemas como RSA no cifran por bloques propiamente tal: cifran un número único.)

1.5.1.1 Criptosistemas Simétricos

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y posteriormente descifrar un documento. El principal problema de seguridad reside en el

intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave. Es importante que dicha clave sea muy difícil de pronosticar ya que hoy en día existen programas que pueden descifrar claves rápidamente. Por ejemplo el algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 72 mil billones de claves posibles.

Actualmente ya existen computadoras especializadas que son capaces de probar todas ellas en cuestión de horas. Hoy por hoy se están utilizando ya claves de 128 bits que aumentan el "espectro" de claves posibles (2 elevado a 128) de forma que aunque se uniesen todas las computadoras existentes en estos momentos no lo conseguirían en miles de millones de años.

1.5.1.2 Criptosistemas Asimétricos

La criptografía de la clave asimétrica es la base de la moderna encriptación. La criptografía asimétrica utiliza dos claves complementarias llamadas clave privada y clave pública. Lo que está codificado con una clave privada necesita su correspondiente clave pública para ser descodificado. Y viceversa, lo codificado con una clave pública sólo puede ser descodificado con su clave privada.

Las claves privadas deben ser conocidas únicamente por su propietario, mientras que la correspondiente clave pública puede ser dada a conocer abiertamente.
Si A quiere enviar a B un mensaje de forma que sólo él pueda entenderlo, lo codificará con la clave pública de B. B utilizará su clave privada, que solo él tiene, para poder leerlo. Pero otra posible utilidad del sistema es garantizar la identidad del remitente. Si A envía a B un mensaje codificado con la clave privada de A, B necesitará la clave pública de A para descifrarlo. Es posible combinar ambos: A puede enviar a B un mensaje codificado dos

veces, con la clave privada de A y con la clave pública de B. Así se consigue garantizar la identidad del emisor y la confidencialidad.

La criptografía asimétrica está basada en la utilización de números primos muy grandes. Si multiplicamos entre sí dos números primos muy grandes, el resultado obtenido no puede descomponerse eficazmente, es decir, utilizando los métodos aritméticos más avanzados en los ordenadores más evolucionados sería necesario utilizar durante miles de millones de años tantos ordenadores como átomos existen en el universo. El proceso será más seguro cuanto mayor sea el tamaño de los números primos utilizados. Los protocolos modernos de encriptación tales como SET y PGP utilizan claves generadas con números primos de un tamaño tal que los hace completamente inexpugnables.

1.5.2.1 Requisitos de seguridad de un sistema

-El algoritmo de cifrado y descifrado deberá ser rápido y fiable.
-Debe ser posible transmitir ficheros por una línea de datos, almacenarlos o transferirlos.
- No debe existir retardo debido al cifrado o descifrado
- La seguridad del sistema deberá residir solamente en el secreto de una clave y no en las funciones de cifra
-La fortaleza del sistema se entenderá con la imposibilidad computacional (tiempo de cálculo en años que excede cualquier valor razonable), de romper la cifra o encontrar una clave secreta, a partir de otros datos de carácter público.

Conociendo el algoritmo de cifra, el criptoanalista intentará romper la cifra en uno de estos escenarios: contando únicamente con el criptograma, contando con el texto en claro conocido, eligiendo un texto claro, a partir de texto cifrado elegido: ataque por fuerza bruta, buscando todas las combinaciones posibles de las claves.

Un algoritmo de cifrado será fuerte si, conociendo su funcionamiento o código, conociendo el texto cifrado y conociendo el texto en claro, el ataque a la clave de cifra secreta es computacionalmente muy difícil, como ya anteriormente se mencionó.

1.5.2.2 Cifrado en bloque

- El mismo algoritmo de cifras se aplica a un bloque de información (grupo de caracteres, número de bytes, etc.) repetidas veces, usando la misma clave. El bloque de texto o información a cifrar, normalmente será de 64 ó 128 bits.

1.5.2.3 Cifrado en flujo.

- El algoritmo de cifra se aplica a un elemento de información (carácter) mediante un flujo de clave en teoría aleatoria y de mayor longitud que el mensaje. La cifra se hace carácter a carácter y de bit a bit.
- Comparativas: cifrado en bloque: ventajas; alta difusión de los elementos en el criptograma. Inmune: imposible introducir bloques extraños sin detectarlo.
- Desventajas: baja velocidad de cifrado al tener que leer antes el bloque completo, propenso a errores de cifra. Un error se propagará a todo el bloque.

- Cifrado en flujo: ventajas; alta velocidad de cifra al no tener en cuenta otros elementos, resistente de errores. La cifra es independiente en cada elemento.
- Desventajas; baja difusión de elementos en el criptograma, vulnerable pueden alterarse los elementos por separado.

Concluyendo, los sistemas de clave pública son muy rápidos al ejecutarse pero tienen un fácil intercambio de clave y cuentan con firma digital. Los sistemas de clave secreta son muy rápidos pero, carecen de lo anterior.

Para Cifrado de la información se recomienda usar: sistemas de clave secreta
Para firmas e intercambios de clave de sesión: sistema de clave pública.

1.5.3 Existen tres puntos importantes en la seguridad informática:

a) P1: El intruso del sistema utilizará el artilugio que haga más fácil su acceso al sistema y posteriormente el ataque.

Existirá una diversidad de frentes desde los que puede producirse un ataque, tanto internos como externos. Esto dificultará el análisis de riesgo ya que el delincuente aplicará la filosofía del ataque hacia el punto más débil: el equipo ò las personas.

b) P2: Los datos confidenciales deben protegerse sólo hasta que el secreto pierda su valor como tal.

Se habla por lo tanto de la caducidad del sistema de protección, tiempo en que debe perderse la confidencialidad o secreto de dato.
Esto nos llevará a la fortaleza del secreto de cifra.

c) P3: Las medidas de control se implementan para que tengan un comportamiento efectivo, eficiente, sean fáciles de usar y apropiadas al medio.

- Efectivo: que funcione en el momento oportuno.
- Eficiente: que optimice los recursos del sistema.
- Apropiadas: que pasen desapercibidas por el usuario.

Y lo más importante ningún sistema de control resulta efectivo hasta que debemos utilizarlo, al surgir la necesidad de aplicarlo. Junto con la concientización de los usuarios, esté será uno de los grandes problemas de la gestión de la seguridad informática.

1.6 Seguridad Informática

La ACM (Association for Computing Machinery), estableció el 30 de noviembre de 1988 como el día Internacional de la Seguridad en Cómputo, con la finalidad de incrementar el nivel de conciencia en los problemas relacionados a la seguridad informática, con el paso del tiempo este propósito se cumplió, y el interés mundial en la seguridad se ha estado incrementando, así como la tecnología informática, que busca asegurar los recursos de los sistemas informáticos de alguna empresa o institución, los cuales almacenan información que se procesa en computadoras, que pueden estar independientes o conectadas a una red, cableada o inalámbrica, las cuales pueden estar constituidas por un sistema de seguridad, de los cuales no existe uno que sea 100% seguro, sin embargo, se puede considerar a un sistema seguro, si cuenta con:

Confidencialidad: Asegura que la información sólo pueda ser utilizada por el usuario que se especifica.

Integridad: Consiste en proteger a la información de alteraciones y cambios.

Disponibilidad: Es la garantía de que la información se encuentre disponible dentro de las reglas especificadas.

1.6.1 Seguridad Inalámbrica

A finales del siglo XX la IEEE ratifica el estándar 802.11, que establece la comunicación para las redes inalámbricas, Wireless Local Area Network (WLAN), que se caracterizan por la transmisión y recepción de información mediante ondas electromagnéticas, y no por medios de transmisión guiados. Dado que la tecnología inalámbrica no puede ser restringida a un espacio determinado, se vuelve más cómoda, accesible, práctica, rápida y relativamente fácil de implementar en la actualidad, siendo cada vez más utilizada por diversos equipos informáticos organizadores (PDA), consola de videojuegos e incluso impresoras, que ocupan esta tecnología para facilitar su conexión, sin embargo, los riegos en la trasferencia de

información aumentan. Las más usadas actualmente son Bluetooth[6] y las redes Wi-Fi (Wireless Fidelity - Fidelidad no cables).

Pero la problemática principal en este tipo de redes es la dificultad de limitar el medio y controlar el área de transmisión de los ordenadores, que decidimos formen parte de la red, y es por eso que se recomienda colocar los puntos de acceso, tan lejos sea posible de las paredes, ventanas exteriores, probar la eficiencia de señal y cerciorarse de la conexión de los usuarios autorizados, de esta manera los problemas que se presentan con las redes inalámbricas, están relacionados con el hecho de que personas desconocidas sean capaces de tener acceso a una red privada.

1.6.1.1 Filtrado de direcciones físicas (MAC)

Es una medida de seguridad relacionada con la capa de enlace de datos (capa 2) del modelo OSI, que se encarga de restringir el acceso a las interfaces no autorizadas a la red, mediante la creación de una tabla de datos en cada uno de los puntos de acceso de la red inalámbrica. Esta tabla contiene las direcciones físicas, conocidas como MAC (Media Access Control address), de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Toda tarjeta de red posee una dirección MAC única, al ser única, deberá estar registrada en nuestra tabla de datos antes creada, para poder ingresar a la red, con esto se logra autenticar el equipo.

La principal ventaja de este método es su sencillez, por lo que se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen poco efectivo para uso en redes medianas o grandes:

[6] Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.

- Es poco práctico debido a que si se quiere autorizar o dar de baja un equipo, es necesario editar la tabla de direcciones de todos los puntos de acceso, y si ésta es demasiado grande, se volverá inmanejable.

- Debido a que el formato de las direcciones MAC, normalmente se escriben como 6 bytes en Hexadecimal, se pueden cometer errores en la manipulación de las listas.

Ya que las direcciones MAC viajan sin cifrar por el aire, un atacante podría capturar direcciones MAC, de tarjetas matriculadas en la red empleando un sniffer[7], para luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, de este modo, el atacante puede hacerse pasar por un cliente válido dentro de nuestra red.

En caso de robo de un equipo, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso, el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Los pasos que sigue una estación solicitante, es ubicar el PA, a continuación, solicita la autenticación, que puede ser concedida o denegada por el PA de acuerdo a los filtros y medidas de seguridad. Una vez que se ha autenticado la estación solicitante, procede a solicitar la asociación al PA como se representa en la figura 1.5, las redes IBSS[8] únicamente llegan al estado 2, debido a que no cuentan con un punto de acceso, en cuanto un filtrado MAC se puede realizar en el PA, o en el servidor.

[7] Programa para monitorear y analizar el tráfico de datos en una red, éste capta los datos transmitidos en la red
[8] Independent basic service set, también conocido como modo ad-hoc, se ha diseñado para facilitar las conexiones punto a punto.

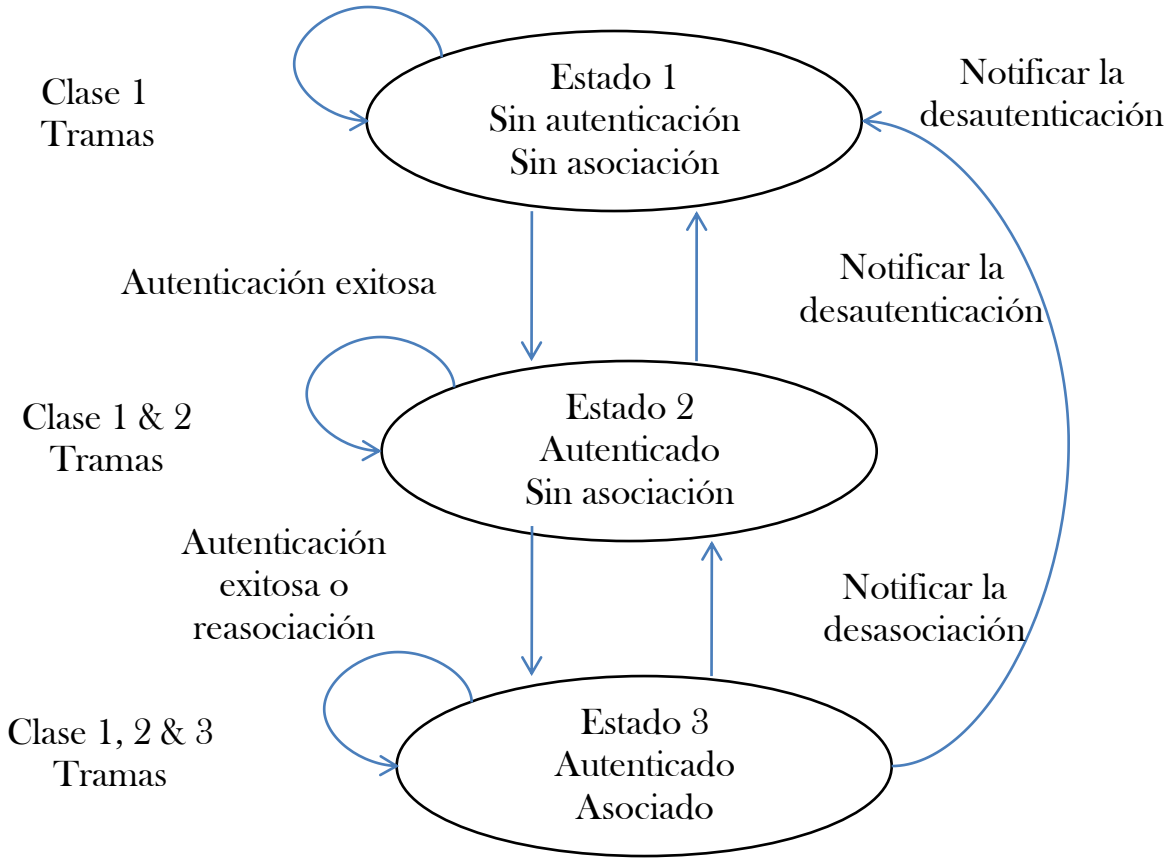


Figura 1. 5 Diagrama de Estado para transmisión de paquetes

1.6.1.2 Privacidad Equivalente a red Cableada (WEP)

Este algoritmo forma parte de la especificación 802.11, diseñado con el fin de otorgar un cierto grado de privacidad y con ello proteger los datos, que se transmiten en una conexión inalámbrica mediante compresión y cifrado de trama de datos, siendo el primer mecanismo de seguridad implementado, aunque no se puede comparar con protocolos de redes más seguros como IPsec, que se implementan en la creación de Virtual Private Networks (VPN).

El algoritmo WEP opera en el nivel 2 del modelo OSI, y es compatible por la gran mayoría

de fabricantes de soluciones inalámbricas. . WEP utiliza una clave secreta, utilizada para el cifrado de los paquetes antes de su retransmisión. El algoritmo utilizado para el cifrado es RC4 con claves de 64 bits o 128 bits. Por defecto, WEP está deshabilitado.
El protocolo WEP consiste en establecer una clave secreta de 40 a 128 bits, la cual se debe declarar tanto en el punto de acceso, como en los equipos cliente. La clave se usa para crear un número que parece aleatorio y de la misma longitud que la trama de datos.

Cada transmisión de datos se cifra de la siguiente manera. Al utilizar el número que parece aleatorio como una "máscara", se usa una operación "O excluyente", para combinar la trama y el número que parece aleatorio en un flujo de datos cifrado.

La clave de sesión que comparten todas las estaciones es estática, es decir, que para poner en funcionamiento un número elevado de estaciones inalámbricas, éstas deben configurarse con la misma clave de sesión. Por lo tanto, con sólo saber la clave se pueden descifrar las señales. Además, para la inicialización se usan sólo 24 bits de la clave, lo que implica que sólo 40 de 64 bits o 104 de 128 bits de la clave, se utilizan realmente para el cifrado.

El algoritmo WEP, resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro:
La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave, y pueda intentar un ataque por fuerza bruta.

WEP no ofrece servicio de autenticación. El usuario no puede autenticar a la red, ni la red puede ver si el equipo puede tener acceso a la red, tan solo basta con que el equipo móvil y el punto de acceso compartan la clave WEP, para que la comunicación pueda llevarse a cabo.

WEP no es suficiente para garantizar verdaderamente la privacidad de los datos. Sin embargo, se recomienda utilizar al menos una clave WEP de 128 bits, para garantizar un nivel de privacidad mínimo. Esto puede reducir el riesgo de una intrusión en un 90 por ciento.

1.6.1.4 Acceso Protegido Wi-Fi (WPA)

Es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para redes inalámbricas), en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejora el cifrado de los datos y ofrece un mecanismo de autenticación. Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Dicho protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama, con respecto a WEP.

El mecanismo de autenticación usado en WPA, emplea 802.1X [5]. Según la complejidad de la red, un punto de acceso compatible con WPA, puede operar en dos modalidades:
Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1X para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

Modalidad de red casera: WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez

logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. La norma WPA fue introducida en abril de 2003 [7].

Capítulo 2 "Autenticación"

2.1 Introducción de Capítulo

La necesidad de las redes empresariales e institucionales, en la realización de consultas de información publicadas de forma masiva, a través de Internet, el cual constituye un medio adecuado para facilitar el acceso, de forma eficaz y rápida, a esa gran cantidad de información que cuenta de una disponibilidad global, así como la viabilidad de crear un canal de comunicaciones bidireccional, el cual aparte de permitir la captura de información de servidores web, ftp, etc. les aumenta la posibilidad de realizar transferencias punto a punto, ya sea por medio de formularios o simplemente archivos de diferente nomenclatura de carácter privado, representan de la misma forma un método eficiente de proporcionar datos personales e información privada desde cualquier lugar del mundo.

Lo que da un aviso para evitar el suministro de información confidencial por Internet, ni el almacenamiento en servidores, mientras no se cuente con algún tipo de protección, en específico lo referente a datos financieros, comerciales críticos u otra información confidencial, debido a que existe la posibilidad de escuchar los paquetes circulantes en la red (Internet), por lo que la encriptación se vuelve muy importante en la transferencia de información, pero el hecho de que se realice la transferencia cifrada, genera problemas de autenticación en la comunicación. A medida que aumenta la información públicamente disponible y trasportada vía Internet, también lo hace la necesidad de protegerla, cuidándola de algún tipo de captura o intromisión.

De tal manera que se busca alcanzar la globalización en el acceso a la información, sin dejar de lado su seguridad, brindando una protección a la confidencialidad e integridad, tanto de

los datos que se pudieran encontrar en servidores, como de aquellos que son trasportados dentro del esquema cliente-servidor.

Para esto es necesario formar grupos de autorización de acceso, para gestionar de manera más excluyente, para evitar una gran inestabilidad en las redes, con distintos criterios como: dirección IP o nombre de huésped, suprimiendo duplicaciones, autenticación básica, certificados digitales, etc. También la implementación de SSL [10] o SSH [9], para la protección del tráfico de servidores, de manera que los datos confidenciales que viajan en el esquema cliente-servidor, resulten protegidos a través de subredes o segmentos de red.

Junto con la creciente tendencia que permite tener acceso a los sistemas de información, casi desde cualquier lugar, se necesita que exista una infraestructura de seguridad robusta para poder tener una plena confianza en aquellas conexiones que interactúan con medios susceptibles a cualquier tipo de ataque y así disminuir el riego en la transmisión de información.

Por lo que podemos determinar que los riesgos, en términos de seguridad, se caracterizan mediante las capacidades que permiten anticipar, resistir y recuperarse del impacto de una amenaza, respecto al grado de exposición siendo esto la vulnerabilidad de nuestro sistema, a lo que debemos aumentar las amenaza, que son todas las acciones que representa probabilidad de ocurrencia de un evento potencialmente nocivo, por último, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse, no sólo son soluciones técnicas, sino también involucran la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo, teniendo una perspectiva de todos los

posibles ataques, para conocer la mejor forma de reducir el riesgo de intrusiones y buscar el método de autenticación más adecuado.

2.2 Panorama de la Autenticación

La autenticación es el proceso mediante el cual los sistemas homólogos involucrados (emisor-receptor) en un canal de transmisión, identifican, verifican y aseguran la identidad de usuarios, dispositivos o sistemas legítimamente involucrados de los no autorizados en una transacción, garantizando la integridad de la información, y determinando la validez de la pareja de correlación (peer-entity) u origen de la misma, determinando especificaciones o características de una acción, previniendo transmisiones fraudulentas. Siendo un proceso en donde se busca verificar la identidad digital del remitente de una comunicación, como una petición para conectarse, es un modo de asegurar que el usuario que intenta realizar funciones en un sistema, es de hecho el usuario que tiene la autorización.

La autenticación en términos de seguridad informática, es uno de los servicios con los que debe contar un sistema seguro, considerándose uno de los tres pasos de la familia de protocolos AAA (Autenticación, Autorización y Auditoria).

La Autorización es el proceso por el cual la red de datos permite al usuario identificado acceder a determinados recursos y realizar ciertas operaciones. Una vez autenticado, se procede a verificar qué tareas tiene autorizadas dentro del sistema. Cada vez que el usuario autorizados o no, lleva a cabo una acción, queda registrada para poder realizar una Auditoría en caso de que se produzca algún incidente.

Debe tenerse bien presente que la autenticación, precede a la autorización. Para distinguirlas existen unas notaciones de taquigrafía, que son: A1 y A2 respectivamente aunque, también existen los términos AuthN y AuthZ, que son usados en algunas comunidades.

La autenticación está diseñada como un mecanismo de control de acceso, para proteger contra conexiones fraudulentas. En caso de que el proceso no se llevara a cabo, existirá la posibilidad de que una entidad asuma un modo promiscuo, comprometiendo la privacidad y la integridad de la información.

2.2.1 Métodos de Autentificación de red

Los métodos de autenticación presentan una gran demanda en los sistemas de llave pública, debido que en la actualidad, ya no se puede tener la confiabilidad de transmitir una llave de cifrado, asegurando que las entidades autorizadas sean las que en realidad se hayan encontrado, y no un adversario activo como los escuchas del medio (sniffer), que puede burlar el modelo sin romper el criptosistema. Por éste y otros motivos, se necesita reforzar la autenticación de las llaves públicas, para obtener una certificación de entidades homologadas.

Las reglas establecidas en una autentificación, son todas las limitaciones o filtrajes de tipos de datos, y con base a éstas, se definen las listas de métodos de autenticación, los cuales definen requisitos de comprobación de identidad en las redes, a las que se aplican las reglas asociadas. Estos métodos normalmente utilizan protocolos de autenticación, que se define durante el establecimiento de la conexión. Para que una comunicación sea posible, es necesario que los interlocutores cuenten, con mínimo, un método de autenticación común, y para aumentar la posibilidad de encontrar un método común para las entidades, será necesario crear varios métodos de autenticación, con esto aseguramos una mayor seguridad.

Independientemente de la cantidad de métodos de autenticación que se configuren en los equipos, solo se podrá utilizar uno entre las entidades homólogas. Para lo que es necesaria la configuración de la lista de métodos de autenticación, si fueron aplicadas varias reglas a los dispositivos relacionados a la red. (Por ejemplo, si una regla entre un par de equipos especifica únicamente el protocolo Kerberos para la autenticación, y sólo filtra datos de TCP,

mientras que otra regla especifica únicamente certificados para la autenticación, y sólo filtra datos de UDP, la autenticación no será posible.)

2.3 Autenticación Centralizada

La seguridad depende de mucho más que la sola encriptación. Es necesario disponer de un sólido mecanismo de autenticación, que, además de garantizar la identidad de los usuarios y estaciones de trabajo, ayude a escalar sin temores los entornos inalámbricos 802.11. La nueva norma 802.1X [11, ayuda en la tarea proporcionando un mecanismo estándar para autenticar centralmente estaciones y usuarios, simplificando así el soporte de cientos o miles de puestos.

Figura 2. 1 Procedimiento de autenticación

802.1X será además lo suficientemente flexible para soportar distintos algoritmos de autenticación, y, como estándar abierto, facilitará a los fabricantes el desarrollo de innovaciones y mejoras complementarias. Básicamente, 802.1X se apoya en el protocolo de autenticación EAP (Extensible Authentication Protocol), vinculándolo al medio físico de la red. Para ello, los mensajes EAP son encapsulados en mensajes 802.1X, creando lo que se conoce como EAP over LAN[9].

[9] Ofrece un marco eficaz para la autenticación y control de tráfico de usuarios a una red protegida, así como dinámicamente variables claves de cifrado. EAPOL es un estándar para pasar protocolo de autenticación extensible (EAP) sobre un cable o LAN inalámbrica.

2.3.1 Esquema Funcional

La autenticación 802.1X para WLAN, se basa en tres componentes principales: el solicitante (generalmente el software cliente), el autenticador (el punto de acceso) y el servidor de autenticación (por lo general, pero no necesariamente, un servidor RADIUS - Remote Authentication Dial-In User Service).

Cuando un cliente intenta conectarse con el punto de acceso, éste le detecta y activa su puerto para proceder a la autenticación, al tiempo que no le autoriza transmitir algún tipo de tráfico, salvo el relacionado con 802.1X. El cliente entonces, utilizando EAP, envía un mensaje de inicio al punto de acceso, que, al recibirlo, devuelve un mensaje de petición de identidad. El cliente le remite acto seguido, un mensaje de respuesta con su identidad, que será pasado al servidor de autenticación. El resultado es un paquete de aceptación o rechazo, que el servidor envía al punto de acceso, y cuando es recibido, vuelve a autorizar al puerto del cliente a que comience la transmisión.

Con este simple esquema centralizado de funcionamiento, 802.1X tiene el potencial de simplificar la gestión de la seguridad de grandes despliegues inalámbricos. Pero hay que recordar que la autenticación no es la única pieza del rompecabezas, de la seguridad de los entornos 802.11. Su utilización requiére obviamente la presencia de un algoritmo de autenticación, y de un sistema de encriptación de datos. Juntos, los tres componentes, ofrecen a los administradores de redes un modo efectivo de proporcionar servicios de red móviles, flexibles, gestionables y escalables.

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

El marco de trabajo AAA consiste en tres componentes fundamentales: el servidor AAA, los módulos específicos a las aplicaciones (ASM[10]) 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 acceder información de auditoría específica de un usuario.

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

2.3.2 Descripción de la Norma 802.1X

802.1X es una Norma de control de acceso y autenticación, basado en la arquitectura cliente/servidor, la cual restringe la conexión de equipos no autorizados a una red. En un principio dicha Norma fue creada por la IEEE, para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad, ya son compatibles con ésta Norma.

Se ilustra en la figura 2.2 la estructura de la norma 802.1X que involucra tres participantes:

[10] Application Security Manager

- **El solicitante**, o equipo del cliente, que desea conectarse con la red.
- **El servidor de Autorización y autenticación**, que contiene toda la información necesaria, para saber cuáles equipos o usuarios están autorizados para acceder a la red. 802.1X, fue diseñado para emplear servidores RADIUS. Estos servidores, fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica, pero debido a su popularidad, se optó por emplearlos también para autenticación en las LAN.
- **El autenticador**, que es el equipo de red (switch, enrutador, servidor), que recibe la conexión del solicitante. El autenticador actúa como intermediario entre el solicitante y el servidor de autenticación, y solamente permite el acceso del solicitante a la red, cuando el servidor de autenticación así lo autoriza, y se muestran en la Figura 2.2.

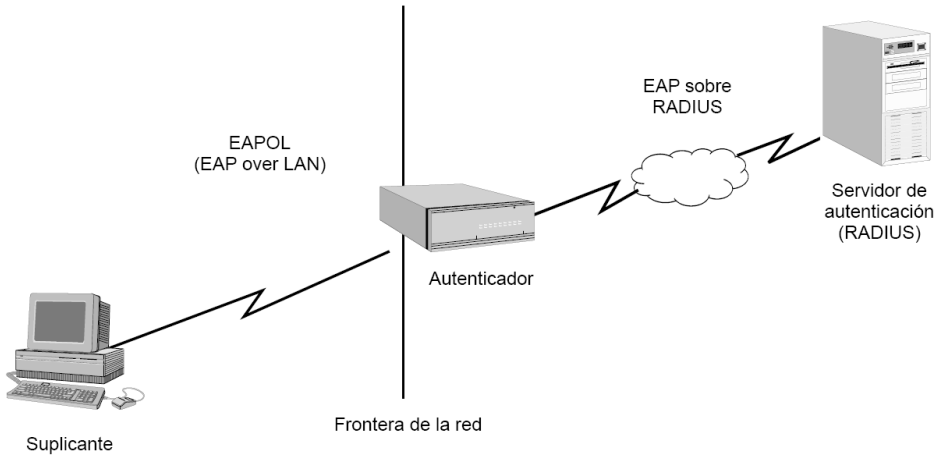


Figura 2. 2 Estructura 802.1X

2.3.4 Funcionamiento de la Norma 802.1X

Se encarga del control para acceder a la red, por medio de habilitar e inhabilitar un puerto físico de la red, este tipo de autenticación es denominado puerto base [8]. El cual está determinado por tres componentes, el solicitante, autentificador y el servidor de autenticación, como se observa en la Figura 2.3.

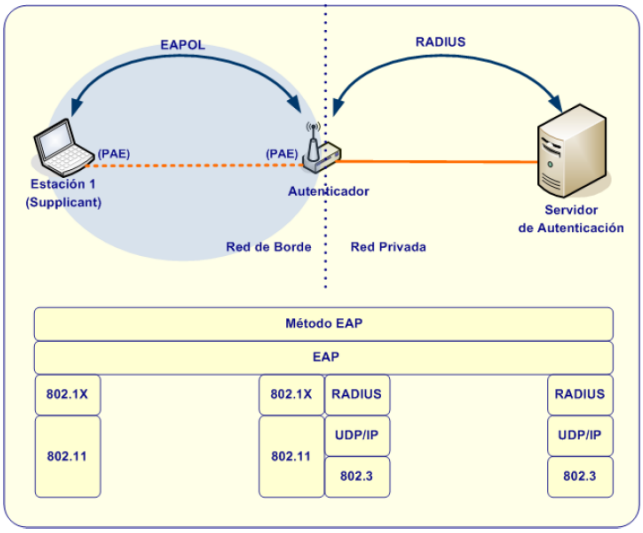


Figura 2. 3 Funcionamiento 802.1X

En la especificación 802.1X el solicitante y el autentificador son considerandos Entidades de Autentificación por Puerto (PAEs), los puertos no autorizados evitan que el usuario pueda acceder a la red, restringiendo únicamente al envío de marcos de autenticación EAPOL (EAP over LAN) inicializando este proceso antes de permitir paso de tráfico de datos.

2.3.5 Certificados Digitales

Un certificado digital es un archivo, mediante el cual un tercero de confianza, garantiza la vinculación entre la identidad del usuario y su clave pública, la cual se refiere a una combinación de hardware, software, políticas y procedimientos de seguridad, que permiten la ejecución de garantías de operaciones criptográficas, como: cifrado, la firma digital o el no repudio en transacciones electrónicas.

La certificación se lleva a cabo mediante empresas tales como VeriSign[11] o CAcert[12], que son las más grandes en este campo, la primera de ellas es de origen norte americano y la segunda es australiana.

2.3.6 Claves públicas

La clave pública es administrada por la autoridad certificante y es parte del certificado emitido, PKI por sus siglas en inglés (public key infrastructure), la tecnología PKI [12], permite a los usuarios autenticarse frente a otros usuarios o servidores y viceversa, y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios), para cifrar y descifrar mensajes.

En una operación criptográfica que use infraestructura PKI, intervienen conceptualmente como mínimo las siguientes partes:

- Un usuario iniciador de la operación
- Un sistema de servidores que dan fe de la ocurrencia de la operación, y garantizan la validez de los certificados implicados en la operación
- Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser el mismo)

Existen varios tipos de certificados:

- Certificados personales, que acredita la identidad del titular
- Certificados de pertenencia a empresa, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja
- Certificado de representante, que además de la pertenencia a empresa, acredita también los poderes de representación que el titular tiene sobre la misma

[11] Es una empresa de seguridad informática famosa por ser una autoridad de certificación reconocida mundialmente. Emite certificados digitales RSA para su uso en las transmisiones seguras por SSL, principalmente para la protección de sitios en Internet en su acceso por https.

[12] Es una Autoridad de certificación administrada por la comunidad que otorga gratuitamente certificados de clave pública.

La forma más común de certificado actualmente es la definida por ITU-T X.509 (que también es una infraestructura de llave pública), aunque ésta no es la única forma que pueden tomar los certificados, ésta por ejemplo: PGP entre otras.

2.3.7 Procedimiento de autenticación en una red

Actualmente existen tres versiones de x.509, v1, v2 y v3.
El x.509 da tres procedimientos alternativos para la autenticación en peticiones de servicio, mensajes o envío de información.

Autenticación en una vía:

- El mensaje mínimo está formado por el testigo y la marca de tiempo. Puede además contener una clave de sesión temporal entre A y B.

El envío de información de A asía B, define:

- La identidad de A y que el mensaje fue generado por A
- Que el mensaje estaba dirigido a B
- La integridad y unicidad del mensaje

Autenticación de dos vías

- Consiste en el envío de información de A a B, y a continuación de B a A. Define además de los anteriores:
- La identidad de B, y que el mensaje fue generado por B
- Que el mensaje estaba dirigido a A
- La integridad y unicidad del segundo mensaje

Autenticación de tres vías

La autentificación de tres vías se emplea cuando el destino y el iniciador no tienen relojes sincronizados, o no desean confiar en los relojes. Además de pasar por la autentificación de dos vías, el iniciador envía entonces una respuesta a la respuesta del destino, incluyendo el nuevo testigo contenido en la respuesta original. Después de verificar que los valores del testigo son idénticos, ya no hay necesidad de verificar las marcas de tiempo.

2.3.8 Firma digital

Los datos emitidos por el certificante "CA" (por sus siglas en inglés Certificate Authoritym) están firmados por la función HASH, MD5 y RSA.

Una firma digital es el equivalente de la firma convencional, en el sentido de que es un añadido al final del mensaje, conforme se está de acuerdo con lo que allí se dice. Formalmente, una firma digital es una transformación de un mensaje de forma que cualquier persona con conocimiento del mensaje y de la clave pública del firmante pueda comprobar que dicha transformación ha sido realizada realmente por el firmante.

Aparte de los datos del emisor y del propietario del certificado, éste puede contener información referente a las limitaciones que se hayan establecido para su uso: e-mail, www, etc. Un ejemplo de certificado puede ser el siguiente, depende del navegador que manejemos, en este caso utilizamos un navegador Netscape y recibimos un certificado:

La información "Encryption: Highest Grade (RC4 with 128-bit secret key)" no tiene nada que ver con el certificado presentado por el servidor, sólo depende del navegador utilizado y del servidor, a distinto navegador distinto grado de cifrado. Ya que de menos de 128 bits, es más fácil en descifrar y los navegadores como Explorer v8 o Mozzila Firefox v3, son más seguros que algunos otros. Actualmente aún se está desarrollando el marco legal que regule el reconocimiento de la validez legal de las firmas digitales, y cuáles han de ser los requerimientos mínimos, que han de reunir las autoridades certificadoras para ser reconocidas como tales.

Capítulo 3 "Seguridad en Linux"

3.1 Sistema Operativo Linux (Fedora)

Linux es el término que se utiliza al referirse a la combinación de núcleo o Kernel de un sistema operativo libre, similar a Unix, desarrollado gracias a contribuciones provenientes de todo el mundo, Linux es uno de los mejores ejemplos de software libre, cuyos desarrolladores originales siguieron la filosofía de ese movimiento.

Linux fue creado por un estudiante del MIT en 1991, muy pronto otras comunidades de desarrolladores en todo el mundo contribuyeron con este proyecto.

Fedora es una distribución Linux con gran parte de librerías y APIS donadas por el proyecto "Red Hat", Fedora [14] que se mantiene gracias a una comunidad internacional de ingenieros, diseñadores gráficos y usuarios que informan de fallos y prueban nuevas tecnologías.
El proyecto Fedora fue creado a finales del 2003, cuando Red Hat Linux fue descontinuado.

El proyecto Fedora se distribuye actualmente de muchas formas.

- Fedora DVD. Un dvd con todos los paquetes disponibles
- medios vivos (live cd's) . imágenes de cd o dvd, que también pueden ser instalados en unidades usb.
- Imágenes de Cd o USB. Que pueden ser instalados en servidores http o ftp.
- Imágenes de rescate. Cuando el sistema operativo falla, de alguna manera se utiliza este cd.

Es el administrador de paquetes del sistema Yum (Yellow dog updater modified) que es utilizado en modo consola para ejecutar una instalación, las interfaces gráficas como el pirut o pup, presentan visualizaciones cuando existen actualizaciones disponibles. Apt-rpm es una alternativa a yum, y puede ser familiar para aquellas personas que hayan trabajado antes con Debían o Ubuntu.

En las primeras 6 versiones existían dos repositorios principales, fedora core y fedora extras, dónde:
Fedora core: Era la distribución donde estaban todos los paquetes básicos del sistema operativo.
Fedora extras.- Este solo era mantenido y administrado por la comunidad de fedora

A partir de fedora 7, estos dos repositorios se unieron desde que la distribución abandonó el terminó core de su nombre.

Actualmente, Fedora recomienda (o utiliza) únicamente aquellos repositorios que disponen de paquetes de software libre, o código abierto, sin problemas de patentes. Ejemplos de paquetes problemáticos a nivel de patentes, son determinados codecs de audio, módulos NTFS drivers de ATI y NVIDIA.

Lanzamientos:

Fedora core (Yarrow): 6 de noviembre del 2003

Fedora core 2 (tettnang): lanzado el 18 de mayo del 2004, fue descontinuado por problemas de alteraciones, ya que el sistema cambiaba casi totalmente la forma de trabajar

Fedora core 3 (heidelberg): lanzado el 8 de noviembre del 2004 , esta fue la primera versión que incluyó el navegador Mozilla Firefox

Fedora core 4 (stentz): liberado el 13 de junio del 2005, además incluía la última versión de open office.

Fedora core 5 (bordeux): liberado el 20 de marzo del 2006, fue la primera versión en incluir mono[13].

Fedora core 6 (zod): lanzada el 24 de octubre del 2006, incluye el navegador web mozilla firefox 1.15.

Fedora 7 liberada el 31 de marzo del 2007.

Fedora 8 (werewolf) liberada el 8 de noviembre del 2007.

Fedora 12 (sulphur) liberada el 31 de mayo del 2008, es en la distribución donde se trabajara.

3.2 Mecanismos de seguridad en Fedora

La Arquitectura de seguridad SELinux ("Security-Enhanced Linux"), se destaca entre las características de seguridad de Fedora, pues implementa una gran variedad de políticas de seguridad, incluyendo control de acceso obligatorio (MAC "Mandatory Access Control"), a través de los Módulos de Seguridad de Linux que están en el núcleo Linux del sistema.

La distribución Fedora, está como líder de las distribuciones que incorporan SELinux, habiéndolo introducido en Fedora Core 2. Sin embargo, lo desactivó como elemento predeterminado, pues alteraba radicalmente la forma en que el sistema operativo funcionaba,

[13] Es el nombre de un proyecto de código abierto iniciado por Ximian y actualmente impulsado por Novell (tras la adquisición de Ximian) para crear un grupo de herramientas libres, basadas en GNU/Linux y compatibles con .NET según lo especificado por el ECMA.

pero fue activada por defecto en Fedora Core 3 e introducía una política menos estricta. Fedora también tiene métodos propios para prevenir la sobrecarga del buffer, y la utilización de rootkits[14].

Específicamente en Fedora 12: Continúa mejorando sus muchas características de seguridad proactivas.

Soporte para contraseñas SHA-256 y SHA-512
El paquete glibc en Fedora 8, tenía soporte para contraseñas usando el hashing SHA-256 y SHA-512. Antes, solamente DES y MD5 estaban disponibles. Estas herramientas han sido extendidas en Fedora 12. Ahora hay soporte para el hashing de contraseñas, usando las funciones de hash SHA-256 y SHA-512.

Para cambiar a SHA-256 o SHA-512 en un sistema instalado, se requiere de unos sencillos comandos.

En Fedora 12, el comportamiento predeterminado del cortafuego cambió. No hay puertos abiertos por defecto, excepto el SSH (22), que está abierto por Anaconda (Instalador de Fedora).

3.3 Servidores en Linux

Fedora es una de las distribuciones más estables y fáciles de configurar algún servicio de red, tal como lo son los servidores.

[14] Es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder otros programas.

Dentro de Fedora tenemos una variedad extensa de servidores, ya sea de servicios, soporte de red o de seguridad, Dentro de este último grupo Fedora cuenta con freeRADIUS [13], solo habrá que habilitarlo, ya que viene con la instalación inicial.

3.4 Protocolo FreeRADIUS

Por su acrónimo en inglés (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**erver.)* Es un protocolo de autenticación y autorización para aplicaciones y servicios de red, que utiliza el esquema cliente / servidor. Se decidió utilizar Servidor RADIUS de autenticación por su popularidad y fácil configuración, siendo RADIUS la base en la que planeo CISCO, la creación de TACACS, la cual comercializa la empresa a costos algo elevados, mientras que RADIUS se puede conseguir en software libre.

Originalmente RADIUS fue desarrollado por Livingston Enterprises, después evoluciona a RADIUS Cistron, actualmente existen muchas distribuciones de RADIUS, tanto comerciales como de código abierto, una de ellas es FreeRADIUS, que es la distribución con la que haremos pruebas en Fedora 12 y en Windows server 2003.
Antes de comenzar la explicación del funcionamiento, es conveniente resaltar que existen alrededor de 18 RFC's acerca de RADIUS. Nosotros nos basaremos solamente en uno, que es el más completo y que describe el funcionamiento de este protocolo, el RFC 2865.
RADIUS inicialmente trabajaba en el puerto UDP 1645, pero entraba en conflicto con el servicio de "Datametrics", así que se le reasignaron los puertos UDP 1812 y 1813.

3.4.1 Funcionamiento de RADIUS

"Para administrar y restringir el acceso a cualquier red, y los diferentes servicios que ésta pueda otorgar, podemos crear una base de datos de usuarios, que permite la autenticación (verificación nombre de usuario y contraseña)".

El servidor RADIUS contiene toda la información de los usuarios, almacenando sus contraseñas y perfiles, el cliente es el encargado de pasar las peticiones de conexión del usuario al servidor, para que este procese toda la información y proceda con el cliente, diciéndole si este usuario está o no registrado.

El Cliente puede ser un NAS (servidor de acceso a la red), que bien podría ser cualquier enrutador que soporte RADIUS, en nuestro caso específico, sería el enrutador Linksys modelo WRT54G2, éste actúa en dependencia de la respuesta del servidor.

Un servidor RADIUS puede actuar como cliente proxy, para otro tipo de servidores u otros servidores de autenticación.

3.4.2 Atributos de RADIUS

Entre el cliente y el servidor se intercambian paquetes fundamentales de 6 tipos:

- Access-request: paquete de solicitud de conexión enviado por el cliente al servidor
- Access-reject: paquete que se envía del servidor al cliente, ordenándole que no establezca conexión para el usuario en cuestión, puesto que la autenticación falló
- Access-accept : paquete de respuesta del servidor al cliente, para que establezca conexión con el cliente en cuestión, dado que la autenticación fue satisfactoria
- Accounting-request : paquete de solicitud, que es enviado del cliente al servidor para marcar el inicio o fin del acounting (contabilidad)
- Access-challenge: paquete enviado por el servidor, cuando los datos enviados por el cliente no son suficientes. El servidor necesita tener más información del usuario, ya sea para autenticar o para saber qué tipo de servicio le va a dar al usuario

- Accounting-response: Cuando el servidor recibe un "accounting-request", el servidor guarda la información necesaria para establecer la conexión. Si este proceso tiene lugar de forma satisfactoria, le envía al cliente un paquete "acounting-response"

La información que se intercambia en cada paquete, son pares atributo-valor. Entre los atributos que se envían en los paquetes de "Access –request", están nombre del usuario, contraseña etc. Estos atributos son checados por el servidor para determinar si son valídos o no. En caso de ser correctos, el servidor envía un paquete "access- accept"

3.4.3 Seguridad con RADIUS

La comunicación entre cliente y servidor es autenticada mediante una clave compartida, que es establecida por el administrador, y que debe ser la misma en ambos extremos, la cual nunca es enviada a través de la red, Además cualquier contraseña de usuario es encriptada y enviada del cliente al servidor. Para evitar así que cualquier intruso pueda obtener la contraseña de un usuario.

Los campos de respuesta que recibe el cliente del servidor, contienen un campo llamado "request- aunthenticator", este campo consiste en una cadena de octetos encriptados con el algoritmo MD5, y contiene: código, id, longitud y autenticador de mensaje, como se muestra en la figura 3.1:

Figura 3. 1 Paquete RADIUS

3.4.4 Mecanismos flexibles para la autenticación

El servidor RADIUS puede soportar una variedad de mecanismos para autenticar a un usuario, cuando se establece nombre y contraseña por el usuario, éste puede soportar, *PAP*[15] *o CHAP*[16], Unix autenticación o cualquier otro mecanismo.

3.4.5 Operación de RADIUS.

Cuando un cliente está configurado para soportar RADIUS, cualquier usuario del cliente presenta autenticación o información al cliente, esto podría ser con un acceso rápido personalizable, donde el usuario espera para ingresar su nombre de acceso y contraseña. Alternativamente, el usuario puede usar un protocolo de enlace.

Una vez que el cliente tiene dicha información, puede optar por autenticar con RADIUS. Para hacerlo, el cliente crea un "access-request" que contiene atributos, tales como: el nombre de usuario, la contraseña del usuario, el identificador del cliente y el identificador del puerto, por el cual el cliente está ingresando.

Cuando una contraseña es enviada del cliente al servidor RADIUS, esta contraseña es ocultada usando un método basado en RSA y algoritmo de mensaje digerido (MD5).

El "access-request" se presenta al servidor RADIUS a través de la red. Si la respuesta no es regresada en un tiempo determinado. La solicitud es re enviada un cierto número de veces. El cliente puede reenviar solicitudes a un servidor o servidores de respaldo, en el caso que el

[15] 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.

[16] 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).

servidor primario sea inalcanzable. Los servidores suplentes pueden ser utilizados después de una serie de intentos, en donde el servidor primario falle.

Cuando esto sucede, se utilizan algoritmos de reintento como round-robin o fallback, estos algoritmos son temas de investigación en la actualidad, pero no nos adentraremos mucho en esto.

Una vez que el servidor RADIUS recibe la solicitud, éste valida el envío del cliente. Una solicitud cliente para la cual el servidor RADIUS no tiene un secreto compartido, debe ser descartada. Para que el cliente sea válido, el servidor deberá consultar una base de datos de usuarios, para encontrar un usuario cuyo nombre coincide con la solicitud. La entrada de usuarios en la base de datos contiene una lista de requerimientos, que deben de cumplirse para permitir el acceso del usuario. Esto siempre incluye la verificación de la contraseña, pero puede también especificar los clientes o puertos a los cuales el usuario es permitido acceder.

El servidor RADIUS puede hacer peticiones a otros servidores, con el fin de satisfacer las necesidades o cuyo caso actuar como cliente, RADIUS trabaja con paqutes específicos como se observa en la siguiente figura 3.2.

Valor	Descripción
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

Tabla 3. 1 Octeto que contiene los tipos de paquetes

Si alguna condición no se cumple (no existe el usuario, ó no coincide la contraseña etc) el servidor manda un "access-reject", la respuesta que indica que la solicitud del usuario no es válida. Si el servidor desea podría incluir un mensaje de texto en el "access-reject", explicando por qué no es posible acceder a la red. Además se podría mostrar por el cliente en el usuario. Ningún otro atributo es permitido en el "access-reject".

Si no todas las condiciones son cumplidas, el servidor emite un reto al cual puede responder el usuario. El servidor manda un "accses-challenge" de respuesta. Se podría incluir un mensaje de texto a ser mostrado por el cliente en el usuario, esperando una respuesta al reto.

Si el cliente recibe un "accses-challenge" y soporta el reto de la respuesta, esté podría mostrar el mensaje de texto, en su caso al usuario, y el usuario a continuación da una respuesta prontamente, el cliente entonces representa la solicitud original "access-request", con una nueva solicitud de identificación, con el atributo de contraseña reemplazada por la respuesta (encriptada), e incluyendo el estado del atributo para el "access-challenge", solo debe mostrar 0 o 1 en los estados de atributos.

El servidor puede responder a un nuevo "access-request", ya sea con "access-accept" o un "access-reject", o de otro modo un "access-challenge".

Una vez que la autenticación fue satisfactoria, el cliente le envía al servidor un "accounting-request" para indicarle al servidor que comience la contabilidad, o registro de actividades del usuario, y a la vez le envía hora y fecha en que se inició la conexión, entre otros parámetros. Cuando el usuario desee desconectarse, el cliente envía al servidor un "accounting-response", pero esta vez ordenándole que debe detener el registro para el usuario en cuestión, y puede enviarle atributos como el tiempo en que el usuario duró conectado, o a qué hora fue desconectado de la red, como se visualiza en la siguiente figura 3.3.

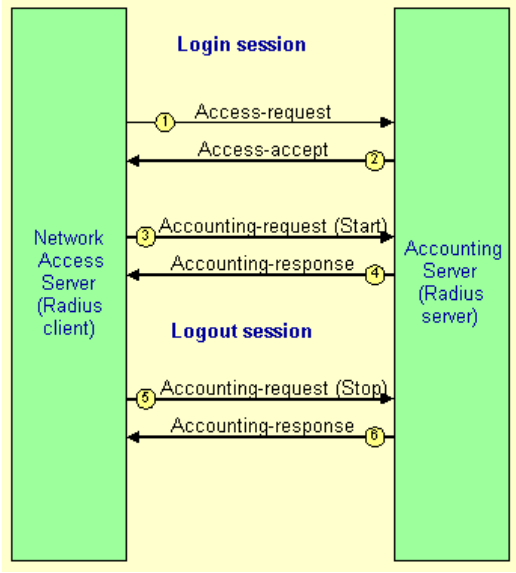


Figura 3. 2 Secuencia de paquetes

De alguna forma hemos descrito una sesión de usuario completa, desde que solicita conexión, hasta que se desconecta.

A continuación mostramos el intercambio de paquetes entre un cliente y servidor. Donde el puerto de solicitud de conexiones para RADIUS, es el UDP 1812, y las peticiones de contabilidad por el puerto UDP 1813.

Este primer paquete es un acces request:

- **TIPO DE PROTOCOLO ENVIADO**

  Framed-protocol = ppp

- **NOMBRE DE USUARIO**

  User name= juan

- **CONTRASEÑA**

  User-Pasword=contraseña de juan

- **INTERFAZ DEL NAS POR EL CUAL FUE HECHO LA SOLICITUD DE CONEXIÓN**

  Cisco-nas-port= async5/51

- **PUERTO**

  Nas-port= 699

- **TIPO DE PUERTO**

  Nas-port-type= ansyc

- **TIPO DE SERVICIO SOLICITADO**

  Service-type= framed user

- **DIRECCIÓN IP DEL NAS (Network Attached Storage)QUE RECIBIÓ LA SOLICITUD**

  Nas- ip- address= 192.168.1.23

Luego de recibir la solicitud el servidor, autenticará al usuario y posteriormente autorizara la conexión para lo cual debe procesar los parámetros recibidos.
En caso de que la autenticación y /o autorización fallen, el servidor mandará un "acces-reject", en el que puede enviar un mensaje de error para el usuario algo como:
Sending acces-reject of id 92 to 192.168.1.23 :21717.
Reply-menssage : su cuenta no tiene acceso a esta red

En caso que la autenticación y/o autorización sean satisfactorias, el paquete enviado por el servidor será un "acces-accept", por ejemplo:
Sending acces-accept of id 92 to 192.168.1.23 :21717
Framed-filter-id : ip-filter
Service-type =framed-user

Framed-mtu= 576

Framed compresión= van-jacobson-tcp-ip

Sesión-timeup=88521

Donde ip-filter, es el filtro que hay que aplicarle al cliente para definir el nivel de acceso al usuario, la conexión estará activa durante 88521 segundos, según lo establecido por sesión-timeout.

El paquete acces-accept recibido por el cliente, le indica que se establezca una nueva sesión para el usuario, el cliente entonces responde con un tipo accounting-request, indicándole al servidor que inicia la contabilidad, y le envía además los datos que deben ser registrados en la base de datos del servidor.

Act-session-id = 0004A3D5

Framed-protocol =ppp

Framed-ip-address =192.168.1.23

Acct-athentic =RADIUS

User name= juan

Acct-status-type= start

Cisco.nas-port =ansyc 5/51

Nas-port= 669

Nas-port.type =ansyc

A este paquete[17] el servidor responde con un paquete accountig-response, lo cual indica que han registrado exitosamente los datos de una nueva conexión establecida, cuando el usuario cierra la conexión, el cliente manda al servidor una petición del tipo accounting-stop , a la vez le envía al servidor el tiempo que duró la conexión, y causas por las que se perdió está,

[17] es una unidad fundamental de transporte de información en todas las redes de computadoras modernas. El término datagrama es usado a veces como sinónimo. Un paquete está generalmente compuesto de tres elementos: una cabecera (header en inglés) que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos (payload en inglés) que contiene los datos que se desean trasladar, y la cola (trailer en inglés), que comúnmente incluye código de detección de errores.

todo lo explicado anteriormente es para obtener una infraestructura como se muestra en la figura 3.4.

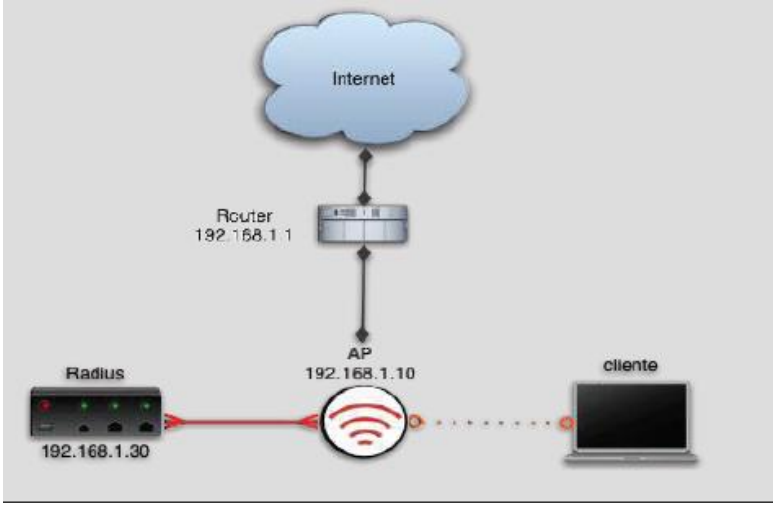


Figura 3. 3 Estructura 802.1X con RADIU

Esta sería la conversación entre cliente y servidor, la configuración dentro de Fedora de freeRADIUS es muy extensa, hay documentación en: www.freeRADIUS.org, instalación en: http://wiki.freeRADIUS.org/Installation y configuración http://wiki.freeRADIUS.org/RADIUSd#Configuration.

3.5 Protocolo de Autenticación Extensible (EAP)

Se da a notar en el estudio de la norma 802.1X, que uno de los elementos básicos es el protocolo de autenticación nombrado EAP (Extensible Authentication Protocol), desarrollado para ampliar la seguridad y funcionalidades del protocolo PPP (Point to Point Protocol), "usuario" y "contraseña" de modo que tiene la capacidad de admitir otros métodos más específicos y sofisticados para realizar autenticación como certificados, tarjetas inteligentes, ntlm, Kerberos, LDAP, etc. Su funcionamiento principal viene siendo su comportamiento como intermediario entre un solicitante y un proceso de validación permitiendo la comunicación entre ambos. Dicho proceso de validación está conformado

por tres elementos, el solicitante que busca ser validado mediante unas credenciales, un PA y un sistema de validación situado en la red.

Para establecer la conexión a la red, el solicitante se identifica por medio de credenciales, que pueden ser una pareja nombre/usuario, un certificado digital u otros datos. Al mismo tiempo el cliente solicitante necesita añadir el sistema de validación que va a utilizar. A grandes rasgos EAP se comporta de esta manera, recibe una solicitud de validación que envía a otro sistema que se encuentra dentro de la red, que sepa cómo resolverla. El PA rechaza todas las tramas que no se encuentren validadas, que provengan de clientes no identificados, salvo aquellas que sean una solicitud de validación. Los paquetes EAP que circulan por una LAN al momento de consultar su solicitud al Sistema Autentificador encargado de resolver dicha petición, se denominan EAPOL (EAP over LAN). Hasta el momento en que es validado el PA permite todo el tráfico del cliente como se observa en la figura 3.4.

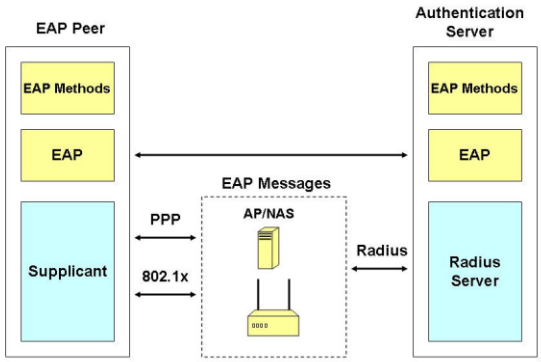


Figura 3. 4 Autenticación Típica EAP

En este caso el Sistema de Autenticación es un servidor RADIUS (802.1X), que seguirá son los siguientes:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.

- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajeno al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.
- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

Sobre los puntos que se han desarrollado de la Norma 802.1X, se observa que consta con un mecanismo de autenticación independiente de Sistemas de cifrado. Si se da a la tarea de configurar con mayor detenimiento el servidor de autenticación 802.1X, podría utilizarse para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación.

De lo que el PA utilizara las claves de sesión para construir firmas y cifrar el mensaje de clave EAP que se envía después del mensaje de aceptación, y a la vez el cliente puede utilizar el contenido del mensaje de clave para definir, las claves de cifrado aplicables. En los casos prácticos de aplicación del Norma 802.1X, el cliente puede cambiar automáticamente las claves de cifrado con la frecuencia necesaria para evitar que haya tiempo suficiente como para poder averiguarla.

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos citar:

EAP-TLS EAP-TTLS/MSCHAPv2, el PEAPv0/EAP-MSCHAPv2, el PEAPv1/EAP-GTC y el EAP-SIM.

3.5.1 EAP-TLS (Transport Layer Security)

Estándar abierto del Grupo de Trabajo de Ingeniería de Internet (IETF), pudiendo ser el de mayor uso tanto en clientes inalámbricos como en servidores RADIUS, entre los que se establece una sesión de TLS cifrada [7], considerándose una seguridad fuerte (es decir, el servidor autentica al cliente y viceversa), debido a que se basa en certificados digitales de clave pública, tanto del cliente como del servidor, requiriendo una confirmación PKI (Public Key Infraestructure) en ambos extremos autenticándose mutuamente y soporta el uso de claves dinámicas para WEP. Siendo esta la configuración para el PA raíz, dando la capacidad de extender fácilmente la configuración a los PA que funcionan como repetidores, con el simple requerimiento de asociar correctamente.

Mientras que un Servidor de Autenticación configura una sesión de seguridad, del nivel de transporte (TLS) con el solicitante con el que intercambiara un certificado digital, produciéndose la autenticación siempre que ambas partes confíen en los certificados de la otra parte. Considerada como la implementación más segura de 802.1X que hay disponible para redes inalámbricas, especialmente cuando se combina con el uso del estándar 802.11i WPA2. A su vez EAP-TLS [15] se considera tiene una mayor necesidad de recursos, debido a que sería necesario un gran número de certificados para dicha implementación, al mismo tiempo que la infraestructura de clave pública. Teniendo un mayor costos de compatibilidad e implementación en comparación con PEAP con MS-CHAP v2.

Requisitos de 802.1X EAP-TLS

Como se mencionó anteriormente, EAP-TLS necesita más recursos que las implementaciones PEAP debido a los requisitos de certificados adicionales. Por supuesto, se pueden usar proveedores de terceros para emitir los certificados de requisitos para todos los clientes inalámbricos y servidores de autenticación, pero este método es más costoso que

implementar una infraestructura de certificados, excepto cuando el número de clientes inalámbricos está limitado estrictamente a unos pocos usuarios.

En total, un sencilla implementación de EAP-TLS necesitaría al menos cuatro servidores, más en el caso de compañías más grandes o de redes con distribución geográfica. Dos de los cuatro servidores actuarán como servidores RADIUS IAS redundantes y los otros dos como la infraestructura de certificados. De los dos servidores de certificados, se recomienda que uno (el servidor de certificados raíz) esté separado de la red y desconectado de ésta, lo que puede significar que se puede reducir el número de servidores en uno en determinadas circunstancias.

Capítulo 4 "Estructura de la Red Inalámbrica de ESIME Zacatenco"

4.1 Red ESIME

La red de ESIME Zacateco, está conformada por 11 nodos fundamentales, que son conectados a la red institucional mediante fibra óptica, la cual atraviesa de norte a sur el edificio Z, hasta llegar al Nodo principal que se encuentra en el edificio 1 del cual se hacen ramificaciones hacia los edificios 2, 3, 4, 5 y Z, así como también hacia el Nodo de la Unidad de Informática (Isla) y los laboratorios pesados de ICA, como se muestra en la Figura 4.1.

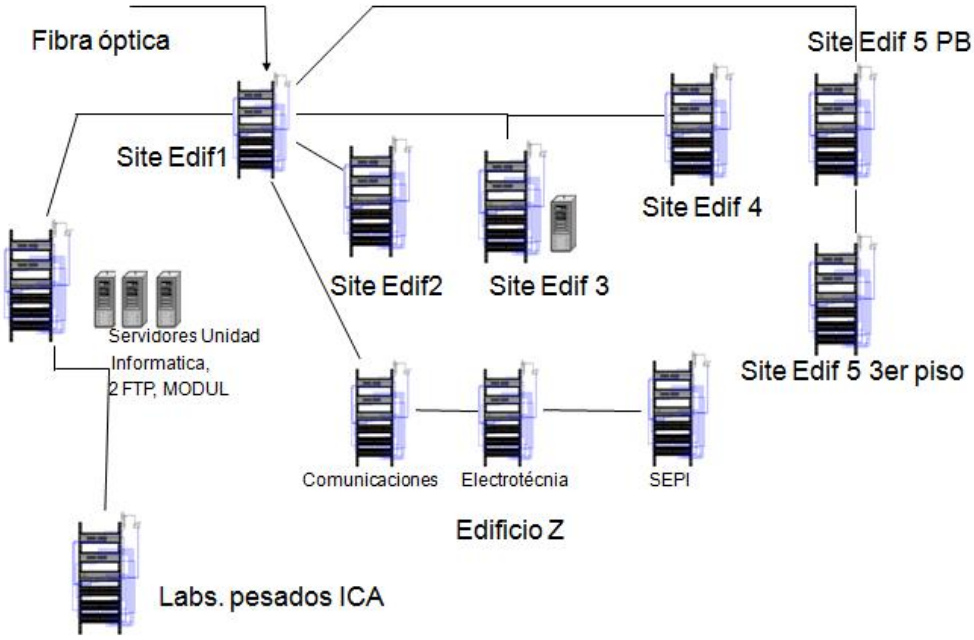


Figura 4. 1 Topología de ESIME Zacatenco

De los nodos antes ilustrados, se puede observar la existencia de servidores como son: 2 servidores FTP en el nodo de la Unidad de Informática, así como un servidor de bases de datos para Control Escolar, ubicado en el edificio 3.

La distribución del direccionamiento de la red de ESIME Zacatenco, ha tenido últimamente algunas modificaciones, aunque se sabía que la distribución de direcciones IP de los Edificios 3,4 y 5, correspondía al rango de 148.204.71.0/24, como se muestra en la siguiente tabla.

Origen FQDN	< IP Origen >	Sentido	< IP Destino >
ubuntu	192.168.1.118	-->	67.228.49.186
m054-edif345.esimez.ipn.mx	148.204.71.54	-->	67.228.49.186
ubuntu	192.168.1.118	-->	75.126.97.3
m054-edif345.esimez.ipn.mx	148.204.71.54	-->	75.126.97.3

Tabla 4. 1 Análisis de tráfico

Aunque actualmente el edificio 5 y los anexos de profesores, tienen el siguiente direccionamiento: 148.204.36.0/24.

La realización de un sondeo de las redes inalámbricas de las instalaciones de ESIME Zacatenco, se llevó a cabo pudiendo visualizar las zonas más concurridas por las redes inalámbricas.

La detección de un número mayor de redes a la altura del Edificio 1 ilustración 4.1, se presentaron del lado oeste (Edificio Z) de las instalaciones de la ESIME Zacatenco, detectando 7 redes, para establecer conexión a la red institucional e Internet.

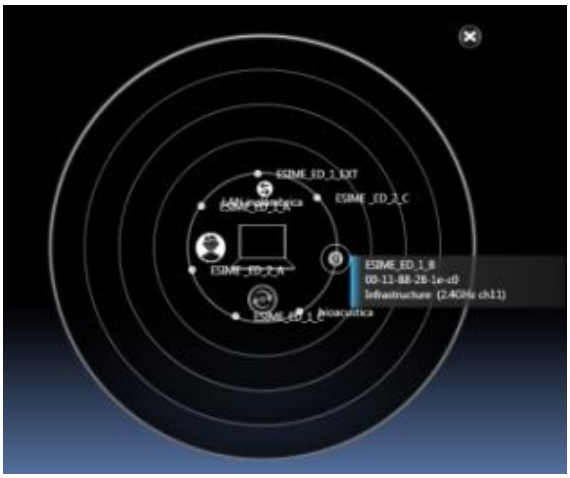


Ilustración 4. 1 Zona del Edificio 1 próxima al Edificio Z

De la misma forma el sondeo del Edificio 2 ilustración 4.2, arrojó un vasto número de redes que prestan sus servicios a los usuarios, pero en esta ocasión fueron detectadas del lado del estacionamiento, suministrando una amplia cobertura a la ESIME.

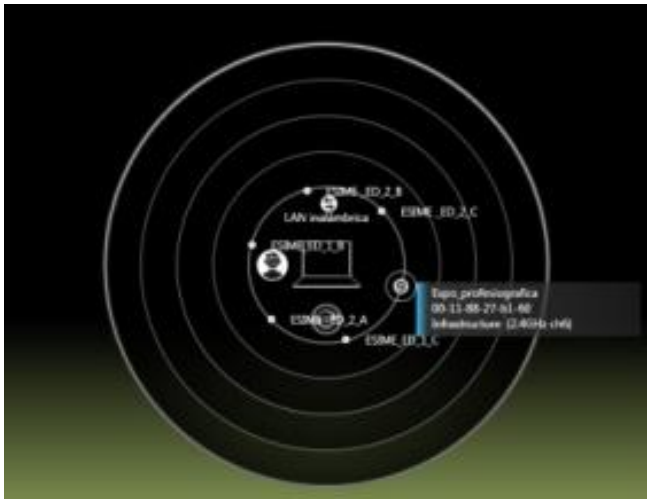


Ilustración 4. 2 Zona de estacionamientos del Edificio 2

En las ilustraciones 5.3 y 5.4, se puede observar que son las más abundantes en conectividad por vía inalámbrica, debido a que son los edificios céntricos de la configuración de redes inalámbricas de ESIME, se puede mencionar que en la mayor parte del edificio se pueden detectar un gran número de redes.

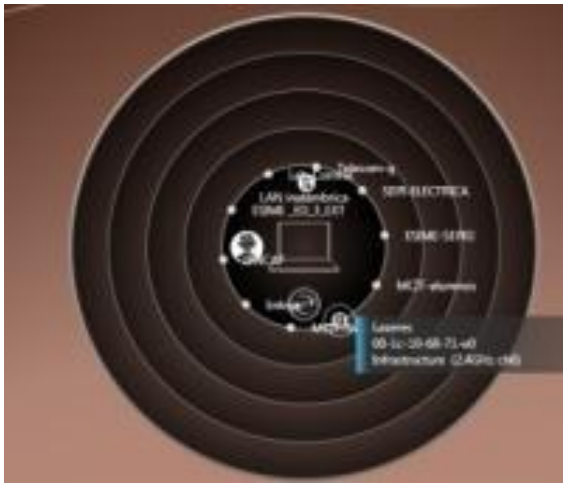


Ilustración 4. 3 Zona del Edificio 3 próxima al edificio Z

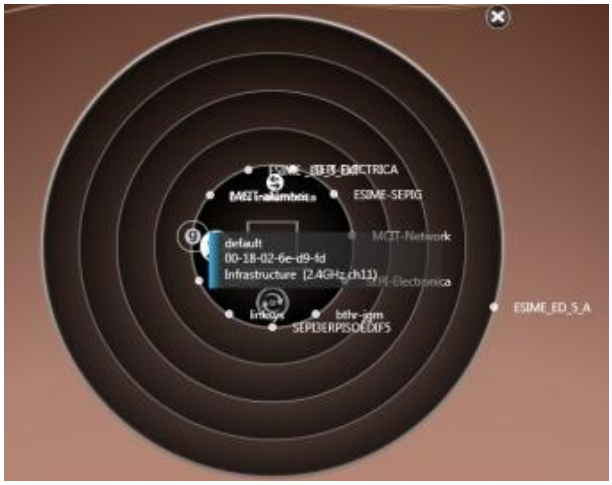


Ilustración 4. 4 Zona del Edificio 4 próxima al Edificio Z

La detección de las redes inalámbricas en el Edificio 5 ilustración 4.5, es de principal importancia, ya que en esta zona se encuentran una mayor cantidad de redes protegidas contra usuarios no autorizados, pero esto al mismo tiempo las convierte en las redes más atacadas, debido a que si se realiza una conexión a una red segura, cabe la posibilidad que sea menos congestionada. Por lo tanto la prioridad de este trabajo es, controlar el acceso a las redes de los anexos de profesores, los cuales requieren de una alta confidencialidad e integridad, en la transferencia de información.

Ilustración 4. 5 Zona céntrica del Edificio 5

Dentro de la distribución de la red de ESIME Zacatecno, se resaltarán los PA, existentes que dan servicio de red, a estudiantes y personal docente, desde el edificio 1 hasta el 5 que cuenta con las siguientes redes inalámbricas, que se podrían organizar por canal de transmisión, orden alfabético, seguridad, pero en este caso se realizó por la posición en la que se encuentran desde el primer edificio de ESIME Zacatenco, al último correspondiente a sus instalaciones, contando sus respectivas secciones del edificio Z. Para poder entender con mayor claridad la siguiente tabla 5.2, se establece el número del edificio correspondiente y las letras E, C y Z, dependiendo de la ubicación en la que se pueda detectar la señal de una red inalámbrica, ya sea del lado oeste o del estacionamiento, en el centro del edificio o el ala este o edificio Z, correspondientemente a las letras antes especificadas.

Nombre de red	MAC	Canal 2.4 GHz	Seguridad	Edificios
linksys	00-16-e3-a0-a7-0f	ch6	×	1 Z, 2Z,3Z,3C
bioacustica	00-1c-10-67-cd-3f	ch6 o ch5	✓	1 Z
Lab-Control	00-0f-b5-69-a0-bc	ch6	✓	1 Z,2Z,3Z
ESIME-ED_1_EXT	00-11-88-28-39-e0	ch1	×	1 Z,C,2Z
ESIME-ED_1_A	00-11-88-27-45-a0	ch1	×	1 C
ESIME_ED_2_A	00-11-88-27-fd-50	ch11	×	1 C,E
ESIME_ED_1_C	00-11-88-28-05-50	ch5	×	1E
ESIME_ED_1_B	00-11-88-28-1e-c0	ch11	×	1E
ESIME_ED_2_C	00-11-88-28-36-80	ch1	×	1E
ESIME_ED_2_B	00-11-88-27-14-70	ch6	×	1E,2E,2C
ESIME_ED_3_B	00-11-88-27-fa-d0	ch6	×	2E,2C,3E
ESIME_ED_3_A	00-11-88-27-FA-50	ch6	×	2C,3C,3E
LINKSYS	00-16-E3-A0-A7-0F	ch7	×	2C
MCIT-Network	00-16-f3-c1-05-69	ch1	✓	2C
IPNCAF	00-0d-54-a1-f0-6f	ch6	✓	2Z,3Z,3C,3E,4C
ESIME-SEPIG	00-13-10-ec-15-46	ch11	✓	3Z,4Z,4C,5Z
MCIT-alumnos	00-1d-7e-c2-61-09	ch6	×	3Z
MCIT-Network	00-16-f3-c1-06-b0	ch1	✓	3Z,4Z,4Z
ESIME_ED_3_EXT	00-11-88-27-ae-90	ch6	×	3Z,3C,4Z,4C,4E
Telecom-g	00-90-4b-63-43-ce	ch11	×	3Z
SEPI-Electronica	00-18-f8-55-28-24	ch10	✓	3Z,5C,5E
SEPI-ELECTRONICA	00-0c-c8-61-17-a4	ch11	✓	3Z,EC
Laseres	00-1c-10-68-71-e0	ch6	✓	3Z,4Z
ESIME_ED_4_A	00-11-88-28-21-40	ch6	×	4C,4E
ESIME_ED_4_B	00-11-8828-2c-80	ch11	×	4C,4E
ESIME_ED_3_C			×	3E
linksys	00-21-29-ad-4e-56	cH6	×	4Z
SEPI3ERPISOEDIF5	00-18-f8-55-28-21	ch11	✓	4Z,4E,5E
default	00-18-02-6c-d9-fd	ch11	×	4Z
linksys	00-21-29-ad-4e-56	ch5	×	4C,5Z
SEPI-ELECTRICA	00-0c-c8-64-17-a4	ch11	✓	4C
SEPIBIBLIOTECA	00-14-bf-76-f9-b5	ch5	✓	5E
NETGEA	00-09-5b-6c-4B-32	ch11	×	5E
ESIME_ED_5_C	00-11-88-28-2c-20	ch11	×	5E
ESIME_ED_5_A	00-11-88-27-f9-00	ch1	×	5E
linksys	00-21-29-b3-be-a7	ch6	✓	5E
Bthr-jgm	0e-8f-0c-0f-9e-87	ch11	✓	5C
T02	00-21-29-b3-95-d3	ch6	✓	5C
RedOfficceEspina	00-06-b5-64-1a-f8	ch11	✓	5C

Tabla 4. 2 Redes inalámbricas de ESIME Zacatenco y sus principales características

4.2 Concurrencia de las necesidades de servicios inalámbricos en ESIME Zacatenco

Como se mencionó en capítulos anteriores, se podrán exponer los grandes beneficios y ventajas que una red inalámbrica puede brindar a los usuarios contra una red cableada, ya que le permitirá tener acceso desde puntos en los que no se encuentra una roseta, para realizar una conexión por medio de cable, aparte de que las redes inalámbricas pueden brindar el uso de múltiples aplicaciones, así como el soporte de los diferentes servicios que el Instituto presta por medio de su red, por parte de sus servidores FTP, WEB, DNS, etc., a su vez también brindado servicios de redes locales, como impresiones, copias, etc. Estas ventajas, así como la conectividad de sitios remotos a un laboratorio o aula, son las que brindan las redes inalámbricas, tanto así que pueden brindar estos servicios a varios usuarios a la vez, permitiéndoles realizar diferentes tareas a cada uno de ellos por separado, por este motivo, se han subdividido las WLAN, de ESIME Zacatenco, ya que las necesidades y privacidad que un docente necesita tener, son completamente distintas a todos los recursos que un alumno puede utilizar al momento de conectarse a una red inalámbrica, pero esto ha llevado a que los alumnos estén inconformes con la conectividad de dichas redes, debido a que existe una mala administración de ellas, y buscan alcanzar mejores servicios migrando a las redes restringidas únicamente para docentes, realizando un análisis de paquetes y con esto capturando las contraseñas, para poder tener acceso a este tipo de redes más ricas en características de servicios.

4.3 Estado de la red inalámbrica de los anexos de profesores

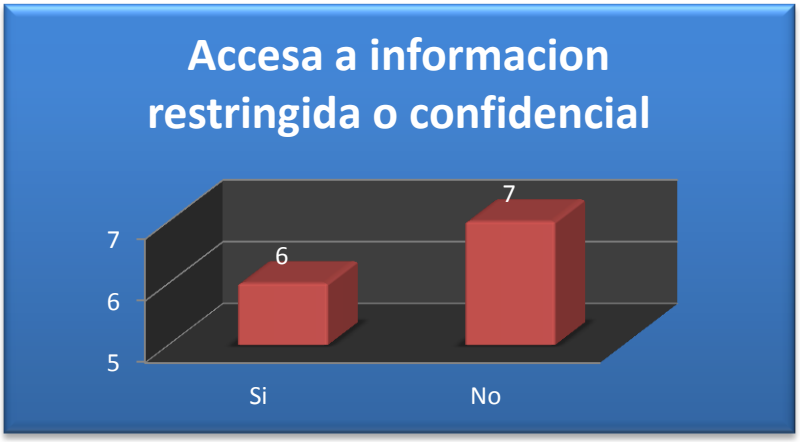
Como justificación de este proyecto, se realizó una encuesta para saber qué deficiencias o vulnerabilidades podrían presentar los usuarios de esta red, que son los profesores y estudiantes de maestría de estos anexos, los resultados se pueden ver en las grafica 4.1 y 4.2, y cada una de ellas arrojan conclusiones muy interesantes para el estudio del problema que nos concierne.

Las siguientes gráficas nos muestran el tiempo en horas gráfica 4.1 y días gráfica 4.2 que la red se encuentra en uso, de esta manera podemos concluir que la red tiene mucha demanda, pues la mayoría de los usuarios la usa más de tres días a la semana, y durante el día hacen uso de la red, seis horas en promedio.

Gráfica 4. 1 Uso de la red por horarios

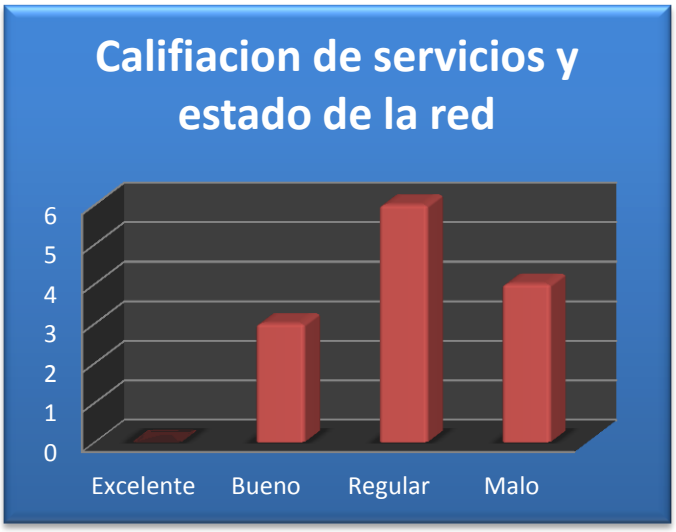
Gráfica 4. 2 Uso de la red por día

Al hacer uso de la red (principalmente profesores), se puede tener acceso a cualquier tipo de información, en ocasiones esta información puede ser que sea confidencial y muy importante para el usuario, por lo tanto ningún agente externo deberá tener acceso a dicha información, la gráfica 4.3 nos indica que poco menos del 50% de los usuarios de la red, deben acceder a información confidencial, es por ello que la red debe garantizar que su información no será vista por agentes externos a la red institucional.



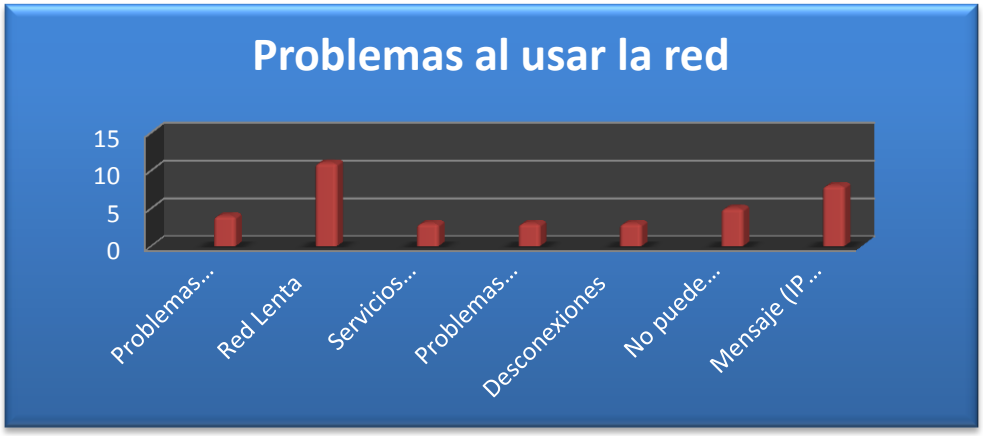
Gráfica 4. 3 Tipo de información que utiliza

Dentro de la encuesta que se realizó a los usuarios de la red institucional, se les pidió que calificaran los servicios que ofrece la red y el estado de la misma, y el resultado estadístico que se obtuvo, fue que la mayoría no se encuentra conforme con estos dos parámetros de la red, en mayor número los usuarios califican a la red como regular, siguiéndole muy de cerca los usuarios que opinan que la red en cuanto a servicios y estado es mala, entonces surge la pregunta, la duda, de qué es lo que hace que los usuarios muestren esta inconformidad, esto se puede ver reflejado en la gráfica 4.4.



Gráfica 4. 4 Calificación de la red

Los usuarios exponen que tienen diversos problemas al hacer uso de la red institucional, el problema en el que más usuarios coinciden, es que la red es lenta y de la aparición de un mensaje el cual dice que la dirección IP está duplicada, esto se debe a la saturación de la red por agentes externos a ella, debido a que la cantidad de usuarios (profesores y estudiantes) que tienen un lugar asignado dentro de la red institucional, no debería de ocasionar estos problemas, ya que la demanda es baja(por ser pocos usuarios). Otro de los problemas más frecuentes, es que experimentan desconexiones y problemas al querer conectarse, estos datos se ven reflejados en la Gráfica 4.5.



Gráfica 4. 5 Problemas al usar la red

El siguiente gráfico 4.6 nos muestra, que los usuarios piensan que no solo los estudiantes y maestros de los anexos son los que hacen uso de la red, esto hace vulnerable la información confidencial o no, de las personas que si tienen un lugar asignado dentro de esta red. Una vez identificado el problema, la pregunta es: ¿con que fin se conectan estas personas a la red? Si sólo es para usar los recursos de ésta, o para averiguar o alterar la información de otros usuarios.

Gráfica 4. 6 Usuarios de la red

En la gráfica 4.7, podemos observar que los usuarios temen que gente ajena a la red se conecta con fines malicioso, es decir, que usan la red para alterar o sólo averiguar información de otros usuarios, es por todas estas razonas que se vuelve necesaria la utilización de un sistema de autenticación, que no sólo servirá para garantizar seguridad a la red, sino que proporcionará una mayor eficiencia en los servicios que ofrece.

Gráfica 4. 7 Uso de la red con fines maliciosos

4.4 Requerimientos para la implementación de un Sistema de Autentificación

Autenticar: es el acto de establecimiento o confirmación de algo (o alguien) como auténtico

En cualquier sistema que ofrezca algún tipo de servicio, necesitamos establecer niveles de "confianza", para ello debemos catalogar a ciertos usuarios mediante atributos, previamente establecidos. Para lograr esto, necesitamos herramientas capaces de realizar tareas de autenticación, servidores tales como RADIUS soportan a un conjunto de protocolos diseñados específicamente, para realizar autenticación, uno de estos protocolos es EAP.

EAP es descrito como un framework de autenticación, esta arquitectura es enviada al usuario para introducir su identificación, su nombre así como contraseña, una vez hecho esto, el servidor RADIUS es el encargado, para nuestro caso, el que decide si se le otorgará servicio o no al usuario .

Hemos descrito un sistema de autenticación muy simple, pero funcional, dependiendo de las necesidades, es como incrementará la utilización y combinación de diferentes protocolos, para generar un sistema aún más exclusivo, dentro de estos sistemas más complejos tenemos como ejemplo a:

- EAP-TLS
- EAP-TTLS
- EAP-mschap v2

Se trabajará con EAP-TLS en la realización del proyecto, para esto tendremos que generar certificados con openssl [10], los certificados sólo generan "confiabilidad" entre cliente y servidor, es por eso que no se profundizará en este punto.

Capítulo 5 "Propuesta del Sistema de Autenticación para la Red Inalámbrica de los anexos de ESIME Zacatenco"

5.1 Utilización de la norma 802.1X

Como alternativa realmente viable, para quienes tienen dispositivos inalámbricos, surgió la integración del mecanismo de control de acceso y autenticación a la red 802.1X, con el uso de cifrado WEP y manejo dinámico de claves (WEP dinámico). La norma 802.1X, tiene la característica de poder incorporarse con más de un protocolo, para proporcionar un mecanismo mucho más robusto, de lo que un solo protocolo de seguridad podría brindar.

5.2 Propuesta a Implementar

Debido a los problemas de seguridad presentados en los anexos de profesores del edificio 5 de ESIME Zacatenco, En el capítulo anterior, se decidió por una estructura de autenticación. Encabezada por el servidor RADIUS y que esté trabajando con EAP-TLS, para realizar comunicación entre servidor cliente, una encriptación basada en RSA para los certificados y llaves privadas, software openSSL para la creación de los certificados.

Por parte del ruteador se trabaja con un modelo wrt54g2 de linksys, específicamente este modelo soporta la norma 802.1X, y su funcionalidad es de punto y control de acceso a la red de servicios, por medio de los permisos otorgados por el servidor.

Para realizar una solicitud de servicios, tanto usuarios con sistema operativo Windows, como Linux, deben de introducir el nombre de usuario y la contraseña, con la que se encuentran registrados en el Servidor RADIUS, esto es posible gracias al protocolo de autenticación

extensible, el cual construye una interfaz (framework) en la máquina del usuario, para ingresar los parámetros ya antes mencionados.

La forma de ingresar al medio es de forma inalámbrica, lo cual hace más vulnerable la comunicación entre cliente-usuario, en una simple captura de paquetes realizadas por cualquier espía (sniffer), se puede apoderar de la identidad, es decir, de nombre de usuario y contraseña. Pero sin un certificado y una clave privada para descifrar los datos, el espía simplemente verá toda la información en un lenguaje no entendible.

Los certificados creados con openSSL, son de gran importancia por las razones expuestas. Es muy caro obtener un certificado de alguna empresa expedidora (verising, thawte, etc, los cuales sus precios se encuentran entre los US$250,000), es por eso que se decidió utilizar un software libre lo suficientemente eficaz, para representar la autoridad certificadora.

5.3 Pruebas de Implementación

De acuerdo a los resultados obtenidos, en la encuesta, se hace notar la necesidad urgente de una mejora en la administración y control de acceso de los anexos de profesores, de lo cual se valoraron las principales vulnerabilidades, y de la misma forma se realizó un estudio de las características con las que podría contar una implementación de un sistema de autenticación basada en la norma 802.1X, por lo que se realizó un esquema principal de éste, que conforma un enrutador conectado a un servidor RADIUS, que se encargará de otorgar los permisos a los usuarios para acceder a otros servicios de la red institucional, como es la Internet, figura 5.1.

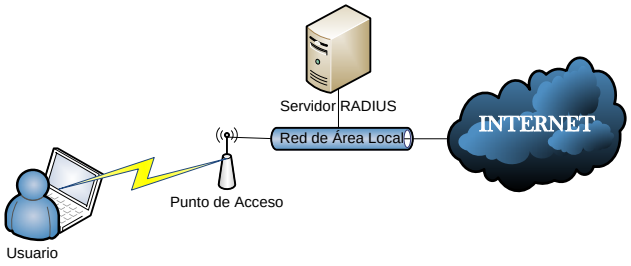


Figura 5. 1 Esquema del Sistema de Autenticación propuesto

Al momento de iniciar el funcionamiento del servicio, en la PC en la que se tiene configurado, freeRADIUS entra en marcha como servidor de autentificación, detectando al enrutador como el servidor de acceso a la red, y comienzan a intercambiar paquetes para reconocerse dentro de la red. Esperando el momento en que un usuario realice una solicitud de servicios, en ese momento comienza la transferencia de paquetes RADIUS figura 5.2, que en el capítulo anterior se mencionan, con el fin de realizar una conexión a la red y obtener los servicios de ésta, se podrán capturar los paquetes que viajan entre el servidor y el control de acceso, pero si se quisiera extraer alguna información de éstos**,** para realizar una suplantación de usuarios, en principio no se comprendería nada**,** porque la información que proporciona una entidad certificante en este caso realiza una encriptación MD5, así como también sobre EAP y puede incluirse una clave de tipo WEB.

201	958.225995	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=137)
202	958.227120	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=64)
203	958.233055	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=414)
204	958.239522	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=1090)
205	958.243343	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=137)
206	958.244179	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=293)
207	958.253655	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=275)
208	958.257739	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=298)
209	958.263003	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=137)
210	958.263807	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=101)
211	958.268156	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=227)
212	958.278835	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=117)
213	958.283106	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=227)
214	959.284162	192.168.1.101	192.168.1.1	RADIUS	Access-Reject(3) (id=0, l=44)

Figura 5. 2 Análisis de tráfico del Sistema de Autentificación

De igual manera, en el servidor se puede observar cómo permanece en escucha de alguna petición o solicitud de servicio, hasta que llega ese momento el servidor comienza a transferir paquetes para corroborar que el usuario, es una entidad autorizada, realizando el envío de mensajes de autentificación como se muestra en la figura 5.3.

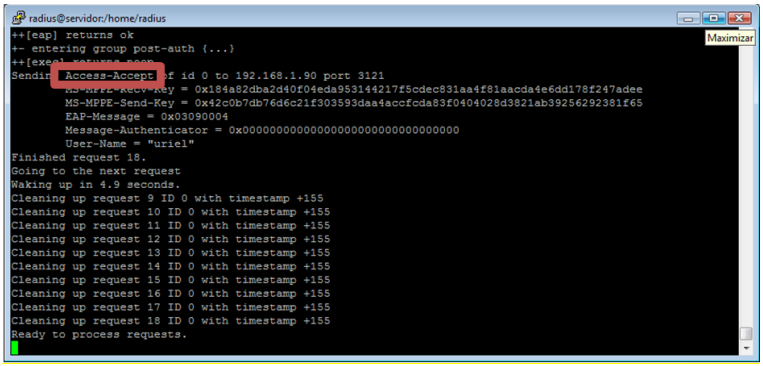


Figura 5. 3 Servidor RADIUS en escucha y transferencia de paquetes

5.4 Pruebas de funcionalidad

5.4.1 Objetivo de la autorización de acceso de una terminal a través de RADIUS

Verificar la autorización de acceso a una red, de una terminal Windows XP, a través del protocolo RADIUS.

5.4.2 Material y Equipo

Para la realización de este proyecto fue necesario contar con un ruteador WRT54G2, que es una pieza fundamental para nuestro sistema, el servidor RADIUS lo instalamos en una PC con las siguientes características:

- Memoria en BIOS de 128KiB
- Procesador Athlon 64 AMD Sempron(tm) a 3300+
- Memoria cache L1 de 128KiB
- Memoria cache L2 de 128KiB
- Memoria del sistema de 1280MiB
- Tarjetas de memoria de 256MiB DIMM y otra de 1GiB DIMM
- Disco duro MCP51 Serial ATA con puente MCP51 PCI

- Tarjeta de red eth1 10/100BaseTX [RTL81xx]
- Tarjeta de comunicación HSF 56k Data/Fax Modem
- Tarjeta multimedia MCP51 AC97 Audio
- Tarjeta de red eth0 MCP51 Ethernet Controller
- Puentes K8 [Athlon64/Opteron]
- Y sistema operativo Fedora 10

También una computadora portátil DELL con:

- Procesador Intel
- Memoria RAM 2 GB
- Tarjeta de red eth0 Realtek y adaptador de red inalámbrica Intel PRO 3945ABG
- Sistema operativo Windows XP

5.4.3 Topología a utilizar

La topología a implementar Figura 5.4, se compondrá de un servidor freeRADIUS [15], que se comportará como servidor Web, servidor para almacenar base de datos y archivos planos de los usuarios pertenecientes a la red.

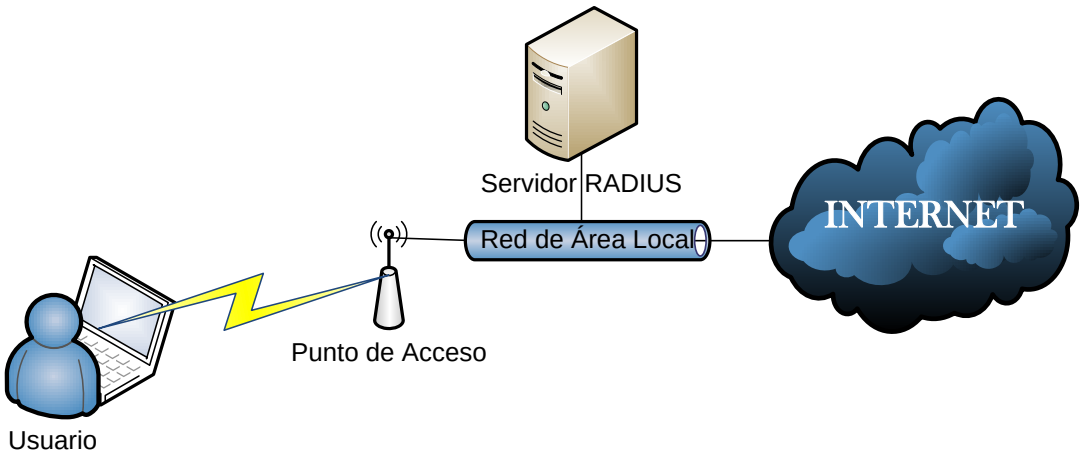


Figura 5. 4 Topología a implementar

El punto de acceso estará conectado al servidor y al proveedor de Internet, al momento que el cliente se autentica como usuario permitido el servidor, le brindará la conexión a la red y junto con ello la conexión a Internet.

Dentro del servidor se crearán los clientes en el archivo /etc/raddb/user, así como sus certificados correspondientes como se muestra en la figura 5.5, los cuales el cliente tiene que instalar en su equipo portátil, el certificado cacert contiene la información de la clave privada, el certificado radius1keycert se creó con la información de la clave pública y privada, y el certificado urielcert contiene la información del cliente que el servidor almacena para su autenticación.

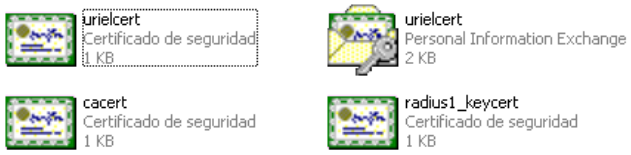


Figura 5. 5 Certificados creados para el cliente

Como antes se mencionó, hasta este momento se obtuvo una configuración inicial exitosa, y con este nivel de configuración se puede proceder con el ruteador:

En el cual se declaran principalmente la subred a la que pertenecerá, la máscara de subred, su puerta de enlace a la red y el dominio en el cual se encontrará establecido, como se muestra en la figura 5.6.

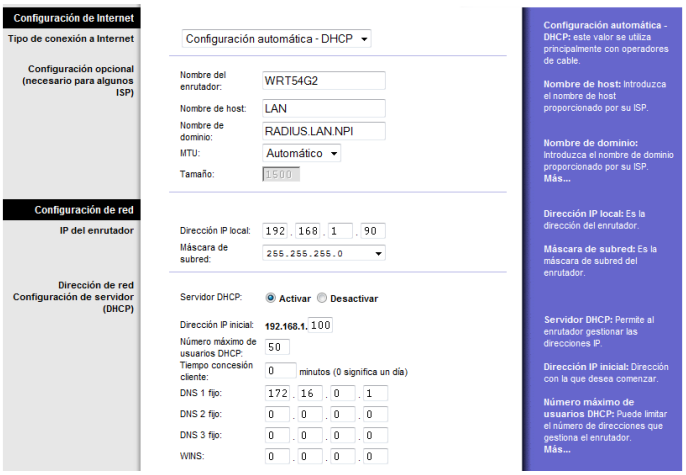


Figura 5. 6 Configuración Ruteador

Dentro de la configuración del ruteador, especificaremos el tipo de seguridad colocando la opción de RADIUS, indicando el puerto por la que se comunicará con el servidor y la dirección IP que tendrá el servidor RADIUS, como se visualiza en la figura 5.7.

Figura 5. 7 Configuración inalámbrica del RUTEADOR

Dentro de las configuraciones extras que se realizaron en el enrutador, fueron la declaración de los puertos con tráfico permitidos, con los cuales se puede realizar conexiones, como son los puertos 5022 para conexión por medio de ssh y los puertos 1812 a 1814, asignados que se muestran en la figura 5.8, para el funcionamiento de RADIUS.

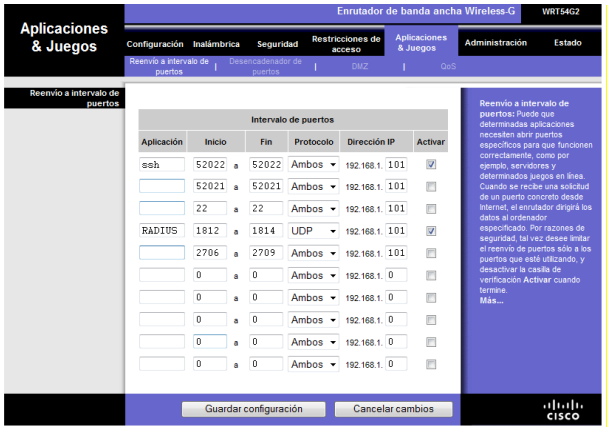


Figura 5. 8 Asignación de puertos habilitados

La computadora portátil de cliente se configura solo si cuenta con el SP2 (Service Pack 2) de Windows XP, se instalan los certificados del cliente y la de llave privada dándole doble click, y siguiendo las indicaciones de almacenamiento. Para el adaptador de redes inalámbricas se tendrá que modificar.

En la máquina del cliente se configura que el tipo de seguridad es 802.1X o RADIUS, y eligiendo el tipo de autenticación EAP, como se muestra en la figura 5.9.

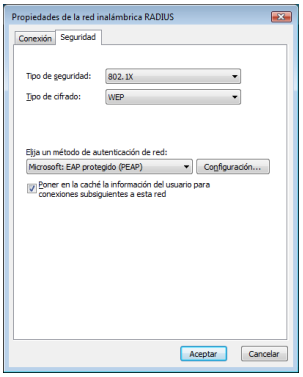


Figura 5. 9 Configuración de la red inalámbrica del cliente

A la configuración de la conexión de la red inalámbrica, se le puede agregar la solicitud de usuario cliente por medio de CHAP v2, lo que solicitará que se ingrese un nombre de usuario y contraseña, para que después verifique los certificados del cliente, la configuración de nombre de usuario y contraseña se puede evitar, y sólo autenticar con los certificados.

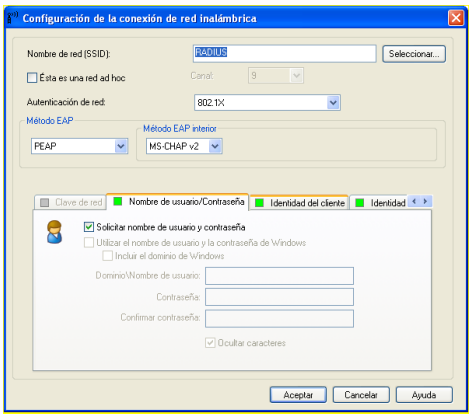


Figura 5. 10 Configuración Nombre de usuario y contraseña

Dentro de la misma configuración de la conexión de red inalámbrica del cliente, se puede ingresar el certificado del cliente y el del servidor, como se muestra en la figura 5.11, para que el servidor pueda autenticar al usuario.

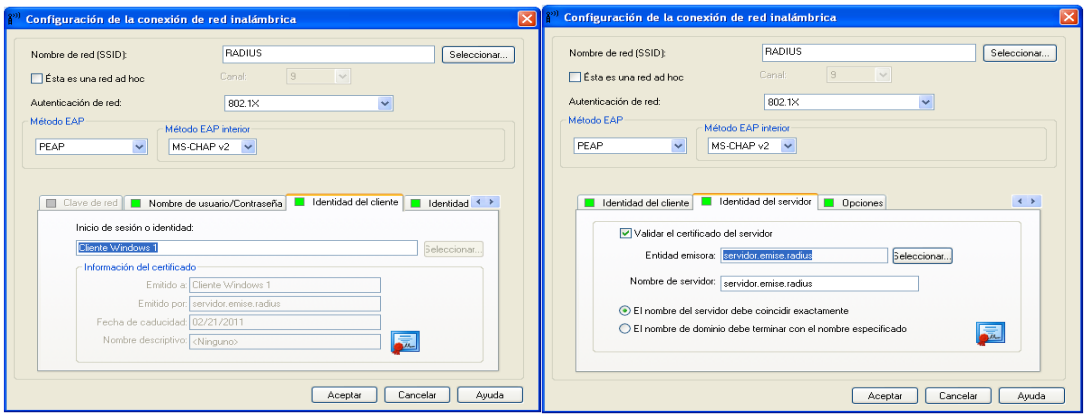


Figura 5. 11 Certificado de cliente y servidor

5.4.4 Prueba de funcionamiento con Autenticación aceptada

Para demostrar el funcionamiento de los certificados después de tenerlos instalados en la portátil del cliente, se realiza la solicitud de conexión a la red inalámbrica figura 5.12, la cual solicitará el nombre del usuario y contraseña, si dejamos la configuración de CAHPv2, si no únicamente corroborará con el servidor, la existencia o emisión de los certificados con los que se desea autenticar el cliente.

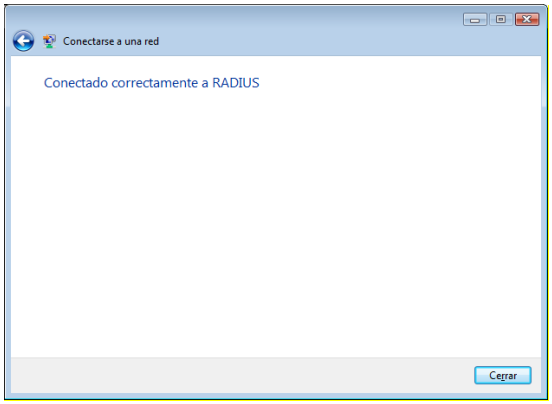


Figura 5. 12 Confirmación al cliente de una conexión correcta.

Del lado del servidor podemos observar con un analizador de tráfico, que en este caso es Wireshark, que la autenticación fue correcta. Al momento de verificar los mensajes que arrojan los paquetes de intercambio entre el cliente y el servidor. Y podemos observar que existe el paquete Access-Accept, el cual confirma la conexión figura 5.13, como pudimos ver anteriormente.

192.168.1.101	189.141.26.146	TCP	52022 > 52815 [ACK] Seq=231954 Ack=71853 Win=10240 Len=1460
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [ACK] Seq=233414 Ack=71853 Win=10240 Len=1460
192.168.1.90	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=174)
189.141.26.146	192.168.1.101	TCP	52815 > 52022 [ACK] Seq=71853 Ack=231954 Win=65700 Len=0
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [ACK] Seq=234874 Ack=71853 Win=10240 Len=1460
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [PSH, ACK] Seq=236334 Ack=71853 Win=10240 Len=48
192.168.1.101	192.168.1.90	RADIUS	Access-challenge(11) (id=0, l=101)
189.141.26.146	192.168.1.101	TCP	52815 > 52022 [PSH, ACK] Seq=71853 Ack=234874 Win=65700 Len=52
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [ACK] Seq=236818 Ack=71905 Win=10240 Len=1460
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [PSH, ACK] Seq=238278 Ack=71905 Win=10240 Len=82
189.141.26.146	192.168.1.101	TCP	52815 > 52022 [ACK] Seq=71905 Ack=239098 Win=65700 Len=0
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [PSH, ACK] Seq=239098 Ack=71905 Win=10240 Len=38
192.168.1.90	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=174)
192.168.1.101	192.168.1.90	RADIUS	Access-Accept(2) (id=0, l=167)
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [ACK] Seq=239486 Ack=71905 Win=10240 Len=1460
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [PSH, ACK] Seq=240946 Ack=71905 Win=10240 Len=28
192.168.1.101	189.141.26.146	TCP	52022 > 52815 [PSH, ACK] Seq=241234 Ack=71905 Win=10240 Len=11
189.141.26.146	192.168.1.101	TCP	52815 > 52022 [ACK] Seq=71905 Ack=240946 Win=65700 Len=0
189.141.26.146	192.168.1.101	TCP	52815 > 52022 [ACK] Seq=71905 Ack=241350 Win=65296 Len=0
0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x759234c4
192.168.1.90	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x759234c4
fe80::f924:2943:5bf3:	ff02::1:2	DHCPv6	Solicit

Figura 5. 13 Tráfico de aceptación entre el cliente y el servidor

Dentro de una consola de Linux de nuestro servidor, también podemos observar el proceso de autenticación de RADIUS, con nuestro servicio en modo depurador radiusd –X figura 5.14, el cual mostrará todas las acciones que se presente entre el servidor y el punto de acceso, podremos corroborar también que se realizó la autenticación adecuadamente.

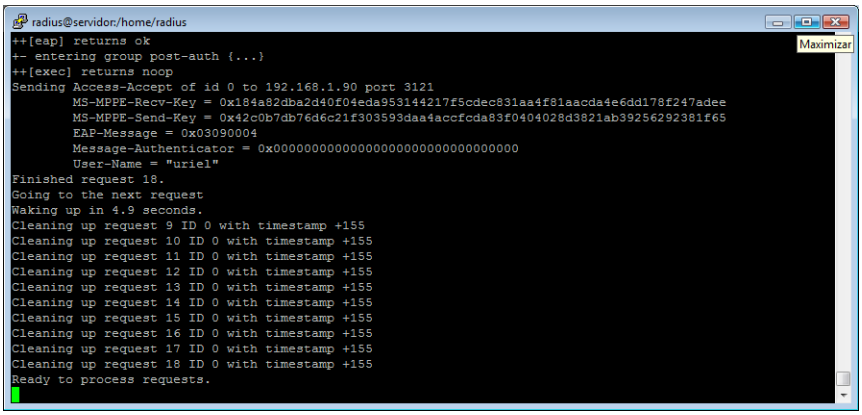


Figura 5. 14 Depurador de RADIUS

Al momento de realizar la autenticación correctamente, tendremos como resultado la conexión a Internet, única y exclusivamente de los usuarios declarados por el administrador.

5.4.5 Prueba de funcionamiento con autenticación rechazada

Para esta prueba, se utiliza el nombre de un usuario que no se encuentra en la base de datos del servidor, y se observará como es rechazada su solicitud de conexión. En la computadora portátil del cliente, mandará el mensaje de que Windows no puede conectarse a la red, como se muestra en la Figura 5.15.

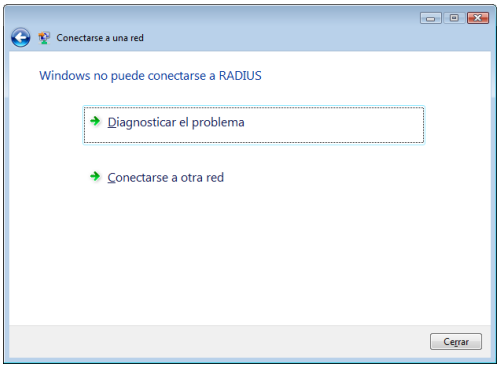


Figura 5. 15 Conexión rechazada

En el analizador de tráfico podremos ver como se envían los paquetes Access-Reject, Figura 5.16, que indican el rechazo de la autenticación.

201	958.225995	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=137)
202	958.227120	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=64)
203	958.233055	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=414)
204	958.239522	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=1090)
205	958.243343	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=137)
206	958.244179	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=293)
207	958.253655	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=275)
208	958.257739	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=298)
209	958.263003	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=137)
210	958.263807	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=101)
211	958.268156	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=227)
212	958.278835	192.168.1.101	192.168.1.1	RADIUS	Access-challenge(11) (id=0, l=117)
213	958.283106	192.168.1.1	192.168.1.101	RADIUS	Access-Request(1) (id=0, l=227)
214	959.284162	192.168.1.101	192.168.1.1	RADIUS	Access-Reject(3) (id=0, l=44)

Figura 5. 16 Tráfico de rechazo entre el servidor y el cliente

De la misma manera en el modo depurador Figura 5.17, se puede observar como es rechazada la solicitud con un mensaje Access-Reject.

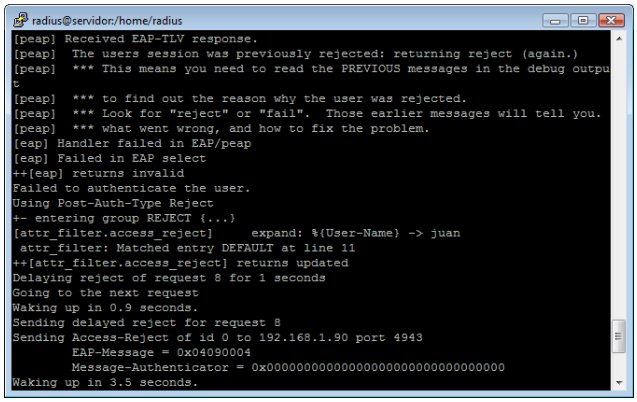


Figura 5. 17 Modo depurador de RADIUS

5.5 Políticas de Seguridad

La creación de las políticas de seguridad tiene como finalidad, proporcionar el mayor nivel de detalle a los usuarios y administradores, para cumplir con los mecanismos que deben desempeñar y utilizar, para proteger los componentes de los sistemas de la ESIME Zacatenco.

Y en sí, las políticas de seguridad informática se presentan como una herramienta organizacional, para tener presente la importancia y sensibilidad de la información y servicios, que se prestan única y exclusivamente a los profesores de la ESIME Zacatenco, por lo tanto, el identificar o proponer una política de seguridad requiere una gran agudeza técnica, para detectar fallas y debilidades, así como tener un gran compromiso, tener una constante actualización de dichas políticas. Las cuales no se pueden considerar que sea una descripción técnica de mecanismos, ni mucho menos una expresión legal que involucre sanciones a los usuarios de la red, es más bien una descripción de lo que se desea proteger y el porqué de ello. Por tal motivo, deben concluir en una posición consciente y vigilante de los usuarios, teniendo en cuenta las limitaciones de los recursos y servicios informáticos que tienen permitido utilizar.

Para su mayor entendimiento, es necesario puntualizar los componentes de una política de seguridad:

- Política de privacidad
- Política de acceso
- Política de uso
- Política de mantenimiento para la red

5.5.1 Política de Privacidad

Para establecer las políticas de privacidad, es necesario identificar y seleccionar la información que se desea proteger, por lo tanto para la implementación, se establecerá como política:

- Buscar la protección de la información que se encuentra en las computadoras de los profesores, así como la de los servidores académicos.

5.5.2 Políticas de Acceso

Para establecer este tipo de políticas, es necesario especificar cómo deben conectarse al sistema, desde dónde y de qué manera deben autenticarse.

- Los usuarios accederán al sistema por medio de un certificado de autenticación que el mecanismo le otorga, al momento de intentar establecer una conexión a Internet, generado con la información personal.
- Queda prohibido prestar las contraseñas de acceso, así como los certificados personales.

5.5.3 Políticas de uso

Especifica lo que se considera un uso adecuado o inadecuado del sistema por parte de los usuarios, así como lo que está permitido y lo que está prohibido, dentro de la red.

- Está estrictamente prohibido, ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios.
- Prohibido utilizar programas espías, o analizadores de tráfico.

5.5.3 Políticas de mantenimiento de la red

En estas políticas se especifican las acciones que se deben de tomar, para un funcionamiento excelente de la red, como son la constante revisión de los puntos de acceso, y la distribución de direcciones IP, a las computadoras de los accesos.

- Está prohibido realizar un cambio de dirección IP del equipo que está asignado al usuario.

Por último tenemos que tener claro, que a pesar de los esfuerzos para definir directrices de seguridad, existe un gran número de personas mal intencionadas, que buscan el uso de información para su beneficio, y también el descuido de los mismos usuarios en mantener sus contraseñas seguras.

Conclusiones

Por medio de una encuesta, se llevó a cabo el análisis de la problemática existente de los usuarios de los anexos de profesores, con la cual detectamos las vulnerabilidades, carencias en el control de acceso, la necesidad de una administración y seguridad más robusta, dando como resultado la consideración de los diferentes mecanismos, y protocolos de seguridad que nos condujeron a la siguiente propuesta, eligiendo el sistema operativo Linux, dado que cuenta con un soporte en seguridad, como son las herramientas para protecciones contra ataques Zero-Day (ataques basados en vulnerabilidades que no han sido corregidas por los fabricantes y desarrolladores a tiempo), herramientas como SELinux o AppArmor, a su vez Linux cuenta con mejores herramientas de gestión, que genera que las actualizaciones afecten a todos los componentes, y no como Windows, que espera que la actualización sea parchada, brindando a su vez mejor configuración de serie, ya que fue diseñado como un sistema multiusuario, y como tal, los ficheros importantes están protegidos aun cuando la identidad de usuario se vea comprometida. Hoy en día montar redes en Linux, es sin duda una apuesta por la seguridad y la estabilidad. Un administrador de sistemas, debe proporcionar a los usuarios el entorno más eficiente y seguro posible, independientemente del sistema operativo. En Linux hay un único administrador root, quien se encarga de garantizar esa seguridad, también cuenta con un diseño modular que facilita la desactivación de componentes del sistema, que se encuentran fallando para que estos no ocasionen problemas, y como punto fundamental, la constitución de una arquitectura open source, de modo que cualquiera puede colaborar para la corrección de fallos de toda la diversidad de entornos que Linux presenta. Debido a estos detalles que Linux nos brinda, así como la utilización de diversos software de forma gratuita. Se enfocó este proyecto en el cumplimiento de las características de la norma 802.1X, como son la forma de acceder al medio, apoyándose en diversos protocolos de seguridad, para lo que fue necesario instalar un servidor RADIUS, el cual utilizara EAP-TLS por medio de openssl, cifrado de certificados en md5 por medio de RSA, y cuenta con un punto de acceso, esto para llevar a

cabo la implementación. Realizando el análisis con lo que actualmente cuenta la red, se tenderá a que es necesario implementar el sistema para aumentar la seguridad, por medio de la incorporación de un servidor RADIUS que almacena los usuarios, contraseñas y certificados, realizando la autentificación por medio de una corroboración del solicitante con lo existente en la base de datos, expidiendo un certificado, el cual es fácil de utilizar, ya que se almacena en la máquina del usuario y automáticamente realiza, la operación entre el servidor, el cual se tiene que renovar periódicamente para mantener la seguridad. El sistema que se incorporó en una PC con las especificaciones mencionadas en el estudio económico, podría brindar una capacidad de usuarios, en paralelo con las características del punto de acceso, y la red en la que se incorporará.

Se recomienda para ampliar el sistema, ya que pueden interactuar con otros servidores RADIUS.

Apéndice 1

El sistema a utilizar en la configuración del servidor RADIUS a implementar es Fedora 10, al cual se le realizarán las actualizaciones más recientes del proyecto Fedora [14], para poder alcanzar un funcionamiento más óptimo, esta distribución de Linux es de propósitos generales basada en RPM, mantenida gracias a una comunidad internacional de ingenieros, diseñadores gráficos y usuarios que informan de fallos y prueban nuevas tecnologías. Contando con el respaldo de la promoción Red Hat. Dentro los puntos más relevantes y de mayor interés para nosotros es la seguridad que es proporcionada por la arquitectura SELinux, la cual se destaca entre las características de seguridad de Fedora, ya que implementa una gran variedad de políticas de seguridad, incluyendo control de acceso obligatorio (MAC "Mandatory Access Control"), a través de los Módulos de Seguridad de Linux que están en el núcleo Linux del Sistema.

Para realizar el proceso de instalación de Fedora, necesitaremos:

- Un CD o DVD o un dispositivo USB vacío de por lo menos 1GB
- Un procesador de 400 MHz o más rápido
- Como mínimo 512 MB de memoria (RAM), aunque para un mejor desempeño se recomienda 1 GB
- Como mínimo 10 GB de espacio en el disco duro

En el momento que contemos con un equipo con mínimo estas características, es necesario descargar la imagen ISO de la página oficial del proyecto Fedora y grabarlo en el CD, DVD o USB.

Instalación

Insertando el CD, DVD o USB en la computadora seleccionada para la instalación comenzará a leer la información para proceder a la instalación, las pantallas que se presentan son muy explícitas, la primer pantalla Figura A1 1, preguntará si queremos confirmar la integridad de los archivos del CD, DVD o USB o deseamos entrar al proceso de instalación.

Figura A1 1 Selección de proceso de instalación o verificación de datos

Al momento de seleccionar el proceso de instalación se inicia el ambiente gráfico Figura A1 2, el cual nos guiará hasta finalizar la instalación.

Figura A1 2 Proceso de instalación inicio de modo gráfico

El primer paso es elegir el idioma del sistema Figura A1 3, como la configuración del teclado, Figura A1 4.

Figura A1 3 Selección de idioma del Sistema

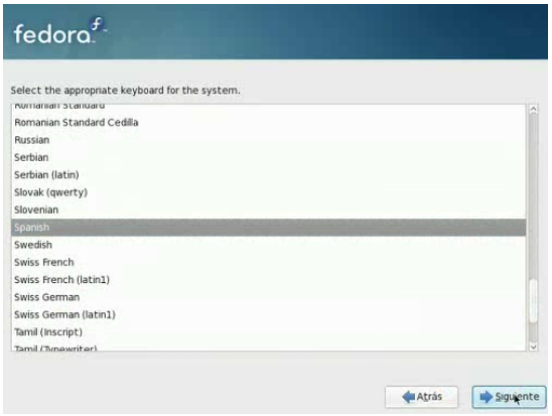


Figura A1 4 Selección del idioma del teclado

El siguiente paso será asignarle un nombre al equipo, Figura A1 5.

Figura A1 5 Nombre del Equipo

Se seleccionará la zona geográfica en la que nos encontramos Figura A1 6.

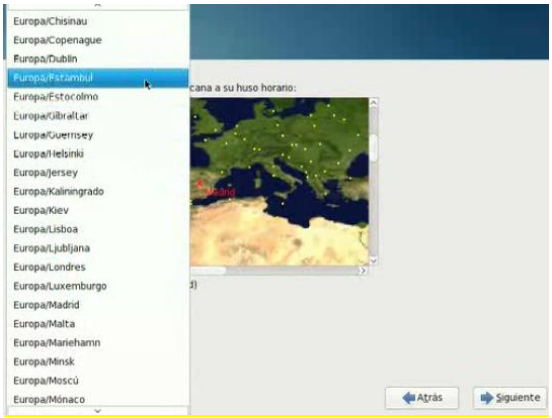


Figura A1 6 Selección de Zona geográfica

Configuración de contraseña de root figura A1 7.

Figura A1 7 Configuración de contraseña de root

La opción siguiente figura A1 8, es muy importante si se tiene otro sistema operativo instalado y se desea conservar, ya que es necesario redimensionar las particiones existentes.

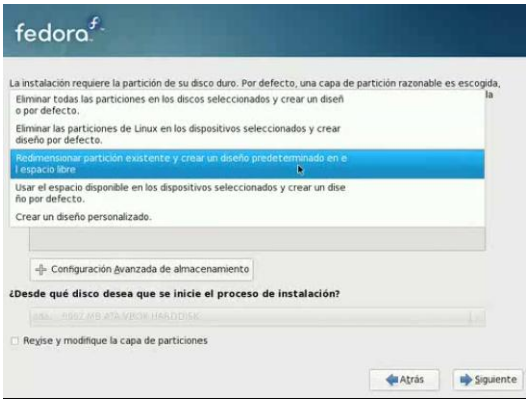


Figura A1 8 Selección de tipo de instalación

En la siguiente opción particionamos el disco en su parte primaria figura A1 9, y creamos el espacio de intercambio swap figura A1 10, que por recomendación de cualquier instalación Linux, debe ser al menos el doble de la memoria RAM que tenemos. Al momento de estar completamente seguros guardamos los cambios en el disco duro figura A1 11.

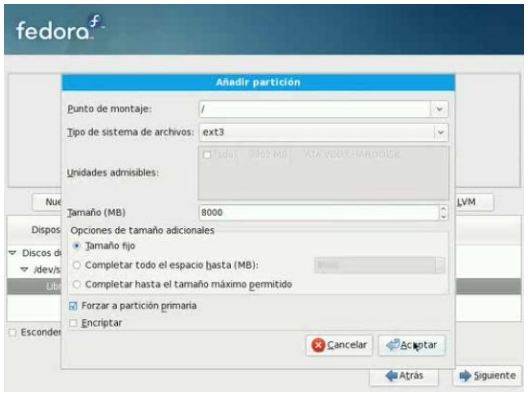


Figura A1 9 Creación de partición primaria

Figura A1 10 Creación de memoria de intercambio swap

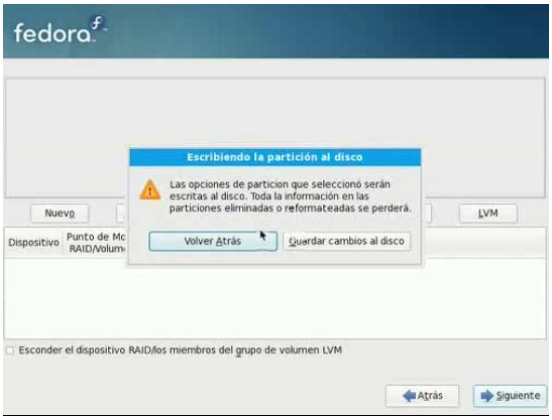


Figura A1 11 Guardar cambios en el Disco duro

Antes de instalar propiamente el sistema, nos preguntará si queremos instalar el gestor de arranque figura A1 12. Así como seleccionar la instalación de otras aplicaciones como desarrollo de software y servidor Web figura A1 13.

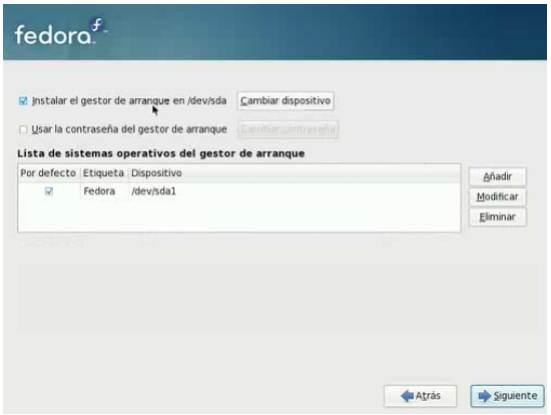


Figura A1 12 Crear gestor de arranque

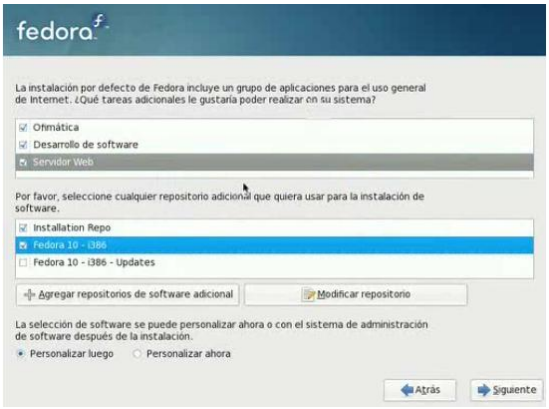


Figura A1 13 Selección de paquetes adicionales

Después de haber seleccionado los paquetes que se desean instalar se procede a realizar la instalación, que tardará un tiempo promedio de 1 hora dependiendo de la velocidad de la computadora, o la cantidad de paquetes a instalar figura A1 14.

Figura A1 14 Instalación de sistema

Y nos damos la tarea para arrancar el sistema por primera vez figura A1 15, pasando por la presentación figura A1 16, información de licencia figura A1 17, creación de usuario figura A1 18, configuración básica de la zona horaria del sistema figura A1 19, así como la solicitud de envío de hardware al proyecto Fedora y comenzar su uso.

Figura A1 15 Inicio del Sistema

Figura A1 17 Información de licencia

Figura A1 16 Pantalla de bienvenida

Figura A1 18 Creación de Usuario

Figura A1 19 Configuración zona horaria

Que pueda proporcionar la hora y fecha confiable, ya que procederá de un servidor que reciba la información lo más directo posible de un reloj atómico.

La configuración de NTP en el servidor se realiza en el archivo /etc/ntp.conf figura A1 20, donde se agregarán los servidores de donde se tomará la hora, para asignarla a nuestra red local y comportarse como servidor NTP dentro de ella.

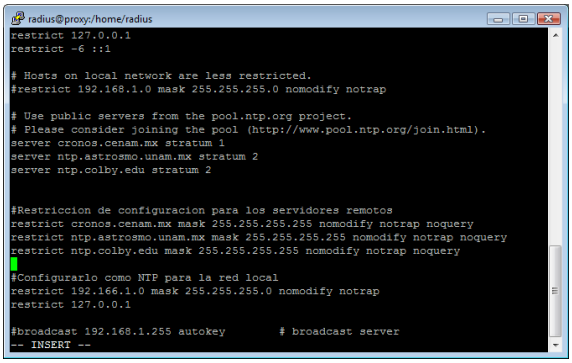


Figura A1 20 Configuración del archivo ntp.conf

Ahora si podemos proceder a instalar freeRADIUS, para esto realizamos primero el listado de los paquetes, que se encuentra disponibles con el comando yum search freeRADIUS figura A1 21.

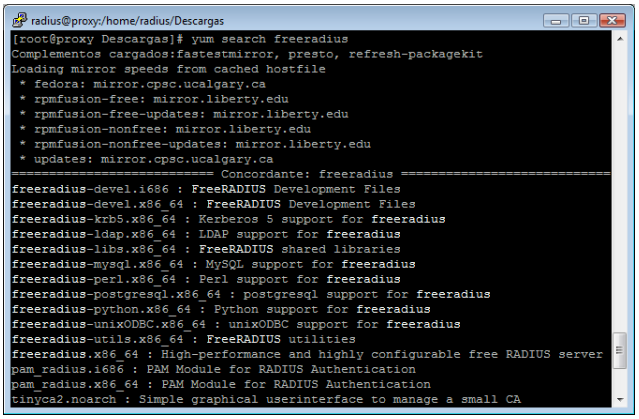


Figura A1 21 Lista de paquetes complementarios de freeRADIUS

De la lista seleccionaremos la siguiente lista de repositorios:

- freeRADIUS.x86_64
- freeRADIUS-ldap.x86_64 : LDAP support for freeRADIUS
- freeRADIUS-libs.x86_64 : FreeRADIUS shared libraries
- freeRADIUS-mysql.x86_64 : MySQL [16] support for freeRADIUS
- freeRADIUS-python.x86_64 : Python support for freeRADIUS
- freeRADIUS-utils.x86_64 : FreeRADIUS utilities

Identificando estos repositorios ejecutamos el comando yum install "nombre del repositorio", y se comenzarán a instalar los paquetes requeridos. Teniendo freeRADIUS instalado en nuestro servidor procedemos a arrancar, los servicios con el comando service radiusd start el demonio es activado, y comienza a ejecutar su configuración. Con los comandos service radius stop detenemos el servicio con service radiusd status. verificamos si el proceso está en ejecución, figura A1 22.

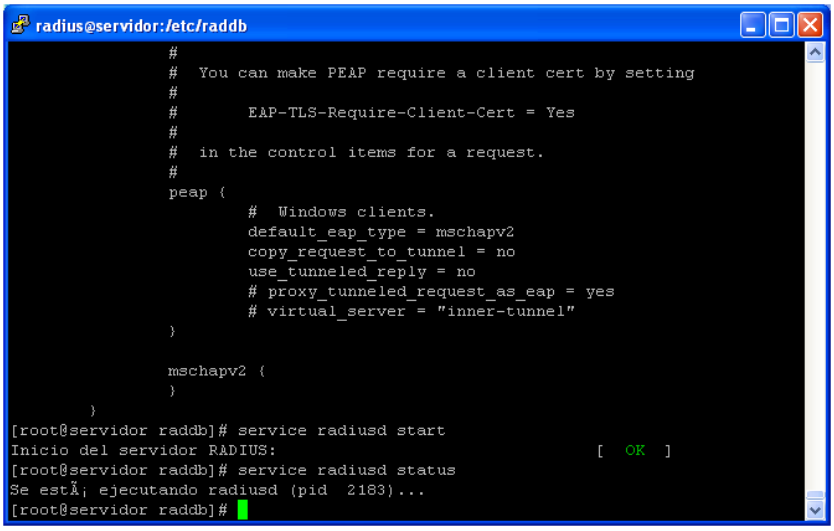


Figura A1 22 Inicializar servicio de freeRADIUS

La configuración de freeRADIUS se realiza principal mente dentro del directorio /etc/raddb/, donde se encuentran todos los archivos, que se pueden modificar para adecuarlo a nuestras necesidades. Los archivos en los que nos vamos a enfocar van a ser 4 radius.conf, clients.conf, EAP.conf y users.

Archivo radius.conf

Este archivo contiene la configuración principal, que tendrá nuestro servidor RADIUS para su funcionamiento, como las directivas de los demás archivos de configuración que serán leídos por freeRADIUS, desde este fichero.

```
prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = /usr/sbin
logdir = ${localstatedir}/log/radius
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct
#
listen {
        type = auth
        ipaddr = *
        #  Port on which to listen.
        #  Allowed values are:
        #       integer port number (1812)
        #       0 means "use /etc/services for the proper port"
        port = 0
#       interface = eth0
}

#  This second "listen" section is for listening on the accounting port, too.
listen {
        ipaddr = *
#       ipv6addr = ::
        port = 0
        type = acct
#       interface = eth0
#       clients = per_socket_clients
}
```

Archivo clients.conf

Este archivo es el encargado de almacenar la información del punto de acceso al que estará conectado el servidor, y pueda realizar su comunicación adecuada.

```
##
## clients.conf -- client configuration directives
##
##      $Id$
#############################################################################
client localhost {
        secret          = testing123
        require_message_authenticator = no
        shortname       = localhost
        nastype     = other     # localhost isn't usually a NAS...
}


client 192.168.1.90 {
                        secret = testing123
                        shortname = AP RADIUS
                        nastype = cisco
                }
```

Archivo eap.conf

La modificación de este archivo de configuración, se realiza para que el servidor identifique el método de autentificación EAP con el que se va activar, en este caso lo configuraremos para realizar autenticación EAP-TLS, por medio de certificados digitales.

```
eap {
        default_eap_type = mschapv2 #md5
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
                tls {
                certdir = /etc/certs/server
                cadir = ${confdir}/certs/masterCA
                private_key_password = 802.1x
                private_key_file = /etc/certs/server/radius1_keycert.pem
                certificate_file = /etc/certs/server/radius1_keycert.pem
                CA_file = ${cadir}/cacert.pem
                dh_file = /etc/certs/dh
                random_file = /etc/certs/random
                cipher_list = "DEFAULT"
                cache {
                      enable = no
                      lifetime = 24 # hours
                      max_entries = 255
                        }
                }

        ttls{
                default_eap_type = md5
                copy_request_to_tunnel = no
                use_tunneled_reply = no
                #virtual_server = "inner-tunnel"
                #include_length = yes
        }
        peap {
                #  Windows clients.
                default_eap_type = mschapv2
                copy_request_to_tunnel = no
                use_tunneled_reply = no
                # proxy_tunneled_request_as_eap = yes
                # virtual_server = "inner-tunnel"
        }
        mschapv2 {
        }
}
```

Archivo users

En este archivo se podrán declarar los usuarios que deseemos, con sus correspondientes atributos. Este archivo es recomendable utilizar únicamente en las primeras pruebas de autenticación, ya que para una administración mucho más favorable, se puede configurar una base de datos mucho más sofisticada, para esto utilizando mysql, sql, Oracle, etc.

```
"uriel" User-Password := "802.1x"
        Framed-IP-Address = 192.168.0.105,
        Framed-IP-Netmask = 255.255.255.0,
        Framed-Routing = Broadcast-Listen,
        Reply-Message = "Estas conectado, %{User-Name}"
"Fernando" User-Password := "Noya"
        Reply-Message = "%{User-Name} estas conectado"

"Cliente Windows 1" Auth-Type := Accept
        Reply-Message = "%{User-Name} estas conectado"

```

Glosario

AAA

Las propuesta de los protocolos y sistemas AAA son desarrollados por el grupo de trabajo AAA de la IETF (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., 49

Demonio

Son procesos que se ejecuta en segundo plano, 112

IP

Acrónimo de Protocolo de Internet el cual 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 no fiable de mejor entrega posible sin garantias., ix

LAN

Acrónimo de Local Area Network (Red de Área Local), vii

MAC

Acrónimo de Media Access Control o control de acceso al medio., viii

OSI

Acrónimo de Open Systems Interconnection (Interconexión abierta entre sistemas)., vii

RADIUS, 94

Acrónimo de Remote Authentication Dial-In User Server, 16

RPM

Originalmente llamado Red Hat Package Manager, pero se convirtió en acrónimo recursivo[1]) es una herramienta de administración de paquetes pensada básicamente para GNU/Linux, 104

SELinux

Acrónimo de Security-Enhanced Linux, Seguridad Mejorada de Linux) es una característica de seguridad de Linux que provee una variedad de políticas de seguridad, incluyendo el estilo de acceso a los controles del Departamento de Defensa de Estados Unidos, a través del uso de módulos de Seguridad en el núcleo Linux. No es una distribución de Linux, sino un set de modificaciones que puede ser aplicado a un sistema Tipo-Unix como Linux y BSD, 107

swap

Acrónimo de Information Technology o Tecnología de la Información, 107

TI

Acrónimo de Information Technology o Tecnología de la Información, 15

WEP

Acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado, viii

Wi-Fi

Acrónimo de Wireless Fidelity o Fidelidad Inalámbrica, 15

WPA

Acrónimo de Wireless Application Protocol o Protocolo de Aplicaciones Inalámbricas., viii

Referencias

[1] http://www.ruckuswireless.com/company/more SUNNYVALE, CA - 24 de mayo 2010 - Ruckus Wireless

[2] Entrevista a Edgar Figueroa, Director Ejecutivo de Wi Fi Alliance 02/09/2009 http://www.pcwla.com/pcwla2.nsf/noticias_de_it/

[3] http://www.librosmaravillosos.com/inventos/capitulo11.html

[4] Evolución de las redes inalámbricas Publicado el 11 de Febrero, 2008, *www.maestrosdelweb.com*

[5] Introducción a WiFi (802.11) kioskea está puesto a disposición bajo la licencia Creative Commons. Puede copiar, modificar bajo las condiciones puestas por la licencia, siempre que esta nota sea visible (es.kioskea.net).

[6] http://www.virusprot.com/Nt120542.html

[7] *http://www.idg.es/pcworldtech/mostrararticulo.asp?id=177008&seccion=seguridad*

[8] Ing. Pablo Fidel Gómez Vergara: Arquitectura Unificada para Control de Acceso en Redes Inalámbricas Seguras, Universidad de Mendoza Facultad de Ingeniería, Agosto de 2007.

[9] http://www.openssh.org/es/manual.html

[10] http://www.openssl.org/

[11 http://blyx.com/public/wireless/Seguridad_en_el_aire.pdf

[12] http://www.scribd.com/doc/14115805/PKI

[13] http://freeradius.org/

[14] Página oficial de la comunidad responsable de la producción de la distribución Linux Fedora http://fedoraproject.org

[15] Configuración EAP http://dns.bdat.net/seguridad_en_redes_inalambricas/x80.html

[16] http://www.mysql.com/