ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

DESARROLLO DE UNA PLATAFORMA DE SIMULACIÓN DE REDES INALÁMBRICAS PARA EL ANÁLISIS Y EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD DEL ESTÁNDAR 802.11i

JOSUÉ ISRAEL CONRADO MENA

SANGOLQUÍ – ECUADOR

2013

CERTIFICACIÓN

Certificamos que el presente proyecto titulado:

“DESARROLLO DE UNA PLATAFORMA DE SIMULACIÓN DE REDES INALÁMBRICAS PARA EL ANÁLISIS Y EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD DEL ESTÁNDAR 802.11i”

Ha sido desarrollado en su totalidad, por el Señor: JOSUÉ ISRAEL CONRADO MENA, bajo la dirección de:

Ing. Carlos Romero	Ing. Fabián Sáenz
DIRECTOR	CO-DIRECTOR

RESUMEN

Una de las ventajas que ofrece una red inalámbrica es que cualquier usuario que se encuentre dentro del área de cobertura de la red pueda tener acceso a la misma, pero de igual forma es una puerta abierta para usuarios mal intencionados que deseen leer o modificar registros de la red.

En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo los usuarios de un sistema identificados con nombre/contraseña o la posesión de un certificado digital.

802.11i limita mediante mecanismos de seguridad el acceso a la red para usuarios no autorizados, para ello emplea claves, encriptación, cifrado y servidores externos AAA que elevan la seguridad de las redes. Para el análisis redes inalámbricas se da como solución, la simulación para evaluar diferentes topologías.

Para realizar estudios específicos se emplean simuladores sobre los cuales se experimenta en base a topologías específicas, condiciones controladas para determinar la confiabilidad de los mecanismos de seguridad.

Con la elección del software Packet Tracer 5.3 se analizará la robustez o falencia de cada topología configurando WEP, WAP, WAP2.

DEDICATORIA

A mi abuelito Victor.

Por haber sido un Padre amoroso, mi modelo y ejemplo de vida al cual quiero llegar a ser,

A mis madres Fanny, Anita y Clara.

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mi tío Fernando y hermano.

Por los ejemplos de perseverancia y constancia que los caracterizan, por el valor mostrado para salir adelante siempre y por su amor.

Josué I. Conrado M.

AGRADECIMIENTO

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mis tutores.

Que me brindaron su sabiduría en varios campos del conocimiento ayudándonos así en varios aspectos que requerimos para el desarrollo de nuestro proyecto.

PRÓLOGO

El desarrollo de la plataforma de simulación está enfocado a analizar y evaluar el acceso no autorizado a redes inalámbricas sin seguridad, y con seguridad basadas en el estándar 802.11i.

Se justifica el desarrollo de la plataforma de simulación para redes inalámbricas para determinar y evaluar qué mecanismos de seguridad son óptimos frente a determinada topología y así evitar accesos no autorizados a la red, más aún si se trata de una red privada, donde toda la información debe ser protegida de agentes externos, solo los usuarios validados bajo los mecanismos de protección que conlleva el estándar 802.11i tendrán acceso a la red.

Por medio del desarrollo de esta plataforma se podrán realizar investigaciones en el área de seguridad de la información, así también será un apoyo a procesos de docencia e investigación para la creación de nuevos proyectos que desarrollen aún más la plataforma propuesta en este proyecto.

ÍNIDICE DE CONTENIDO

ÍNDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

802.11: Grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN).

AES (*Advanced Encryption Standard*): Algoritmo de encriptación del gobierno de EE.UU, basado en el algoritmo Rijndael, método de encriptación simétrica con clave de 128 bits desarrollada por los belgas Joan Daemen y Vincent Rijmen.

***Access Point* (AP, Punto de Acceso):** Estación base que conecta una red cableada con uno o más dispositivos wireless.

Ad-Hoc: Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point.

Ancho de banda (*Bandwidth*): Fragmento del espectro radioeléctrico que ocupa toda señal de información.

Asociación: Servicio del protocolo 802.11 que asocia un cliente wireless a un Punto de Acceso.

Autentificación: Proceso de identificación de un equipo o usuario.

Bridge: Dispositivo que conecta dos segmentos de red que emplean el mismo protocolo.

BSSID, *Basic Service Set Identification*: Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo Ad-Hoc.

Clave de encriptación: Conjunto de caracteres que se utilizan para encriptar y desencriptar la información.

Cliente: Cualquier equipo conectado a una red y que solicita servicios.

DHCP, *Dynamic Host Configuration Protocol*: Protocolo para la configuración automática de los parámetros de red de los equipos.

DSSS, *Direct Sequence Spread Spectrum*: Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en el uso de bits de redundancia.

ESSID, *Extended Service Set Identification*: Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

Ethernet: Es el nombre común del estándard IEEE 802.3, que define las redes locales con cable coaxial o par trenzado de cobre.

ETSI, *European Telecommunications Standard Institute*: Organización europea sin ánimo de lucro para el desarrollo de estándares de telecomunicación, agrupa 699 miembros de 55 países.

FCC, *Federal Communication Commision*: Agencia gubernamental de los EE.UU. para la regularización de las comunicaciones por radio, televisión, cable y satélite.

FHSS, *Frequency Hopping Spread Spectrum*: Técnica de transmisión de la señal para paliar los efectos de las interferencias, que se basa en cambios sincronizados entre emisor y receptor de la frecuencia empleada.

Firewall: Sistema de seguridad que previene el acceso no autorizado a la red, restringiendo la información que entra o sale de la red.

Gateway: Dispositivo que conecta a distintas redes entre sí, gestionando la información entre ellas.

Hot Spot: Es un lugar donde se puede acceder a una red wireless pública, ya sea gratuita o de pago. Pueden estar en cyber-cafes, aeropuertos, centros de convenciones, hoteles, y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados.

Hub: Dispositivo de red multipuerto para la interconexión de equipos vía Eterhnet o wireless.

Infraestructura, modo: Es una topología de red inalámbrica en la que se requiere un Punto de Acceso.

IEEE, *Institute of Electrical and Electronics Engineers*: Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones.

IP: Un número de 32 bits que identifica a un equipo a nivel de protocolo de red en el modelo OSI.

MAC (*Media Access Control*): Es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo OSI, consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí.

Network name: Identificador de la red para su diferenciación del resto de las redes.

PHY: Nombre abreviado del nivel más bajo del modelo OSI, el nivel físico, que describe el medio físico en el que se transmite la información de la red.

Roaming: Nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

Router: Dispositivo de red que traslada los paquetes de una red a otra.

Shared Key: Proceso de autentificación por clave secreta. Habitualmente, todos los dispositivos de la red comparten la misma clave.

Spread Spectrum: Técnica de trasmisión consistente en dispersar la información en una banda de frecuencia mayor de la estrictamente necesaria, con el objetivo de obtener beneficios como una mayor tolerancia a las interferencias.

SSID, *Service Set Identification*: Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica.

TKIP, *Temporal Key Integrity Protocol*: Algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes wireless.

WEP, *Wired Equivalent Privacy*: Algoritmo de seguridad, de uso opcional, definido en el estándar 802.11.

Wi-Fi, *Wireless Fidelity*: Nombre dado al protocolo 802.11b. Los dispositivos certificados como Wi-Fi son interoperables entre sí, como garantía para el usuario.

Wi-Fi Alliance: También llamada *Wireless Ethernet Compability Alliance* (WECA).

WPA, Wi-Fi *Protected Access*: Protocolo de seguridad desarrollado por la WECA para mejorar la seguridad de la información en las redes wireless y permitir la autentificación de usuario, puntos débiles del WEP.

CAPÍTULO 1

DIAGNÓSTICO ACTUAL DE LOS MECANISMOS DE SEGURIDAD EN LOS SISTEMAS INALÁMBRICOS

1.1 Visión General

En un ambiente de comunicaciones en constante desarrollo y crecimiento, las redes inalámbricas de área local (WLAN), tienen un rol cada vez más importante en las comunicaciones, debido a su facilidad de instalación, conexión y bajo costo; se puede brindar servicio y conexión hacia la red local a lugares en las que el acceso mediante una red cableada es muy limitado.

Dichas redes inalámbricas permiten mayor movilidad a los usuarios conectados a la red mediante diferentes dispositivos móviles como PDA, PALM, PC's portátiles, teléfonos celulares, etc.; permitiendo intercambiar información en tiempo real.

Debido a la naturaleza de las comunicaciones inalámbricas, cualquier dispositivo inalámbrico presente en un área cubierta por una red inalámbrica podrá utilizarla e interceptar datos transferidos en la misma a menos que esté protegida.

Existen mecanismos de seguridad desarrollados para evitar el acceso no autorizado a los datos transferidos y a la red, tales mecanismos son, WEP, WPA y WPA2, los mismos que impiden el acceso no autorizado y cifran los datos que se envían a través de la red.

1.1.1 Usos de las redes inalámbricas

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

Enlace de áreas físicas independientes mediante Puntos de Acceso:

Un ejemplo de la comunicación de áreas físicas independientes mediante puntos de acceso es el enlace entre diferentes pisos o plantas, estos permiten realizar el enlace entre las diferentes WLAN's, mediante un mínimo cableado Ethernet cuando existe un obstáculo físico de por medio.

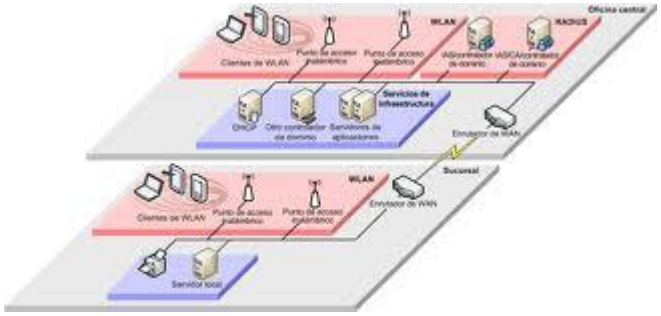

Figura. 1.1. Interconexión de distintas LAN inalámbricas por medio de Red Ethernet

Enlaces entre Edificios:

Otra aplicación importante es la interconexión entre edificios vecinos, sean LAN cableadas o no, se usa un enlace no guiado entre los edificios, los dispositivos que actúan son dispositivos de encaminamiento.

La combinación del Punto de Acceso y el Puente permite llevar a cabo el enlace entre dos áreas inalámbricas, cuando resulta imposible o demasiado caro realizar esta unión mediante un cable.

Figura. 1.2. Conexión entre 2 Edificios

Redes inalámbricas en la misma área física:

Otra aplicación es la coexistencia de varias redes inalámbricas, tanto en modo Ad-Hoc como de infraestructura, éstas pueden coexistir simultáneamente en la misma área física de cobertura de sus antenas, de forma totalmente transparente a los usuarios de cada una de las redes. Adicionalmente con una configuración de asignación de canales, ambas redes pueden operar a pleno rendimiento de su ancho de banda a 2 Mbps.

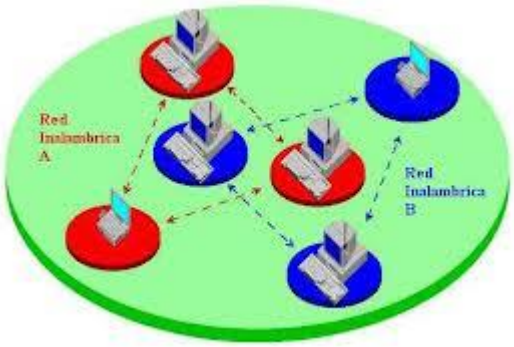

Figura. 1.3. Dos LAN inalámbricas en una misma área sin interferencias

Red Ad-Hoc

Una red ad hoc es una conexión sin servidor central, es decir, un grupo de ordenadores que se comunican cada uno directamente con los otros a través de las señales de radio si usar un punto de acceso, estas conexiones con punto a punto; y solamente los dispositivos que estén dentro del rango de cobertura podrán tendrán comunicación entre sí. Esta conexión se establece momentáneamente para satisfacer una necesidad inmediata.

Figura. 1.4. LAN inalámbrica Ad-hoc

1.1.2 Requerimientos de las redes inalámbricas[2]

Los requisitos básicos para diseñar e implementar una red inalámbrica son: alta capacidad, coberturas de pequeñas distancias, conectividad total de las estaciones conectadas y capacidad de difusión. A continuación se enuncian las especificaciones para el diseño de las WLAN's.

- **Rendimiento:** el protocolo de acceso al medio debería hacer uso tan eficiente como fuera posible del medio no guiado para maximizar la capacidad.

- **Número de Nodos:** las LAN inalámbricas pueden necesitar dar soporte a cientos de nodos mediante el uso de varias celdas.

- **Conexión a la LAN troncal:** en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de las LAN inalámbricas con infraestructura, esto se consigue fácilmente a través del uso de módulos de control que se conectan con ambas tipos de LAN.

- **Área de Servicio:** una superficie de cobertura para una red LAN inalámbrica tiene un diámetro típico de entre 100 y 300 metros.

- **Consumo de Batería:** los usuarios móviles utilizan estaciones de trabajo con baterías que se necesitan tener una larga vida cuando se usan adaptadores sin cable. Esto sugiere que resulta inapropiado un protocolo MAC que necesita dos móviles para supervisar constantemente los puntos de acceso o realizar comunicaciones frecuentes con una estación base. Las implementaciones típicas de LAN inalámbricas poseen características propias para reducir el consumo de potencia mientras no se esté usando la red, como un modo de descanso (*sleep mode*).

- **Robustez en la Transmisión y Seguridad:** a menos que exista un diseño apropiado, una LAN inalámbrica puede ser propensa a sufrir interferencias y escuchas. El diseño de una LAN inalámbrica e incluso entornos ruidosos y debe ofrecer ciertos niveles de seguridad contra escuchas.

- **Funcionamiento de redes adyacentes:** a medida que las LAN inalámbricas se están haciendo más populares, es probable que dos o más de estas redes operen en la misma zona o en alguna en la que sea posible la interferencia entre ellas. Estas interferencias pueden repercutir negativamente en el funcionamiento normal del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.

- **Funcionamiento sin licencia:** los usuarios preferirían adquirir y trabajar sobre LAN inalámbricas que no precisen de una licencia para la banda de frecuencias usada por la red.

- **Traspasos (*Handoff*)/Itinerancia (*Roaming*):** el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.

- **Configuración Dinámica:** los aspectos de direccionamiento MAC y de gestión de la red de la LAN deberían permitir la inserción, eliminación y traslados dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

- **Medios de Enlace:** en este caso es el inalámbrico, el cual se propuso inicialmente para la transmisión de datos.

- **Especificaciones del medio físico:** En la normalización 802.11 al se definen tres esquemas de transmisión.
  - Infrarrojos.
  - Espectro expandido de secuencia directa.
  - Espectro expandido de salto de frecuencia.

1.1.3 Ventajas e inconvenientes de las redes inalámbricas

Ventajas de las redes inalámbricas

Una red WLAN ofrece a los usuarios mayor flexibilidad, debido a que no necesitan un medio físico para la conexión y no necesariamente deben estar en sus puestos de trabajo para acceder a los datos de la red.

A continuación se enuncian ciertas ventajas de las redes inalámbricas:

- **Accesibilidad:** La mayoría de los dispositivos portátiles de hoy vienen equipados con la tecnología Wi-Fi necesaria para conectarse directamente a una red inalámbrica. Se puede hacer uso a los datos de la red siempre y cuando los usuarios se encuentren autenticados para acceder de forma

segura desde cualquier ubicación dentro del área de cobertura. La accesibilidad y rango de cobertura de la red inalámbrica, depende del diseño y de cada punto de acceso, ésta cobertura se puede ampliar colocando repetidoras para la expansión de la señal.

- **Movilidad:** Cada usuario puede permanecer conectado a la red incluso cuando no se encuentren en sus puestos de trabajo. Dentro de cada área los usuarios pueden acceder a documentos y aplicaciones obteniendo información importante para su desempeño, la movilidad puede darse con cualquier dispositivo terminal.

- **Productividad:** El acceso a la información y a las aplicaciones clave de una compañía permite a los usuarios desempeñar su trabajo y fomentar la colaboración. Los grupos de usuarios como propios de la empresa, ó agentes externos debidamente autenticados pueden tener acceso de invitado seguro a internet y a los datos de empresa.

- **Fácil configuración:** Debido a la ausencia de cableado físico para la implementación, la instalación puede ser más rápida y rentable. Las redes inalámbricas también facilitan la conectividad de red en ubicaciones de difícil acceso sobre las cuales exista una limitante u obstáculo físico, como en una bodega.

- **Escalabilidad:** Conforme se presenta un crecimiento en los usuarios y las labores que cada uno ejerce en la red, crece la funcionalidad y operaciones de la misma, puede que necesite ampliar la red rápidamente y esto se puede lograr sin un costo adicional, es decir, se logra con el equipo existente; mientras que una red cableada puede necesitar cableado adicional.

- **Seguridad:** Mediante la especificación de cada estándar 802.11, se puede controlar y gestionar el acceso a la red inalámbrica, y depende de esto su

éxito. Estas protecciones de seguridad son sólidas para que los datos sólo estén disponibles a los usuarios a los que se les permita el acceso.

- **Costes:** Con una red inalámbrica se puede reducir los costes, ya que se eliminan o se reducen los costes de cableado durante los traslados de puestos de trabajo a los usuarios, nuevas configuraciones o expansiones.

Inconvenientes de las redes inalámbricas

- **Velocidad:** Los estándares para redes inalámbricas más utilizados son el IEEE 802.11a, 802.11b, 802.11g y 802.11n. Así que dada la descripción de cada estándar la velocidad máxima de transmisión que se tiene actualmente en una red inalámbrica, es de 600Mbps, en la práctica. Y realizando una comparación con una red cableada utilizando cable UTP categoría 5e, permite velocidades de transmisión de hasta 1Gigabit (1000 Mbps); es decir, casi el doble.

- **Seguridad:** La seguridad en las redes inalámbricas siempre ha sido una de sus principales debilidades, desde el protocolo de cifrado WEP que es el más débil hasta el WPA2 que en la actualidad es considerado de los más seguros actualmente.[3]

- **Estabilidad:** Hay muchos factores que afectan las conexiones en una red inalámbrica:

  - Los materiales de construcción del lugar en donde se va a instalar la red (si son techos o paredes muy gruesas o hay muchas estructuras metálicas, etc.)
  - Si hay muchas redes cercanas en la misma banda, la velocidad se ve afectada porque se interfieren unas con otras.
  - Teléfonos inalámbricos, portones automáticos, hornos de microondas y cualquier dispositivo que utilice la misma banda que utiliza la red inalámbrica que se instala puede causar interferencia

En una red cableada, la mayoría de las fallas se deben a un cable o un puerto en mal estado.[3]

1.2 Esquemas de Transmisión – Robustez

Los equipos inalámbricos emplean ondas de radio en sus comunicaciones, de esta manera, se puede llevar la información de un punto a otro sin necesidad de una instalación para ello, evitando posibles obstáculos entre emisor y receptor. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora (modulación) de radio y el receptor debe extraerlos de ésta (demodulación).[4]

Las redes LAN inalámbricas se clasifican, generalmente, de acuerdo con la técnica de transmisión usada. Actualmente existen tres tipos de tecnología de transmisión que utilizan las redes WLAN:

1.2.1 Infrarrojos (IR)

Las WLAN por infrarrojos son aquellas que usan el rango infrarrojo del espectro electromagnético para transmitir información mediante ondas por el espacio libre, estos sistemas son simples y con menos costo, de esta forma los infrarrojos son susceptibles de ser interrumpidos por cuerpos opacos pero se pueden reflejar en determinadas superficies.

Los infrarrojos no restringen su ancho de banda ya que la señal no se dispersa, algunos dispositivos que utilicen infrarrojos pueden usar todo el ancho de banda del infrarrojo, cuando se estén comunicando con otro sin provocar ningún tipo de interferencia con algún otro dispositivo.

Un sistema basado en infrarrojos es que éste no requiere ningún tipo de licencia por el uso del espectro. La radiación infrarroja cae en el segmento visible del espectro electromagnético el cual no es regulado por ninguna entidad.

Para la capa infrarroja tenemos las siguientes velocidades de transmisión:

- 1 y 2 Mbps Infrarrojos de modulación directa.
- 4 Mbps mediante Infrarrojos portadora modulada.
- 10 Mbps Infrarrojos con modulación de múltiples portadoras.

Clasificación[5]

De acuerdo al ángulo de apertura con que se emite la información en el transmisor, los sistemas infrarrojos pueden clasificarse en sistemas de corta apertura o llamados de rayo dirigido o de línea de vista (*line of sight*, LOS) y en sistemas de gran apertura, reflejados o difusos (*diffused*).

Los sistemas infrarrojos de corta apertura, resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente. Este mecanismo solo es operativo en enlaces punto a punto exclusivamente. Por ello se considera que es un sistema inalámbrico pero no móvil, o sea que está más orientado a la portabilidad que a la movilidad.

Los sistemas de gran apertura*,* consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso, hacia el cual dirigen los dispositivos inalámbricos su información, y desde el cual ésta es difundida hacia esos mismos dispositivos. La dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión (la trayectoria

reflejada llega con un retraso al receptor). Esta es una de las dificultades que han retrasado el desarrollo del sistema infrarrojo en la norma 802.11.

1.2.2 **Sistemas de Banda Estrecha**

Se transmite y recibe en una específica banda de frecuencia lo más posible para el paso de la información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias.
Así mismo, un filtro en el receptor de radio se encarga de dejar únicamente la señal esperada en la frecuencia asignada.

Estas WLANs operan en el rango de las microondas pero no hacen uso del espectro expandido. Algunos de estos productos operan a frecuencias para las que es necesario licencia para su uso, mientras que otras lo hacen en alguna de las bandas ISM (Industria, Científica y Médica), para las cuales no es necesario tener licencia.

1.2.3 Sistemas Basados en Banda Ancha o Espectro Expandido

El fundamento básico es el ensanchamiento de la señal a transmitir a lo largo de una banda muy ancha de frecuencias, mucho más amplia, de hecho, que el ancho de banda mínimo requerido para transmitir la información que se quiere enviar. No se puede decir que las comunicaciones mediante espectro ensanchado son medios eficientes de utilización del ancho de banda. Sin embargo, rinden al máximo cuando se los combina con sistemas existentes que hacen uso de la frecuencia.

La señal de espectro ensanchado, una vez ensanchada puede coexistir con señales en banda estrecha, ya que sólo les aportan un pequeño incremento en el ruido. En lo que se refiere al receptor de espectro ensanchado, él no ve las señales de banda estrecha, ya que está escuchando un ancho de banda mucho más amplio gracias a una secuencia de código preestablecido. [6]

Las señales de Espectro Expandido son similares al ruido, difíciles de detectar, y aún más difícilmente de interceptar o demodular sin el equipo apropiado. Dado que las señales de radio comunes tienen un espectro estrecho sólo interferirán en una pequeña porción de la señal esparcida en el espectro, obteniendo como resultado una menor interferencia y menores errores en la transmisión.

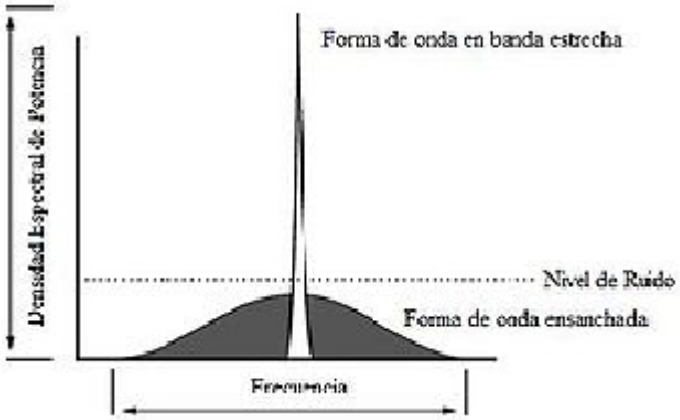

Figura. 1.5. Banda estrecha vs Banda ancha o espectro expandido.

La IEEE 802.11 define dos posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa o DSSS (*Direct Sequence Spread Spectrum*).

- Espectro expandido por salto de frecuencias o FHSS (*Frecuency Hopping Spread Spectrum*)

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación, por un lado, y prestaciones y fiabilidad, por otra. [7]

1.2.3.1 Espectro expandido por salto de frecuencias o FHSS (*Frecuency Hopping Spread Spectrum*)[7,8]

La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada dwell time e inferior a 400 ms.
Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo. El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, y que tanto el emisor y el receptor deben conocer.

Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en le tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

Esta técnica también utiliza la zona de los 2.4GHz, la cual organiza en 79 canales con un ancho de banda de 1MHz cada uno. El número de saltos por segundo es regulado por cada país, así, por ejemplo, Estados Unidos fija una tasa mínima de saltas de 2.5 por segundo.

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia FSK (*Frequency Shift Keying*), con una velocidad de 1Mbps ampliable a 2Mbps. En la revisión del estándar, la 802.11b, esta velocidad también ha aumentado a 11Mbps, la técnica FHSS sería equivalente a una multiplexación en frecuencia.

Tabla. 1.1. Rango de frecuencias empleadas en FHSS

Canal	Frec. U.S.A	Frec. Europa	Frec. Japón
1	2412 MHz	N/A	N/A
2	2417 MHz	N/A	N/A

3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	N/A	2484

1.2.3.2 Ensanchado por Secuencia Directa o DSSS (Direct Sequence Spread Spectrum)[7,8]

En esta técnica se genera un patrón de bits redundante (señal de chip) para cada uno de los bits que componen la señal. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original.

La secuencia de bits utilizada para modular los bits se conoce como secuencia de *Barker* (también llamado código de dispersión o *PseudoNoise*). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0.

Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Esta secuencia proporciona 10.4dB de aumento del proceso, el cual reúne los requisitos mínimos para las reglas fijadas por la FCC.

Una vez aplicada la señal de chip, el estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado por secuencia directa (DSSS), la modulación DBPSK (*Differential Binary Phase Shift Keying*) y la modulación DQPSK (*Differential Quadrature Phase Shift Keying*), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente.

En configuraciones donde existan más de una celda, estas pueden operar simultáneamente y sin interferencias siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz.

Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal, la técnica de DSSS podría compararse con una multiplexación en frecuencia.

Tabla. 1.2. Rango de frecuencias DSSS

Límite Inferior	**Límite Superior**	**Rango Regulatorio**	**Área Geográfica**
2.402 GHz	2.480 GHz	2.400 - 2.4835 GHz	América del Norte
2.402 GHz	2.480 GHz	2.400 - 2.4835 GHz	Europa
2.473 GHz	2.495 GHz	2.471 - 2.497 GHz	Japón
2.447 GHz	2.473 GHz	2.445 - 2.475 GHz	España

2.448 GHz	2.482 GHz	2.4465 - 2.4835 GHz	Francia

1.3 Vulnerabilidades[9,10]

La seguridad informática es vulnerada fácilmente en muchas empresas y actualmente han surgido nuevas técnicas de robo informático, técnicas de suplantación de identidad, donde individuos u organizaciones ajenas acceden a la red para manipular información confidencial que puede tener la empresa, trayendo pérdidas financieras y espionaje corporativo.

La vulnerabilidad de las redes inalámbricas es el medio de transporte, ya que el aire es un medio de acceso para cualquier persona. Por lo tanto cualquiera que capte señal del punto de acceso, podrá acceder a la red. Con la posibilidad de navegar gratis en Internet, emplear la red como punto de ataque hacia otras redes, robar software o información, introducir virus o software maligno, entre otras cosas.

Además los dispositivos de acceso son manejados con niveles de autorización de forma individual, donde es necesario registrar a los usuarios en cada dispositivo. Lo cual demanda al administrador mayor tiempo para gestionar el acceso de autorización, ocasionando que con el tiempo se pierda este control y eso causa que se dejen puertos abiertos para el ingreso de usuarios no autorizados o de usuarios con cuentas caducadas.

Como primera medida de seguridad se recomienda que la red WLAN se encuentre físicamente separada (mediante Firewalls) de la red LAN de la empresa. Así mismo, debido a la creciente necesidad de movilidad por los empleados nómadas o itinerantes, se recomienda que el mecanismo de seguridad seleccionado para entorno corporativo sea compatible (en última instancia el mismo) con el que utilicen los empleados fuera del límite físico de su empresa.

Los ataques a las redes inalámbricas se hacen en dos etapas, en la primera se obtiene información de la red mediante ataques pasivos, y en la segunda se accede a la red mediante ataques activos.
El objetivo de la seguridad en redes inalámbricas es proveer el mismo nivel de seguridad y confianza que se tendría con una red cableada, utilizando mecanismos basados en métodos de cifrado y de autenticación/autorización.

Ataques Pasivos. El principal objetivo del atacante es obtener información. Estos ataques suponen un primer paso para ataques posteriores. Algunos ejemplos de este tipo de ataques serían el espionaje, escuchas, *wardriving* y los ataques para el descubrimiento de contraseñas.

Ataques Activos. Estos ataques implican la modificación en el flujo de datos o la creación de falsos flujos en la transmisión de datos. Pueden tener dos objetivos diferentes: pretender ser alguien que en realidad no se es o colapsar los servicios que puede prestar la red.

En la actualidad existen diferentes mecanismos de seguridad para redes WLAN, los cuales están evolucionando continuamente para adaptarse a las necesidades de seguridad de los usuarios móviles. Estas necesidades de seguridad vienen a su vez impuestas por las vulnerabilidades existentes en los mecanismos de seguridad de las redes WLAN (mecanismos como WEP ó WPA) así como por la diversidad de ataques conocidos.

El mecanismo IEEE 802.11i es el único mecanismo específico para redes WLAN cuyo algoritmo de cifrado no ha sido vulnerado, por lo que puede ser considerado como un mecanismo seguro para entornos corporativos. El inconveniente de esta solución, es que en el caso de algunos fabricantes es necesario cambiar los puntos de acceso previamente instalados por unos puntos de acceso que soporten IEEE 802.11i. Además, actualmente los dispositivos PDA existentes no son compatibles con el algoritmo de cifrado AES empleado por el mecanismo IEEE 802.11i por falta de capacidad de procesado.

1.4 Evolución estándares wifi[11, 12]

1.4.1 802.11 *legacy*

La versión original del estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 megabits por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR). IR sigue siendo parte del estándar, si bien no hay implementaciones disponibles. [11]

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

1.4.2 802.11a

El estándar 802.11a utiliza el mismo protocolo principal que el estándar original, funciona en 5 GHz de banda, y utiliza una multiplexación por división de frecuencias ortogonales (OFDM) sub-portadora 52 con una velocidad de datos brutos máxima de 54 Mbps. Esto produce una capacidad alcanzable neta real de aproximadamente 25 Mbps. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 y luego a 6 Mbps si se requiere.

802.11a posee 12 canales que no se superponen, 8 dedicados a interiores y 4 a punto a punto. No es interoperable con 802.11b/g, salvo que se utilice un equipo que implemente ambos estándares.

1.4.3 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 Mbits sobre TCP y 7,1 Mbit/s sobre UDP.

El aumento dramático en la capacidad de 802.11b (comparado con el estándar original) junto con una reducción importante de precios condujo a la rápida aceptación del 802.11b como la tecnología de redes LAN inalámbricas definitiva.

1.4.4 802.11 c

Es menos usado que los primeros dos, pero por la implementación que este protocolo refleja. El protocolo ‘c’ es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. El protocolo ‘c’ es más utilizado diariamente, debido al costo que implica las largas distancias de instalación con fibra óptica, que aunque más fidedigna, resulta más costosa tanto en instrumentos monetarios como en tiempo de instalación.

El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos capa 2 del modelo OSI).

1.4.5 802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos

intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil.

1.4.6 802.11e

La especificación IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, ésta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad con ellos. Estas prestaciones resultan fundamentales para las redes domésticas y para que los operadores y proveedores de servicios conformen ofertas avanzadas. El documento que establece las directrices de QoS, aprobado el pasado mes de noviembre, define los primeros indicios sobre cómo será la especificación que aparecerá a finales de 2001. Incluye, asimismo, corrección de errores (FEC) y cubre las interfaces de adaptación de audio y vídeo con la finalidad de mejorar el control e integración en capas de aquellos mecanismos que se encarguen de gestionar redes de menor rango. El sistema de gestión centralizado integrado en QoS evita la colisión y cuellos de botella, mejorando la capacidad de entrega en tiempo crítico de las cargas. Estas directrices aún no han sido aprobadas. Con el estándar 802.11, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado *Hybrid Coordination Function* (HCF) con dos tipos de acceso:

- (EDCA) *Enhanced Distributed Channel Access*, equivalente a DCF.
- (HCCA) *HCF Controlled Access*, equivalente a PCF.

En este nuevo estándar se definen cuatro categorías de acceso al medio (Ordenadas de menos a más prioritarias).

- *Background* (AC_BK)
- Best Effort (AC_BE)
- *Video* (AC_VI)
- *Voice* (AC_VO)

Para conseguir la diferenciación del tráfico se definen diferentes tiempos de acceso al medio y diferentes tamaños de la ventana de contención para cada una de las categorías.

1.4.7 802.11f

Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

1.4.8 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Que es la evolución del estándar 802.11b, Este utiliza la banda de 2,4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o equipos de radio apropiados.

Existe una variante llamada 802.11g+ capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

1.4.9 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ECC/DEC/(04)08).

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión. Selección Dinámica de Frecuencias y Control de Potencia del Transmisor DFS (*Dynamic Frequency Selection*) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin

de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles. TPC (*Transmitter Power Control*) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

1.4.10 802.11i

Está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (*Estándar de Cifrado Avanzado*). Se implementa en WPA2.

1.4.11 802.11j

Es equivalente al 802.11h, en la regulación Japonesa.

1.4.12 802.11k

Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión. Está diseñado para ser implementado en software, para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

1.4.13 802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La

velocidad real de transmisión podría llegar a los 300 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO *Multiple Input – Multiple Output*, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (3). Existen también otras propuestas alternativas que podrán ser consideradas. El estándar ya está redactado, y se viene implantando desde 2008.

A principios de 2007 se aprobó el segundo boceto del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo estuviera implantado). Ha sufrido una serie de retrasos y el último lo lleva hasta noviembre de 2009. Habiéndose aprobado en enero de 2009 el proyecto 7.0 y que va por buen camino para cumplir las fechas señaladas.1 A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física. En la actualidad la mayoría de productos son de la especificación b o g, sin embargo ya se ha ratificado el estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen el estándar N con un máximo de 300 Mbps (80-100 estables).

El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empiezan a fabricar de forma masiva y es

objeto de promociones por parte de los distintos ISP, de forma que la masificación de la citada tecnología parece estar en camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador wifi integrado, para poder conectarse a la red.

Sin duda esta es la principal ventaja que diferencia wifi de otras tecnologías propietarias, como LTE, UMTS y Wimax, las tres tecnologías mencionadas, únicamente están accesibles a los usuarios mediante la suscripción a los servicios de un operador que está autorizado para uso de espectro radioeléctrico, mediante concesión de ámbito nacional.

La mayor parte de los fabricantes ya incorpora a sus líneas de producción equipos wifi 802.11n, por este motivo la oferta ADSL, ya suele venir acompañada de wifi 802.11n, como novedad en el mercado de usuario doméstico.

Se conoce que el futuro estándar sustituto de 802.11n será 802.11ac con tasas de transferencia superiores a 1 Gb/s.[4]

1.4.14 802.11p

Este estándar opera en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

1.4.15 802.11r

También se conoce como *Fast Basic Service Set Transition*, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función, que una vez enunciada parece obvia e indispensable en un sistema de datos inalámbricos, permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa

magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

1.4.16 802.11v

IEEE 802.11v servirá para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías: mecanismos de ahorro de energía con dispositivos de mano VoIP Wi-Fi en mente; posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación; temporización, para soportar aplicaciones que requieren un calibrado muy preciso; y coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

1.4.17 802.11w

Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envían la información del sistema en tramas desprotegidos, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

CAPÍTULO 2

FUNDAMENTACIÓN TEÓRICA DEL ESTÁNDAR 802.11i

2.1 Qué es 802.11i?

Debido a la complejidad que se introduce la seguridad en las WLAN con el estándar 802.11i, gran parte de usuarios posponen su adopción por cuestiones de coste, complejidad e interoperabilidad; en lo posterior todos los usuarios y de acuerdo a las políticas de las organizaciones implementarán este tipo de seguridad haciéndose obligatorio para el uso interno de los recursos de las instituciones.

Desde un tiempo atrás en el mercado los productos *Wireless* LAN (WLAN) que implementan el nuevo estándar de seguridad inalámbrica 802.11i resuelven sin duda algunos de los inconvenientes que las organizaciones presentan a la introducción de manera indiscriminada de redes inalámbricas en sus empresas.

Dicho estándar elimina muchas de las debilidades de seguridad de los estándares predecesores, tanto en lo que autenticación de usuarios como a robustez de los métodos de encriptación se refiere. Esto se logra gracias a la capacidad para trabajar en colaboración con 802.1X e incorporación de encriptación *Advanced Encryption Standard* (AES), también reduce considerablemente la complejidad y el tiempo de roaming de los usuarios entre varios puntos de acceso.

El estándar 802.11i es una mejora y una evolución de las tecnologías anteriores, WEP (*Wired Equivalent Privacy*) es el primer protocolo de seguridad inalámbrica que la IEEE reconoció. Este permite utilizar claves encriptadas de 40

bits según el algoritmo de encriptación RC4 asignando a cada usuario una clave por sesión. Pero desde que en el verano de 2001 fuera hackeado empezó a considerarse como el Talón de Aquiles de la cadena de seguridad inalámbrica. Se trató de reparar en algo lo ocurrido combinando WEP con el protocolo de autenticación 802.1X, ya que con esta implementación el usuario WEP está obligado a solicitar acceso a la red utilizando EAP (*Extensible Authentication Protocol*), esto es mencionado en 802.1X.

La mejora de seguridad propuesta no tuvo los resultados esperados, debido a que solamente cubría la deficiencia de WEP en el área de la autenticación, dejando sin procesar y aun lado la falencia sobre una parte de la ecuación, la encriptación. Debido a este proceso sin término se desarrolla WPA, que incrementa la potencia de la encriptación mediante la aplicación de la técnica TKIP (*Temporal Key Integration Protocol*). Mediante este protocolo, la clave utilizada por cada usuario cambia por varias ocasiones durante cada sesión. Aparte de TKIP, otro cambio fue dado en la sustitución de RC4 por el algoritmo más robusto AES, desarrollado para el ejército estadounidense por el *National Institute of Standards*, aportaba una ventaja más a las prestaciones de seguridad ideadas para WPA.

A la final WPA no concluyó con AES debido a la impaciencia de los fabricantes ante la urgente demanda de productos WLAN con mayores niveles de seguridad que los proporcionados por WEP. Como tal, se empezó la comercialización de productos WPA sólo con TKIP.

La técnica de TKIP fue ideada como solución temporal para WEP, incluyendo en su solución gran parte de las características, como son el mecanismo de encriptación y el algoritmo RC4. La principal característica y ventaja es el carácter temporal en las claves utilizadas, pudiendo cambiar incluso para cada paquete dentro de una misma sesión. De la misma manera, las claves son de mayor longitud, siempre de 128 bits; por lo que resulta más difícil el acceso no autorizado o violación que las claves utilizadas en el modelo WEP con RC4. A pesar de que TKIP (con WPA) constituyó probablemente en su momento la mejor solución disponible, nunca se superó los problemas que acarreaba ya que el

protocolo debía operar sobre el hardware existente y, por tanto, no puede introducir encriptación avanzada si antes dicho hardware no se actualiza con más potencia informática.

Otras tecnologías de seguridad que sugiere el organismo Wi-Fi son servidores RADIUS, para trabajar con claves de acceso en usuarios inalámbricos y remotos, VPN (*Virtual Private Network*), que supone un canal más seguro entre el usuario y la red, Firewalls, para controlar los datos salientes y entrantes de las máquinas de tal manera de impedir que usuarios sin autorización tengan acceso a la información, y Kerberos, servicio de autentificación desarrollado en el MIT (*Massachussets Institute of Technology*).[14]

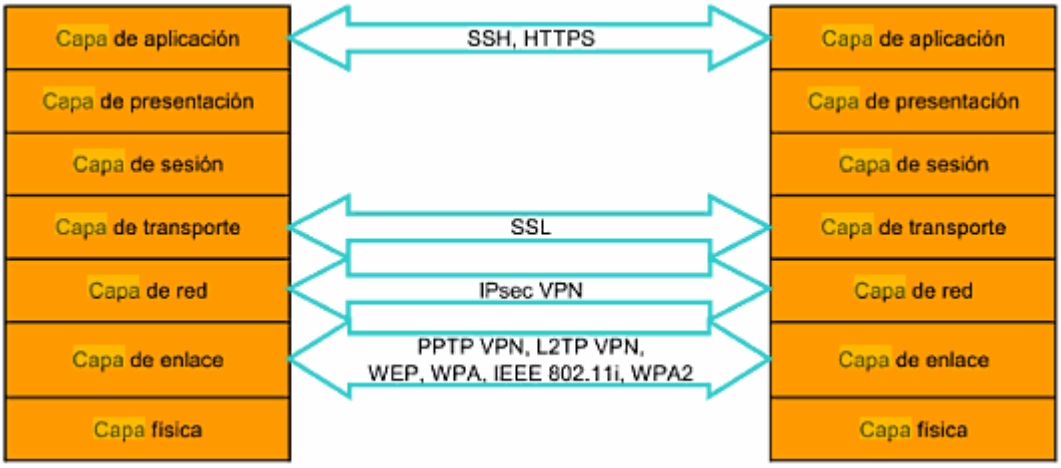

Figura. 2.1. Mecanismos de seguridad existentes en las distintas capas del modelo OSI

2.1.1 Evolución de la seguridad

El canal de transmisión en las redes inalámbricas es un medio inseguro, debido a que la información que se transmite puede ser escuchada y modificada por cualquiera, introduciendo información nueva y falsa además de modificar o eliminar la información que ya existe en una determinada organización.

Denotando este problema sobre las WLAN, el IEEE se encarga de publicar un mecanismo de seguridad, llamado WEP (*Wired Equivalent Privacy*), en la especificación de las redes inalámbricas 802.11. Debido a que es el primer

mecanismo de seguridad adoptado para las redes WLAN, WEP ha sido vulnerado de distintas maneras, por lo que se evidencia como una protección no útil e inservible para entornos en los que es fundamentalmente necesaria la seguridad.

Como respuesta a esta problemática, el IEEE empieza el desarrollo de una nueva norma de seguridad para este tipo de redes, conocida como 802.11i, no se adopta inmediatamente este mecanismo debido a la demora en su aprobación, en vista de esto las organizaciones deciden utilizar otro tipo de tecnologías como las VPNs, que aseguran los extremos de la comunicación. La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN. De hecho, como hemos comentado antes, ambos canales de transmisión deben considerarse inseguros. Una desventaja de las VPNs es el costo elevado para la implementación en redes WLAN.

Como medida urgente y oportuna la WiFi Alliance lanza un mecanismo de seguridad intermedio hasta la adopción y disponibilidad del estándar 802.11i, como resultado es el aparecimiento de WPA (Wi-Fi Protected Access).

La aparición de WPA2 (*Wi-Fi Protected Access 2*) se da para eliminar y corregir las vulnerabilidades y fallas generadas en WPA, la alianza Wi-Fi nombra es esta versión como clave pre-compartida WPA-Personal y WPA2-Personal y a la versión mediante autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

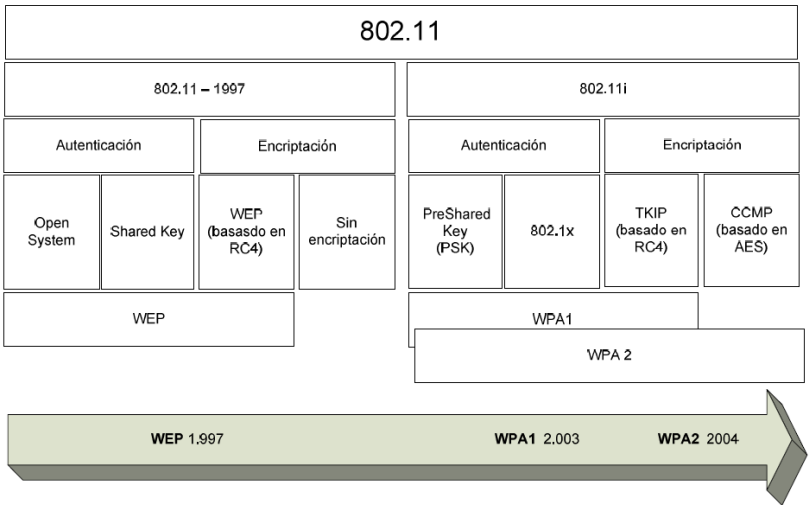

Figura. 2.2. Evolución de Mecanismos de seguridad del estándar 802.11

2.1.1.1 WEP (*Wired Equivalent Privacy*)

El diseño WEP (Wireless Equivalent Privacy) fue dado para brindar seguridad a los clientes mediante los servicios de autenticación, integridad y confidencialidad. Este intento por cubrir las debilidades de seguridad no se cumplieron, debido a fallos tanto en el concepto de diseño, como en el mecanismo usado para el cifrado.

El protocolo WEP no fue creado por expertos en seguridad o criptografía, así que pronto se demostró que era vulnerable ante los problemas RC4 descritos por David Wagner cuatro años antes. En 2001, Scott Fluhrer, Itsik Mantin y Adi Shamir (FMS para abreviar) publicaron su famoso artículo sobre WEP, mostrando dos vulnerabilidades en el algoritmo de encriptación: debilidades de no-variación y ataques IV conocidos. Am bos ataques se basan en el hecho de que para ciertos valores de clave es posible que los bits en los bytes iniciales del flujo de clave dependan de tan sólo unos pocos bits de la clave de encriptación (aunque normalmente cada bit de un flujo de clave tiene una posibilidad del 50% de ser diferente del anterior).

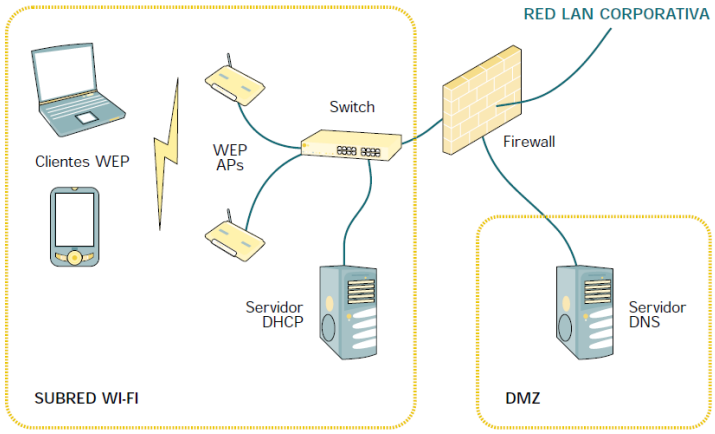

Figura. 2.3 Arquitectura de seguridad mediante WEP

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva en la mayoría de ocasiones, que la clave se cambie poco o nunca.

Al utilizar el algoritmo de clave simétrica RC4 para cifrar los datos, se expande la clave compartida y se genera un flujo de bits pseudoaleatorios llamados Key Stream. Para cifrar el mensaje se realiza la operación XOR (OR-exclusiva) entre el Key Stream y el mensaje a enviar, generándose un flujo de datos cifrados llamado *Cipher Stream*. Para recuperar el mensaje se vuelve a realizar la operación XOR entre el *Cipher Stream* recibido y el *Key Stream*.

WEP dispone de la utilización de una clave estática para cada uno de los elementos que componen la red con una longitud de 104 bits (o 40 bits para claves más cortas), la misma que la define el administrador de la red. Esta clave estática se concatenará con una clave dinámica (IV) elegida pseudo aleatoriamente por el nodo emisor, con una longitud de 24 bits en todos los casos, y enviada en el paquete WEP sin encriptación alguna. La secuencia de bits obtenida por la concatenación de la clave estática definida por el usuario en adición a la clave dinámica establecida por el nodo emisor, le servirán al algoritmo

RC4 como parámetro de entrada para el cálculo de un flujo de salida utilizado posteriormente en la operación XOR, dando como resultado el cifrado completo del mensaje a transmitir. Este parámetro de entrada utilizado por el RC4 es comúnmente llamado semilla. El emisor por su parte podrá generar la misma salida RC4 o *keystream* debido a que posee la misma clave estática que el emisor y además puede obtener la clave dinámica del paquete WEP enviado por el emisor pudiendo así generar la misma semilla utilizada para cifrar el mensaje. Al obtener el mismo *keystream* utilizado para encriptar, será posible finalmente para el receptor, recuperar el mensaje original aplicando la operación XOR entre el *keystream* y el mensaje recibido, como se explicó anteriormente. La secuencia de pasos utilizados por el mecanismo de encriptación WEP para transformar un flujo de datos en texto cifrado añadiendo cifras CRC se realiza como se describe en el siguiente gráfico:

Proceso de cifrado[15]

- A la trama en claro se le computa un código de integridad (*Integrity Check Value*, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.

- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aleatorios.

El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).
- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.
- El IV y la trama se transmiten juntos.

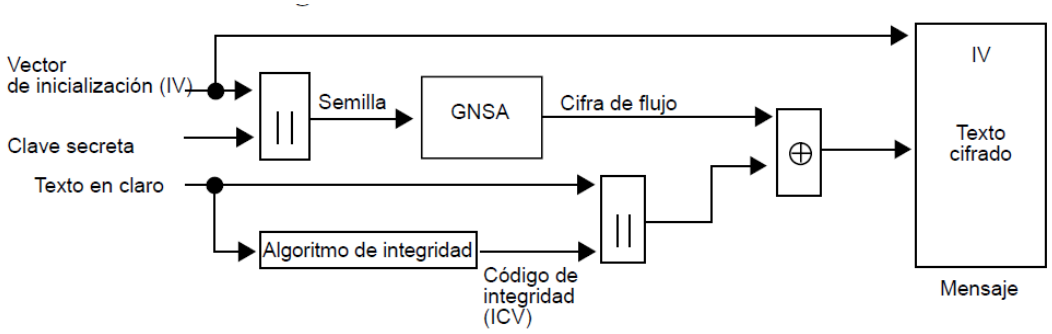

Figura. 2.4. Algoritmo WEP, función cifrado.

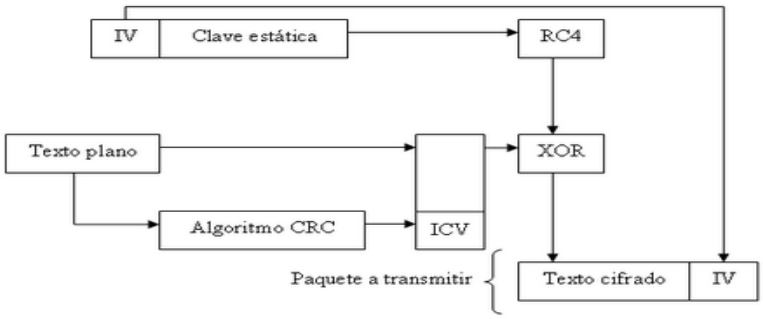

Figura. 2.5. Algoritmo WEP, función cifrado.

El paquete que será transmitido se compone de:

Figura. 2.6. Descripción de paquetes a trasmitir.

En donde:

- Cabecera 802.11: información relativa al tipo de paquete, las direcciones MAC del emisor y receptor del mensaje y determinada información de sincronismo.

- Vector de inicialización (IV): clave dinámica dada por el emisor y utilizada para concatenar con la clave estática dando origen a la semilla RC4. Esta secuencia de bits es crítica para conservar la privacidad de los datos que viajan por la red sin ningún tipo de cifrado.

- Datos encriptados: el mensaje que se desea transmitir de manera segura desde un nodo emisor a un nodo receptor.

- CRC encriptado: código de redundancia cíclica correspondiente al mensaje que se va a transmitir.

- CRC del paquete: código de redundancia cíclica correspondiente al paquete completo.

Código de Redundancia Cíclica o CRC

El código de redundancia cíclica es una función que permite el ingreso de datos de longitud variable y da como resultado una salida de longitud fija, es decir, a cada bloque de datos le corresponde una secuencia fija de números binarios conocida como código CRC. Cuando uno de estos bloques de datos es ingresado, la función es aplicada nuevamente a estos datos, si el código CRC que se genera no es igual al código CRC original, significa que el bloque de datos presenta un error. Esto conlleva que nuevamente se lea el bloque de datos o se reenvíe la información.

Si los dos códigos CRC coinciden se puede asumir que el bloque no presenta errores. CRC es el método más eficiente de comunicación digital para detectar errores.

“Suponiendo que se desea transmitir un paquete M de datos con una longitud de K bits; el objetivo del algoritmo CRC será crear una secuencia de bits F con longitud N para añadir a M para su posterior transmisión. A la unión de las secuencias M y F la llamaremos T y tendrá una longitud de K+N a fines de simplificar este ejemplo. La secuencia de bits F o bits de redundancia se generarán de forma que T sea exactamente divisible por un patrón fijo de bits P llamado polinomio CRC o polinomio generador. Tanto el emisor como el receptor tendrán fijado el valor de P, por lo que el receptor de un mensaje deberá verificar que la secuencia T recibida sea divisible por la secuencia P; en caso que no lo sea significa que existió un error en la transmisión.

Tanto el proceso del cálculo de la secuencia F, como la revisión por el receptor, requieren pocos pasos y son muy sencillos de implementar tanto en hardware como en software por lo que prácticamente no le quitan eficiencia al protocolo WEP.” [16]

Para calcular F el emisor deberá:

- Obtener la secuencia de bits a transmitir M.
- Añadir a la secuencia M la cantidad de G bits 0 a la derecha, siendo G la cantidad de bits que contiene el polinomio CRC menos 1.
- Dividir lo obtenido en el paso anterior por P.
- El resto de la división binaria será F.
- Añadir F a M y transmitir el paquete.

Por otro lado el receptor al recibir el paquete podrá comprobar su validez realizando las siguientes operaciones:

- Recibir el paquete.
- Dividir la secuencia recibida por el patrón o polinomio P.
- Si el resto de la división anterior es cero, el paquete ha sido correctamente transmitido.

Algoritmo RC4

El funcionamiento del algoritmo es simple y se divide en dos fases:

- Primera fase (KSA), se desordena una secuencia de números consecutivos inicialmente ordenados. En esta fase es donde se utiliza la clave WEP compuesta por el vector de inicialización junto a la clave estática definida por el usuario. Existen en total una gran cantidad de posibilidades de ordenamiento de 256 números diferentes; más precisamente se podrán obtener 256! combinaciones correspondientes a las permutaciones de los 256 elementos. La clave WEP completa influirá directamente en cómo estos números son ordenados debido a que la posición en la que quedará un número determinado será dependiente de los distintos caracteres de la clave, a los cuales se les aplicarán operaciones MOD (resto de la división) y sumas para determinar dicha posición.
- Segunda fase (PRGA), aquí se genera la secuencia de números pseudo aleatorios a los cuales el protocolo WEP le aplicará la operación XOR con el mensaje que se desea encriptar, en esta fase se utilizará la secuencia de números desordenados en la etapa KSA a los cuales se les aplicarán nuevamente operaciones MOD y sumas para ir calculando los diferentes bytes que compondrán el keystream utilizado para encriptar el mensaje.

Proceso de descifrado[15]

En el receptor se lleva a cabo el proceso de descifrado:

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.

- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.

- Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.

- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.

- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

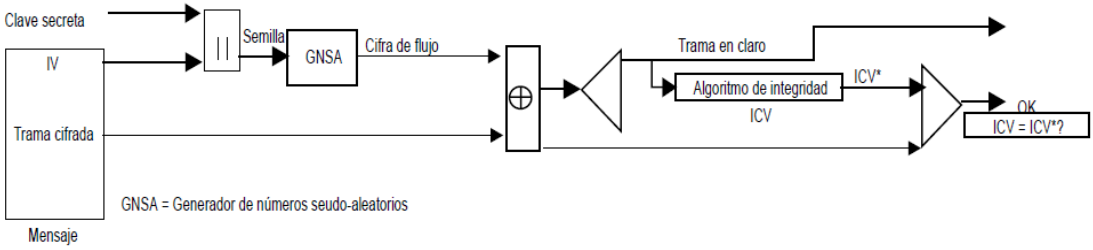

Figura. 2.7. Algoritmo WEP, función descifrado.

Desventajas WEP

- Al no disponer WEP de autenticación, no es necesario una vinculación directa con la red por lo que, simplemente con que un dispositivo y el punto de acceso compartan la misma clave se tendrá acceso a la red.

- Las claves WEP son estáticas, una vez configurada la clave en el punto de acceso casi nunca se la cambia.

- Para una red que genere gran cantidad de tráfico, el IV es de longitud insuficiente (24 bits). Debido a que el cifrado de cada trama se lo realiza con un IV distinto, es inevitable que las 224 IV distintos se agoten. Con dos tramas de IV idéntico, se puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico.

- Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

- Debilidades del algoritmo RC4 dentro del protocolo WEP debido a la construcción de la clave.

- Los IVs son demasiado cortos (24 bits – hacen falta menos de 5000 paquetes para tener un 50% de posibilidades de dar con la clave) y se permite la reutilización de IV (no hay protección contra la repetición de mensajes).

- No existe una comprobación de integridad apropiada (se utiliza CRC32 para la detección de errores y no es criptográficamente seguro por su linealidad).

- No existe un método integrado de actualización de las claves.

Se han dado dos variantes para mejorar el IV de WEP. Así tenemos:

- WEP2: Es el mismo sistema aumentado en tamaño el IV y una protección de encriptación de 128 bits.

- WEP+: Este mecanismo es propietario de la empresa Lucent Technologies, es basado en la eliminación de los IV “débiles”, este sistema debe ser implementado en los dos lados de la trasmisión. Al no ser una tecnología libre, no existen muchos fabricantes que lo integren y por tanto no presenta de una gran disponibilidad.

2.1.1.2 802.1.x

802.1x es una solución de autenticación hacia un usuario, se basa en el modelo de cliente servidor restringiendo la conexión de equipos o usuarios no autenticados o autorizados a la red.

802.1X facilita el sistema de control de dispositivos de red, de admisión, de tráfico y gestión de claves. Basa su funcionamiento en puertos, a cada solicitante se asigna un puerto utilizado para administrar la conexión punto a punto. Sin una validación previa el puerto de la comunicación solicitante permanece cerrado.

Prácticamente 802.1x asocia tres componentes elementales que son:

- Cliente: usuario que solicita la conexión.
- Servidor de autorización y autenticación (RADIUS): define que usuarios son los autorizados para el acceso a la información.
- Autenticador: es un equipo de red que recepta a conexión del solicitante, es un componente intermediario que permite el acceso solamente cuando el servidor de autenticación lo autoriza.
- PAE (*Port Access Entity*): Entidad software asociada con cada puerto que soporta funcionalidad tanto de cliente como de autenticador.
- Puerto controlado: cualquier puerto del *switch* que tenga activada la característica de seguridad basada en EAP.

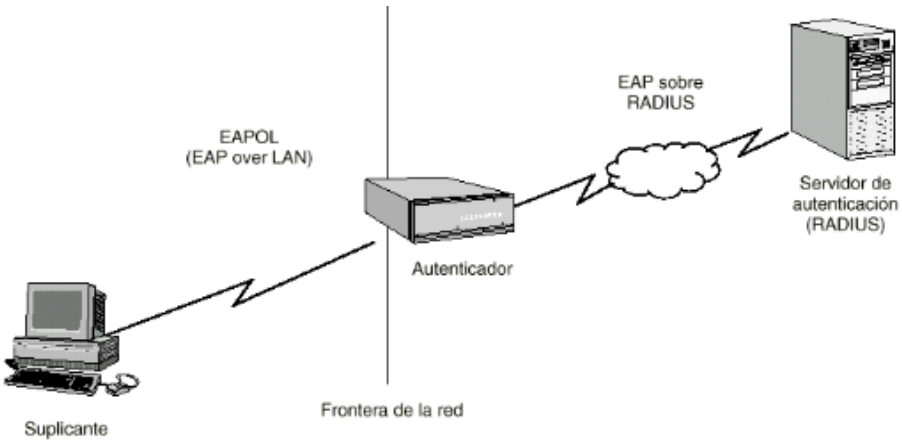

Figura. 2.8. Autenticación 802.1x

802.1x basa su funcionamiento en el protocolo EAP (Protocolo de autenticación extensible), definido por el IETF. Este protocolo se usa para transportar la información de identificación del usuario.

EAP *Extensible Authentication Protocol*

EAP es un protocolo basado en el uso de un controlador de acceso, llamado autenticador, este permite o deniega el acceso a la red a un solicitante. El autenticador es una especie de contrafuegos que se ubica entre el usuario y el server, sus características no deben presentar robustez ya que su función es muy básica.

El servidor de autenticación que en la mayoría de veces es un servidor RADIUS es conocido como NAS (Servicio de autenticación de red o Servicio de acceso a la red), este componente es el encargado de permitir el acceso de un usuario a la red según la configuración de sus credenciales.

Proceso de autenticación mediante EAP y RADIUS:

- Una vez encendido el suplicante se enlaza hacia el punto de acceso, el tráfico normal por la interfaz de conexión se encuentra bloqueado.

- El suplicante envía un mensaje *EAPOL-start* hacia el autenticador para iniciar la autenticación.

- El autenticador envía al suplicante una identiicación mediante un EAP *Request/Identity*.

- El suplicante se identifica con un EAP *Response/Identity*.

- Una vez que se recibe la información de identidad el autenticador envía un mensaje *RADIUS-Access- Challenge*, en este momento se debe resolver un desafío por el suplicante para obtener el acceso, dicho desafío se envía en un *EAP/Request*.

- El suplicante responde con un *EAP/Response* al autenticador con las credenciales, el autenticador reenvía la información al servidor con un *RADIUS-Access-Response*.

- Validada toda la información obtenida el servidor envía al autenticador un mensaje *RADIUS Access Acept* al autenticador para que otorgue los permisos al cliente sobre el puerto solicitante, además de toda la

información para efectuar la conexión de red. En el caso de una red inalámbrica el servidor RADIUS envía en el mensaje *RADIUS Access Acept* las claves WEP dinámicas para cifrar las conexiones entre el suplicante y el punto de acceso; el servidor es el encargado de cambiar periódicamente las claves para evitar la obtención de la misma.

- El autenticador envía un mensaje *EAP-Success* al suplicante y apertura el puerto con las instrucciones del servidor RADIUS.

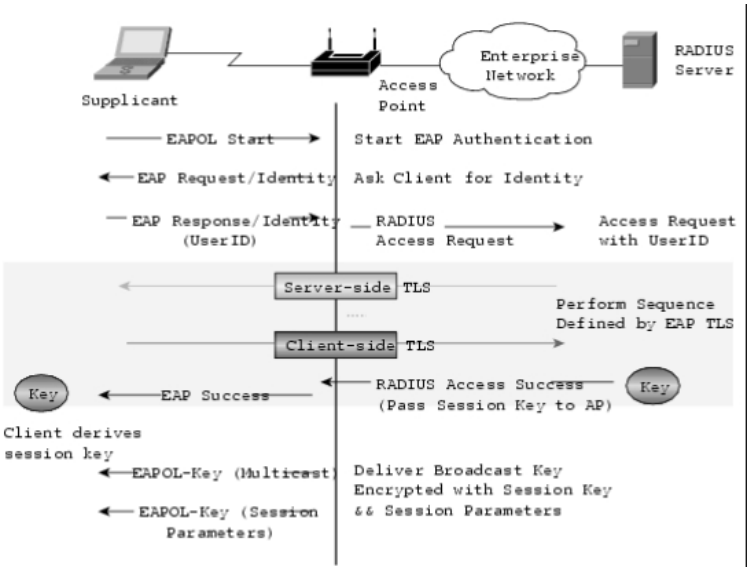

Figura. 2.9. Autenticación EAP- RADIUS

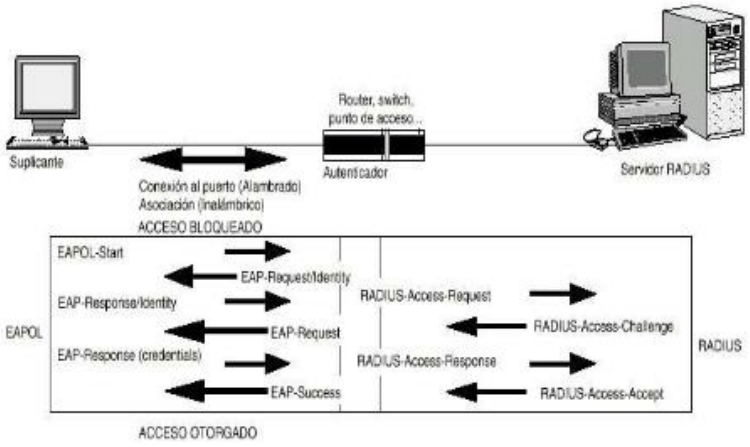

Figura. 2.10. Autenticación EAP- RADIUS

Según la autenticación que se emplee EAP puede variar de diferentes formas, entre los que contienen los certificados de seguridad y los que utilizan contraseñas.

Certificados de seguridad

- **EAP-TLS**

  El servidor autentica al cliente y viceversa utilizando claves dinámicas WEP, requiere la instalación de certificados en el suplicante y servidor; el proceso de autenticación entre el suplicante y autenticador emplea el cifrado TLS (*Transparent Layer Substrate*)

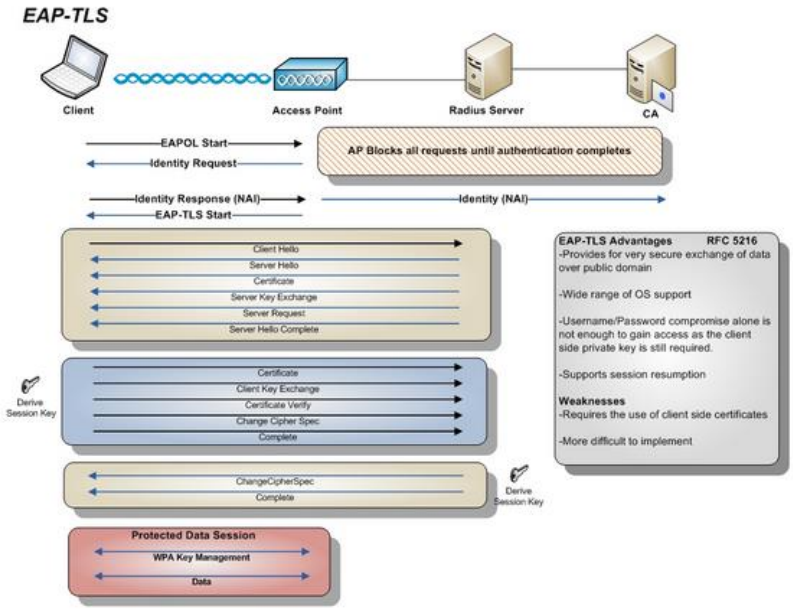

Figura. 2.11. Funcionamiento EAP-TLS

- **EAP-TTLS**

  Función similar a EAP-TLS, con la diferencia que solamente se necesita de la instalación de certificado en el servidor.

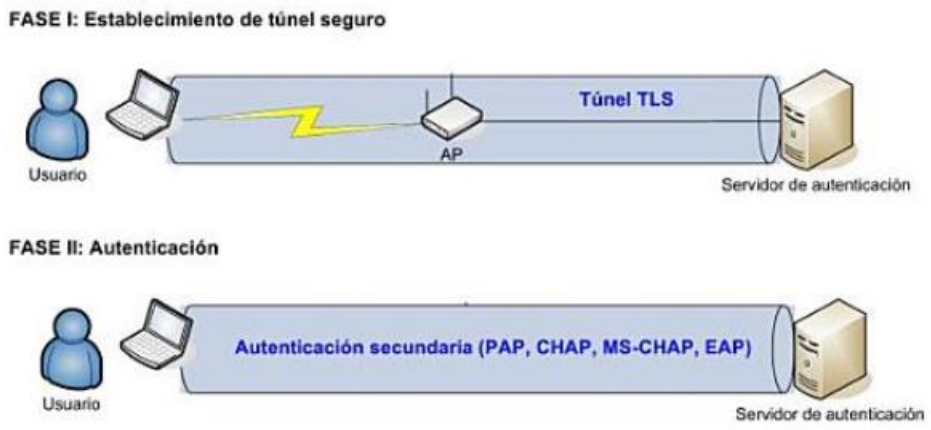

Figura. 2.12. Funcionamiento EAP-TTLS

- **PEAP**

  Establece la protección a través de un túnel seguro TLS entre el suplicante y autenticador.

  Desventajas:

  - Administrar los certificados es costoso ya que se debe adquirir los certificados con una autoridad de certificación AC.
  - El proceso de autenticación es largo, molesto para los usuarios.
  - En caso de robo a un dispositivo con el certificado, la red corre un alto riesgo.

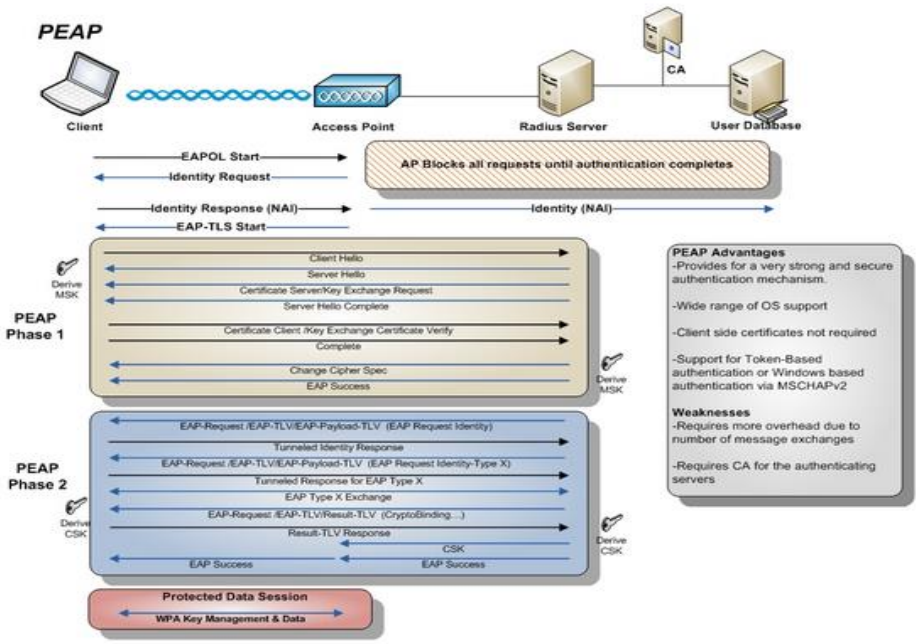

Figura. 2.13. Funcionamiento PEAP

Contraseñas

- **EAP-MD5**

  Se establece un usuario y contraseña para la autenticación, tiene una seguridad limitada, no existe autenticación hacia el servidor y solamente se genera claves WEP estáticas.

- **LEAP**

  Se establece un usuario y contraseña además de claves WEP dinámicas, es una variante propietaria de CISCO por lo que establece que los AP sean de la misma marca y la compatibilidad de RADIUS.

2.1.1.3 WPA Acceso Wi-Fi protegido

Este mecanismo fue desarrollado para corregir la vulnerabilidad de WEP, WPA eleva los niveles de seguridad elevados en comparación con su antecesor. Para solventar las debilidades que evidencia WEP, se han desarrollado varias soluciones de seguridad, como *Lightweight Extensible Authentication Protocol*

(LEAP), de *Cisco Systems*; las mismas que no presentan una gran interoperabilidad por sus limitaciones, marcas propietarias e infraestructura.

Este mecanismo adopta en su mayoría el estándar 802.11i, es decir es un puente entre WEP y el total desarrollo de 802.11i/WAP2, se adopta la autenticación de los suplicantes mediante un servidor donde se guardan las credenciales con los respectivos tipos de accesos, además de una clave pre-compartida PSK (*Pre-Shared Key*) Clave Pre-compartida.

La gran característica del WPA es la implementación de redes inalámbricas en sitios públicos, a diferencia de WEP sobre el cual se presenta una gran problemática que es la seguridad, la Wi-Fi Alliance exigió incorporar este nuevo mecanismo en las certificaciones Wi-Fi. De esta forma, será un mecanismo por defecto de los sistemas inalámbricos WLAN; esto es una gran forma de seguridad para los pequeños negocios.

En definitiva WPA involucra dos aspectos:

- Sistema de encriptación mediante TKIP

- Proceso de autenticación mediante 802.1x.

En este sistema se introduce el Protocolo de Integridad de Clave Temporal TKIP (*Temporal Key Integrity Protocol*), una de las características es el cambio de claves dinámicamente a medida que se da la utilización de la red. Otro factor cambiante es que el VI presenta una longitud más amplia de 48 bits, evitando con esta mejora los intentos de intrusión hacia la red.

Otros factores que se implementan en este mecanismo son MIC Código de Integridad de Mensaje (*Message Integrity Code*), protección contra ataques de repetición (*replay attacks*). Para evitar y limitar los ataques de riesgo, los controladores de los suplicantes se desconectan durante un tiempo establecido por el fabricante, si reciben más de una colisión MIC en menos de un minuto, se pueden reenviar las claves o dejar de responder durante un tiempo específico.

Esto para no llegar a que se realicen los ataques de fuerza bruta, destinados a intentar hasta lograr el propósito.

MIC es un hash criptográfico en una sola vía, este reemplaza al CRC32, tiene una función matemática de gran fuerza en la cual tanto el receptor como transmisor deben computar.

Autenticación

Para cifrar el contenido del *payload* discriminando el tipo de tráfico del paquete *unicast, broadcast, multicast*, WPA utiliza varias claves temporales llamadas PTK (*Primary Temporal Key*) para el primer paquete y GTK (*Group Temporal Key*) para los faltantes. Estas claves se regeneran cada determinado tiempo, esto para evitar la captura de la clave. PSK no es la cadena utilizada para encriptar los paquetes y autenticar el suplicante al punto de acceso; PSK forma parte de PMK (*Primary Master Key*), de esto se obtiene una cadena de 256 bits.

Para generar la PMK se utiliza:

- Clave precompartida
- EDDID del punto de acceso
- Longitud del ESSID
- Barajado de 4096 procesos.

PMK = PBKDF21 (Frase secreta, ESSID, Long(ESSID), 4096, 256)

Previo la obtención de la clave, comienza la autenticación con el punto de acceso, este proceso se conoce como *4-Way Handshake*.

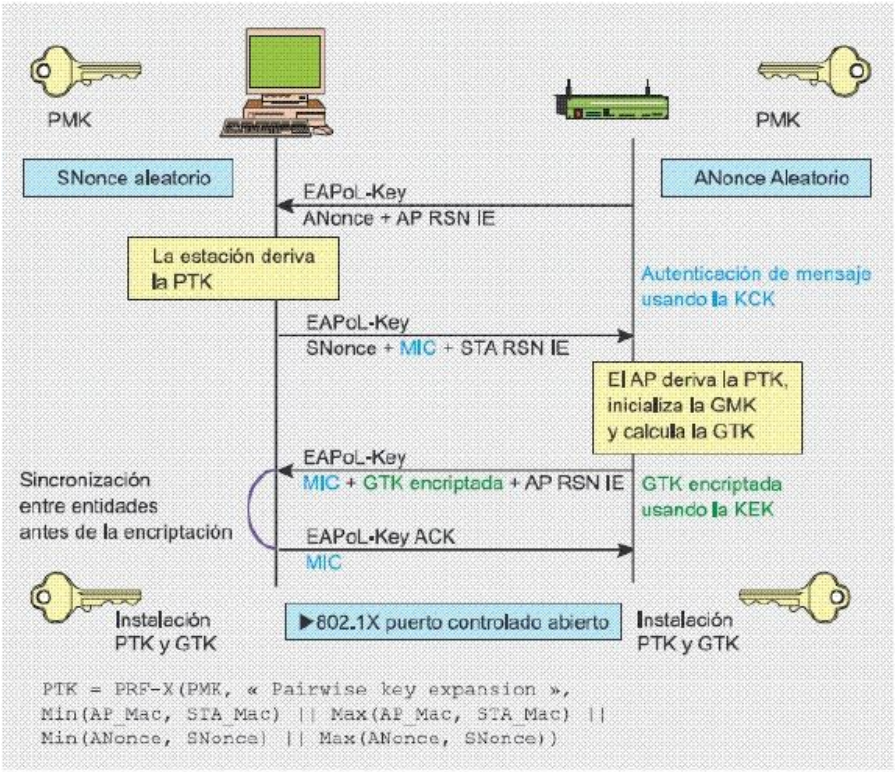

Figura. 2.14. Proceso 4-Way Handshake

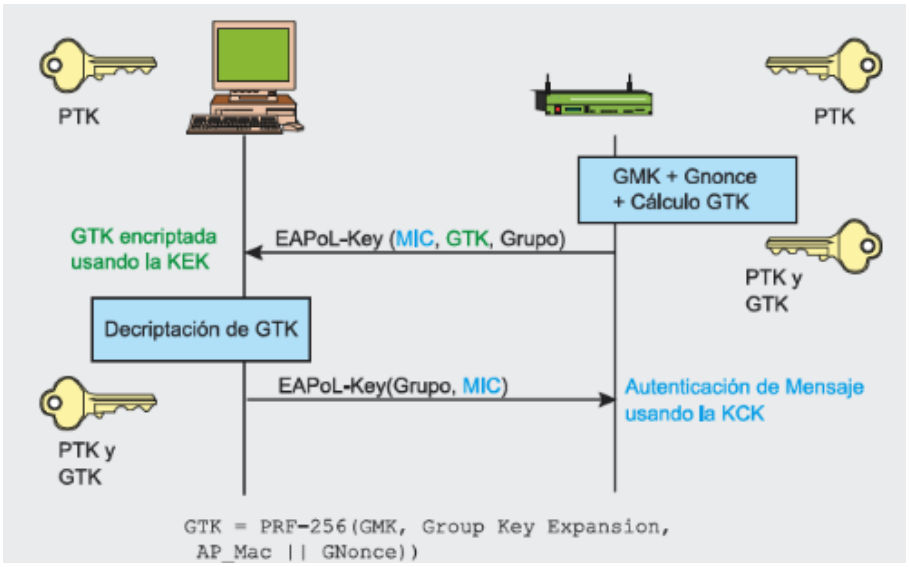

Figura. 2.15. Generación GTK

Así pues tanto la estación como el AP generan a partir de los siguientes valores la PTK y GTK utilizada para cifrar los datos. Siendo ambas diferentes en cada sesión.

WPA-PSK

WPA-PSK es una clave compartida, la diferencia radica en la gestión dinámica de claves que eleva el nivel de seguridad. WPA-PSK utiliza una clave de acceso con longitud entre 8 y 63 caracteres, y al igual que WEP, la misma clave se la configura en todas las estaciones suplicantes y puntos de acceso de la red WLAN. Cada suplicante que comparta la misma identificación tendrá acceso a la red.

Este mecanismo es una buena opción para ofrecer seguridad a negocios pequeños debido a:

- Configuración simple.
- Seguridad aceptable.
- No necesita ningún componente adicional.

Debilidades de WPA-PSK

- Clave compartida entre estaciones.
- Al establecer el diálogo de autenticación con el suplicante, se conoce el contenido del paquete de autenticación y el valor cifrado; mediante un proceso de ataque de diccionario o fuerza bruta, se puede intentar determinar la contraseña.

TKIP *Temporal Key Integrity Protocol*

Este protocolo gestiona las claves dinámicas admitidas por cualquier adaptador que permite utilizar una clave distinta para cada paquete transmitido. La clave se construye a partir de la clave base, la dirección MAC de la estación emisora y del número de serie del paquete como vector de inicialización.

Al transmitir información usando el protocolo TKIP se incluye un único número de serie único de 48 bits que varían incrementa en cada nueva

transmisión para asegurar las distinción de claves; evitando de esta manera ataques de colisión, que se basan en paquetes cifrados con la misma clave.

Se evitan vectores de inicialización duplicados al usar el número de serie del paquete como vectores de inicialización, si se inyectara un paquete con una contraseña temporal que hubiese sido detectada, los paquetes estarían fuera de secuencia y serían descartados.

En cuanto a la clave base, se genera a partir del identificador de asociación, un valor que crea el punto de acceso cada vez que se asocia una estación. Además del identificador de asociación, para generar la clave base se utilizan las direcciones MAC de la estación y del punto de acceso, la clave de sesión y un valor aleatorio.

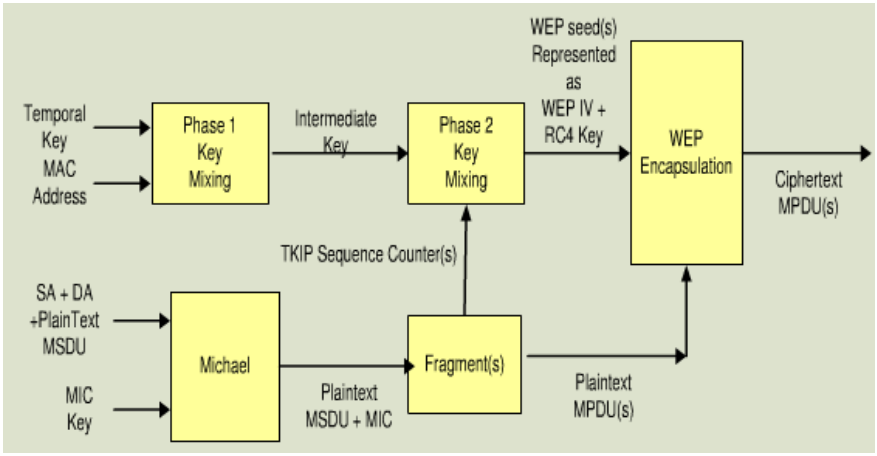

Figura. 2.16. Proceso de Encriptación TKIP

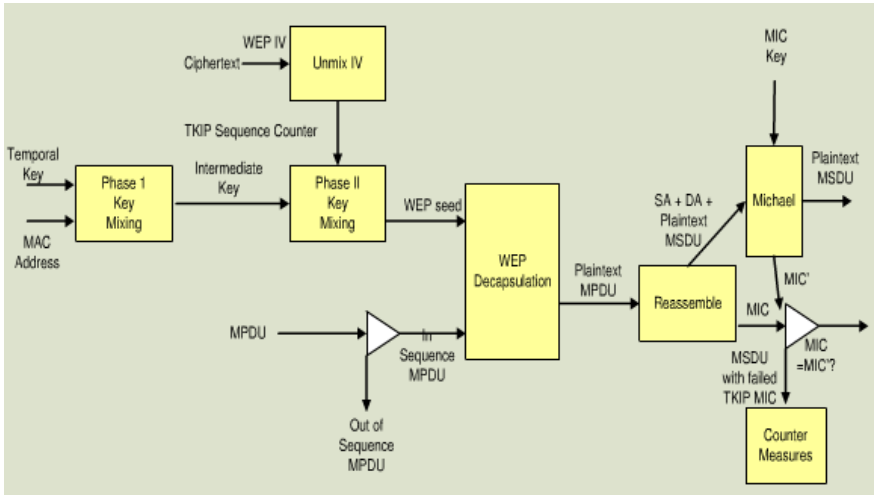

Figura. 2.17. Proceso de Desencriptado TKIP

En definitiva las funciones principales de TKIP son:

- Encripta el contenido de la Capa 2.

- Lleva a cabo un control de la integridad del mensaje (MIC) en el paquete encriptado. Esto ayuda a asegurar que no se altere un mensaje.

WPA Empresarial

Para sistemas de redes empresariales es prioritario contar con sistemas que validen en su totalidad los accesos a determinada información corporativa. Se trata de un sistema más complejo y funciona mediante el uso de usuario y contraseña o sistemas de certificados. Se suele utilizar con equipos de gran potencia como servidores, para la gestión de usuario o certificados.

2.1.1.4 WPA2

Durante el completo desarrollo del estándar 802.11i, se podría considerar a WPA como una migración, WPA2 es la versión certificada del estándar de la IEEE 802.11i ratificado en junio del 2004 y lanzado en septiembre 2004. Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (*Advanced Encryption Standard*).

Durante el intercambio de información en el proceso de conexión RSN, si el cliente no soporta las autenticaciones que especifica el AP (Punto de Acceso), será desconectado pudiendo sufrir de esta manera un ataque DoS específico a WPA.

Existen dos variantes las cuales marcan la diferencia entre WPA y WPA2:

- Cambio o migración del algoritmo MIC-Michael por Counter-Mode/CBC-Mac" (CCMP) que corresponde a un código de autenticación, considerado criptográficamente seguro.

- El reemplazo del algoritmo RC4 por el AES (*Advanced Encryption Standard*).

Los términos utilizados por la Wi-Fi Alliance para los diferentes mecanismos son:

- Versión de clave pre-compartida: WPA-Personal y WPA2-Personal.

- Versión con autenticación 802.1x/EAP: WPA-Enterprise y WPA2-Enterprise.

El estándar IEEE802.11i define dos modos de operación que son:

- WPA-Personal: Implementación de infraestructura basada en WPA sin utilizar un servidor de autenticación.

- WPA-Enterprise: Este modo requiere de una infraestructura de autenticación 802.1x con un servidor de autenticación, generalmente un servidor RADIUS.

IEEE 802.11i y WPA2 son prácticamente los mismos ya que utilizan el código de cifrado AES/CCMP en lugar de RC4/TKIP. WPA2 funciona en un modo mixto con TKIP y CCMP para la compatibilidad con WPA, este mecanismo pierde ciertas características en el servicio de voz en cuanto a latencia se refiere

Autenticación

Debido a la transición WPA2 utiliza los mecanismos definidos en IEEE802.11i y WPA, los cuales se enunciaron anteriormente.

Cifrado CCMP - *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*

Este protocolo es un algoritmo de cifrado utilizado por AES, tiene como características confidencialidad e integridad. Basado en el modo CCM utiliza una longitud de 128 bits para la llave y con VI de 48 bits.
Este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (*Advanced Encryption Standards*), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC y La utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

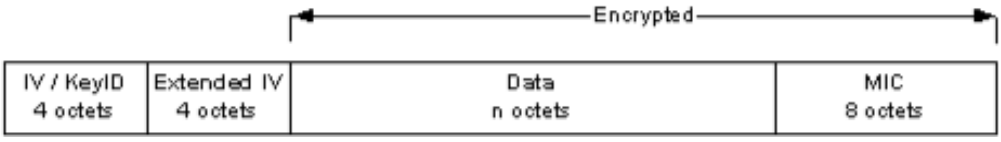

Figura. 2.18. Estructura de la encriptación CCMP

Proceso de encriptación CCMP

CCMP utiliza un IV de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

En el proceso de encriptación CCMP, la encriptación de los bloques utiliza la misma llave temporal tanto para el cálculo del MIC como para la encriptación del paquete. Como en TKIP, la llave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x. Como podemos observar en la figura 5, el cálculo del MIC y la encriptación se realiza de forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabe cera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES. [19]

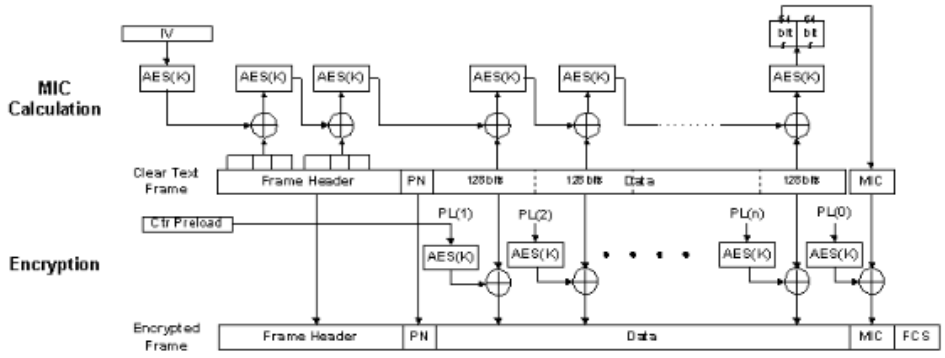

Figura. 2.19. Encriptación CCMP

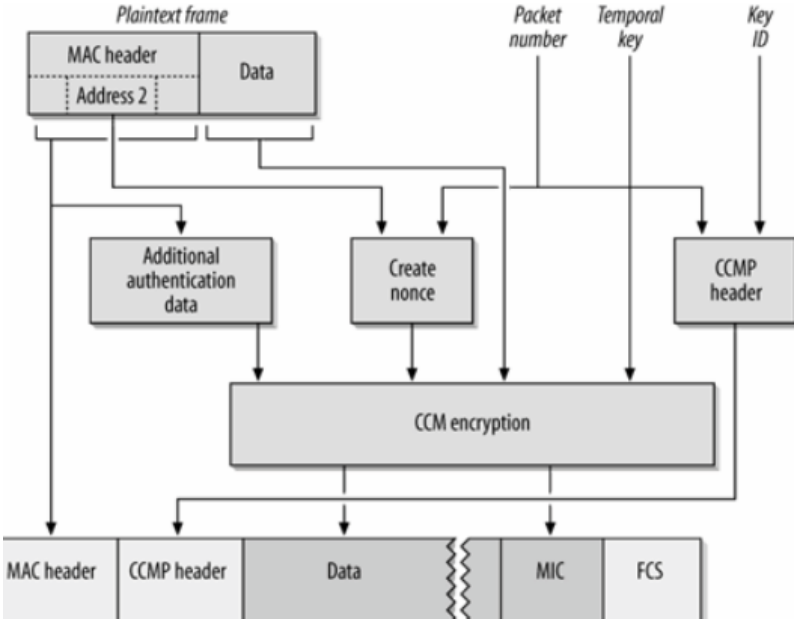

Figura. 2.20. Procesamiento de datos CCMP

CBC Encadenamiento por Cifrado de Bloques

CBC se basa en que a cada bloque de texto plano se le aplica la operación XOR con el bloque cifrado anterior antes de ser cifrado. De esta forma, cada bloque de texto cifrado depende de todo el texto en claro procesado hasta este punto. Para hacer cada mensaje único se utiliza asimismo un vector de inicialización.

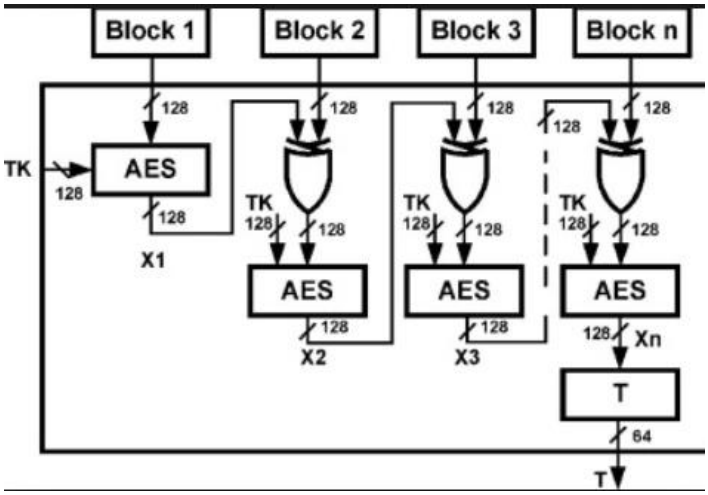

Figura. 2.21. Encadenamiento CBC

CBC-MAC

CBC-MAC transforma un algoritmo de cifrado con CBC en una función MAC. Al aplicar CBC al mensaje y tomar el último bloque se obtiene la etiqueta MAC. Es de vital importancia que la clave utilizada en la obtención del MAC sea distinta a la clave utilizada para cifrar el mensaje, ya que si no sucede esto el MAC sería igual al último bloque del mensaje y podrían debilitarse tanto el cifrado como la autenticación.

2.1.2 Modos de operación 802.11

La arquitectura para este tipo de redes WLAN 802.11 permite dos tipos de operaciones:

IBSS Conjunto de Servicios Básicos Independientes-*Independent Basic Service Set*

A este tipo de redes se lo conoce como Ad-Hoc, en este tipo de arquitectura los dispositivos se interconectan entre cada uno dinámicamente sin la necesidad de un AP, de esta forma cada dispositivo funciona como enrutador. Los dispositivos deben estar en el mismo rango de direccionamiento para establecer la comunicación.

El IBSS al establecer una red temporal permite a los usuarios que estén en la misma conexión y cobertura intercambiar datos. Para ello la red se identifica a través de un SSID. En IBSS es una red inalámbrica restringida ya que la red Ad-Hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra.

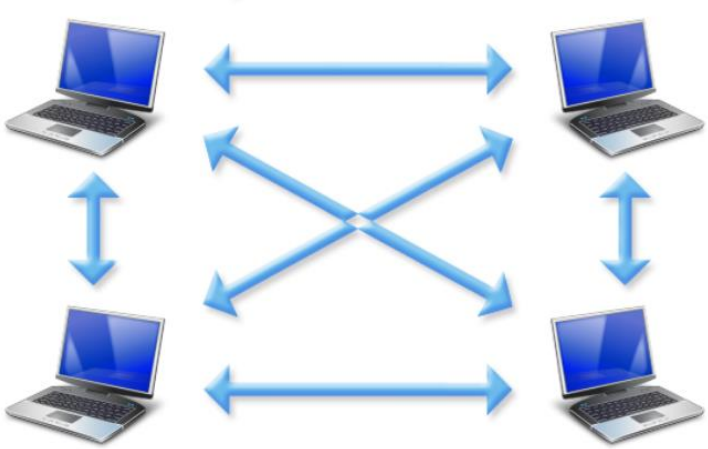

Figura. 2.22. IBSS Conjunto de Servicios Básicos Independientes

BSS Conjunto de Servicios Básicos - Basic Service Set

Esta arquitectura también se la conoce como Infraestructura en la cual los dispositivos no tienen la capacidad de comunicación directamente entre ellos y se hace necesaria la integración de un punto de acceso, éste tendrá como funciones principales gestionar esa información y enrutarla.

El AP administra las comunicaciones entre los diferentes dispositivos, ya sea en su área de cobertura inalámbrica o BBS, o a través de la red de distribución o DS (*Distribution Service*), que por lo general es una red Ethernet. El AP tiene las características de puente entre la red cableada y la inalámbrica. Al ver la necesidad de ampliar las BSS's se genera un nuevo grupo llamado ESS (*Extended Service Set*).

El ESS permite a los diferentes usuarios o dispositivos conectarse de un BSS a los diferentes creados en la red sin necesidad de perder la conexión.

Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 48 bits, el BSSID corresponde al punto de acceso de la dirección MAC.

Un ESS se identifica a través de un ESSID (identificador del conjunto de servicio extendido), es un identificador de 32 caracteres en formato ASCII y se traduce como su nombre en la red. Generalmente se lo conoce como SSID, muestra el nombre de la red y es la primera medida de seguridad ya que una estación debe saber el SSID para conectarse a la red extendida.

Existen diferentes tipos de conexión para esta arquitectura, pueden ser:

Estrella: Conexión típica de WLAN, usada por un *hotspot*, puede ser en aeropuertos o telecentros, topología usada por un WISP (*Wireless Internet Service Provider*).

Tabla. 2.1. Configuración típica Estrella

Configuración	**Punto de acceso/Gateway**	**Nodo**
Modo	Infraestructura	Infraestructura
SSID	Defina MI_SSID	MI_SSID
Canal	Defina el canal x	Descubre el canal
Dirección IP	Normalmente tiene un servidor DHCP	Toma la IP que se le asigna por DHCP

PtP Punto a Punto: Dicha topología se puede establecer en modo Ad- Hoc e Infraestructura, es una conexión simple entre dos dispositivos, son parte de una topología tipo estrella.

Figura. 2.23. Topología PtP

Tabla. 2.2. Configuración típica PtP

Configuración	**Nodo 1**	**Nodo 2**
Modo	Cualquiera	Cualquiera
SSID	MI_SSID	MI_SSID
Canal	Cualquiera	Cualquiera
Dirección IP	Normalmente Fija	Normalmente Fija
Dirección MAC	Podría referirse a la MAC de otro nodo	Podría referirse a la MAC de otro nodo

Repetidores: Su uso se da cuando la conexión hacia otro punto se encuentra obstruida por algún tipo de obstáculo, la configuración de este dispositivo es variable ya que depende del hardware y software.

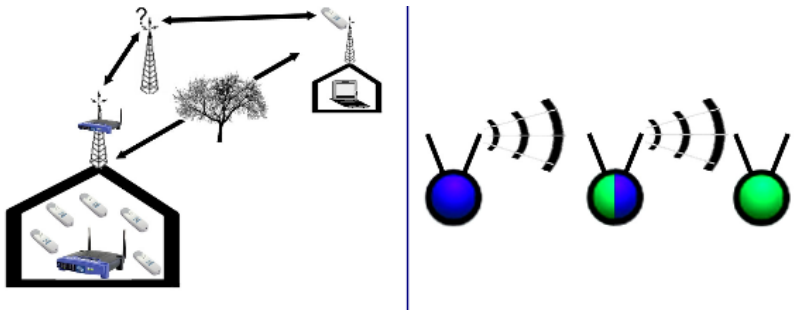

Figura. 2.24. Infraestructura con repetidores

Malla: Su uso se hace obvio en ambientes donde implementar una infraestructura central no es posible, se la encuentra en redes municipales, campus

universitarios, etc. No es útil en este tipo de topología parámetros dinámicos, las conexiones se las realizan entre algunos nodos y no entre todos.

Tabla. 2.3. Configuración típica Malla

Configuración	**Nodo 1**	**Nodo 2**
Modo	ad hoc	ad hoc
SSID	MI_SSID	MI_SSID
Canal	Canal x	Canal x
Dirección IP	Normalmente estática y definida manualmente	Normalmente estática y definida manualmente
Dirección MAC	Podría referirse a la MAC de otro nodo	Podría referirse a la MAC de otro nodo

2.1.3 Tramas 802.11

Se definen varios tipos de tramas para el estándar 802.11, se las clasifica dependiendo de la función que desempeñan. Se tiene:

- Tramas de datos.
- Tramas de gestión.
- Tramas de control.

2.1.3.1 Tramas de gestión

Las tramas 802.11 de gestión son las que permiten mantener comunicaciones a las estaciones inalámbricas y tenemos distintos tipos:

Trama de autenticación

Para establece la comunicación con estas tramas depende del sistema de autenticación que use el punto de acceso, si es abierto o con clave compartida.

- Sistemas abiertos: el suplicante la trama de autenticación y el punto de acceso responde con otra trama de autenticación aceptando o rechazando la conexión.

- Clave compartida: se comprueba que la estación disponga de la llave correcta, se tienen dos tramas de autenticación en el diálogo, una que envía el punto de acceso con un texto para que lo cifre la estación con su clave y otra de respuesta de la estación cliente con el desafío cifrado.

Trama de des autenticación

Esta trama es enviada cuando se desea terminar la comunicación.

Trama de solicitud de asociación

Esta trama inicia el proceso de asociación, el suplicante es quien inicia la comunicación enviado al punto de acceso una trama de solicitud de asociación y el punto de acceso establece un ID de asociación para identificar al cliente y le reserva memoria.

Trama de respuesta de asociación

Los puntos de acceso utilizan esta trama para responder una solicitud de asociación, mediante la cual se acepta o rechaza la asociación. Si se acepta la asociación la trama también incluye el ID de asociación y las tasas de transferencia admitidas.

Trama de solicitud de re-asociación

Similar a la trama de asociación, se la envía cuando existe desplazamiento de un suplicante hacia otro punto de acceso, el cliente le envía una trama de re asociación.

Trama de respuesta de re-asociación

La trama de respuesta de re asociación es similar a la trama de respuesta de asociación, se asocia con un nuevo punto de acceso.

Trama de des-asociación

La trama permite al punto de acceso liberar los recursos que tiene asignado a la estación durante el proceso de asociación.

Trama *beacon*

El AP envía estas tramas con frecuencia difundir la información de la red, SSID, etc. a las estaciones clientes, se obtiene información de diferentes puntos de acceso disponibles. Estas tramas contienen información para identificar las características de la red y poder conectar con el punto de acceso deseado.

Trama de solicitud de prueba

Se la utiliza para obtener información de otra estación.

Trama de respuesta de prueba

Esta trama es la respuesta de una estación a una solicitud de prueba.

2.1.3.2 Tramas de Control

Las tramas 802.11 de control se utilizan para colaborar en la entrega de tramas de datos entre estaciones.

Trama *Request to Send* (RTS)

Reduce colisiones de estaciones asociadas a un punto de acceso pero a la vez fuera de rango de cobertura, esta trama inicia la comunicación de transmisión de una trama.

Trama *Clear to Send* (CTS)

Las estaciones usan estas tramas para responder a una trama RTS y dejar el canal libre de transmisiones, tienen un valor de tiempo durante el cual, ningún dispositivo transmite hasta transmitir esta trama.

Tramas *Acknowledgement* (ACK)

Tramas ACK confirman la recepción de una trama. En caso de no llegar la trama ACK el emisor vuelve a enviar la trama de datos.

2.1.3.3 Tramas de datos

Evidentemente existen tramas de datos que son las encargadas de transportar la información de las capas superiores.

2.1.4 Formato de paquetes MAC

Con respecto al modelo OSI existen tres especificaciones orientadas a la interconexión, la capa PHY, subcapa MAC y subcapa LLC (*Logical Link Control*).

- PHY: contiene el conjunto de reglas que establece MAC.
- Subacapa MAC: establece como acceder al medio y envío de datos enviar los datos
- Subcapa LLC: encapsula la información del protocolo 802.11para el manejo de los protocolos superiores.

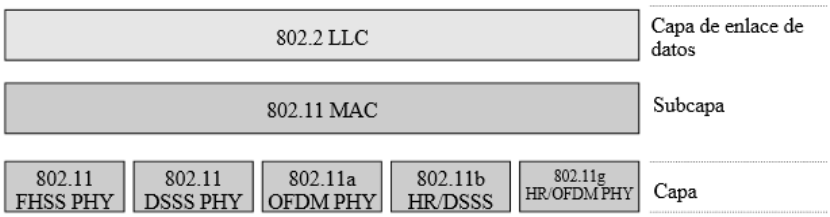

Figura. 2.25. Relación con el modelo OSI, 802.11

Los paquetes MAC consisten de un encabezado MAC, datos y un FCS (*Frame Check Sequence*), en el encabezado MAC se encuentra información de:

- Manejo de la fragmentación.
- Proceso de transmisión.
- Mecanismo de encriptación.
- Datos de transporte del paquete.

No es un encabezado de longitud fija ya que depende del paquete que se esté transmitiendo, por esto los campos Dirección 2, 3 y 4, y el control de secuencia, pueden estar o no presentes. En el FCS se guarda un CRC de 32 bits que permite verificar la integridad del paquete.

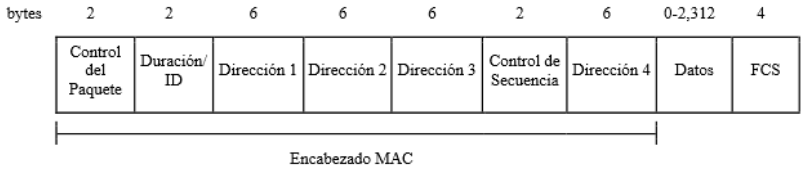

Figura. 2.26. Formato de paquetes MAC

2.1.4.1 Control del Paquete

Este campo contiene 2 bytes y a su vez contienen los subcampos de:

- Versión del Protocolo: indica que versión de 802.11 MAC, el valor del campo es 0 ya que no existe otra versión.
- Tipo y Subtipo: identifican que paquete se usa, los valores de este campo depende del paquete que se trasmita.
- Para DS y Desde DS: estos valores informan si un paquete está o no dirigido para un DS (*Distribution System*) y determinan que campos de direcciones aparecen en los paquetes de datos.

- Más Fragmentos: indica la existencia de fragmentos subsecuentes de un paquete de datos, 1=si, 0= otro caso.

- Retransmisión: indica la transmisión de un paquete, 1=se transmitió; esto para no retransmitir paquetes.

- Administración de Energía: indica el ingreso a un modo de ahorro de energía por parte de los dispositivos móviles, 1=ahorro de energía.

- Más Datos: indican a los dispositivos sin actividad que existen paquetes para estos, se envía un paquete Ps-Poll al AP para la retransmisión de los paquetes.

- WEP: cuando el valor del campo es igual a 1, indica que los datos del paquete han sido encriptados, cambiando de esta manera la estructura del paquete

- Orden: indica la necesidad de un orden estricto de paquetes para la transmisión, cuando esto se necesita el valor del campo es igual a 1.

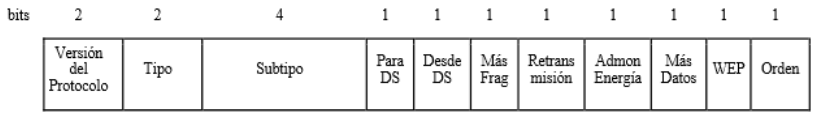

Figura. 2.27. Control del paquete

Valor del Subtipo	Nombre del Subtipo
Paquetes de Administración (Tipo=00)	
0000	Petición de asociación
0001	Respuesta de asociación
0010	Petición de reasociación
0011	Respuesta de reasociación
0100	Petición de sondeo
0101	Respuesta de sondeo
1000	Beacon
1001	ATIM (*Announcement Traffic Indication Message*, Mensaje de indicación de anuncio de tráfico)
1010	Deasociación
1011	Autenticación
1100	Deautenticación
Paquetes de Control (Tipo=01)	
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Reconocimiento (ACK)
1110	Contention-Free (CF)- End
1111	CF-End+CF-Ack
Valor del Subtipo	**Nombre del Subtipo**
Paquetes de Datos (Tipo=10)	
0000	Datos
0001	Datos+CF+Ack
0010	Datos+CF-Poll
0011	Datos+CF-Ack+CF-Poll
0100	Datos nulos (no existen datos transmitidos)
0101	CF-Ack (no existen datos transmitidos)
0110	CF-Poll (no existen datos transmitidos)
0111	Datos+CF-Ack+CF-Poll

Figura. 2.28. Identificadores de los campos Tipo y Subtipo

	Para DS = 0	Para DS = 1
Desde DS = 0	Todos los paquetes de Administración y Control, y los paquetes de Datos dentro de una red Ad-hoc	Paquetes de Datos entrando al DS
Desde DS = 1	Paquetes de Datos saliendo desde el DS	Paquetes de datos distribuidos desde un AP a otro en diferentes DSs (WDS[11]) (*Bridge*)

Figura. 2.29. Interpretaciones de los campos Para DS y Desde DS

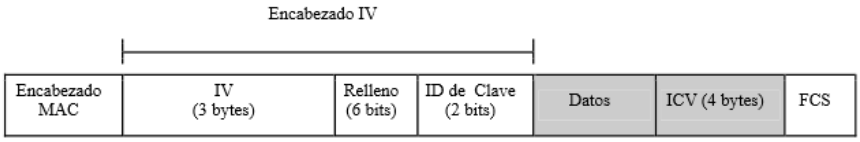

Figura. 2.30. Extensiones WEP del paquete

2.1.4.2 Duración/ID

Es un campo de longitud de 16 bits, los dispositivos inalámbricos monitorean los encabezados de todos los paquetes recibidos y por consiguiente deben actualizar el Vector de Asignación de Red NAV, cuando el bit 15 del campo Duración/ID es 0, el valor de este campo indica la cantidad de tiempo μseg con que se debe actualizar el NAV.

Para paquetes transmitidos durante los Períodos de Contención Libre CFP, el valor de este campo es interpretado como un NAV constante de 32,768 μseg.

Para los paquetes PS-Poll, del campo Duración/ID se obtiene el Identificador de Asociación AID que indica el BSS al cual los dispositivos móviles pertenecen.

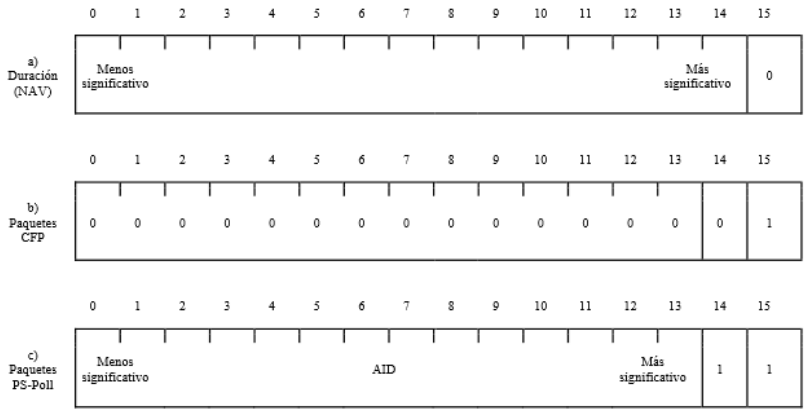

Figura. 2.31. Campo Duración/ID

2.1.4.3 Direcciones

Existen cuatro campos de direcciones, dichas direcciones están formadas de 48 bits y diseñadas para dispositivos que integran una red.

DA *Destination Address*: identificador de 48 bits que corresponde al dispositivo receptor final, el cual manejará el paquete para el procesamiento de protocolos de las capas más altas.

SA Destination Address: identificador de 48 bits que identifica al dispositivo que ha creado el paquete.

RA *Receiver Address:* dirección de 48 bits que indica que dispositivo inalámbrico procesará el paquete. Si se trata de una estación inalámbrica, entonces RA es el DA. En caso de que el paquete vaya dirigido a un dispositivo conectado en una red Ethernet a través de un AP, RA contendrá la dirección MAC del AP.

TA *Transmitter Address:* dirección de 48 bits que identifica el dispositivo inalámbrico que transmite el paquete dentro del medio inalámbrico.

BSSID *Basic Service Set ID*: dirección MAC que identifica la red inalámbrica a la cual un dispositivo ha sido asignado, para las redes con infraestructura, el BSSID es la dirección MAC perteneciente al AP.

Ya que el uso de los campos Dirección dependen sobre el tipo y subtipo del paquete, es común que en la mayoría de los paquetes se utilicen tres campos para el DA, SA y BSSID. Sin embargo, para los paquetes de tipo datos, el uso de los campos Dirección dependen de la forma en que la red se encuentre diseñada.

Función	Para DS	Desde DS	Dirección 1 (receptor)	Dirección 2 (transmisor)	Dirección 3	Dirección 4
IBSS	0	0	DA	SA	BSSID	No usado
Para AP (infraestructura)	1	0	BSSID	SA	DA	No usado
Desde AP (infraestructura)	0	1	DA	BSSID	SA	No usado
WDS (puenteo)	1	1	RA	TA	DA	SA

Figura. 2.32. Uso de los Campos Dirección en paquetes

2.1.4.4 Control de Secuencia

Campo de 16 bits que se utiliza en el proceso de desfragmentación y ayuda a eliminar la duplicación de paquetes con los subcampos Número de Fragmento y Número de Secuencia.

Número de Fragmento: se tiene control en el re ensamblaje de los paquetes, colocando un identificador numérico de 4 bits, el cual, adquiere un valor de cero para el primer fragmento y un valor incrementado en uno para los fragmentos sucesivos. Este identificador permanece constante en todas las retransmisiones de los fragmentos.

Número de Secuencia: campo de 12 bits, la asignación de estos valores se basan de acuerdo al funcionamiento de un contador de módulo 4096, en donde al primer paquete se le asigna un Número de Secuencia de 0 y para los paquetes subsecuentes el valor de este subcampo se incrementa en uno. Esto no sucede para las retransmisiones.

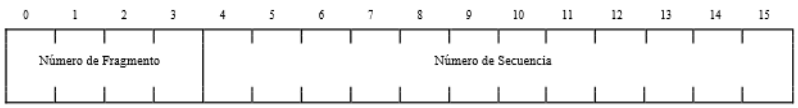

Figura. 2.33. Campo Control de Secuencia

2.1.4.5 Datos

La longitud de este campo es variable y depende del tipo de paquete que se transmita, tiene la información específica de varios de paquetes que pertenecen a protocolos de capas superiores. La capacidad máxima es de 2,304 bytes, incluyendo la información agregada por WEP (Encabezado IV y el campo ICV), y su capacidad mínima es de 0 bytes.

2.1.4.6 FCS

Contiene un Código de Redundancia Cíclica CRC de 32 bits con el cual se puede verificar la integridad del paquete. El CRC se lo puede calcular con el encabezado MAC y campo Datos, bajo redes donde se implemente 802.3 además del 802.11, el FCS debe ser recalculado ya que los encabezados MAC son diferentes en ambas tecnologías.

Con el valor del FCS los receptores verifican si un paquete fue alterado durante su transmisión comparándolo con el CRC que estos han calculado. Si el CRC coincide con el del paquete, se debe enviar un paquete de reconocimiento positivo al dispositivo transmisor, caso contrario, el tiempo de espera terminará y por lo tanto el dispositivo transmisor deberá retransmitir el paquete. En 802.11 no existen los reconocimientos negativos.

2.1.5 Ejemplo de Análisis de paquetes 802.11

Se detalla el contenido del paquete que se muestra en la figura. El paquete capturado con aplicación externa.

Para el análisis, el paquete se dividirá en:

- Encabezado 802.11 MAC.
- Encabezado 802.11 LLC.

- Encabezados siguientes.

- Datos.

Encabezado 802.11 MAC

El encabezado 802.11 está conformado por 24 bytes, cuenta con 3 direcciones MAC. Se procede con la descripción byte a byte.

No byte (Hexadecimal)	Contenido del paquete en bytes (Hexadecimal)															
0000	08	02	00	00	ff	ff	ff	ff	ff	ff	00	11	09	23	04	f3
0010	00	07	E9	d3	89	77	40	f3	aa	aa	03	00	00	00	08	00
0020	45	00	00	4e	46	1b	00	00	80	11	72	1a	C0	a8	00	1a
0030	c0	a8	00	ff	00	89	00	89	00	3a	98	2e	80	57	01	10
0040	00	01	00	00	00	00	00	00	20	46	44	45	46	46	43	46
0050	47	45	4a	45	45	45	50	46	43	43	41	43	41	43	41	43
0060	41	43	41	43	41	43	41	41	41	00	00	20	00	01		

Figura. 2.34. Contenido del paquete en bytes

- Los bytes 0 y 1

  Forman al campo Control del Paquete tomándolos de derecha a izquierda (0x0208). En este campo se incluye información para el procesamiento del paquete. En este caso, en el byte 0 (0x08), los primeros 2 bits indican que se está utilizando la versión 0 del protocolo 802.11 y los siguientes 6 bits indican que el paquete transporta datos de protocolos de niveles superiores. En el byte 1 (0x02), los primeros 2 bits indican que el paquete está saliendo de un DS *Distribution System* y los siguientes bits indican, respectivamente, que el paquete: puede no ser un fragmento o puede ser el último fragmento, no ha sido retransmitido, la estación que lo transmitió está activa, la estación que lo transmitió no tiene paquetes almacenados, no se le ha aplicado el mecanismo de encriptación WEP y no debe ser procesado en un orden estricto.

- Los bytes 2 y 3

  Estos bytes forman al campo Duración/ID tomándolos de derecha a izquierda (0x0000). Este campo determina que el medio permanecerá ocupado 0 μseg en la transmisión de este paquete.

- Los bytes del 4 al 9

  Estos bytes representan la dirección MAC destino del paquete y se toman de izquierda a derecha (ff:ff:ff:ff:ff:ff). Por su valor el paquete va dirigido a todas las estaciones de la red (*Broadcast*).

- Los bytes del 10 al 15

  Estos bytes representan el BSSID de la red al que va dirigido el paquete y se toman de izquierda a derecha (00:11:09:23:04:f3). Como se puede apreciar el BSSID es una dirección MAC.

- Los bytes del 16 al 21

  Estos bytes representan la dirección MAC origen del paquete y se toman de izquierda a derecha (00:07:e9:d3:89:77).

- Los bytes 22 y 23

  Estos bytes forman al campo de Control de Secuencia tomándolos de derecha a izquierda (0xf340). Este campo es usado en el proceso de desfragmentación y para descartar la duplicación de paquetes.

  Los primeros 4 bits del campo (subcampo Número de Fragmento) indican que el paquete es el fragmento número 0, por lo que se puede concluir con la ayuda del campo Control del Paquete (Ver los bytes 0 y 1), que la información del paquete no ha sido fragmentada. Los 12 bits restantes del

campo Control de Secuencia (subcampo Número de Secuencia) establecen que el paquete tiene un número de secuencia igual a 3892, lo que significa que los paquetes subsecuentes tendrán un número de secuencia mayor (3893, 3894, etc.).

Encabezado 802.2 LLC

De acuerdo al análisis del encabezado anterior se puede argumentar que el paquete contiene datos de protocolos de capas superiores a 802.11 (Ver los bytes 0 y 1). En este caso, por la estructura de los datos se deduce que el siguiente encabezado pertenece al protocolo 802.2 LLC. Este encabezado es usado por 802.11 para transportar protocolos de la capa de red. Para conseguirlo, 802.2 hace uso del método SNAP Protocolo de Acceso a la Subred, insertando un encabezado SNAP, en el cual se almacenan los parámetros para el encapsulado de los datos pertenecientes a la subcapa LLC. El encabezado SNAP se compone de los campos DSAP Punto de Acceso del Servicio Destino, SSAP Punto de Acceso del Servicio Origen, Control, Código Organizacional y Tipo. Los bytes del 24 al 31 representan al encabezado 802.2 LLC (sección cerrada con línea punteada).

- Los bytes 24 y 25

  Estos bytes forman a los campos DSAP y SSAP respectivamente. El valor 0xaa es siempre usado para ambos campos.

- El byte 26

  Este byte forma al campo Control. Este campo, con el valor de 0x03, denota a los datos siguientes al encabezado SNAP como información no enumerada. La información no enumerada indica que las transmisiones no son orientadas a conexión y que los datos no necesitan ser secuenciados o reconocidos.

- Los bytes del 27 al 29

  El campo Código Organizacional está formado por estos bytes y es usado para determinar cómo serán interpretados los bytes siguientes al encabezado SNAP. La información IP es encapsulada por 802.2 LLC utilizando el método marcado en RFC 1042, el cuál especifica el uso del OUI Identificador Organizacionalmente Único 0x00-00-00. En este caso el campo Código Organizacional contiene este OUI 13.

- Los bytes 30 y 31

  Estos bytes forman al campo Tipo, el cual es usado para indicar el protocolo de red que se está transportando en el paquete. Este campo es el mismo que los paquetes Ethernet incluyen en sus encabezados. En este caso, el campo Tipo indica que el protocolo IP (0x0800) está incluido en el paquete. En redes IP, este campo puede adquirir también el valor de 0x0806 para especificar el uso del protocolo ARP.

Encabezados siguientes

Estos encabezados constan del encabezado IP (sección sombreada) seguido por el encabezado UDP (sección cerrada con línea delgada) como se muestra en la figura 2.34. El análisis de estos encabezados puede hacerse de forma análoga a los encabezados anteriores, aunque en este trabajo no hayan sido considerados. Sólo por brindar información diremos que los últimos 8 bytes del encabezado IP (c0 a8 00 1a c0 a8 00 ff) representan las direcciones IP origen (192.168.0.26) y destino (192.168.0.255) respectivamente, y que los primeros 4 bytes del encabezado UDP (00 89 00 89) representan los puertos origen 137 y destino 137 que en este caso se trata de los puertos netbios_ns.

Datos

Después del encabezado UDP vienen los datos del paquete. Estos constan de 50 de los 1,500 bytes (tomando en cuenta los encabezados 802.2 LLC, IP y

UDP) que pueden ser transmitidos por el protocolo 802.11 sobre redes IP (RFC 1191) y en los cuales normalmente se incluye información de protocolos o aplicaciones de capas superiores (ej. FTP, HTTP, TELNET, etc.).

Resumen de Análisis de Datos

Tabla. 2.4. Resumen de análisis de paquete

ENCABEZADO 802.11			
No. de Byte	**Campo (s)**	**Valor (es)**	**Significado**
0 y 1	Control del Paquete	0x0208	Paquete de datos, está saliendo de un DS, no ha sido fragmentado ni retransmitido y no está encriptado entre otras cosas.
2 y 3	Duración/ID	0x0000	NAV igual a 0 µseg
4 al 9	Dirección MAC destino	0xffffffffffff	ff:ff:ff:ff:ff:ff
10 al 15	BSSID	0x0011092304f3	00:11:09:23:04:f3
16 al 21	Dirección MAC origen	0x0007e9d38977	00:07:e9:d3:89:77
22 y 23	Control de Secuencia	0xf340	Número de secuencia igual a 3892
ENCABEZADO LLC			
24	DSAP	0xaa	
25	SSAP	0xaa	
26	Control	0x03	Información IP no enumerada
27 al 29	Código Organizacional	0x000000	Encapsulamiento por RFC 1042
30 y 31	Tipo	0x0800	Paquete IP

2.2 Servicio AAA

2.2.1 Qué es un servicio AAA?

El estándar AAA bajo las notas del RFC 2903 establece la arquitectura para configurar un sistema de seguridad en la red, se indican tres funciones principales que son:

- Autenticación.
- Autorización.
- Auditoria.

El servicio AAA está en la capacidad de establecer políticas de autenticación para los solicitantes, responder de manera directa y sin errores a las peticiones de autorización de los usuarios, y por último recolectar datos que faciliten realizar una auditoría sobre los recursos a los que se ha tenido acceso en la infraestructura de red.

A continuación se definen los tres procesos del modelamiento AAA:

Autenticación

Proceso de identificar a los usuarios, con el nombre de usuario y contraseña, desafío y respuesta, soporte de mensajería, y, según el protocolo de seguridad que seleccione, puede ofrecer cifrado.

Es el método que permite identificar a un suplicante antes de conceder acceso a la red y los servicios que esta contiene. Configurar la autenticación AAA mediante la definición de una lista llamada métodos de autenticación, y luego aplicando esa lista a varias interfaces. En la lista de métodos se definen los tipos de autenticación a realizar y la secuencia en la que se llevará a cabo, esto debe ser aplicado a una interfaz específica antes de que cualquiera de los métodos de

autenticación definidos se utilicen. La única excepción es la lista método por defecto (que se denomina "default").

La lista método por defecto se aplica automáticamente a todas las interfaces si ninguna lista de otro método está definida. Una lista de método definida reemplaza automáticamente la lista de método por defecto.

Todos los métodos de autenticación, excepto local, line de contraseña y habilitación de la autenticación, deben ser definidas a través de AAA.

La autenticación se puede realizar por diversos esquemas:

- **Secuencia de agente:** el servidor AAA permanece como delegado entre el equipamiento que presta el NAS y el usuario final. El usuario contacta inicialmente con el servidor AAA, quien autoriza su petición y notifica al equipamiento de su decisión para que se le preste el servicio al usuario. El equipamiento del servicio notifica al servidor AAA cuando ha cumplido su petición, y el mismo servidor AAA notifica en última instancia al usuario.

- **Secuencia de tiro o *pull*:** servicio dial tradicional de marcación telefónica. El usuario realiza la petición directamente al NAS y éste comprueba con el servidor AAA si debe proporcionar acceso.

- **Secuencia de empuje o *push*:** el usuario pide una certificación al servidor AAA, la cual deberá presentar más tarde al equipamiento que presta el servicio para garantizar su identidad y acceso al mismo.

Autorización

No es más que la asignación de recursos para tener un control de acceso definido a cada usuario después de la autenticación.

En esta fase del modelamiento, mediante un grupo de reglas se establece lo que el usuario está habilitado a usar o acceder en la red interna o externa. Estas

reglas son comparadas con la información que contiene la base de datos que se encuentra en el servidor AAA para denegar o permitir la capacidad del usuario. En algunos casos la base de datos se almacena en un servidor remoto de seguridad, RADIUS o TACACS+. Estos servidores o los responsables de autorizar a los usuarios los derechos específicos que cada uno posee con la asociación de las reglas antes definidas.

Todos los métodos de autorización deben ser definidos a través de AAA. Así como en la autenticación, configurar AAA Autorización es definida por una lista llamada métodos de autorización, y luego aplicando esa lista a varias interfaces.

Registro o Contabilización

Es la última fase del modelamiento AAA ya que recolecta y envía la información al servidor de seguridad, el cual valida:

- Nombres de usuarios.
- Tiempo de inicio y final.
- Comandos ejecutados (como PPP).
- Cantidad de paquetes enviados.
- Número de *bytes*.

Gracias a esta fase se realiza el seguimiento de todos quienes tengan acceso a los servicios, así como el consumo de recursos que cada usuario genera. Una vez se detecta actividad, el acceso a la red del servidor informa la actividad del usuario al servidor de seguridad en forma de los registros contables, estos se guardan en un servidor de control de acceso.

Estos métodos de registro son definidos a través de AAA, al igual que con la autenticación y autorización, se configura el registro mediante la definición de una lista llamada métodos de registro, y luego la aplicación de esa lista a varios interfaces.

AAA provee los siguientes beneficios:

- Incrementación de flexibilidad y control de configuración de acceso.
- Escalabilidad.
- Métodos de autorización estandarizados, como RADIUS, TACACS+ o Kerberos.
- Múltiples sistemas de *backup*.

AAA permite que el administrador de la red pueda configurar dinámicamente el tipo de autenticación y autorización, por usuario o por servicio base (IP, IPX, o VPDN).

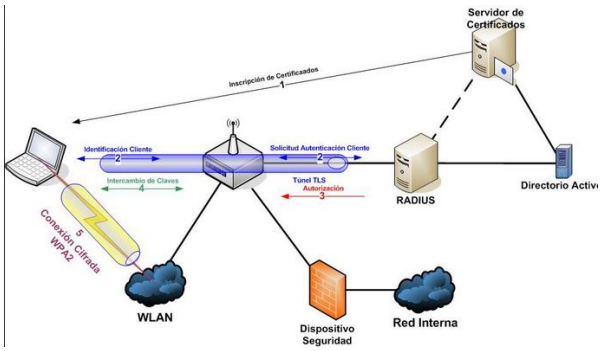

Figura. 2.35. Establecimiento de la conexión

Los protocolos AAA más utilizados para configurar el acceso son:

- Radius (Remote Authentication Dial-in User Service).
- TACACS+ (Terminal Access Controller Access Control System Plus).

2.2.2 RADIUS *Remote Authentication Dial-in User Service*

RADIUS es una implementación concreta del modelamiento AAA, se encuentra definido en los RFC 2865 para la autentificación y autorización, y RFC 2866 para el registro (*accounting*).

Los mensajes de intercambio de RADIUS se envían como mensajes de datagramas UDP. El puerto UDP 1812 se utiliza para los mensajes de autenticación y el 1813 para los mensajes de administración. La carga UDP de un paquete RADIUS sólo incluye un mensaje RADIUS.

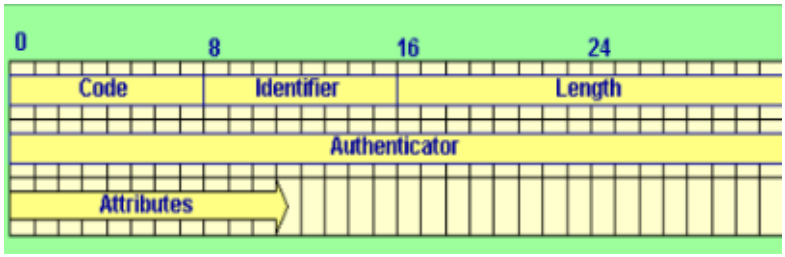

Figura. 2.36. Formato de mensaje RADIUS

Los campos en un paquete RADIUS son:

- *Code* (Código), octeto que contiene el tipo de paquete.
- *Identifier* (Identificador), octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud adecuada.
- Length, longitud del paquete de 2 octetos.
- *Authenticator* (Verificador), es un valor que sirve para autenticar la respuesta del servidor RADIUS. Es usado en el algoritmo de encubrimiento de contraseña.
- *Attributes* (Atributos), se almacenan atributos variables. Los únicos atributos obligatorios son el usuario y contraseña.

Provee varios servicios comunes personalizables que utilizan un esquema de autorización de secuencia *pull.*

Debilidades

- RAIUS utiliza MD5 como algoritmo de dispersión para almacenar contraseñas, lo cual no es seguro
- La escalabilidad presenta problemas.
- Al basarse en UDP y no estar orientado a la conexión, no tiene control sobre el uso de los servicios cuando ya ha sido autenticado.
- Es un protocolo salto a salto, las cadenas de autenticación son largas e implican diversos servidores de distintas agrupaciones. Por lo que el modelo salto a salto es inseguro.

Este protocolo utiliza identificadores llamados *realms* o dominios para realizar una discriminación de cada usuario y saber en todo momento quién debe autenticarlos. Los dominios se presentan como sufijos o prefijos ubicándose junto al nombre de usuario, separados por caracteres como barras o arrobas. Por tal motivo un servidor RADIUS pronostica patrones en los nombres de los usuarios para autenticar a un usuario cuando lo amerite.

2.2.3 Integración y funcionabilidad de un servidor AAA

1. El suplicante inicia solicitando conexión de red. Se inicia el proceso de autenticación enviando un mensaje EAPoL de inicio hacia el equipo de acceso AP.
2. El autenticador envía un mensaje de solicitud de identidad al usuario.
3. El usuario envía un EAP de identidad al autenticador.
4. La trama *EAP response identity* se encapsula en un mensaje RADIUS y el autenticador envía un mensaje de petición de acceso al servidor RADIUS.

5. El servidor RADIUS inicia la negociación del método EAP que se utilizará para el establecimiento del canal seguro enviando una trama RADIUS *Access-challenge*.

6. El autenticador envía al usuario un EAP con petición de establecimiento de canal con EAP de tipo PEAP.

7. El usuario negocia el método de la conexión y envía al autenticador un EAP de respuesta con el saludo para establecimiento del canal TLS (*client hello*).

8. El autenticador encapsula el mensaje EAP-*Response* en un mensaje RADIUS-*Request* y lo envía al servidor.

9. El servidor verifica el mensaje enviado por el usuario y le responde con su certificado en un mensaje RADIUS-*Challenge*. El mensaje contiene un *server hello*+ *server certificate* + *server hello done*.

    a. *Server hello*.- Saludo del servidor en respuesta de un *client hello*.
    b. *Server Certificate*.- Certificado del servidor).

10. El autenticador recibe el mensaje RADIUS y envía el certificado del servidor al usuario en un EAP-*Request* TLS de credencial del usuario.

11. El usuario responde un mensaje EAP intercambiando la contraseña en el canal cifrado. El mensaje EAP-*Response* TLS contiene el *client key Exchange*, *change cipher spec* y *encrypted handshake message*.

12. La trama EAP-*Response* TLS se encapsula en un mensaje RADIUS-*Request* y se envía al servidor RADIUS, el mensaje llega encriptado con la contraseña del usuario y es verificada en la base de datos LDAP.

13. El servidor responde:

a. Si la contraseña del usuario es correcta el servidor responde con un mensaje RADIUS-*Challange* para finalizar el establecimiento del canal TLS.

b. Si las credenciales no son correctas rechaza la conexión (RADIUS-*Reject*) y el puerto del *switch* al que se conecta el usuario se pone en estado *down*.

14. El autenticador recibe un RADIUS-*Challenge* para finalizar de establecer el canal TLS y le envía al usuario un EAP-*Request* de canal cifrado completo.

15. El usuario envía un mensaje EAP-PEAP de respuesta y solicita acceso a la red.

16. La solicitud de acceso a la red es enviara al servidor mediante un mensaje RADIUS-*Request*.

17. El servidor responde con un mensaje de RADIUS-*ACCEPT* hacia el autenticador.

18. El autenticador envía un mensaje EAP-*Succsess* y el usuario ya se encuentra habilitado para usar los recursos de la red.

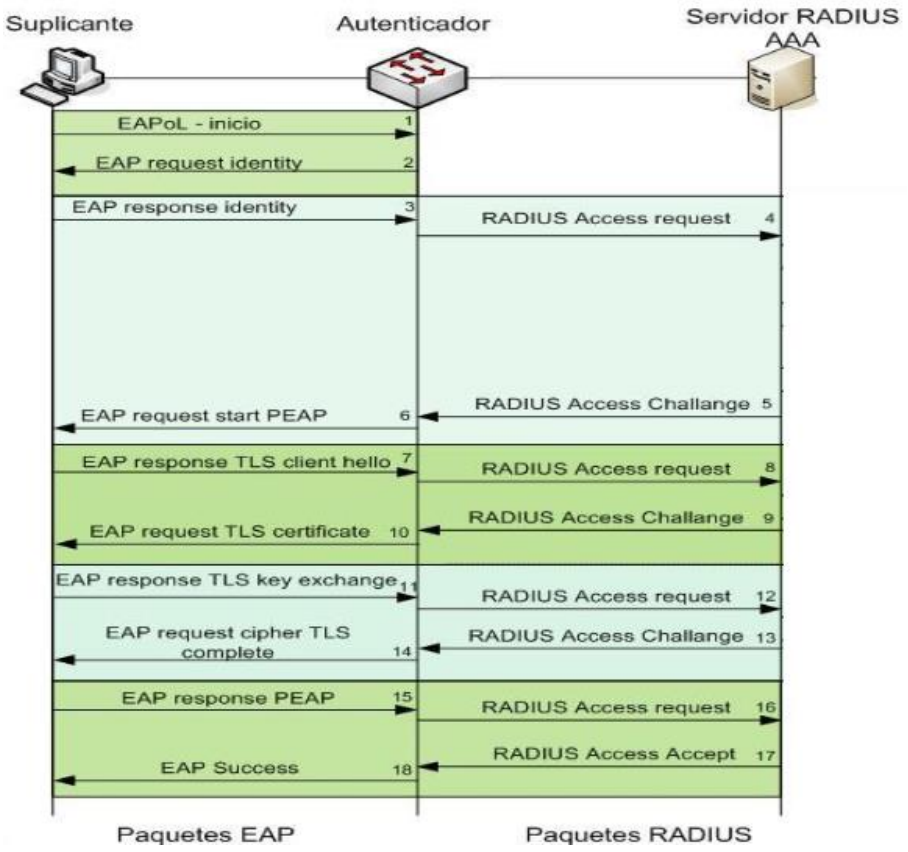

Figura. 2.37. Funcionamiento de Autenticador - AAA RADIUS

CAPÍTULO 3

ANÁLISIS DE SOLUCIONES EN SOFTWARE PARA EL DESARROLLO DE LA SIMULACIÓN

3.1 Análisis comparativo de soluciones en software para desarrollar diferentes topologías con mecanismos de seguridad definidos en el estándar 802.11i

Previo realizar las simulaciones de los mecanismos y protocolos de seguridad del estándar 802.11, 802.1X, 802.11i se evaluará cada una de las soluciones de software que permitan desarrollar la implementación y el análisis de sistemas de comunicación cada vez más complejos.

En dichos procesos, es necesaria una investigación de diferentes sistemas con base en características específicas, ello se logrará con un estudio individual de cada solución. Es necesaria la simulación ya que muchas veces contar con un sistema real para experimentar sobre él, es costoso ó virtualmente imposible por los componentes de cada sistema.

Para realizar estudios específicos se emplean simuladores para diseñar experimentos en base a topologías específicas, con condiciones controladas y brindando la confiabilidad en las conclusiones que arroje un estudio determinado.

Existen dos tipos de métodos para desarrollar diferentes eventos, los cuales son:

- Simuladores de eventos discretos: Esta clase de simulador es particularmente útil para el análisis de sistemas secuenciales o que usen colas, los cuales son muy comunes en el ambiente de las comunicaciones

- Simuladores de tiempo continuo: Funcionan utilizando modelos matemáticos y ecuaciones diferenciales que describen la evolución del sistema de manera continua, es usado cuando el proceso que se desea analizar cambia de manera muy sutil y continua.

A continuación se explican las características, funciones de los simuladores más comunes y sobre los cuales, las características intrínsecas de cada uno permitirán desarrollar las simulaciones propuestas en el proyecto.

A continuación se analizarán los siguientes simuladores:

- OMNET ++.
- GLOMOSIM.
- OPNET MODELER™..
- NCTuns.
- *NETWORK SIMULATOR*.
- Packet Tracer.
- GNS3.
- FLAN (F- *Links And Nodes*).
- KIVA.
- COMNET III™.

OMNET++

Herramienta eficiente, enfocada al área académica y desarrollada para modelar y simular eventos discretos en redes de comunicaciones; recrea eventos discretos por módulos orientados a objetos; puede ser utilizado para modelar el tráfico de información sobre las redes, los protocolos de red, las redes de colas, multiprocesadores y otros sistemas de hardware distribuido; además para validar arquitecturas de hardware y evaluar el rendimiento de sistemas complejos.

Utiliza el lenguaje de programación NED, que se basa en el lenguaje C++; este lenguaje facilita la descripción modular de una red, se construye con módulos jerárquicos mediante el lenguaje NED, dichos módulos pueden contener estructuras complejas de datos y tienen sus propios parámetros usados para personalizar el envío de paquetes a los destinos a través de rutas, compuertas y conexiones. Los módulos de más bajo nivel son llamados “simple modules” y son programados en C++ usando la librería de simulación.

Básicamente, con el lenguaje NED se definen tres módulos: módulos simples, módulos compuestos y de redes; dentro de los cuales se encuentran los componentes y especificaciones de la descripción de una red de comunicaciones. Permite al usuario trabajar gráficamente empleando el editor del lenguaje NED (GNED). Este editor es la interfaz gráfica que permite crear, programar, configurar y simular redes de comunicaciones, sin necesidad de hacerlo utilizando la codificación del lenguaje NED; ya que automáticamente, GNED se encarga de generar el código del lenguaje, de acuerdo al diseño y configuración que realiza el usuario en forma gráfica.

Tabla. 3.1. Ventajas y desventajas de OMNET ++

Ventajas	**Desventajas**
OMNeT++ es gratuito solamente para propósitos académicos, lo que facilita su utilización en universidades y grupos de investigación. Es multiplataforma. Gracias a la programación por módulos, es posible simular procesos paralelos y	Para fines de investigación y desarrollo, es necesario saber programar en lenguaje NED, ya que el trabajo con el editor gráfico, es un poco más rígido. Por ser un software de aplicación en áreas

distribuidos, los cuales pueden utilizar varios mecanismos para comunicarse entre sí.	comerciales y para efectos de investigación y desarrollo, tiene un alto grado de complejidad en su manejo.

OPNET MODELER™

Originalmente fue desarrollado por MIT e introducido al mercado en 1987 como el primer simulador comercial. Esta herramienta se utiliza para el modelado y simulación; está basada en la teoría de redes de colas e incorpora las librerías para facilitar el modelado de las topologías de red. El desarrollo de los modelos se realiza mediante la conexión de diferentes tipos de nodos, utilizando diferentes tipos de enlaces. Mediante OPNET MODELER, se deben especificar tres tipos de modelos.

Tabla. 3.2. Jerarquía de diseño en OPNET

MODELO DE RED	Redes y subredes
MODELO DE NODOS	Nodos y estaciones
MODELO DE PROCESOS	Especifica la funcionalidad de cada nodo.

Tabla. 3.3. Ventajas y desventajas de OPNET

Ventajas	**Desventajas**
El programa incluye las librerías para acceder a un extenso grupo de aplicaciones y protocolos como: HTTP, TCP, IP, OSPF, BGP, EIGRP, RIP, RSVP, *Frame Relay*, FDDI, Ethernet, ATM, LANs, 802.11 (*Wireless*), aplicaciones de voz, MPLS, PNNI, DOCSIS, UMTS, IP *Multicast, Circuit Switch*, MANET, IP Móvil; entre otras.	Es un software propietario, lo cual lo hace costoso para ambientes universitarios.
Tiene interfaces para visualización del modelo en 3D.	Es necesario obtener la licencia para poder utilizar el software, ya que no existen versiones académicas o de prueba.
Los APIs de simulación permiten acceder libremente al código fuente, lo cual facilita la programación de nuevos protocolos de red.	Complicada determinación de los intervalos de confianza.
Las librerías de modelos de red estándar, incluyen dispositivos de red comerciales y genéricos.	El tiempo de aprendizaje es elevado.
Modelos de red jerárquicos.	

Maneja topologías de red complejas con subredes anidadas ilimitadas. Permite mostrar el tráfico por la red a través de una animación, durante y después de la simulación. Los resultados se exhiben mediante gráficos estadísticos.	

NCTuns

NCTUns utiliza una sintaxis sencilla pero muy efectiva para describir la topología, los parámetros y la configuración de una simulación, esta descripción se genera a partir de la interfaz gráfica del usuario. NCTUns fue desarrollado basado en el simualdor NS, de ahí su nombre, solo que incluye una interfaz más amigable para la implementación de los modelos de red que se simulan. Este programa permite la simulación de arquitecturas de redes sencillas, sin embargo, su mayor potencial está en la simulación de redes tan complejas como las redes GPRS, satelitales y ópticas.

El NCTUns también puede ser utilizado como emulador, especialmente para redes móviles e inalámbricas; para dichas aplicaciones provee recursos para manejo y estudio de sistemas de radiofrecuencia y permite obtener mediciones para establecer niveles de calidad de servicio (QoS) de las señales irradiadas. El hecho de que el simulador permita definir obstáculos, trayectorias de movimiento y que los terminales móviles (como celulares GPRS y portátiles) se puedan desplazar siguiendo dicha trayectoria, al mismo tiempo en que se hacen mediciones de atenuación, interferencia y de ancho de banda, dan cuenta de las

sobresalientes características del NCTUns y justifican los diferentes reconocimientos que ha obtenido a nivel mundial. Adicionalmente, permite simular redes ópticas y como si fuera poco, puede usarse fácilmente como un emulador, cuando se desee desarrollar funciones de desempeño de un host real y ver cómo se comportaría bajo diferentes tipos de condiciones de red sin modificar su protocolo interno.

Esto quiere decir que NCTUns tiene la posibilidad de emular un dispositivo de red del mundo real en su entorno gráfico e interconectarlo con dispositivos simulados o virtuales, para intercambiar paquetes. También posee una característica importante, la cual, sumado a lo anteriormente expuesto, hacen de NCTUns uno de los más poderosos simuladores de redes de telecomunicaciones. La arquitectura de sistema abierto, en la cual la GUI y el motor de simulación son elementos separados que utilizan un modelo cliente servidor, permite ejecutar simulaciones remotas, paralelas, distribuidas y concurrentes, lo cual permite entre muchas otras cosas, correr simulaciones simultáneamente en diferentes nodos de una red y cuyos resultados individuales sirven para el análisis de un sistema único.

Esto quiere decir, que un usuario, puede enviar su proyecto de simulación a un servidor remoto que esté ejecutando el motor de simulación, utilizando su propia GUI y además correr múltiples simulaciones concurrentes en diferentes hosts conectados a dicho servidor.

Tabla. 3.4. Ventajas y desventajas de NCTuns

Ventajas	**Desventajas**
Es un software libre, con distribución de código abierto. Utiliza directamente el conjunto de protocolos TCP/IP de Linux, por consiguiente se generan resultados de simulación de alta fidelidad y permite que la configuración y el uso de una red simulada, sea exactamente igual a los usados en redes IP del mundo real. Puede ser utilizado como emulador. Esto permite que un host externo conectado a una red del mundo real, pueda intercambiar paquetes con nodos (por ejemplo: host, enrutadores o estaciones móviles celulares) en una red simulada en NCTUns. Puede utilizar cualquier	Solamente funciona en sistemas Fedora core 3, para otras distribuciones de Linux es necesario hacer pruebas y configuraciones adicionales. Existe muy poca información sobre el funcionamiento y configuración del software. El anterior punto lleva a que sea mayor el tiempo de aprendizaje del simulador. El servicio de soporte proporcionado por los autores del proyecto NCTUns es deficiente y en algunas ocasiones no funciona.

aplicación de UNIX existente en la vida real, como un generador de tráfico, además, puede utilizar las herramientas de configuración y monitoreo de UNIX. Puede simular redes fijas, inalámbricas, redes celulares, redes GPRS y redes ópticas. Puede simular una gran variedad de dispositivos de red, como: *hubs, switches, enrutadores*, estaciones móviles, puntos de acceso de WLANs, teléfonos GPRS, etc, así como obstáculos para las señales inalámbricas, además ofrece alta velocidad de simulación. Simula varios protocolos de redes como: IEEE 802.3, IEEE 802.11, IP, IP Mobile, Diffserv, RIP, OSPF, UDP, TCP, RTP/RTCP, SDP, FTP, etc.	

Netwok Simulator

NS es una herramienta con un amplio rango de uso y que continuamente sirve como base para el desarrollo de otros programas de simulación; además este software soporta una gran cantidad de protocolos de las capas de aplicación y transporte, además de otros utilizados para el enrutamiento de los datos, entre los cuales están: HTTP, FTP CBR, TCP, UDP, RTP, SRM, entre otros; los cuales pueden ser implementados tanto en redes cableadas, como inalámbricas locales o vía satélite; y que son aplicables a grandes redes con topologías complejas y con un gran número de generadores de tráfico. Para visualizar los resultados es necesario instalar el Network Animador (NAM), el cual es una herramienta de interfaz gráfica muy sencilla de utilizar. NS depende de algunos componentes externos como: Tcl/TK, Otcl, TclCL20 que hacen parte del compilador de para Linux, además del xgraph, que es un componente opcional solo para cuando se necesite evaluar series.

Tabla. 3.5. Ventajas y desventajas de Network Simulator

Ventajas	Desventajas

Este programa contiene módulos que cubren un extenso grupo de aplicaciones, protocolos de ruteo, transporte, diferentes tipos de enlaces, estrategias y mecanismos de ruteo; entre otros. Algunos de estos son: http, TcpApp, telnet, CBR (Constat Bit Rate), TCP, RTP, algoritmos de ruteo, enrutamiento jerárquico y enrutamiento manual.	La configuración de las simulaciones a través de código, hace que sea mayor el tiempo de desarrollo. Además también se incrementa el tiempo necesario para el aprendizaje del software.
Por ser uno de las más antiguas herramientas de simulación, el NS se ha convertido en un estándar de su área, esto ha llevado a que sea ampliamente utilizado y a que se encuentren en Internet un gran número de ayudas y proyectos realizados sobre NS.	NS requiere varios componentes adicionales instalados para su correcto funcionamiento.

Packet tracer

Packet Tracer es un simulador que permite realizar el diseño de topologías, la configuración de dispositivos de red, así como la detección y corrección de errores en sistemas de comunicaciones. Ofrece como ventaja adicional el análisis de cada proceso que se ejecuta en el programa de acuerdo a la capa de modelo OSI que interviene en dicho proceso; razón por la cuál es una herramienta de gran ayuda en el estudio y aprendizaje del funcionamiento y configuración de redes de comunicaciones y aplicaciones telemáticas

Tabla. 3.6. Ventajas y desventajas de Packet Tracer

Ventajas	**Desventajas**
El enfoque pedagógico de este simulador, hace que sea una herramienta muy útil como complemento de los fundamentos teóricos sobre redes de comunicaciones. El programa posee una interfaz de usuario muy fácil de manejar, e incluye documentación y tutoriales sobre el manejo del mismo. Permite ver el desarrollo por capas del proceso de transmisión y	Es un software propietario, y por ende se debe pagar una licencia para instalarlo. Solo permite modelar redes en términos de filtrado y retransmisión de paquetes. No permite crear topologías de red que involucren la implementación de tecnologías diferentes a Ethernet; es decir, que con este programa no se

recepción de paquetes de datos de acuerdo con el modelo de referencia OSI. Permite la simulación del protocolo de enrutamiento RIP V2 y la ejecución del protocolo STP y el protocolo SNMP para realizar diagnósticos básicos a las conexiones entre dispositivos del modelo de la red.	pueden implementar simulaciones con tecnologías de red como *Frame Relay*, ATM, XDSL, Satelitales, telefonía celular entre otras. Ya que su enfoque es pedagógico, el programa se considera de fidelidad media para implementarse con fines comerciales.

GNS3

GNS3 es un emulador de plataformas de redes de varios fabricantes, se creó como emulador de enrutadores Cisco 7200 pero a partir de ahí ha crecido tanto el soporte como la comunidad de usuarios. Actualmente se tiene soporte para emulación de varias plataformas de enrutadores Cisco (1700, 2600, 2691, 3600, 3700, 7200), *firewalls* (PIX y ASA), *switches* (*ethernet*, ATM, *Frame Relay*), IDSs, PCs.

La gran ventaja de GNS3 sobre otras aplicaciones es que es un emulador, es decir, ejecuta una máquina virtual en la que se carga un IOS real, por medio de ésta es posible usar cualquier comando que soporte un enrutador real.

Tabla. 3.7. Ventajas y desventajas de GNS3

Ventajas	**Desventajas**
Es un programa *Open Source*. Se puede utilizar en múltiples Sistemas Operativos. Puede Trabajar con la IOS de *routers* reales. Emulacion de muchas plataformas de *routers*. Diseño de alta calidad y topologías de red complejas. Conexión de la red simulada con el mundo real. Paquete de captura con *Wireshark*.	En el área de consola se informa con demasiada asiduidad de fallos al guardar la topología, al borrar un enlace borrar un dispositivo. Con cierta regularidad durante la simulación de topologías el programa parece bloquearse. No permite la emulación de redes inalámbricas.

FLAN (F- *Links And Nodes*)

FLAN es una herramienta de simulación que permite el diseño, la construcción, y la prueba de una red de comunicaciones en un ambiente simulado. El programa hace el análisis de las redes asociando su estructura basada en nodos y enlaces, con bloques simples, por medio de los cuales se puede entender el funcionamiento especialmente de los protocolos de enrutamiento que maneja la capa de red.

Tabla. 3.8. Ventajas y desventajas de FLAN

Ventajas	Desventajas
Este es un software multiplataforma, es decir que puede ser implementado sobre cualquier sistema operativo que soporte la máquina virtual de Java. El programa contiene además, unas herramientas llamadas manejadores, que son protocolos específicos que ayudan a determinar cómo es recibida la información, cómo procesarla y además cómo dirigir la simulación. Los manejadores podrían incluir Protocolo IP por ejemplo, que conduce la simulación hacia el mundo del IP. Esto incluiría tomar datos abstractos tales como entradas y direcciones de la tabla de encaminamiento, y el proceso de las según el estándar del IP. Los manejadores también incluyen paquetes de datos para distintos tipos de datos.	FLAN está diseñado para la prueba de protocolos en redes pequeñas, es decir, que tengan menos de 100 nodos. Aunque el usuario puede tener tantos nodos como desee, el funcionamiento se verá afectado mientras se agreguen más y más nodos. El programa permite que se trabaje con la interfaz gráfica, sin embargo es necesario tener conocimientos básicos sobre el lenguaje de programación Java, para poder hacer más configuraciones con el software y dar solución a problemas que se presenten al momento de definir características o

	parámetros de los dispositivos, protocolos y/o aplicaciones. Por otra parte, pueden presentarse problemas al compilar los instaladores de FLAN, si no se tiene la versión apropiada del JDK de JAVA.

KIVA

KIVA es una herramienta software orientada principalmente a simular el comportamiento del protocolo IP, y especialmente para el estudio del tratamiento de los datagramas y el encaminamiento de los mismos por una red. También al utilizarlo, se puede estudiar el funcionamiento de los protocolos auxiliares ARP e ICMP y emular el funcionamiento básico de tecnologías de enlace como *ethernet*. Con esta herramienta, se puede diseñar una topología de red con la interfaz gráfica, configurar el direccionamiento y las tablas de encaminamiento para los dispositivos y simular el envío de paquetes de un equipo a otro.

La principal aplicación del programa es en la enseñanza de los fundamentos sobre el funcionamiento de redes de datos; pero este entorno, también puede ser muy útil para el diseño y comprobación del encaminamiento en redes de datos a nivel comercial.

El objetivo principal de este programa, es ayudar a diseñar y comprender el funcionamiento de redes de datos y en especial el encaminamiento de paquetes en la arquitectura TCP/IP, sin necesidad de una infraestructura real y de herramientas de análisis de tráfico; éste programa, también es capaz de simular

distintos tipos de errores en el funcionamiento de las redes, como la pérdida de paquetes o fallos en tablas de encaminamiento.

El programa es multiplataforma, dado que todo su entorno fue desarrollado con el programa de simulación Java, además KIVA ofrece un API que permite usar las funciones de simulación desde otras aplicaciones de Java.

Tabla. 3.9. Ventajas y desventajas de KIVA

Ventajas	**Desventajas**
El programa se distribuye con software libre y además es multiplataforma. Permite el estudio de las redes IP y especialmente el seguimiento y análisis del funcionamiento, el envío, el tratamiento y la recepción de los datagramas a través de arquitecturas TCP/IP. Su orientación académica, hacen que sirva de ayuda para el diseño y comprensión del funcionamiento de redes de datos. Sirve como complemento de los	En la versión actual, la interfaz de usuario está implementada con un conjunto de clases, las cuales deben ejecutarse en el equipo del usuario, cada vez que se desee trabajar con éste programa. Se deben descargar varios archivos para poder instalar el programa; además se debe tener especial cuidado en descargar las versiones que se especifican ya que otras versiones de dichos paquetes, no permitirán que se complete la instalación.

fundamentos teóricos sobre arquitecturas por niveles, protocolos de enlace y arquitecturas TCP/IP.	Para el diseño y comprobación del encaminamiento en redes de datos a nivel comercial o para fines de investigación y desarrollo; se debe hacer programación en Java.

COMNET III™

Este software gráfico permite analizar y predecir el funcionamiento de redes informáticas, desde topologías básicas de interconexión hasta esquemas mucho más complejos de simulación con múltiples redes interconectadas con diversos protocolos y tecnologías como Ethernet, ATM, Satelitales, *Frame Relay*, X25, etc.

Dentro del área de trabajo del programa, se hace la descripción gráfica del modelo de red, se asocian las fuentes generadoras de tráfico en la red, se configuran los parámetros y las características de los dispositivos de acuerdo a la aplicación que se desea implementar; luego se pone en marcha la simulación y finalmente, se analizan los resultados estadísticos sobre el desempeño de la red, los cuales son programados antes de iniciar la simulación y que se generan automáticamente cuando se concluye la simulación.

Algunos de los parámetros que se pueden incluir dentro de los informes de la red esta: la ocupación de enlaces o nodos, la cantidad de mensajes generados, las colisiones, entre otros.

Este programa contiene una gran variedad de dispositivos de red como: *hosts*, *hubs*, *switches*, *routers*, *access points*, satélites, entre otros; los cuales pueden ser interconectados con enlaces y tecnologías como: *ethernet*, FDDI,

punto a punto, *frame relay*, Aloha, PVC, CSMA, entre otros; a la vez que permite implementar gran variedad de protocolos; es decir COMNET III presenta características muy completas e interesantes, en cuanto a las interfaces que soporta para su uso, sin embargo cabe mencionar que el máximo desempeño de este simulador se alcanza al utilizar las librerías para los diferentes tipos de dispositivos de redes con sus diferentes parámetros.

Además, esta herramienta es muy útil para fines didácticos en el área de las telecomunicaciones ya que adentra al usuario al mundo de las redes de forma amena, obligándolo a familiarizarse con los términos reales de los estándares existentes en las redes de comunicaciones independientemente de cual sea la aplicación. El simulador es capaz de soportar cualquier tipo de redes de comunicaciones, aunque se necesita un panorama muy completo en cuanto a lo que existe en el mercado y la implementación de redes en la práctica.

COMNET III es un software muy poderoso, sin embargo en la edición universitaria, presenta algunas limitaciones ya que no se pueden realizar las simulaciones que involucren más de 20 nodos.

Tabla. 3.10. Ventajas y desventajas de COMNET III

Ventajas	**Desventajas**
El programa ofrece la posibilidad de simular una gran cantidad de protocolos y tecnologías de red, y ofrece la posibilidad de crear protocolos a medida que se van necesitando. Permite configurar y observar una gran cantidad de	Es un software propietario. Por ser una de las herramientas de simulación más completas del mercado, la programación de los parámetros de los dispositivos y enlaces

parámetros durante la simulación como: colisiones, capacidad de los buffers de entrada y salida de los dispositivos, utilización del canal, anchos de banda, etc. Ofrece la posibilidad de ver el intercambio de mensajes entre los nodos de la red de manera gráfica, según avanza la simulación. Permite obtener gráficos y/o archivos de texto con las estadísticas de la simulación. Se pueden diseñar, configurar y simular redes complejas, que incluyan planes de contingencia, seguridad e implementación de tecnologías de superposición como LAN *Emulation*.	de la red tiende a ser compleja. Además de los conocimientos sobre el manejo y el diseño de redes de comunicaciones, se requieren conocimientos en otras áreas como por ejemplo la estadística. La versión universitaria del software, solo permite la implementación de redes con un máximo de 20 nodos. Por ser un simulador de lenguaje específico, es un poco rígido para fines de investigación y desarrollo.

3.2 Criterios de Simulaciones

Existen ciertos parámetros que se deben tomar en consideración para obtener un buen resultado de una simulación:

- Topología como el tamaño de la de la grilla.
- Número de nodos presentes.

- Ubicación espacial de los nodos.

- El tráfico que se va a simular, la cantidad paquetes, el retardo, y el tiempo de conmutación de los mismos.

- El modelo de propagación.

3.3 Variables a analizar para determinar el desempeño de la simulación

Es demasiado complejo lograr una simulación idéntica de la topología con respecto a la real, en ocasiones por la pérdida de conexiones entre nodos debido a las limitaciones de los modelos de propagación, que no consideran los efectos de algunos obstáculos físicos en el caso de las simulaciones de redes inalámbricas, para esto se asume un exponente que afecta de igual manera a cada conexión entre nodos y finalmente se obtienen representaciones muy óptimas.

Las comparaciones de latencias en las redes se realizan mediante variaciones en el número de saltos en estas, en las simulaciones las latencias presentadas tienden siempre a mostrar menores valores con respecto a las latencias reales debido a las inconsistencias que se presentan al modelar la velocidad de transmisión de una red real y a la pérdida de tiempo adicional en la ejecución del ambiente en el modelamiento. Los errores relativos en la latencia para los diferentes modelos de red son calculados dividiendo la diferencia promedio de latencia por la latencia promedio de una red real, entre menor sea el número de saltos existentes en la red habrá una mayor consistencia entre los resultados simulados y los reales.

Ventajas y desventajas de los simuladores de redes

Ventajas

- Son fácilmente reproducibles y comparables con el mundo real.

- Están libres de todo tipo de factores incontrolables que puedan afectar la simulación.

- Bajos costos de experimentación en el caso de simuladores de licencia libre.

- Permite cambiar diferentes variables en la red con gran facilidad.

- Permite la simulación y estudio de redes de grandes tamaños y gran complejidad

Desventajas

- En algunas ocasiones el hecho de no tener factores externos como tráfico y errores de transmisión que deben ser agregados de manera independiente se traduce en que los resultados de las simulaciones pueden alejarse mucho de los reales.

- Otra desventaja es que cuando se desea simular una topología con muchos nodos y durante un largo tiempo esto puede agotar los recursos del sistema donde se simula.

Tabla. 3.11. Resumen de las herramientas de simulación

	ORIENTA-CIÓN Y ÁREA DE USO	**TIPO DE LICEN-CIA**	**REQUERI-MIENTO DEL SISTEMA Y DEL S.O**	**PROTOCO-LOS Y TECNOLO-GÍAS**	**CARÁCTE-RÍSTICAS GENERA-LES**
FLAN	Simulador de propósito general orientado a objetos	Licencia pública GNU	Microsoft Windows 98/ 2000, Linux, UNIX, Mac OS X Procesador Pentium de 250 MHz ,64 MB de RAM y 20 MB de espacio libre en el disco.	IP, TCP/IP, RIP, OSPF	Flan es una herramienta de simulación que permite el diseño, la construcción, y la prueba de una red de comunicaciones en un ambiente simulado Sitio web: http://www.picolibre.enstbretagne.

KIVA	Orientado al estudio del protocolo IP y las redes con arquitectura TCP/IP. Se utiliza en el área de la enseñanza.	Software libre	Plataformas Microsoft Windows y Linux Procesador Pentium de 250 MHz o equivalente 32 MB de RAM y 20 MB de espacio libre en el disco.	IP , TCP/IP y otros especificados por el usuario	Es un simulador de redes basado en Java que permite especificar diferentes esquemas de redes de datos y simular el encaminamiento de paquetes a través de dichas redes. Sitio web: http://disclab.ua.es/kiva
PACKET TRACER	Simulador de aplicación en el área educativa.	Propietaria de Cisco	Plataformas Windows 98, ME, 2000, XP y Macintosh. Procesador Intel Pentium de 200 MHz o equivalente 64 MB de RAM y	Tecnologías Ethernet, Fast Ethernet, Gigabit Ethernet e inalámbrica, VLAN, NAT,PAT, Protocolos DHCP, RIP	Packet Tracer es un simulador de entorno de redes de comunicaciones de fidelidad media, que permite crear, configurar y detectar

			30 MB de espacio libre en el disco.		errores en topologías de redes de comunicaciones. Sitio web: http://www.ciscopress.com
OMNET III	Programa orientado a simular objetos y a modular eventos discretos en redes de comunicaciones	Software libre, solamente para propósitos académicos	Plataformas tipo UNIX y Microsoft Windows Procesador Pentium de 300 MHz o equivalente, 64 MB de RAM y 50 MB de espacio libre en el disco.	Protocolos creados por el usuario	Es una herramienta eficiente, y puede ser puede ser utilizado para modelar el tráfico de información sobre las redes, los protocolos de red, las redes de colas, multiprocesadores y otros sistemas de hardware distribuido; además para validar arquitecturas

					de hardware y evaluar el rendimiento de sistemas complejos. Sitio web: http://www.omnetpp.org
OPNET MODELER	Orientado a simular objetos y puede ser usado en diferentes tipos de áreas como la académica, comercial y el área investigativa.	Propietario (OPNET)	Windows NT, 2000, XP, y tipo UNIX Procesador Pentium de 250 MHz o equivalente 32 MB de RAM y 20 MB de espacio libre en el	HTTP, TCP, IP, OSPF, BGP, RIP, RSVP, Frame Relay, FDDI, Ethernet, ATM, LANs 802.11 (Wireless),MPLS, PNNI, DOCSIS, UMTS, IP	Permite diseñar y estudiar redes, dispositivos, protocolos y aplicaciones, brindando escalabilidad y flexibilidad, cualidades que le permiten ofrecer a sus

			disco.	Multicast, Circuit Switch, MANET, IP Móvil, IS-IS; entre otras.	usuarios trabajar en procesos de investigación y desarrollo. Está basada en la teoría de redes de colas e incorpora las librerías para facilitar el modelado de las topologías de red. Sitio web: http://www.opnet.com
NS	El Network Simulator es un software orientado a simular eventos discretos; este programa ha sido	Software Libre	Plataformas Unix (Free BSD, Linux, SunOS, Solaris) y plataformas Windows desde la versión 95 Procesador	HTTP, FTP, CBR, TCP, UDP, RTP, SRM, entre otros.	Es una herramienta con un amplio rango de uso, soporta una gran cantidad de protocolos de las capas de aplicación y

	diseñado especialmente para el área de la investigación de redes telemáticas y el área de la enseñanza.		Pentium II de 200 MHz, 32MB de memoria RAM y mínimo 320 MB de espacio libre en el disco		transporte, además de otros utilizados para el enrutamiento de los datos, permite simular redes cableadas, no cableadas, vía satélite; y aplicaciones a grandes redes con topologías complejas y varios generadores de tráfico. Sitio web: http://www.isi.edu/nsnam/ns/

COMNET III	Orientado al diseño, configuración y estudio de redes de comunicaciones Tiene uso en áreas como la enseñanza y el área comercial.	Propietario (CACI)	Para Windows 95 en adelante, procesador Pentium / 32MB RAM, 25 MB de espacio libre en D.D. En Unix; Solaris 2.5 o SunOS 5.5 Procesador Pentium 32 MB RAM, 50MB de espacio libre en el disco.	CSMA/CD, CSMA/CA, Token Ring, Inalámbrico, Ethernet, ATM, Satelitales, Frame Relay, X25 y muchos más	Permite crear topologías de redes complejas, configurar varias tecnologías, protocolos y dispositivos de red, para hacer un análisis detallado del funcionamiento y del rendimiento de redes tipo LAN, MAN y WAN, utilizando una interfaz gráfica en un ambiente de ventanas. Sitio web: http://www.compuware.com

NCTUNS	Orientado al estudio, investigación y desarrollo de redes; se utiliza en el área de la enseñanza.	Software libre	Red hat Linux; Fedora core 3.0. 256 MB de memoria RAM y 200 MB de espacio libre en el disco.	Protocolos creados por el usuario	Es un simulador y emulador de redes y sistemas de telecomunicaciones avanzado, permite desarrollar, evaluar y diagnosticar el desempeño de protocolos y aplicaciones en diferentes tipos de redes (LAN, WAN), familiarizando al usuario con interfaces similares a la de los sistemas reales. Generan resultados de

					simulación de alta fidelidad. Sitio web: http://nsl.csie.nctu.edu.tw/nctuns.html

3.4 Selección del Software

En base a las características analizadas de cada uno de las soluciones en software, y de acuerdo a los requerimientos necesarios para desarrollar las simulaciones con cada uno de los mecanismos de seguridad del estándar 802.11; se opta por la elección de Packet Tracer ya que en sus características internas contiene cada una de las seguridades analizadas en el CAPÍTULO 2.

SOFTWARE SELECCIONADO: Packet Tracer.

Descripción General

Esta herramienta software ofrece una interfaz basada en ventanas, la cual ofrece al usuario facilidades para el diseño, configuración y simulación de redes. Presenta tres modos de operación: el primero de estos es el modo topología, que aparece en la ventana de inicio cuando se abre el programa, el otro es el modo simulación, al cual se accede cuando se ha creado el modelo de la red; finalmente aparece el modo tiempo real, en donde se pueden programar mensajes SNMP (Ping), para detectar los dispositivos que están activos en la red y si existen algún problema de direccionamiento o tamaño de tramas entre las conexiones.

Interfaz gráfica del usuario

Packet Tracer tiene tres modos de operación:

- *Topology* (topología).
- Modo *simulation* (simulación).
- Modo *realtime*.

3.4.1 Capacidad de diseño de topologías sin seguridad

Es posible desarrollar una topología sin activar ningún tipo de mecanismo de seguridad en el punto de acceso.

Topología

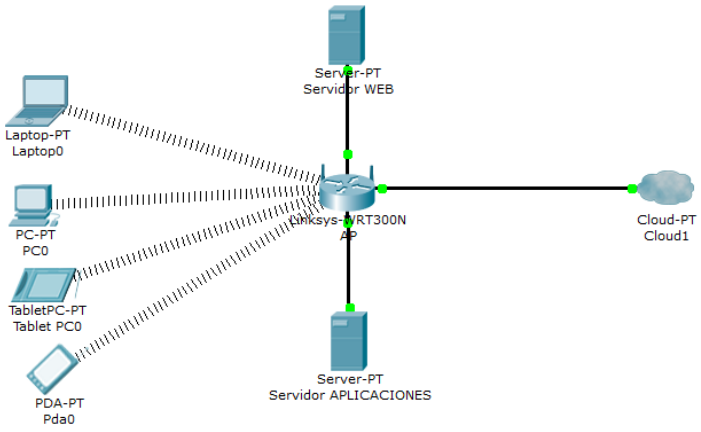

Figura. 3.1. Topología inalámbrica básica

Tabla. 3.11. Punto de acceso sin mecanismo de seguridad

Equipo	Dispositivo Wireless
Modelo	Linksys WTR 300N
Tipo de seguridad	N/A

Clave	N/A

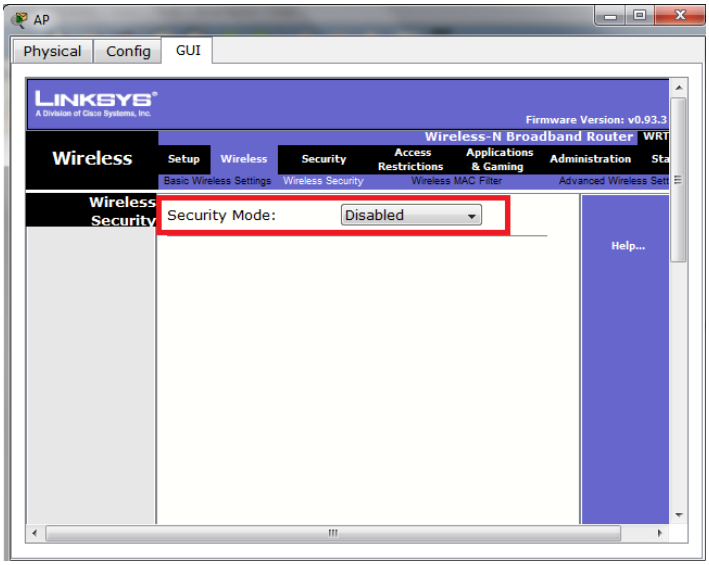

Figura. 3.2. Punto de acceso sin mecanismo de seguridad

3.4.2 Capacidad de diseño de topologías con seguridad

Escenario WEP

Tabla. 3.12. Punto de acceso utilizando WEP

Equipo	Dispositivo Wireless
Modelo	Linksys WTR 300N
Tipo de seguridad	WEP
Clave	ABCDEF1A1B

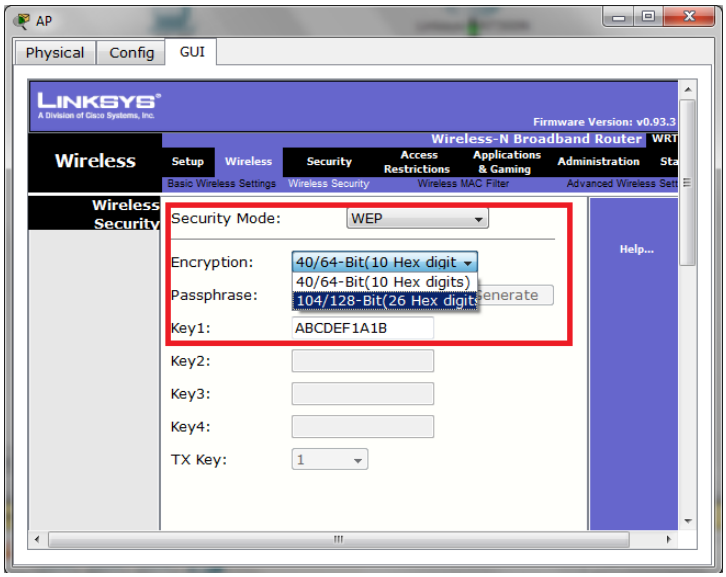

Figura. 3.3. Punto de acceso utilizando WEP

Escenario WPA Personal

Tabla. 3.13. Punto de acceso utilizando WPA

Equipo	Dispositivo Wireless
Modelo	Linksys WTR 300N
Tipo de seguridad	WPA Personal
Cifrado	TKIP/AES

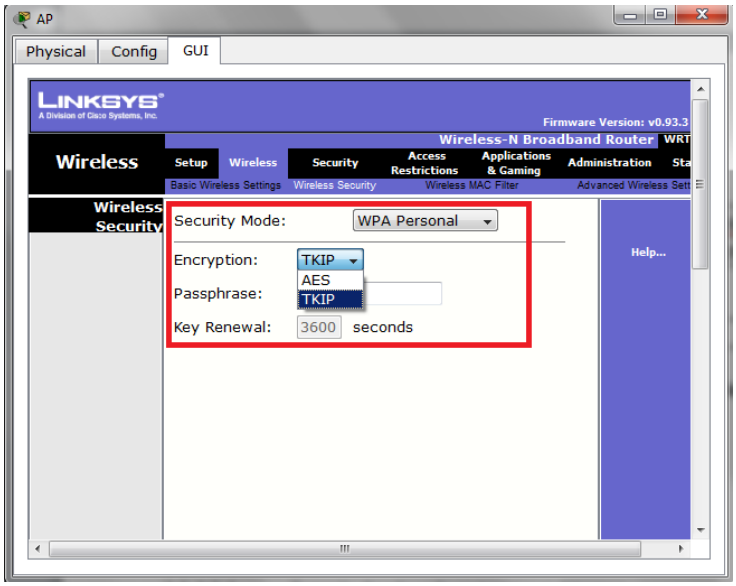

Figura. 3.4. Punto de acceso utilizando WPA Personal

Escenario WPA Enterprise

Tabla. 3.14. Punto de acceso utilizando WPA Enterprise

Equipo	Dispositivo Wireless
Modelo	Linksys WTR 300N
Tipo de seguridad	WPA Enterprise
Cifrado	TKIP/AES
Servidor de autenticación	RADIUS

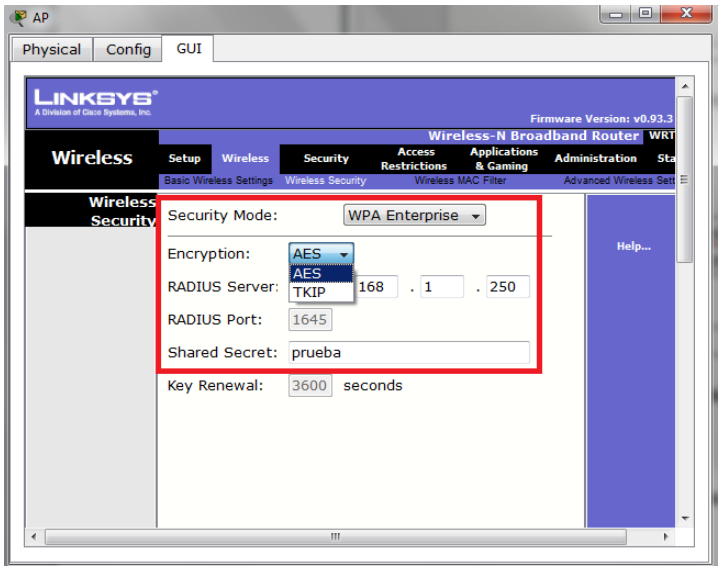

Figura. 3.5. Punto de acceso utilizando WPA Enterprise

Para los mecanismos con WPA2 y WPA2 Enterprise son las mismas configuraciones gráficas de las tablas Tabla. 3.13 y Tabla. 3.14.

CAPÍTULO 4

DESARROLLO DE TOPOLOGÍAS EN SOFTWARE

4.1 Configuración en modo infraestructura sin seguridad

Topología

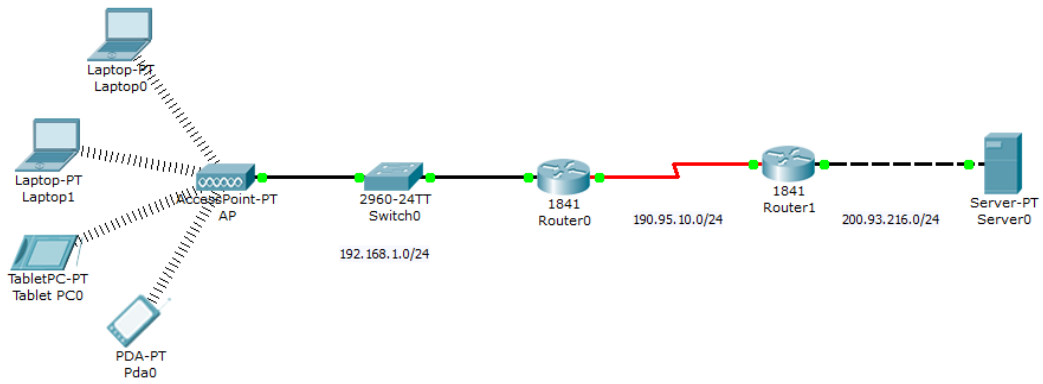

Figura. 4.1. Topología sin seguridad

Punto de Acceso

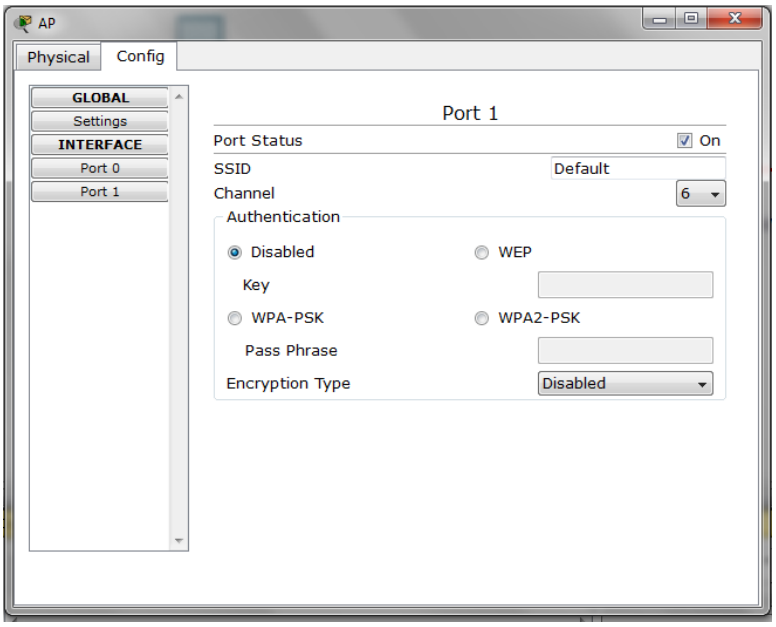

Figura. 4.2. Des habilitación de seguridad en AP

- Se desactiva la seguridad en el punto de acceso.

- No se configura un SSID.

Dispositivos Inalámbricos

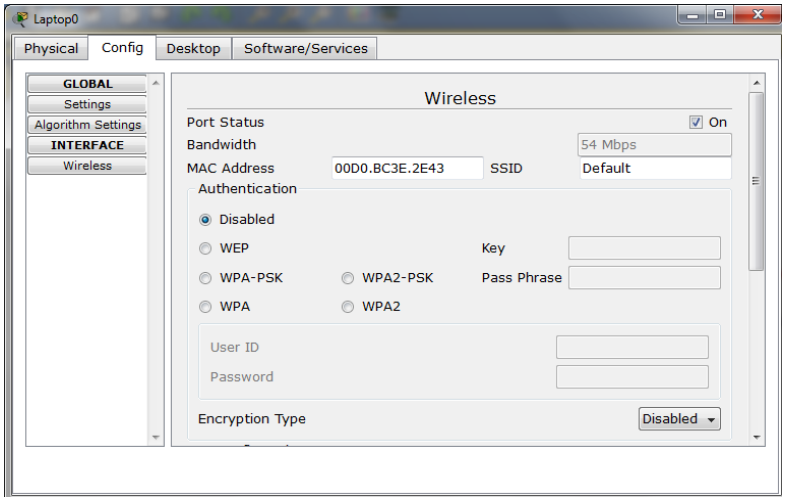

Figura. 4.3. Des habilitación de seguridad en dispositivo

- En las tarjetas inalámbricas no se activa el tipo de seguridad.

- El SSID se encuentra por defecto, la conexión hacia el AP es automática por parte de los dispositivos.

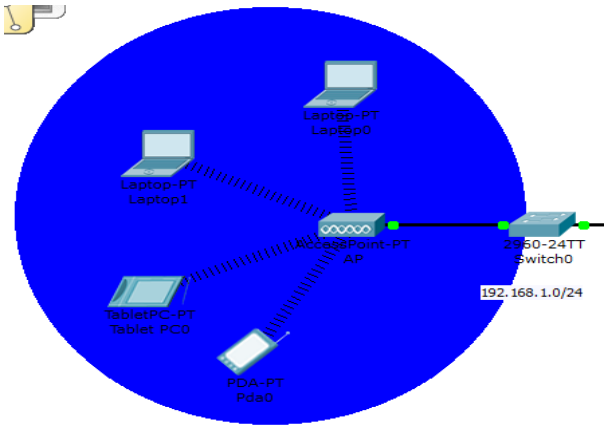

Figura. 4.4. Conexión establecida, red sin seguridad

Al simular el acceso al servidor mediante ICMP se observa que se tiene acceso completamente y la respuesta es satisfactoria (cuadro rojo).

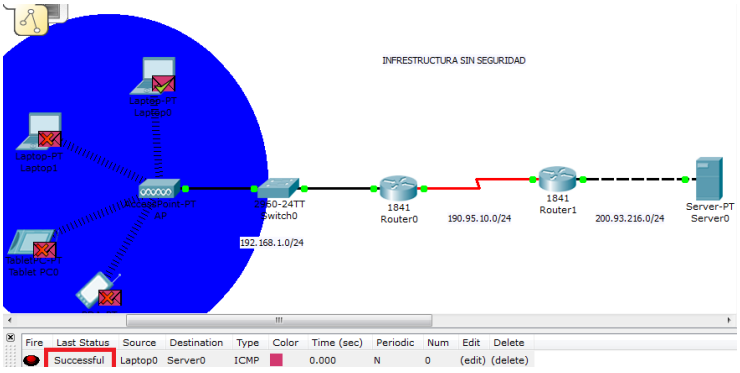

Figura. 4.5. Respuesta hacia servidor, red sin seguridad

4.2 Configuración modo infraestructura con seguridad

4.2.1 Escenario WEP

Topología

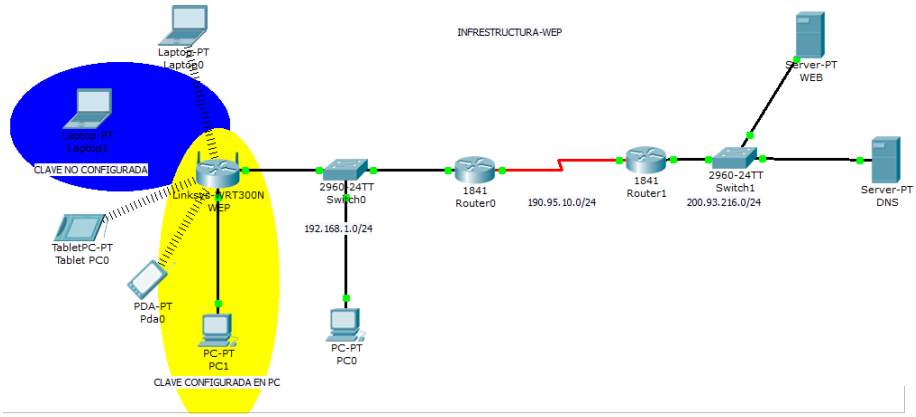

Figura. 4.6. Topología con seguridad, WEP

Punto de acceso

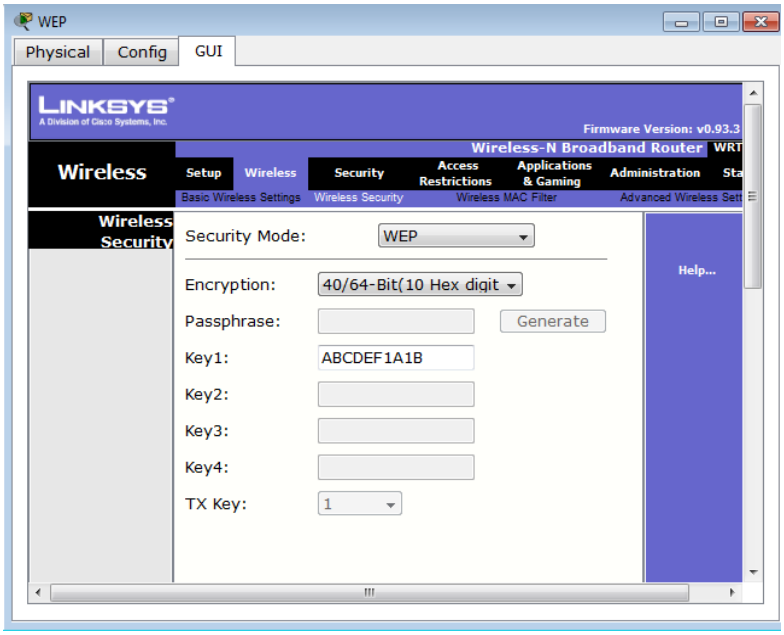

Figura. 4.7. Configuración AP, WEP

- Se activa la seguridad WEP y clave de diez dígitos hexadecimales.

- Se configura un SSID WEP.

Dispositivos Inalámbricos

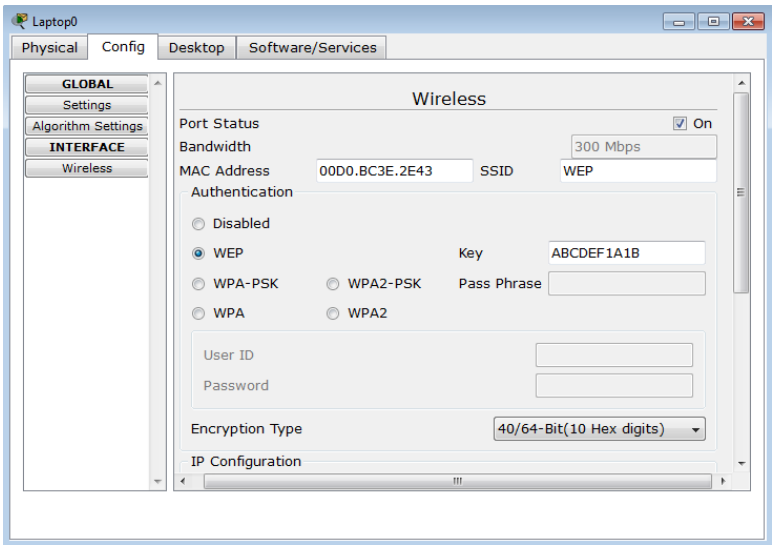

Figura. 4.8. Configuración PC, WEP

- En las tarjertas inalámbricas se activa el tipo de seguridad WEP y contraseña.

- Se configura el SSID, una vez configurado estos parámetros la conexión hacia el AP se concreta.

4.2.2 Escenario WAP Personal

Topología

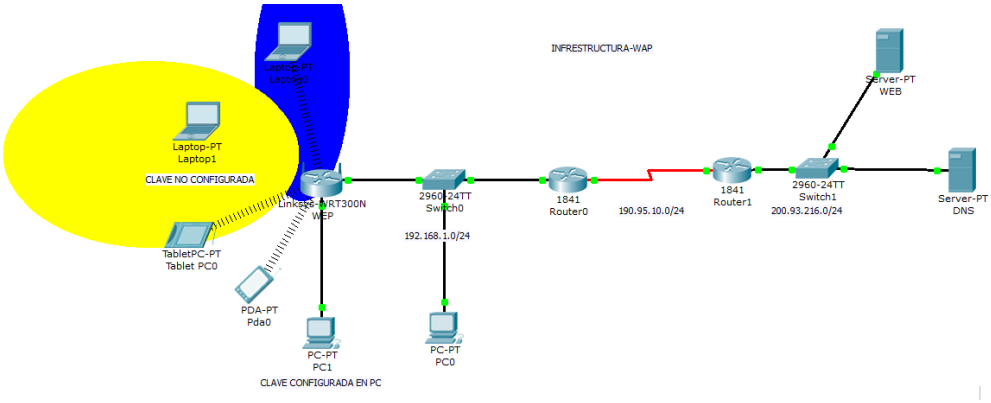

Figura. 4.9. Topología con seguridad, WPA

Punto de Acceso

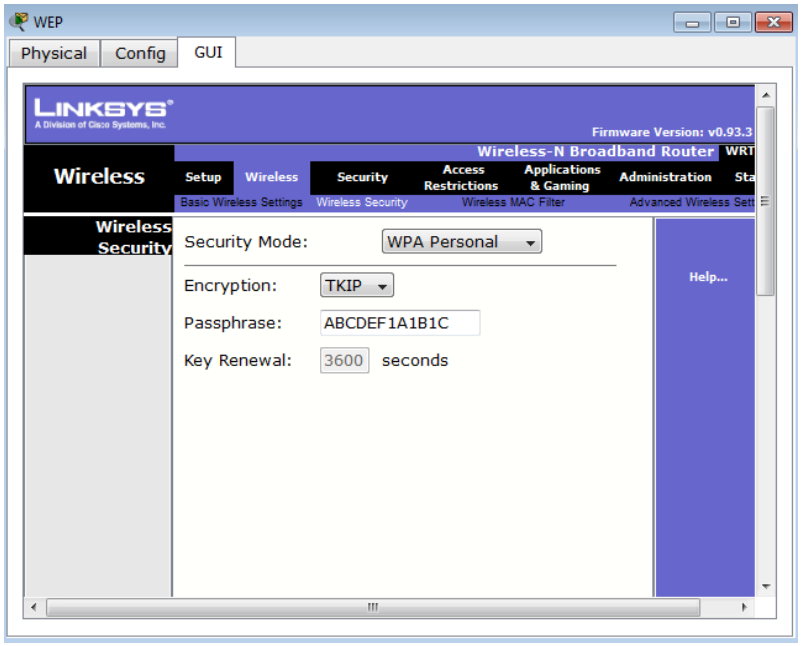

Figura. 4.10. Configuración, WPA

- Se activa la seguridad WAP Personal, encriptación TKIP y clave más extensa.

- Se configura un SSID.

Dispositivos Inalámbricos

Figura. 4.11. Configuración PC, WPA

- En las tarjertas inalámbricas se activa el tipo de seguridad WAP, encriptación TKIP y contraseña.

- Se configura el SSID, una vez configurado estos parámetros la conexión hacia el AP se establece.

4.2.3 Escenario WAP Enterprise

Topología

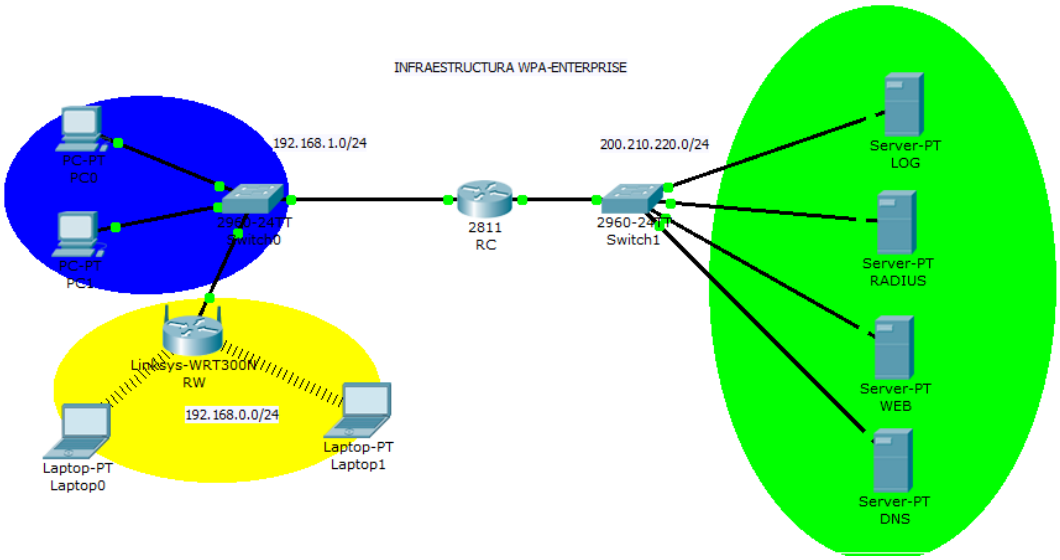

Figura. 4.12. Topología con seguridad, WPA Enterprise

Configuración Router RC

Configuración y habilitación de interfaces Fa0/0 y Fa0/1

Fa0/0: 192.168.1.1/24
Fa0/1: 200.210.220.1/24

Configurar en RC la forma de logeo, de acuerdo al mecanismo de seguridad WPA Enterprise se lo configura a través del servidor RADIUS, para ello ingresamos a la línea de comandos.

Se habilita la autenticación

- aaa new-model

Se indica que al hacer un logeo al router RC, se utilice un servidor RADIUS

- aaa authentication login default group radius none

Mediante el comando “none", se dice a RC que si no existe un servidor RADIUS, el usuario no ingresar por telnet.

- radius-server host 200.210.220.20 auth-port 1645 key cisco123

Se configura el direccionamiento del servidor RADIUS, además la llave que debe ser la misma configurada en el servidor RADIUS.

- aaa authentication login telnet group radius

Ahora se configura la forma sobre la cual se realizará la autenticación dentro de telnet, y se lo validará con RADIUS. Habilitar Telnet.

- line vty 0 4

- login authentication telnet

Después de haber configurado esta aplicación podemos por ejemplo poder acceder al ROUTER1 vía telnet desde una PC solo si hemos sido autenticado en el servidor RADIUS.

Configuración Servidor RADIUS

- Dirección ip

- Máscara de subred

- Puerta de enlace de servidor RADIUS

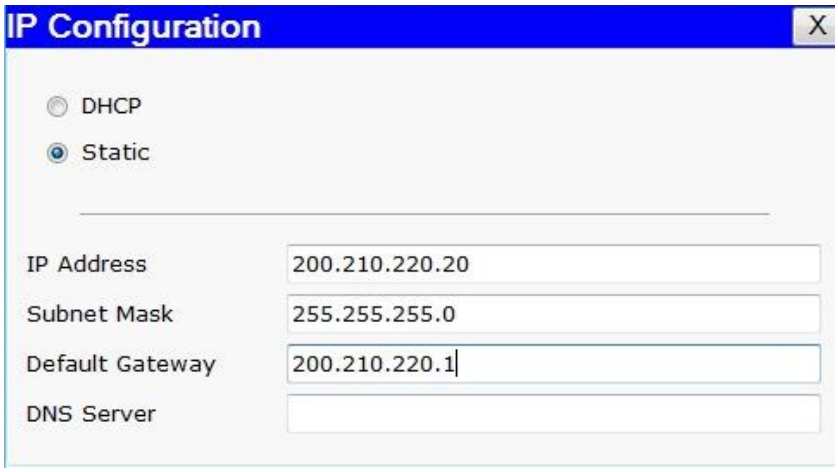

Figura. 4.13. Topología con seguridad, servidor RADIUS

Se configura los clientes que el servidor RADIUS administrará, en este caso son RC, RW y WEB.

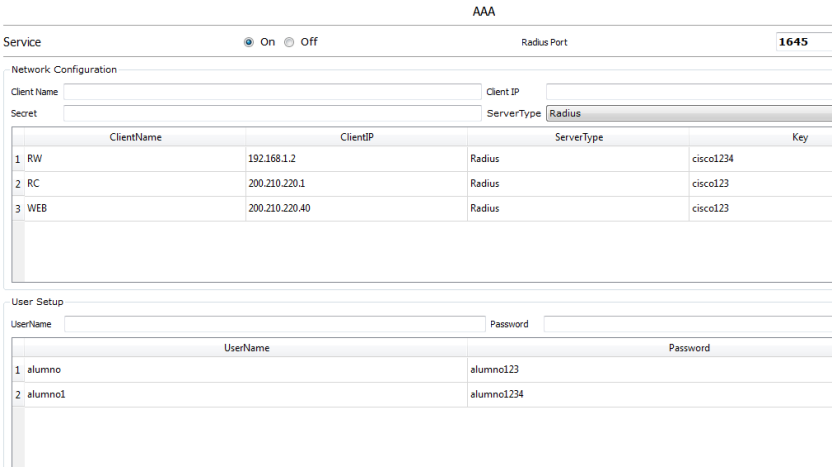

Figura. 4.14. Topología con seguridad, clientes RADIUS

- CLIENT NAME: Nombre del dispositivo a administrar.

- CLIENT IP: IP del dispositivo a administrar.

- SECRET: Palabra de conexión, palabra igual en los extremos de la comunicación.

Se agregan los usuarios que van a ser validados con la base de datos del servidor:

- Nombre de usuario: alumno
- Password: alumno123

Configuración Router Inalámbrico RW

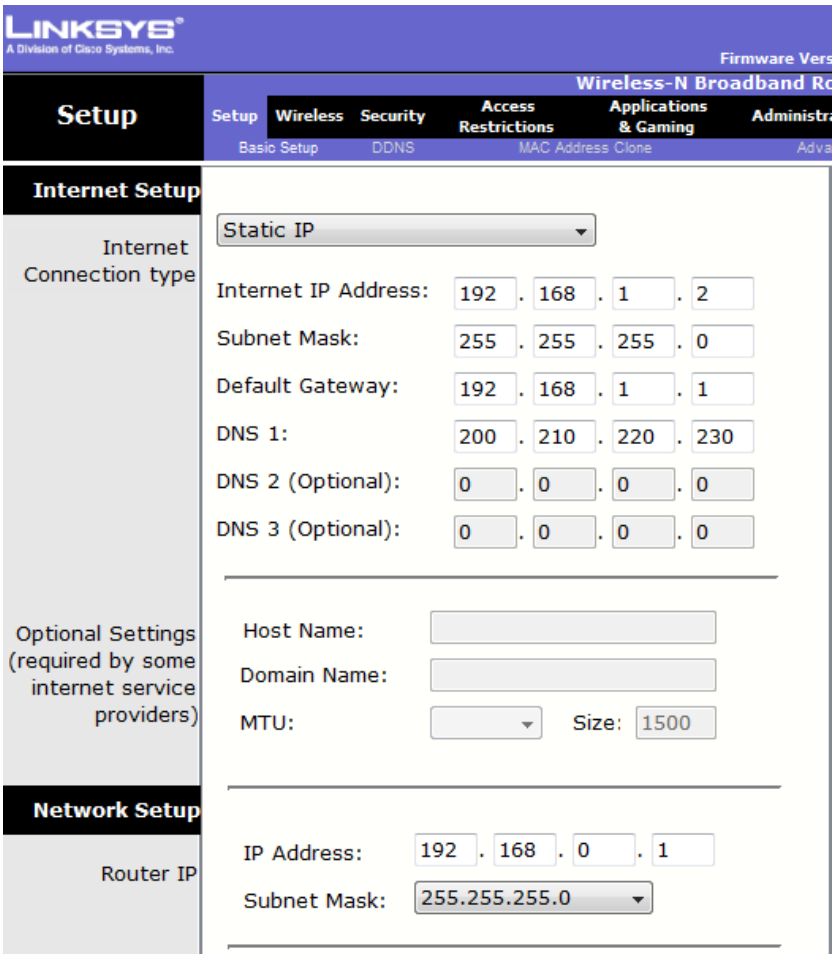

Figura. 4.15. WPA Enterprise, direccionamiento AP

Se configura los campos de Internet y Network que corresponden a la interfaz que es la conexión hacia el *switch* y la red LAN correspondientemente.

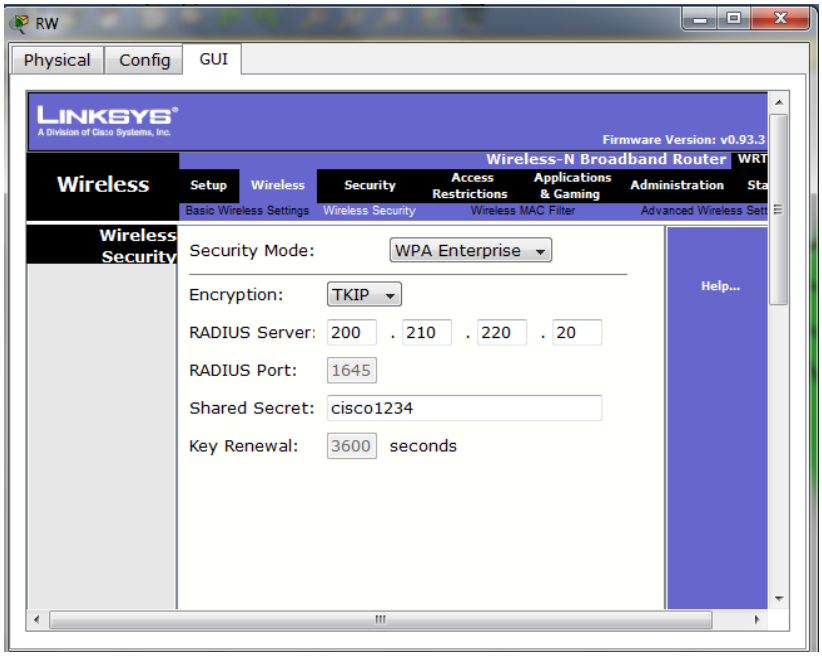

Figura. 4.16. Configuración WPA Enterprise

Se establece el tipo de seguridad y modo de encriptación, se despliega otro campo que es la dirección IP del servidor RADIUS, además del *password* que como se indicó antes debe coincidir con el configurado en RC.

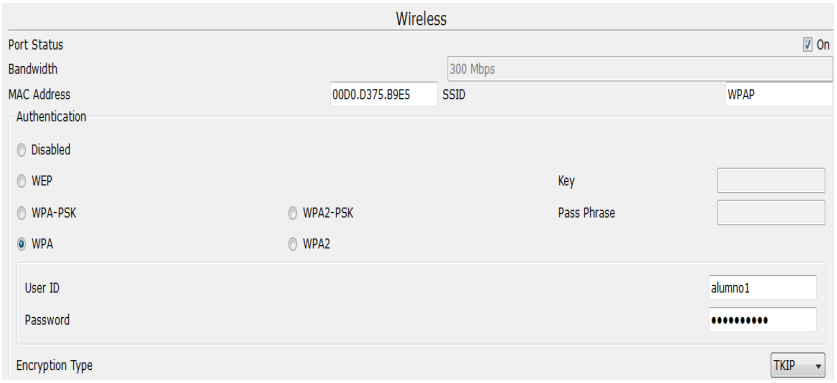

Figura. 4.17. Configuración PC, WPA Enterprise

Se configura en los dispositivos inalámbricos el mecanismo de seguridad, tipo de encriptación y las credenciales de validación para el servidor RADIUS.

Se configura las tarjetas inalámbricas de la siguiente forma:

1. Editar el perfil del host. Seleccionamos el perfil *click Profiles*.

Figura. 4.18. Configuración PC, WPA Enterprise-1

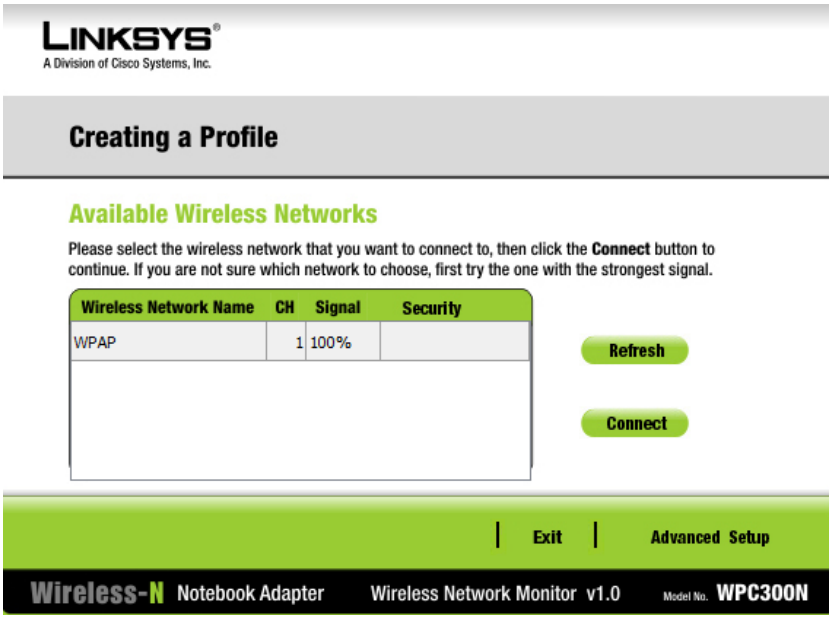

Figura. 4.19. Configuración PC, WPA Enterprise-1-1

2. Seleccionamos el SSID del AP y seleccionar *Advanced Setup*

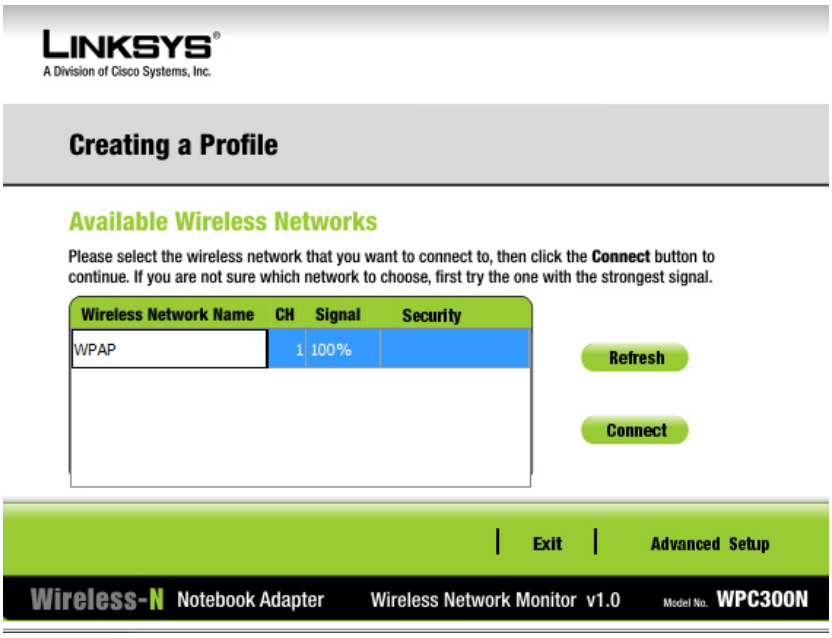

Figura. 4.20. Configuración PC, WPA Enterprise-2

3. Verificamos el SSID del AP, *click Next*.

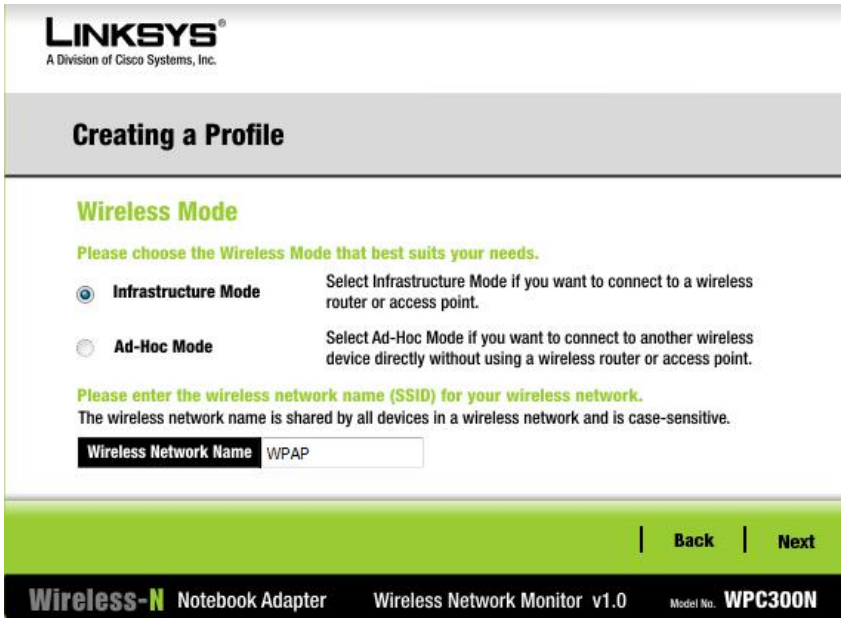

Figura. 4.21. Configuración PC, WPA Enterprise-3

4. La configuración es DHCP, se deja la opción marcada, *click Next*

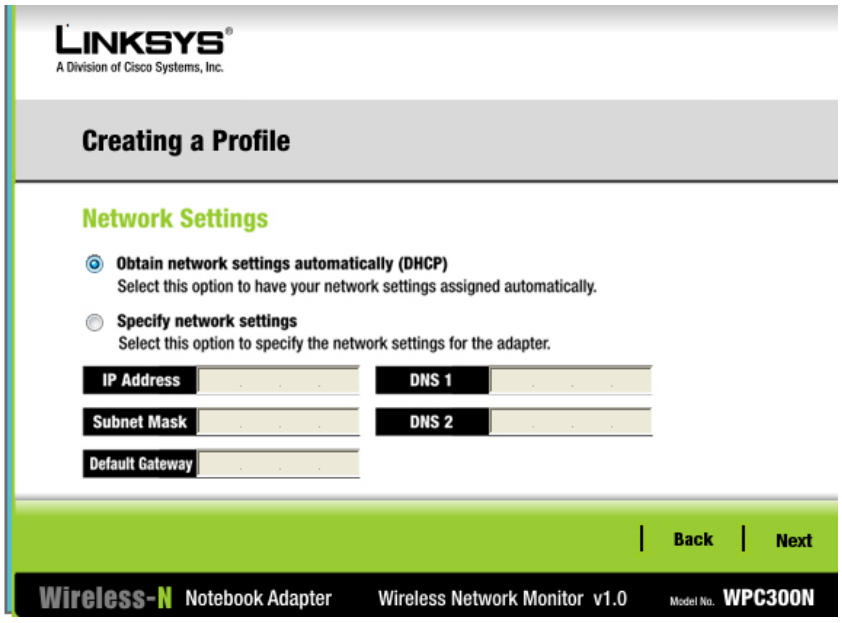

Figura. 4.22. Configuración PC, WPA Enterprise-4

5. Seleccionamos el tipo de encriptación que usa el AP y damos *click Next*.

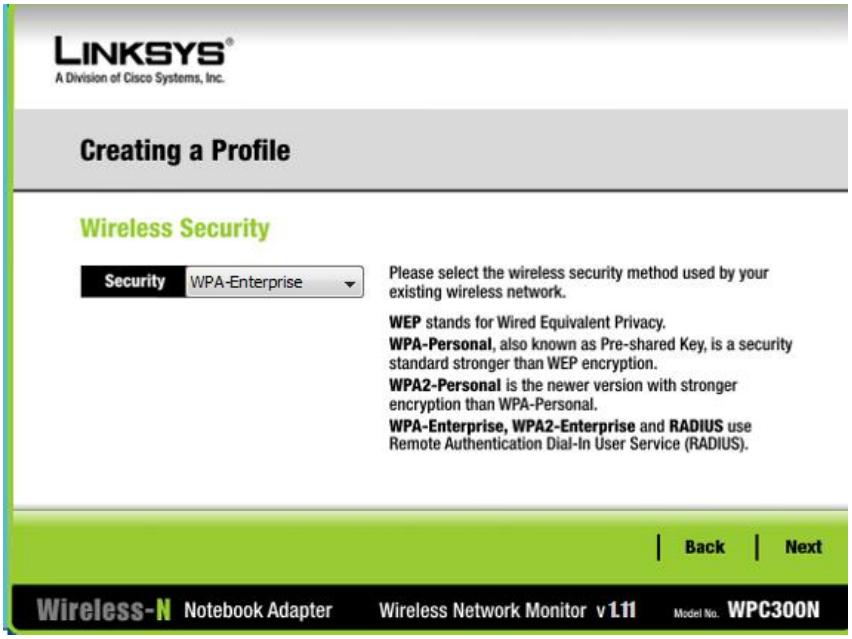

Figura. 4.23. Configuración PC, WPA Enterprise-5

6. Ingresar el usuario y contraseña que se ingresó a la base de datos del servidor RADIUS, *click Next*.

Figura. 4.24. Configuración PC, WPA Enterprise-6

7.Click *Save*.

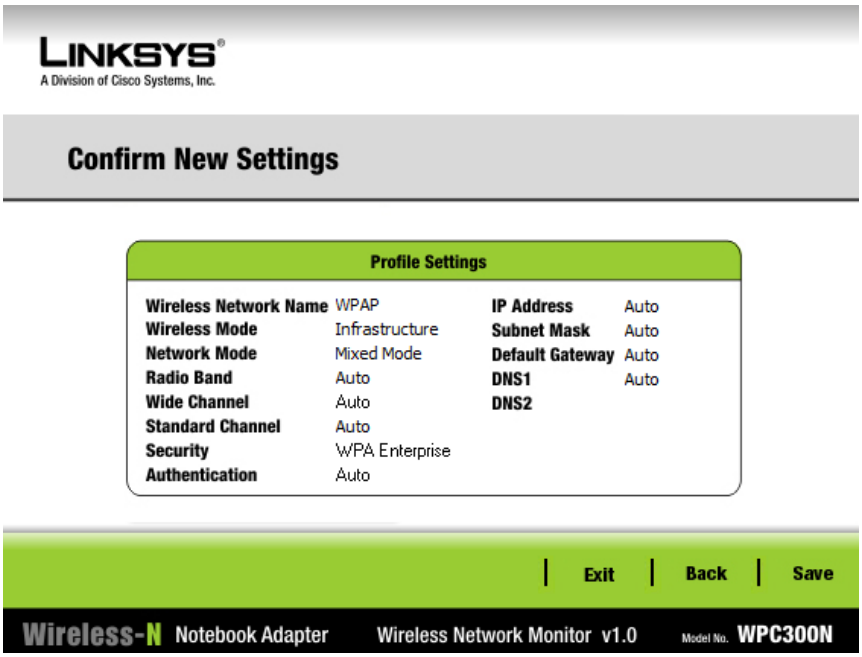

Figura. 4.25. Configuración PC, WPA Enterprise-7

Por último se conecta a la red, de esta manera se establece la conexión con autenticación y encriptación con un servidor RADIUS.

Figura. 4.26. Conexión establecida PC, WPA Enterprise

4.2.4 Escenario WAP2

Topología

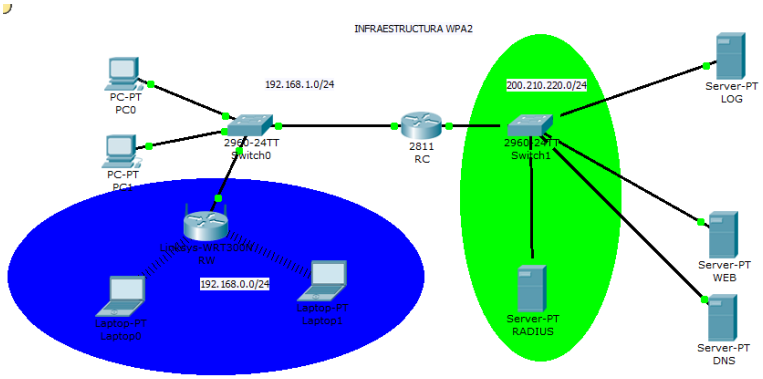

Figura. 4.27. Topología con seguridad, WPA2-AES

Configuración Router RC

Configuración y habilitación de interfaces Fa0/0 y Fa0/1

Fa0/0: 192.168.1.1/24
Fa0/1: 200.210.220.1/24

Configurar en RC la forma de logeo, de acuerdo al mecanismo de seguridad WPA Enterprise se lo configura a través del servidor RADIUS, para ello ingresamos a la línea de comandos.

Se habilita la autenticación

- aaa new-model

Se indica que al hacer un logeo al router RC, se utilice un servidor RADIUS

- aaa authentication login default group radius none

Mediante el comando “none", se dice a RC que si no existe un servidor RADIUS, el usuario no ingresar por telnet.

- radius-server host 200.210.220.20 auth-port 1645 key cisco123

Se configura el direccionamiento del servidor RADIUS, además la llave que debe ser la misma configurada en el servidor RADIUS.

- aaa authentication login telnet group radius

Ahora se configura la forma sobre la cual se realizará la autenticación dentro de telnet, y se lo validará con RADIUS. Habilitar Telnet.

- line vty 0 4

- login authentication telnet

Después de haber configurado esta aplicación podemos por ejemplo poder acceder al ROUTER1 vía telnet desde una PC solo si hemos sido autenticado en el servidor RADIUS.

Configuración Servidor RADIUS

- Dirección ip

- Máscara de subred

- Puerta de enlace de servidor RADIUS

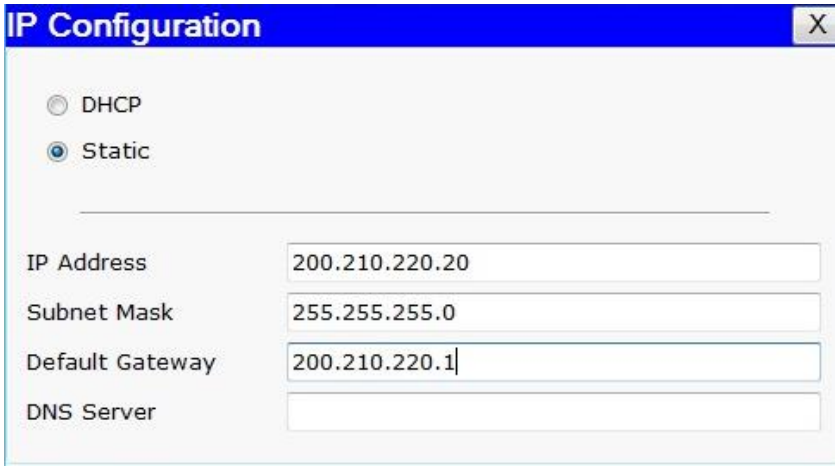

Figura. 4.28. Topología con seguridad, servidor RADIUS

Se configura los clientes que el servidor RADIUS administrará, en este caso son RC, RW y WEB.

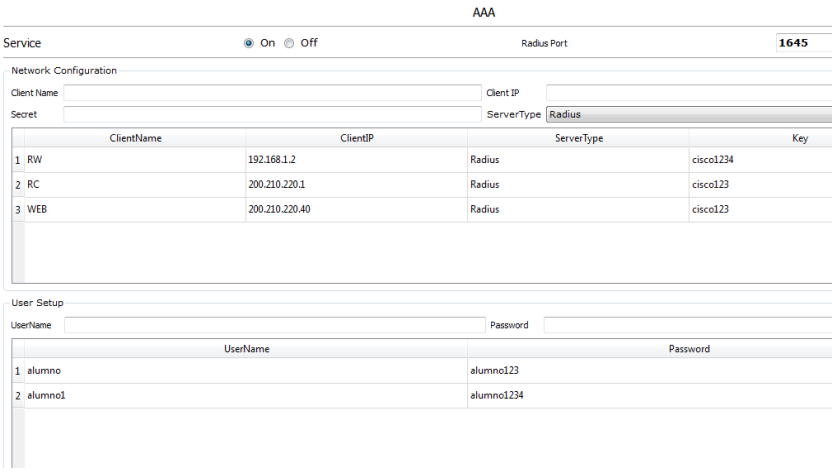

Figura. 4.29. Topología con seguridad, clientes RADIUS

- CLIENT NAME: Nombre del dispositivo a administrar.

- CLIENT IP: IP del dispositivo a administrar.

- SECRET: Palabra de conexión, palabra igual en los extremos de la comunicación.

Se agregan los usuarios que van a ser validados con la base de datos del servidor:

- Nombre de usuario: alumno
- Password: alumno123

Configuración Router Inalámbrico RW

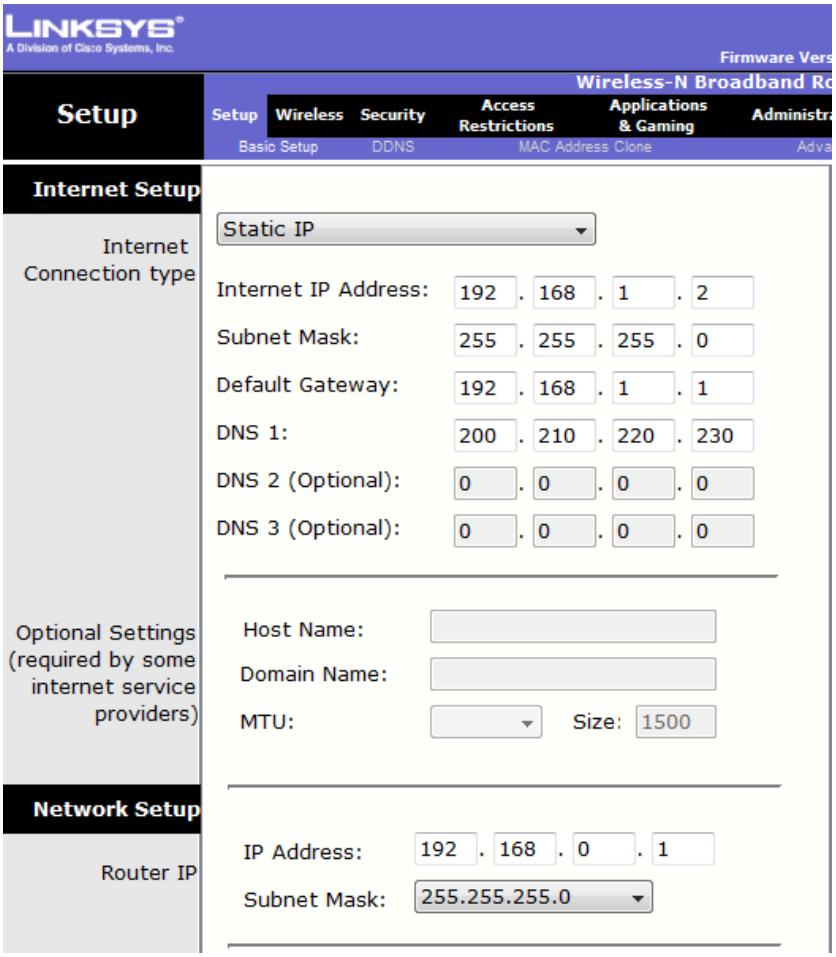

Figura. 4.30. WPA2, direccionamiento AP

Se configura los campos de Internet y Network que corresponden a la interfaz que es la conexión hacia el *switch* y la red LAN correspondientemente.

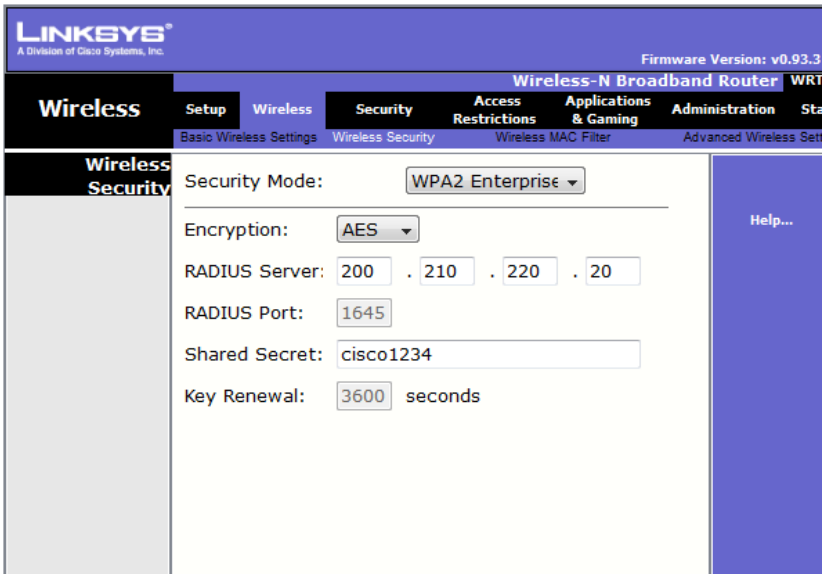

Figura. 4.31. Configuración WPA2-AES

Se establece el tipo de seguridad y modo de encriptación, se despliega otro campo que es la dirección IP del servidor RADIUS, además del *password* que como se indicó antes debe coincidir con el configurado en RC.

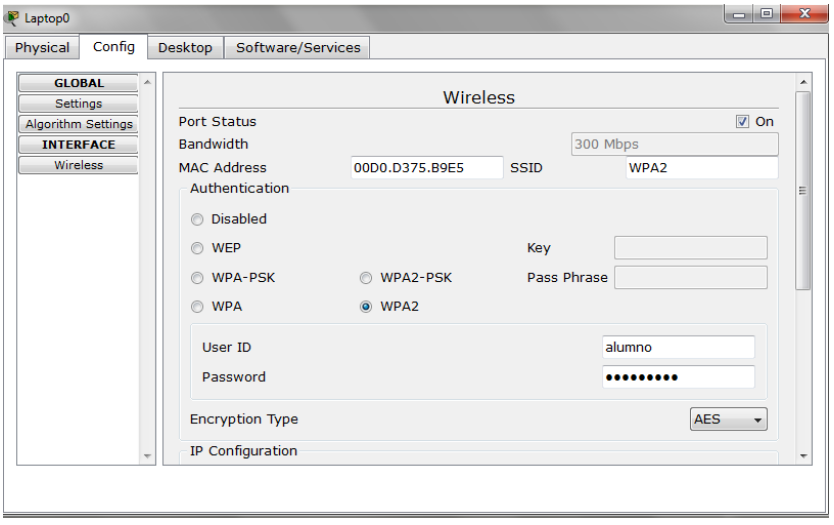

Figura. 4.32. Configuración PC, WPA2-AES

Se configura en los dispositivos inalámbricos el mecanismo de seguridad, tipo de encriptación y las credenciales de validación para el servidor RADIUS.

Se configura las tarjetas inalámbricas de la siguiente forma:

1. Editar el perfil del host. Seleccionamos el perfil *click Profiles*.

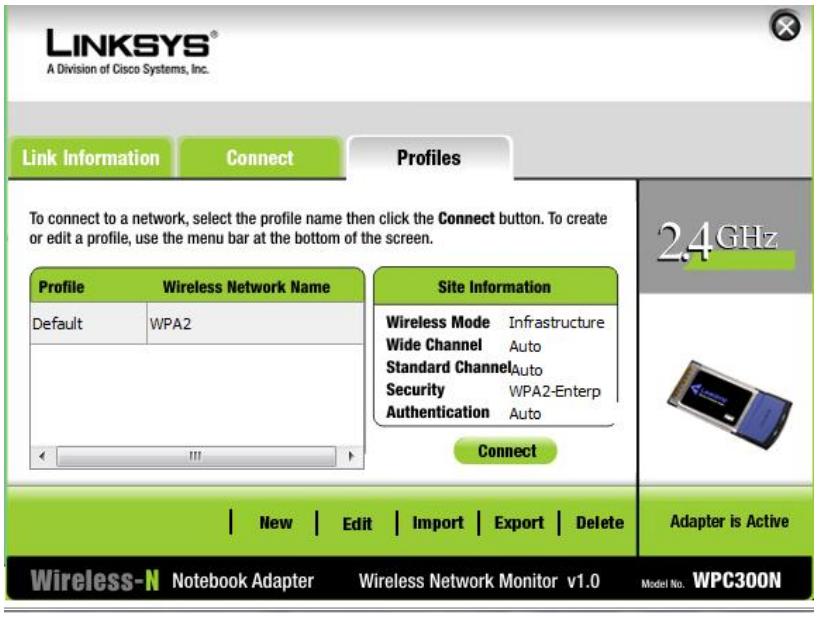

Figura. 4.33. Configuración PC, WPA2-1

3. Seleccionamos el SSID del AP y seleccionar *Advanced Setup*

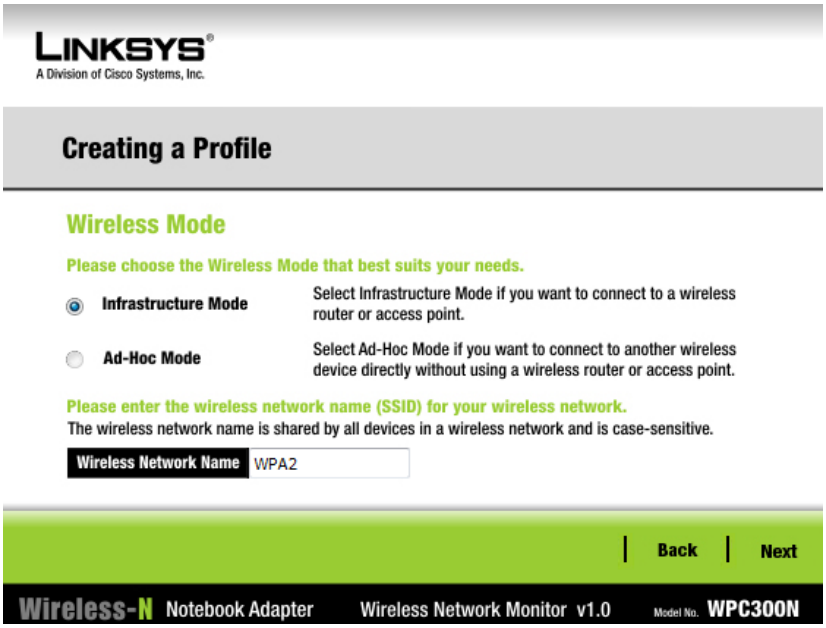

Figura. 4.34. Configuración PC, WPA2-2

4. Verificamos el SSID del AP, *click Next*.

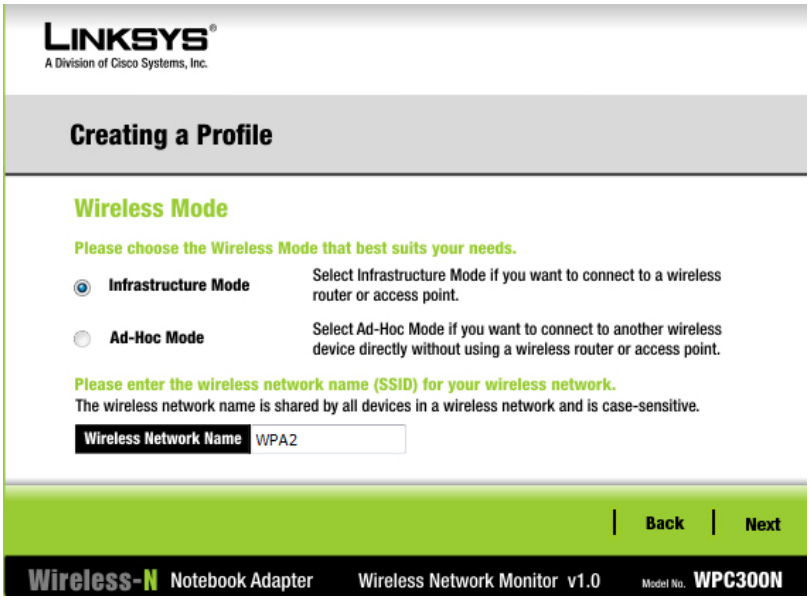

Figura. 4.35. Configuración PC, WPA2-3

5. La configuración es DHCP, se deja la opción marcada, *click Next*

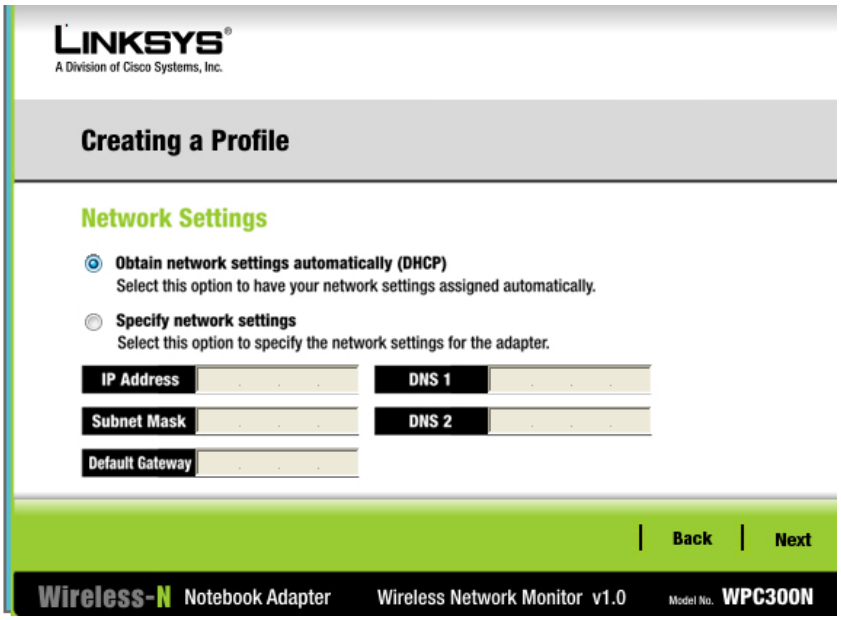

Figura. 4.36. Configuración PC, WPA2-4

6. Seleccionamos el tipo de encriptación que usa el AP y damos *click Next*.

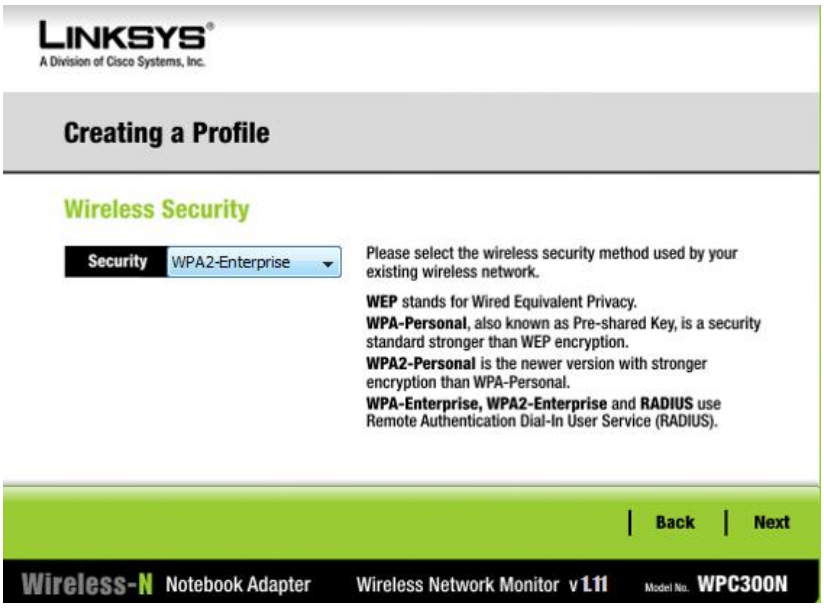

Figura. 4.37. Configuración PC, WPA2-5

6. Ingresar el usuario y contraseña que se ingresó a la base de datos del servidor RADIUS, *click Next*.

Figura. 4.38. Configuración PC, WPA2-6

7.Click en *Save*.

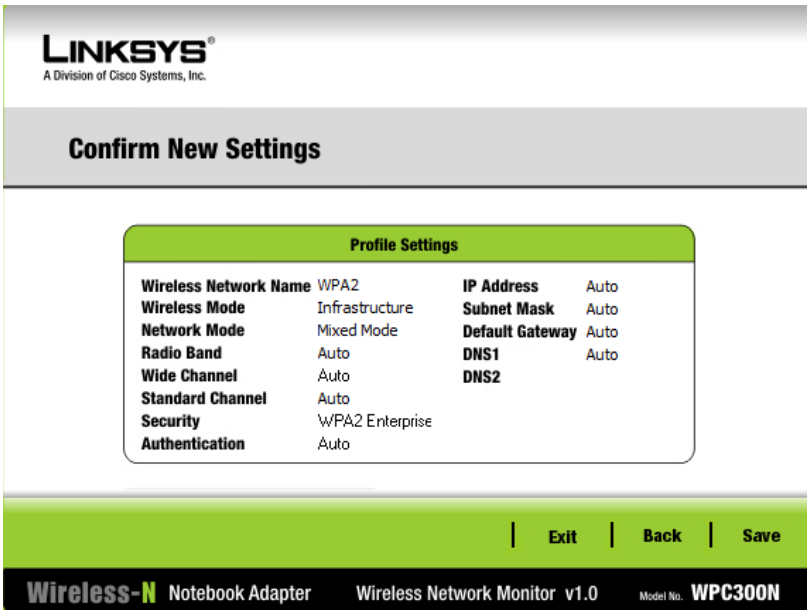

Figura. 4.39. Configuración PC, WPA2-7

Por último se conecta a la red, de esta manera se establece la conexión con autenticación y encriptación con un servidor RADIUS.

Figura. 4.40. Conexión establecida PC, WPA2

4.3 Análisis de las topologías simuladas.

4.3.1 Escenario WEP

Equipo autenticado - Paquetes al acceder a servidor WEB

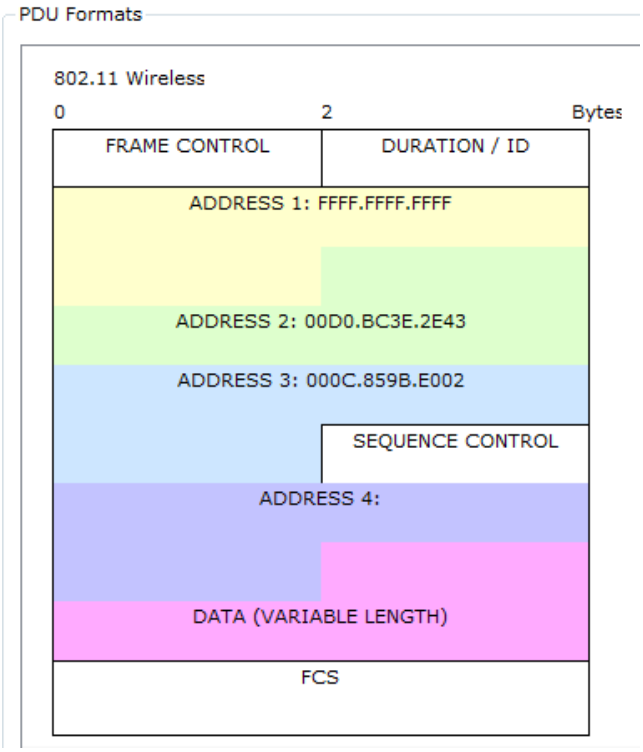

Figura. 4.41. PDU WEP-MAC

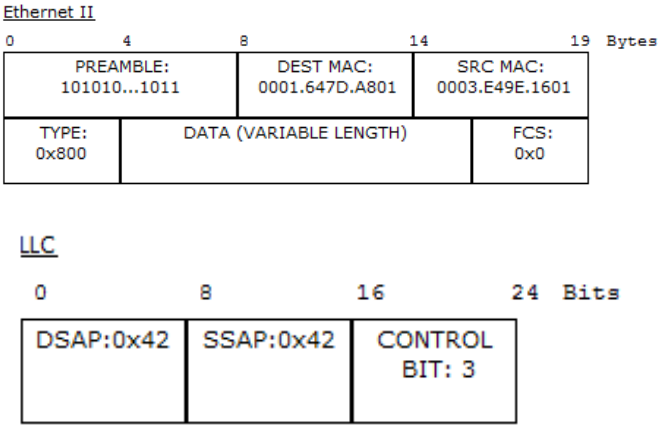

Figura. 4.42. PDU WEP-LLC

Tabla. 4.1. Análisis paquete PDU MAC y LLC

ENCABEZADO 802.11		
No. de Byte	**Campo (s)**	**Valor (es)**
0 y 1	Control del	N/D

	Paquete	
2 y 3	Duración/ID	0x13
4 al 9	Dirección MAC destino	0001.647d.a801
10 al 15	BSSID	N/D
16 al 21	Dirección MAC origen	0003.e49e.1601
22 y 23	Control de Secuencia	N/D
ENCABEZADO LLC		
24	DSAP	0x42
25	SSAP	0x42
26	Control	0x03
27 al 29	Código Organizacional	0x000000
30 y 31	Tipo	0x0800

Observación: No es posible determinar todos los bytes de la tramas 802.11, no se puede capturar el tráfico de autenticación WEP para el análisis completo de tramas, el sistema de simulación es controlado, simplemente se nota que al configurar la clave y SSID en el dispositivo inalámbrico se establece la conexión entre el AP y el suplicante.

Equipo sin autenticar - Paquetes al acceder a servidor WEB

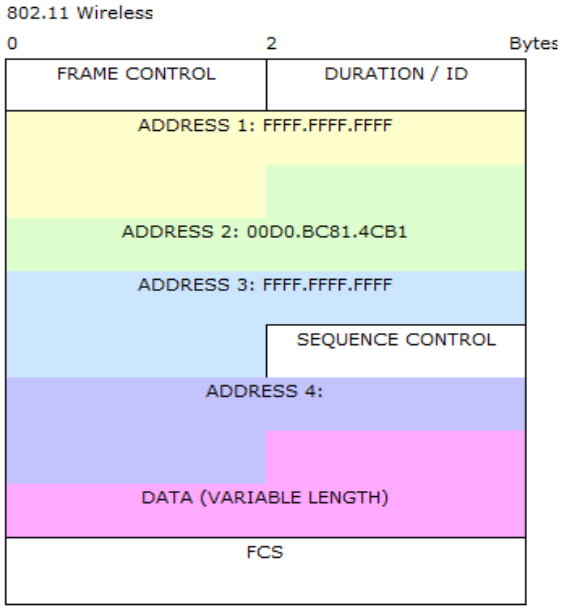

Figura. 4.43. PDU WEP-MAC, sin autenticación

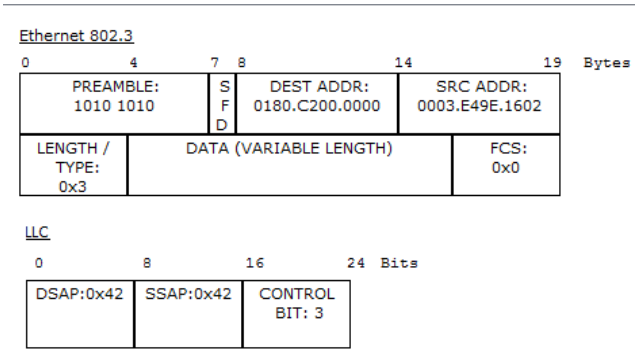

Figura. 4.44. PDU WEP-LLC, sin autenticación

Tabla. 4.2. Análisis paquete PDU MAC y LLC-Sin autenticación

ENCABEZADO 802.11		
No. de Byte	**Campo (s)**	**Valor (es)**
0 y 1	Control del Paquete	N/D
2 y 3	Duración/ID	0x00
4 al 9	Dirección MAC	0180.c200.0000

	destino	
10 al 15	BSSID	N/D
16 al 21	Dirección MAC origen	0003.e49e.1602
22 y 23	Control de Secuencia	N/D
ENCABEZADO LLC		
24	DSAP	0x42
25	SSAP	0x42
26	Control	0x03
27 al 29	Código Organizacional	0x000000
30 y 31	Tipo	0x0800

Observación: No es posible determinar todos los bytes de la tramas 802.11, no se puede capturar el tráfico de autenticación WEP para el análisis completo de tramas, el sistema de simulación es controlado, simplemente se nota que al no configurar la clave WEP hexadecimal de 10 dígitos hexadecimales no se establece la conexión entre el AP y el suplicante.

4.3.2 Escenario WPA – Personal

Equipo autenticado - Paquetes al acceder a servidor WEB

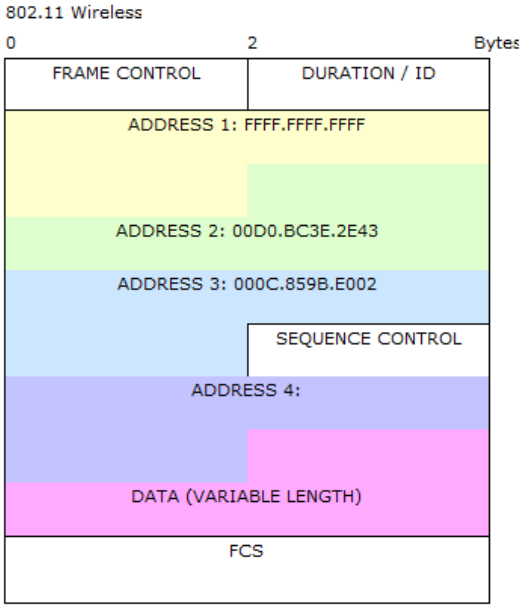

Figura. 4.45. PDU WPA-TKIP, MAC

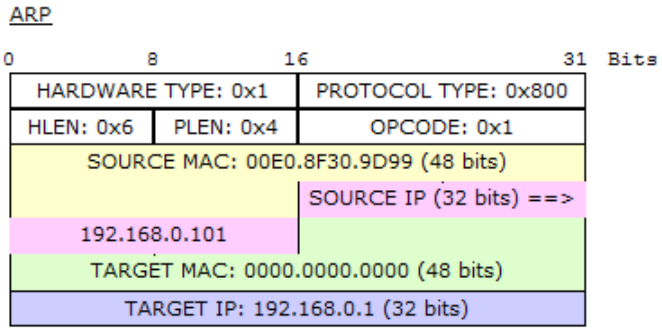

Figura. 4.46. PDU WPA-TKIP, ARP

Tabla. 4.3. Análisis paquete PDU MAC y LLC, WPA-TKIP

ENCABEZADO 802.11		
No. de Byte	**Campo (s)**	**Valor (es)**
0 y 1	Control del Paquete	N/D
2 y 3	Duración/ID	0x44
4 al 9	Dirección MAC destino	0001.647d.a801

10 al 15	BSSID	N/D
16 al 21	Dirección MAC origen	00e0.8f30.9d99
22 y 23	Control de Secuencia	N/D
ENCABEZADO LLC		
24	DSAP	N/D
25	SSAP	N/D
26	Control	0x03
27 al 29	Código Organizacional	0x000000
30 y 31	Tipo	0x0800

Observación: No es posible determinar todos los bytes de la tramas 802.11-LLC, no se puede capturar el tráfico de autenticación WPA-TKIP para el análisis completo de tramas, el sistema de simulación es controlado, al configurar la clave y método de cifrado se establece la conexión entre el AP y el suplicante.

4.3.3 Escenario WPA – Enterprise

Equipo autenticado - Paquetes al acceder a RC

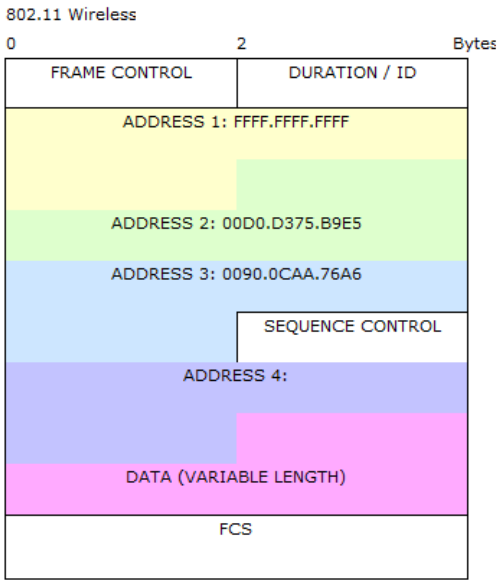

Figura. 4.47. PDU WPA Enterprise-MAC

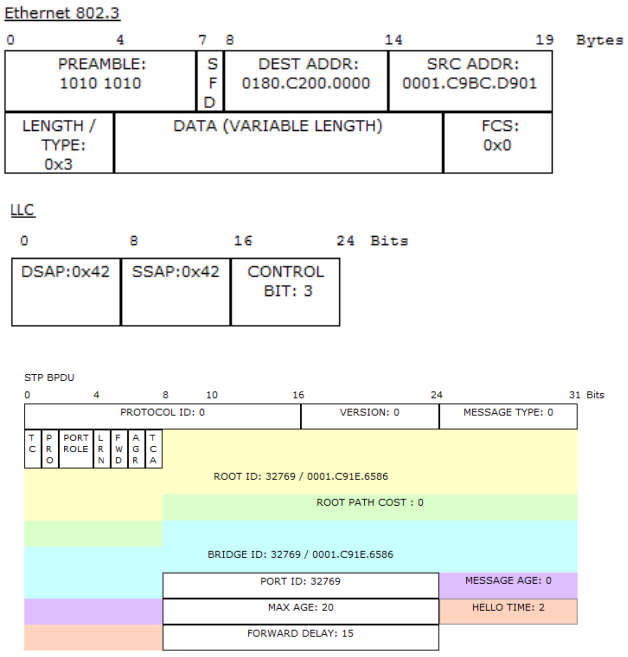

Figura. 4.48. PDU WPA Enterprise-LLC

Tabla. 4.4. Análisis paquete PDU MAC y LLC, WPA Enterprise

ENCABEZADO 802.11		
No. de	**Campo (s)**	**Valor (es)**

Byte		
0 y 1	Control del Paquete	N/D
2 y 3	Duración/ID	0x13
4 al 9	Dirección MAC destino	0180.c200.0000
10 al 15	BSSID	N/D
16 al 21	Dirección MAC origen	0001.c9bc.d901
22 y 23	Control de Secuencia	N/D
ENCABEZADO LLC		
24	DSAP	0x42
25	SSAP	0x42
26	Control	0x03
27 al 29	Código Organizacional	0x000000
30 y 31	Tipo	0x0800

Observación: Se obtienen los valores de los campos DSAP, SSAP, control y tipo, se tiene que establecer el direccionamiento del servidor RADIUS el cual autentica a RC y RW para que los dispositivos de sus redes tengan acceso vía TELNET a RC, se configura el modelamiento aaa en RC y encriptación TKIP en AP y dispositivos inalámbricos.

Equipo sin autenticar - Paquetes al acceder a RC

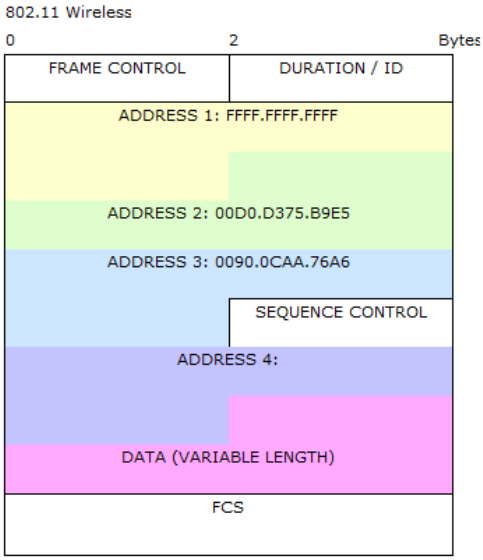

Figura. 4.49. PDU MAC WPA Enterprise-TKIP, sin autenticación

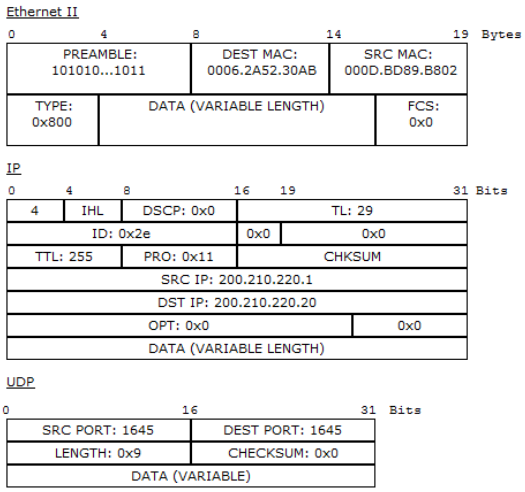

Figura. 4.50. PDU RADIUS, sin autenticación

Tabla. 4.5. Análisis paquete PDU MAC WPA Enterprise-TKIP, sin autenticación

ENCABEZADO 802.11		
No. de Byte	**Campo (s)**	**Valor (es)**
0 y 1	Control del Paquete	N/D
2 y 3	Duración/ID	0x2e

4 al 9	Dirección MAC destino	0006.2a52.30ab
10 al 15	BSSID	N/D
16 al 21	Dirección MAC origen	000d.bd89.b802
22 y 23	Control de Secuencia	N/D
ENCABEZADO LLC		
24	DSAP	N/D
25	SSAP	N/D
26	Control	N/D
27 al 29	Código Organizacional	0x000000
30 y 31	Tipo	0x0800

Observación: No existe gran variación en la PDU del paquete RADIUS, no se puede analizar el proceso de negociación del servidor hacia el solicitante, el software para el análisis de tráfico es bastante limitado, esta configuración está realizada con WPA Enterprise con cifrado TKIP, no se observa en los paquetes una variación notoria.

4.3.4 Escenario WPA2

Equipo autenticado - Paquetes al acceder a RC

Tabla. 4.4. Análisis paquete PDU MAC y LLC, WPA Enterprise

ENCABEZADO 802.11		
No. de Byte	**Campo (s)**	**Valor (es)**
0 y 1	Control del Paquete	N/D

2 y 3	Duración/ID	0x13
4 al 9	Dirección MAC destino	0180.c200.0000
10 al 15	BSSID	N/D
16 al 21	Dirección MAC origen	0001.c9bc.d901
22 y 23	Control de Secuencia	N/D
ENCABEZADO LLC		
24	DSAP	N/D
25	SSAP	N/D
26	Control	N/D
27 al 29	Código Organizacional	0x000000
30 y 31	Tipo	0x0800

Observación: Se obtienen los valores de los campos DSAP, SSAP, control y tipo, se tiene que establecer el direccionamiento del servidor RADIUS el cual autentica a RC y RW para que los dispositivos de sus redes tengan acceso vía TELNET a RC, se configura el modelamiento aaa en RC y encriptación AES en AP y dispositivos inalámbricos.

Equipo sin autenticar - Paquetes al acceder a servidor WEB

Tabla. 4.5. Análisis paquete PDU MAC WPA Enterprise-TKIP, sin autenticación

ENCABEZADO 802.11		
No. de Byte	**Campo (s)**	**Valor (es)**
0 y 1	Control del Paquete	N/D
2 y 3	Duración/ID	0x2e
4 al 9	Dirección MAC	0006.2a52.30ab

	destino	
10 al 15	BSSID	N/D
16 al 21	Dirección MAC origen	000d.bd89.b802
22 y 23	Control de Secuencia	N/D
ENCABEZADO LLC		
24	DSAP	0x42
25	SSAP	0x42
26	Control	0x03
27 al 29	Código Organizacional	0x000000
30 y 31	Tipo	0x0800

Observación: No existe gran variación en la PDU del paquete RADIUS, no se puede analizar el proceso de negociación del servidor hacia el solicitante, el software para el análisis de tráfico es bastante limitado, esta configuración está realizada con WPA Enterprise con cifrado AES, no se observa en los paquetes una variación notoria.

CAPÍTULO 5

5.1Conclusiones

La vulnerabilidad de las redes inalámbricas con los mecanismos de seguridad desarrollados por la IEE 802.11i para redes en modo infraestructura son casi nulos ya que mediante su encriptación y cifrado apoyados en servidores AAA, solamente permiten el ingreso a una red privada a los usuarios sobre los cuales se tengan configurados sus credenciales con sus respectivos permisos.

Para las redes Ad-Hoc la seguridad tiene un gran vacío ya que no existe un dispositivo de control o autenticador que valide la conexión de usuarios seguros.

El análisis de los mecanismos de seguridad permite visualizar la complejidad de las tramas que se transmiten para su validación, es decir, las llaves que se generan en los diferentes protocolos WPA, WPA2; cada mecanismo cuenta con una configuración específica que permite que la generación de llaves sea dinámico, se lo administre desde un servidor de autenticación externo.

Existen muchas soluciones en software para el desarrollo de topologías y ambientes controlados que facilitan el análisis de seguridad que sucede en la red, al mismo tiempo no existen simuladores que reflejen características completas de análisis, es decir, solamente se ven limitados a la configuración y análisis de tramas básicas que no dejan obtener datos completos para observar el intercambio de paquetes en una comunicación de seguridad.

A pesar de la configuración que permite el simulador Packet Tracer 5.3, no se obtuvieron resultados satisfactorios en cuanto a captura de tramas se refiere, el nivel de paquetes obtenidos es básico y no contiene toda la información de un análisis en ambiente real. Se analizaron diversas soluciones en software como la

potente herramienta que es GNS3 pero no cada solución no contiene los elementos activos necesarios para desarrollar las topologías como en este caso no cuenta con herramientas inalámbricas de simulación.

No se tiene una conclusión determinante de la evaluación de los mecanismos de seguridad por la limitante en software, la cual no permitió un análisis completo de cada mecanismo de seguridad.

5.2 Recomendaciones

En todo caso, siempre es recomendable implementar algún tipo de seguridad para que los datos de nuestra red no sean vulnerados.

Debido a los diferentes mecanismos de seguridad y los diferentes ambientes sobre los cuales implementarlos, se recomienda realizar un análisis sobre la red, ya que por ejemplo para la implementación de WPA2 sobre una empresa pequeña (cyber) resulta un poco costoso la adquisición de un servidor AAA o de una licencia que permita emular a dicho servidor; en cambo sería más eficiente implementar WPA Personal que facilita seguridad con solo la compartición de una clave.

En ambientes empresariales, se recomienda hacer uso de mecanismos ya sea hardware o software para la detección y protección contra ataques externos o propiamente internos, de esta forma se podrá identificar al atacante y con la configuración de una ACL sobre un equipo de borde se podrá mitigar dicho ataque.

El desarrollo de este proyecto es una base para simular un ambiente híbrido, es decir combinación de software y hardware que permita analizar completamente lo que sucede en un ambiente real de redes inalámbricas.

REFERENCIAS BIBLIOGRÁFICAS

[1] (s.f.). Obtenido de http://es.wikipedia.org/wiki/Espectro_ensanchado

[2] (s.f.). Recuperado el 09 de 2012, de http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

[3] (s.f.). (BUFFALO) Recuperado el 09 de 2012, de http://www.buffalo-technology.com/es/wireless-802-11-technologies.html

[4] (s.f.). (Acent White Pappers) Obtenido de http://www.acens.com/wp-content/images/whitepaper-redes-seguridad-acens-julio-2012.pdf

[5] (s.f.). (Corelan Team) Recuperado el 11 de 2012, de http://www.corelan.be:8800/index.php/2009/02/24/cheatsheet-cracking-wpa2-psk-with-backtrack-4-aircrack-ng-and-john-the-ripper/

[6] Balao, M. (17 de 03 de 2012). Recuperado el 09 de 2012, de http://martin.com.uy/sec/autenticacion-de-mensajes-cbc-mac/

[7] Cabrera E., C. (01 de 2009). Recuperado el 08 de 2012, de http://cesarcabrera.info/blog/explorando-el-sdm-con-gns3/

[8] Cano Baños, M. D., & López Martínez, N. (s.f.). Recuperado el 10 de 2012, de http://ocw.bib.upct.es/pluginfile.php/6726/mod_resource/content/1/Practica2.pdf

[9] Filippetti, M. (s.f.). *www.youtube.com*. Recuperado el 11 de 2012, de http://www.youtube.com/watch?v=OetSCVG-kN4

[10] Radvan, S. (05 de 2010). Recuperado el 08 de 2012, de http://docs.fedoraproject.org/es-ES/Fedora/13/html-single/Wireless_Guide/index.html

[11] Yanover, D. (13 de 01 de 2005). Recuperado el 07 de 2012, de http://www.mastermagazine.info/articulo/3123.php

[12] *IDG.es*. (01 de 07 de 2005). Recuperado el 07 de 2012, de http://www.networkworld.es/Seguridad-WLAN-802.11i-_Pros-y-contras/seccion-/articulo-169579

[13] (14 de 07 de 2010). (UNEFA Curso de Comunicaciones) Recuperado el 07 de 2012, de https://sites.google.com/site/unefacursodecomunicaciones/sistemas--de-espectro-expandido

[14] (13 de 07 de 2011). (Buenas Tareas) Recuperado el 08 de 2012, de http://www.buenastareas.com/ensayos/Sistema-De-Espectro-Expandido-Teor%C3%ADa-De/2541392.html

[15] (2011). (Comunidad Digital de Conocimiento) Recuperado el 09 de 2012, de http://cursoslibres.academica.mx/206/seguridad-en-redes/3-protecciones-y-herramientas-de-seguridad/servicios-aaa

[16] *wikipedia.org*. (30 de 10 de 2012). Recuperado el 10 de 2012, de http://es.wikipedia.org/wiki/IEEE_802.11

[17] *es.kioskea.com*. (02 de 2013). Recuperado el 02 de 2013, de http://es.kioskea.net/contents/wifi/wifirisques.php3

[18] Abreu, J. J. (s.f.). Recuperado el 09 de 2012, de http://www.urbe.edu/publicaciones/telematica/indice/pdf-vol6-2/1-ponencia6-2-estudiofactibilidad.pdf

[19] Alapont Miquel, V. (s.f.). Recuperado el 09 de 2012, de http://www.uv.es/~montanan/ampliacion/trabajos/SeguridadWireless.pdf

[20] Buettrich, S., & Escudero Pascual, A. (07 de 2007). Recuperado el 10 de 2012, de http://www.it46.se/courses/wireless/materials/es/04_Topologia-Infraestructura/04_es_topologia-e-infraestructura_guia_v01.pdf

[21] Daniel. (24 de 11 de 2007). *Formatoweb.com.ar*. Recuperado el 10 de 2012, de http://www.formatoweb.com.ar/blog/2007/11/24/el-sistema-de-cifrado-wep/

[22] de Miguel Ponce, E. (s.f.). Recuperado el 08 de 2012, de http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

[23] *dns.bdat.net*. (s.f.). Recuperado el 10 de 2012, de http://dns.bdat.net/seguridad_en_redes_inalambricas/x38.html

[24] Ernesto. (07 de 2008). Recuperado el 11 de 2012, de http://aprenderedes.com/2008/07/autenticacion-y-asociacion-wlan/

[25] Gast M. (2003). Recuperado el 10 de 2012, de http://flylib.com/books/en/2.519.1.49/1/

[26] *http://es.scribd.com/doc/63129589/Vision-general-de-un-sistema-de-video-en-red#*. (s.f.). Obtenido de http://es.scribd.com/doc/63129589/Vision-general-de-un-sistema-de-video-en-red#.

[27] *http://salomonrt.wordpress.com/tag/ventajas-de-red-por-cable-contra-red-inalambrica/*. (s.f.). Obtenido de http://salomonrt.wordpress.com/tag/ventajas-de-red-por-cable-contra-red-inalambrica/.

[28] *ipsimulator.googlecode.com*. (s.f.). Recuperado el 10 de 2012, de https://ipsimulator.googlecode.com/svn/simuladores%20actuales.pdf

[29] Lazo García, N. A. (01 de 08 de 2012). (Respositorio Digital PUCP) Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/123456789/1445

[30] Mendoza Acevedo, E. (04 de 2005). Recuperado el 11 de 2012, de http://mixteco.utm.mx/~resdi/historial/Tesis/Tesis_Emmanuel.pdf

[31] Pellejero, I., Andreu, F., & Lesta, A. (s.f.). *www.enpresadigitala.net*. (Sociedad para la Promoción y Reconversión Industrial) Obtenido de www.euskadinnova.net/documentos/303.aspx

[32] Perez Crespo, J. (09 de 02 de 2005). Recuperado el 11 de 2012, de http://blackspiral.org/docs/pfc/itis/node12.html

[33] Varea, F. (s.f.). *monografías.com*. Recuperado el 09 de 2012, de http://www.monografias.com/trabajos14/segur-wlan/segur-wlan.shtml

[34] *www.cisco.com*. (s.f.). (CISCO systems) Recuperado el 10 de 2012, de http://www.cisco.com/en/US/docs/routers/access/wireless/alolh/sp/sec_2.htm

[35] *www.galeon.com*. (s.f.). Recuperado el 08 de 2012, de http://ieeestandards.galeon.com/aficiones1573579.html

Sangolquí ___ de Marzo del 2013

_____

Ing. Darío Duque

Director de la Carrera

Ingeniería Electrónica y Telecomunicaciones

_____

Sr. Josué Conrado M.

Autor