INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACÁN

SEMINARIO DE TITULACIÓN
"SEGURIDAD DE LA INFORMACIÓN"

TESINA

"Diseño de un Sistema de Seguridad de Control de Acceso con RADIUS configurado en un Sistema Operativo LINUX para una LAN Inalámbrica"

QUE PRESENTAN PARA OBTENER EL TÍTULO DE
LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

CÓRDOBA TÉLLEZ ANABEL
DURÁN MARTÍNEZ GRICEL
FLORES SÁNCHEZ VERÓNICA

Asesores:
DR. GABRIEL SÁNCHEZ PÉREZ
ESP. LIDIA PRUDENTE TIXTECO

VIGENCIA: DES/ESIME-CUL-2008/23/1/09

México, D.F., Abril 2010

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

POR LA OPCIÓN DE TITULACIÓN SEMINARIO EN SEGURIDAD DE LA INFORMACIÓN

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

DEBERÁN DESARROLLAR:

CÓRDOBA TÉLLEZ ANABEL
DURÁN MARTÍNEZ GRICEL
FLORES SÁNCHEZ VERÓNICA

"DISEÑO DE UN SISTEMA DE SEGURIDAD DE CONTROL DE ACCESO CON RADIUS CONFIGURADO EN UN SISTEMA OPERATIVO LINUX PARA UNA LAN INALÁMBRICA"

INTRODUCCIÓN

LAS REDES INALÁMBRICAS NO SON CIEN POR CIENTO SEGURAS, SE HAN PRESENTADO ATAQUES EN LOS QUE CUALQUIER PERSONA QUE POSEE UNA TARJETA INALÁMBRICA Y QUE SE ENCUENTRE DENTRO DE LA ZONA DE COBERTURA, TENGA LA POSIBILIDAD DE ACCESAR A LA RED INALÁMBRICA. DEBIDO A LAS VULNERABILIDADES QUE EN LA ACTUALIDAD SE PRESENTAN EN LAS REDES INALÁMBRICAS POR LA FALTA DE UN SISTEMA DE SEGURIDAD Y LA AUSENCIA DE APLICACIÓN DE POLÍTICAS DE SEGURIDAD, EN ESTE PROYECTO DE INVESTIGACIÓN SE PROPONE LA IMPLEMENTACIÓN DE UN CONTROL DE ACCESO CON RADIUS CONFIGURADO EN UN SISTEMA OPERATIVO LINUX PARA CONTROLAR EL ACCESO A UNA RED DE ÁREA LOCAL INALÁMBRICA, DICHO CONTROL SE CONFIGURARÁ PARA VALIDAR LA AUTENTICACIÓN DE LOS USUARIOS A LA RED.

CAPITULADO

I. SEGURIDAD EN REDES DE DATOS
II. RADIUS
III. DISEÑO DE UN CONTROL DE ACCESO UTILIZANDO RADIUS

México D.F., Abril de 2010

VIGENCIA: DES/ESIME-CUL-2008/23/1/09

DR. GABRIEL SÁNCHEZ PÉREZ
Coordinador del Seminario

ESP. LIDIA PRUDENTE TIXTECO
Instructora del Seminario

M. EN C. LUIS CARLOS CASTRO MADRID
Jefe de la carrera de I.C.

ÍNDICE GENERAL

OBJETIVO GENERAL I
OBJETIVOS ESPECÍFICOS I
JUSTIFICACIÓN II
INTRODUCCIÓN III
CAPÍTULO I. SEGURIDAD EN REDES DE DATOS 1
1.1 Redes de Datos 1
1.2 Tipos de Redes 4
1.3 Seguridad en redes de datos 12
1.3.1 Manejo de Riesgos 14
1.3.2 Políticas de Seguridad Informática 15
1.4 Control de acceso a la red 16
1.4.1 Tipos de Control de Acceso a la Red 17
1.4.2 Operación de un Control de Acceso a la Red 19
1.4.3 Elementos de un Control de Acceso a la Red 20
1.5 Arquitectura AAA 20
1.5.1 Autenticación 23
1.5.2 Autorización 24
1.5.3 Accounting 26
1.6 Seguridad en redes inalámbricas 27
1.6.1 Mecanismos de protección de redes inalámbricas 28
CAPÍTULO II. RADIUS 30
2.1 Introducción a RADIUS 30

2.1.1Orígenes 30
2.1.2 Descripción del protocolo 31
2.1.3 Multiplataforma 33
2.2 Métodos de autenticación 33
2.2.1 Autenticación simple y autenticación mutua 36
2.2.2 Tipos de Autenticación 36
2.2.3 Reautenticación 38
2.3 Estructura de las comunicaciones RADIUS 38
2.3.1 Estructura de un mensaje RADIUS 38
2.3.2 Secuencia de autenticación de RADIUS 40
CAPÍTULO III.DISEÑO DE UN CONTROL DE ACCESO UTILIZANDO RADIUS 43
3.1 Antecedentes y Problemática 43
3.2 Propuesta de Solución 44
3.3 Desarrollo 44
3.3.1 Instalación de FreeRADIUS. 47
3.3.2 Configuración de los archivos de FreeRADIUS 47
3.3.3 Arranque de FreeRADIUS 51
3.3.4 Configuración de AP 52
3.3.5 Configuración de cliente Windows para autentificar en FreeRADIUS 53
3.3.6 Funcionamiento 55
CONCLUSIONES 57
GLOSARIO 58
REFERENCIAS 61
ANEXOS 62

ÍNDICE DE FIGURAS

Figura 1.1 Interconexión de los dispositivos en red....2
Figura 1.2 Red de Área Local....3
Figura 1.3 Redes LAN, MAN y WAN....4
Figura 1.4 Red alámbrica....5
Figura 1.5 Componentes de una Wireless LAN....8
Figura 1.6 Topología BSS. Basic Service Set....10
Figura 1.7 Topología ESS. Extended Service....11
Figura 1.8 Topología IBSS. Independent Basic Service Set....11
Figura 1.9 Equilibrio entre las necesidades empresariales y la seguridad informática....12
Figura 2.1 Infraestructura simple RADIUS....33
Figura 2.2 Estructura de un paquete RADIUS....39
Figura 2.3 Secuencia AAA de RADIUS....43
Figura 3.1 Elementos del Control de Acceso....47
Figura 3.2 Archivo radiusd.conf....49
Figura 3.3 Archivo users....50
Figura 3.4 Archivo clients.conf....50
Figura 3.5 Script para arrancar FreeRADIUS....53
Figura 3.6 Configuración del Access Point....54
Figura 3.7 Propiedades de la red inalámbrica....55
Figura 3.8 Solicitud de autenticación....55
Figura 3.9 Denegación de acceso a la red....56
Figura 3.10 Aceptación de acceso a la red....57

ÍNDICE DE TABLAS

Tabla 2.1 Comparación de los principales métodos EAP……..……36
Tabla 2.2 Valores del campo código……40
Tabla 2.3 Atributos RADIUS……..41
Tabla 3.1 Infraestructura para la implementación del Control de Acceso……..47

OBJETIVO GENERAL

Proponer e implementar el diseño de un Sistema de Seguridad de Control de Acceso con RADIUS configurado en un Sistema Operativo Linux para controlar la autenticación de los usuarios en el acceso a una Red de Área Local Inalámbrica.

OBJETIVOS ESPECÍFICOS

Describir los conceptos básicos relacionados con la Seguridad Informática y el Control de Acceso.

Entender cómo funcionan las tecnologías inalámbricas existentes, así como los mecanismos de seguridad que se pueden enfocar a éstas.

Investigar y describir conceptos relacionados con la autenticación y el protocolo RADIUS, así como las especificaciones que faciliten su uso.

Proponer políticas para el control de acceso a una red, mediante la instalación y configuración de FreeRADIUS en un Sistema Operativo LINUX.

JUSTIFICACIÓN

La seguridad es un aspecto que cobra especial relevancia cuando se habla de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red, sin embargo, en una red inalámbrica, un tercero podría acceder a la red sin la necesidad de estar ubicado en las instalaciones de una empresa, sólo bastaría estar en un lugar próximo donde llegara la señal si la red no estuviera convenientemente protegida.

El canal de las redes inalámbricas, al contrario que en las redes cableadas, debe considerarse inseguro, ya que cualquiera podría estar escuchando la información que se transmite y podría modificarla.

Por lo anterior, es importante contar con un sistema de seguridad para una red inalámbrica que permita controlar el acceso a ella como medio de protección y evitar amenazas por el ingreso a la red de personas y equipos no autorizados.

INTRODUCCIÓN

Las redes inalámbricas no son cien por ciento seguras, se han presentado ataques en los que cualquier persona que posee una tarjeta inalámbrica y que se encuentre dentro de la zona de cobertura, tiene la posibilidad de accesar a la red inalámbrica.

Debido a las vulnerabilidades que en la actualidad se presentan en las redes inalámbricas por la falta de un sistema de seguridad y la ausencia de aplicación de políticas de seguridad, en este proyecto de investigación se propone la implementación de un control de acceso con RADIUS configurado en un Sistema Operativo Linux para controlar el acceso a una Red de Área Local Inalámbrica. Se instalará la solución de código abierto FreeRADIUS 2.1 el cual se configurará para validar la Autenticación de los usuarios a la Red.

RADIUS es un protocolo ampliamente empleado para controlar el acceso a los servicios de la red. El presente trabajo de investigación propone un Sistema de Seguridad basado en el protocolo RADIUS el cual permite gestionar la "autenticación, autorización y arqueo" de usuarios remotos sobre un determinado recurso.

En este trabajo de investigación se explicará también la definición de este protocolo, la definición de redes de datos, el concepto de redes inalámbricas y la seguridad en este tipo de redes.

CAPÍTULO I. SEGURIDAD EN REDES DE DATOS

1.1 Redes de Datos

Una red de datos es un sistema de comunicación entre computadoras que permite la transmisión de datos de una máquina a otra con lo que se lleva a cabo un intercambio de todo tipo de información y de recursos [1]. Una red está integrada por los siguientes componentes:

- Clientes. Usuarios de la red, como PC´s, laptops, impresoras, cámaras, teléfonos, etc.
- Servidores de aplicaciones y bases de datos.
- El hardware de red, que comprende la infraestructura física de la red, a la cual se conectan los clientes y servidores. Como ejemplos se tienen a los switches y hubs, routers, gateways, access points y tarjetas de red.
- El medio en una red interconecta todos los componentes de la red. La conexión se puede llevar a cabo utilizando cables, fibra óptica e incluso el aire.
- Por último se encuentran los protocolos de red, los cuales sirven como estándar de comunicación entre los componentes de la red.

En la figura 1.1 se puede apreciar la interconexión de los dispositivos de una red.

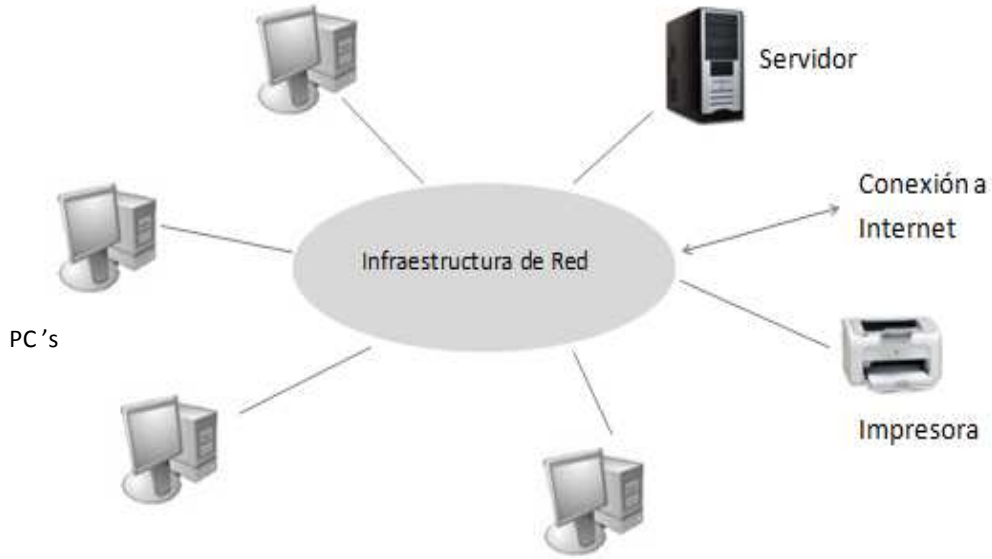
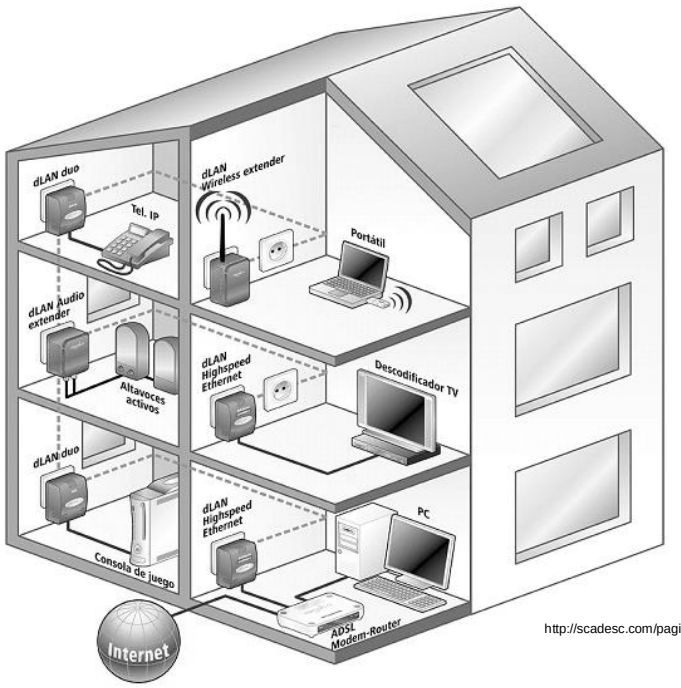


Figura 1.1 Interconexión de los dispositivos en red

Las redes se pueden clasificar de acuerdo a diferentes criterios, los cuales de acuerdo a su cobertura se clasifican en redes LAN, WAN y MAN y cuya breve descripción se explica a continuación:

- Redes de Área Local, LAN (***Local Area Networks***). Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología. Una LAN también puede definirse como la interconexión de varios equipos y dispositivos. Su extensión está limitada físicamente a un edificio o a un entorno no muy distante y su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas, en la figura 1.2 se ejemplifica una red de área local.



http://scadesc.com/pagina/red%20lan.jpg

Figura 1.2 Red de Área Local

- Redes de Área Metropolitana, MAN (***Metropolitan Area Network***). La MAN es una red que abarca un área metropolitana. Una MAN, generalmente consta de una o más redes de tipo LAN dentro de un área geográfica común. El concepto de MAN representa una evolución del concepto de LAN, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de tipo MAN. Es una red de alta velocidad que, dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado.
- Redes de Área Amplia, WAN (***Wide Area Network***). Es un tipo de red de computadoras que puede cubrir distancias desde 100 hasta 1000 km, dando el servicio a un país o a un continente.

Las WAN son construidas para una organización y son de uso privado, otras son construidas por los Proveedores de Servicio de Internet, ISP (***Internet Service Provider***) para proveer de conexión a sus clientes y permiten que las computadoras, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes, proporcionando comunicaciones instantáneas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias [2]. En la figura 1.3 se puede apreciar la conexión de las LAN, MAN y WAN.

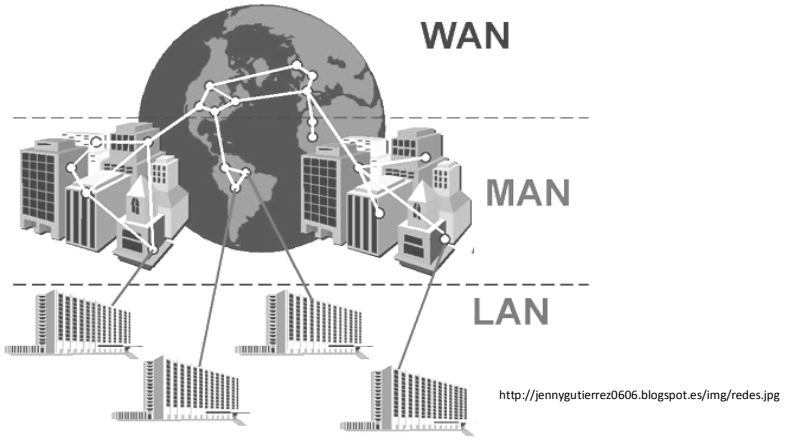


Figura 1.3 Redes LAN, MAN y WAN

1.2 Tipos de Redes

Otro tipo de clasificación de redes que compete a este proyecto es la que se hace de acuerdo al medio de comunicación que se utiliza. Cuando se utilizan medios guiados, como cable coaxial, cable de par trenzado y fibra óptica, se denomina a las redes como redes alámbricas. Si el tipo de medio que se utiliza es radio, infrarrojo o microondas, las redes son llamadas redes inalámbricas. A continuación se explica brevemente en qué consisten las redes alámbricas y para efectos de este trabajo se explica con mayor detalle la definición de redes inalámbricas:

- Redes Alámbricas ó wired networks. Se comunican a través de cables de datos en tecnologías IEEE 802.3 (Ethernet). Los cables de datos, conocidos como cables de red conectan computadoras y otros dispositivos que forman las redes. Las redes alámbricas son mejores cuando se necesita mover grandes cantidades de datos a altas velocidades. Entre las ventajas de las redes alámbricas se tiene que, si se planean correctamente, sus costos de instalación son relativamente bajos, ofrecen un buen rendimiento, y cuentan con gran velocidad. En la mayoría de las organizaciones se utiliza este tipo de red. Algunas desventajas que pueden presentar este tipo de redes son el paso de los cables a través del acceso físico, en caso de que no se planeen correctamente pueden tener costos de instalación altos, pueden presentar dificultad en su expansión y se requiere que los dispositivos se encuentren físicamente en un nodo de la red para poder operar. En la figura 1.4 se puede apreciar la conexión entre los dispositivos de una red alámbrica.

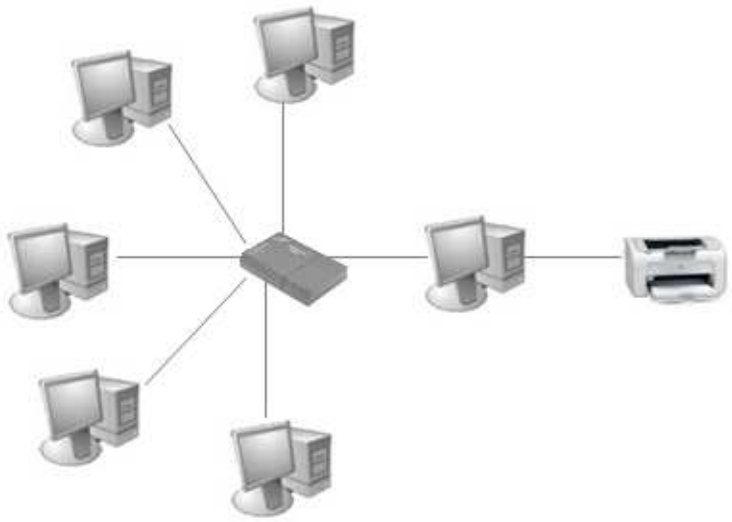


Figura 1.4 Red alámbrica

- Redes inalámbricas o wireless networks. Son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de

antenas. Cuentan con la libertad y la flexibilidad de operar dentro y entre edificios; proporcionan todas las características y ventajas de las tecnologías LAN tradicionales sin las limitaciones de los cables. La libertad de moverse manteniendo la conectividad ha ayudado a que las redes inalámbricas alcancen una gran aceptación [3]. Algunas ventajas de este tipo de redes son:

- Rápida instalación de la red sin la necesidad de usar cableado.
- Movilidad. Los empleados pueden permanecer conectados a la red incluso cuando no se encuentren en sus mesas.
- Accesibilidad. Todos los equipos portátiles y la mayoría de los teléfonos móviles de hoy día vienen equipados con la tecnología Wi-Fi necesaria para conectarse directamente a una LAN inalámbrica.
- Productividad. El acceso a la información y a las aplicaciones clave de una empresa ayuda a su personal a realizar su trabajo y fomentar la colaboración.
- Escalabilidad. Conforme crecen las operaciones comerciales de una empresa, puede que se necesite ampliar la red rápidamente. Generalmente, las redes inalámbricas se pueden ampliar con el equipo existente, reduciendo costos, mientras que una red cableada puede necesitar cableado adicional.

Las redes inalámbricas, además, se clasifican de acuerdo a la cobertura que abarcan en Redes de Área Local Inalámbricas, Wireless LANs (***Wireless Local Area Networks***), Redes de Área Metropolitana Inalámbricas, Wireless MANs (***Wireless Metropolitan Area Networks***) y Redes de Área Amplia Inalámbricas, Wireless WANs (***Wireless Wide Area Networks***), las cuales se describen a continuación, haciendo mayor

hincapié en las Wireless LANs, debido a que el Sistema de Seguridad que se propone en este proyecto es para este tipo de redes.

- Wireless LANs. Las Wireless LANs proporcionan las características de las redes alámbricas, y agregan las ventajas de las redes inalámbricas, como la movilidad de usuarios. En estas redes se pueden encontrar tecnologías inalámbricas basadas en Wi-Fi (***Wireless Fidelity***). Wi-Fi es un conjunto de estándares certificados por una alianza independiente llamada Wi-Fi Alliance.

  Los estándares sobre los que trabaja Wi-Fi forman parte de la serie 802.11 del grupo IEEE y actúan sobre las capas uno y dos del modelo OSI. Enseguida se explica de manera general su modo de funcionamiento y sus componentes:

  - Punto de Acceso, AP (***Access Point***). Es el Servidor de Acceso a la Red, NAS (***Network Access Server***), capaz de trabajar sobre una red de radiofrecuencia, que se utiliza para hacer de intermediario en las comunicaciones inalámbricas entre equipos o para convertir una red cableada en inalámbrica.
  - Identificador de Celda de Servicio, SSID (***Service Set IDentifier***). Es un nombre de red para definir la red a la que se quiere conectar algún usuario. Este nombre de red se divulga por parte del AP mediante beacons, que son pequeños paquetes, los cuales se utilizan para localizar la red, así como para mostrar sus características.
  - Canal. Dependiendo del tipo de red Wi-Fi y de su normativa, el espectro o espacio radioeléctrico asignado para el desempeño de estas redes se divide en canales. Estos canales definen

unas frecuencias fijas de trabajo para los equipos que los utilizan.

- Cobertura. El área o la zona de cobertura de un AP la determina la potencia de transmisión del equipo y el tipo de antena que se va a utilizar, además de otros factores externos como las estructuras de las construcciones o el clima.
- Antenas. Cada antena tiene un diseño diferente, según la direccionalidad de la antena, ésta se puede clasificar en antena isotrópica (que transmite a igual potencia en todos sus ángulos, creando una proyección en forma de una esfera), antena omnidireccional (parecida a la antena isotrópica, transmite en horizontal hacia todos los ángulos), y antena direccional (enfoca mayoritariamente la señal hacia ángulos más concretos) [4]. En la figura 1.5 se pueden apreciar los componentes de una Wireless LAN.

Figura 1.5 Componentes de una Wireless LAN

- Wireless MANs. Para este tipo de redes se encuentran tecnologías basadas en la Interoperabilidad Mundial para Acceso con Microondas, WiMAX (***Worldwide Interoperability for Microwave***

Access), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda.

- Wireless WANs. Las Wireless WANs cubren áreas amplias. La Internet es una WAN de la cual dependen muchas personas y compañías cada día para tener soporte de e-mail, transferencia de archivos y acceso remoto a aplicaciones.

  En estas redes también encontramos tecnologías como las del Sistema Universal de Telecomunicaciones Móviles, UMTS (***Universal Mobile Telecommunications System***), tecnología utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología del Sistema Global para las Comunicaciones Móviles, GSM (***Group Special Mobile***) para móviles de segunda generación (2G). Asimismo, se pueden conectar diferentes localidades utilizando conexiones satelitales o por antenas de radiomicroondas. Estas redes son mucho más flexibles, económicas y fáciles de instalar [4].

Las redes inalámbricas definen varios modelos de estructura dependiendo de su diseño y topología:

- Grupo de Servicio Básico, BSS (***Basic Service Set***). Topología de red formada por un punto de acceso y estaciones inalámbricas. El modelo BBS es el punto de acceso que realiza las funciones de coordinación. Todo el tráfico desde y hacia las estaciones inalámbricas tienen que atravesar el punto de acceso, por lo que hay una clara pérdida de eficiencia cuando dos estaciones dentro de un mismo BSS desean comunicarse entre sí (los paquetes de

información son enviados una vez al punto de acceso y otra vez al destino. Es una arquitectura apropiada cuando la mayor parte del tráfico se origina o finaliza en las redes exteriores a las cuales está conectado el punto de acceso, como se muestra en la figura 1.6. Es el modo que se emplea habitualmente para conectar una red inalámbrica en el hogar ó dentro de una empresa para conectar las estaciones inalámbricas en la LAN.

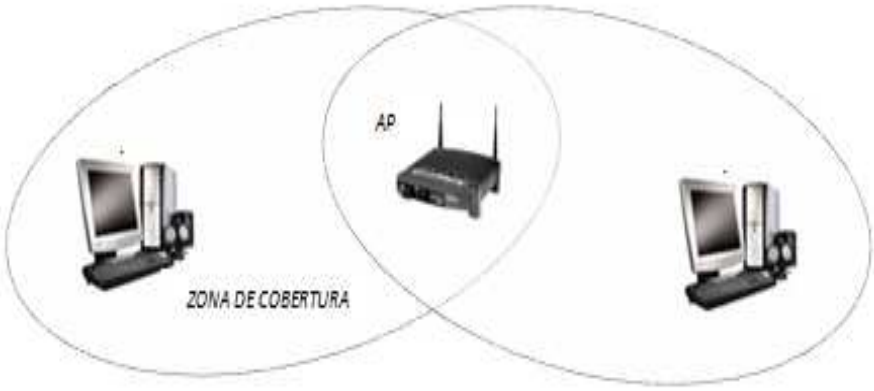


Figura 1.6 Topología BSS. Basic Service Set. [4]

- Grupo de Servicio Extendido, ESS (***Extended Service Set***). Cuando existen más de una BSS interconectadas entre ellas. El modelo ESS está formado por un conjunto de BSS asociadas mediante un sistema de distribución formando una subred única. Esto permite una serie de prestaciones opcionales como el roaming entre celdas. Teniendo en cuenta que la mayoría de las WLAN tendrán la necesidad de conectarse a las LAN cableadas, este será el modo de operación generalmente adoptado en las WLAN de empresas con más de un AP y en las WLAN públicas o hotspost. El sistema de distribución de una topología ESS puede ser cableado o inalámbrico, en la figura 1.7 se muestra la distribución.

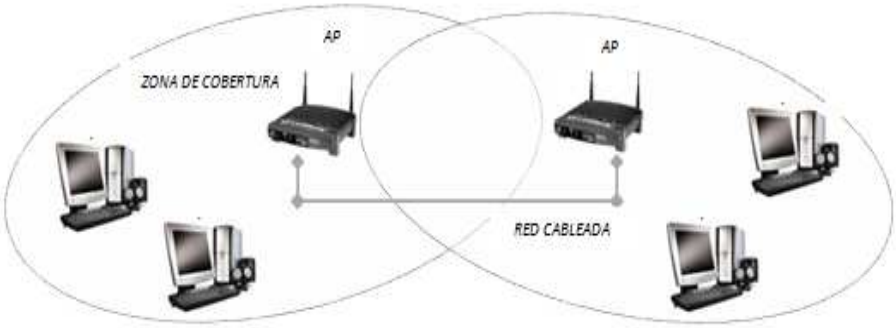


Figura 1.7 Topología ESS. Extended Service. [4]

- Grupo de Servicio Independiente, IBSS (***Independent Basic Service Set***). Cuando una BSS está formada únicamente por estaciones inalámbricas, operando en modo ad-hoc. El modelo IBSS es aquel en el cual no hay punto de acceso, las estaciones inalámbricas se comunican entre sí, como se muestra en la figura 1.8; las funciones de coordinación son asumidas de forma aleatoria por una de las estaciones inalámbricas presentes. El tráfico de información se lleva a cabo directamente entre los equipos implicados, sin tener que recurrir a una jerarquía superior centralizadora, obteniéndose un aprovechamiento máximo del canal de comunicaciones. Es un modo que puede ser muy útil cuando el tráfico existente se reparte entre todos los equipos cercanos físicamente.

Figura 1.8 Topología IBSS. Independent Basic Service Set [4]

1.3 Seguridad en redes de datos

La seguridad informática es una disciplina que se relaciona con diversas técnicas, aplicaciones y dispositivos, cuyo objetivo principal es asegurar la integridad, confidencialidad y disponibilidad de la información de un sistema informático y sus usuarios. Es difícil lograr que un sistema informático sea ciento por ciento seguro, pero al establecer medidas de seguridad se evitan daños y problemas que los intrusos pueden ocasionar.

El establecimiento de políticas de seguridad ayuda a que en una organización se reduzcan los ataques que un sistema informático pueda sufrir. Es necesario administrar cuidadosamente las políticas de seguridad para mantener el equilibrio entre el acceso y uso transparentes y la seguridad de la red; en la figura 1.9 se muestra un diagrama del equilibrio entre las necesidades de la organización y la seguridad informática [3].

Figura 1.9 Equilibrio entre las necesidades empresariales y la seguridad informática [3].

En la actualidad, la seguridad informática ha adquirido gran auge dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización, esta situación ha llevado a la aparición de nuevas amenazas en los sistemas

computarizados. Algunas amenazas a la seguridad de un sistema informático o computadora son las siguientes:

- Programas malignos. Virus, espías, troyanos, gusanos, phishing, spamming, entre otros.
- Siniestros. Robos, incendios, humedad, etc.
- Intrusos. Piratas informáticos que pueden acceder remota o físicamente a un sistema para provocar daños.
- Operadores. Los propios operadores de un sistema pueden debilitar y ser una amenaza a la seguridad de un sistema ya sea por boicot, o por falta de capacitación o de interés.

Ante tales amenazas, uno de los puntos a cubrir son las claves de acceso, no se deben usar claves que en su constitución son muy comunes y no se deben compartir. En cada nodo y servidor se deben usar antivirus, actualizar o configurar para que automáticamente se integren las nuevas actualizaciones del propio software y de las definiciones o bases de datos de virus registrados. También se deben utilizar programas que detecten y remuevan spywares (programas o aplicaciones que recopilan información sobre una persona u organización sin su conocimiento). Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

- Seguridad lógica. Es un conjunto de políticas y mecanismos que permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos en un sistema, según los requerimientos de la organización. Debido a la existencia de amenazas, se hace imprescindible la implantación de barreras de seguridad como: cortafuegos, antivirus, antiespías, encriptación de la información y uso de contraseñas, capacitación a los usuarios de los sistemas y capacitación a la población sobre las nuevas tecnologías.

- Seguridad física. Es el tipo de seguridad que se utiliza cuando las amenazas son físicas, tales como humedad, incendios u otro medio que ponga en riesgo la seguridad. Ejemplos de seguridad física para este tipo de amenazas son el mantenimiento eléctrico y sistemas anti-incendios.

1.3.1 Manejo de Riesgos

Para brindar seguridad a la información es imprescindible realizar una evaluación metódica de los riesgos existentes. Los riesgos pueden ser: acceso o copia de manera indebida a la información, las descargas de programas con virus, hackers, daños por fuego, agua, etc.; éstos riesgos pueden llegar a afectar datos, programas, equipos e incluso redes.

El primer paso es conocer los riesgos, una vez identificados los riegos se debe realizar una evaluación de los mismos, la cual debe identificar, cuantificar y priorizar riesgos contra los objetivos relevantes de la organización. La evaluación de los riesgos debe realizarse de manera periódica, y los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos.

La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio para la identificación y clasificación de riesgos, las opciones para el tratamiento de estos y la gestión general de riesgos aplicable a la organización [5].

1.3.2 Políticas de Seguridad Informática

Las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Las políticas de seguridad proporcionan las reglas que gobiernan el cómo deben ser configurados los sistemas y cómo deben de actuar los empleados de una organización en circunstancias normales y el cómo deben reaccionar si se presentan circunstancias inusuales.

El objetivo de las políticas de seguridad es dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos de la organización, las leyes y las regulaciones.

Toda política debe tener un propósito y procedimiento bien específico que articule claramente por qué fueron creadas tales políticas y qué beneficios espera la organización derivada de las mismas.

Las políticas de seguridad definen los requerimientos técnicos para la seguridad en un sistema informático y la red. Definen la manera en que un administrador de redes o sistema debe configurar un sistema respecto a la seguridad que requiere la empresa o el momento. Esta configuración también afecta a los usuarios y a alguno de los requerimiento establecidos en la política y debe de comunicarse a la comunidad de usuarios en general de una forma pronta, oportuna y explícita [5].

Una política de seguridad debe asegurar cuatro aspectos fundamentales en una solución de seguridad:

- Autenticación.
- Control de acceso.
- Integridad.
- Confidencialidad.

1.4 Control de acceso a la red

Un control de acceso a la red, NAC (***Network Access Control***)**,** se refiere a la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular. Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, recursos lógicos ó recursos digitales. El objetivo del control de acceso es realizar exactamente lo que su nombre implica, es decir, controlar el acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos y dispositivos a los que pueden acceder los usuarios y verificar lo que pueden hacer en la red.

Cada vez se utilizan soluciones de control de acceso para proteger los datos y sistemas de las empresas, asegurar el cumplimiento de las políticas legales y empresariales, y bloquear los equipos desconocidos o no autorizados. Al mismo tiempo, deben ser compatibles con las necesidades de acceso ininterrumpido a la red de los usuarios legítimos. Una solución NAC efectiva reduce el riesgo y los costos de la seguridad, identificando e impidiendo las amenazas y vulnerabilidades. Por medio de una evaluación constante de todos los equipos con respecto a las políticas definidas, el control de acceso a la red puede verificar, por ejemplo, que los parches de seguridad están instalados y que no

se utilizan aplicaciones no permitidas. Los objetivos generales que persigue un NAC son:

- Reducción del riesgo de ataques desconocidos. El punto clave de las soluciones del NAC es la habilidad de prevenir el acceso a la red de equipos terminales que no posean software antivirus, parches de seguridad, o software de prevención de intrusión al equipo, evitando así poner en riesgo los demás equipos de la red contra contaminación de gusanos, virus o código malicioso.
- Ejecución de políticas de seguridad. Las soluciones del NAC permiten a los administradores de red definir políticas, tales como cuáles tipos de computadoras, ó cuáles perfiles de usuarios deben tener acceso a determinadas áreas de la red, y forzar su ejecución a través de switches o routers.
- Manejo de identidad y acceso. Mientras las redes IP convencionales ejecutan sus políticas de seguridad y acceso en base a direcciones IP, un NAC lo hace basándose en identidades autenticadas, al menos para equipos terminales de usuarios, tales como laptops y desktops. [6]

Para llevar a cabo un adecuado control de acceso se debe realizar una autenticación, es decir, identificar a los usuarios válidos que puedan acceder a los sistemas informáticos. Además, se debe realizar una correcta asignación de privilegios a dichos usuarios. Y por último un registro de las operaciones ejecutadas en el sistema.

1.4.1 Tipos de Control de Acceso a la Red

Existen diferentes tipos de control de acceso a una red los cuales se explican a continuación:

- Basado en hardware. Tanto si es “in-line” o “out-of-band”, esta opción necesita habitualmente de un equipo (appliance) que tendrá que estar instalado en casi cualquier ubicación donde sea preciso contar con un NAC. Algunos de estos appliances han sustituido a los switches de acceso, mientras que otros operan entre la capa de acceso a red y los switches de red.
- Basado en agentes software. El siguiente paso es el basado en pequeños programas residentes en los ordenadores y dispositivos, instalándose estos agentes en cada uno de los sistemas que deban ser controlados por el NAC. Dichos agentes escanean y monitorizan el dispositivo, generalmente enviando los resultados a un servidor central. Los sistemas que no cumplen con los requisitos no tendrán autorización de acceso a la red, y a menudo se les envía algún tipo de medida correctora para que cumplan las directivas de seguridad.
- Sin agentes software. El NAC sin agentes es otra de las variantes, y consiste en partes software que se ejecutan puntualmente. Con esta configuración, la idea es que un agente temporal (generalmente algún tipo de control ActiveX) escanee el cliente periódicamente en búsqueda de vulnerabilidades o incumplimientos en la política de seguridad. Los resultados del escaneo son enviados al servidor central de políticas, y se ejecuta una acción si es necesario en caso de que el sistema no cumpla con los requerimientos. Cuando el proceso se completa, el agente se descarga.
- NAC dinámico. El NAC dinámico, que utiliza agentes sólo en un porcentaje determinado de equipos. También se conoce como NAS peer-to-peer, siendo una opción que no requiere cambios a nivel de red o software que deba ser instalado en cada equipo. Los agentes, que en ocasiones pueden llegar a ser obligatorios, son instalados en sistemas seguros.

1.4.2 Operación de un Control de Acceso a la Red

A continuación se explica brevemente la operación de un NAC:

- Detección e Identificación de nuevos dispositivos conectados a la red. Esto se lleva a cabo por la identificación de peticiones de autenticación, lo anterior se realiza a través de los switches.
- Autenticación de usuarios y dispositivos. La Autenticación hablando de sistemas informáticos es un procedimiento que consiste en comprobar la identidad de una entidad (persona ó equipo), con vistas a la autorización del acceso de dicha entidad a ciertos recursos (sistemas, redes ó aplicaciones). La autenticación se realiza utilizando el estándar 802.1x y un servidor RADIUS, mismos que se describen más adelante.
- Evaluación o revisión de sistemas finales en cuanto a su cumplimiento y/o vulnerabilidades. En esta parte se hace una revisión de las condiciones en las que se encuentra el equipo, que busca conectarse a la red en cuanto a su cumplimento con políticas previamente establecidas como son sistema operativo, programas y aplicaciones instalados, actualizaciones de antivirus así como nivel de parcheo. Esto se realiza con el objetivo de que si un equipo de usuario deja de cumplir con las políticas establecidas, éste será redireccionado a la zona de remediación.
- Autorización para usar la red basado en los resultados de la autenticación y evaluación. Como ya se mencionó esta fase depende de los resultados obtenidos previamente, entonces se determina el roll o función que desempeña la estación o equipo final de usuario, y de acuerdo con esto se autoriza el uso de recursos de red.
- Remediación para equipos con problemas de cumplimiento de políticas de seguridad. Aquí se resuelven problemas de cuarentena de sistema finales, y/o usuarios para evitar impacto negativamente en la red.

1.4.3 Elementos de un Control de Acceso a la Red

Los elementos que integran un control NAC se listan a continuación:

- Equipo cliente. En una red, los equipos clientes son empleados por los usuarios de una red tales como PC's, impresoras, servidores, entre otros.
- Autenticador. Entidad en un extremo de un segmento punto a punto de una LAN que facilita la autenticación de la entidad conectada al otro extremo del enlace.
- Nac Gateway. Es un dispositivo que se encuentra entre el servidor de autenticación y el equipo de usuario final. Este dispositivo permite controlar las acciones de autenticación y autorización mediante la manipulación de los atributos que entrega el servidor de autenticación, a fin de indicar al autenticador la acción a seguir.
- Servidor de autenticación. Entidad que facilita servicio de autenticación al autenticador.

1.5 Arquitectura AAA

El desarrollo tecnológico ha traído como consecuencia la vulnerabilidad a amenazas informáticas que pueden comprometer la operación de una organización, por ello se están adoptando mecanismos que permiten una gestión eficiente de todos los requerimientos de seguridad, asignando roles y privilegios para el acceso a todos los sistemas que consuman los servicios proporcionados, permitiendo una gestión eficiente a fin de mantener la disponibilidad y confidencialidad de la información.

Autenticación + Autorización + Arqueo, AAA (***Autentication + Authorization + Accounting***) es un estándar para el diseño basado en la autenticación, no es un sistema en sí, sino una colección y definición de normas para la creación de sistemas. La fusión de los tres permite crear un sistema de gestión completo de usuarios que controle todos los aspectos relativos a su identificación, gestión de recursos o servicios permitidos para su uso y estadísticas para el control de su utilización.

Para la creación de AAA se formó un grupo de trabajo en la IETF (***Internet Enginering Task Force***) dedicado al estudio y desarrollo de un estándar de autenticación. Las metas que se planteó el grupo de trabajo son:

- Búsqueda de claridad sobre las normas de funcionamiento de un modelo basado en la autenticación, que pueda ser interconectado con otros.
- Organizar los tipos de mensajes que necesita este tipo de sistema para desempeñar óptimamente su servicio, informando de todas las incidencias que se produzcan.
- Independencia del tipo de transporte, definiendo un método principal de transporte y dejando abiertas otras futuras posibilidades.
- Reforzamiento de la seguridad en todos los procesos procurando no sobrecargar el tráfico.
- Posibilidad de implementación en los equipos existentes y futuros.

La arquitectura AAA permite la existencia de servidores Proxy para descentralizar peticiones hacia otros servidores, con lo que una petición de autenticación o arqueo podrá ser transferida a otro servidor secundario por el servidor principal, este proceso es independiente para cada una de las tres “aes”, por lo que se pueden construir redes complejas que gestionen independientemente la autenticación hacia un servidor, la autorización hacia

otro u otros y el arqueo hacia otros. Todo esto proporciona las características de redundancia, descentralización y balanceo de carga.

En la arquitectura AAA, existen diferentes componentes:

- Solicitante. Equipo o usuario que solicita autenticación o entrada.
- El NAS. Es el equipo de red que hace de puerta de entrada física y tramita la autenticación. Este equipo suele ser quien inicia la secuencia de autenticación al detectar una conexión activa, por ello se denomina autenticador.
- Servidor de autenticación (para este proyecto se utilizará un servidor RADIUS). Es el que dirige todo el proceso AAA de los equipos y usuarios que soliciten acceso, puede hacer el papel de Proxy elevando las consultas a otros servidores.
- Servidor de directorio o servidor de base de datos de usuarios y credenciales. Al cual el servidor de autenticación va a solicitar los datos de autenticación de los solicitantes de acceso. Este puede ser la misma máquina que el servidor de autenticación, un servidor de Directorio Activo, AD (***Active Directory***), una base de datos SQL (MySQL, Microsoft SQL Server, Oracle, etc.), o un servidor UNIX con credenciales de usuario.
- Proveedor de servicios, SP (***Service Provider***). Es el propietario de la infraestructura de acceso a la que se conecta el usuario y por lo tanto es el propietario del servidor AAA y del equipo de servicio o NAS. Las tres “aes” proporcionan respuesta a las tres preguntas necesarias para acceder a un servicio que se presta a un solicitante [4]:

    - Autenticación ¿Quién es el solicitante?
    - Autorización ¿A qué servicios le voy a permitir acceder?
    - Arqueo ¿Qué hace el cliente con los servicios que presto?

1.5.1 Autenticación

La autenticación es el proceso de verificación de la identidad de un remitente que hace una petición para conectarse a un sistema. El remitente puede ser una persona que usa un ordenador u otro medio electrónico, un ordenador por sí mismo o programa. La autenticación es un modo de asegurar que los usuarios son realmente quienes dicen ser y que tienen la autorización para realizar funciones en el sistema. Debe dar una respuesta inequívoca a la pregunta ¿Quién o qué entidad pretende acceder a los servicios que presto?

Los primeros sistemas utilizaban una estructura simple de nombre de usuario y contraseña en texto plano, basando todo este sistema en estos dos datos, que podrían ser interceptados o robados por otra persona. Con el tiempo, este sistema fue mejorando mediante el acceso a través de desafío (Challenge), mediante dicho proceso no hay intercambio de contraseñas durante el transporte de la autenticación, sino mediante la encriptación de mensajes de una misma clave y un mismo algoritmo, evitando el transporte de la contraseña en sí.

Posteriormente se implantan otros métodos, como el acceso a través de equipos telefónicos con identificador (número de teléfono o número de serie), el generador de contraseñas portátil (token), tarjetas de acceso, sistemas biométricos, etc.; hasta llegar en la actualidad a un sistema más seguro basado en certificados llamado Infraestructura de Clave Pública, PKI (***Public Key Infraestructure***), que es una tecnología o conjunto de protocolos y estándares, que utilizan para su puesta en funcionamiento un conjunto de hardware y software, además de una serie de procedimientos de implementación de seguridad y normativas.

Durante este proceso no es el solicitante quien habla lenguaje AAA con el servidor de Autenticación, sino que el solicitante habla con el NAS o autenticador, y es éste quien traduce o encamina los paquetes hacia el servidor de autenticación. De esta manera no existe un camino abierto entre el solicitante y el servidor de autenticación, con lo que se garantiza bastante la seguridad del servidor de autenticación contra ataques directos, ya que un atacante tendría que estar en el interior de su infraestructura. AAA es versátil, ya que no provee de un único método de autenticación, sino que es considerado un protocolo extensible porque permite cualquier tipo de autenticación que se integre o adapte a su formato. En la fase de autenticación se produce un mensaje inicial de solicitud de acceso desde el equipo NAS al servidor de autenticación en forma de:

Solicitud de Acceso (Access - Request). El solicitante envía el nombre de usuario y la contraseña cifrada, si procede hacia en NAS. Este envía entonces al servidor de autenticación el mensaje de Access-Request solicitando además el puesto de acceso para el solicitante [4].

1.5.2 Autorización

La autorización es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que éste ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido. Este proceso contesta a la pregunta: ¿A qué servicios se va a permitir acceder al solicitante, una vez autenticado?

En este paso se produce la consulta del servidor de autenticación a la base de datos de usuarios, certificándose en la información del usuario que solicita acceso.

En los registros relacionados con este usuario, se podrá consultar todo tipo de derechos y deberes relacionados con él, de esta manera el servidor conocerá detalles como: si el solicitante está autorizado a acceder a la red en este momento, si le debe asignar la dirección IP concreta, si habrá de configurarle parámetros específicos para su conexión, si deberá concederle un ancho de banda determinado, si debe solicitar otro tipo de credenciales, o simplemente si deberá denegar su acceso. Todas estas reglas son definidas para cada usuario en concreto, para un grupo de usuarios o para todos los usuarios.

En esa fase el servidor de autenticación, tras conocer todos los atributos necesarios para el solicitante, responderá a su solicitud de autenticación mediante un mensaje estándar enviado al equipo NAS para permitir, denegar o volver a preguntar sobre su acceso:

- Aceptación de Acceso (Access-Accept). Cuyo fin de la solicitud de autenticación es la aceptación del acceso. Si el mecanismo de acceso ha sido correcto, se envía el mensaje al NAS con los atributos necesarios para regular el acceso del solicitante de forma personalizada.
- Denegación de Acceso (Access-Reject). Debido a usuario inexistente, contraseña incorrecta, derechos reservados, se le deniega de forma incondicional el acceso a este solicitante. Se puede incluir en este mensaje el motivo de la denegación del servicio. El NAS que recibe este mensaje no permite el acceso al solicitante, enviando un mensaje (si se incluye) al solicitante.
- Solicitud de información adicional para el acceso (Access-Challenge). Se le requiere al solicitante información adicional, como contraclave, tarjeta de acceso, PIN de acceso, o cualquier otro método alternativo o

adicional de acceso. El NAS transmite la petición al solicitante. Este mensaje puede ser intercambiado en múltiples ocasiones dependiendo del tipo de autenticación y de la información.

1.5.3 Accounting

Una vez realizado el proceso de autorización se produce la fase de arqueo, proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluida la cantidad de tiempo que permanece conectado, los servicios a los que accede, así como los datos transferidos durante la sesión.

Los datos registrados durante este proceso se utilizan con fines estadísticos. Estos datos correctamente manejados y gestionados nos permiten tomar decisiones en cuanto al uso de recursos por parte de los usuarios, con el fin de denegar conexiones, cambiar anchos de banda, impedir descargas, etc.

La fase de arqueo está limitada por la capacidad del equipo NAS de registrar información de sesiones. Mediante este proceso se podrá facturar a los usuarios los servicios prestados ya sea en forma de tiempo o de flujo de datos; por ejemplo al accesar a internet mediante conexiones móviles (UMTS, 3G, etc.), se suele tarifar el servicio por descarga de datos, si no se tiene contratada tarifa plana.

En el área de arqueo se acumula la información de sesiones para posteriormente tarifarlas, de esa manera el Accounting es el responsable de proporcionar los datos necesarios para enlazar con un sistema de tarificación adecuado.

Durante esta fase se producen los siguientes mensajes:

- Solicitud de inicio de arqueo (Accounting - Request [Start]). Solicitud de inicio enviada desde el equipo NAS al servidor, que indica que ha comenzado la fase de arqueo y se comenzarán a registrar los datos de la sesión de usuario.
- Respuesta de asentimiento al inicio de arqueo (Accounting - Response [Start]). Responde a la solicitud inicial. Registrando la información de inicio y enviando este paquete NAS para mostrar su conformidad.
- Solicitud final de arqueo (Accounting - Request [Start]. El NAS comprueba la desconexión del usuario y envía al servidor un mensaje final de la fase de arqueo.

1.6 Seguridad en redes inalámbricas

Anteriormente no existía una preocupación por la intercepción de datos, espionaje, etc., por lo cual las redes inalámbricas carecían de seguridad. A medida que las redes inalámbricas se comenzaron a distribuir y debido a su gran demanda, se empezó a hacer evidente su falta completa de seguridad. Un propósito esencial de la seguridad es proteger y mantener los recursos de red, garantizar que los usuarios no puedan dañar los datos, aplicaciones o entorno operativo de un sistema, lo que implica protegerse contra ataques malintencionados, así como controlar los efectos de los errores y fallos del equipo. Las redes inalámbricas pueden presentar vulnerabilidades a ataques especializados, a puntos débiles en la configuración y en las políticas de seguridad de las empresas u organizaciones. Por ejemplo:

- Débil autenticación, sólo del dispositivo. Los dispositivos cliente están autenticados, no así los usuarios, esto permite que los usuarios sin autorización accedan a los recursos de la red.

- Cifrado débil de los datos. Sin los datos cifrados, los intrusos pueden leer cuando son transmitidos por el enlace inalámbrico.
- No hay integridad del mensaje. Sin integridad, un intruso puede modificar el contenido de cualquier trama inalámbrica.

El acceso inalámbrico puede representar una gran amenaza para el acceso a la red, debido a que la mayoría de las redes inalámbricas tienen pocas o ninguna restricción.

1.6.1 Mecanismos de protección de redes inalámbricas

Son muchos los motivos para preocuparse por la seguridad de una red inalámbrica. Para resolver los problemas de seguridad que presenta una red inalámbrica se tendrá que poder, por un lado, garantizar el acceso mediante algún tipo de credencial a la red y por otro, garantizar la privacidad de las comunicaciones aunque se hagan a través de un medio inseguro. Debido a esto surgen estándares de seguridad, algunos de los cuales son los siguientes:

- Privacidad Equivalente a Cableado, WEP (***Wired Equivalent Privacy***). Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite, basado en el algoritmo de cifrado RC4. Hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. Se pueden utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida. En la autenticación de Sistema Abierto, este método se puede dividir en cuatro fases:

- La estación cliente envía una petición de autenticación al Punto de Acceso.
- El punto de acceso envía de vuelta un texto modelo.
- El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al Punto de Acceso en otra petición de autenticación.
- El Punto de Acceso descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el Punto de Acceso envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

- Acceso Wi-Fi protegido WPA**,** (***Wi-Fi Protected Access***). Consiste en un mecanismo de control de acceso a una red inalámbrica. También se le conoce con el nombre de TSN (***Transition Security Network***). WPA implementa la mayoría del estándar IEEE 802.11i y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. Adopta la autentificación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red y permite la autentificación mediante Clave Compartida, PSK (***Pre-Shared Key***), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red. Puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema, ó simplemente utilizar una contraseña compartida para identificarse.
- Acceso Protegido Wi-Fi 2, WPA2 (***Wi-Fi Protected Access 2***). Es un sistema para proteger las redes inalámbricas, creado para corregir las vulnerabilidades detectadas en WPA. Está basada en el nuevo estándar 802.11i, puede inferir que es la versión certificada del estándar 802.11.

CAPÍTULO II. RADIUS

2.1 Introducción a RADIUS

El Servidor de Autenticación Remota para sistemas de Marcado Telefónico a Redes, RADIUS (***Remote Authentication Dial-Up Server***), es ampliamente empleado para controlar el acceso a servicios de red. El nombre de RADIUS proviene desde sus comienzos, donde su único uso era el acceso a redes a través de módem, actualmente su funcionalidad es mucho más amplia, ya que a pesar de algunas de sus limitaciones ha ido adoptando una serie de mejoras que le han permitido gestionar desde pequeñas redes seguras hasta redes de alto nivel, por tal motivo RADIUS es el protocolo AAA principal en la actualidad [3].

2.1.1 Orígenes

Siempre que se habla de sistemas basados en la autenticación se habla de RADIUS como mejor alternativa. RADIUS es un protocolo que existe antes que AAA, tan es así, que prestó sus códigos y conocimientos al grupo de trabajo que comenzó a diseñar las bases de AAA, por lo que cumple con todas las normas de este estándar. RADIUS es creado debido a que en los años 90, las redes crecieron considerablemente haciendo más difícil el control de acceso a éstas. Cada fabricante de sistemas de acceso remoto telefónico (***dial-up***) utilizaba sus sistemas propietarios de control de acceso,

lo que llevó a una empresa llamada Merit a buscar una solución para desarrollar un mecanismo de autenticación común. Merit lanzó en 1991 una RFI (***Request For Information***) a las principales empresas de networking. Una de las empresas que respondió a esa solicitud fue Livingston Enterprises, dando una clara descripción de lo que posteriormente pasó a llamarse RADIUS. Después de varias mejoras se publicó el estándar RADIUS, el cual ha seguido trabajando en la introducción de nuevos tipos de autenticación, autorización y arqueo para continuar mejorando su seguridad, transporte e información [3].

2.1.2 Descripción del protocolo

RADIUS es un protocolo que se ejecuta en una de las múltiples plataformas que permite (Unix, GNU/Linux, Windows y Solaris, entre otras) y que permanece de forma pasiva a la escucha de solicitudes de autenticación. Para lograrlo utiliza el Protocolo de Datagrama de Usuario, UDP (***User Datagram Protocol***) y permanece a la escucha en los puertos 1812 para la autenticación y 1813 para el arqueo. El motivo por el cual RADIUS utiliza UDP y no el Protocolo de Control de Transporte, TCP (***Transport Control Protocol***), es porque UDP no se hace cargo del control de llegada de los paquetes que envía a su destino (característica de UDP al ser "stateless" o "connectionless"), con lo que las retransmisiones se pueden hacer más rápidamente, ya que el puerto no queda ocupado por el control de la conexión, lo que sí ocurre con TCP. UDP guarda una copia del paquete de solicitud sobre la capa de transporte con el propósito de poder recuperarlo para reenviarlo, si fuera necesario. RADIUS es el servidor de autenticación, que junto con el solicitante y el autenticador, son los componentes principales del estándar AAA. RADIUS está basado en un modelo cliente-servidor, ya que escucha y espera en forma pasiva las solicitudes de sus clientes o Servidores NAS. En este modelo el NAS es el

responsable del envío y de la correcta recepción de las solicitudes de acceso, y es el servidor RADIUS el responsable de verificar las credenciales del usuario y de ser correctas, de enviar al NAS los parámetros de conexión necesarios para prestar el servicio a los solicitantes. En la figura 2.1 se puede observar el modelo típico de implantación de un servidor RADIUS, en dicha figura se tiene una zona segura donde se encuentran el servidor RADIUS y el servidor de directorio y base de datos (***BD***), esta zona está protegida para los usuarios externos, los cuales primeramente deben autenticarse mediante el NAS para poder llegar a ella. El solicitante deberá realizar una petición al NAS o al Conmutador Ethernet, mismos que gestionarán su solicitud al servidor RADIUS. Este a su vez, consultará el servidor de directorio o BD de credenciales y permitirá o no el acceso al solicitante [3].

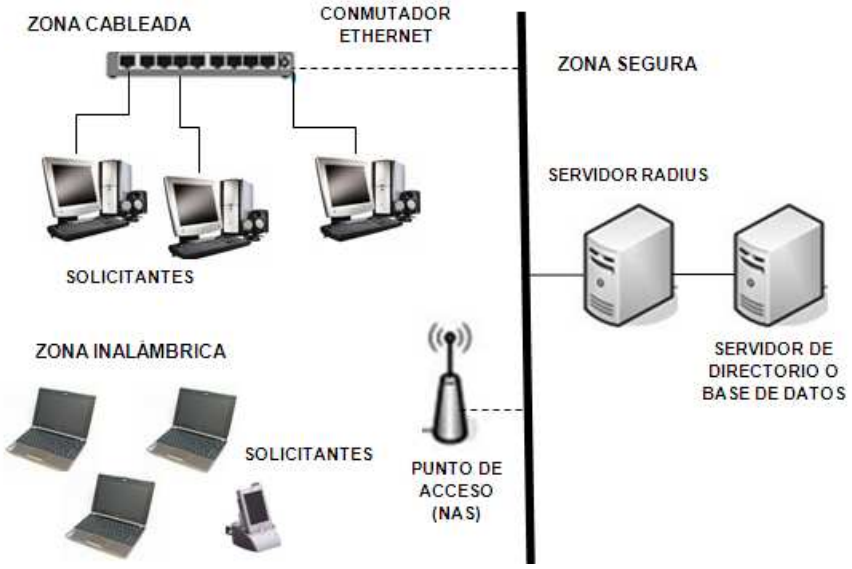


Figura 2.1 Infraestructura simple RADIUS

2.1.3 Multiplataforma

Los primeros servidores basados en RADIUS fueron hechos para Unix y funcionan perfectamente en GNU/Linux. Muchos de estos sistemas han ido migrando hacia Windows. En GNU/Linux podemos encontrar soluciones RADIUS de tipo OpenSource como FreeRADIUS. En el presente trabajo se opta por el uso de FreeRADIUS 2.1 debido a sus características de calidad y funcionalidad, además de que no se paga el valor al fabricante, lo cual sí ocurre con el software comercial. Adicionalmente, se ha elegido trabajar con Ubuntu 9.04, una distribución de GNU/Linux, por ser una plataforma potente, por su sencillez de configuración, por su gran difusión actual, por su ligereza y por los recursos que utiliza; a diferencia de trabajar sobre una plataforma Windows, la cual utiliza muchos más recursos [3].

2.2 Métodos de autenticación

Los métodos de autenticación son módulos de software sobre los que se basa RADIUS para llevar a cabo el proceso de autenticación de usuario. Estos módulos son complejas cajas matemáticas encargadas de realizar el cifrado, descifrado y empaquetado de todos los procesos de autenticación. Cuando RADIUS recibe una solicitud de acceso, va pasándola por cada uno de los módulos de autenticación que tenga activados en su configuración, hasta que alguno de esos módulos reconozca las credenciales del usuario y se encargue de validar la autenticación. Desde el método nativo de RADIUS que es el Protocolo de Autenticación mediante Contraseña, PAP (***Password Authentication Protocol***), hasta los más actuales como algunos tipos nuevos del Protocolo de Extensión de Autenticación, EAP (***Extensible Authentication Protocol***), la evolución en cuanto a seguridad ha sido notable.

PAP y el Protocolo de Autenticación por Desafío Mutuo, CHAP (***Challenge Handshake Authentication Protocol***) son los métodos nativos de autenticación incluidos en los primeros servidores RADIUS, y por lo mismo los más vulnerables. Todas las versiones de RADIUS tienen soporte nativo para estos métodos.

Cuando los métodos de autenticación de RADIUS PAP y CHAP**,** estaban en duda de seguridad, surge el nuevo método EAP que llega a extender la autenticación. EAP es un protocolo que se encarga de transportar, encapsular y ofrecer seguridad en la autenticación, y dentro de él se encuentran los métodos de autenticación a utilizar.

Los métodos de autenticación EAP pueden ser de los siguientes tipos:

- Métodos basados en claves compartidas. Estos métodos tienen el problema en su forma de distribución, transporte o almacenamiento de las credenciales, debido a que se da por hecho que cada usuario debe tener bien guardada su clave en un lugar seguro.
- Métodos basados en certificados. Estos métodos son los más seguros pero también los más difíciles de implantar. Aquí tenemos a los Certificados PKI, los cuales son la clave central en la infraestructura PKI, ya que con ellos se enlaza la clave pública, que es la clave que un solicitante comparte con otras entidades a fin de que puedan leer su información con los datos que permiten identificarlo. Ejemplos de estos métodos son EAP-TLS, EAP-TTLS y EAP-PEAP.
- Métodos no tunelados. En este tipo de métodos el tráfico EAP completo no es cifrado por el solicitante, autenticador y servidor de autenticación, solamente la información de contraseñas de usuario y otra información importante se cifra en el interior de los paquetes que circulan por la red. Esto hace posible que los paquetes que se generan en el proceso de

autenticación se puedan interceptar para obtener las credenciales de los usuarios.

- Métodos tunelados. Estos métodos utilizan un sistema criptográfico para encapsular el tráfico completo en el proceso de autenticación, autorización y arqueo, incrementando así la seguridad contra la interceptación de tráfico.

En la tabla 2.1 se muestra una comparación de las características principales de los métodos más comunes de EAP [3].

	EAP-MD5	**EAP-TLS**	**EAP-TTLS**	**EAP-PEAP**
Basado en claves compartidas	Si	No	No	No
Certificado de servidor	No	Si	Si	Si
Certificado de cliente	No (Usuario y contraseña mediante Challenge	Obligatorio	Opcional (credenciales de usuario)	Opcional (credenciales de usuario)
Validación de certificados	No	Si	Si	Si
Autenticación mutua	No (sólo cliente)	Si	Si	Si
Tunelamiento	No	Si, TLS	Si, TLS	Si, TLS
Desarrollador	Estándar	Microsoft	Funk y Certicom	Microsoft, Cisco y RSA
Solicitantes que lo soportan	Microsoft WPA MacOs	Microsoft MacOs Linux	WPA MacOS	Microsoft MacOS Linux
Vulnerable Main in the Middle	Si	No	No	No
Vulnerable actualmente	Si	No	No	No
Usos recomendados	Redes cableadas	Alámbrica e Inalámbrica, Smartcards	Alámbrica e Inalámbrica	Alámbrica e Inalámbrica

Tabla 2.1 Comparación de los principales métodos EAP

2.2.1 Autenticación simple y autenticación mutua

La autenticación simple se basa en que el sistema solicitante (usuario) pide la autenticación al servidor de autenticación, presuponiendo que éste sea el servidor lícito al que se quiere conectar, por lo que le entrega sus credenciales para ser autenticado. En la autenticación mutua, basada en la desconfianza mutua, el solicitante verifica primero la identidad del servidor al que enviará sus credenciales.

En los casos de autenticación mutua mediante certificados, como en los protocolos EAP tunelados mediante TLS, antes de que se produzca el intercambio de credenciales tunelado entre solicitante y servidor, ambos pasan por un proceso de verificación de identidades, normalmente mediante el uso de un certificado de cliente y otro de servidor. Los protocolos EAP-TLS, EAP-TTLS y EAP-PEAP, se basan en la autenticación mutua, ya sea utilizando certificados de cliente y de servidor o por combinación de certificados de servidor y credenciales de usuario [3].

2.2.2 Tipos de Autenticación

La manera de almacenar los nombres de usuarios y contraseñas de los solicitantes, puede realizarse de diferentes maneras:

- Autenticación contra archivo de usuarios. Esta es la forma más básica utilizada por los servidores de autenticación. Utiliza un fichero de texto en el cual se almacenan las credenciales de los usuarios y los parámetros asociados a estos. Se recomienda sólo para redes con un número reducido de usuarios.

- Autenticación contra el sistema operativo. Aquí basta dar los privilegios suficientes para que un módulo del servidor de autenticación pueda leer los usuarios y sus contraseñas almacenadas en las formas nativas que utilizan los sistemas operativos. Por ejemplo, en el caso de Linux sería el fichero *passwd o shadow*. Al crear un usuario y sus credenciales, éste queda automáticamente disponible para ser usado en el proceso de autenticación.
- Autenticación contra bases de datos. En este tipo de autenticación contra una base de datos, generalmente del tipo SQL, como Oracle, Microsoft SQL Server, MySQL y PostGreSQL, los datos de credenciales de usuarios, sus atributos de autorización y la información de arqueo de cuentas se almacenan en bases de datos pudiéndolo hacer de manera cifrada utilizando funciones como MD5 o SHA1, por ejemplo. La administración de los datos se realiza de manera muy sencilla, pudiendo hacer consultas, edición y eliminación de la información. Adicionalmente se pueden realizar copias de seguridad. Para la administración de un gran número de usuarios la base de datos es la mejor solución, pudiéndose crear scripts automáticos en lenguaje SQL para ejecutar durante los procesos de Autenticación, Autorización y Arqueo.
- Autenticación contra servicios de Directorio. Este tipo de autenticación es apropiado para empresas medianas a grandes que quieran autenticar a sus empleados contra sus sistemas internos de gestión de usuarios. Los servicios de directorio son Active Directory mediante Kerberos, LDAP y eDirectory, entre otros. RADIUS realiza las consultas de autenticación y autorización contra las bases de datos almacenadas en los servidores de directorio, en los cuales se gestionan de forma común las políticas de acceso y trabajo en la red corporativa [3].

2.2.3 Reautenticación

La reautenticación del solicitante se lleva a cabo si se pierde la conexión y necesita volver a autenticarse en el servidor RADIUS. También se puede forzar esta reautenticación en intervalos de tiempo para incrementar la seguridad; sin embargo, se debe tener cuidado para programar este tiempo a fin de evitar saturar al servidor [3].

2.3 Estructura de las comunicaciones RADIUS

A continuación se describe la estructura de un paquete RADIUS estándar y la secuencia de un proceso completo de autenticación.

2.3.1 Estructura de un mensaje RADIUS

Todos los paquetes RADIUS tienen la misma estructura básica, la cual consiste de los campos: código, identificador, tamaño, autenticador y atributos. En la figura 2.2 se observa esta estructura, así como el tamaño de cada campo [2].

Octetos:	1	1	2	16	Variable
	Código	**Identificador**	**Tamaño**	**Autenticador**	**Atributos**

Figura 2.2 Estructura de un paquete RADIUS

Este paquete RADIUS viene encapsulado dentro de un paquete UDP estándar. A continuación se describe cada campo:

- *Código.* Este campo tiene un octeto de longitud e identifica el tipo de paquete RADIUS. La tabla 2.2 identifica algunos valores de código y su correspondiente tipo de paquete. Por ejemplo: si el valor del código es "1", el paquete es una solicitud de acceso (RADIUS Access-Request).

Código	Tipo de paquete
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
6	Accounting-Status
7	Password-Request
9	Password-Reject
11	Access-Challenge

Tabla 2.2 Valores del campo código

- *Identificador.* Su tamaño es de un octeto. Es un campo utilizado para relacionar los paquetes que conforman una conversación, por ejemplo: solicitud y respuesta. Este campo hace posible relacionar paquetes del tipo Access-Challenge (solicitud de información adicional para el acceso) con paquetes tipo Access-Request (solicitud de acceso). Por ejemplo, el campo identificador en un paquete Access-Request enviado por el autenticador, puede contener el valor "00001101". El servidor de autenticación responderá con un paquete Access-Challenge cuyo campo identificador tendrá el mismo valor "00001101".
- *Tamaño.* El tamaño de este campo es de dos octetos e identifica el número de octetos que forman un paquete RADIUS.

- *Autenticador.* El campo autenticador es de 16 octetos. Es generado pseudoaleatoriamente, utilizado para validar la legitimidad del servidor RADIUS con el que se está conversando. Es también un sistema de comprobación de la integridad del paquete.
- *Atributos.* Los atributos contenidos en el paquete RADIUS son datos comunicados entre el NAS y el servidor RADIUS. Estos datos sirven para el funcionamiento de todo el proceso AAA. Existen atributos de todo tipo, como los atributos User-Name y User-Password, que se utilizan en las solicitudes de autenticación y que definen al usuario y a su contraseña. Todos los procesos que realiza RADIUS se realizan mediante atributos, existiendo atributos para la fase de Autenticación, para la de Autorización y para la de Arqueo. Algunos de estos atributos se muestran en la tabla 2.3, y se incluye el campo código, el cual debe ir en el paquete RADIUS.

Código	Atributo
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
46	Acct-Sesion-Time
64	Password-Reject

Tabla 2.3 Atributos RADIUS

2.3.2 Secuencia de autenticación de RADIUS

La comunicación entre el solicitante, el NAS y el Servidor de autenticación tiene la siguiente secuencia, aunque no se sigue siempre de la misma forma debido a factores que pueden variar, por ejemplo, el método de autenticación o los reintentos.

1. La secuencia comienza por un Access-Request, esta solicitud de acceso es un mensaje que contiene atributos como el nombre de usuario, la contraseña, el número de puerto NAS y el ID de cliente. El NAS envía esta solicitud al servidor RADIUS que tenga preestablecido en su lista de servidores, si es que tuviera más de uno. Si no recibiera respuesta en un tiempo determinado, reintentará el envío cierto número de veces.
2. El servidor RADIUS que recibe la solicitud comprueba si proviene de un equipo NAS autorizado, si no es así, la descarta de forma silenciosa. Si el cliente NAS está en su lista y el shared secret es el correcto comprueba en su base de datos el nombre de usuario y la contraseña. El shared secret o secreto compartido de RADIUS es una contraseña con formato alfanumérico de hasta 128 bytes que se define en los dos extremos de un canal RADIUS, esos extremos son el servidor RADIUS y su cliente, el cliente puede ser un equipo NAS, un servidor Web o un Proxy RADIUS. Este secreto se utiliza para encapsular las comunicaciones entre el cliente y el servidor RADIUS.
3. Si el tipo de autenticación está basada en el desafío, se envía al solicitante un mensaje de Access-Challenge con una frase aleatoria que debe calcular. Después de esto, el solicitante enviará este cálculo y el NAS a su vez, enviará nuevamente un Access-Request con los datos calculados.
4. Una vez comprobados todos estos datos de autorización y la base de datos de credenciales, se decidirá si se acepta o deniega la solicitud. Así, se enviará ya sea un mensaje de Access-Accept o uno de Access-Reject al NAS con los atributos necesarios para activar o denegar el servicio.
5. Si el mensaje anterior es un Access-Accept, el NAS abrirá el puerto con los atributos designados y enviará un mensaje de Accounting-Request

[Start] al servidor RADIUS, indicándole que ha comenzado el arqueo de la sesión del usuario. El servidor RADIUS confirmará la recepción del inicio de sesión enviando al NAS un mensaje Accounting-Response [Start] y guardará los datos de inicio de sesión de usuario que le envío el NAS con el Accounting-Request [Start].

6. Al terminarse la sesión del usuario, por él mismo o por otra razón el NAS envía al servidor un mensaje Accounting-Request [Stop], indicándole el fin de la sesión del usuario, así como los datos de consumo del usuario.
7. Finalmente el servidor confirma la recepción de esos datos mediante un mensaje Accounting-Response [Stop], enviándolo al NAS, terminando así el proceso de autenticación. En la siguiente figura se muestra la secuencia RADIUS.

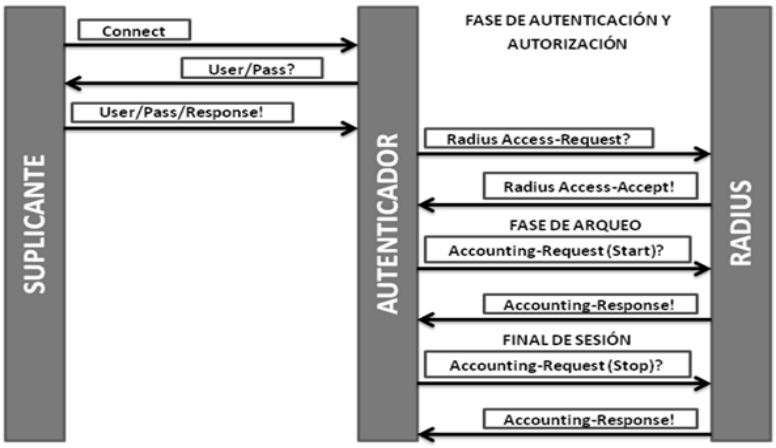


Figura 2.3 Secuencia AAA de RADIUS [4]

CAPÍTULO III. DISEÑO DE UN CONTROL DE ACCESO UTILIZANDO RADIUS

El presente capítulo contiene el diseño de un control de acceso implementado en una red LAN inalámbrica.

3.1 Antecedentes y Problemática

Las WLAN son un punto de riesgo que debe ser protegido y administrado dentro de la infraestructura de cualquier organización, sin embargo, no siempre se protege como es debido.

Se presenta en este proyecto el caso de una organización, la cual, a pesar de su gran nombre en el mercado de los cosméticos, no cuenta con la seguridad requerida en su red inalámbrica, lo que sin duda representa un área de oportunidad en la seguridad informática, ya que cualquier usuario puede tener acceso a la red.

La información que genera esta organización es de vital importancia, ya que ayuda a la toma de decisiones, implantación de políticas de administración, informes económicos, informes de competencias, entre otros; y sin la debida protección es susceptible a cualquier variación, modificación o pérdida.

3.2 Propuesta de Solución

En base a la problemática detectada en esta organización, se propone como solución la implantación de un Sistema de Seguridad para el control de acceso de equipos a la red; sin la necesidad de invertir en nueva tecnología, se mostrará el gran beneficio que ofrece. Se realizan pruebas sobre la red inalámbrica actual, implementando un control de acceso a través del servidor RADIUS, con el fin de solucionar la deficiente seguridad en la red.

El control de acceso que se utilizará para ingresar a la red se realizará con una solución de código abierto denominada FreeRADIUS y se configurará para un uso concreto: regular el acceso a la red inalámbrica de la organización. El servidor FreeRADIUS se instalará sobre una plataforma LINUX, en específico UBUNTU, y se configurará para que brinde servicio de autentificación a un punto de acceso.

3.3 Desarrollo

Basándose en los tipos de relaciones que se puedan establecer entre los componentes de una relación de confianza en AAA, se pueden distinguir diferentes tipos de relaciones de autorización o secuencias de autorización, como:

- Secuencia de agente o Agent Sequence: en esta secuencia de autorización el usuario solicita un servicio a AAA, que decide si prestar el servicio y notifica al equipo el tipo de servicio que se preste. El equipo de servicio notifica al servidor AAA si se produce la prestación del servicio.

- Secuencia de empuje o Push Sequence: en este caso, el usuario realiza una solicitud de servicio al servidor AAA en forma de ticket de servicio o certificado, este ticket regula el servicio que se prestará, el usuario sólo debe presentar el ticket al equipo NAS, que conocerá por sus características y prestará el servicio al usuario, no se produce una comunicación directa entre el equipo prestador del servicio o NAS y el servidor autenticador.
- Secuencia de tiro de itinerancia o Roaming Pull Sequence: este tipo de secuencia es similar a la secuencia de tiro, pero contempla dos proveedores de servicio, puede ser la infraestructura de acceso a Internet por Banda Ancha (conocido como Service Provider). El usuario puede contratar su acceso a través de otros proveedores (conocido como User Home Provider) o a través del propio propietario, si lo hace a través de otro proveedor, la solicitud a los proveedores AAA del proveedor del usuario, que autorizan a los equipos de prestación o NAS a prestar finalmente el servicio contratado por el usuario. El propietario tendrá algún tipo de facturación por servicio con el proveedor.
- Para la implementación del control de acceso basado en RADIUS, se toma como base la Secuencia de tiro o Pull Sequence: que es la secuencia clásica de protocolos de marcación o de servicios de Autenticación como RADIUS. Se necesitan de tres elementos que son solicitante, NAS y servidor de autenticación, en el cual el solicitante pide el acceso al equipo NAS y éste en comunicación con el servidor de autenticación tramita la solicitud, si el servidor la considera correcta, éste se lo comunica al NAS y éste acepta el acceso a la red, en caso contrario deniega el servicio. En la figura 3.1 se ilustra lo anterior.

Figura 3.1 Elementos del Control de Acceso

Para la implementación de este control de acceso se utilizaron las herramientas de hardware y software que se muestran en la Tabla 3.1.

Hardware / Software	
Switch Linksys SD208	
Access Point Wireless A+G Model No. WAPSSAG	
Lap Top (3 equipos) Sistema Operativo Windows Vista (Máquina Virtual.- Sistema Operativo Linux) Procesador Pentium Dual Core 2.0 GHz RAM 3.0 Gb	
VMWare Workstation Versión 6	vmware
Ubuntu Versión 9.04 Desktop	ubuntu linux for human beings
RADIUS Freeradius 2.1	freeRADIUS

Tabla 3.1 Infraestructura para la implementación del control de acceso.

Para la instalación del servidor RADIUS se instaló una máquina virtual configurada con Sistema Operativo Linux en su versión Ubuntu 9.04; la instalación de la maquina virtual se explica en el Anexo 1.

3.3.1 Instalación de FreeRADIUS.

FreeRADIUS como servidor de autenticación ofrece un rendimiento y potencia muy elevada, es compatible con casi cualquier plataforma o sistema operativo (Windows, Linux, MacOS, etc.) y da soporte para gran cantidad de módulos de autenticación.

Para la implementación del servidor, se instaló la versión de FreeRADIUS 2.1 desde los archivos binarios que se deben descargar previamente o se tiene que contar con la versión en DVD. Para lo cual se necesitó la compilación del paquete make, el cual se instala de la siguiente manera:

```
root@radius1:~# apt-get install make
root@radius1:~# mount /cdrom
root@radius1:~# dpkg –i /cdrom/utils/freeradius_2.1.4-0_i386.deb
```

Para solucionar el error por falta de dependencias, se recurre a apt-get en modo forzado:

```
root@radius1:~# apt-get –f install
```

3.3.2 Configuración de los archivos de FreeRADIUS

Para la configuración de nuestro servidor RADIUS, FreeRADIUS cuenta con diversos archivos que deben modificarse para lograr que el control de acceso funcione como se requiere.

Para el desarrollo de este proyecto los archivos serán modificados mediante el editor de textos Nano y los archivos a modificar son: *radiusd.conf, users, clients.conf, eap.*conf, éstos se localizan en la ruta /etc/freeradius y las modificaciones realizadas en estos archivos se presentan a continuación:

Archivo **radiusd.conf**. Es el principal archivo de configuración de RADIUS y en él se encuentran la mayor parte de configuraciones y directivas importantes para hacer funcionar correctamente el servidor RADIUS; para la configuración de este proyecto, en este archivo se modifica la opción with_ntdomain_hack declarándola como "yes". La figura 3.2 muestra el archivo radiusd.conf visto desde el editor Nano.

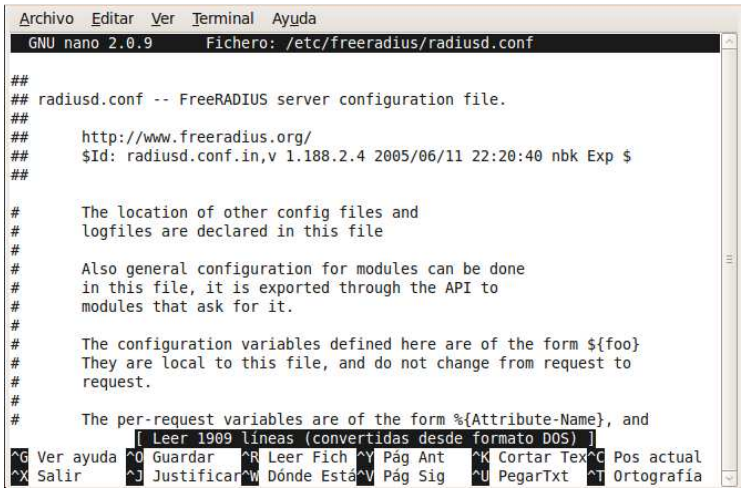


Figura 3.2 Archivo radiusd.conf

Archivo de definición de usuarios: **users**. En este archivo se pueden crear a los usuarios que se deseen, con sus atributos relacionados. Para el desarrollo de este proyecto este archivo contiene a el (los) usuario (s) que se autenticarán en el acceso a la red. La figura 3.3 muestra el archivo users desde el editor Nano.

En el archivo se declaró un usuario y contraseña de la siguiente forma:

"radius1" User-Password == "pruebarad1"

Donde radius1 es el usuario a autenticar y pruebarad1 corresponde a la contraseña.

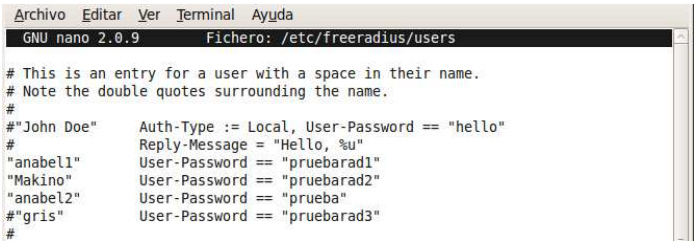


Figura 3.3 Archivo users

Archivo de NAS **clients.conf:** Otro archivo que se debe modificar para este proyecto es el archivo clients.conf. En él se configuran todos los clientes o NAS que se desee que interactúen con el servidor RADIUS. El presente trabajo sólo utiliza la parte de autenticación para poder distinguir a los usuarios del sistema. En este archivo se configura el punto de acceso, para esto se escribe la IP del Access Point y el secreto. La figura 3.4 muestra la edición del archivo clients.conf. En este caso la IP del Access Point es 192.168.3.65 y configuración es la siguiente:

```
client 192.168.3.65 {
secret = secretomi
shortname = sradius
}
```

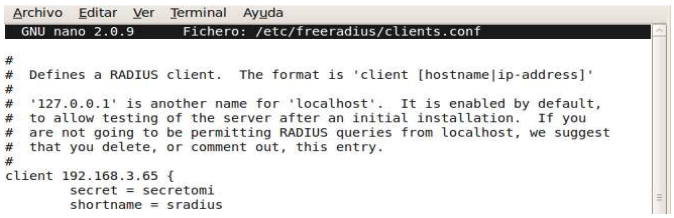


Figura 3.4 Archivo clients.conf

Archivo de Configuración de EAP: **eap.conf**. Este archivo se utiliza para configurar los procesos de autenticación basados en los métodos EAP. Para el desarrollo de este proyecto, el archivo se modifica de la siguiente manera para que pueda autenticar introduciendo un usuario y un password:

```
tls {
private_key_password = whatever
private_key_file = ${raddbdir}/certs/cert-srv.pem
# If Private key & Certificate are located in
# the same file, then private_key_file &
# certificate_file must contain the same file
# name.
certificate_file = ${raddbdir}/certs/cert-srv.pem

# Trusted Root CA list
CA_file = ${raddbdir}/certs/demoCA/cacert.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
# This can never exceed the size of a RADIUS
# packet (4096 bytes), and is preferably half
# that, to accomodate other attributes in
# RADIUS packet. On most APs the MAX packet
# length is configured between 1500 - 1600
# In these cases, fragment size should be
# 1024 or less.
#
fragment_size = 1024
# include_length is a flag which is
# by default set to yes If set to
# yes, Total Length of the message is
# included in EVERY packet we send.
# If set to no, Total Length of the
# message is included ONLY in the
# First packet of a fragment series.
include_length = yes
# Check the Certificate Revocation List
# 1) Copy CA certificates and CRLs to same directory.
# 2) Execute 'c_rehash <CA certs&CRLs Directory>'.
# 'c_rehash' is OpenSSL's command.
# 3) Add 'CA_path=<CA certs&CRLs directory>'
```

```
# to radiusd.conf's tls section.
# 4) uncomment the line below.
# 5) Restart radiusd
# check_crl = yes
# If check_cert_cn is set, the value will
# be xlat'ed and checked against the CN
# in the client certificate. If the values
# do not match, the certificate verification
# will fail rejecting the user.
# check_cert_cn = %{User-Name}}
peap {
# The tunneled EAP session needs a default
# EAP type which is separate from the one for
# the non-tunneled EAP module. Inside of the
# PEAP tunnel, we recommend using MS-CHAPv2,
# as that is the default type supported by
# Windows clients.
default_eap_type = mschapv2}
```

En este punto ya se cuenta con los archivos del FreeRADIUS configurados.

3.3.3 Arranque de FreeRADIUS

Una vez que se cuenta con los archivos del FreeRADIUS se puede arrancar el daemon (servicio), para lo que se dispone de un script que utiliza tres modificadores de forma independiente: start, stop y restart. Para llamar a este script se debe ejecutar la ruta /etc/init.d/. En la figura 3.5 se muestra el script para arrancar el FreeRADIUS y el cual se presenta a continuación:

```
root@radius1:~# etc/init.d/freeradius start
root@radius1:~# etc/init.d/freeradius stop
root@radius1:~# etc/init.d/freeradius restart
```

Para arrancar FreeRADIUS se debe hacer en modo programa y no en modo daemon, además de solicitar que arranque en modo debug (depuración), para observar todas las fases del arranque para cada uno de los módulos de autenticación, autorización y arqueo. Para esto se descarga el daemon de la memoria mediante el script situado en /etc/init.d/ con el modificador stop, antes de poder ejecutarlo en modo programa. Se utiliza el siguiente comando para arrancar freeradius en modo debug trace:

```
root@radius1:~# etc/init.d/freeradius stop
root@radius1:~# freeradius -X
```

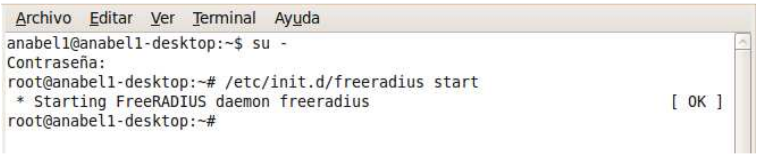


Figura 3.5 Script para arrancar FreeRADIUS

Con esto se termina la configuración de los archivos para el servidor FreeRADIUS y se realizan pruebas para verificar que el servidor funcione correctamente.

3.3.4 Configuración de AP

El Punto de Acceso cuenta con opciones de configuración para autorizar el acceso mediante un servidor RADIUS. Para ello se ingresa a su configuración y desde el menú Wireless/Wireless Security se selecciona el modo de seguridad RADIUS y se modifica la IP del servidor, en este caso la IP 192.168.3.100; se debe seleccionar el puerto por el cual se accede al shared secret de la red, en este caso se define el puerto 1812.

El shared secret es la clave utilizada para que RADIUS y el AP se reconozcan ente sí, ésta se asigna a la IP del AP en el archivo “clients.conf”, el cual quedó configurado con la IP 192.168.3.65. La configuración en las opciones del AP se muestra en la figura 3.6.

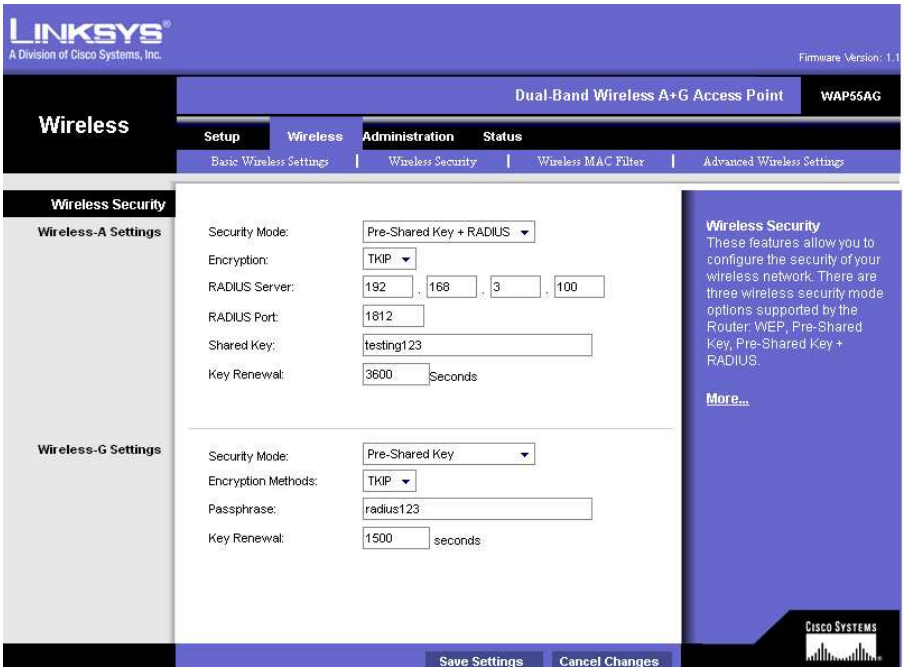


Figura 3.6 Configuración del Access Point

3.3.5 Configuración de cliente Windows para autentificar en FreeRADIUS

Al activar el interruptor de la red inalámbrica desde un solicitante con Windows y detectar la red de la organización, en este caso radius2, si se desea accesar a ésta, se deberán configurar las propiedades de la red inalámbrica para autenticarse en el servidor RADIUS; ésto se realiza desde la opción de Propiedades/Seguridad/, seleccionando en tipo de seguridad WPA-Enterprise y tipo de cifrado TKIP, como se muestra en la figura 3.7.

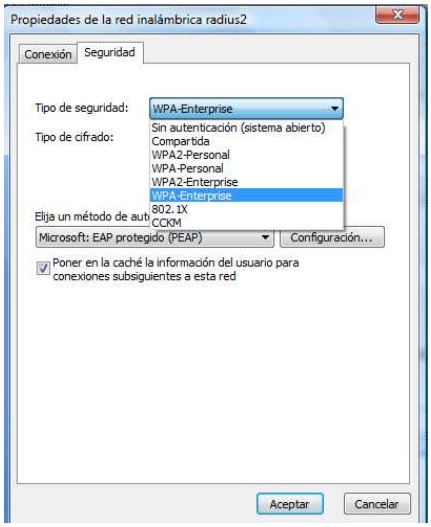


Figura 3.7 Propiedades de la red inalámbrica

Una vez seleccionado WPA-Enterprise se elige el método de autenticación EAP protegido (PEAP) y se ingresa a la pestaña de configuración. Al grabar las nuevas configuraciones y seleccionar la Red inalambrica “radius2” se mostrará una ventana en la cual se solicita el nombre de usuario y contraseña. Se deberán capturar el usuario y contraseña que se definieron en el archivo users y en este caso el dominio de inicio de sesión queda en blanco. La figura 3.8 muestra la pantalla para autenticación.

Figura 3.8 Solicitud de autenticación

3.3.6 Funcionamiento

Para el funcionamiento del Control de Acceso implementado se consideran los siguientes escenarios:

Escenario 1. Usuario que no cumple con Políticas de Seguridad.- Se refiere a un equipo que requiere ingresar a la red de la organización pero no se encuentra definido como un usuario de la red y por esta razón incumplirá en la política de seguridad y se le denegará el acceso.

Para comprobar la funcionalidad de este escenario se realizaron pruebas con 3 equipos en los que al tratar de ingresar con un usuario y contraseña que no se encuentran definidos como datos válidos se les denegó el acceso a la red. En la figura 3.9 se muestra la autenticación de rechazo.

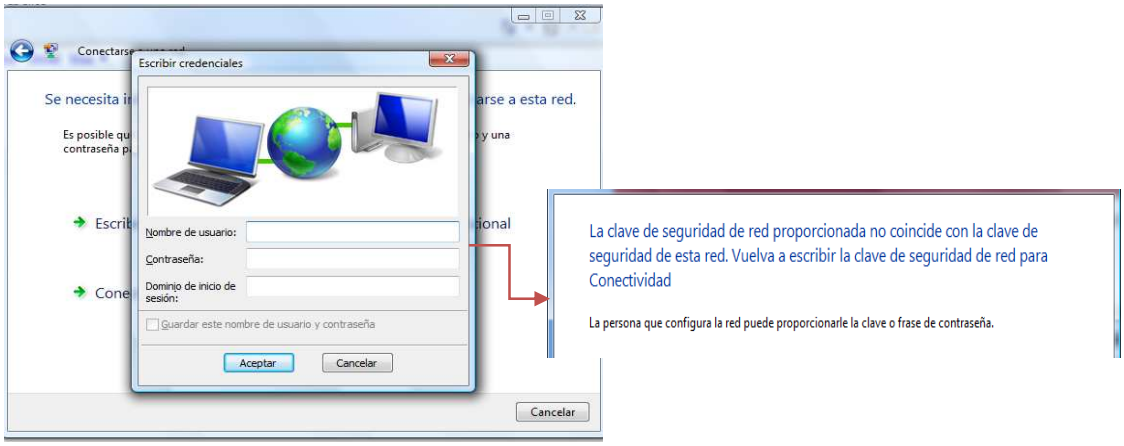


Figura 3.9 Denegación de acceso a la red

Escenario 2. Usuario que cumple con las Políticas de Seguridad.- Se refiere a un equipo que requiere ingresar a la red de la organización, el cual cumple con la política de seguridad establecida, por lo que el sistema NAC le permite el acceso a la red.

Para comprobar la funcionalidad de este escenario se realizaron pruebas con 3 equipos en los que al tratar de ingresar con un usuario y contraseña que fueron definidos como usuarios dentro de la configuración de los archivos del servidor RADIUS, al solicitar el ingreso a la red con datos válidos se permite el acceso. La figura 3.10 muestra el proceso de autenticación.

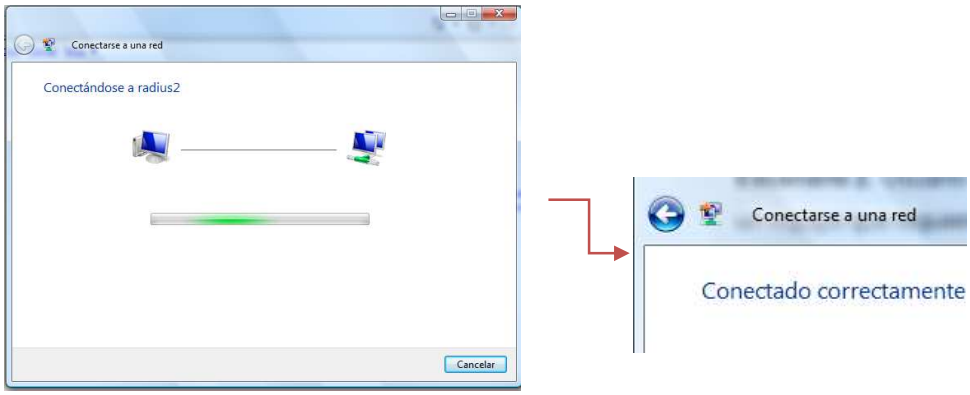


Figura 3.10 Aceptación de acceso a la red.

Una vez terminadas las etapas de instalación, configuración y pruebas del servidor RADIUS, así como la configuración del Access Point y de los equipos solicitantes, la organización aprueba la implementación del control de acceso y se comienza con la etapa de capacitación a los usuarios sobre la forma en que se autenticarán para el acceso a la red inalámbrica de la organización.

La implementación del control de acceso permitirá a la organización contar con un sistema de seguridad en el que sólo los usuarios que se autentiquen podrán accesar a la red de la organización, dando solución a la problemática de restricción de acceso a usuarios no autorizados.

CONCLUSIONES

Con la realización de este proyecto de Tesina se pudieron identificar los conceptos de redes inalámbricas, seguridad para este tipo de redes y conceptos relacionados con el protocolo RADIUS, además de la implementación de un sistema de seguridad a través de la autenticación de los usuarios para el acceso a una red inalámbrica.

La implementación del control de acceso en la red inalámbrica de la organización permitirá contar con un sistema de seguridad en el que sólo los usuarios que se autentiquen podrán accesar a la red; con lo anterior se aprecia que el sistema de seguridad implementado cubre la necesidad de la organización y da solución a su problemática de restringir el acceso a personas no autorizadas.

Como un trabajo a futuro, si se requiere contar con un sistema de seguridad de control de acceso más robusto, se puede modificar la configuración de los archivos del servidor RADIUS actualizando las políticas de control de acceso y brindar privilegios a los usuarios de acuerdo a sus roles, para que la seguridad de la organización sea mayor y se pueda tener control de los usuarios que accesan a la red inalámbrica y las actividades que realizan.

Un punto importante sobre la realización de esta investigación es que sirve como base para la implementación de un control de acceso para la red inalámbrica de cualquier organización cuando se desee tener un control sobre los usuarios que pueden accesar a la red, y brinda los conceptos importantes para ser implementado utilizando la parte de autenticación del protocolo RADIUS.

GLOSARIO

Ataque Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

Beacons Son pequeños paquetes, los cuales se utilizan para localizar la red, así como para mostrar sus características.

Biometría Ciencia que estudia las características del ser humano (el iris, la huella dactilar, la voz, etc.) para su aplicación a la seguridad informática como medio de identificación del usuario.

Cable coaxial Cable usado por las redes de cómputo al igual que en la televisión por cable, protege la señal del alambre interior contra interferencias eléctricas.

Confidencialidad Consiste en asegurar que a la información sólo accede quien está autorizado para ello.

Conmutador Dispositivo analógico de interconexión de redes de computadores.

Cracker Persona que elimina las protecciones lógicas y físicas de los sistemas para acceder a los mismos sin autorización y generalmente con malas intenciones.

Criptografía Es la ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Delito Informático Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

Encapsulamiento Es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear.

Fibra óptica Sistema de transmisión que utiliza fibra de vidrio como conductor de frecuencias de luz visible o infrarrojas. Este tipo de transmisión tiene la ventaja de que no se pierde casi energía pese a la distancia y que no le afectan las posibles interferencias electromagnéticas.

Hacker Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no se maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo.

Hardware Equipo informático. Todo aquello de un sistema informático que es tangible.

Host Máquina conectada a una red. Tiene un nombre que la identifica, el Hostname. La máquina puede ser una computadora, un dispositivo de almacenamiento por red, una impresora, etc.

Hubs Es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

Phishing Término informático que denomina un tipo de delito dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma no autorizada.

PIN Personal Identification Key. Número de Identificación Personal, es una contraseña o clave numérica que se utiliza para acceder a móviles, cajeros automáticos, servicios de telefonía, etc.

Protocolo Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

Proxy Programa o dispositivo que realiza una acción en representación de otro, que sirve para permitir el acceso a Internet a todos los equipos de una organización.

Red Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.

Router Enrutador, encaminador. Dispositivo hardware o software para interconexión de redes de computadoras.

Seguridad Característica de cualquier sistema (informático o no) el cual indique que esté libre de peligro, daño o riesgo.

Software Equipamiento lógico o soporte lógico de una computadora digital, comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).

Spam Correo basura, mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

Switch Es un dispositivo que permite la interconexión de redes sólo cuando esta conexión es necesaria.

Token Es un bloque de texto categorizado. Por un operador, un identificador, un número, etc.

Topología Cadena de comunicación, la forma en que están distribuidos los equipos en una red y es usada para comunicarse.

Virus Programa que está diseñado para copiarse a sí mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

REFERENCIAS

[1] Lanzillotta Analía, **Mastermagazine,** Núm. 6496, Año 2008.

[2] Geier Jim, **Implementing 802.1x Security Solutions for wired and wireless Networks**, Editorial Wiley, Año 2008, Págs. 3-30, 76-79.

[3] Academia de Networking de Cisco Systems, **Fundamentos de Redes inalámbricas**, Ed. Cisco Press, Última reimpresión, Año 2008, Págs. 5-7, 473-480.

[4] Fern Hansen Yago, Ramos Varón Antonio, García Morán Jean Paul, **AAA/RADIUS/802.1x. Sistemas basados en la autenticación en Windows y Linux/GNU**, Editorial Alfaomega Ra-Ma, 1a Edición Año 2009, Págs. 108-110.

[5] Audelo González, Jesús, Material docente del Seminario de Seguridad en la Información, Modulo de Seguridad Informática, Año 2009. [8], [9]

[6] http://esp.sophos.com/security/topic/your-nac-compliance, Diciembre de 2009

[7] García Serrano Alberto, **Redes Wi-Fi**, Editorial Anaya Multimedia, Año 2008, Pags. 75-88, 191-227.

[8] http://esp.sophos.com/security/topic/your-nac-compliance

[9] http://esp.s ophos.com/security/topic/your-nac-compliance

[10] http://www.linux-itt.com/2007/12/nac-control-de-acceso-la-red.html

ANEXOS

A1. Instalación de VMware Workstation 6

Es un software de virtualización disponible para Windows, Mac y Linux que permite tener un sistema operativo en una máquina virtual, corriendo sobre el sistema operativo principal (Figura A-1). Para la realización de este proyecto se crearon máquinas virtuales y se instaló Linux (Ubuntu).

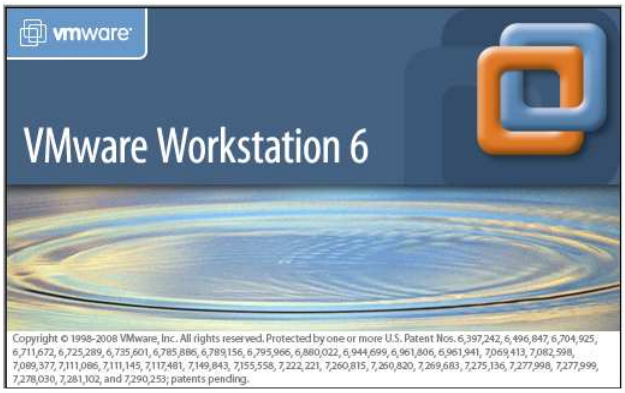


Figura A-1 VMware Workstation 6

Para la instalación de VMware se ejecuta el asistente, se acepta la licencia y se da clic en la opción Siguiente para continuar con la instalación.

Se selecciona la ruta donde se instala el software y se seleccionan los accesos directos e iconos que se crearán en la instalación. Al dar clic en el botón siguiente se inicia la instalación del software (Figura A-2). Al finalizar se debe reiniciar el equipo.

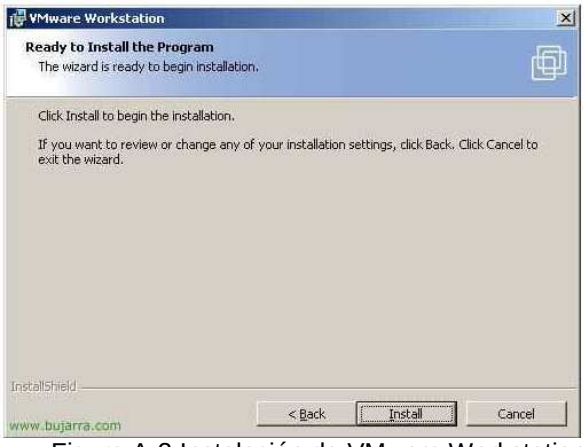


Figura A-2 Instalación de VMware Workstation 6

Al ejecutar la aplicación se crea una máquina virtual en la cual se indica el espacio en Gb que ocupará el disco virtual y se selecciona la ruta donde se creará la Maquina Virtual. Al finalizar la creación, se instala Linux (Ubuntu 9.04) y después se inicia la ejecución de la máquina virtual como se aprecia en la figura A-3.

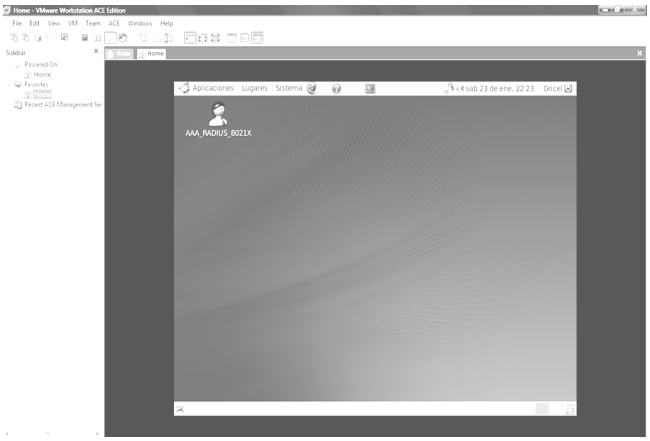


Figura A-3 Ejecución de la Máquina Virtual