DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA,
REDES Y COMUNICACIÓN DE DATOS

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORES:
MILTON LEONARDO ARGUELLO RAMOS
ANDRÉS ALEJANDRO VACA VILLARREAL

TEMA: "HERRAMIENTAS Y TÉCNICAS DE MONITORIZACIÓN DE TRAFICO IEEE 802.11 A B G N MULTICANAL"

DIRECTOR: ING. ROMERO, CARLOS
CODIRECTOR: ING. SAENZ, FABIAN

SANGOLQUÍ, ENERO DEL 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

CERTIFICADO

Ing. Carlos Romero G.
Ing. Fabián Sáenz E.

CERTIFICAN

Que el trabajo titulado ¨Herramientas y Técnicas de Monitorización de Tráfico IEEE 802.11 A B G N Multicanal¨, realizado por Milton Leonardo Arguello Ramos y Andrés Alejandro Vaca Villarreal, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la Universidad de las Fuerzas Armadas ESPE en su reglamento.

Debido a que se trata de un trabajo de investigación recomiendan su publicación.
El mencionado trabajo consta de un documento empastado y un disco comparto en cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Milton Leonardo Arguello Ramos y Andrés Alejandro Vaca Villarreal que lo entreguen al Doctor Nikolai Espinosa, en su calidad de Coordinado de la Carrera.

Sangolquí, 28 de enero del 2015.

_____	_____
Ing. Carlos Romero G.	Ing. Fabián Sáenz E.
DIRECTOR	**CODIRECTOR**

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

DECLARACIÓN DE RESPONSABILIDAD

Milton Leonardo Arguello Ramos
Andrés Alejandro Vaca Villarreal

DECLARAMOS QUE:

El proyecto de grado denominado ¨Herramientas y Técnicas de Monitorización de Trafico IEEE 802.11 A B G N Multicanal¨, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas cuyas fuentes se incorporan en las referencias bibliográficas.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto en mención.

Sangolquí, 28 de enero de 2015.

_____ _____

Milton Leonardo Arguello Ramos Andrés Alejandro Vaca Villarreal

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Nosotros, Arguello Ramos Milton Leonardo y Vaca Villarreal Andrés Alejandro

Autorizamos a la Universidad de las Fuerzas Armadas – ESPE la publicación, en la biblioteca virtual de la Institución del trabajo ¨Herramientas y Técnicas de Monitorización de Trafico IEEE 802.11 A B G N Multicanal¨, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 28 de enero de 2015.

_____	_____
Milton Leonardo Arguello Ramos	Andrés Alejandro Vaca Villarreal

DEDICATORIA

El presente proyecto se lo dedico a Dios y a la Virgen Dolorosa quienes han sido mi protección y mi guía durante toda la vida, a toda mi familia en especial a mi Madre, mi Padre y mi hermana, por apoyarme todo este tiempo, con su cariño, consejos y sobre todo con su paciencia para poder alcanzar mis metas planteadas. A mi tío abuelo, Padre Julián Bravo, que aunque no me acompaña en este momento, fue mi guía tanto espiritual como emocional y sé que desde el cielo hizo que esto que hoy culmino se pueda hacer realidad.

Andrés Alejandro Vaca Villarreal

Porque cada día me han bendecido y apoyado para seguir adelante luchando dedico este proyecto a Dios, mis padres, mis hermanos toda mi familia. Hubo momentos en que descuidaba mucho el lograr esta meta pero día a día mis padres mi hermanos me aconsejaron me dieron aliento y muchas fuerzas para cumplirla y tan solo digo que sus palabras no quedaron en el olvido todo lo que me enseñaron y me apoyaron se encuentra plasmado en este proyecto. Muchas gracias familia por ayudarme en esta meta.

Milton Leonardo Arguello Ramos

AGRADECIMIENTO

Primero agradezco a Dios por permitirme un día más de vida y haberme concedido culminar una etapa en mi vida. A mi madre Elizabeth por su paciencia pos su comprensión y apoyo. A mi Padre Víctor que aunque tengamos diferencias muy marcadas hemos sabido sobrellevar la situación y me ha sabido aconsejar en lo que se ha podido, a mi Hermana Majo que aunque nos peleemos a ratos, sabe que la quiero y que espero pronto culmine su carrera. A mi bis Abuelito Saulo que siempre ha estado preocupado por nosotros.

Agradezco también a mi Abuela Bachita por todo su apoyo incondicional, a mis tíos Pato, Paty, a mis primos Luis, Juan por ser mi otra familia y mi apoyo en los momentos difíciles.

A mis profesores de la Universidad en especial al Ing. Carlos Romero quien nos ha apoyado en esta etapa y confió en nosotros para poder desarrollar esta tesis, al Ing. Darwin Aguilar quien con su amistad supo guiarme y aconsejarme tanto en la vida estudiantil como uno que otro consejo personal.

Finalmente y no menos importante quiero agradecer a todos mis amigos, Pato, Astu, Filo, Lore, Adrián, Troyita, Ricardo, Pozito, Diana, Miguel y Pitbull con quienes me formé en la Universidad y con quienes viví inolvidables experiencias que serán muy difíciles de olvidar, a Leonardo, Daniel, Alexandra, compañeros de trabajo quienes me han apoyado con sus palabras y consejos para que culmine una etapa más de mi vida.

Gracias a todas las personas que de una u otra forma fueron parte de mi vida y aportaron con un granito de arena para que este sueño y meta se vuelva realidad.

Andrés Alejandro Vaca Villarreal

A Dios, mi madre Piedad mi padre Humberto mis hermanos Fabián, Marco, Holguer, Lidia mi cuñado Guido mis cuñadas Paty Pao mis sobrinos en especial Liz en quienes he pensado mucho durante la elaboración de esta tesis les agradezco porque me han dado siempre el apoyo me han contagiado con sus alegrías con sus buenos deseos y han sido muy comprensibles y sobretodo pacientes para que pueda cumplir y culminar esta etapa de mi vida.

A mi tío Atu y Lalita quienes siempre han sido un ejemplo y me han brindado sus consejos y su ayuda incondicional muchas gracias.

Agradezco al Inge Carlos Romero porque ha sido un profesor que ha dedicado su tiempo, sus conocimientos, su comprensión y su paciencia para culminar este proyecto. Al Inge Aguilar con quien me ha brindado su amistad sus consejos y es con quien hemos compartido algunos momentos chéveres durante la universidad.

De igual manera a mis amigos Pato, Andrés, Astu, Lore, Troya, Adrián, Ricardo, Kari, Danilox, Pozito, Diana, Miguel y Pitbull con quienes he compartido los mejores momentos de la universidad y quienes han estado en las buenas y malas de mi vida.

A Rubén y Hoover con quienes trabaje y pase muchas anécdotas.

De igual manera agradezco al Doc. Edison Almeida a quien conocí durante una etapa difícil de mi vida y quien mediante sus palabras y guía me ha brindado mucha ayuda y he podido salir adelante.

Muchas gracias a todas las personas que durante esta etapa de mi vida formaron parte de ella.

Milton Leonardo Arguello Ramos

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En los últimos años se ha evidenciado un crecimiento elevado en el uso de redes inalámbricas, gracias a las ventajas presentadas sobre redes cableadas, como la movilidad, escalabilidad, entre otras. Estas redes inalámbricas se usan tanto en el hogar como en una oficina y es aquí donde un administrador de red necesita técnicas y herramientas para poder verificar el comportamiento de su red y poder brindar a sus usuarios un servicio bueno, asegurando tanto velocidad de transmisión como seguridad y conectividad. Con el estudio de diferentes herramientas y el planteamiento de diferentes escenarios, se desarrollarán técnicas y procedimientos para poder analizar el comportamiento del tráfico IEEE 802.11. Se utilizará el adaptador AirPcap Nx que nos permitirá capturar tráfico monocanal y multicanal, Wireshark que nos permitirá visualizar los paquetes del tráfico de los escenarios y obtener mediante filtros datos del comportamiento de la red, Cascade Pilot (SteelCentral Packet Analyzer) que nos permite realizar filtros y generar reportes del análisis realizado. Se generará tráfico mediante D-ITG para poder estudiar el comportamiento del canal en diferentes ambientes.

La implementación de los escenarios se la hará en 3 fases, fase 1, se realizará la familiarización de las tarjetas AirPcap con el monitoreo en monocanal y multicanal, fase 2, nos centraremos en un canal específico y verificaremos la utilidad de las herramientas y por último la fase 3, implementaremos escenarios con aplicaciones comunes en las que verificaremos QoS, Roaming, Interferencia, etc.

PALABRAS CLAVES

1. Herramientas y Técnicas
2. Análisis Multicanal
3. AirPcap Nx
4. Wireshark
5. D-ITG

ABSTRACT

In recent years there has been an increase in the use of wireless networks, thanks to the advantages presented on wired networks, such as mobility, scalability, among others. These wireless networks are used both at home and in an office and this is where a network administrator need techniques and tools to verify the performance of its network and to provide users with good service, ensuring both transmission speed and security and connectivity. By studying different tools and approach different scenarios, techniques and procedures to analyze traffic behavior will develop IEEE 802.11. The AirPcap Nx adapter that will allow us to capture single and multichannel traffic, Wireshark will allow us to display the packets traffic scenarios and data obtained by filtering network behavior, Cascade Pilot (SteelCentral Packet Analyzer) that allows us to use filters and generate analysis reports. Traffic is generated by D-ITG to study the behavior of the channel in different environments. The implementation of the scenarios will make it into 3 phases, Phase 1, familiarization of AirPcap cards with single and multichannel monitoring, phase 2 will take place we will focus on a specific channel and verify the usefulness of the tools and finally phase 3, implement scenarios with common applications that will verify QoS, Roaming, interference, etc.

KEYWORDS

6. 1. Tools and Techniques
7. 2. Multichannel Analysis
8. 3. AirPcap Nx
9. 4. Wireshark
10. 5. D-ITG

ANTECEDENTES

En nuestra era han surgido los adictos a la información, gente que necesita estar todo el tiempo en línea (conectador a la red). Para estos usuarios móviles, el cable de par trenzado, el cable coaxial y la fibra óptica no son tan útiles. Ellos necesitan obtener datos para sus computadoras, laptop, notebook, dispositivos de bolsillo, de mano o reloj pulsera, sin estar limitados a la infraestructura de comunicaciones terrestre. Para estos usuarios, la comunicación inalámbrica es la respuesta.

Muchas personal creen que en el futuro existirán 2 clases de comunicación: de fibra óptica e inalámbrica. Todos los dispositivos fijos como computadoras, teléfonos, faxes, etc., se conectarán con fibra óptica, esto quiere decir que serán una conexión física, en cambio todos los aparatos móviles usarán comunicación inalámbrica.

Sin embargo, la comunicación inalámbrica tiene muchas ventajas para los dispositivos fijos en ciertas circunstancias. Por ejemplo, si no es factible tender fibra óptica hasta un edificio debido a la dificultad de acceso a un terreno (montañas, selvas, pantanos, etc.), una opción factible podría usar un sistema inalámbrico.

Las LAN inalámbricas son sistemas en los que cada computadora tiene un módem de radio y una antena mediante los que se puede comunicar con otros sistemas. Las LAN inalámbricas se están haciendo cada vez más comunes en los hogares y oficinas pequeñas, donde instalar tecnología Ethernet se considera muy problemático o costoso, así como en oficinas ubicadas en edificios antiguos, cafeterías de empresas, salas de conferencias y otros lugares. Para hacer uso de esta tecnología surgió el estándar IEEE 802.11, que la mayoría de los sistemas implementa y que se ha extendido ampliamente.

En 1999 IEEE (The Institute of Electrical and Electronics Engineers) definió el primer estándar, IEEE 802.11, para la regulación de las redes de área local inalámbricas. Este estándar proporciona tasas de transmisión entre 1 y 2 Mbps, en la banda de los 2,4 GHz, y soporta medios de transmisión: por infrarrojos y por radiofrecuencia. En este último caso se tiene dos tipos de transmisiones por espectro ensanchado: Frequency Hopping Spread Spectrum (FHSS) y Direct Sequence Spread Spectrum (DSSS). Desde su nacimiento, dicho estándar ha evolucionado dando lugar a diferentes estándares. Por un lado se encuentra el IEEE 802.11b, que permite tasas de transmisión de 1, 2, 5,5 y 11 Mbps en la misma banda de frecuencias, utilizando radiofrecuencia con tecnología DSSS. Por otro lado apareció IEEE 802.11a, que alcanza tasas de transmisión de 54 Mbps, pero en la banda de frecuencia de 5 GHz. Sin embargo, en junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, este utiliza la banda de 2,4 GHz (al igual que 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, esto debido a que puede operar con las Tecnologías RF DSSS y OFDM. El estándar actual es 802.11n el cual fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física, 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).

En base al costo, facilidad de implementación así como la movilidad de estaciones de trabajo que nos permite el estándar IEEE 802.11, varias empresas, escuelas, colegios y universidades optan por migrar a este tipo de tecnología y por ende los administradores de red tienen como obligación mantener la operatividad de la misma. Para lograrlo utilizan herramientas y técnicas de análisis de red [6], las mismas que permiten la optimización de red, la detección de ataques y reflejan el comportamiento de la red ante presencia de obstáculos, ruidos, interferencia de otros dispositivos

generadores de radiofrecuencia, cobertura y capacidad de los medios para que los usuarios accedan a la red.

Los métodos de análisis de red se basan en el monitoreo de tráfico y son enfocados específicamente al análisis de tráfico generado en un solo canal esto se da debido a que los dispositivos de acceso al medio de tipo SISO son muy utilizados en este tipo de redes por el mismo hecho de ser económicos, fáciles de configurar e instalar, pero la evolución continua de la tecnología ha permitido la fabricación de dispositivos MIMO los cuales tiene la funcionalidad de proporcionar conectividad a través de varios canales de radiofrecuencia, por ende su costo y configuración aumentan.

Los estándares IEEE802.11 a/b/g/n soporta dos tipos de topologías: redes con infraestructura y redes ad-hoc. En las redes con infraestructura se tiene una estación que actúa como punto de acceso, coordinando el comportamiento de la red. Esta topología puede funcionar bajo dos mecanismos: en modo DCF (Distributed Coordination Function) o PCF (Point Coordination Function). El primero de ellos se basa en el protocolo CSMA/CA (Carrier Sense Medium Access/Collision Avoidance), y presenta dos técnicas para la transmisión de paquetes: el modo básico y el RTS/CTS. Por otro lado, el mecanismo PCF utiliza una estación de la red como coordinadora de las demás estaciones. Dicha estación será la encargada de dar permisos a las demás, para que éstas puedan transmitir datos.

Las redes ad-hoc están formadas por un grupo de estaciones inalámbricas, que comparten una misma área de cobertura y operan en modo DCF. Estas estaciones, a través de sus tarjetas de red inalámbrica, forman una red de área local. Estas redes se caracterizan por su gran simplicidad, pero presentan algunas desventajas, como su limitada cobertura y el hecho de tratarse de redes aisladas, sin posibilidad de comunicación con otras.

JUSTIFICACION E IMPORTANCIA

Las herramientas y técnicas para el análisis de tráfico de red son de gran utilidad para los administradores de red debido a que permiten la optimización de la misma, la detección de ataques de red reflejan el comportamiento de la red ante presencia de obstáculos, ruidos, interferencia de otros dispositivos generadores de radiofrecuencia, cobertura y capacidad de los medios para que los usuarios accedan a la red.

Los métodos de análisis de red se basan en la monitorización de tráfico y son enfocados específicamente al análisis de tráfico generado en un solo canal, esto se da debido a que los dispositivos más utilizados para el acceso a la red son de tipo SISO por ser económicos y fáciles de configurar e instalar; pero actualmente existen dispositivos de tipo MIMO los cuales tienen la funcionalidad de proporcionar conectividad a través de varios canales de radiofrecuencia, por ende su costo y configuración aumentan; también los entornos de red en los que se mantiene un monitoreo son muy variados y existen casos en los cuales tenemos varios punto de acceso de red inalámbrica y el monitorearlos se vuelve difícil y costoso debido a que esto conllevaría a llevar una monitorización específica para cada Access Point.

Nuestro estudio se centra en utilizar herramientas y técnicas para el análisis de tráfico multicanal a nivel de capa física y enlace de datos y nos permita determinar cuál es el comportamiento de la red. Monitorizar una red es importante en un entorno de trabajo ya que se logra optimizar la red inalámbrica y se tiene diferentes aspectos que van a permitir un buen desempeño de la red, tales como aspectos de la ubicación de los usuarios con respecto a los AP (Access Point), valor de Throughput, valores de Back off, los mismos que son muy variables ya que puede existir problemas de interferencia, presencia de ruido, cobertura influencia del tamaño de los paquetes, parámetros de configuración de los dispositivos (uso del protocolo RTS/CTS o acceso básico, tamaño de la ventana de contienda inicial, tasas

de transmisión) como el efecto del número de dispositivos que conforman la red los mismos que afectan el funcionamiento de la red.

OBJETIVOS

GENERAL

- Validar herramientas y técnicas para el análisis de redes inalámbricas (802.11) usando los diferentes estándares (a, b, g, n) en base al análisis de tráfico multicanal a nivel de capa física y enlace de datos del modelo OSI con el fin de determinar y analizar los posibles riesgos producidos por interferencias o ruido dentro de una red implementada en dicho estándar.

ESPECÍFICOS

- Investigar el funcionamiento del estándar IEEE 802.11 así como técnicas intrusivas y no intrusivas presentes actualmente para este estándar.
- Investigar la funcionalidad de las tarjetas AirPcap Nx Adapter a fin de emplear la propagación y captura de tráfico de red multicanal así como las herramientas y técnicas de análisis de tráfico disponibles para el estándar IEEE 802.11.
- Diseñar e implementar escenarios de prueba los que permitirán realizar el análisis de tráfico multicanal de una red inalámbrica implementada en los estándares IEEE802.11 a/b/g/n.
- Analizar el tráfico multicanal de la capa física y de enlace de datos del Modelo OSI, utilizando software Commview, Cascade Pilot, Aircrackng y configuraciones de la estaciones en el escenario de pruebas.
- Establecer en base al análisis realizado las herramientas y técnicas de captura de tráfico multicanal útiles para el estándar 802.11

CAPITULO 1

1. FUNDAMENTO TEÓRICO ESTANDAR 802.11

1.1. REDES WLAN

El término WLAN conocido en inglés como Wireless Local Area Network, o en español como Redes de Área Local Inalámbrica, son el tipo de redes que nos proporcionan un sistema de comunicación muy flexible ya que se elimina la utilización de cables, aunque se debe tener en cuenta que la utilización de redes inalámbricas no intenta suplantar por completo a las redes cableadas ya que sirve como un complemento a la misma, haciendo extensiones en la red en la cual se quiere brindar un servicio. Las redes inalámbricas permiten una mayor movilidad por parte de los usuarios ya que usa una tecnología de radiofrecuencia, con esto ya que no es necesario estar físicamente conectados a la red para poder tener acceso a la misma, con todos estos beneficios podemos desplazar nuestros equipos a diferentes lugares atendiendo así nuestras necesidades. Este tipo de redes han alcanzado introducirse en muchos campos entre ellos tenemos al de la medicina, ventas, ingeniería, manufacturación, almacenes, etc., de modo que esta manera de acceder a una red o de acceder a un servicio de la red ya no es difícil de una manera inalámbrica (García Galende).

El uso de estas redes se ha vuelto muy popular en los hogares para compartir el acceso a Internet entre varias computadoras, actualmente, incluso el uso de este tipo de redes se ha incrementado en los diferentes lugares en donde se tiene una concurrencia alta de gente como son lugares comerciales o centros de exposiciones en los cuales administradores de la red o las personas que implementan este servicio, buscan que los usuarios tengan una experiencia más agradable en donde puedan también sentir seguridad, rapidez y que sea de fácil el acceso a los servicios que una red inalámbrica puede ofrecer.

Para implementar una red inalámbrica se debe tener presente diferentes factores importantes como una Alta disponibilidad, Escalabilidad, Gestionabilidad y Arquitectura abierta, los cuales harán que dentro de la red Inalámbrica que se implemente no se tenga inconvenientes de desconexión o de seguridad.

Las redes inalámbricas al igual que las redes cableadas, requieren de un medio físico por el cual pasan las señales de transmisión. Las WLANs utilizan luz infrarroja (IR[1]) o frecuencias de radio (RF[2]), en el caso de la utilización de RF es mucho más popular su uso debido a su mayor alcance, mayor ancho de banda y una cobertura mayor. Las WLANs utilizan las bandas de frecuencia de 2,4 GHz y 5 GHz, en la mayoría de partes del mundo estas dos porciones del espectro de Radio Frecuencia están reservadas para dispositivos sin licencia (Cisco Networking Academy).

El término de Wireless LAN o WLAN son usados para indicar una red de área local inalámbrica, ejemplo, una red entre dos o más estaciones que usa radio frecuencia en vez de una comunicación cableada.

1.1.1. Características Generales

- Muchos usuarios y empleados de empresas requieren para realizar sus tareas, acceder en forma remota a sus archivos, trabajos y recursos. La red Wireless permite hacerlo sin realizar ninguna tarea compleja de conexión o configuración y evita que cada usuario se traslade hasta su puesto de trabajo para poder acceder a los recursos de su red de datos.
- Escalable
- Simple de Instalar
- Menos compleja en su administración
- Adaptable a casi cualquier entorno físico para su implementación

[1] IF.- Tecnología Infrarrojo
[2] RF.- Tecnología de Radio Frecuencia

- Puede disponerse de conexión a Internet casi en cualquier lugar donde se cuente con un servidor con tal servicio siempre y cuando se tome en cuenta las distancias para la conexión y asociación a un AP.

1.1.2. Beneficios y Desventajas

En la actualidad la mayoría de negocios e instituciones por lo general ya tienen implementada una red de comunicación interna, la cual de ser inalámbrica presentaría muchas ventajas y comodidad para los usuarios de la misma.

Beneficios

- Las redes inalámbricas no reemplazan las soluciones “cableadas”, las complementa, ya que proporcionan conectividad de red en áreas en las que es complicado establecer una red cableada tales como lugares de trabajo temporales (Aguero Calvo).
- La movilidad es uno de los factores más importantes que presenta este tipo de redes ya que permite obtener la información o acceder a un servicio en tiempo real en cualquier parte de la empresa o del lugar donde se haya implementado la red siempre y cuando se esté dentro del área de cobertura de la red.
- La facilidad de la instalación es otro beneficio que presenta este tipo de redes ya que no se necesita realizar trabajos adicionales como en la instalación de una red cableada como es el cableado estructurado o la colocación de cables por muros o techos (García Galende).
- El Desplazamiento, a más de poder acceder a aplicaciones y servicio que nos brinde la red inalámbrica, también tendremos la tranquilidad de desplazarnos sin perder la comunicación, nos brinda comodidad y también una facilidad de trabajo (Bedoya & Medina, 2010).
- La flexibilidad en su uso, es otro aspecto que importa mucho en la implementación de una red inalámbrica, ya que se puede tener una conexión a la red sin tener la presencia de cables, por lo tanto en

lugares incómodos o que no fáciles de acceder este tipo de redes es muy útil. También se puede usar este tipo de redes en lugares donde el uso de los servicio sea de una manera esporádica, para poder evitar la utilización de cables (García Galende).

- La escalabilidad que presenta este tipo de redes cuando se presenta un cambio en la topología se lo realiza de forma sencilla y el trato es igual en redes pequeñas como en redes de mayor tamaño. Si se desea expandir la red inalámbrica a comparación con la red cableada es mucho más fácil ya que no debemos pensar por donde irá el nuevo cableado para aquel punto de red, sino solo nos preocupamos que esté en el área de cobertura para que pueda acceder a los servicios que brinde la red inalámbrica (García Galende).

Desventajas

- No existen estudios certeros sobre la peligrosidad o no, de las radiaciones utilizadas en las redes inalámbricas (Bedoya & Medina, 2010).
- Seguridad: Pueden llegar a ser redes inseguras, ya que cualquier usuario que esté cerca podría acceder a la red, para evitar este inconveniente se debe usar las suficientes técnicas de seguridad para poder implementar un sistema de seguridad y que sean más difícil hackearlas[3].
- Velocidad: Las redes inalámbricas presentan una velocidad menor de transmisión en comparación con las redes cableadas ya que se tiene una velocidad de 11 Mbps y 54Mbps.
- Inversión Inicial: Tiene un precio elevado al inicio lo cual provoca que por parte de los usuarios se perciba un alejamiento para su uso en entornos profesionales. La inversión en la que se tiene más costo es la seguridad de la red inalámbrica y es esta seguridad que hace que

[3] Hackear.- Acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.

una red inalámbrica sea aprovechada en su totalidad, brindando tranquilidad a sus usuarios.

- Interferencia: Las redes inalámbricas funcionan utilizando el medio radio eléctrico en la banda de 2,4 GHz, al no ser una banda que necesita licencia administrativa para su uso, existen diversos dispositivos que usan esta misma banda por lo que generan interferencias. Por lo tanto la red inalámbrica no funcionará en su más alto rendimiento (Bedoya & Medina, 2010). Cuando mayor sean los equipos que produzcan estas interferencias, menor será el rendimiento de nuestra red.
- Alcance: la determina la potencia de los equipos y la ganancia de las antenas, por lo cual existirá áreas en la que la cobertura no sea toral en la localidad física.

1.1.3. Dispositivos compatibles con el Estándar

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica el cual pudiera ser compatible entre los distintos dispositivos que el mercado tenía pensado desarrollar. En la búsqueda esta compatibilidad entre los dispositivos fue que en 1999 las empresas 3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies, se reunieron para crear la WECA[4] (Wireless Ethernet Compatibility Alliance), por sus siglas en inglés, que en la actualidad se las llama Wi-Fi Alliance.

El objetivo de la misma fue designar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta forma, en el mes de abril del año 2000 la WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, y le bautiza con el nombre de Wi-Fi (Wireless Fidelity). Esto quiere decir que el usuario tiene la total garantía de que todos los equipos que tengan el sello Wi-Fi

[4] WECA.- Alianza de Compatibilidad de Tecnología Ethernet - Inalámbrica

pueden trabajar juntos sin problemas, siendo totalmente independientemente el fabricante de cada uno de ellos.

Existen varios dispositivos Wi-Fi, los cuales se pueden dividir en dos grandes grupos: Dispositivos de Distribución o Red, entre los que destacan los routers, puntos de acceso y Repetidores; y Dispositivos Terminales que en general son las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB (SERVERCOMP Computing Systems).

- **Dispositivos de Distribución o Red:**
  - Los puntos de acceso son dispositivos que generan un "set de servicio", que podría definirse como una "Red Wi-Fi" a la que se pueden conectar otros dispositivos. Los puntos de acceso permiten, en resumen, conectar dispositivos en forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red para generar redes de una cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal y se pueda tener una recepción más óptima.
  - Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica, éstos se conectan a una red existente que tiene señal más débil y crean una señal limpia a la que se pueden conectar los equipos dentro de su alcance. Algunos de ellos funcionan también como punto de acceso.
  - Los Routers inalámbricos son dispositivos compuestos, especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen, un Router (encargado de interconectar redes, por ejemplo, nuestra red del hogar con internet), un punto de acceso y generalmente un switch que permite conectar algunos equipos vía cable (Ethernet y USB), esto se lo ocupa con mayor frecuencia en un lugar como oficinas donde se necesita diferenciar el tráfico de la red o simplemente conectar de forma

cableada diferentes dispositivos para poder adquirir un mismo servicio. Su tarea es tomar la conexión a internet, y brindar a través de ella acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.

- **Dispositivos Terminales**

El Wifi puede ser desactivado por un dispositivo terminal.

- Las tarjetas PCI[5] para Wi-Fi se agregan o vienen de fábrica en los ordenadores de escritorio. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.
- Las tarjetas PCMCIA[6] son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en el desuso, debido a la integración de tarjeta inalámbricas internas en estos ordenadores. La mayor parte de estas tarjetas solo son capaces de llegar a cubrir la tecnología B de Wi-Fi, no permitiendo por tanto disfrutar de una velocidad de transmisión demasiado elevada.
- Las tarjetas USB para Wi-Fi son el tipo de tarjeta más común que existe en las tiendas y más sencillo de conectar a un pc de escritorio o incluso a una portátil que no tenga una conexión Wi-Fi, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse incluso tarjetas USB con el estándar 802.11N (Wireless-N) que es el último estándar liberado para redes inalámbricas.
- También existen impresoras, cámaras Web y otros periféricos que funcionan con la tecnología Wi-Fi, permitiendo un ahorro de cableado, gran movilidad, lo cual dentro de una empresa o inclusive dentro del hogar, facilita el trabajo y la conexión con dichos dispositivos.

[5] PCI: Interconexión de componentes periféricos
[6] PCMCIA: Personal Computer Memory Card International Association

1.2. PROTOCOLO 802.11

La versión original del estándar IEEE 802.11 fue publicada en 1997 en la cual se especifica dos velocidades de transmisión teóricas de 1 y 2 megas bit por segundo (Mbits/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz, IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar también define como método de acceso al protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones). 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 (Metro Mexico, 2006).

1.2.1. Arquitectura

La norma 802.11 sigue el mismo modelo o arquitectura de la familia 802, es decir especifica la capa física y la subcapa MAC de la capa de enlace.

En la capa física se distinguen dos subcapas. La inferior llamada PMD[7], corresponde al conjunto de especificaciones de cada uno de los sistemas de trasmisión a nivel físico. La subcapa superior, PLCP[8] se encarga de homogenizar el tramado de cara a la capa MAC las peculiaridades de las diversas especificaciones de la subcapa PMD.

La subcapa MAC se especifica el protocolo de acceso al medio propiamente dicho, así como una serie de peculiaridades propias de redes inalámbricas como son el envío de mecanismos de encriptación para dar

[7] PMD.- Dependiente del Medio Físico, subcapa física 802.11
[8] PLCP.- Procedimiento de Convergencia de la Capa física, subcapa física 802.11

confidencialidad a los datos transmitidos (Wheelers Lane Technology College).

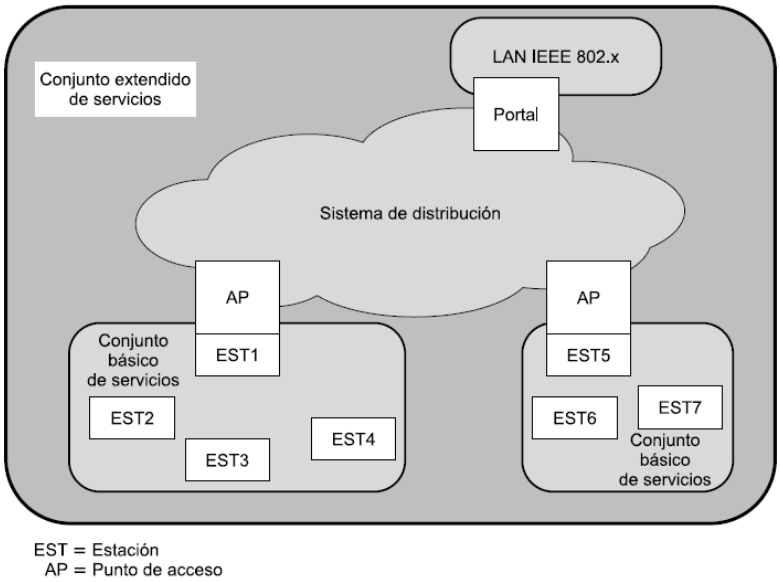


Figura 1-1 Arquitectura IEEE 802.11.

Un grupo de estaciones, en un área de cobertura llamada Área Básica de Servicios (BSA), dentro de la cual viene garantizada la interconexión y viene utilizada una única función de coordinación, forman un Conjunto Básico de Servicios(BSS). Por función de coordinación se entiende la función lógica que determina cuando una estación perteneciente al BSS puede transmitir o recibir sobre el medio de comunicación compartido, el aire (Navarro Gavira, 2005).

El estándar prevé dos funciones de coordinación: Función de Coordinación de Distribución (DCF) y Función de Punto de Coordinación (PCF), que se basa sobre un único nodo de coordinación. El estándar prevé que más BSS puedan ser conectadas con un Backbone[9] llamada Sistema de Distribución (DS) dentro de un Conjunto Extendido de Servicios (ESS), a través de un punto de acceso (AP).

[9] Backbone.- Red Principal que conecta las redes internas.

Un AP es una estación particular que proporciona una interfaz hacia el DS para las estaciones pertenecientes a una BSS. Todas las estaciones presentes en una BSS pueden comunicarse directamente entre ellas (Navarro Gavira, 2005).

Tabla 1 Términos IEEE802.11.

TERMINO	DEFINICIÓN
Punto de Acceso (AP)	**Cualquier entidad que tenga la funcionalidad de una estación y proporcione acceso al sistema de distribución a través del medio inalámbrico a las estaciones asociadas.**
Conjunto Básico de servicios (BSS)	**Conjunto de estaciones controladas por una sola función de coordinación.**
Función de Coordinación	**Función lógica que determina cuándo una estación funcionando dentro de un BSS tiene permiso para transmitir y puede recibir PDU.**
Sistema de Distribución (DS)	**Sistema utilizado para interconectar un conjunto de BSS y LAN Integradas para crear un ESS.**
Conjunto extendido de servicios (ESS)	**Conjunto de uno o más BSS interconectados y LAN integradas que aparece como un único BSS en la capa LLC de cualquier estación asociada con uno de tales BSS.**
Unidad de datos del protocolo MAC (MPDU)	**Unidad de datos intercambiada entre entidades MAC paritarias usando los servicios de la capa física.**
Unidad de datos del servicio MAC (MSDU)	**Información entregada como una unidad entre usuarios MAC.**
Estación	**Cualquier dispositivo que contenga capas físicas y MAC compatibles con IEEE802.11**

1.2.1.1. IBSS Red en modo Adhoc

En las redes IBSS, cada estación puede comunicar directamente con otra perteneciente a la misma BSS sin que el tráfico sea llevado hacia cualquier AP o a través de más estaciones intermedias. El concepto IBSS se avecina mucho a las características de una red ad-hoc, en cuanto a que su objetivo es aquel de hacer comunicar las estaciones directamente entre ellas, sin tener que acceder a redes dotadas de infraestructura (Navarro Gavira, 2005).

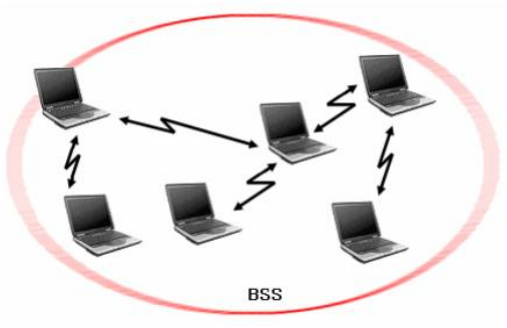


Figura 1-2 Red IBSSS.

1.2.1.2. Red Extendida ESS

Las redes ESS están formadas por muchas BSS interconectadas a través de un Sistema de Distribución, el cual puede ser realizado tanto con tecnología cableada como con tecnología sin cables. Este se ocupa de transferir al MAC la denominada MSDU[10] entre AP pertenecientes a diversas BSS. Esta tipo de red es necesaria con el fin de permitir la interacción entre terminales que no se encuentran al interno de la cobertura radio de un único BSS (Navarro Gavira, 2005).

[10] MSDU.- Unidad de Servicio de datos MAC

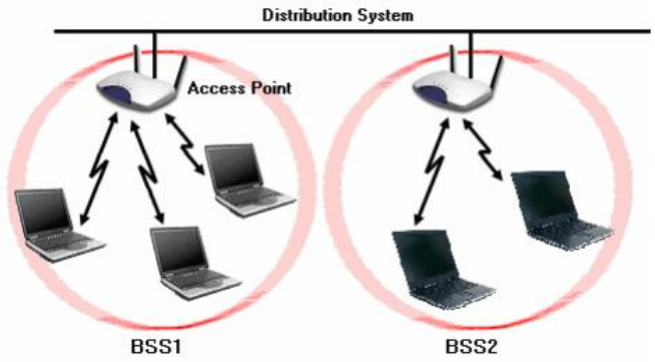


Figura 1-3 Red Extendidas ESS.

1.2.2. Servicios

El estándar 802.11 afirma que cada LAN inalámbrica que se apegue a él debe proporcionar nueve servicios. Éstos se dividen en dos categorías: cinco servicios de distribución y cuatro de servicios de estacin (Tanenbaum, 2003).

1.2.2.1. Servicio de Distribución

En contraste, los servicios de estación se relacionan con la actividad dentro de una sola celda.

Los cinco servicios de distribución son proporcionados por las estaciones y tienen que ver con la movilidad de la estación conforme entran y salen de las celdas, conectándose ellos mismos a las estaciones base y separándose ellos mismos de dichas estaciones. Estos servicios son los siguientes:

- **Asociación.** Este servicio es utilizado por las estaciones móviles para conectarse ellas mismas a las estaciones base. Por lo general, se utiliza después de que una estación se mueve dentro del alcance de radio de la estación base. Una vez que llega, anuncia su identidad y sus capacidades. Éstas incluyen las tasas de datos soportadas, necesarias para los servicios PCF (es decir, el sondeo), y los requerimientos de administración de energía. La estación base podría aceptar o rechazar la estación móvil. Si se acepta, dicha estación debe autenticarse (Tanenbaum, 2003).

- **Disociación**. Es posible que la estación o la estación base se disocie, con lo que se rompería la relación. Una estación podría utilizar este servicio antes de apagarse o de salir, pero la estación base también podría utilizarlo antes de su mantenimiento (Tanenbaum, 2003).
- **Reasociación**. Una estación podría cambiar su estación base preferida mediante este servicio. Esta capacidad es útil para estaciones móviles que se mueven de una celda a otra. Si se utiliza correctamente, no se perderán datos como consecuencia del cambio de estación base. (Pero 802.11, al igual que Ethernet, es sólo un servicio de mejor esfuerzo) (Tanenbaum, 2003).
- **Distribución**. Este servicio determina cómo enrutar tramas enviadas a la estación base. Si el destino es local para la estación base, las tramas pueden enviarse directamente a través del aire. De lo contrario, tendrán que reenviarse a través de la red cableada (Tanenbaum, 2003).
- **Integración**. Si una trama necesita enviarse a través de una red no 802.11 con un esquema de direccionamiento o formato de tramas diferentes, este servicio maneja la traducción del formato 802.11 al requerido por la red de destino (Tanenbaum, 2003).

1.2.2.2. Servicios de Estación

Se relacionan con la administración de membresías dentro de la celda y con la interacción con estaciones que están fuera de la celda. Se utilizan después de que ha ocurrido la asociación y son las siguientes (Tanenbaum, 2003):

- **Autenticación.** Debido a que las estaciones no autorizadas pueden recibir o enviar con facilidad la comunicación inalámbrica, una estación debe autenticarse antes de que se le permita enviar datos. Una vez que la estación base asocia una estación móvil (es decir, la ha aceptado en su celda), le envía una trama especial de desafío

para ver si dicha estación móvil sabe la clave secreta (contraseña) que se le ha asignado. La estación móvil prueba que sabe la clave secreta codificando la trama de desafío y regresándola a la estación base. Si el resultado es correcto, la estación móvil se vuelve miembro de la celda. En el estándar inicial, la estación base no tiene que probar su identidad a la estación móvil, pero se está realizando trabajo para reparar este defecto en el estándar (Tanenbaum, 2003).

- **Desautenticación.** Cuando una estación previamente autenticada desea abandonar la red, se des autentica. Después de esto, tal vez ya no utilice la red (Tanenbaum, 2003).
- **Privacidad.** Para que la información que se envía a través de una LAN inalámbrica se mantenga confidencial, debe codificarse. Este servicio maneja la codificación y la decodificación. El algoritmo de codificación especificado es RC4, inventado por Ronald Rivest del M.I.T (Tanenbaum, 2003).
- **Entrega de datos.** Por último, la transmisión de datos es la parte esencial, por lo que el 802.11 naturalmente proporciona una forma de transmitir y recibir datos. Puesto que el 802.11 está basado en Ethernet y no se garantiza que la transmisión a través de Ethernet sea 100% confiable, tampoco se garantiza que la transmisión a través del 802.11 sea confiable. Las capas superiores deben tratar con la detección y la corrección de errores (Tanenbaum, 2003).

1.2.3. IEEE802.11 MAC

El protocolo de la subcapa MAC para el estándar 802.11 es muy diferente del de Ethernet debido a la complejidad inherente del entorno inalámbrico en comparación con el de un sistema cableado. Con Ethernet, una estación simplemente espera hasta que el medio queda en silencio y comienza a transmitir. Si no recibe una ráfaga de ruido dentro de los primeros 64 bytes, con seguridad la trama ha sido entregada correctamente.

Esta situación no es válida para los sistemas inalámbricos (Tanenbaum, 2003).

La capa MAC se encarga de tres funciones principales: entrega confiable de datos, control de acceso y seguridad (Bernal I. , 2005).

1.2.3.1. Resolución de Colisiones

El protocolo CSMA/CA[11] pertenece a la clase de protocolos de acceso CSMA que efectúan un censado del canal antes de iniciar una transmisión. En el estándar 802.11, la capa física sondea el nivel de energía sobre la frecuencia radio para determinar si hay o no transmisión. Eso prevé que la capa física pruebe el canal de transmisión y proporcione esta información al protocolo MAC: la estación podrá transmitir sólo si el canal está libre, sino, esperará a que lo esté, buscando evitar de este modo las colisiones (Navarro Gavira, 2005).

A la clase de los protocolos CSMA pertenece también el CSMA/CD, utilizado en el estándar 802.3 y en todas las redes Ethernet cableadas, el cual prevé que una estación que está transmitiendo sobre el canal libre escuche aquello que efectivamente está sobre el canal: de hecho podría existir una colisión debida al hecho que dos o más estaciones hubiesen sentido el canal libre en el mismo momento. Sin embargo, el CSMA/CA del 802.11, a diferencia del CSMA/CD, no implementa la revelación de las colisiones por, al menos, dos motivos: la capacidad de percibir las colisiones requiere la posibilidad tanto de enviar como de recibir al mismo tiempo y eso puede ser costoso; pero más importante es el hecho que aunque se revelaran las colisiones y al momento del envío no revelara alguna, una colisión se podría verificar siempre al receptor (Navarro Gavira, 2005).

- **El problema de la atenuación (fading):** debido a la atenuación de la señal cuando se propaga a través del aire, dos estaciones pueden transmitir simultáneamente hacia el mismo nodo y provocar en el

[11] CSMA/CA: Carrier Sense Multiple Access / Collision Avoidance

receptor colisiones no advertidas (Navarro Gavira, 2005). Esto se esquematiza en el gráfico de la figura 1-4:

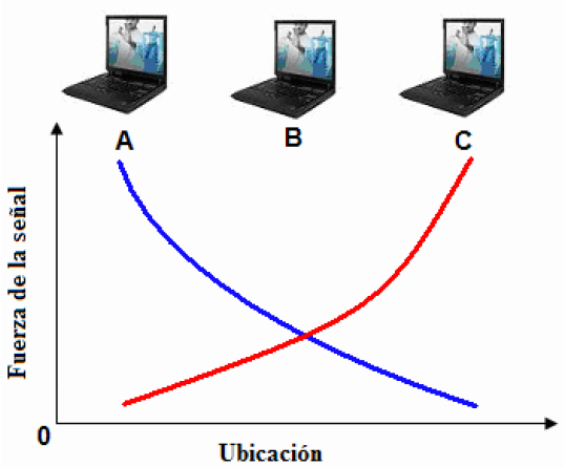


Figura 1-4 Fading.

- **El problema del terminal oculto (hidden terminal problem)**: los obstáculos físicos en el ambiente (por ejemplo una montaña) o la distancia pueden hacer que la estación A compruebe el canal, lo encuentre libre e inicie una transmisión hacia el nodo B que está ya recibiendo una trama desde otra estación C. A B le llegan dos paquetes desde nodos diferentes provocando así una colisión (Navarro Gavira, 2005).

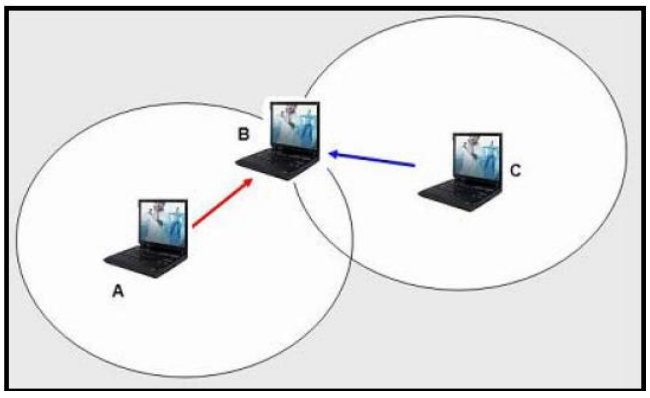


Figura 1-5 Nodo Escondido.

- **El problema de la estación expuesta (exposed node)**: haciendo referencia a la figura 1-6, se nota que B está transmitiendo una trama

a A; el nodo C (nodo expuesto) no puede transmitir hacia D porque siente el canal ocupado por la transmisión de B (se encuentra en su radio de acción), aunque su transmisión no creara una colisión en A (Navarro Gavira, 2005). Este problema lleva a una baja utilización de la banda disponible.

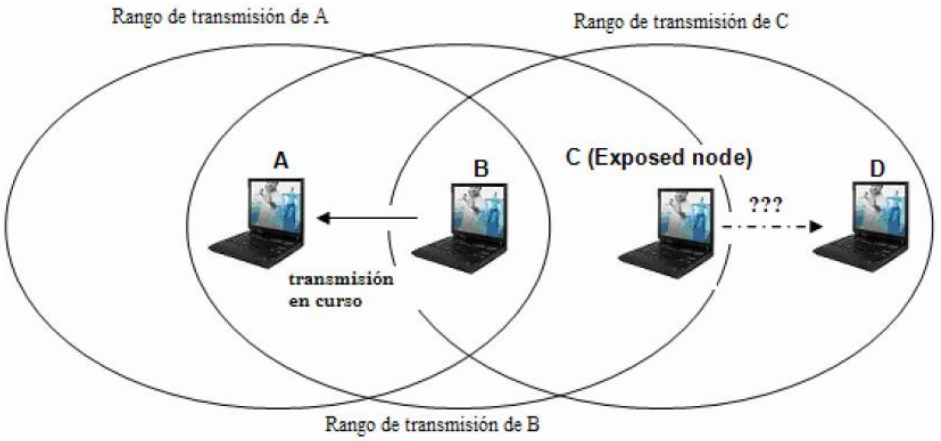


Figura 1-6 Nodo Expuesto.

La idea para evitar las colisiones es que el transmisor y el receptor intercambien tramas de control antes que el transmisor envíe algún dato. Este intercambio indica a los nodos cercanos que va a iniciarse una transmisión.

1.2.3.2. Entrega Fiable de Datos

Al igual que cualquier otra red inalámbrica, una LAN inalámbrica que utilice las capas física y MAC especificadas en el estándar IEEE 802.11 está sujeta a una considerable falta de fiabilidad. El ruido, las interferencias y otros efectos de propagación repercuten en la pérdida de un número significativo de tramas. Incluso disponiendo de códigos correctores de errores, es posible que muchas tramas MAC no sean recibidas apropiadamente. Se puede hacer frente a esta situación con mecanismos que proporcionen fiabilidad en capas más altas, como TCP. Sin embargo, los contadores de tiempo utilizados para la retransmisión en capas superiores

son, por lo general, del orden de segundos. Es, por tanto, más eficiente abordar el problema de los errores en el nivel MAC. Con esta finalidad, el estándar IEEE 802.11 incluye un protocolo de intercambio de tramas. Cuando una estación recibe una trama de datos de otra estación, devuelve una trama de confirmación (ACK[12]) a la estación de origen. Este intercambio es tratado como una unidad atómica, sin ser interrumpido por una transmisión procedente de cualquier otra estación. Si la fuente no recibe la confirmación en un intervalo corto de tiempo, bien porque la trama de datos resultó dañada, o bien porque lo fue la trama ACK de retorno, la fuente retransmite la trama (Stalings, Comunicaciones y Redes de Computadores, 2004).

Para mejorar más aún la fiabilidad, es posible utilizar un intercambio de cuatro tramas. En este esquema, la fuente emite inicialmente una trama de solicitud para enviar (RTS, Request to Send) hacia el destino. La estación de destino responde con una trama de permiso para enviar (CTS, Clear to Send). Tras recibir la trama CTS, la fuente emite la trama de datos y el destino responde con una confirmación (ACK). La trama RTS alerta a todas las estaciones que se encuentran dentro del rango de recepción de la fuente de que una transmisión está en curso. El resto de estaciones se abstiene de transmitir con objeto de evitar que se produzca una colisión entre dos tramas transmitidas al mismo tiempo. Análogamente, la trama CTS alerta a todas las estaciones que están en el rango de recepción del destino de que se va a producir un intercambio. Aunque la parte RTS/CTS del protocolo de intercambio es una función requerida de la capa MAC, es posible deshabilitarla (Stalings, Comunicaciones y Redes de Computadores, 2004).

[12] ACK: Acuse de Recibo

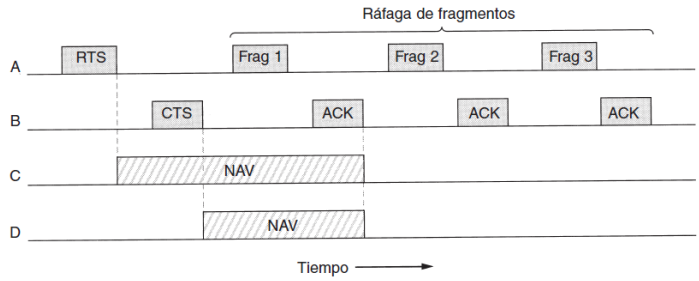


Figura 1-7 Ráfaga de Fragmentos.

- **Con un AP**

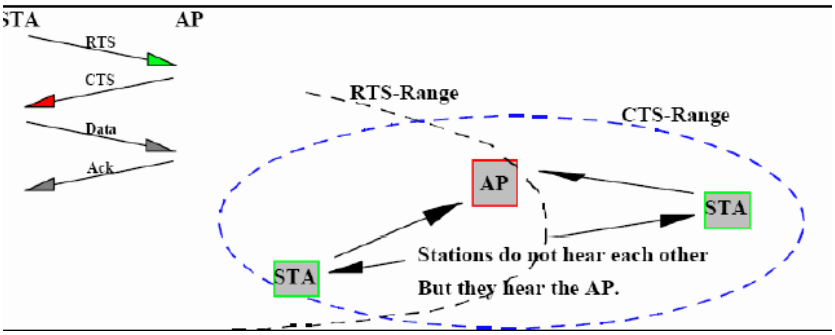


Figura 1-8 Proceso Intercambio de Tramas.

1.2.3.3. Control de Acceso

El grupo de trabajo 802.11 ha considerado dos tipos de propuestas para algoritmos MAC: protocolos de acceso distribuido, en los que, como en el caso de Ethernet, la decisión para transmitir se distribuye sobre todos los nodos usando un mecanismo de detección de portadora; y, por otro lado, protocolos de acceso centralizado, que implican una regulación de la transmisión por una autoridad central de toma de decisiones. Un protocolo de acceso distribuido tiene sentido en el caso de una red *ad hoc* de estaciones paritarias, aunque puede ser también interesante en otras configuraciones de LAN inalámbricas que trabajen principalmente con tráfico a ráfagas. Un protocolo de acceso centralizado es más natural para configuraciones en las que una serie de estaciones inalámbricas se encuentran interconectadas entre sí y con algún tipo de estación base que actúa como pasarela hacia una LAN troncal cableada. También es especialmente útil cuando parte de los datos tiene algún requisito de tiempo

real o alta prioridad (Stalings, Comunicaciones y Redes de Computadores, 2004).

El resultado final en el caso de 802.11 es un algoritmo MAC denominado DFWMAC (*Distributed Foundation Wireless MAC*) que proporciona un mecanismo de control de acceso distribuido sobre el que se ubica un control centralizado opcional. La subcapa MAC inferior es la función de coordinación distribuida (DCF, *Distributed Coordination Function*). La DCF utiliza un algoritmo de contención para proporcionar acceso a la totalidad del tráfico. El tráfico asíncrono ordinario hace uso directamente de la DCF. La función de coordinación puntual (PCF, *Point Coordination Function*) es un algoritmo MAC centralizado usado para ofrecer un servicio libre de contención. La PCF se ubica justo por encima de la DCF y utiliza las características de ésta para asegurar el acceso a sus usuarios (Stalings, Comunicaciones y Redes de Computadores, 2004).

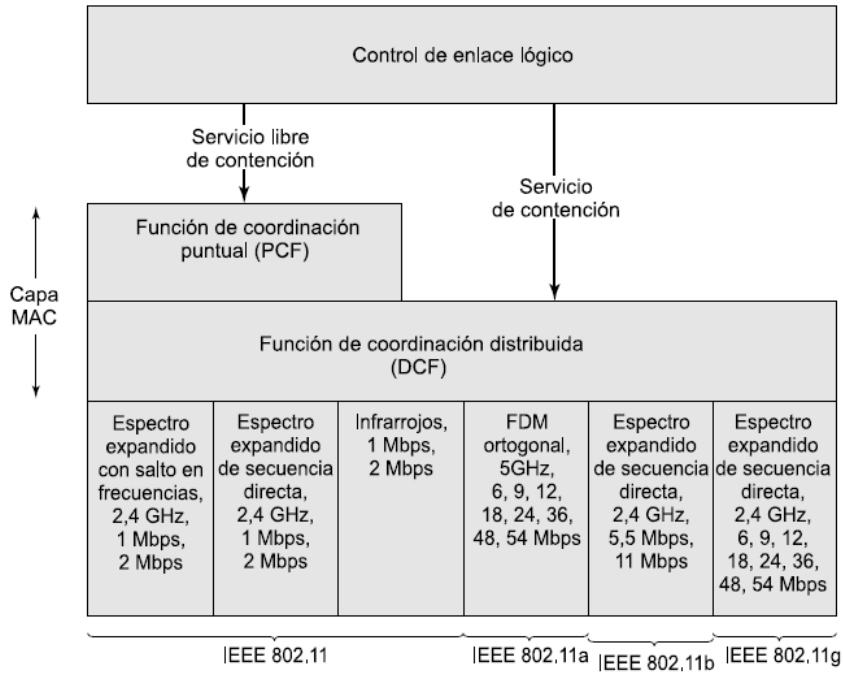


Figura 1-9 Arquitectura IEEE802.11.

Función de coordinación distribuida DCF

La subcapa DCF hace uso de un sencillo algoritmo CSMA (*Carrier Sense Multiple Access*, acceso múltiple con detección de portadora). Una estación

escucha el medio cuando dispone de una trama para transmitir. Si el medio está libre, la estación puede transmitir; en otro caso, la estación debe esperar antes de transmitir hasta que se complete la transmisión en curso. La DCF no incluye una función de detección de colisiones (es decir, CSMA/CD[13]) porque ésta no resulta práctica en una red inalámbrica. El rango dinámico de las señales en el medio es muy elevado, de tal forma que una estación que desee transmitir no puede distinguir de manera efectiva entre una señal entrante muy débil, y el ruido más los efectos de su propia transmisión (Stalings, Comunicaciones y Redes de Computadores, 2004).

Para asegurar un funcionamiento adecuado y equitativo de este algoritmo, la DCF incluye un conjunto de retardos que se ordenan de acuerdo con un esquema de prioridades. Comenzaremos considerando un retardo simple denominado espacio entre tramas (IFS, *Interframe Space*) (Stalings, Comunicaciones y Redes de Computadores, 2004).

De hecho, existen tres valores diferentes para el IFS, pero el algoritmo se explica mejor ignorando inicialmente este detalle. Usando un IFS, las reglas de acceso CSMA son las siguientes:

- Una estación que disponga de una trama lista para ser transmitida sondea el medio. Si éste se encuentra libre, la estación espera a ver si el medio permanece libre durante una cantidad de tiempo igual al IFS. Si es así, la estación puede transmitir inmediatamente.
- Si el medio está ocupado (bien porque la estación lo encuentra inicialmente así, o bien porque este hecho sucede durante el tiempo de espera IFS), la estación pospone la transmisión y continúa monitorizando el medio hasta que la transmisión en curso finalice.
- Una vez que la transmisión actual haya terminado, la estación espera otro IFS. Si el medio permanece libre durante ese periodo, la estación espera durante una cantidad aleatoria de tiempo y vuelve a sondear el medio de nuevo. Si el medio continúa libre, la estación puede transmitir. Si, por el contrario, el medio queda ocupado

[13] CSMA/CD: Carrier Sense Multiple Access / Collision Detection

durante el periodo de espera, el contador de espera se para, comenzando de nuevo cuando el medio quede libre.

Para asegurar que el proceso de espera mantenga la estabilidad, se utiliza una espera exponencial binaria, que proporciona una forma de manejar cargas elevadas. Los intentos repetidos y fallidos de transmitir se traducen en periodos de espera cada vez mayores, hecho éste que ayuda a reducir la carga. En el caso de que este mecanismo no existiera se podría dar la siguiente situación: dos o más estaciones intentan transmitir al mismo tiempo, ocasionando una colisión. Ambas intentan retransmitir inmediatamente, causando una nueva colisión (Stalings, Comunicaciones y Redes de Computadores, 2004).

El esquema anterior se refina para permitir que la DCF proporcione un acceso basado en prioridades. Para ello se utiliza un mecanismo simple basado en el uso de tres valores para el IFS (Stalings, Comunicaciones y Redes de Computadores, 2004):

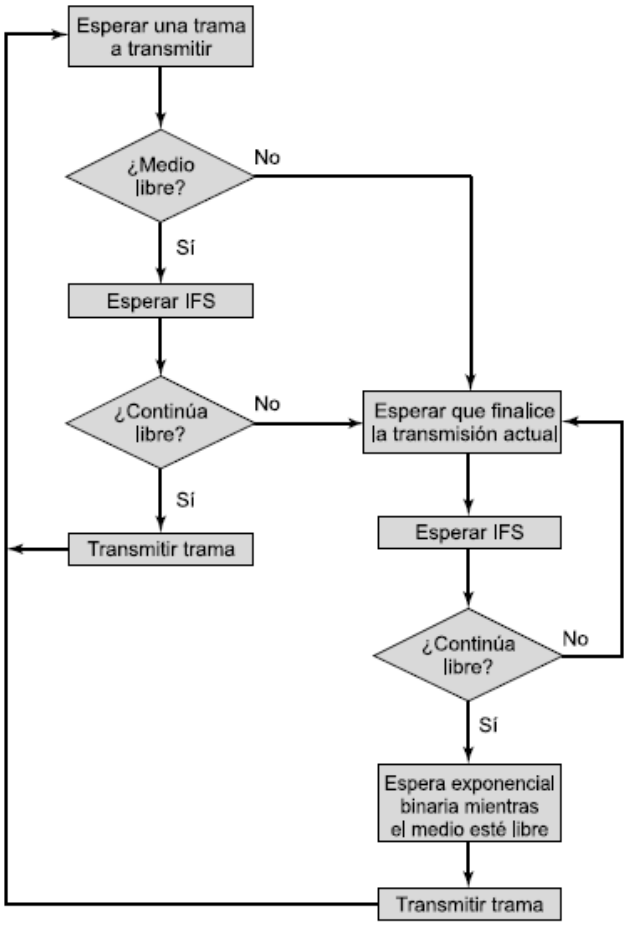


Figura 1-10 Lógica de control de acceso al medio IEEE802.11.

SIFS (IFS corto, *short IFS*): es el IFS más pequeño y se utiliza para todas las acciones de respuesta inmediatas, tal y como se explica más adelante (Stalings, Comunicaciones y Redes de Computadores, 2004).

PIFS (IFS de la función de coordinación puntual, *Point coordination function IFS*): se trata de un IFS de tamaño medio, utilizado por el controlador central en el esquema PCF cuando emite un sondeo (Stalings, Comunicaciones y Redes de Computadores, 2004).

PIFS = aSlotTime + SIFS > SIFS

DIFS (IFS de la función de coordinación distribuida, *Distributed coordination function IFS*): constituye el IFS más grande y se usa como un retardo mínimo para las tramas asíncronas que compiten por el acceso al medio (Stalings, Comunicaciones y Redes de Computadores, 2004).

DIFS = aSlotTime + PIFS > PIFS

La Figura 1-11 ilustra el uso de estos valores de tiempo. Consideremos primeramente el caso del SIFS. Cualquier estación que utilice un SIFS para determinar la ocasión de transmitir tiene, en efecto, la prioridad más alta, dado que siempre ganará el acceso antes que cualquier otra estación que espere una cantidad de tiempo igual a un PIFS o a un DIFS. El uso de SIFS se produce en las siguientes circunstancias: (Stalings, Comunicaciones y Redes de Computadores, 2004)

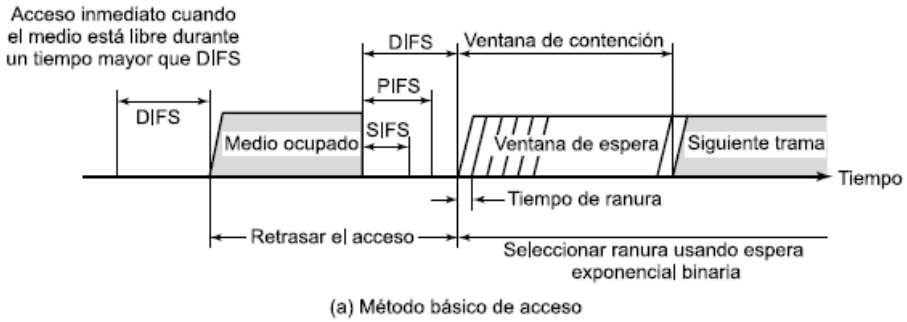


Figura 1-11 Relaciones IFS modo DCF.

- **Confirmación (ACK):** cuando una estación recibe una trama dirigida exclusivamente a ella (es decir, sin difusión ni multidifusión), ésta responde con una trama ACK tras esperar únicamente un espacio de tiempo igual a un SIFS. Esto tiene dos efectos deseables. En primer lugar, dado que no se utiliza detección de colisiones, la probabilidad de las colisiones es mayor que con CSMA/CD, de forma que la confirmación a nivel MAC proporciona un mecanismo eficiente de recuperación ante colisiones. En segundo lugar, el SIFS puede ser utilizado para proporcionar una entrega eficiente de una PDU correspondiente a un protocolo de nivel LLC que requiera varias tramas MAC. En este caso se da el siguiente escenario. Una estación con una PDU LLC multi trama lista para ser transmitida envía las tramas MAC una a una. Cada trama es confirmada tras un periodo de tiempo igual a un SIFS por el destinatario. Cuando la fuente recibe la confirmación (ACK), envía inmediatamente (tras un SIFS) la siguiente trama de la secuencia. El resultado es que, una

vez que la estación ha competido por el canal, mantendrá el control sobre el mismo hasta que haya concluido el envío de todos los fragmentos de una PDU LLC (Stalings, Comunicaciones y Redes de Computadores, 2004).

- **Permiso para enviar (CTS):** una estación puede asegurar que su trama de datos se enviará satisfactoriamente si primero emite una pequeña trama de solicitud para enviar (RTS). La estación a quien va dirigida la trama RTS debería responder inmediatamente con una trama CTS si se encuentra preparada para recibir. El resto de estaciones reciben la trama RTS y se abstienen de usar el medio (Stalings, Comunicaciones y Redes de Computadores, 2004).
- **Respuesta a sondeo (*poll response*):** este punto es explicado posteriormente en la discusión sobre PCF. El siguiente intervalo IFS en longitud es el PIFS. Éste es utilizado por el controlador central para la emisión de sondeos y tiene prioridad sobre el tráfico de contención normal. Obsérvese, sin embargo, que las tramas transmitidas utilizando SIFS tienen prioridad sobre un sondeo PCF. Finalmente, el intervalo DIFS se utiliza para el tráfico ordinario asíncrono (Stalings, Comunicaciones y Redes de Computadores, 2004).

Procedimiento Back off

El procedimiento del back off (tiempo de espera) viene llevada a cabo en estas situaciones: Inmediatamente después de que la estación, comprobando el medio antes de la transmisión de la trama, haya sentido el canal ocupado; cuando una trama debe ser retransmitida; después de las transmisiones llevadas a cabo con éxito en particulares tramas (aquellas con el bit More Fragments igual a 0 o aquellas con el campo Subtype igual al PS-Poll) (Navarro Gavira, 2005).

Cada estación que intenta iniciar una transmisión debe primero efectuar el carrier-sense (comprobación del canal), y sólo después de haber sentido el canal libre por un tiempo mayor o igual a un DIFS (o a un EIFS, en el caso de que una transmisión anterior no haya sido completada con éxito) podría

transmitir una trama. Por lo tanto, en el caso en que el canal resultase ocupado, la estación debería retrasar la transmisión hasta que el canal quede libre mediante un DIFS o un EIFS, según los casos. Además, para precaver la posibilidad de colisión con otras estaciones que queriendo transmitir habían igualmente sentido libre el canal con un DIFS o un EIFS, viene calculado un tiempo casual de back off, es decir, un posterior tiempo de espera (Navarro Gavira, 2005).

El tiempo de back off generado casualmente, indica cuanto tiempo debe esperar la estación después de que el canal se sienta libre con un DIFS o un EIFS. El valor del back off viene calculado según la siguiente expresión:

Back off Time = Random () * aSlotTime

Donde,

Random () es un número entero pseudo casual extraído de una distribución uniforme en el intervalo [0, CW], donde CW (Contention Window) es un número entero expresado entre dos parámetros característicos del nivel físico llamados

aCWmin y aCWmax.

aCWmin ≤ CW ≤ aCWmax

aSlotTime es el parámetro que define la duración del time slot (tiempo de slot) a nivel físico, y depende de la particular tecnología de transmisión utilizada (50μs para el Frequency Hopping Spread Spectrum, 20μs para el Direct Sequence Spread Spectrum, 8μs para el Infrarrojo).

Después de haber esperado que el canal quedase libre mediante un DIFS o un EIFS, la estación, para poder transmitir su trama, debe decrementar un contador llamado Back off Timer, que parte del valor del Back off Time y decrece en una unidad con cada intervalo de aSlotTime. Durante este decremento, la estación sigue sondeando el canal para tener en cuenta si, mientras tanto, cualquier otra estación ha ocupado el medio. En el caso en el que esto ocurra, todas las estaciones detienen el decremento y el valor del contador viene congelado para utilizarlo como valor inicial en la próxima contienda, garantizando a las relativas estaciones un tipo de prioridades de acceso al medio. Cuando el Back off Timer se pone a cero, la

estación podrá transmitir su trama ocupando el canal. Sin embargo se podrá verificar que dos estaciones, habiendo generado el mismo número de back off, inician a transmitir simultáneamente sobre el canal, provocando una colisión de la cual se perciben no recibiendo la trama ACK de confirmación.

El parámetro CW varía dinámicamente en cada una de las estaciones con el intervalo [aCWmin, aCWmax]. Se parte de un valor inicial igual a aCWmin y viene incrementado exponencialmente al verificarse una colisión, hasta alcanzar el valor aCWmax, según la siguiente expresión:

CW = 2 * CW + 1

En cambio, si la transmisión de la trama va a buen fin (recepción del ACK), entonces CW vuelve a configurarse como aCWmin.

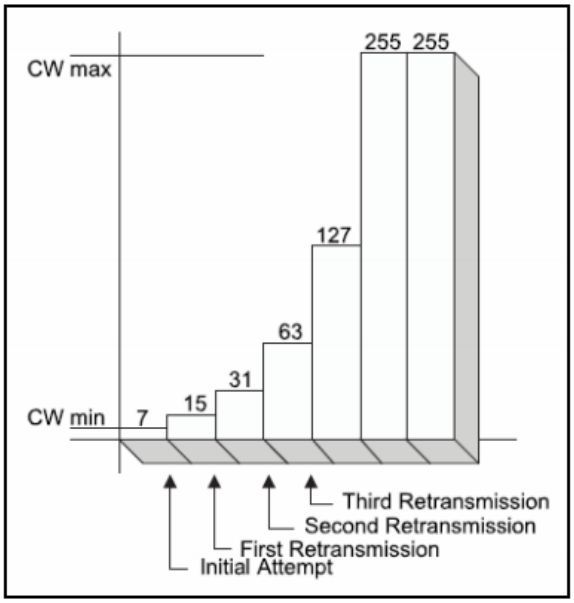


Figura 1-12 Incremento Exponencial CW.

Función de coordinación puntual

PCF es un método de acceso alternativo implementado sobre DCF, cuya función consiste en un sondeo realizado por un elemento central de sondeos (coordinador puntual) (Navarro Gavira, 2005). El coordinador puntual hace uso de un PIFS cuando emite un sondeo. Dado que un PIFS es más pequeño que un DIFS, el coordinador puntual puede adueñarse del medio y bloquear todo el tráfico asíncrono mientras emite un sondeo y recibe las respuestas.

Como caso extremo puede considerarse el siguiente escenario posible. Una red inalámbrica se configura de tal manera que una serie de estaciones con tráfico sensible a los retardos se controla por medio del coordinador puntual, mientras que el resto del tráfico compite por el acceso usando CSMA. El coordinador puntual podría emitir consultas a todas las estaciones configuradas para el sondeo siguiendo un esquema de turno rotatorio. Cuando se emite un sondeo, la estación consultada puede responder utilizando un SIFS. Si el coordinador puntual recibe una respuesta, entonces emite un nuevo sondeo usando un PIFS. Si no se recibe respuesta alguna durante el tiempo correspondiente al turno, el coordinador emite un sondeo (Stalings, Comunicaciones y Redes de Computadores, 2004).

Si la disciplina expuesta en el párrafo anterior fuese implementada, el coordinador puntual podría bloquear todo el tráfico asíncrono sin más que emitir repetidamente sondeos. Para prevenir la ocurrencia de este hecho se define un intervalo conocido como súper trama. Durante la primera parte de este intervalo, el coordinador puntual emite sondeos a todas las estaciones configuradas para el sondeo siguiendo un esquema de turno rotatorio. A continuación, el coordinador espera un tiempo igual a lo que reste de la súper trama, permitiendo así la existencia de un periodo de contención para el acceso asíncrono (Stalings, Comunicaciones y Redes de Computadores, 2004).

En la Figura 1-13 se ilustra el uso de la súper trama. Al principio de una súper trama, el coordinador puntual puede hacerse con el control opcionalmente y emitir sondeos durante un periodo de tiempo dado. Este intervalo varía debido al tamaño variable que pueden tener las tramas de respuesta de las estaciones. El tiempo restante de la súper trama queda disponible para el acceso competitivo. Al final del intervalo de súper trama, el coordinador puntual compite por el acceso al medio usando un PIFS. Si el medio se encuentra disponible, el coordinador gana el acceso inmediatamente, siguiendo a continuación una súper trama completa. Sin embargo, el medio puede estar ocupado al final de la súper trama. En este caso, el coordinador puntual debe esperar hasta que el medio quede libre para conseguir el acceso, lo que

se traducirá en un periodo de súper trama más corto para el siguiente ciclo (Stalings, Comunicaciones y Redes de Computadores, 2004).

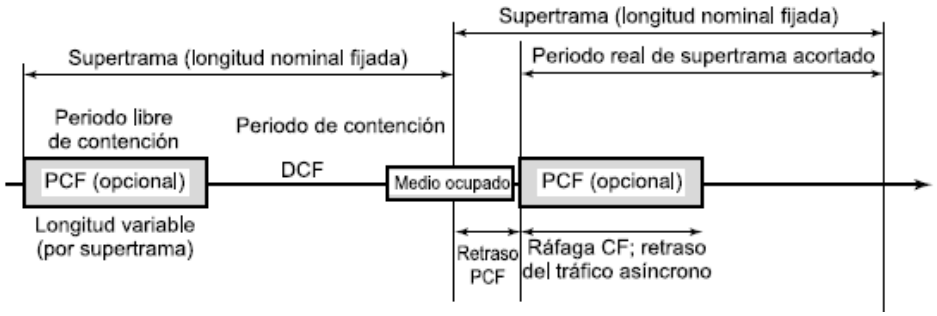


Figura 1-13 Relaciones IFS modo PCF.

1.2.3.4. Subcapa MAC Administración

1.2.3.4.1. Sincronización

La sincronización tiene como funciones el encontrar y permanecer en la WLAN.

- **Temporizador TSF:** se usa para la administración de potencia mediante Beacons enviados a intervalos preestablecidos y bien conocidos. Adicionalmente los temporizadores de las estaciones en un BSS están sincronizados ya que todas las estaciones mantiene timers locales. TSF se usa para temporización del punto de coordinación prediciendo el inicio del periodo libre de contención. En FH[14] es útil para temporizar los saltos de frecuencia permitiendo de esa manera que las estaciones salten al mismo tiempo. En una red de infraestructura los APs controlan la temporización y en IBSS la función es distribuida (Bernal I. , 2005).
- **Beacon:** permiten transportar la temporización en instantes planificados (intervalos beacon) y no requieren escuchar a todos los Beacons para permanecer sincronizados. En redes de infraestructura los APs envían los Beacons. Contienen a los time stamps para los

[14] FH: Frequency Hopping

BSS los mismos que se usan en el receptor para calibrar el reloj local y tienen el valor Timer del transmisor en el instante de transmitir. Adicionalmente los Beacons contiene información para administración de potencia o para roaming. La transmisión del beacon puede retrasarse por el uso del canal y transmisiones posteriores se envían en los instantes en los que se planificó, considerando el intervalo beacon (Bernal I. , 2005).

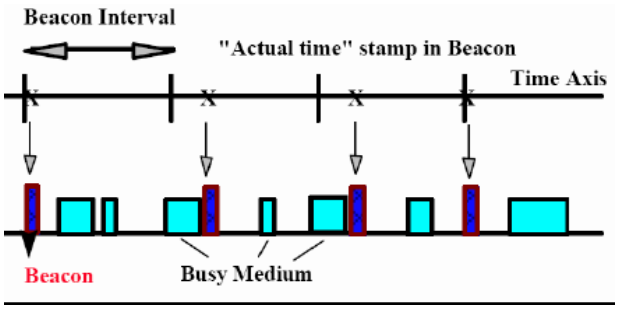


Figura 1-14 Intervalos Beacon.

1.2.3.4.2. Administración de Potencia

Es fundamental para disponer la movilidad para lo cual se dispone el protocolo 802.11 de administración de potencia el mismo que permite que el transceiver este apagado el mayor tiempo posible. Los APs conocen que estaciones están en modo de ahorro de energía y los paquetes transmitidos a dichas estaciones las almacenan en un buffer enviándolas a las estaciones respectivas cuando regresan al modo activo o cuando las estaciones le solicitan mediante una trama power-save poll. Cada AP sabe que una estación ha despertado cuando la estación lo indica cambiando el valor de un bit en el campo de control de la trama MAC (Bernal I. , 2005). Cada estación conoce que tiene tramas almacenadas en el AP despertándose periódicamente mediante las señales beacon enviadas por el AP, dichas señales de beacon contiene una lista de estaciones que tiene tramas almacenadas en el AP conocido como TIM[15].

[15] TIM.- Mapa de indicación de tráfico

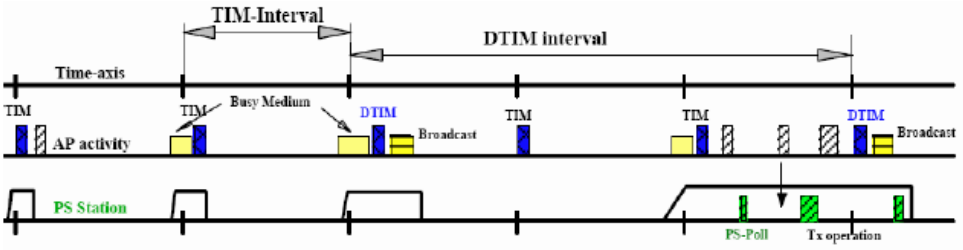


Figura 1-15 Administración de Potencia.

Las tramas de broadcast/multicast se ubican también en buffers en un AP y son enviadas solo después de DTIM[16] el cual es un múltiplo de TIM. Las estaciones se despiertan previo aun TIM/DTIM planificado enviando un PS-Poll (pawer save poll) y permanecen despiertas para recibir los datos (Bernal I. , 2005).

1.2.3.4.3. Asociación y Re asociación

- **Roaming**: La estación decide que el enlace del AP actual es pobre, por lo que utiliza el scanning para encontrar otro AP o puede usar información de scannings previos. Una vez efectuado dicho proceso la estación envía peticiones de Reasociación (Reassociation Request) al nuevo AP, si la respuesta (Reassociation Response) es exitoso la estación ha migrado (roamed) al nuevo AP caso contrario la estación realiza otro proceso de scanning. Un Ap que ha aceptado un pedido de Reasociación informa sobre la Reasociación al DS, el AP original es notificado y la información del DS se actualiza (Bernal I. , 2005).

[16] DTIM.- Mapa de Indicación de Entrega de trafico

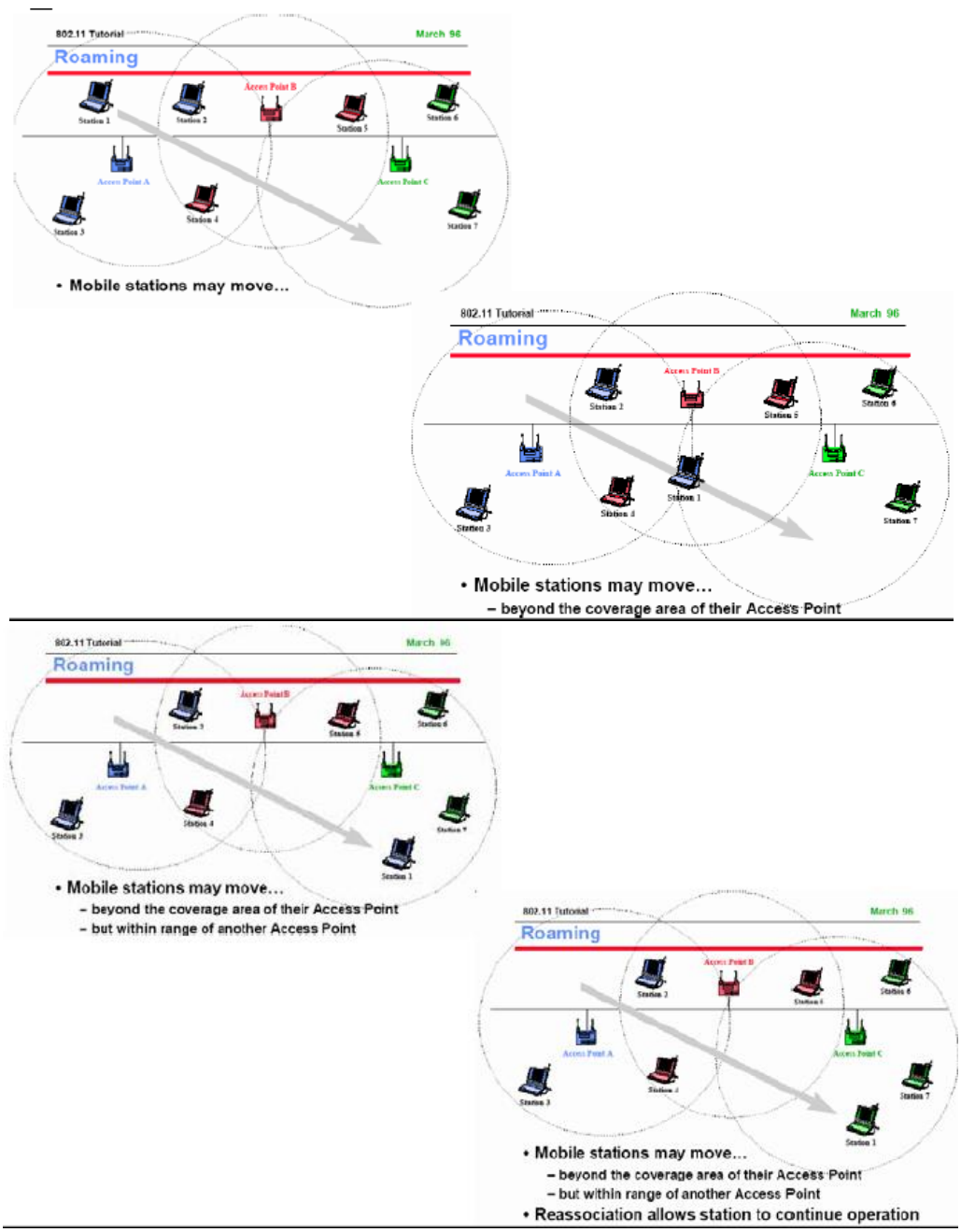


Figura 1-16 Roaming.

- **Scanning**: es requerido par funciones como encontrar y unirse a una red, encontrar un nuevo AP mientras la estación está en roaming e inicializar un IBSS. La MAC utiliza un mecanismo común para todas las opciones de capa física como es el scanning que puede ser pasivo o activo en un solo canal o multicanal donde pasivo se refiere a encontrar redes simplemente escuchando los Beacons y el activo en cada canal se envía un sondeo hasta esperar la respuesta que

incluirá la información necesaria para unirse a la red (Bernal I. , 2005).

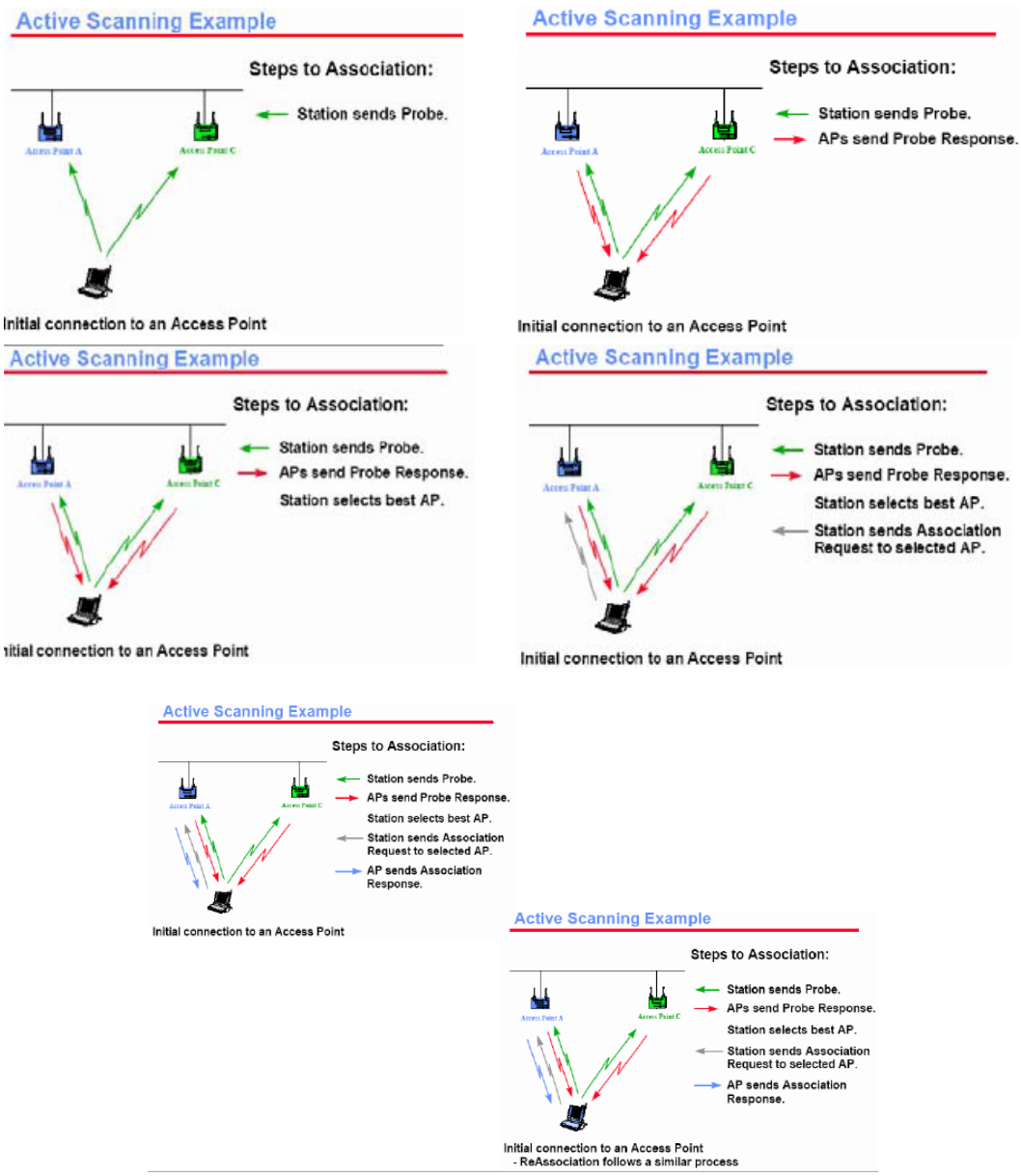


Figura 1-17 Scanning.

1.2.4. Tramas MAC

La estructura de las tramas MAC implementadas por cualquier estación es común e independiente del tipo de trama. Una vez se forme la trama, esta

se pasará a la PLCP[17] para que esta la prepare para enviarla al medio. (IEEE STANDARDS ASSOCIATION, 2012)

Las tramas MAC contienen los siguientes componentes básicos: una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia; un cuerpo de trama de longitud variable, que contiene la información de las tramas de los niveles superiores y una secuencia de comprobación de errores (FCS) que contiene un código de redundancia cíclico (CRC) de 32 bits (Yunquera Torres).

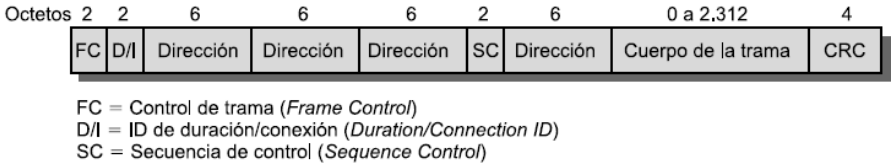


Figura 1-18 Trama MAC.

- **Campo de control**: Este campo contiene toda la información de control. Se divide a su vez en una serie de subcampos por lo que merece examinar aparte.
- **Duration/ID:** En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar el tiempo que el medio va a estar ocupado. Se utiliza por tanto, para establecer el NAV.
- **Campos dirección 1-4:** Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino. Las direcciones pueden ser individuales o de grupo. Podemos diferenciar dos tipos de grupos, para múltiples usuarios (multicast) o de difusión (broadcast). Las de múltiples usuarios se dirigen a grupo lógico de estaciones y las de difusión se dirigen a todas las estaciones.

[17] PLCP: Physical Layer Convergence Protocol

Tabla 2 Contenido de los campos de dirección.

escenario	To_DS	From_DS	Add.1	Add.2	Add.3	Add.4
red ad-hoc	0	0	destino	origen	BSSID	-
red centralizada	0	1	destino	BSSID	origen	-
red centralizada	1	0	BSSID	origen	destino	-
En el DS	1	1	receptor	transmisor	destino	origen

- **Campo de control de secuencia:** Los últimos cuatro bits de este campo de dos octetos lo componen el subcampo de número de fragmento, que indica el número de fragmento dentro de la MSDU. Este número empieza en cero y se va incrementando en uno por cada fragmento añadido. Los doce bits anteriores son el número de secuencia, empezando en cero e incrementándose en uno por cada subsecuencia de MSDU transmitida. Con estos campos, la estación receptora podrá filtrar tramas duplicadas.
- **Cuerpo de la trama:** Este campo es de longitud variable y lleva la información que se pretende enviar en la trama. Su longitud se establece entre 0 y 2312 octetos. En el caso de tratarse de una trama de datos, este campo contendrá unidades de datos de la LLC. Si se tratase de una trama que no necesita transportar información este campo tendría longitud cero.
- **FCS (secuencia de comprobación de la trama):** La capa MAC calcula una secuencia de comprobación, sobre la trama, de 32 bits. Usa para esto un código de redundancia cíclico (CRC) y el resultado lo plasma en este campo. El polinomio generador se usa tanto en la cabecera MAC como en el cuerpo de la trama para calcular el FCS. El polinomio generador usado es:

  $G(x) = x_{32}+x_{26}+x_{23}+x_{22}+x_{16}+x_{12}+x_{11}+x_{10}+x_8+x_7+x_5+x_4+x_2+x+1$

1.2.4.1. Formato de Trama de Control

2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
Versión Protocolo	**Tipo Trama**	**Subtipo**	**Para DS**	**De DS**	**Más Frag.**	**Retr**	**Gest Energ**	**Más Info**	**WEP**	**Orden**

Figura 1-19 Formato campo e control MAC.

- **Versión del protocolo:** Este campo deja sus dos bits a cero, para usos futuros (Yunquera Torres).
- **Tipo de trama:** Este campo define el tipo de trama que se está tratando, codificando el tipo en sus dos bits, de la forma que se muestra en la Tabla 3.

Tabla 3 Posibilidades de Tipo de Trama.

Combinación de los bits	Tipo de trama
0 0	Gestión
0 1	Control
1 0	Datos
1 1	Reservado

- **Subtipo:** Con este campo se indica el subtipo de trama, dentro de los grupos anteriores, con sus 4 bits. Se muestra una tabla resumen en la Tabla 4.

Tabla 4 Posibilidades campo subtipo.

Tipo de trama	Subcampo	Función de la trama
Gestión 0 0	0 0 0 0	Solicitud de asociación
	0 0 0 1	Respuesta de asociación
	0 0 1 0	Solicitud de reasociación
	0 0 1 1	Respuesta de reasociación
	0 1 0 0	Solicitud de sondeo
	0 1 0 1	Respuesta de sondeo
	0 1 1 0 – 0 1 1 1	Reservado
	1 0 0 0	Faro
	1 0 0 1	Trafico anunciado
	1 0 1 0	Disociación
	1 0 1 1	Autenticación
	1 1 0 0	Deautenticación
	1 1 0 1 – 1 1 1 1	Reservado
Control 0 1	0 0 0 0 – 1 0 0 1	Reservado
	1 0 1 0	Ahorro de energía
	1 0 1 1	RTS
	1 1 0 0	CTS
	1 1 0 1	ACK
	1 1 1 0	Fin CF
	1 1 1 1	Fin CF + CF ACK
Datos 1 0	0 0 0 0	Datos
	0 0 0 1	Datos + CF ACK
	0 0 1 0	Datos + trama CF
	0 0 1 1	Datos + CF ACK + Trama CF
	0 1 0 0	Null
	0 1 0 1	CF ACK
	0 1 1 0	Trama CF
	0 1 1 1	CF ACK + Trama CF
	1 0 0 0 – 1 1 1 1	Reservado
Reservado 1 1	0 0 0 0 – 1 1 1 1	

- **To DS:** Se compone de un solo bit que se establece a uno cuando la trama se dirige al sistema de distribución.
- **From DS:** Este único bit se pone a uno cuando la trama procede del sistema de distribución. Jugando con este campo y con el anterior se pueden conseguir diferentes significados.

Tabla 5 To DS y From DS.

Para DS	De DS	Significado
0	0	Trama transmitida de una estación a otra.
1	0	Trama destinada al punto de acceso.
0	1	Trama procedente del punto de acceso.
1	1	Trama transmitida entre puntos de acceso.

- **Más fragmentos:** Este campo de un bit se establece a uno cuando detrás de este fragmento de MSDU viene otro de esta misma MSDU.
- **Retransmisión:** Si esta trama es la retransmisión de una trama anterior, este bit se establece a uno.

- **Gestión de energía:** Este bit indica si la estación va a entrar en un estado de ahorro de energía tras la trama actual, estableciéndolo a uno. Con un cero se indica que la estación está a pleno funcionamiento.
- **Más información:** Sirve para que estaciones en ahorro de energía, interroguen al punto de acceso para ver si tiene más tramas para ellas.
- **WEP[18]:** Lo compone un solo bit que indica si el cuerpo de la trama fue procesado con el algoritmo WEP, estableciéndolo a uno y a cero en otro caso.
- **Orden:** Este campo se establece a uno para indicar al receptor que las tramas enviadas deben ser procesadas en orden.

1.2.4.2. Tipos de Tramas MAC

Las tramas MAC se pueden clasificar según tres tipos: Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso; Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda y Tramas de datos (Yunquera Torres).

1.2.4.2.1. Tramas de gestión

El propósito de las tramas de gestión es establecer la comunicación inicial entre las estaciones y los puntos de acceso. Esto se puede hacer mediante los servicios de autenticación y asociación (IEEE STANDARS ASSOCIATION, 2012).

La trama de gestión presenta la dirección de destino en el campo de dirección 1, la de origen en el 2 y el BSSID en el tercero.

[18] WEP: Wired Equivalent Privacy

2 Oct.	2 Oct.	6 Oct.	6 Oct.	6 Oct.	2 Oct.	0-2312 Oct.	4 Oct.
Trama Control	**Duración**	**DA**	**SA**	**BSSID**	**Sec. Control**	**Cuerpo Trama**	**FCS**

Figura 1-20 Trama de Gestión.

Durante el periodo de contienda todas las tramas de gestión establecen el campo de duración como sigue:

- Si la dirección destino es la dirección de un grupo, se establece a cero.
- Si el campo de más fragmentos está a cero y la dirección destino es una dirección individual, el campo de duración contendrá el número de microsegundos requeridos para transmitir un ACK después de un intervalo SIFS.
- Si el campo de más fragmentos contiene el valor uno y la dirección destino es una dirección individual, el campo contendrá el número de microsegundos requeridos para transmitir la siguiente trama. Más dos ACK y tres SIFS.

Dentro de las tramas de gestión, nos podemos encontrar con los siguientes subtipos (Yunquera Torres):

a) **Solicitud de asociación:** Esta trama la envía una estación a un punto de acceso si se quiere asociar con éste.

b) **Respuesta de asociación:** El punto de acceso enviará una respuesta de asociación a la estación que le envió una solicitud de asociación para indicarle si la aceptó o no.

c) **Solicitud de Reasociación:** Una estación envía esta trama cuando quiere reasociarse con un punto de acceso, con el que ya tuvo una relación de asociación.

d) **Respuesta de Reasociación:** Después que el punto de acceso reciba la solicitud de Reasociación, este responderá con esta trama para indicar si acepta o no la Reasociación.

e) **Solicitud de sondeo:** La estación enviará esta trama para obtener información de otra estación o del punto de acceso.
f) **Respuesta de sondeo:** Si una estación o un punto de acceso recibió una solicitud de sondeo, responderá con esta trama donde incluirá sus parámetros específicos.
g) **Beacon:** En una red en modo infraestructura, el punto de acceso periódicamente enviará una trama faro para mantener el sincronismo entre las estaciones que usen la misma capa física. Cuando el punto de acceso realiza funciones de punto coordinador, este usará las tramas faro para indicar el comienzo de un periodo libre de contienda.
h) **Disociación:** La misión de esta trama es permitir a un punto de acceso o a una estación terminar con una relación de asociación.
i) **Autenticación:** Una estación envía esta trama a un punto de acceso con el que se quiere autentificar.
j) **Desautenticación:** Esta trama permite terminar con una relación de autenticación, o lo que es lo mismo una comunicación segura.
k) **ATIM:** En las redes ad-hoc cada estación debe guardar sus datos a las estaciones que duermen. Cada estación debe anunciar a qué estaciones debe enviar datos. Para esto se utilizan las tramas ATIM (Adhoc Traffic Indication Map). Existe un periodo concreto para enviar ATIM y viene indicado por la ventana ATIM (ATIM window).

En cuanto al contenido del cuerpo de las tramas de gestión dependerá del tipo que consideremos. Veamos de forma breve sus funciones específicas:

- Número de autenticación del algoritmo. Indica el algoritmo que sigue el punto de acceso para que la estación pueda autentificarse. Su valor es cero en sistemas abiertos y uno para los de llave compartida.
- Número de secuencia de autenticación de la transacción. Indica el estado del proceso de autenticación.

- Intervalo de faro. Para indicar las unidades de tiempo entre transmisiones de faro (tramas beacon).
- Capacidad de información. Este campo indica la capacidad de información de una estación.
- Dirección actual del AP. Contiene la dirección del punto de acceso con el que la estación se encuentra asociada.
- Intervalo de escucha. Este campo contiene un valor que establece el valor de las unidades de tiempo de los intervalos de faro.
- Código de razón. Indica porque una estación está generando una solicitud de disociación o Desautenticación no deseada.
- Asociación ID. Es un identificador (ID) que un punto de acceso asigna durante el proceso de asociación.
- Código de estado. Indica el estado de una cierta operación (éxito, fallo no especificado, etc.)
- Timestamp. Contiene el valor del reloj de la estación emisora cuando transmite una trama.
- SSID (Identificador del servicio). Este campo contiene el identificador de una ESS.
- Tasas soportadas. Identifica las tasas de transmisión que esa estación puede soportar. La capa MAC tiene la capacidad de cambiar las tasas de datos para optimizar la transmisión de tramas.
- Parámetros FH. Indica la duración del tiempo de vida, dwell time.
- Parámetros DS. Para identificar el número de canal.
- Parámetros CF. Contiene los parámetros de la PCF.
- TIM. Indica las estaciones que tienen tramas almacenadas en el punto de acceso.

Tabla 6 Tramas de Gestión.

Contenido de la Trama	Petición de Asociación	Respuesta de Asociación	Petición de Reasociación	Respuesta de Reasociación	Respuesta de Prueba	Petición de Prueba	Beacon	Disociación	Autenticación	Desautenticación
Número de algoritmo de Autenticación									X	
Numero de Secuencia Trans. Autenticación									X	
Intervalo Beacon					X		X			
Dirección IP Actual			X							
Intervalo de Escucha	X		X							
Código de Razón								X		X
ID de Asociación		X		X						
Código de Estado		X		X					X	
Marca de Tiempo						X	X			
SSID	X		X		X	X	X			
Velocidades Soportadas	X	X	X	X	X	X	X			
Conjunto de Parámetros FH					X		X			
Conjunto de Parámetros DS					X		X			
Conjunto de Parámetros CF					X		X			
Información de Capacidad	X	X	X	X	X		X			
Mapa Indicación de Tráfico							X			
Conjunto de Parámetros IBSS					X		X			
Texto de Prueba									X	

- Parámetros de la IBSS. (Independent Basic Service Set). Son los parámetros necesarios para soportar una IBSS.
- Texto de desafío. Este campo contiene el texto de desafío de una secuencia de autenticación de llave compartida.

Estas son las principales funcionalidades de las tramas de gestión, aunque conviene decir que diferentes vendedores pueden implementar extensiones opcionales a estas, fuera de las definidas en el estándar.

1.2.4.2.2. Tramas de Control

Después de establecer la asociación y la autenticación entre estaciones y el punto de acceso, las tramas de control serán las encargadas de establecer y asistir el envío de tramas de datos (Yunquera Torres).

- **RTS (Request To Send):** Una estación enviará una trama RTS a otra estación para negociar el envío de tramas de datos. La

estructura usual del RTS es la que se muestra en la siguiente figura. Con un campo de duración en microsegundos, que contiene el tiempo necesario para transmitirla, más el tiempo necesario para enviar un CTS, un ACK y tres SIFS. RA y TA son las direcciones del receptor y el transmisor respectivamente (IEEE STANDARS ASSOCIATION, 2012).

2 Octetos	2 Octetos	6 Octetos	6 Octetos	4 Octetos
Trama Control	**Duración**	**RA**	**TA**	**FCS**

Figura 1-21 Trama de control RTS.

- **CTS (Clear To Send):** Tras recibir un RTS, la estación que lo recibió enviará un CTS para aceptar el envío de datos por parte de la estación. El campo de duración de estas tramas está en microsegundos y contiene el tiempo de la anterior trama de RTS, menos el tiempo necesario para enviar el CTS y un SIFS. La trama sólo contendrá la dirección del receptor (IEEE STANDARS ASSOCIATION, 2012).

2 Octetos	2 Octetos	6 Octetos	4 Octetos
Trama Control	**Duración**	**RA**	**FCS**

Figura 1-22 Trama de control CTS.

- **ACK:** Si una estación recibe una trama libre de errores responderá con este tipo de trama, para confirmar la recepción correcta de la información.

- **PS Poll:** Si una estación recibe esta trama, ésta actualizará el valor de su NAV, el cual indica el tiempo en el que la estación no podrá iniciar una comunicación. Conociendo el periodo en el que no podrá transmitir, la estación podrá entrar en un estado de ahorro de

energía. La trama contiene un identificador de la asociación (AID), el BSSID (identificador de la BSS) y la dirección del transmisor.

2 Octetos	2 Octetos	6 Octetos	6 Octetos	4 Octetos
Trama Control	**AID**	**BSSID**	**TA**	**FCS**

Figura 1-23 Trama control Power Save Poll.

- CF End: Esta trama indica el final de un periodo libre de contienda. En éstas, el campo de duración se establece a cero y en la dirección del receptor (RA) va una dirección de difusión.

2 Octetos	2 Octetos	6 Octetos	6 Octetos	4 Octetos
Trama Control	**Duración**	**RA**	**BSSID**	**FCS**

Figura 1-24 Trama control CF End.

- **CF End + CF ACK:** Esta trama confirma el final de un periodo libre de contienda, anunciado por la trama CF End.

1.2.4.2.3. Tramas de Datos

La función principal de este tipo de tramas es el transporte de datos. Estas tramas podrán contener información específica, tramas de supervisión o tramas no numeradas procedentes de la capa LLC (IEEE STANDARS ASSOCIATION, 2012).

Existen ocho subtipos de tramas de datos, organizados en dos grupos. Los primeros cuatro subtipos definen tramas que transportan datos de una capa superior desde la estación origen hasta la estación de destino (Stalings, Comunicaciones y Redes de Computadores, 2004). Las cuatro tramas de transporte de datos son las siguientes:

- **Datos:** se trata de la trama de datos más simple. Puede ser utilizada tanto en el periodo de contención como en el periodo libre de contención.

- **Datos CF-Ack:** únicamente puede ser enviada durante el periodo libre de contención. Además de transportar datos, esta trama confirma la recepción de otros previamente recibidos.
- **Datos CF-Poll:** se utiliza por parte de un coordinador puntual para entregar datos a una estación móvil y para solicitar que ésta envíe una trama de datos que puede haber sido almacenada temporalmente.
- **Datos!CF-Ack!CF-Poll:** combina en una sola trama las funciones de las tramas Datos! CF-Ack y Datos!CF-Poll.

Los cuatro subtipos restantes de tramas de datos no transportan, en realidad, datos del usuario. La trama conocida como función nula (*Null Function*) no transporta datos, sondeos o confirmaciones. Se utiliza para transportar el bit de gestión de energía en el campo de control de una trama destinada al AP, indicando así que la estación va a entrar en un estado de operación de baja energía (Stalings, Comunicaciones y Redes de Computadores, 2004).

Las tres tramas restantes (CF-Ack, CF-Poll y CF-Ack CF-Poll) poseen la misma funcionalidad que los subtipos de tramas de datos correspondientes que se han comentado en la lista anterior (Datos CF-Ack, Datos CF-Poll, Datos CF-Ack CF-Poll), pero sin transportar datos (IEEE STANDARS ASSOCIATION, 2012).

1.2.5. Capa Física 802.11

La capa física de IEEE 802.11 se ha emitido en cuatro etapas. La primera parte, simplemente llamado IEEE 802.11 la cual incluye la capa MAC (Control de Acceso al Medio) y tres especificaciones de la capa física, dos en la banda de 2,4 GHz y uno en el infrarrojo, todo funciona a 1 y 2 Mbps (Bernal I. , 2005). IEEE 802.11a trabaja en la banda de 5 GHz a velocidades de datos de hasta 54 Mbps (Stalings, Comunicaciones y Redes de Computadores, 2004). IEEE 802.11 b opera en la banda 2.4 GHz y tiene

un tasa de transmisión de 5.5 y 11 Mbps. La figura 1-25, muestra la relación entre las diversas normas desarrolladas para la capa física y la tabla 7 proporciona algunos detalles de los estándares 802.11.

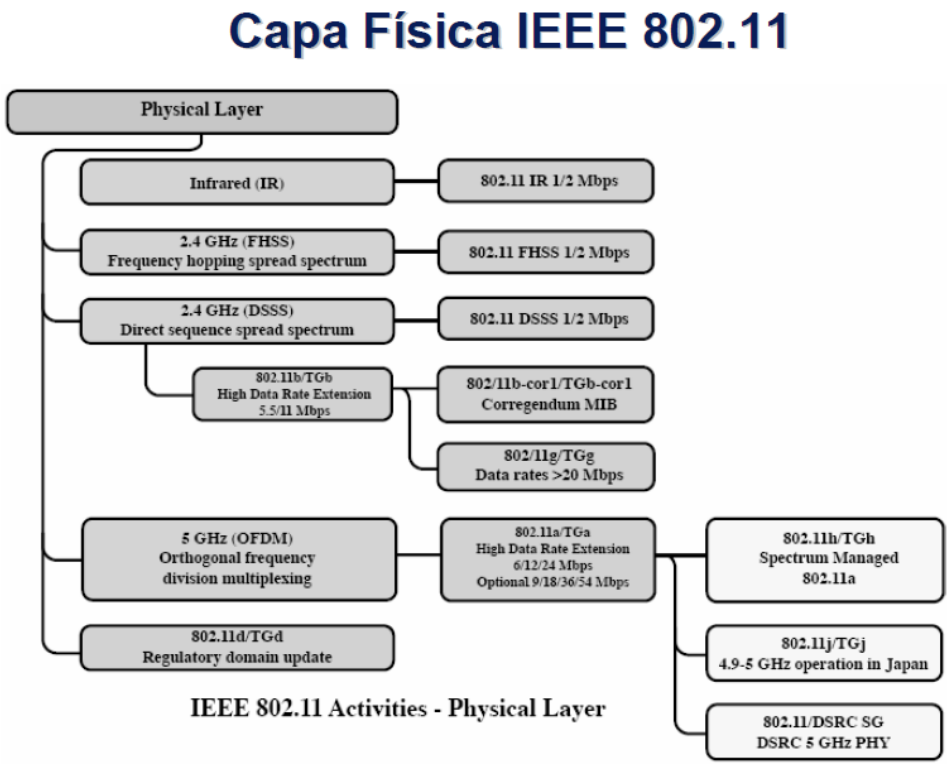


Figura 1-25 Relación Entre normas de la Capa Física.

Tabla 7 Detalles de los estándares del 802.11.

	802.11	802.11 a	802.11 b	802.11 g
AB Disponible	**83.5 MHz**	**300 MHz**	**83.5 MHz**	**83.5 MHz**
Frecuencia de Operación no Licenciada	**2.4 – 2.4835 GHz DSSS FHSS**	**5.15 – 5.35 GHz OFDM 5.725 – 5.825 GHz OFDM**	**2.4 – 2.4835 GHz DSSS**	**2.4 – 2.4835 GHz DSSS OFDM**
# Canales no solapados	**3**	**4**	**3**	**3**
Tasa de Datos por Canal	**1.2 Mbps**	**6,9,12,18,24,36,48,54 Mbps**	**1,2,5.5,11 Mbps**	**1,2,5.5,6,9,12,18,24, 36,48,54 Mbps**
Compatibilidad	**802.11**	**Wifi 5**	**Wifi**	**Wifi a 11 Mbps e inferiores**

Capa Física original 802.11

Tres soportes físicos están definidos en el estándar original 802.11

1.2.5.1. DSSS (Direct Sequence spread Spectrum)

Conocido como Espectro Ensanchado de Secuencia Directa, opera en la banda de 2.4 GHz (ISM), con una velocidad de datos de 1 Mbps y 2 Mbps. En los Estados Unidos la FCC[19] (Comisión Federal de Comunicaciones) no requiere licencia para el uso de esta banda (Stalings, Wireless Communications and Networks, 2002). Se han definido 14 canales cada uno de 5MHz. El número de canales disponibles depende del ancho de banda asignado por las agencias regulatorias de cada país. Esto va desde 13 en la mayoría de países de Europa y 1 en Japón (Stalings, Wireless Communications and Networks, 2002).

DSSS es uno de los métodos de codificación de canal (previa a la modulación) en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan. Tanto DSSS como FHSS[20] están definidos por la IEEE en el estándar 802.11 para redes de área local inalámbricas WLAN. Este esquema de transmisión se emplea, con alguna variación, en sistemas CDMA asíncronos (Wikipedia).

El espectro ensanchado por secuencia directa es una técnica de codificación que utiliza un código de pseudorruido para "modular" digitalmente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada). La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radiorreceptores les parecerá ruido menos al que va dirigida la señal. Debido a la semejanza de este mecanismo de codificación con la modulación ordinaria (una "modulación digital", análoga a la que se realiza sobre una onda sinusoidal), en ocasiones se utiliza el término modulación como sinónimo de codificación, de manera impropia si nos atenemos al verdadero concepto de modulación en telecomunicación (Wikipedia).

[19] FCC Comisión Federal de Comunicaciones
[20] FHSS: Frecuency Hopping Secuency spread

En esta técnica se genera un patrón de bits redundante para cada uno de los bits que componen la señal. Cuanto mayor sea este patrón de bits, 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 (Wikipedia).

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o pseudorruido). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de esta secuencia es el siguiente. +1-1+1+1-1+1+1+1-1-1-1-1 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. En la Figura 1-26, se puede observar un claro ejemplo de DSSS con la señal de información de datos original, el código de dispersión y finalmente se puede visualizar la información después de pasar por el código de dispersión (Wikipedia).

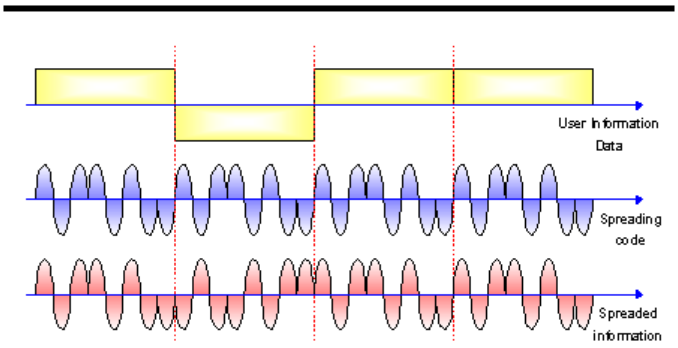


Figura 1-26 Ejemplo de DSSS con una señal Digital.

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 secuencia de Barker, el estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado por secuencia directa (DSSS), (Wikipedia)la modulación DBPSK[21] (Differential Binary Phase Shift Keying) y la modulación DQPSK[22] (Differential Quadrature Phase Shift Keying), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente (Wikipedia).

Las frecuencias vienen comprendidas entre 2.412 y 2.484GHz. Estas son divididas en canales las mismas que puede variar según los organismos reguladores de cada país (Wikipedia), en la tabla 8, se detallan las frecuencias de cada canal y en la figura 1-27 a) se puede observar los canales con su frecuencia central y en la figura 1-27 b) se puede observar un espectro aproximado de los canales.

Tabla 8 Frecuencias de los Canales 802.11.

Numero de Canal	Frecuencia (GHz)	Norte América	Europa	España	Francia	Japón
1	**2.412**	**X**	**X**			
2	**2.417**	**X**	**X**			
3	**2.422**	**X**	**X**			
4	**2.427**	**X**	**X**			
5	**2.432**	**X**	**X**			
6	**2.437**	**X**	**X**			
7	**2.442**	**X**	**X**			
8	**2.447**	**X**	**X**			
9	**2.452**	**X**	**X**			
10	**2.457**	**X**	**X**	**X**	**X**	
11	**2.462**	**X**	**X**	**X**	**X**	
12	**2.467**		**X**		**X**	
13	**2.472**		**X**		**X**	
14	**2.483**					**X**

[21] DBPSK: Differential Binary Phase Shift Keying
[22] DQPSK: Differential Quadrature Phase Shift Keying

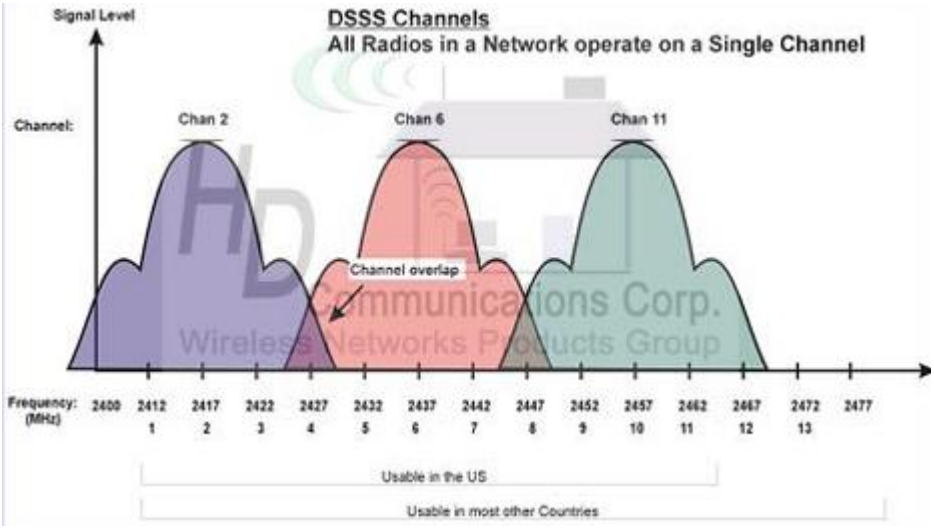


Figura 1-27 Canales 802.11 y sus frecuencias de corte.

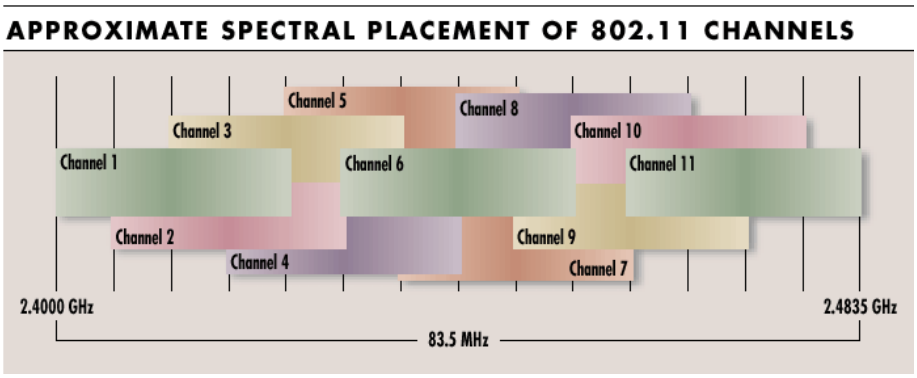


Figura 1-28 Espectro de los canales 802.11.

Para cada canal es necesario un ancho de banda de unos 22MHz para poder transmitir la información, por lo que se produce un inevitable solapamiento de los canales próximos (Wikipedia). Para prevenir interferencias con redes trabajando con canales adyacentes, se los debe separar al menos 22MHz, entre las frecuencias centrales de los canales ya que con una separación de 5 MHz entre canales, las redes deben estar separadas por 5 números de canales (Bernal I. , 2005), si tenemos que poner algunos puntos de accesos cercanos inevitablemente, deberíamos separarlos lo suficiente siendo recomendable usar los canales que no se solapen entre sí.

Dentro de las técnicas de modulación que 802.11 (Tabla 9) usa una vez implementado DSSS como método de codificación se tiene: DBPSK (Differential Binary Phase Shift Keying) y DQPSK para 2 Mbps, las cuales no son de estudio de este tema pero si para un conocimiento general en la elaboración de la tesis de grado.

Tabla 9 Técnicas de Modulación para 802.11.

Data rate	Chipping code length	Modulation	Symbol rate	Bits/symbol
1 Mbps	11 (Barker sequence)	DBPSK	1 Msps	1
2 Mbps	11 (Barker sequence)	DQPSK	1 Msps	2
5.5 Mbps	8 (CCK)	DQPSK	1.375 Msps	4
11 Mbps	8 (CCK)	DQPSK	1.375 Msps	8

1.2.5.2. FHSS (Frequency Hopping Spread Spectrum)

Conocido como Espectro Ensanchado por Salto de Frecuencia, es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits (Wikipedia).

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 (Wikipedia).

El orden en los saltos en frecuencia se determina según una secuencia pseudo aleatoria 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 el 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 saltos de 2.5 por segundo. (1sg/2'5)= 400ms (Wikipedia).

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia FSK[23] (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 (Bernal I. , 2005). En la tabla 10, se puede observar los canales usados en los diferentes entes reguladores del mundo.

Tabla 10 Canales usados en los Entes Reguladores.

Regulatory domain	Allowed channels
US (FCC)	2 to 79 (2.402-2.479 GHz)
Canada (IC)	2 to 79 (2.402-2.479 GHz)
Europe (excluding France and Spain) (ETSI)	2 to 79 (2.402-2.479 GHz)
France	48 to 82 (2.448-2.482 GHz)
Spain	47 to 73 (2.447-2.473 GHz)
Japan (MKK)	73 to 95 (2.473-2.495 GHz)

La distancia de salto mínima en frecuencia es 6 MHz en Norte América y la mayoría de Europa ya que para Japón es de 5MHz. Los conjuntos de saltos son basadas en funciones matemáticas y son parte de las especificaciones de FH PHY de 802.11, Para USA y Europa son 26 elementos, teniendo una secuencia 1 para USA {3, 26, 65, 11, 46, 19, 74, 50, 22,…} (Bernal I. , 2005). (Tabla 11).

[23] FSK: Frecuency Shift Keying

Tabla 11 Tamaño de conjunto de saltos en los Entes Reguladores.

Regulatory domain	Hop set size
US (FCC)	26
Canada (IC)	26
Europe (excluding France and Spain) (ETSI)	26
France	27
Spain	35
Japan (MKK)	23

La modulación usada en FHSS es FSK Gaussiana (modulación por desplazamiento de frecuencia Gaussiana), es un tipo de modulación donde un 1 lógico es representado mediante una desviación positiva (incremento) de la frecuencia de la onda portadora, y un 0 mediante una desviación negativa (decremento) de la misma (Bernal I. , 2005).

GFSK es una versión mejorada de la modulación por desplazamiento de frecuencia (FSK). En GFSK la información es pasada por un filtro gaussiano antes de modular la señal. Esto se traduce en un espectro de energía más estrecho de la señal modulada, lo cual permite mayores velocidades de transferencia sobre un mismo canal (Frenzel, Carrasco, Monachesi, & Chaile, 2010) (Tabla 12).

- GFSK de dos niveles para 1Mbps

  Los 0s y 1s se codifican como desviaciones de la frecuencia actual de la portadora (Bernal I. , 2005).

- GFSK de 4 niveles para 2Mbps

  Cuatro desviaciones diferentes de la frecuencia central definen las 4 combinaciones de 2 bits (Bernal I. , 2005). (Frenzel, Carrasco, Monachesi, & Chaile, 2010)

Tabla 12 FHSS.

Tasa de Datos	Modulación	Tasa de Símbolo	Bits/Símbolo
1 Mbps	**2 GFSK**	**1 Msps**	**1**
2 Mbps	**4 GFSK**	**1 Msps**	**2**

1.2.5.3. Infrarrojo

El esquema infrarrojo 802.11 es omnidireccional en lugar de un punto a punto. Tiene un alcance posible de hasta 20 metros, el esquema de modulación para la velocidad de datos de 1Mbps es conocida como 16-PPM (Pulse Position Modulation) (Stalings, Comunicaciones y Redes de Computadores, 2004), En la modulación por posición de pulso (PPM, Figura 1-28), el valor de entrada determina la posición de un pulso estrecho en relación al tiempo del reloj del sistema.

La ventaja de PPM es que reduce la potencia de salida requerida de la fuente de infrarrojos. Para 16-PPM, cada grupo de 4 bits de datos se asigna a uno de los símbolos de 16-PPM, cada símbolo es una cadena de 16 bits. Cada cadena de 16 bits consta de 15 ceros (0) y un uno binario (1) (Stalings, Comunicaciones y Redes de Computadores, 2004).

Para una velocidad de datos de 2 Mbps, cada grupo de 2 bits de datos se le asigna una de los 4 símbolos de PPM, cada símbolo es una cadena de 4 bits. Cada cadena consta de 3 bits de ceros (0) y un uno binario (1). La transmisión actual usa un esquema de modulación de intensidad, en la que la presencia de una señal corresponde a un 1 binario y la ausencia de señal representa un 0 binario (Stalings, Comunicaciones y Redes de Computadores, 2004).

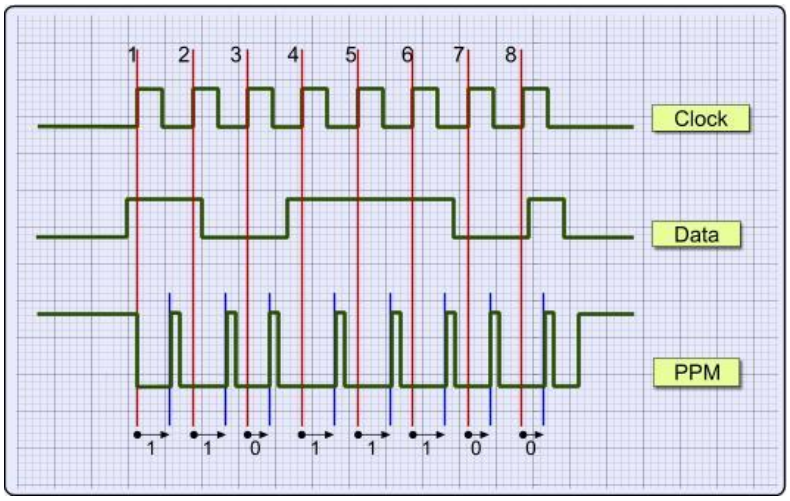


Figura 1-29 PPM.

1.2.6. Estándares 802.11

1.2.6.1. IEEE 802.11a

Hace uso de la banda de frecuencia llamada UNNI[24] (Universal Networking Information Infraestructure) (Bernal I. , 2005), dividido en 3 partes (Tabla 13).

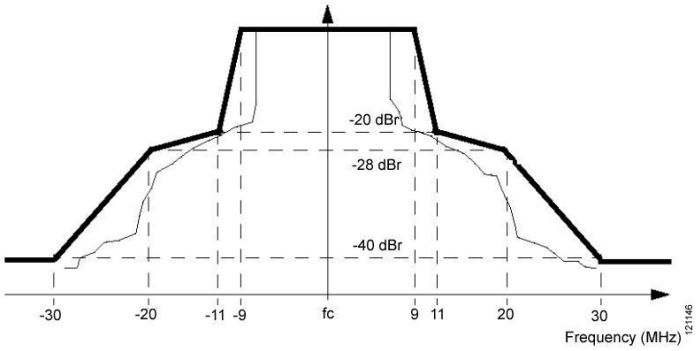
Tabla 13 Clasificación UNNI 802.11a.

UNNI	Banda	Uso
UNNI-1	**5.15 a 5.25 GHz**	**Para uso en Interiores**
UNNI-2	**5.25 a 5.35 GHz**	**Uso en interiores y exteriores**
UNNI-3	**5.725 a 5.825 GHz**	**Para uso en Exteriores**

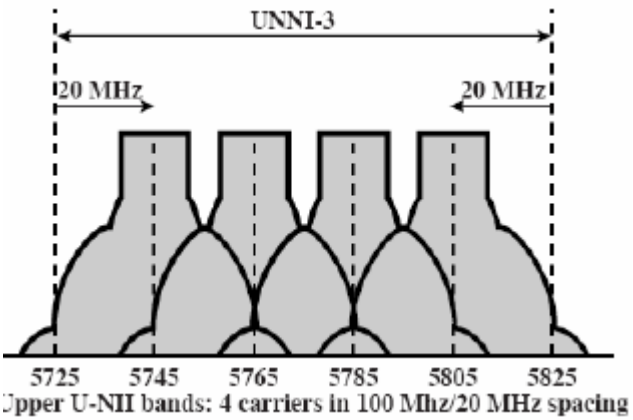
802.11a tiene varias ventajas sobre los estándares 802.11 b/g. IEEE 802.11a utiliza más ancho de banda disponible que 802.11b / g. Cada banda UNNI proporciona 4 canales que no se superponen con un total de 12 en todo el espectro asignado. Proporciona velocidades de datos mucho más altas que 802.IIb y la misma velocidad de datos máxima como 802.11g, utiliza un espectro de frecuencia diferente (5GHz), relativamente no congestionado (Bernal I. , 2005).

[24]UNNI: Universal Networking Information Infraestructure

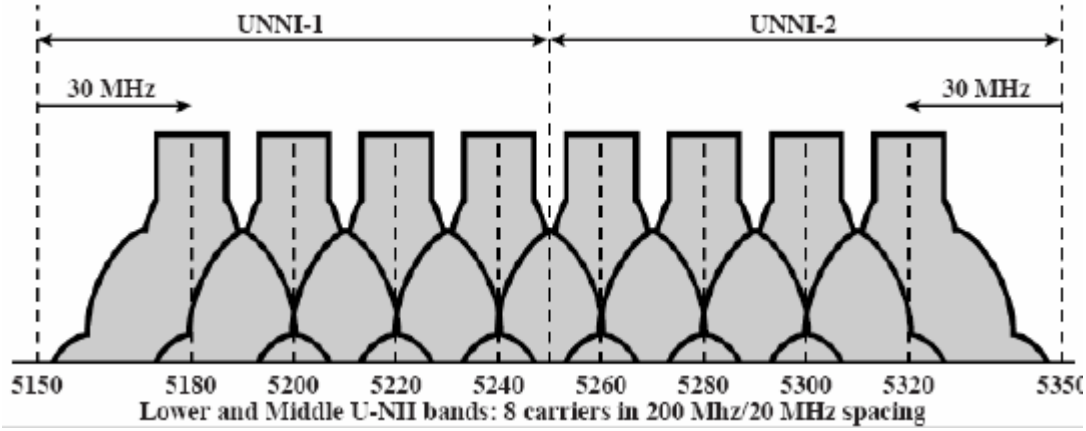
La figura 1-30a, muestra la estructura del canal usado por 802.11a. La primera parte de la figura indica la máscara del espectro de transmisión, que es definido en 802.11b de la siguiente forma: La máscara de espectro transmitido deberá tener un 0 dBr (dB con respecto a la máxima densidad espectral de la señal) ancho de banda no superior a 18 MHz, - 20 dBr en 11 MHz de frecuencia offset, - 28 dBr en 20 MHz de frecuencia de offset y -40 dBr en 30 MHz de frecuencia offset. La densidad espectral de transmisión de la señal transmitida será de la máscara espectral. El propósito de la máscara de espectro es restringir las propiedades espectrales de la señal transmitida tal que las señales en los canales adyacentes no interfieren uno con el otro. La figura 30b y 30c muestran los 12 canales disponibles para el uso de 802.11a.



a) Mascara del espectro de Transmisión.



b) UNNI-3



c) UNNI1 y UNNI 2.

Figura 1-30 IEEE 802.11 Escenario de Canales.

Codificación y Modulación

A diferencia de las especificaciones de 2,4 GHz, IEEE 802.11 no utiliza un esquema de espectro ensanchado sino que utiliza la Multiplexación por división de frecuencia ortogonal (OFDM), también llamada modulación multiportadora, utiliza varias señales portadoras a diferentes frecuencias, el envío de algunos de los bits en cada canal. Esto es similar a la de FDM[25], sin embargo, en el caso de OFDM, todos los subcanales están dedicados a una sola fuente de datos (Bernal I. , 2005).

Cada canal de 20 MHz se compone de 52 subportadoras (numeradas desde -26 hasta 26), (figura 1-30), 48 portadoras usadas para transmitir datos y 4 se usan como portadoras piloto (-21, -7, 7, 21) las cuales son usadas para monitoreo de ICC (Inter Carrier Interference), desplazamiento de frecuencia debido al efecto Doppler, la portadora 0 no se usa por razones de DSP[26].

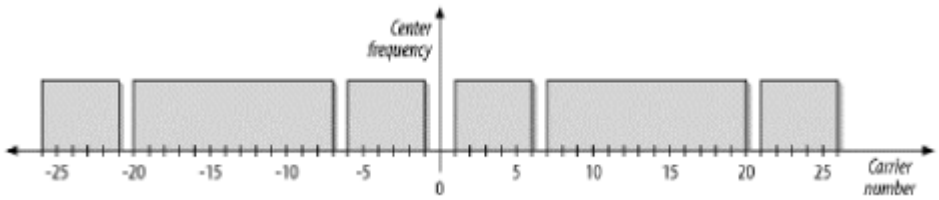


Figura 1-31 Estructura de un canal OFDM.

[25] FDM: Frecuency Division Multiplexing
[26] DSP: Procesador Digital de Señales

Para complementar OFDM, la especificación permite el uso de una variedad de modulación y las alternativas de codificación. El sistema, utiliza hasta 48 subportadoras que se modulan usando BPSK, QPSK, 16-QAM, o 64-QAM. La separación entre la frecuencia de la subportadora es 0.3125 MHz. Un código convolucional a una tasa de ½, 2/3, o ¾ proporciona corrección de errores hacia adelante. La combinación de la técnica de modulación y la velocidad de codificación determina la velocidad de datos. La Tabla 14 resume los parámetros claves de OFDM para 802.11a (Bernal I. , 2005).

Tabla 14 OFDM (802.11a).

Tasa de Datos	Modulación	Tase Codigo	Bit Codificado por Subportadora	Bits Codificado por Símbolo OFDM	Datos de Bits por Símbolo OFDM
6 Mbps	**BPSK**	**½**	**1**	**48**	**24**
9 Mbps	**BPSK**	**¾**	**1**	**48**	**36**
12 Mbps	**QPSK**	**½**	**2**	**96**	**48**
18 Mbps	**QPSK**	**¾**	**2**	**96**	**72**
24 Mbps	**16-QAM**	**½**	**4**	**192**	**96**
36 Mbps	**16-QAM**	**¾**	**4**	**192**	**144**
48 Mbps	**64-QAM**	**2/3**	**6**	**288**	**192**
54 Mbps	**64-QAM**	**¾**	**6**	**288**	**216**

Estructura de la trama de Capa Física

El propósito principal de la capa física es transmitir, el control de acceso al medio (MAC), unidades de protocolo de datos (MPDU) según las indicaciones de la capa MAC 802.11. La subcapa PLCP provee los bits de encuadre y la señalización de bits necesarios para la transmisión OFDM y la subcapa PDM realiza la codificación y el funcionamiento de la transmisión (Bernal I. , 2005).

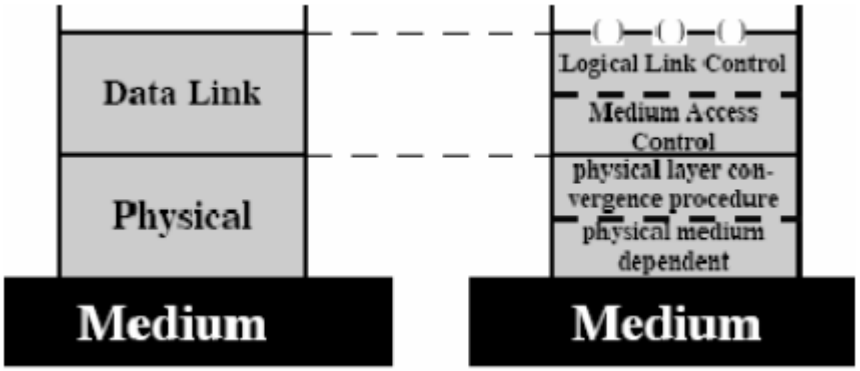


Figura 1-32Subcapa PLCP.

La figura 1-32 muestra el formato de la trama de la capa física. El campo de preámbulo PLCP permite al receptor tomar la señal OFDM entrante y sincroniza el dd3demodulador, el siguiente es el campo “Señal”, que consta de 24 bits codificados como un único símbolo OFDM. Los campos preámbulo y de señales se transmiten a los 6Mbps usando BPSK (Bernal I. , 2005).

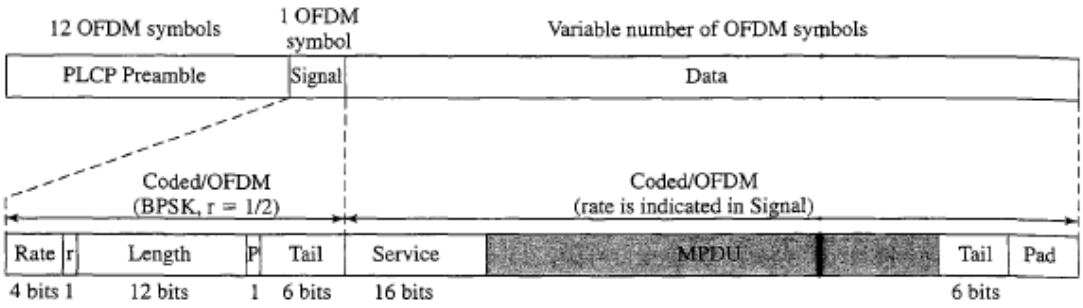


Figura 1-33 PDU Físico IEEE 802.11 a.

El campo de la señal se compone de los siguientes subcampos:

- **Tasa (Rate):** especifica la velocidad de datos en la que se transmite la parte de campo de datos de la trama.
- **R:** Reservado para un futuro uso.
- **Longitud (Length):** Número de octetos en la MAC PDU.
- **P:** Un bit de paridad para los 17 bits de los subcampos: tasa, r y longitud
- **Cola (Tail):** Consiste de 6 bits ceros (0) añadidos al símbolo para llevar al codificador convolucional al estado de cero.

El campo de datos consta de un número variable de símbolos OFDM transmitidos a la velocidad de datos especificada en el subcampo de tasa (rate). Antes de la transmisión, todos los bits de campo de datos están codificados (Bernal I. , 2005). El campo de datos consiste en 4 subcampos:

- **Servicio:** se compone de 16 bits, con los primeros 6 bits tienen el valor de 0 para sincronizar el decodificador en el receptor, y los 9 bits restantes (todos en 0) reservados para un futuro uso.
- **MAC PDU:** Transmitido desde la capa MAC.
- **Cola (Tail):** Usado para volver a iniciar el codificador de convolución.
- **Pad:** Un número de bits necesario para hacer que el campo “Datos” sea múltiplo del número de bits de un símbolo OFDM (48, 96, 192 o 288).

1.2.6.2. IEEE 802.11b

IEEE 802.11b es una extensión del sistema de DSSS de 802.11, que proporciona velocidades de datos de 5.5 y 11 Mbps en la banda ISM. La velocidad de datos de Chipping es 11 Mbps, que es el mismo que el esquema original DSSS (Tabla 4), proporcionando así el mismo ancho de banda ocupado. Para obtener una mayor velocidad de trasmisión en el mismo ancho de banda y con la misma velocidad de chipping se utiliza un esquema de modulación llamado CCK (Stalings, Comunicaciones y Redes de Computadores, 2004) (Figura 1-33).

La figura 1-34 proporciona una visión general para 11 Mbps, primero se incrementa la velocidad del reloj de los datos de 1 a 1.375 Mbps, los datos de entrada se precedan como bloques de 8 bits ($\frac{8\ bits}{símbolo} * 1{,}375\ MHz = 11\ Mbps$), en vez de usar la secuencia de Barker se usan series de secuencias complementarias que cuentan con 64 palabras únicas que pueden usarse, en contraposición a las secuencias de Barker, por CCK se pueden representar 6 bits de datos en una sola palabra y no 1 bit de datos por palabra como hacían las secuencias de Barker. La salida obtenida en la

asignación, más los 2 bits adicionales, forman la entrada al modulador OPSK.

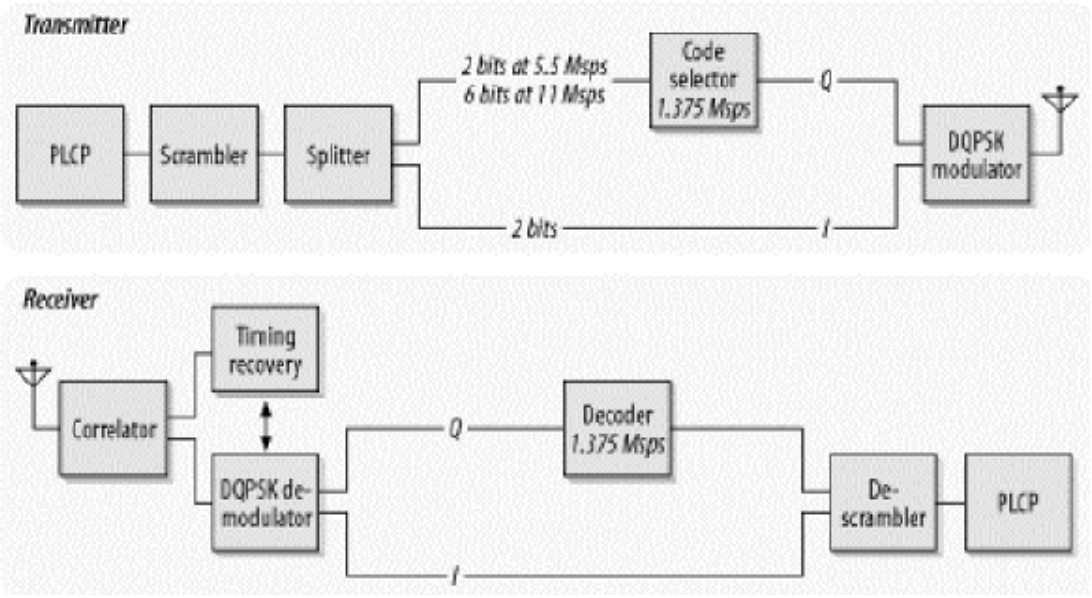


Figura 1-34 Modulación CCK.

Estructura de la capa Física

La estructura de trama de la capa física de IEEE 802.11b define 2 formatos de trama de capa física que solo difieren en la duración del preámbulo.

El preámbulo más grande de 144 bits, es el mismo que se usa en el esquema DSSS original de 802.11 y permite interoperabilidad con otros sistemas legados, el preámbulo corto de 72 bits proporciona una mejor eficiencia en el Throughput, la figura 1-34 muestra la trama de la capa física con el preámbulo corto. Los 2 preámbulos se transmiten a 1 Mbps (Bernal I. , 2005).

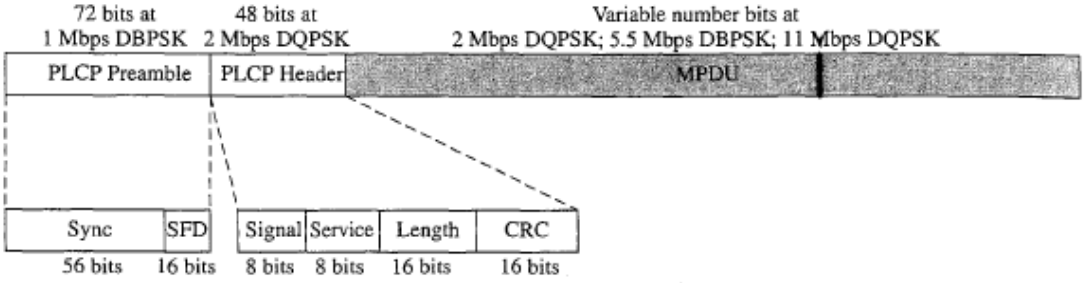


Figura 1-35 PDU 802.11b.

El campo de preámbulo PLCP habilita al receptor para adquirir una señal entrante y sincronizar el demodulador. Se compone de dos subcampos un campo de Sincronización (Sync) de 56 bits y un delimitador de 16 bits de inicio de trama (SFD).

La cabecera PLCP que se transmite a 2 Mbps usa DQPSK, se compone de los siguientes sub campos:

- **Señal (Signal):** Especifíca la velocidad de transmisión a la cual se transmite la parte del MPDU de la trama.
- **Servicio (Service):** Solo 3 de los 8 bits se usan en 802.11 b, 1 bit indica la frecuencia de transmisión y el reloj de los símbolos usan el mismo oscilador local, 1 bit indica si se usa CCK o PBCC y 1 bit actúa como una extensión del subcampo de longitud.
- **Longitud (Length):** Indica la longitud del MPDU, de forma indirecta, se especifica el número de microsegundos necesarios para transmitir el MPDU, dada la tasa de bits se puede calcular el MPDU en octetos, para cualquier tasa superior a 8Mbps, el bit de extensión de longitud del subcampo Servicio es necesario para resolver ambigüedades por redondeo.
- **CRC:** Código de Detección de errores de 16 bits, protege a los campos señal, servicio y longitud.
- **Campos MPDU:** Consiste de un número variable de bits transmitidos a la velocidad indicada en el subcampo señal, antes de transmitir todos los bits del PDU de la capa física son aleatorizados.

1.2.6.3. IEEE 802.11g

IEEE 802.11 g extiende a 802.11 b a ritmos de transmisión mayores a 20 Mbps, hasta 54 Mbps, al igual que 802.11b, el IEEE 802.11g opera en el rango de 2.4 GHz y por lo tanto los dos son compatibles. El estándar está diseñado para que los dispositivos 802.11b puedan conectarse con los AP 802.11g y los dispositivos 802.11g puedan conectarse con AP 802.11b, en

ambos casos trabajando con la velocidad más baja de 802.11b (Stalings, Wireless Communications and Networks, 2002).

IEEE802.11g ofrece una gama más amplia de opciones de combinación de los tipos de datos y modulación, como se muestra en la tabla 9. IEEE 802.11g ofrece compatibilidad con 802.11 y 802.11b especificando la misa modulación y esquemas para el entramado para 1.2, 5.5 y 11 Mbps (Stalings, Wireless Communications and Networks, 2002).

Para tasas de datos de 6, 9, 12, 18, 24, 36 y 54 Mbps, 802.11g adopta el esquema OFDM de 802.11a, adoptado para 2.4 GHz, lo que se conoce como ERP-OFMD, con el ERP (Extended Rate Physical Layer), transmisión extendida de capa física. Además el esquema ERP-PBCC es usado para proporcionar velocidad de datos de 22 y 33 Mbps (Stalings, Wireless Communications and Networks, 2002).

Tabla 15 Opciones de Capa Física IEEE 802.11g

Tasa de Datos (Mbps)	Esqueam de Modulación	Tasa de Datos (Mbps)	Esqueam de Modulación
1	**DSSS**	18	**ERP – OFDM**
2	**DSSS**	22	**ERP – PBCC**
5.5	**CCK O PBCC**	24	**ERP – OFDM**
6	**ERP – OFDM**	33	**ERP – PBCC**
9	**ERP – OFDM**	36	**ERP – OFDM**
11	**CCK – PBCC**	48	**ERP – OFDM**
12	**ERP – OFDM**	54	**ERP – OFDM**

1.2.6.4. IEEE 802.11n

En enero de 2004. El IEEE anunció la formación de un grupo de trabajo para el desarrollar una nueva versión del estándar 802.11. La velocidad real de trasmisión podría llegar a los 600 Mbps y debería ser hasta 10 veces más rápida que una red bajo el estándar 802.11 a y 802.11 g y unas 40 veces más rápida que la red bajo el estándar 802.11 b. también se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la utilización de la tecnología MIMO (Multiple Input – Multiple

Output), que permitía utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (Wikipedia).

Existen también varias propuestas alternativas que podían ser consideradas- el estándar ya está redactado y se viene implementado desde 2008. A principios del 2007 se aprobó el segundo boceto del estándar. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar. El estándar sufrió una serie de retrasos y el último lo lleva hasta noviembre del 2009. Habiéndose aprobado en enero del 2009 el proyecto 7.0 el cual iba por un buen camino para cumplir las fechas señaladas en el proyecto (Wikipedia).

A diferencia de las otras versiones del Wi-Fi, 802.11 n 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 esta característica 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5GHz ya que está menos congestionada y en 802.11 n permite alcanzar mayor rendimiento (Wikipedia).

El estándar 802.11n fue ratificado por el IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física.

En la actualidad la mayoría de los 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 5.4 GHz. Las redes que trabajan bajo los estándares de 802.11b y 802.11g, tras la reciente ratificación de 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 un buen 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 (Wikipedia).

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 el uso de espectro radioeléctrico, mediante concesión de ámbito nacional (Wikipedia).

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 1Gbps (Wikipedia). Los estándares 802.11 no incluyen una especificación de velocidad con respecto a las distancias de los objetivos, diferentes vendedores indican diferentes valores dependiendo del ambiente, la tabla 16 muestra los valores estimados para un ambiente de oficina típico.

Tabla 16 Distancias estimadas vs. La velocidad de transmisión.

Transmisión de Datos (Mbps)	802.11b	802.11a	802.11g
1	**90+**	**-**	**90+**
2	**75**	**-**	**75**
5.5(b)/6(a/g)	**60**	**60+**	**65**
9	**-**	**50**	**55**
11(b)/12(a/g)	**50**	**45**	**50**
18	**-**	**40**	**50**
24	**-**	**30**	**45**
36	**-**	**25**	**35**
48	**-**	**15**	**25**
54	**-**	**10**	**20**

CAPITULO 2

2. PROTOCOLOS DE SEGURIDAD IEEE 802.11 Y TÉCNICAS DE MONITORIZACIÓN DE TRAFICO DE RED.

2.1. Seguridad.

El Estándar inalámbrico de comunicación IEEE 802.11 y los grupos de trabajo establecieron la posibilidad de conferir a esta tecnología diferentes características tales como, la capacidad de integridad de datos, confidencialidad y autenticidad de las estaciones. De estos parámetros existe 3 protocolos de seguridad basados en la norma IEEE 802.11 y IEEE 802.11i.

- **Confidencialidad:** Los datos son protegidos a la intercepción de personas no autorizadas.
- **Integridad:** Garantizar que los datos no han sido modificados.
- **Autenticación:** Garantizar que los datos vienen de quien se supone deben venir (origen de los datos), Autorización y control de acceso, antes de garantizar el acceso a los datos se debe encontrar, quien es el usuario (autenticación) y la operación de acceso que está permitida (autorización) (Bernal I. , 2005).

Las WLANs son vulnerables a ataques especializados que se centran en las debilidades tecnológicas, las seguridades de 802.11 en las WLAN son relativamente nuevas. Hay debilidades en la parte de configuración, ya que algunas compañías no utilizan las características de seguridad de WLAN en todos sus campos, muchos dispositivos vienen con password de administrador predefinidos que nunca se cambian.

Hay debilidades en cuanto a políticas, sino existe una política clara en el uso de dispositivos inalámbricos, los empleados, o gente extraña a la red pueden instalar sus propios APs que muchas de las veces no están asegurados (Bernal I. , 2005).

Teniendo en cuenta todos estos inconvenientes que se pueden presentar en una red Inalámbrica y con el propósito de comprender las vulnerabilidades que afectan a cada uno de los protocolos, se procederá a conocer el funcionamiento de cada protocolo. Estableciendo primordialmente la manera en la cual las estaciones se autentican a un AP y cuál es el cifrado que se ocupa en dicha comunicación.

2.1.1. SSID (Service Set Identifier)

Usado como una forma básica de seguridad, está compuesto de 1 a 32 caracteres ASCII. Muchos de los APs tienen la opción como “SSID broadcast” y “permitir cualquier SSID”, estas características suelen estar habilitadas por defecto y hacen fácil la instalación de la red, permitir cualquier SSID permite el acceso a un cliente con un blank SSID. Con el SSID broadcast se envía paquetes de beacom que contienen el SSID. Si deshabilitamos estas opciones podríamos tener una red no segura (Bernal I. , 2005).

En algunas WLANs se contrala el acceso ingresando las direcciones MAC de cada cliente en los APs, este tipo de seguridad es orientada a la dirección MAC y no a los usuarios, no está especificado en el IEEE802.11, adicional mucho de los vendedores han implementado autentificación a nivel de MAC y alguno de estos dispositivos permiten pedir la lista de direcciones MAC a un servidor centralizado. Todas estas características no están ocultas para un sniffer ya que estos parámetros pueden ser encontrados y visualizados (Bernal I. , 2005).

2.1.2. WEP (Wired Equivalent Privacy)

2.1.2.1. Definición

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable), es el algoritmo opcional de seguridad para poder brindar una protección a las

redes inalámbricas. WEP[27] es un sistema de encriptación estándar soportado por la mayoría de soluciones inalámbricas (Gimenez, 2008).

El canal de Radio Frecuencia RF es un medio de comunicación inseguro, ya que cualquier persona o estación dentro del rango de la señal puede recibir los satos que se están emitiendo por otra estación. La IEEE con estos datos implementó un mecanismo de seguridad que pudiera otorgar al medio inalámbrico características del cableado (Gimenez, 2008).

Aunque en los entornos RF pueden residir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien ajeno a la red pueda comprometer los datos transmitidos consiste en utilizar mecanismos de encriptación. El propósito de WEP es garantizar que los sistemas dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. El segundo propósito de WEP es evitar que personas no autorizadas puedan acceder a las redes WLAN, es decir proporcionar autenticación, este propósito no está anunciado en el estándar IEEE 802.11, pero se considera una importante característica del algoritmo (Gimenez, 2008).

WEP utiliza una misma clave simétrica y estática en las estaciones y el AP, El estándar no descubre ningún mecanismo de distribución de claves automáticas, con esto obligamos a los usuarios a escribir una clave manualmente en cada uno de los elementos de la red. Con esto tenemos algunos inconvenientes tales como que la clave está siendo almacenada en todos los AP, y otro problema es que al ser una distribución manual de la clave ocasiona un aumento de mantenimiento por parte del administrador de la red (Gimenez, 2008).

2.1.2.2. Cifrado

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un AP, todos estos datos enviados y recibidos entre los dos puntos pueden

[27] WEP: Wired Equivalent Privacy

ser encriptados utilizando esta clave compartida, mediante el algoritmo de cifrado RC4 (Rivest Cipher 4) de RSA1 Data Security. Para proteger estos datos que están siendo transportados, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto, lo que genera un valor de comprobación de integridad (ICV). El valor de comprobación de integridad es una especie de huella digital de los datos a transmitir. El Vector IV es simplemente una numeración que está adjunta a cada paquete WEP y que es utilizado tanto para cifrar el mensaje como para descifrarlo (Gimenez, 2008).

El algoritmo de encriptación utilizado RC4 según el estándar es de 64 bits, pudiendo alcanzar los 128 bits. Estos 64 bits están conformados por 24 bits del vector de inicialización más 40 bits de la clave secreta. Estos 40 bits son los que se deben distribuir manualmente, el vector de inicialización (IV), es generado dinámicamente y debería ser diferente para cada trama. El objetivo de IV es cifrar con claves diferentes para impediré que un posible atacante pueda capturar el suficiente tráfico con la misma clave y con esto poder deducir la clave (Gimenez, 2008).

RC4 es uno de los puntos débiles que el protocolo WEP presentó. RC4 consta de 2 módulos diferenciados, un algoritmo barajador o programador de claves llamad KSA y un módulo de generación de números pseudoaleatorios denominado PRNG (Pseudo Random Number Generator), ambos implementados por Ron Rovest en 1987 y publicados de manera clandestina en 1994 (Gimenez, 2008).

KSA[28] (Key Scheduling Algorithm), es un pequeño algoritmo de programación de claves que toma como entrada el par IV-Clave secreta. Dicha entrada consiste en una trama de 64 o 128 bits dependiendo del cifrado utilizado. Como resultado genera un vector S de 256 elementos totalmente desordenados.

PRNG[29], toma como entrada el mencionado vector S generado como salida una trama de bits pseudoaleatoria de igual tamaño a los datos a cifrar.

[28] KSA: Key Scheduling Algorithm
[29] PRNG: Pseudo Random Number Generator

2.1.2.3. Autenticación

WEP proporciona 2 tipos de autenticación, un sistema abierto en el que todos los usuarios tienen permiso para poder acceder a la WLAN y una autenticación mediante claves compartidas que controla el acceso a la WLAN y evita accesos no autorizados (Gimenez, 2008).

De los dos niveles de autenticación, la autenticación mediante la clave compartida es el modo menos seguro, en este método se unas una clave secreta compartida entre todas las estaciones y los APs del sistema WLAN las cuales coinciden con las claves de cifrado. Cuando una estación trata de conectarse con un AP, éste replica con un texto aleatorio, que constituye el desafío. La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío enviado anteriormente. Si estos dos valores son idénticos, el AP envía un mensaje de confirmación a la estación y la acepta dentro de la red. Se la estación no dispone de una clave, o si a su vez la respuesta es incorrecta, el AP rechaza evitando que la estación acceda a la red (Gimenez, 2008).

2.1.2.4. Funcionamiento

En este punto podremos definir la metodología implementada por WEP para cifrar o descifrar una trama de datos con destino el medio inalámbrico, asumiendo que se utiliza una encriptación de 64 bits (Gimenez, 2008).

- En primera instancia la clave compartida formada por una cadena de 40 bits a la cual se le concatena un vector de inicialización (IV) de 24 bits formando así una cadena de 64 bits.
- Se calcula el CRC-32 de los daos que se requieren cifrar (hasta 2312 bates) también llamada ICV, formando el par Datos + ICV.

- Se aplica el algoritmo PRNG de RC4 a la cadena que contienen la clave compartida más el vector de inicialización, resultando la llamada Keystream de igual longitud que la salida del paso 2.
- Finalmente se aplica la función XOR entre el Keystream y le par Datos+ICV
- Al resultado anterior se le añade el IV utilizada y la cabecera IEEE 802.11, resultando una trama cifrada y lista para transmitirse.
- En la figura 2-1, se puede encontrar el procedimiento completo, tanto para el proceso de cifrado como descifrado.

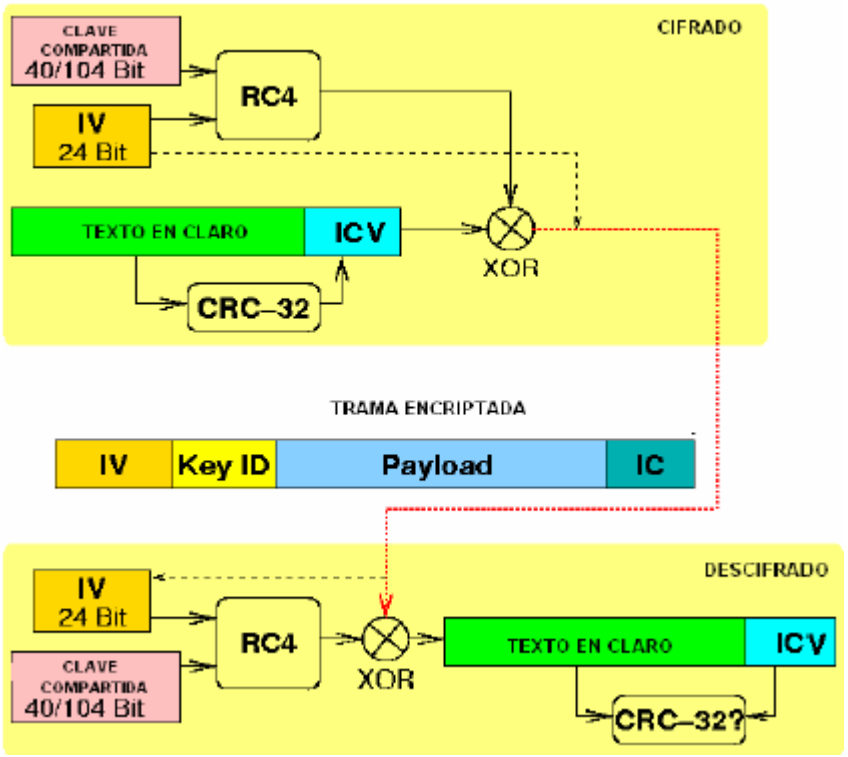


Figura 2-1 Cifrado y Descifrado WEP.

En este instante la trama ha sido inyectada al medio RF siendo recibida por la estación destino. Cabe notar que en todo momento la cabecera de la trama 802.11 viaja pudiendo ser interpretada por cualquier estación que esté a la escucha en el medio. Los datos que se pueden extraer de una trama encriptada y no siendo conocedor de la clave compartida serían, la dirección

BSSID, Dirección Destino, Dirección Origen, IV utilizado (Gimenez, 2008). Así pues un receptor lícito que fuera conocedor del secreto compartido procedería a desencriptar la trama de la siguiente manera:

- El receptor, extrae de la trama el valor del IV transmitido, concatenándole dicho valor a la llave que tanto el emisor como el receptor conocen.
- Seguidamente se le aplica RC4 resultando un Keystream de longitud igual a los datos cifrados.
- Se realiza la operación XOR entre el Keystream y los datos cifrados.
- Resultando el texto más la comprobación de redundancia cíclica.
- Se comprueba que la trama es válida mediante el cálculo de CRC-32 correspondiente.

2.1.3. Protocolo WPA

2.1.3.1. Definición

WPA (Wi-Fi Protected Access) fue desarrollado por la Wi-Fi Alliance[30] y el IEEE en 2003 como resultado de aplicar el borrador del estándar IEEE 802.11i. Su principal objetivo es llenar todas las carencias de seguridad detectadas en el protocolo nativo WEP. WPA no representa un protocolo que pueda asegurar una protección 100% del medio inalámbrico ya que depende como en muchos casos del usuario final. WPA es un estándar a nivel de MAC orientado tanto al mundo de las pequeñas oficinas y al usuario doméstico como a las grandes empresas (Gimenez, 2008).

[30] Wi-Fi Alliance es una asociación internacional son ánimo de lucro creada en 1999, con el objetivo de certificar los productos derivados del estándar 802.11

2.1.3.2. Características

Dentro del protocolo WPA tenemos diferentes característica entre las más sobresalientes tenemos.

- Distribución dinámica de claves.
- Incremento de la robustez del vector de inicialización.
- Aplica nuevas técnicas de integridad y autenticación.

2.1.3.3. Autenticación

El método empleado por WPA para autenticar las estaciones es uno de los puntos débiles del protocolo de seguridad. Por lo que respecta a la autenticación en función al entorno de aplicación del método es posible emplear 2 métodos de autenticación diferentes WPA-PSK (Pre Shared Key) o WPA EAP[31] (Extensible Authentication Protocol) (Gimenez, 2008).

En entornos personales, como usuarios residenciales y pequeñas empresas, se utiliza WPA con clave pre compartida conocida como WPA-PSK y autenticación IEEE 802.1X. En estos entornos de trabajo no es posible colocar un servidor de autenticación centralizado o un marco EAP. En este contexto WPA se ejecuta en un modo especial conocido como “Home Mode” o PSK, que permite la utilización de claves configuradas manualmente y facilitar aso el proceso de configuración del usuario doméstico.

El usuario solo debe introducir una clave de 8 a 64 caracteres, conocida como clave maestra, en su AP modem o Router inalámbrico residencial, así como en cada uno de los dispositivos que quiera conectar a la red. De esta forma solo se permitirá el acceso a aquellos dispositivos que son conocedores de la contraseña. Se puede asegurar que la clave proviene de una relación de acuerdo único para generar el cifrado TKIP[32] (Temporal Key Integrity Protocol) en la red.

[31] EAP: Extensible Authentication Protocol
[32] TKIP: Temporal Key Integrity Protocol

A diferencia de WEP, WPA utiliza varias claves temporales diferentes para cifrar el payload dependiendo del tráfico al que pertenece el paquete, unicast, broadcast o multicast y a las que denomina PTK[33] (Primary Temporal Key) para el primero y GTK[34] (Group Temporal Key) para los dos restantes. Estas Keys tiene un proceso de regeneración de claves cada cierto tiempo, con el objetivo de impedir que una estación legítima pueda llegar a capturar la calve de la sesión utilizada (Gimenez, 2008).

La PSK es conocida por todas las estaciones del medio además del AP, Cabe mencionar que el PK no es la cadena utilizada para encriptar los paquetes de datos, tampoco se lo usa ara autenticar el AP, sino que se construye la PMK (Primary Master Key), a partir de PSK y un proceso de modificación. El resultado es una cadena de 256 bits. Pero se usa varios elementos para formar la PMK, tales como, la contraseña pre compartida, el ESSIP del AP, la longitud del ESSID y una barajado de 4096 procesos. Todo ello es generado por una función matemática llamada PBKDF2 ofreciendo como resultado una clave PMK de 256 bits (Gimenez, 2008).

Una vez obtenida esta clave se puede comenzar con el proceso de autenticación con el AP al que se lo denomina 4-Way Handshake o saludo inicial el cual se lo representa en la siguiente figura 2-2.

[33] PTK: Primary Temporal Key
[34] GTK: Group Temporal Key

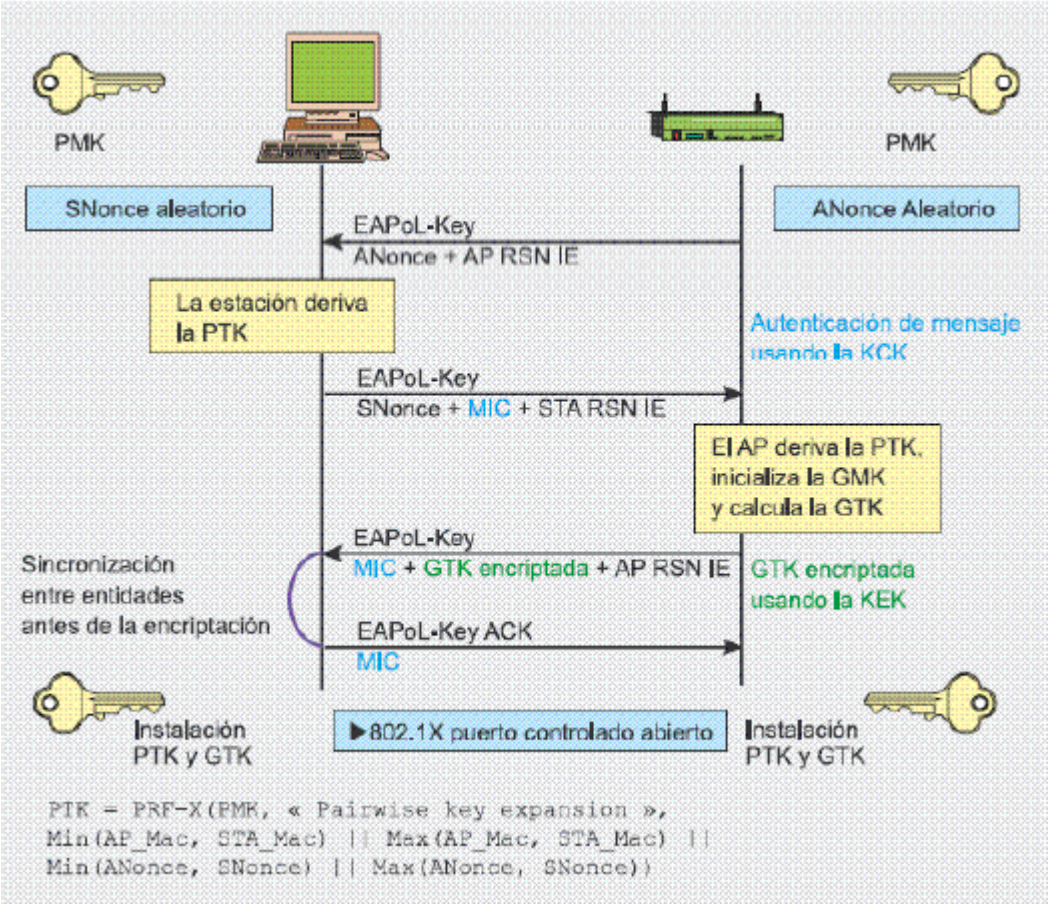


Figura 2-2 4-Way Handshake.

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

Pero para la generación del PTK se utiliza una función pseudoaleatoria PRF-X que toma como fuente los siguientes datos.

- PMK: Calculada mediante la PSK y el algoritmo PBKDF2.
- SNonce: Número aleatorio determinado por la estación.
- ANonce: Número aleatorio determinado por el AP.
- MAC del AP: MAC del punto de acceso.
- MAC de la estación.

En este punto, la comunicación es inicializada mediante el envío de un paquete tipo “EAPOL Start”, desde la estación al AP. Seguidamente el AP genera un número aleatorio “ANonce” que es transmitido a la estación. Ésta

contesta enviándole otro número aleatorio. SNonce. En estos momentos ambos pueden generar su PTK con la que cifraran el tráfico unicast, a partir de los valores mencionados. A su vez el AP está en disposición de generar la GTK procediendo a transmitirla a la estación de forma cifrada. Por último se envía un paquete de reconocimiento cerrando así el proceso de autenticación (Gimenez, 2008).

En tanto a la autenticación en ambientes empresariales los requerimientos estrictos de cifrado y autenticación hacen que sea más adecuada la utilización de WPA con los mecanismos de IEEE 802.1X y el protocolo de autenticación extensible EAP, que disponen de procedimientos de gestión de claves dinámicos. EAP es utilizado para el transporte extremo a extremo para los métodos de autenticación entre el dispositivo de usuario y el pinto de acceso. Mientras que IEEE 802.1X es utilizado como marco para encapsular los mensajes EAP en el enlace radio. El conjunto de estos 2 mecanismos junto con el esquema de cifrado forman una fuerte estructura de autenticación, que utiliza un servidor de autenticación centralizado, como por ejemplo RADIUS.

2.1.3.4. Cifrado.

El equipo de desarrollo de WPA después de tener claras las vulnerabilidades conocidas de WEP incorporó las siguientes mejoras:

- Creación de un vector de inicialización extendido a 48 bits frente a los 24 bits de WEP, a su vez se implementó reglas de secuenciación para la numeración.
- Nuevos mecanismos de derivación y distribución de claves. Gracia a la incorporación de métodos de intercambio inicial de números aleatorios evitando así ataques de “man in the middle”
- WAP Utiliza TKIP (Temporal Key Integrity Protocol) como encriptación, para la generación de claves por paquetes, TKIP utiliza

el algoritmo de cifrado RC4, al igual que su predecesor WEP, pero elimina el problema de las claves estáticas compartidas. A su vez TKIP incrementa el tamaño de las claves pares y claves en grupo para el cifrado de datos de los 40 bits de WEP se pasa a un cifrado de 128 bits. Además las claves empleadas no son compartidas por todos los usuarios de la red.

- WPA utiliza TKIP para codificar los datos. Utiliza una semilla inicial de 128 bits compartida por todos los usuarios y los AP. Después esa clave temporal se combina con la dirección MAC del usuario y se le añade un vector de inicialización de 16 bits para producir la clave que cifrará los datos, mediante este proceso cada usuario utilizará deferentes calves para la encriptación.
- TKIP fuerza por defecto un cambio de las claves entre el usuario móvil y el AP para cada paquete de información transmitida y aplicando un algoritmo de “Hash” o mezclado a los valores del vector de inicialización. El cambio de la clave de cifrado está sincronizado entre el usuario y el AP.
- WPA implementa como WEP, control de integridad de mensaje, pero con mayor robustez, WAP incluye el llamado MIC o “Michael” para verificar que un paquete no ha sido alterado por una estación ilícita. La función MIC, es un Hash criptográfico de un solo sentido, el cual reemplaza al CRC-32 utilizado por WEP. MIC provee una función matemática de alta fortaleza en la cual el receptor y el transmisor deben computar, y luego comparar, sino coinciden los datos se asumen como corruptos desechando el paquete. De este modo TKIP impide que un atacante pueda alterar los datos que se transmiten dentro de un paquete.

2.1.3.5. Funcionamiento

En este punto especificaremos brevemente como se produce el cifrado de la información para una trama unicast (Gimenez, 2008).

- Inicialmente se genera el IV correspondiente al paquete a enviar, esta numeración comienza en 0. Mediante el IV la dirección de destino y la PTK se genera la semilla que utilizará el algoritmo de cifrado CR4.
- Mediante la función PNRG se genera la cadena utilizada para cifrar los datos.
- Por otra parte la MAC origen y destino, la prioridad del paquete y los datos a remitir son pasados como entrada al algoritmo de control de integridad MIC.
- Seguidamente se calcula el ICV de la cadena MIC
- Se produce a continuación la operación XOR entre la tema Datos+MIC+ICV y la cadena de cifrado salida de PNRG.

La siguiente figura nos indica el proceso de encriptación de una trama 802.11

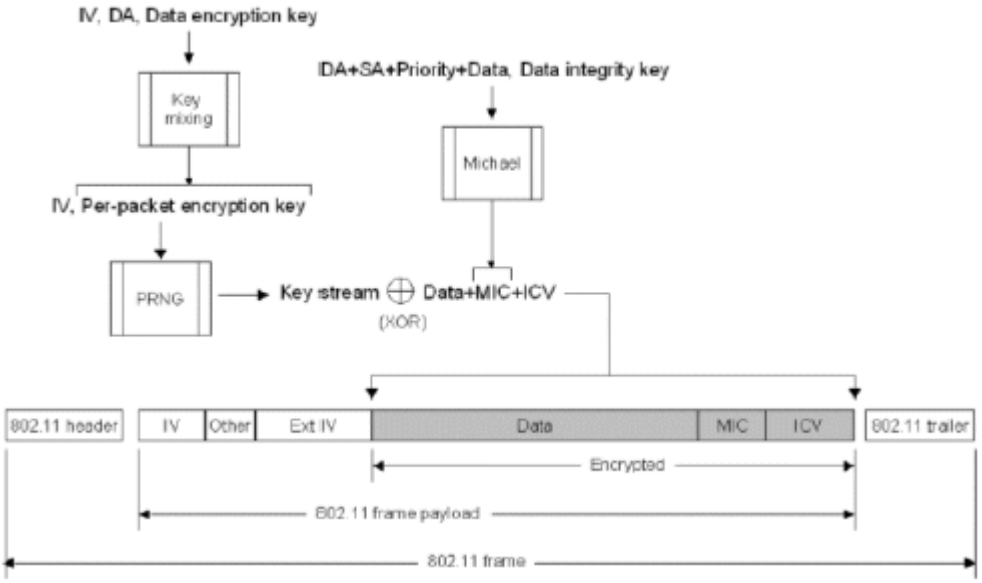


Figura 2-3 Encriptación de una trama 802.11 mediante WPA.

Para desencriptar una trama cifrada mediante TKIP se realiza las siguientes operaciones:

- Se desencapsula el IV, el IV ext., la dirección de destino que son concatenados con la clave PTK.
- La cadena resultante es introducida como entrada al algoritmo PNRG generando la clave de cifrado de paquete.
- A continuación se procede a realizar la XOR entre los datos encriptados y la clave de cifrado calculada anteriormente.
- La salida del punto anterior genera los datos, a los cuales se les aplica MIC para comprobar su integridad.

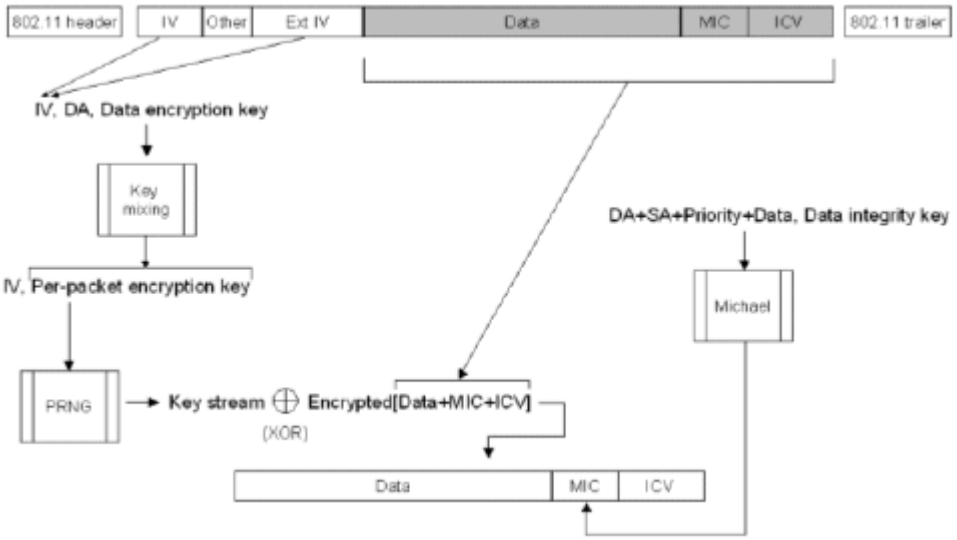


Figura 2-4 Desencriptación trama 802.11 mediante WPA.

2.1.4. WPA2

En septiembre del 2004 la alianza Wi-fi lanzó el protocolo de seguridad WPA2, que suponía ser la versión certificada interoperable de la especificación completa del estándar IEEE 802.11i, que fue ratificado en junio del 2004. Para llevar a cabo la certificación se basa en las condiciones obligatorias de la última versión del estándar IEEE 802.11i. WPA2 es la implantación aprobada por la Wi-fi Alliance interoperable con el estándar IEEE 802.11i (Gimenez, 2008).

Aunque los productos WPA siguen siendo seguros, muchas organizaciones han estado en la búsqueda de una tecnología interoperable y certificada basada en el estándar IEEE 802.11i o han requerido del cifrado de AES por razones internar o reguladores. WPA2 resuelve esta necesidad, basándose en su predecesor WPA y ha sido diseñado para poder cumplir con las exigencias de un entorno empresarial.

IEEE 802.11i y WPA2 son idénticos, siendo mínimas las diferencias entre los dos. Ambos emplean como código de cifrado AES/CCMP en lugar de RC4/TKIP usado en WPA. A su vez existen 2 características importantes.

- WPA2 permite funcionar en modo mixto con TKIP y CCMP para su compatibilidad hacia atrás con WPA.
- WPA2 carece de ciertos aspectos definidos en IEEE 802.11i en cuanto a los servicios de voz inalámbricos utilizados para prevenir la latencia de la señal o la pérdida de información durante el roaming.

WPA2 emplea al igual que IEEE 802.11i un mecanismo de cifrado más avanzado como AES. No obstante WPA2 es compatible con WPA, por ellos algunos productos WPA pueden ser actualizados a WPA2 por software.

WPA2 permite dos modos de llevar a cabo la autenticación según el ámbito de aplicación, si es empresarial (IEEE 802.1X/AP) o personal (PSK). Actualmente el IEEE y la Wi-FI Alliance están intentando unificar WPA2 con IEEE 802.11i.

2.1.4.1. Autenticación

WPA2 utiliza los protocolos de autenticación definidos por el IEEE 802.11i y descritos anteriormente en el capítulo donde se especifica el protocolo WPA.

2.1.4.2. Cifrado

El proceso de cifrado de la información se realiza mediante lo establecido por IEEE 802.11i y comentado en WPA. La principal diferencia entre WPA y WPA2 es la mejora de su algoritmo de cifrado. El ya utilizado por WEP y WPA RC4 es sustituido por AES, un cifrado de bloques de claves simétricas que utiliza grupos de bits de una longitud fija. Un algoritmo de claves simétrica significa que utiliza la misma clave maestra tanto para cifrar como para descifrar los datos.

Mediante AES, las tramas de bits del texto plano son cifradas en bloques de 128 bits calculados independientemente (Gimenez, 2008).

2.1.5. Estándar de seguridad IEEE 802.1X

IEEE 802.1X es un estándar propuesto por el IEEE el cual es implementado ampliamente por los fabricantes de redes LAN tanto cableadas como inalámbricas. Dicho estándar fue diseñado para ofrecer seguridad perimetral de la red, específicamente en autenticación y control de acceso a nivel de puerto, para usuarios LAN (Chiu), el estándar fue diseñado en un principio para redes cableadas pero totalmente adaptables a redes inalámbricas empleando claves dinámicas en lugar de claves estáticas utilizadas en la autenticación WEP por lo que el sistema se compone de:

- Estaciones clientes.
- Puntos de Accesos
- Servidores de Autenticación (AS)

2.1.5.1. Protocolo de autenticación extensible EAP

Es uno de los elementos básicos del 802.11X desarrollado como mejora del PPP, el cual usa como método de autenticación “username” y “password”.

EAP utiliza métodos de autenticación arbitrarios, que sirve como soporte a protocolos propietarios de autenticación, gestiona las contraseñas en mecanismos de desafío-respuesta y es capaz de trabajar con tecnología de clave pública, pudiendo así utilizar métodos de autenticación a través de certificados, tarjetas inteligentes o inalámbricas (Chiu).

El estándar 802.1X describe como encapsular mensajes de EAP en tramas Ethernet, es decir, el funcionamiento del protocolo EAP en redes LAN ya sea cableadas o inalámbricas (EAP over LANs EAPOL).

Adicional para contrarrestar las debilidades de 802.11, diversos fabricantes crearon varios métodos EAP, entre los cuales se destacan los siguientes:

- EAP-LEAP (Light EAP), desarrollado por Cisco y el cual provee un mecanismo de autenticación mutua basada en password, es decir, requiere que la estación del usuario se autentique contra la red, pero que también la red se autentique con el usuario, asegurando de esta manera que los usuarios son los que dicen ser.
- EAP-TLS (Transport Layer Security EAP), desarrollado por Microsoft, el cual ofrece autenticación mutua, credenciales seguras y claves de encriptación dinámicas, requiere de la distribución de certificados digitales por lo que puede llegar a producir overhead.
- EAP-TTLS (tunneled TLS) permite solo certificados del servidor, no de cliente, permite que los usuarios sean autenticados dentro de las WLANs con las credenciales existentes, utilizando criptografía de clave pública/privada, es más sencillo de gestionar y económico que EAP-TLS.

2.1.5.2. Servidor de autenticación RADIUS.

RADIUS (Remote Authentication Dial-Up user Service), es un servidor de punto final que es responsable de recibir solicitudes de conexión y de la autenticación de los usuarios para luego retomar toda la información de

configuración necesaria para el cliente. Este servidor desempeña la autenticación utilizada por EAP. Una de las características importantes es la capacidad de manear sesiones, notificando cuando comienza y termina una conexión, pudiendo utilizar estos valores para generar estadísticas (Chiu).

2.1.5.3. Funcionamiento de 802.1X

El proceso de autenticación se lleva a cabo de la siguiente manera:

- El cliente establece una conexión al AP (una tarjeta de red conectada a un punto de datos o una tarjeta de red inalámbrica asociada a un AP).
- El cliente se encuentra en un estado no autorizado, ya que ninguna dirección IP le es asignada o no se le permite de ninguna manera el acceso a la red, es decir, que el AP sólo le permite al cliente enviar mensajes 802.1x necesarios para su autenticación (estos son mensajes EAP sobre Wireless EAPOW)
- Entonces el cliente envía una solicitud de acceso a la red (Mensaje EAP Start) al AP (802.1x define el uso de este protocolo), mandando las credenciales al usuario, estas pueden ser el nombre de usuario y contraseña.
- El AP reenvía esta petición al servidor de autenticación RADIUS para su aprobación y si las credenciales son válidas, envía de regreso un desafío al autenticador y este desempaqueta el datagrama IP y lo reempaqueta dentro del EAP sobre un protocolo LAN (EAPW), para luego mandar el mensaje al cliente.
- Si el cliente responde de manera exitosa, el servidor le responde a través del AP con un mensaje de éxito (“EAP Succes”), de lo contrario responde con un mensaje de fallo (“EAP Failure”).
- De esta manera queda establecida la autenticación, aunque el autenticador también pueda prepararse para imponer diferentes

atributos o reglas en cada cliente, proveyendo así varios niveles de restricciones de acceso a los mismos.

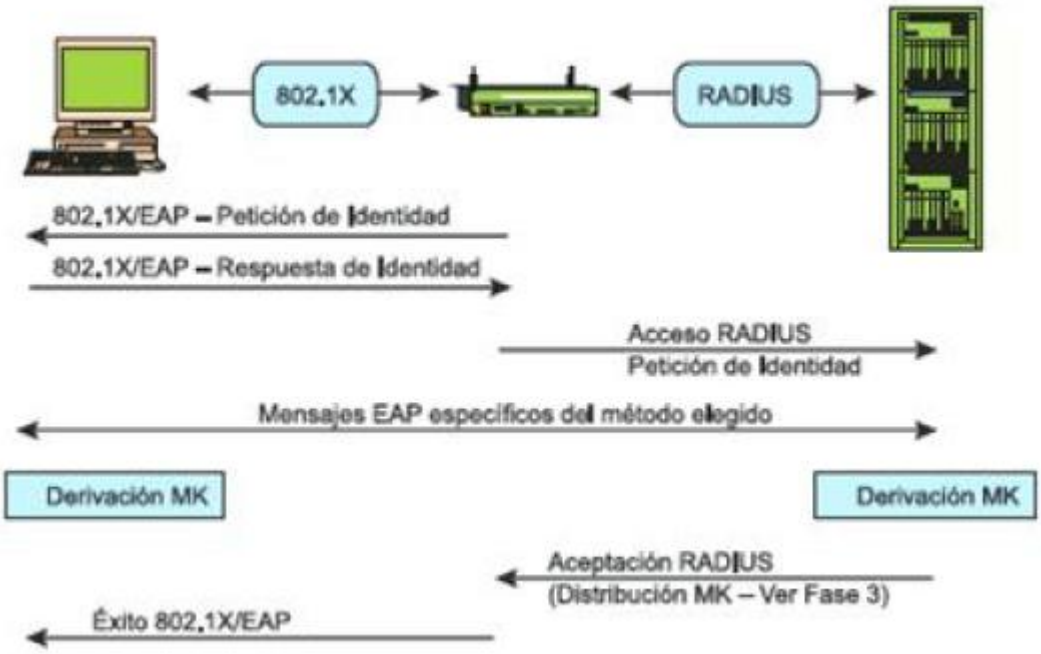


Figura 2-5 Proceso de Autenticación 802.1X.

2.2. Importancia del uso de Herramientas de Monitorización

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red son actividades de mucha importancia y de gran relevancia para poder brindar un buen servicio a los usuarios, sean estos internos o externos. Con estos criterios se puede realizar un esquema que sea capaz de notificar fallas en una red y de mostrarnos el comportamiento mediante el análisis y recolección de tráfico. Dentro de este monitoreo un administrador puede enfocarse en dos tipos de monitorización activa o pasiva y sus diferentes técnicas.

Para poder adquirir el tráfico para poder analizar el comportamiento de la red y poder verificar si existe algún problema dentro de la red, existe un gran número de herramientas, sean éstos gratuitos o con licencia pagada, los cuales nos ayudaran a capturar el tráfico adecuado para su posterior análisis y toma de decisiones.

La elección de estas herramientas depende de varios factores, sean estos humanos, económicos como de infraestructura.

- El perfil de los administradores, sus conocimientos en determinados sistemas operativos.
- Los recursos económicos disponibles.
- El equipo de cómputo que se disponga.

2.3. Método Activo o Intrusivo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este tipo de enfoque tiene la característica de agregar tráfico en la red y es utilizado para medir el rendimiento de una red (Medellin).

2.3.1. Técnicas de Monitoreo Activo

- **Basado en ICMP**
  - Diagnosticar problemas en la red.
  - Detectar retardo, pérdida de paquetes.
  - Disponibilidad de host y redes.

- **Basado en TCP**
  - Tasa de transferencia.
  - Diagnosticar problemas a nivel de aplicación

- **Basado en UDP**
  - Pérdida de paquetes en un sentido (one-way).
  - RTT (Traceroute)

- **Wireless Spoofing**

Hay técnicas de ataque conocidos como la suplantación de identidad en las redes cableadas e inalámbricas. El atacante construye tramas rellenando los campos seleccionados que contienen direcciones o identificadores con los valores que buscan, pero que no existen legítimas, o con valores que pertenecen a otros. El atacante habría recogido estos valores legítimos a través del sniffing.

- **Dirección MAC Spoofing**

El atacante generalmente desea ocultarse, pero la actividad de sondeo inyecta tramas que son observables por los administradores del sistema. El atacante se llena el campo Dirección MAC del remitente de las tramas inyectadas con un valor falso para que su equipo no sea identificado.

APs típicos controlan el acceso al permitir sólo aquellas estaciones con direcciones MAC conocidas. O el atacante tiene que comprometer un sistema informático que tiene una estación, o falsifica con direcciones MAC legítimos en tramas que fabrica.

Las direcciones MAC se asignan en el momento de su fabricación, pero establecer la dirección MAC de la tarjeta inalámbrica o AP a un valor elegido arbitraria es una simple cuestión de la invocación de una herramienta de software apropiado que dialoga con el usuario y acepta valores. Estas herramientas se incluyen de manera rutinaria cuando se compra una estación o AP.

El atacante, sin embargo, cambia la dirección MAC mediante programación, envía varias tramas con esa dirección, y repite esto con otra dirección MAC. En un período de un segundo, esto puede suceder varios miles de veces.

Cuando un AP no está filtrando direcciones MAC, no hay necesidad de que el atacante utilice direcciones MAC legítimas. Sin embargo, en ciertos ataques, el atacante necesita tener un gran número de direcciones MAC de los que podía cobrar por el husmeo. Direcciones MAC se generan al azar.

Sin embargo, no toda la secuencia aleatoria de seis bytes es una dirección MAC. El IEEE asigna a nivel mundial los tres primeros bytes, y el fabricante opta por los últimos tres bytes. Los números asignados oficialmente están disponibles al público. El atacante genera una dirección MAC aleatoria seleccionando un asignadas IEEE tres bytes adjuntas con un tres bytes aleatorios adicionales.

- **Spoofing Frame**

El atacante inyecta tramas que son válidos por especificaciones 802.11, pero cuyo contenido es falso.

Las tramas por si mismas no son autenticadas en las redes 802,11. Así que cuando una trama tiene una dirección de origen falsa, no puede ser detectada a menos que la dirección sea totalmente falsa. Si la trama a ser suplantada es de gestión o control, no hay cifrado de tratar. Si se trata de una trama de datos, tal vez como parte de un ataque MITM en curso, la carga útil de datos debe estar debidamente encriptado.

La construcción de la secuencia de bytes que constituye una trama falsa es una cuestión de programación una vez que el atacante ha reunido la información necesaria a través del husmeo y la exploración. Hay bibliotecas de software que facilitan esta tarea. Ejemplos de estas bibliotecas son libpcap (sourceforge.net/ projects/libpcap), libnet (libnet.sourceforge.net), libdnet (libdnet. sourceforge.net) y libradiate (www.packetfactory.net/projects/libradiate).

La dificultad aquí no es en la construcción de los contenidos de la trama, sino en conseguir, que sea transmitida por la estación o un AP. Para ello es necesario el control sobre el firmware y el controlador de la tarjeta inalámbrica que puede desinfectar ciertos campos de una trama. Por lo tanto, el atacante selecciona su equipo de cuidado. Actualmente, hay tarjetas inalámbricas off-the-shelf que se pueden manipular. Además, la construcción de las tarjetas inalámbricas de propósito especial está al alcance de un atacante con recursos.

- **Red Inalámbrica de prueba**

Casi a menudo el atacante reúne una considerable cantidad de información sobre una red inalámbrica a través del sniffing, sin revelar su presencia inalámbrica en todo, hay piezas que todavía pueden faltar. El atacante envía paquetes construidos artificialmente a un objetivo que desencadenan respuestas útiles. Esta actividad se conoce como la exploración o sondeo activo.

El destino puede descubrir que está siendo investigado, que incluso podría ser un destino honey pot (www.honeynet.org) cuidadosamente construido para atrapar al atacante. El atacante tendría tratar de minimizar este riesgo.

- **Denegación de servicio**

Una denegación de servicio (DoS) se produce cuando el sistema no está proporcionando servicios a los clientes autorizados a causa de agotamiento de los recursos por parte de clientes no autorizados. En las redes inalámbricas, los ataques de denegación de servicio son difíciles de prevenir, difícil de parar un ataque en curso y de la víctima y sus clientes no podrán incluso detectar los ataques. La duración de tales DPM puede variar desde milisegundos a horas. Un ataque DoS contra una estación individual permite el secuestro de sesión.

- **Inundaciones con Asociaciones**

La AP inserta los datos suministrados por la estación en la Solicitud de la Asociación en una tabla, llamada tabla de asociación que la AP mantiene en su memoria. El IEEE 802.11 especifica un valor máximo de 2.007 asociaciones concurrentes a un AP. El tamaño real de este cuadro varía entre los diferentes modelos de puntos de acceso. Cuando esta tabla se desborda, la AP se negaría más clientes.

Habiendo agrietada WEP, un atacante autentica varias estaciones no existentes utilizando direcciones MAC de aspecto legítimos pero generados

aleatoriamente. El atacante envía una avalancha de peticiones asociadas falsificadas para que la tabla de asociación se desborde.

- **Disociación forjado**

El atacante envía una trama de disociación falsa donde la dirección MAC de origen se ajusta a la de la AP. La estación aún está autenticada, pero sólo tiene que volver a asociar y envía solicitudes de Reasociación a la AP. La AP puede enviar una respuesta Reasociación aceptar a la estación y la estación puede entonces reanudar el envío de datos.

Para prevenir la Reasociación, el atacante continúa enviando tramas de disociación durante un período deseado.

- **Forjado Deauthentications**

El atacante monitorea todos los tramas de primas que recogen el origen y destino direcciones MAC para verificar que se encuentran entre las víctimas específicas.

Cuando se observa una trama de datos de respuesta o de la Asociación, el atacante envía una trama falsa Deauthentications donde la dirección MAC de origen no es la del AP. La estación se encuentra ahora no asociada y autenticada, y necesita volver a conectar. Para evitar una reconexión, el atacante continúa enviando tramas Deauthentications durante un período deseado. El atacante puede incluso limitar la velocidad del Deauthentications tramas para evitar la sobrecarga de una red ya congestionada.

Los paquetes traviesos de disociación y Deauthentications se envían directamente al cliente, por lo que estos no se registrarán por la AP o IDS, y ni el filtrado MAC ni protección WEP lo impedirán.

- **Los ataques man-in- the-Middle**

Man-in - the-middle (MITM) ataque se refiere a la situación en la que un atacante en acogida inserciones XX entre todas las comunicaciones entre hosts B y C, y ni B ni C es consciente de la presencia de X. Todos los mensajes enviados por B hacer alcance C, pero a través de X, y viceversa.

El atacante puede simplemente observar la comunicación o modificarlo antes de enviarlo. Un ataque MITM puede romper las conexiones que de otra manera segura. A nivel TCP, SSH y VPN, por ejemplo, son propensos a este ataque.

- **Wireless MITM**

Supongamos que la estación B se autenticó con C, un punto de acceso legítimo. El atacante X es un portátil con dos tarjetas inalámbricas.

A través de una carta, que presentará X como un AP. El atacante X envía una trama Deauthentications a B usando la dirección MAC de C como la fuente y el BSSID que ha recogido.

B es desautenticado y comienza una búsqueda de un punto de acceso y puede encontrar a X en un canal diferente de C.

Existe una condición de carrera entre X y C. Si B está asociado con X, el ataque MITM tuvo éxito. X volverá a transmitir las tramas que recibe desde B a C, y las tramas que recibe desde C a B después de modificaciones adecuadas.

El paquete de herramientas llamado AirJack incluye un programa llamado monkey_jack que automatiza el ataque MITM. Esto está programado así por lo que se mejoran las probabilidades de que la victoria en la condición de carrera se ha mencionado anteriormente.

- **ARP Poisoning**

El envenenamiento de la caché ARP es un antiguo problema en las redes de cable. Las redes de cable han implementado técnicas de mitigación. Pero, la técnica de envenenamiento ARP es volver a habilitar la presencia de puntos de acceso que están conectados a un switch/hub junto con otros clientes cableados.

ARP se utiliza para determinar la dirección MAC de un dispositivo cuya dirección IP se conoce. La traducción se realiza con una tabla de consulta. La caché de ARP se acumula como el anfitrión continúa a la red. Si la caché ARP no tiene una entrada para una dirección IP, el paquete IP saliente está

en cola y un paquete de solicitud de ARP solicita " Si su dirección IP coincide con la dirección IP de destino, por favor hágamelo saber cuál es su dirección Ethernet y se emite".

Se espera que el host con el IP de destino responda con una respuesta ARP, que contiene la dirección MAC de la máquina. Una vez que se actualiza la tabla debido a la recepción de esta respuesta, todos los paquetes IP en cola se pueden enviar. Las entradas de la tabla expiran después de un tiempo determinado con el fin de dar cuenta de los posibles cambios de dirección de hardware para la misma dirección IP.

Este cambio puede haber sucedido, por ejemplo, debido a la NIC siendo reemplazado.

Por desgracia, el ARP no prevé ningún tipo de verificación de respuestas de hosts válidos o que está recibiendo una respuesta como si ha enviado una solicitud de ARP. El envenenamiento ARP es una técnica de ataque explotando la falta de verificación. Corrompe la caché ARP que el sistema operativo mantiene con direcciones MAC equivocadas para algunas direcciones IP.

Un atacante logra esto mediante el envío de un paquete de respuesta ARP que se construye deliberadamente con una mala dirección MAC.

La ARP es un protocolo sin estado. Por lo tanto, una máquina de recibir una respuesta ARP no puede determinar si la respuesta es debido a una solicitud que envió o no.

El envenenamiento ARP es una de las técnicas que permiten el ataque man-in- the-middle.

Un atacante en la máquina X se interpone entre dos hosts B y C por la intoxicación a B de manera que la dirección IP de C se asocia con la dirección MAC de X, la intoxicación la efectúa asimilando ser C de manera que la dirección de B se asocia con la dirección MAC de X, y la retransmisión de los paquetes X son recibidos.

El ataque de envenenamiento ARP es aplicable a todos los hosts de una subred. La mayoría de los puntos de acceso actúan como puentes

transparentes de capa MAC, y así todas las estaciones asociadas a ella son vulnerables.

Si un punto de acceso se conecta directamente a un concentrador o un detector sin intervenir Router/firewall, entonces todos los hosts conectados al hub o switch son susceptibles también.

Tenga en cuenta que los últimos dispositivos dirigidos al mercado de consumo en casa se combinan con un conmutador de red que puede ser de cuatro o cinco puertos, un punto de acceso, un Router y un módem DSL/cable de conexión a la Internet en general.

Internamente, el AP está conectado al conmutador. Como resultado, un atacante en una estación inalámbrica puede convertirse en un MITM entre dos anfitriones cableados, un cable inalámbrico, uno o ambos hosts inalámbricos.

La herramienta llamada Ettercap es capaz de realizar el envenenamiento ARP.

- **El secuestro de sesiones**

Secuestro de sesión se produce en el contexto de un "usuario", ya sea humano o una computadora. El usuario tiene una conexión en curso con un servidor. Secuestro se dice que ocurre cuando un atacante hace que el usuario pierda la conexión, y el atacante asume su identidad y privilegios por un período.

Un atacante deshabilita temporalmente el sistema del usuario, por ejemplo por un ataque DoS[35] o explotar un desbordamiento de búfer. El atacante toma la identidad del usuario. El atacante ahora tiene todo el acceso que el usuario tiene. Cuando se hace esto, se detiene el ataque DOS, y deja la hoja de vida del usuario. El usuario no detecta la interrupción si la interrupción dura más de un par de segundos. Dicho secuestro se puede lograr mediante el uso de forjado ataque DoS disociación.

[35] DoS: Denied of Service

En redes inalámbricas corporativas se establecen que los usuarios se dirijan a un servidor de autenticación cuando su estación intenta una conexión con un punto de acceso. Después de la autenticación, el atacante utiliza el secuestro de sesión utilizando direcciones MAC falsificados (Sons, Hacking Techniques in Wireless Networks, 2005).

2.4. Método Pasivo o no Intrusivo

El enfoque de monitoreo pasivo se basa en la obtención de datos a partir de la recolección y análisis del tráfico que circula por la red. Se emplean dispositivos como sniffers, routers. Este enfoque no agrega tráfico en la red como se lo realiza con el método activo. Es muy utilizado para caracterizar el tráfico de la red y contabilizar su uso (Sons, Hacking Techniques in Wireless Networks, 2005).

2.4.1. Técnicas de Monitoreo Pasivo

Basado en solicitudes remotas

- **Mediante SNMP**

Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para esto se debe tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados traps que indican que un evento fuera de lo normal se ha producido (Medellin).

- **Captura de tráfico**

Se puede llevar acabo de dos formas, la primera mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura. La segunda mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede

ser una computadora con el SW de captura o un dispositivo extra. Análisis de tráfico: se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se pude implementar haciendo uso de dispositivos intermedios con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, entre otros (Medellin).

- **Flujos**

Utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con: La misma IP origen y destino El mismo puerto TCP origen y destino El mismo tipo de aplicación Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos (Medellin).

- **Sniffing**

Es una técnica que se enfoca en la captura de paquetes de datos que pasan a través de una interfaz de red y es utilizada para:

  - Análisis de vulnerabilidades y Seguridades de red.
  - Troubleshooting
  - Evitar cuellos de botella producidos por paquetes de datos erróneos en la red haciéndola más eficiente.

Su aplicación es los packets sniffers como Wireshark, tcpdump, windump, etc.

Generalmente el Packet sniffer captura los paquetes que llegan a la interfaz de monitoreo de la máquina en la cual se lo instala, sin embargo si se configura la interfaz en modo promiscuo se puede capturar el tráfico generado en toda la red.

Sniffing es escuchar a escondidas la red. Un sniffer es un programa que intercepta y decodifica tráfico de red difundido a través de un medio. Sniffing es el acto por una máquina S de hacer copias de un paquete de red enviados por la máquina A destinada a la recepción de la máquina B. Estrictamente hablando, no es un problema de TCP/IP, pero está habilitado

por la elección de emisión medios de comunicación, Ethernet y 802.11, como las capas de enlace de datos y física (Sons, Hacking Techniques in Wireless Networks, 2005).

Sniffing ha sido durante mucho tiempo una técnica de reconocimiento utilizados en las redes de cable. Sniffing es la técnica subyacente utilizada en herramientas que monitorean el rendimiento de una red. También puede ayudar a encontrar equipos de conectividad vulnerable, exploración de los puntos de acceso abierto o capturar las contraseñas utilizadas en una sesión de conexión que ni siquiera utilizan WEP, o en telnet, conexiones rlogin y ftp (Sons, Hacking Techniques in Wireless Networks, 2005).

Es fácil de interceptar el tráfico inalámbrico de un edificio mediante el establecimiento de contienda en un automóvil estacionado en un lote tan lejos como una milla, o mientras se conduce alrededor de la cuadra.

En una red cableada, el atacante debe encontrar una manera de instalar un sniffer en uno o más de los hosts de la subred de destino. Dependiendo del equipo utilizado en una LAN, un sniffer necesita ser ejecutado en la máquina víctima cuyo tráfico es de interés o en algún otro host en la misma subred que la víctima. Un atacante en general en Internet tiene otras técnicas que hacen que sea posible la instalación de un analizador de forma remota en el equipo de la víctima.

- **Escaneo Pasivo**

Escanear es el acto de Sniffing sintonizando a varios canales de radio de los dispositivos. Un escáner de red pasiva instruye la tarjeta inalámbrica para escuchar a cada canal durante unos mensajes. Esto no revela la presencia del escáner.

Un atacante puede analizar de forma pasiva sin transmitir nada. Las estaciones permiten varios modos de operación. Hay un modo llamado modo de monitor de radiofrecuencia que se permite a cada fotograma que aparece en un canal que se desea copiar como el radio de la estación sintoniza a los distintos canales. Esto es análogo a la colocación de una tarjeta de Ethernet por cable en modo promiscuo. Este modo no está

activado por defecto. Uno puede comprar tarjetas inalámbricas cuyo firmware y software del controlador correspondiente permite la lectura de todas las tramas 802.11. Una estación en modo monitor puede capturar los paquetes sin asociarse con una red de AP o ad - hoc (Sons, Hacking Techniques in Wireless Networks, 2005).

El modo promiscuo permite la captura de todos los paquetes inalámbricos de una red asociada. En este modo, los paquetes no se pueden leer hasta que se completen la autenticación y asociación. Un ejemplo sniffer es Kismet. Una tarjeta inalámbrica ejemplo que permite los modos de monitor de radiofrecuencia es Cisco Aironet AIR - PCM342.

- **Detección de SSID**

El atacante puede descubrir el SSID de una red por lo general en los escaneos pasivos porque el SSID se produce en los siguientes tipos de tramas: Beacon, Probe Requests, Probe Responses, Association Requests, y Reassociation Requests. Recordemos que las tramas de gestión están siempre transparentes, incluso cuando WEP está habilitada.

En un número de puntos de acceso, es posible configurar de forma que el SSID transmitido en las tramas Beacon sean enmascaradas, o incluso apagar por completo las tramas Beacons. El SSID mostrado en las tramas Beacon se establece en nulo, con la esperanza de hacer de la WLAN invisible a menos que el cliente ya conozca el SSID correcto. En tal caso, una estación que deseen unirse a una WLAN comienza el proceso de asociación mediante el envío de Probe Requests, a pesar que no pueda detectarse ningún APs a través de Beacons asociados con su SSID.

Cuando el Beacon muestra un SSID nulo, hay dos posibilidades. Eventualmente, un Associate Request puede aparecer desde una estación legítima que ya tiene un SSID correcto. Para dicha solicitud, habrá una trama Associate Response enviada por el AP. Ambas tramas contendrán el SSID, y el atacante husmea estas. Si el emisor desea unirse a cualquier AP disponible, envía Probe Requests en todos los canales, y escucha los Probe Responses que contienen los SSID de los puntos de acceso. La estación

considera a todas las tramas Probe Responses, tal como las tramas Beacon SSID no nulos, para seleccionar un AP. Asociación normal comienza. El atacante espera para olfatear estas respuestas muestra y extraer los SSID.

Si la transmisión Beacon esta desactivada, el atacante tiene dos opciones. El atacante puede seguir husmeando en espera que aparezca una trama Associate Request desde una estación legítima que ya tiene un SSID correcto. El atacante también puede elegir activamente probar mediante la inyección de las tramas que el construye y de esa manera husmear la respuesta (Sons, Hacking Techniques in Wireless Networks, 2005).

- **Recolectar las direcciones MAC**

El atacante recopila direcciones MAC legítimas para su posterior uso en la construcción de tramas falsificadas. La fuente y las direcciones MAC de destino son siempre transparentes en todas las tramas. Hay dos razones por las que un atacante podría recolectar direcciones MAC de las estaciones y puntos de acceso participantes de una red inalámbrica.

- El atacante desea usar estos valores en tramas falsificadas de manera que su estación o AP no sea identificada.
  - El AP dirigido puede estar controlando el acceso al filtrar tramas con direcciones MAC que no fueron registradas.

- **Recolección de la tramas para Cracking WEP**

El objetivo de un atacante es descubrir la clave secreta compartida WEP.

A menudo, la clave compartida puede ser descubierta por las conjeturas basadas en un cierto criterio de ingeniería socialmente referida al administrador de la red que configura la LAN inalámbrica y todos sus usuarios. Algunos programas cliente almacenan las claves WEP en los scripts de Registro o de inicialización del sistema que operan.

El atacante emplea procedimientos sistemáticos en descifrar el WEP. Para este propósito, un gran número (millones) de tramas necesarias son coleccionadas en base al funcionamiento WEP.

Algunas tarjetas son tan simplistas que comienzan su trama como 0 y se incrementará en 1, el restablecimiento en el medio de algunos eventos. Incluso las mejores tarjetas generan tramas débiles de la que los primeros bytes de la clave compartida se pueden calcular después de los análisis estadísticos. Algunas implementaciones generan menos vectores matemáticamente débiles que otros.

El atacante husmea un gran número de tramas de un solo BSS. Estas tramas utilizan todas las mismas claves. Lo que se necesita, sin embargo es una colección de tramas que fueron cifradas matemáticamente débiles. El número de tramas que eran matemáticamente cifradas débiles es un pequeño porcentaje de todas. En una colección de un millón de tramas, sólo puede haber un centenar matemáticamente débiles. Es concebible que la colección puede tardar unas pocas horas hasta varios días, dependiendo de lo ocupado que la WLAN sea.

Dado un número suficiente de tramas matemáticamente débiles, el cálculo sistemático que expone los bytes de la clave secreta es intensivo. Sin embargo, un atacante puede emplear potentes ordenadores. En una PC promedio, esto puede tardar unos segundos en horas. El almacenamiento de la gran cantidad de tramas está en los varios cientos de gigabytes a unos pocos megabytes.

Un ejemplo de una herramienta de craqueo WEP es AirSnort (http://airsnort.shmoo.com). (Sons, Hacking Techniques in Wireless Networks, 2005)

- **Detección de SSID**

La detección de SSID es a menudo posible simplemente monitoreando tramas Beacon.

Si la transmisión de Beacon está desactivada, y el atacante no quiere esperar pacientemente porque un Associate Request aparezca desde una estación legítima que ya tiene un SSID correcto, o Probe Requests de las estaciones legítimas, él recurre a sondear mediante la inyección de tramas Probe Request que contengan una dirección MAC de origen simulada. La

trama Probe Response desde los puntos de acceso contendrá, en sí, el SSID y otra información similar a la de las tramas Beacon que fueron permitidas. El atacante husmea estas respuestas muestra y extrae los SSID.

Algunos modelos de puntos de acceso tienen una opción para desactivar la respuesta a peticiones de sondeo que no contienen el SSID correcto. En este caso, el atacante determina una estación asociada con el AP, y envía la estación de un marco de disociación forjado donde la dirección de MAC de origen se ajusta a la de la AP.

La estación enviará una solicitud Reassociation Request que expone el SSID.

- **Detección de puntos de acceso y estaciones**

Ciertos bits en las tramas se identifican si es de un AP. Si asumimos que WEP o está desactivado, o se rompe, el atacante también puede recopilar las direcciones IP de la AP y las estaciones.

- **Detección de pruebas**

Las tramas que inyecta un atacante también pueden ser escuchadas por los sistemas de detección de intrusos (IDS) de LAN inalámbrica endurecido. Hay equipos con GPS que puede identificar las coordenadas físicas de un dispositivo inalámbrico a través del cual las tramas Probe están siendo transmitidas.

- **Debilidades AP**

APs tienen debilidades que son debido a errores de diseño e interfaces de usuario que promueven contraseñas débiles, etc.

Se ha demostrado públicamente por muchos esfuerzos realizados por war-driving (www.worldwidewardrive.org) que en las principales ciudades de todo el mundo una gran mayoría de los puntos de acceso desplegados están mal configurados, la mayoría con WEP deshabilitados, y por defecto de configuración, como la configuración del fabricante, sin tocar.

- **Configuración**

Las claves WEP por defecto utilizado son a menudo demasiado triviales. Diferentes puntos de acceso utilizan diferentes técnicas para convertir la entrada del teclado del usuario en un vector de bits. Por lo general 5 a 13 caracteres imprimibles ASCII se asignan directamente concatenando sus códigos de 8 bits ASCII en una clave de 40 bits o 104 bits WEP. Una clave más fuerte puede ser construida a partir de una entrada de 26 dígitos hexadecimales. Es posible formar una clave bit WEP incluso stronger104 truncando el hash MD5 de una frase de paso de longitud arbitraria.

- **La anulación del filtro MAC**

APs típicos permiten el acceso sólo a aquellas estaciones con direcciones MAC conocidas. Esto es fácilmente anulado por el atacante que falsifica sus tramas con una dirección MAC que se ha registrado en el AP de entre los que había recaudado a través del husmeo. Que una dirección MAC se ha registrado puede detectarse mediante la observación de los tramas de la AP a las estaciones.

- **Rogue AP**

Los puntos de acceso que se instalan sin la debida autorización y la verificación de la política general de seguridad se llaman puntos de acceso maliciosos. Estos están instalados y utilizados por los usuarios válidos. Estos puntos de acceso se configuran mal, y fácil para los atacantes encontrarlos.

- **Trojan AP**

Un atacante establece un punto de acceso para que la estación dirigida reciba una señal más fuerte de lo que lo que recibe de un AP legítimo. Si WEP está habilitada, el atacante ya se habría agrietado. Un usuario legítimo selecciona el troyano AP debido a las fuertes señales, se autentica y asocia. El AP troyano está conectado a un sistema que recoge el tráfico IP para los análisis posteriores. A continuación, transmite todas las tramas a un AP legítimo para que el usuario víctima no reconozca el ataque MITM en curso.

El atacante puede robar la contraseña de los usuarios, acceso a la red, comprometer el sistema del usuario para darse a sí mismo el acceso root. Este ataque se llama Ataque Evil.

Es fácil de construir un troyano AP debido a un punto de acceso es un sistema informático optimizado para su aplicación prevista. Un PC de propósito general con una tarjeta inalámbrica se puede convertir en un punto de acceso capaz. Un ejemplo de este tipo de software es HostAP.

- **Interferencia de ondas aéreas,**

Un número de aparatos de consumo, tales como hornos microondas, monitores de bebés, y los teléfonos inalámbricos operan en el no regulado de 2,4 GHz de frecuencia de radio. Un atacante puede desencadenar grandes cantidades de ruido utilizando estos dispositivos y atascar las ondas de radio para que la señal de ruido caiga tan bajo, que la LAN inalámbrica deja de funcionar. La única solución a esto es poner a prueba el medio ambiente circundante de RF[36].

- **Ahorro de energía**

Conservación de la energía es importante para los ordenadores portátiles típicos de la estación, por lo que con frecuencia entran en un estado llamado 802,11 Doze.

Un atacante puede robar los paquetes destinados a una estación, mientras que la estación se encuentra en el estado Doze.

El protocolo 802.11 requiere una estación de informar a la AP a través de un intercambio de tramas éxito que desea entrar en el estado Doze desde el estado activo. Periódicamente la estación despierta y envía una trama PS-Poll a la AP. El AP transmite en respuesta a los paquetes que fueron amortiguadas por la estación mientras dormitaba. Este cuadro de sondeo puede ser suplantada por un atacante y causar la AP para enviar los paquetes reunido y lave sus buffers internos.

[36] RF: Radio Frecuencia

Un atacante puede repetir estos mensajes de votación de manera que cuando la estación legítima despierta y encuesta periódicamente, el AP le informará de que no hay paquetes pendientes.

- **War Driving**

Es utilizar herramientas y dispositivos inalámbricos conduciendo un vehículo o estacionado en lugares interesantes con el objetivo de descubrir y conseguir información de una red inalámbrica. War-drivers se define como " El acto benigno de la localización y el registro de los puntos de acceso inalámbrico en movimiento. " Este acto benigno es, por supuesto, útil para los atacantes.

- **Warchalking**

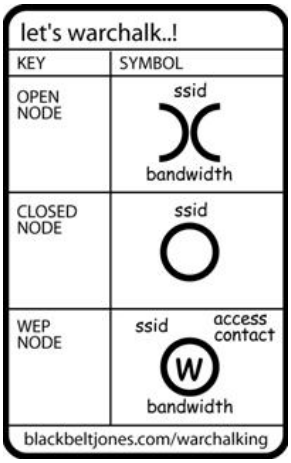


Figura 2-6 Warchalking.

WarChalking es la práctica de marcar aceras y paredes con símbolos especiales para indicar que el acceso inalámbrico está cerca, por lo que los demás no tienen que pasar por la molestia del mismo descubrimiento. Una búsqueda en www.google.com con las palabras clave " guerra mapas de conducción " producirá un gran número de éxitos. Yahoo! Maps puede mostrar " Hotspots Wi-Fi" cerca de la dirección que usted da.

- **Equipamiento Típico**

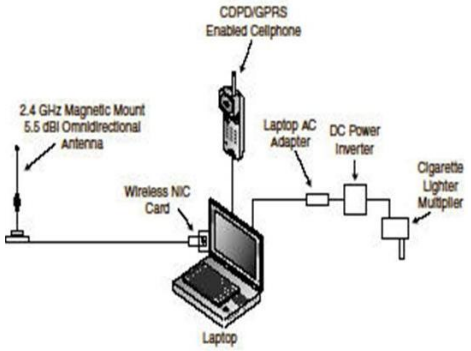


Figura 2-7 Equipamiento para Hackeo Inalámbrico.

El equipamiento típico consiste en un sistema de ordenador portátil o una PDA con una tarjeta inalámbrica, un GPS y una antena de alta ganancia. Elección típica de un sistema operativo es Linux o FreeBSD donde sniffers de código abierto (por ejemplo, Kismet) y Jaqueadores de claves WEP (por ejemplo, AirSnort) están disponibles. Herramientas similares (por ejemplo, NetStumbler) que se ejecutan en Windows están disponibles. Los wardrivers tienen que estar dentro del rango de un punto de acceso o estación ubicada en la red de destino. El rango depende de la potencia de salida de transmisión del AP y la tarjeta, y la ganancia de la antena.

Las antenas de punto de acceso ordinarias transmiten sus señales en todas direcciones. Con frecuencia, estas señales llegan más allá de los límites físicos del área de trabajo previsto, tal vez a los edificios adyacentes, pisos y aparcamientos.

Con las tarjetas de 30mW inalámbricos típicos destinados a los ordenadores portátiles, el rango es de aproximadamente 300 pies, pero en a partir del 2004 las tarjetas inalámbricas para ordenadores portátiles en el mercado tienen 200mW.

2.5. Métricas

La definición de métricas permitirá establecer patrones de comportamiento para los dispositivos que serán monitoreados. También hay diversos tipos de métricas que pueden ser declarados, dependerán de las necesidades que se presenten en la red que se desea analizar y de las características de la misma. Las métricas deben ser congruentes con los dispositivos a monitorear.

- Métricas de tráfico de entrada y salida.
- Métricas de utilización de procesador y memoria.
- Métrica de estado de las interfaces.
- Métrica de conexiones lógicas.

CAPITULO 3

3. HARDWARE Y SOFTWARE

3.1. Tarjetas AirPcap Nx Adapter

Figura 3-1 AirPcap Nx Adapter.

3.1.1. Características Generales (SCOS Software)

- Captura trafico 802.11n en canales de 20Mhz y 40Mhz.
- Captura de paquetes 802.11a/b/g/n canales de 20Mhz
- Inyección de paquetes 802.11a/b/g/n en varias velocidades.
- Información detallada de tramas de control, administración y datos en Wireshark, incluyendo la información de msdus, mspdus y ht.
- Información del radio por paquete
- Resolución de tiempos de retardo en microsegundos
- Dos antenas internas y 2 conectores MC-Card para antenas externas.
- Soporta para 2x2 MIMO
- Soporte para capturas simultaneas multicanal en un solo archivo unido mediante el uso de múltiples adaptadores AirPcap Nx y la tecnología de agregación de canales exclusivo de Cace.
- Completa integración con Wireshark y Cascade Pilot para el análisis, visualización, monitoreo y reporte de tráfico WLAN.

- Interfaz USB provista para potabilidad y flexibilidad en uso.

3.1.2. Funcionamiento y Uso

Los adaptadores AirPcap capturan el tráfico en un solo canal a la vez; el canal configurado por los adaptadores AirPcap puede ser cambiado usando el panel de control o desde el cuadro de diálogo “Advanced Wireless Settings” en Wireshark. Dependiendo de las capacidades de la tarjeta AirPcap, pueden ser configurados en cualquier canal IEEE802.11 a/b/g/n valido para captura de paquetes.

Todos los adaptadores AirPcap pueden operar en un modo completamente pasivo. Esto significa que pueden capturar tráfico en un canal sin asociarse con ningún Access Point o interactuar con algún otro dispositivo inalámbrico (Cace Technologies). A menos que se esté trasmitiendo, ningún adaptador AirPcap Tx o Ex o Nx es detectable por alguna otra estación.

Los adaptadores AirPcap pueden funcionar en un modo llamado monitor. Este modo el adaptador AirPcap captura todas las tramas que son transferidas en un canal y no solo tramas que sean direccionadas a este. Esto incluye tramas de datos, de control y de administración.

Cuando más de un BSS comparte el mismo canal, el adaptador AirPcap capturará las tramas de datos, control y administración desde todos los BSS que estén compartiendo el canal y que están dentro del rango del adaptador AirPcap (Cace Technologies).

Para poder configurar se dispone de una interfaz de control AirPcap Control Panel que proporciona una forma conveniente intuitiva de configurar parámetros de los adaptadores AirPcap que se encuentran conectados.

Figura 3-2 Panel de control AirPcap

Las funciones del panel son las detalladas a continuación:

- La lista desplegable en el cuadro de interfaces en la parte superior del panel muestra una lista de los adaptadores que se encuentran conectados. Seleccionando uno de los adaptadores en la lista permitirá visualizar o editar su configuración. El modo de identificar los adaptadores AirPcap mediante la lista desplegable es utilizando números como 00, 01, etc.
- Se dispone de un botón Blink LED que permitirá el parpadeo de los led acoplados en las tarjetas según la selección efectuada en la lista desplegable de adaptadores y tienen la finalidad de distinguir entre varias tarjetas conectadas el número asociado en el panel de control.
- Channel: muestra los canales disponibles del adaptador seleccionado en la lista desplegable donde cada canal disponible está dado por su frecuencia central y se considera el ancho de banda de cada canal en 20 MHz.

- Extension Channel: en adaptadores 802.11n, se puede usar la lista de canal de extensión para crear un canal amplio. Las elecciones posibles son -1 para la banda de frecuencia precedente de 20 MHz, 0 que indica no extensión y +1 para la banda de frecuencia subsiguiente de 20 MHz. El canal de la banda de frecuencia adicional es llamado canal extendido. No todos los canales tienen extensión, por ejemplo los canales b g 1, 2, 3 y 4 no tienen extensión precedente. La razón es que el centro de frecuencias del canal primario y extendido necesitan ser separados por 20MHz.
- Capture Type: solo trama 802.11, trama 802.11+ información de radio o trama 802.11+ cabecera per Packet Information (PPI). PPI y radio incluyen información adicional no contenida en la trama 802.11: velocidad de transmisión, potencia de señal, calidad de señal, canal e información múltiple de la antena (para PPI). Estos formatos se detallarán posteriormente.
- Include 802.11 FCS in Frames: si tiene un visto, la trama capturada incluirá los 4 bytes correspondientes a revisión de frecuencia de la trama 802.11.

Aplicaciones de las tarjetas AirPcap:

- **Captura de Canales Múltiples:** múltiples adaptadores AirPcap pueden ser usado al mismo tiempo para capturar tráfico simultáneamente de diferentes canales. El controlador AirPcap provee soporte para este tipo de operación mediante la tecnología de agregación multicanal (Multichannel Aggregator), la cual exporta flujos de capturas desde múltiples adaptadores AirPcap como un solo flujo de captura. El agregador multicanal consiste de una interfaz virtual que puede ser usada desde Wireshark u otra aplicación basada para AirPcap. Usando esta interfaz, la aplicación receptara el tráfico desde todos los adaptadores instalados, como si estuviese viniendo desde un solo dispositivo. El agregador multicanal puede

ser configurado como cualquier dispositivo AirPcap real, y sin embargo puede tener su propia des encriptación, revisión de fcs y herramientas de filtrado de paquetes.

- **Configuración como generador de tráfico:** Para usuarios avanzados, AirPcap Tx y AirPcap Ex tienen la capacidad de inyectar tramas 802,11 en su red inalámbrica que les ayuda en la evaluación de la seguridad de su red inalámbrica. El uso de la API AirPcap, AirPcap Tx, Ex y Nx puede inyectar cualquier tipo de trama, incluyendo las tramas de control, gestión y datos. Estas tramas se pueden transmitir en todo caso admisible dependiendo de su adaptador. La aplicación, llamada AirPcapReplay, se incluye en la distribución de software AirPcap. Una vez AirPcap se ha instalado, la aplicación se puede acceder desde el menú Inicio: Inicio → Programas → → AirPcap AirPcapReplay El propósito de esta solicitud, como su nombre indica, consiste en reproducir tráfico de red 802.11. Además de la función de repetición, AirPcapReplay también permite al usuario editar paquetes individuales utilizando un editor hexadecimal integrado. Además de AirPcapReplay, hay varias herramientas de software libre y de código abierto que son compatibles con AirPcap Tx, AirPcap Ex y AirPcap Nx. Aircrack-ng. Este es un conjunto bien conocido de herramientas para redes inalámbricas de auditoría. Esta es una herramienta de seguridad de multifunción para Windows que incluye la detección de punto de acceso inalámbrico y de acogida.

- **Configuración en modo de captura de tráfico:** El adaptador AirPcap captura el tráfico en un solo canal a la vez, el ajuste de canal para el adaptador AirPcap se puede cambiar mediante el panel de control AirPcap, o desde el cuadro de diálogo " Configuración inalámbrica avanzada " en Wireshark. Dependiendo de las capacidades del adaptador AirPcap, se puede ajustar a cualquier

canal 802.11a/b/g/n válida para la captura de paquetes. Todos los adaptadores de AirPcap puede operar en un modo completamente pasivo.

Detalle de funcionamiento de Capture Type:

- **Radiotap**

  Radiotap es un estándar creado para inyección y recepción de tramas 802.11. Dispone de un formato de cabecera que es un mecanismo que proporciona información adicional de las tramas (Berg, 2011).

  Radiotap proporciona información adicional que se añade a cada trama 802.11 al capturarlas mediante una aplicación de análisis. No se trata de parte del formato de trama del estándar 802.11 pero son información adicional añadido en el momento de la captura para proporcionar datos complementarios sobre las tramas capturadas (Nigel, 2013).

  Se compone de la siguiente información para la cabecera:
  Versión: indica cual es la mayor versión de la cabecera radiotap en uso. Esta tiene el valor de 0.
  Pad: no se utiliza.
  Len: indica el tamaño completo de los datos radiotap incluyendo la cabecera radiotap.
  Present: es una máscara de bits de los campos de datos radiotap que sigue el encabezado radiotap.

- **Per Packet Information**

  El encabezado de paquete de información (PPI) es un formato de cabecera de información general y extensible originalmente desarrollado para proporcionar información de radio 802.11n, pero puede manejar otra información.

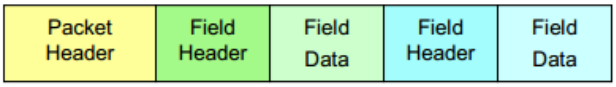


Figura 3-3 Cabecera PPI

Las cabeceras PPI pueden contener sólo un encabezado de paquetes sin los elementos de datos de cabecera de campo o en el campo. También hace que sea posible para guardar los paquetes con múltiples tipos de enlace de datos en un único archivo de captura (CACE Technologies, 2009).

La estructura de la cabecera PPI se conforma de los siguientes campos:

Versión: muestra la versión del encabezado PPI. Debe mantenerse en 0.

Flags: una máscara de 8 bits que define el comportamiento de la cabecera

Len: el tamaño de la cabecera completa PPI incluyendo sus campos. Debe ser entre 8y 65532.

Dlt: debe contener un tipo valido de dato definido en pcap-bpf.h de la distribución libpcap. (Cace Technologies)

3.2. Wireshark

Los analizadores de protocolos de red ("sniffers"), visualizan el tráfico de paquetes que circulan por las redes de computadores, permitiendo analizar el comportamiento de las mismas, detectando errores, congestión, etc.

Su funcionamiento consiste en capturar una copia de estos paquetes para realizar un análisis posterior, el cual se presenta textual o gráficamente, dependiendo de las capacidades de la herramienta en cuestión.

Normalmente realizamos varios tipos de análisis siendo los fundamentales el estructural y el estadístico. Con el análisis estructural observamos la composición y detalles de los paquetes capturados como contenido de cabeceras, nombre, protocolo, datos del cuerpo del mensaje, etc. Con el análisis estadístico obtenemos estimados de tráfico: cantidad de paquete por tipo y tiempo. Por ejemplo, un administrador de red puede estudiar qué partes de la red están más saturadas y cuáles protocolos y máquinas están generando más tráfico, y de ese modo podrá sugerir las acciones correctivas necesarias. (Gallegos León & Ruiz Delgado, 2011)

Adicionalmente, muchos analizadores son capaces de seguir una "conversación" con lo que facilitan la resolución de problemas y la depuración del software de red durante su desarrollo.

El analizador Wireshark, es uno de los más populares analizadores que existen. Se trata de es una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. Hasta el año 2006 el programa se distribuía bajo la denominación de Ethereal (Gallegos León & Ruiz Delgado, 2011).

3.2.1. Características

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red. Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.

- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

3.2.2. Funcionamiento

Al arrancar Wireshark, es necesario seleccionar la tarjeta de red de nuestra máquina sobre la que deseamos hacer capturas Esta será eth0 normalmente, así que seleccionaremos "Capture" sobre esta interfaz de red.

La captura de paquetes comenzará y se mostrará una ventana en la que poco a poco irán apareciendo diferentes estadísticas sobre los paquetes que progresivamente se van capturando hasta que se pulse "detener". Seguramente registraremos tráfico de tipo difusión (broadcast) y poco a poco veremos que se registra alguna actividad. Para crear tráfico de red, es conveniente hacer alguna acción como arrancar un navegador (Firefox o Mozilla en Linux), o dar un comando al sistema operativo que genere actividad (ping www.uah.es), conectarse a otra máquina o todas estas acciones simultáneamente (Gallegos León & Ruiz Delgado, 2011).

3.2.3. Interface Gráfica de Usuario

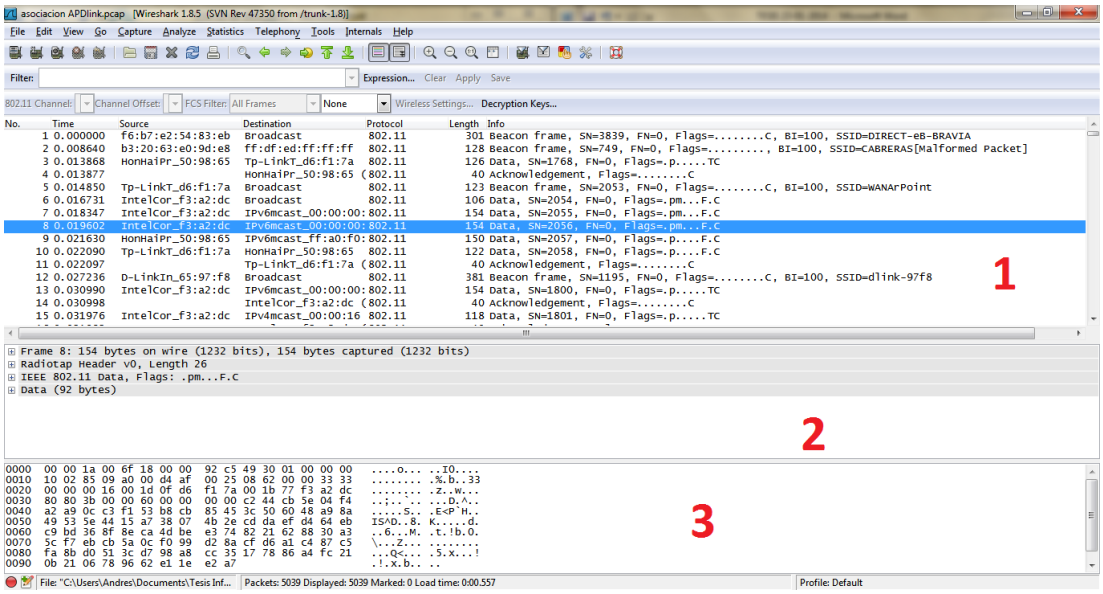


Figura 3-4 Interfaz Gráfica Wireshark.

- **Pantalla principal:** Una vez tengamos algunos paquetes capturados, observemos qué sucede al detener el proceso de captura, Los paquetes capturados se muestran en la ventana principal de Wireshark, esta se compone a su vez de tres ventanas.

1. La ventana superior es la lista de los paquetes capturados. Incluye hora, fuente, destino, protocolo y una descripción breve de cada uno. Según el paquete que esté seleccionado en cada momento, se controla la información que aparece la ventana intermedia

2. La ventana intermedia muestra en detalle el paquete seleccionado en la primera ventana. Incluye el nombre de los protocolos empleados en los distintos niveles de la arquitectura y los valores correspondientes a los campos de cada uno de los protocolos en listas desplegables.

3. La ventana inferior muestra el valor los datos del paquete en hexadecimal y ASCII. Al seleccionar alguno de los campos en la ventana intermedia, se destaca el rango de valores correspondientes a dicho campo en el paquete.

Además en la ventana principal de Wireshark tenemos:

- **Barra Principal:** con acceso a opciones de captura, archivado e impresión, movimiento y búsqueda de paquetes en la lista, zoom, aspecto de visualización, filtrado y edición de preferencias. En esta barra se encuentra "iconizadas" muchas de las opciones de los menús de la parte superior de la GUI de la aplicación.
- **Barra de Filtro:** muestra y permite especificar en el filtro aplicado a los paquetes para visualización aunque también navega a la ventana de definición de filtros de captura y visualización.
- **Barra de status:** Al pié de las ventanas a la izquierda vemos el nombre del fichero temporal donde se ha guardado la captura. A la derecha hay información sobre los paquetes:
    - P: número de paquetes capturados
    - D: número de paquetes que se muestran (superan el filtro)

- M: número de paquetes marcados

- **Opciones:** Controlamos la captura con los primeros iconos de la barra principal. También hallamos estas opciones en el menú Capture. Podemos establecer opciones de captura, iniciar una nueva captura, parar o reiniciar una captura en marcha. Las opciones de captura nos llevan a una ventana en que podemos establecer parámetros de captura: la ventana de diálogo "Capture Options". Las más relevantes son:

Marco de captura:

1. Selección de Interfaz

2. Modo promiscuo: en este modo el programa capturará cualquier paquete que sea visible a la tarjeta de red.

3.- Buffer Size: con el fin de limitar el uso de recursos, podemos indicar la cantidad máxima de bytes que vamos a guardar de cada paquete capturado.

4.- Filtro de captura: podemos navegar a la definición de filtros de captura para desechar la captación de algunos mensajes.

Filtros de Captura en Wireshark:

Wireshark hace uso de libpcap para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (and/or) con la opción de ser negada por el operador not:

[not]Expresion [and/or [not] Expresion...]

La siguiente expresión define un filtro para la captura de paquetes desde/hacia los host con dirección IP 172.17.250.1 y 172.17.1.81:

ip.addr==172.17.250.1 and ip.addr==172.17.1.81

Al diálogo de filtros de captura podemos llegar desde la ventana de opciones de captura o desde el menú de Capturas para establecer un filtro de captación de mensajes. Esto evitará la captación de algunos mensajes: antes solo los excluimos de la presentación en pantalla mediante el filtrado de presentación.

Si recorremos cada uno de los filtros predefinidos, veremos la expresión que los implemente en "Filter String". Esta lista puede aumentarse definiendo nuestras propias expresiones y asignando un nombre para ellas. Una expresión debe evaluarse a "true", se define en minúsculas con una o más primitivas unidas con operadores lógicos. Una primitiva es un calificador seguido de un identificador.

Para el análisis de los paquetes capturados, Al seleccionar cualquiera de los paquetes capturados, se despliega el contenido del paquete en el resto de los paneles que son panel de detalles de paquetes y panel en bytes.

Expandiendo cualquiera parte del árbol presentado en el panel de detalle del paquete, se puede seleccionar un campo en particular cuyo contenido se muestra resaltado en negritas en el panel de bytes.

Existe una manera de visualizar los paquetes mientras esta activo el proceso de captura esto se logra, seleccionando la opción Update list packets in real time desde menú Edit->Preferentes->Capture. Adicionalmente, Wireshark permite visualizar el contenido de un paquete seleccionado en el panel de paquetes capturados en una ventana individualmente seleccionando la opción Show Packets in new Windows en menú principal View. Esto permite comparar con más facilidad dos o más paquetes.

Cuando iniciamos la captura de paquetes por lo general se obtiene una gran cantidad de paquetes que cumple con los filtros y/o expresiones definidas, Wireshark permite realizar búsquedas sobre los paquetes capturados, seleccionando Menú Edit>Find Packets.

Wireshark permite marcar los paquetes para que sean identificados con más facilidad, a partir del menú contextual que se muestra al activar el botón derecho del ratón sobre el paquete en cuestión.

Wireshark proporciona un rango amplio de estadísticas de red que son accedidas desde el menú Statistics que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo (Gallegos León & Ruiz Delgado, 2011).

3.2.4. Análisis de Tráfico

En ocasiones, incluso se ha podido llegar a perder la conectividad o bien ciertos equipos han podido desconectarse sin motivo aparente. En la mayoría de ocasiones, las causas de estos problemas tienen un origen no premeditado y se deben a una mala configuración de la red como puede ser tormentas broadcast, spanning-tree mal configurado, enlaces redundantes, etc.

Pero, en otras ocasiones, puede tratarse de ataques inducidos por terceros que pretenden dejar fuera de servicio un servidor web mediante un ataque DoS, husmear tráfico mediante un envenenamiento ARP o simplemente infectar los equipos con código malicioso para que formen parte de una red zombi o botnet.

En cualquier caso, conocer el origen del incidente es el primer paso para poder tomar las contramedidas necesarias y conseguir una correcta protección. En este punto, los analizadores de tráfico pueden resultar de gran utilidad para detectar, analizar y correlacionar tráfico identificando las amenazas de red para, posteriormente, limitar su impacto.

El primer paso para poder auditar la red será definir dónde analizar el tráfico. Teniendo un escenario de red ya planteado procedemos a verificar en donde colocar el Sniffer para capturar paquetes, este puede ser el paso en donde tomemos más tiempo ya que debemos saber qué es lo que necesitamos hacer, ya que existen casos como por ejemplo si queremos verificar la calidad de servicio de un enlace o la calidad de señal de un AP o la disponibilidad de la red, aspectos como éste nos harán conocer el lugar donde colocar Wireshark, una vez conocido el lugar procederemos a capturar el tráfico de red y posterior a obtener estos datos analizaremos con dichos paquetes el comportamiento de la red analizando las tramas y ocupando filtros para obtener información de importancia.

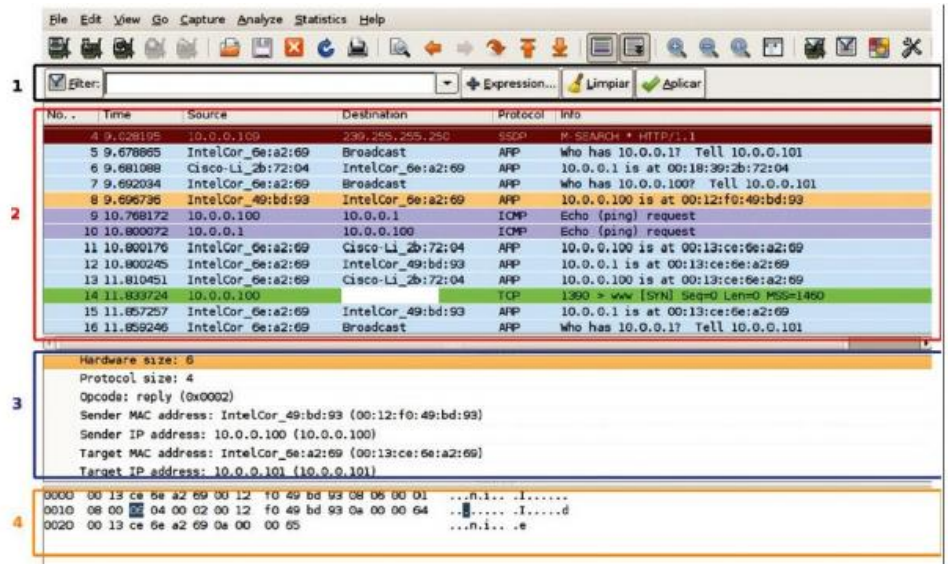


Figura 3-5 Zonas Wireshark.

A continuación, describimos brevemente las áreas más interesantes que nos muestra Wireshark según comienza la toma de datos (Figura 3-5- Zonas de Wireshark)

La zona 1: es el área de definición de filtros y, como veremos más adelante, permite definir patrones de búsqueda para visualizar aquellos paquetes o protocolos que nos interesen.

La zona 2: se corresponde con la lista de visualización de todos los paquetes que se están capturando en tiempo real. Saber interpretar correctamente los datos proporcionados en esta zona (tipo de protocolo, números de secuencia, flags, marcas de tiempo, puertos, etc.) nos va a permitir, en ciertas ocasiones, deducir el problema sin tener que realizar una auditoría minuciosa.

La zona 3: permite desglosar por capas cada una de las cabeceras de los paquetes seleccionados en la zona 2 y nos facilitará movernos por cada uno de los campos de las mismas.

La zona 4: representa, en formato hexadecimal, el paquete en bruto, es decir, tal y como fue capturado por nuestra tarjeta de red.

3.2.5. Filtros

Los filtros son, sin duda, la importancia de Wireshark. Cuando tenemos una captura de datos muy elevada, los filtros nos permiten mostrar únicamente aquellos paquetes que se acoplan con nuestro criterio de búsqueda. Podemos distinguir entre filtros de captura y filtros de visualización en función de la sintaxis con la que se rige cada uno de ellos.

Los filtros de captura se apoyan directamente sobre las librerías libpcap al igual que lo hace tcpdump o Snort, por lo que dependen directamente de las mismas para definir los filtros. Debido a este motivo, podemos utilizar Wireshark para abrir ficheros generados por tcpdump o por aquellas aplicaciones que hagan uso de los mismos. (Borja Meino, 2011).

Los filtros de visualización, en cambio, siguen una nomenclatura propia de la aplicación y se emplean para filtrar resultados sobre paquetes que previamente han sido capturados. Si aun así no estamos acostumbrados a este tipo de reglas, el botón Filters y Expression, situados a ambos lado del input de búsqueda, nos ayudará a buscar los paquetes deseados utilizando la sintaxis adecuada.

3.3. Cascade Pilot (SteelCentral Packet Analyzer)

3.3.1. Características.

- Manejo eficiente de gran volumen de información almacenada en ficheros .pcap de hasta varios gigabytes.
- Disponemos de una colección de vistas o métricas para la rápida identificación de un problema u obtención de diversos tipos de información sobre tráfico, protocolos, conversaciones, etc.
- Manejo de líneas de tiempo para capturas de mucha duración.
- Manejo en tiempo real de estadísticas en capturas de mucho volumen de forma muy rápida.

- Integración completa con Wireshark.
- Filtros y disectores.
- Diferentes tipos de gráficas.
- **Drill-Down** una característica de CACE para el análisis más profundo de capturas.
- Disparadores de activación de alertas según una determinada condición.

3.3.2. Interface y Herramientas de Cascade Pilot

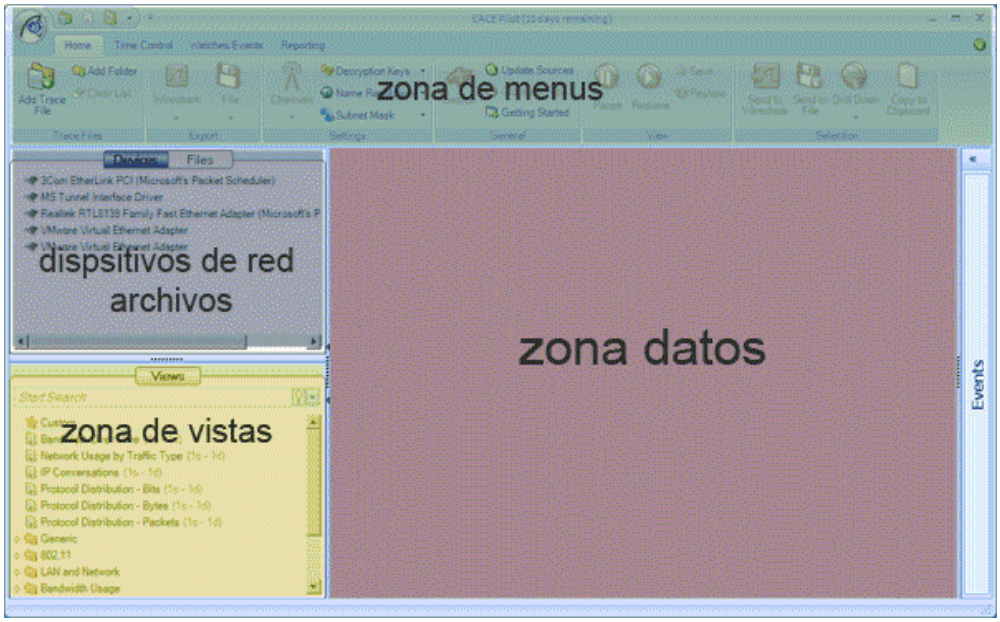


Figura 3-6 Zonas Cace Pilot.

- **En la zona de menús tenemos:** Gestión de archivos, filtros de exportación, manejo de tiempos. Gestión de eventos, creación de informes.
- **En la zona de dispositivos y archivos:** Es donde indicaremos la interface para captura en tiempo real, archivos de captura **.pcap** y aplicación de vistas.
- **Zona de datos:** La zona de datos en donde aparecerán los resultados en forma de gráficas de las distintas vistas aplicadas**,** filtros, etc. (Riverbed)

3.4. InSSIDer

Figura 3-7 Herramienta de monitoreo Inssider.

3.4.1. Funcionamiento

Se encuentra diseñado para que pueda escanear, visualizar y solucionar problemas de redes inalámbricas con mayor rapidez y facilidad, Dentro de entornos Windows o Mac se necesita una herramienta muy útil diseñada para mostrar exactamente lo que su entorno Wi -Fi se parece, tanto física como lógicamente.

Visualización en tiempo real de los canales de los Puntos de Acceso cercanos, permite filtrar gráficamente y verificar las superposiciones de la señal, permite verificar conflictos de canal y problemas de configuración que están degradando el rendimiento de su red inalámbrica como la intensidad de señal. (Metageek, 2014).

3.4.2. Características

- Grafica grupo de Redes de Radio o ESSID para el análisis rápido
- Visualizar - Canal y redes superpuestas
- Filtrar redes de SSID , la dirección MAC , el canal o intensidad de la señal
- Se puede ver redes de 2.4 y 5 GHz simultáneamente en una pantalla paralela.
- Ver gráficos en tiempo real de los canal con más fuerza y las radios que se solapan
- Visualice todas las redes inalámbricas que rodean a la vez y ordenar por Radio MAC, SSID, canal, intensidad de la señal, Tipo PHY, tipo de seguridad, y Min o Max Velocidad de datos.

3.4.3. Commview

3.4.4. Funcionamiento

Commview es un monitor y analizador de red de gran alcance diseñado para administradores de LAN, profesionales de seguridad, programadores de red, usuarios domésticos, prácticamente cualquier persona que quiere una imagen completa del tráfico que fluye a través de una PC o segmento de LAN. Cargado con muchas funciones fáciles de usar, Commview combina rendimiento y flexibilidad con una facilidad de uso sin igual en la industria.

Esta aplicación captura cada paquete en el cable para mostrar información importante, como una lista de paquetes y conexiones de red, estadísticas vitales, gráficos de distribución de protocolos, y así sucesivamente. Se puede examinar, guardar, filtrar, importar y exportar paquetes capturados, ver protocolos decodificados hasta la capa más baja con un completo análisis de más de 100 protocolos soportados. Con esta información, Commview puede ayudar a identificar problemas de red y solucionar problemas de software y hardware.

Commview incluye un analizador de VoIP para el análisis en profundidad, la grabación y la reproducción de las comunicaciones de voz SIP y H.323.

Commview corre sobre Windows XP, Vista, 7, 8 o Windows Server 2003, 2008 2012 (x32 o x64 bits), Se requiere de una interface Ethernet 10/100/1000 Mbps, o una Ethernet Inalámbrica o una tarjeta Token Ring o inclusive un adaptador de acceso telefónico estándar.

Con Commview podemos ver detalles estadísticos de conexiones IP, Direcciones IP, puertos, sesiones, etc. Generar reportes de tráfico en tiempo real, ver distribución de protocolos, uso de Ancho de Banda, nodos de red gráficos y en tablas. (TamoSoft, 1998)

3.5. D-ITG

De sus siglas en inglés “Distributed Internet Traffic Generator”, se trata de una Plataforma de código abierto con capacidad de producir tráfico a nivel de paquetes con mucha precisión (IPv4 e IPv6). Se puede replicar procesos estocásticos para IDT (“Inter Departure Time”) y para las variables PS (“Packet Size”) aleatorias (Pareto, uniforme, exponencial, etc.), es una herramienta para la generación de tráfico la cual permite evaluar activamente las características de desempeño de una red a través de un analizador de resultados.

Fue desarrollada por Stefano Avallone y Antonio Pescapé del Departamento de Sistemas e Informática de la Universidad Federico II de Napoli en Italia. El proyecto está actualmente vigente.

3.5.1. Características.

Una de las capacidades más interesantes de esta aplicación es que permite generar archivos tipo “script” en donde se indican los parámetros de la generación de tráfico que se quiere efectuar, pudiendo emular tráfico de

datos, VoIP, Telnet, etc. Es decir, tráfico de la capa de aplicación, de red o de transporte.

Además, se pueden emular procesos estocásticos y especificar distintas distribuciones de tamaños de paquetes en la generación de tráfico (exponencial, uniforme, normal, cauchy, Pareto, etc.). Dichas atribuciones son las que permiten al final de cuentas generar tráfico equivalente al de una llamada de VoIP por ejemplo.

La herramienta puede inyectar tráfico a nivel de red, de transporte y de aplicación. Además permite medir el retardo de ida OWD (“One Way Delay”), el ETT, la tasa de pérdida de paquetes, el “jitter” y el “Throughput”.

Sigue el paradigma cliente servidor y posee 4 ejecutables principales: ITGSend, ITGRecv, ITGLog e ITGDec, además de 2 secundarios_ ITGPlot e OTGGapi. En la capa de transporte, D-ITG soporte TCP (Trasmission Control Protocol), UDP (User Datagram Protocol), SCTP (Stream Control Transmission Protocol) y DCCP (Datagram Congestion Control Protocol).

3.5.2. Arquitectura.

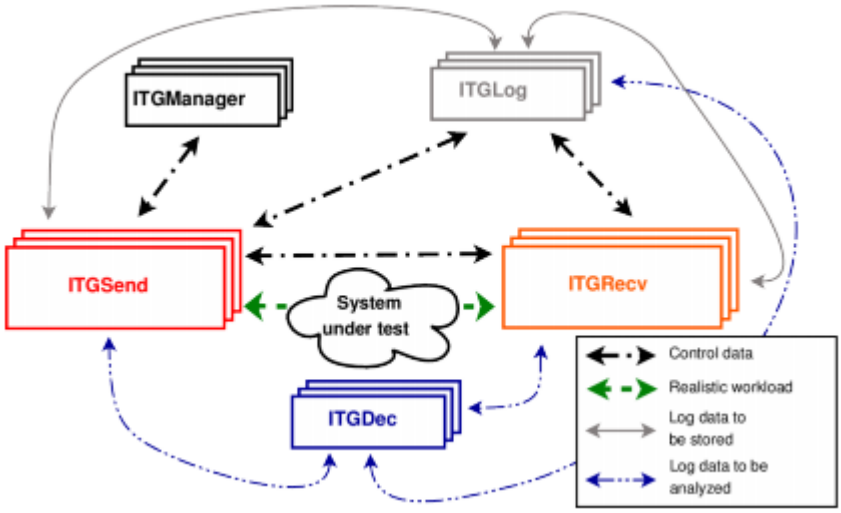


Figura 3-8 Arquitectura D-ITG.

Las características fundamentales de D-ITG son proporcionados por ITGSend e ITGRecv. ITGSend es el componente responsable de la generación de tráfico hacia ITGRecv. La explotación de un diseño de multiproceso, ITGSend puede enviar múltiples flujos de tráfico paralelo hacia varias instancias de ITGRecv e ITGRecv puede recibir múltiples flujos de tráfico paralelo de instancias ITGSend. Se crea un canal de señalización entre cada par de componentes ITGSend e ITGRecv para controlar la generación de todo flujo de tráfico entre ellos.

ITGSend e ITGRecv opcionalmente puede producir archivos de registro que contiene información detallada sobre todos los paquetes enviados y recibidos. Estos registros se puede guardar localmente o enviados a través de la red al componente ITGLog (útil para recoger todas las medidas en un solo punto o en el caso de que un host con capacidades limitadas de almacenamiento, por ejemplo, sensores, dispositivos embebidos, Smartphone, etc.). El componente ITGDec es la encargada de analizar el registro de archivos con el fin de extraer las métricas de rendimiento relacionados con el flujo de tráfico.

3.5.2.1. ITGSend (Sender Component of the D-ITG Platform)

El componente ITGSend es responsable de generar flujos de tráfico y puede trabajar en 3 diferentes modos.

- Flujo Simple: lee la configuración de un flujo de tráfico simple hacia una sola instancia ITGRecv desde la línea de comandos.
- Multi Flujo: lee la configuración de varios flujos de tráfico para generar hacia una o varias instancias de ITGRecv desde un archivo script. El script es hecho de una línea por cada flujo de tráfico, que incluye el conjunto de opciones de líneas de comandos como en el de flujo simple.
- Deamon: Corre como un demonio escuchando en un Socket UDP las instrucciones y puede ser controlado de forma remota utilizando el API de D-ITG.

Todo flujo de tráfico generado es descrito por 2 procesos Estocásticos relacionando con el Tamaño de Paquete (PS) y la hora de salida a Internet (IDT).

3.5.2.2. ITGRecv (Receiver Component of the D-ITG Platform)

Es el componente responsable de recibir múltiples flujos de tráfico generados por una o varias instancias ITGSend. Normalmente se ejecuta como un demonio escuchando en un socket TCP para peticiones de recepción de tráfico entrante.

3.5.2.3. ITGLog (Logger Component of the D-ITG Platform)

El componente ITGLog es responsable de recibir y guardar información de logs posiblemente enviados por ITGSend e ITGRecv. Se ejecuta como un demonio escuchando un socket TCP para peticiones de log entrante. La información de Log es recibida sobre protocolos TCP o UDP en números de puerto dinámicos entre el rango de 9003 – 10003.

3.5.2.4. ITGDec (Decoder Component of the D-ITG Platform)

El componente ITGDec es responsable de decodificar y analizar los archivos log almacenados durante el experimento usando D-ITG.

ITGDec analiza el registro de los archivos generados por ITGSend e ITGRecv y calcula los valores promedios de la tasa de bits, retardos y jitter sea en toda la duración del experimento o en intervalos de tiempo de gran tamaño. (Alessio Botta, 2013)

3.6. Wifi Analyzer

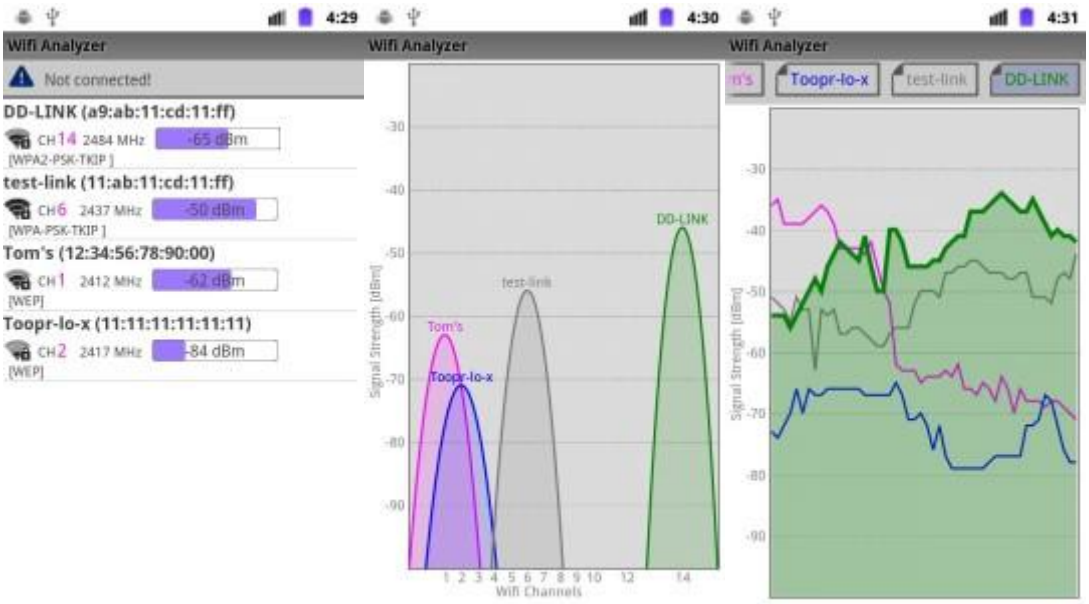


Figura 3-9 Wifi Analyzer.

3.6.1. Funcionamiento

Wifi Analyzer es una potente herramienta con la que podremos medir la calidad de las diferentes redes Wifi que estén a nuestro alrededor, pudiendo medir la intensidad de estas redes, el tráfico que están llevando a cabo y el número de usuarios que están usando dicha red.

Gracias a Wifi Analyzer, podremos conectarnos a la red que esté más vacía, con menos tráfico y con mejor señal, para así tener la mejor experiencia posible con nuestra conexión Wifi.

Wifi Analyzer se puede descargar directamente desde el Android Market de forma gratuita y requiere de Android 1.5+ para funcionar.

3.6.2. Características

- Wifi Analyzer no se ha diseñado para hackear redes inalámbricas ni tampoco robar claves Wifi de los vecinos, sino para comprobar la seguridad desde el móvil.

- Wifi Analyzer audita una vulnerabilidad conocida de algunos routers Wifi cuya configuración de fábrica no ha sido modificada.
- Wifi Analyzer es una App busca redes Wifi de determinados modelos de Router y te muestra al instante su contraseña por defecto.
- Si una red Wifi es vulnerable, Wifi Analyzer la marca como "Vulnerable".
- Podrás entonces calcular la contraseña presionando su nombre. Otro toque y Wifi Analyzer conectará con la red en cuestión.
- El funcionamiento de Wifi Analyzer es similar al de otras aplicaciones, como ReveLA Wifi o pulWifi. Si la App detecta, a partir de su nombre, redes inalámbricas de Movistar, Jazztel o Yacom, calcula su clave. También funciona con routers Comtrend, ZyXEL y DLink.
- La idea de Wifi Analyzer es aprovechar la conexión a Internet de tu dispositivo para navegar desde el ordenador.

3.7. Access Point

3.7.1. DLINK DIR 615

Figura 3-10 Router DLink.

3.7.1.1. Funcionamiento

El Router Wireless N para el hogar, DIR-615, de D-Link, es un dispositivo acorde con 802.11n y diseñado para los usuarios que requieren el mayor rendimiento de red al mejor coste. Al conectar el Router DIR-615 a un módem DSL o de cable, los usuarios podrán compartir el acceso de alta velocidad a internet con cualquier usuario de la red y crear una red inalámbrica segura para compartir fotos, música, vídeo, impresoras y reproductores de medios digitales a través de toda la casa (D-Link).

3.7.1.2. Características

- Alto rendimiento con total cobertura.
- Basado en la tecnología 802.11n, transmite y recibe múltiples flujos de datos, con lo que proporciona una cobertura completa por toda la casa y elimina los puntos muertos.
- Cumple con una política de buen vecindario, lo que garantiza que no creará interferencias en las redes vecinas. Esto se consigue con la reducción del espectro de radio usado cuando detecta una red 802.11g/b en el vecindario.
- Seguridad inalámbrica simplificada.
- Admite el estándar Wi-Fi Alliance para la seguridad inalámbrica con solo tocar un botón. Gracias a WPS (Wi-Fi Protected Setup), el nombre de red inalámbrica (SSID) y las claves de encriptación se generan automáticamente y se difunden a los dispositivos cliente. Los usuarios no han de memorizar complicadas contraseñas ni teclearlas varias veces. Esto simplifica considerablemente el proceso de configuración de la seguridad en la red inalámbrica.
- Compatible con Windows Vista
- Posee funcionalidades tales como detectar y gestionar sus dispositivos con Network Explorer y las características de Network Map en Windows Vista.

- Compatibilidad de servicio con Xbox Live. Por consiguiente, los usuarios disfrutarán de una sencilla configuración y gestión de la red, de un audio y vídeo streaming fiable, de diagnósticos de red integrados y de una conectividad a internet sin fallos para las aplicaciones de streaming, como los juegos en línea y las llamadas VoIP.
- Fácil configuración.
- Se puede usar con cualquier tipo de conexión a internet, ya sea basada en ADSL (no incluye módem), de cable o con ISP que ofrece telefonía o TV con acceso a internet. El asistente Click'n Connect (DCC) de D-Link permite que cualquier persona sin ningún conocimiento técnico previo pueda instalar el Router y conectarlo a internet en unos pocos minutos, simplemente ejecutando el CD-ROM del producto. En unos pocos y sencillos pasos, el asistente guía al usuario para establecer las conexiones físicas (alimentación y cableado), configurar los parámetros inalámbricos de red y la seguridad, y conectar al ISP.
- El soporte de los estándares WEP, WPA y WPA2 garantizan que se puede usar la mejor encriptación posible y, al mismo tiempo, los firewalls duales activos (SPI y NAT) evitan los potenciales ataques desde internet.
- Ha obtenido la certificación 802.11n de Wi-Fi Alliance®, una distinción que garantiza la interoperabilidad entre los productos 802.11n, la adhesión a los protocolos de seguridad y la compatibilidad con anteriores generaciones de equipos Wi-Fi, incluidos los populares productos 802.11g.
- La velocidad máxima de la señal inalámbrica la definen las especificaciones del estándar IEEE 802.11g y 802.11n. Las velocidades 802.11n se obtienen al funcionar con productos Wireless N de D-Link. El rendimiento real variará. Las condiciones de la red y los factores medioambientales, como el volumen de tráfico por la red, los materiales de construcción y las edificaciones, pueden disminuir

la velocidad real de los datos. Los factores medioambientales pueden afectar negativamente al alcance de la señal inalámbrica. Los productos Wireless se basan en las especificaciones IEEE 802.11n y no se garantiza que sean compatibles con futuras versiones de las especificaciones IEEE 802.11n. No se garantiza la compatibilidad con los dispositivos 802.11n de otros fabricantes. (Dlink, DIR-615, 2014)

3.7.2. D LINK DIR 619L

Figura 3-11 Router Link.

3.7.2.1. Características

El Cloud Router Wireless N300, DIR-610L de D-Link, permite compartir una conexión de banda ancha a internet entre varios computadores del hogar. Una vez conectado, se puede crear una red doméstica inalámbrica personal para poder compartir documentos, música y fotografías.

Basado en la tecnología Wireless N con 3 antenas de alta ganancia de 5dBi, alcanza velocidades inalámbricas de hasta 300 Mbps y amplía la cobertura, Cuenta con 4 puerto Ethernet 10/100 Base-Tx que permite conectar varios dispositivos de cable como PC, videoconsolas, etc.

Soporte las últimas características de seguridad inalámbrica para evitar el acceso no autorizado tanto a través de la red inalámbrica como de internet. El soporte de los estándares WEP, WPA, WPA2 garantiza que se usa la mejor encriptación posible, incluye controles parentales, lo que permite bloquear o permitir determinados sitios web. (D-Link)

3.7.3. TPLINK WR541G

Figura 3-12 Router Link.

3.7.3.1. Características (TP-LINK)

- Integra firewall, Router NAT y punto de acceso inalámbrico, dedicado a la pequeña oficina u oficina en el hogar, lo cual le permite establecer una mejor conexión inalámbrica, compartiendo acceso a Internet, juegos en línea o difusión de videos.
- Es compatible con Puente WDS inalámbrico que ofrece una interconexión para ampliar la cobertura de su red, lo que es conveniente para que usted pueda tener señal en las diferentes habitaciones u oficinas.

- Cuando se trata de la instalación, el Asistente de Configuración puede llevarte a través del proceso de instalación paso a paso, e incluso ayuda con la configuración de red inalámbrica y las configuraciones de seguridad, especialmente para los usuarios novatos.
- Compatible con el estándar IEEE 802.11g / b y adopta la tecnología de transmisión WLAN extended Range(TM) 2x a 3x para que la distancia de transmisión sea de 2 a 3 veces de las soluciones tradicionales 11g / b. Es decir, el rango de transmisión se extiende a 4-9 veces, lo que efectivamente podría mejorar el rendimiento inalámbrico.
- IP QoS – Control razonable de Ancho de banda
- Es compatible con la función QoS, permitiendo la utilización óptima del ancho de banda y ofrece un control de ancho de banda por la congestión, la prevención del uso indebido de ancho de banda. De esta manera, los usuarios de una pequeña red reciben un ancho de banda comprometido y específico, evitando que las aplicaciones no críticas degraden el rendimiento de la red.
- Encriptado WPA/WPA2 - Seguridad Avanzada, En cuanto a la seguridad de la conexión WI-FI, el encriptado WEP ha dejado de ser el más fuerte y más seguro como protección de las amenazas externas. TL-WR541G proporciona encriptación WPA/WPA2 (personal y empresas) que son creados por el grupo de la industria Wi-Fi Alliance, la prevención de su red de intrusiones externas de manera eficiente.
- Fácil instalación (TP-LINK)

3.8. Tarjetas de Red Inalámbricas

3.8.1. Atheros AR5B95

3.8.1.1. Funcionamiento

Este módulo es compatible con todas las notebooks HP e IBM que tienen un zócalo mini PCI-E.

La placa de red PCI-Express de chip único AR9285 cuenta con la tecnología Alinear de Atheros que aprovecha el 802. 11n 1–stream para proporcionar la ruta óptima de actualización de 802.11. La característica de flujo único permite una nueva clase de dispositivos Wi-Fi que ofrecen mejoras de rendimiento sobre la tecnología 802.11 g existente, a precios comparables. Alinear ™ soluciones son compatibles hacia adelante con mayor rendimiento, multi-stream, MIMO–based 802. 11n y están disponibles en diseños de referencia para servir a las redes, los mercados de electrónica de PC y de los consumidores. El rendimiento mejorado de alinear 1–stream mejora la eficiencia de la red por el canal inalámbrico de ocupación durante períodos más cortos que los dispositivos más lentos de 11 g: reduce la congestión y aumenta la capacidad de los dispositivos inalámbricos adicionales. Alinear emplea todos las obligatorias y seleccionadas características opcionales de la especificación de grabador y técnicas de diseño de radio avanzada de Atheros, y efectivamente doble cobertura inalámbrica WLAN (Modem Help UK Atheros AR5B95 11bgn PCIe Mini-Card Reference Design).

3.8.1.2. Características

- Soporta hasta 150 Mbps
- Solución de PCI Express CMOS con un único chip altamente integrado con
- Radio de 2,4 GHz y procesador MAC/baseband
- Compatibilidad para 802. 11 g; y compatible para 802. 11n

- Soporta IEEE 802. 11n
- Compatible con IEEE 802. 11b, 802. 11 d, 11e, estándares 802.11 g y especificación de 802. 11i.
- Standard IEEE 802.11 b/g/n, Wi-Fi compliant
- Chipset Atheros AR9285
- Host Interface PCIE half size Mini-Card
- Radio
- Antena
    - Hirose U.FL-R-SMT ANT1:TX/RX ANT2:RX
    - Operating Frequency 2.4 GHz ISM Bands 2.412-2.472 GHz, 2.484 GHz

Número de canales 802.11b: USA, Canadá y Taiwán 1, países Europeos 13, Francia 4, Japón 14, 802.11g: USA y Canadá 11, países Europeos 13,

- Modulación 802.11 g/n: OFDM 802.11b: CCK(11, 5.5Mbps), QPSK(2Mbps), BPSK(1Mbps)
- Transmisión de Datos 802.11b: 11,5.5,2,1 Mbps; 802.11g: 54,48,36,24,18,12,9,6 Mbps; 802011n: up to 150Mbps
- Output Power 802.11b 17dBm +/- 1.5 dBm; 802.11g 16dBm +/- 1.5 dBm; 802.11n (HT20) 15dBm +/- 1.5 dBm; 802.11n (HT40) 12dBm +/- 1.5 dBm
- Sensibilidad de Recepción 802.11b -80dBm at 11Mbps; 802.11g -70dBm at 54Mbps; 802.11n -61 dBm at HT40 MCS7 -64 dBm at HT20 MCS7
- Voltaje de Operación: DC 3.3V ± 5%
- Dimensiones 29.85 X 26.65 x 3.25 mm
- Weight 3.8g
- Software para Windows XP/ Vista/ 7
- Seguridad WEP 64-bit and 128-bit encriptación; WPA (Wi-Fi Protected Access); WPA2 (Wi-Fi Protected Access) Soporta hasta 150 Mbps.

3.8.2. Tarjeta Broadcom BCM4330 (Sony Xperia Z)

3.8.2.1. Características

- Soporta estándares IEEE802.11a/b/g/n
- Soporta Wifi Direct con dispositivos compatibles en frecuencias de 2.4Ghz/5Ghz
- Soporte Wifi Protect Setup
- Wi-fi Miracast
- Soporte para punto de acceso
- Transferencia de datos sobre los 150Mbps
- Autenticación y compartimiento de seguridades
  - EAP-SIM
  - EAP-AKA
  - EAP-TLS
  - EAP-TTLS/MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - WPA Personal and WPA2 Personal
  - WPA Enterprise and WPA2 Enterprise
  - Encriptación WEP 64 bit, WEP 128 bit, TKIP and CCMP (AES) (Broadcom, 2015)

3.8.3. Tarjeta Inalámbrica Intel Pro Wireless 3945ABG

Figura 3-13 Mini Card PCI Intel.

3.8.3.1. Descripción

El adaptador de red Intel Pro/Wireless es un adaptador integrado para un procesador de tecnología Intel Centrino y orientado a computadores personales. Provee libertad y flexibilidad para funcionar sin un conector telefónico, cable de red o conector especial (Distech) (Modem Help UK Atheros AR5B95 11bgn PCIe Mini-Card Reference Design).

3.8.3.2. Características

- Fácil uso y Manejabilidad
  - Software diseñado para usabilidad.
  - Interfaz intuitiva
- La facilidad de uso y capacidad de administración
- Intel PROSet / Wireless Software ® es un cliente inalámbrico avanzado que está diseñado para su uso.
- El software de Intel PROSet permite una experiencia móvil superior para los consumidores y usuarios de la empresa al proporcionar apoyo Soluciones Intel Smart Wireless que incluye:
  - Asistente de seguridad - simplifica la configuración de seguridad WLAN
  - Diagnóstico para redes inalámbricas - ayuda a los usuarios con conectividad Wifi y captura de eventos para solucionar problemas
- Guarde los perfiles que permiten a los usuarios conectarse de forma automática y cambiar entre las redes de seguridad
- Herramienta de administración de TI - permitiendo a los administradores de red gestionar de forma remota y actualizar la configuración inalámbrica en los clientes
- Perfil de gestión centralizada simplifica la distribución de perfil
- Inicio de sesión único apoyo que permite un único conjunto de credenciales para autenticar al usuario , tanto de la red WLAN y de la máquina / de dominio

- Wake on WLAN - permite la activación remota de los clientes móviles para realizar actualizaciones de software
- Apoyo EAP- SIM permite con un solo proyecto de ley la itinerancia entre redes celulares y puntos de acceso WLAN compatibles
- Seguridad
  - La tecnología de procesador Intel Centrino soporta los últimos estándares de la industria que permite conectividad segura notebook. También proporciona soporte mejora de seguridad de terceros para Cisco * Compatible Extensions (como LEAP, EAP-FAST y CKIP.) Con la certificación a los fabricantes de PC, esta función permite la interoperabilidad con Cisco * Arquitectura Inalámbrica Unificada de Cisco y otros * productos validados compatibles.
- Rendimiento
  - Con un rendimiento de hasta 54 Mbps a 5 GHz (802.11a) y 2,4 GHz (802.11g), la familia de red inalámbrica Intel PRO permite conexiones de red rápidas. El Sistema de Convivencia inalámbrica Intel ayuda a reducir la interferencia con ciertos dispositivos Bluetooth.
  - Protocolo de ahorro de energía (PSP) es una característica seleccionable por el usuario, con cinco estados de energía diferentes, lo que permite al usuario hacer su propio poder frente a la elección de rendimiento en el modo de batería.
- Gran duración de la batería
- Especificación

3.8.4. D-Link DWA-110.

Figura 3-14 D-Link DWA-110.

3.8.4.1. Características

El adaptador inalámbrico USB 2.0 USB Wireless 110 de D-Link ofrece una conexión inalámbrica de 54Mbps 802.11g, se podrá tener una conectividad fácil y sencilla en la oficina o en cualquier Punto de Acceso.

Para proteger los datos y tener privacidad el adaptador incorpora como mecanismos de seguridad los estándares de encriptación WEP, WPA/WPA2-PSK y WPA/WPA2-EA para una conexión y tráfico de red seguro a través de una red Wireless.

Compatible con dispositivos inalámbricos anteriores 802.11b para poder garantizar la plena interoperabilidad entre los productos nuevos del mercado y los ya existentes.

Puede ser instalado en Windows Vista, Xp, ME, 2000, 98, 7.

(Dlink, 2014).

CAPITULO 4

4. DISEÑOS E IMPLEMENTACIÓN

El presente capítulo describe los procedimientos a ser efectuados por un administrador de red ante la necesidad de verificar una red inalámbrica. Para ello se ha desarrollado tres fases que permitirán determinar el comportamiento real de las redes.

En la primera fase se diseñaron tres escenarios de configuración básica de una red inalámbrica los cuales nos proporcionarán información en base a monitoreo en modo monocanal o tradicional y multicanal.

La segunda fase nos permite determinar cómo se comportan los equipos si el administrador opta por centrarse en un solo canal.

Finalmente la tercera fase mostrará aplicaciones de red como Roaming, WDS, interferencias, calidad de canal y autenticación con lo cual verificaremos en donde se muestra variaciones respecto de los escenarios básicos detallados en la primera fase.

4.1. FASE 1

En el desarrollo del análisis de tráfico de red inalámbrico WIFI, el administrador debe disponer escenarios de red base sobre los cuales debe guiarse para verificar el comportamiento de la red.

Para dicho proceso se establecieron tres escenarios que varían en función al número de puntos de acceso presentes al igual que los métodos de monitoreo aplicados.

4.1.1. ESCENARIO 1

El primer escenario se encuentra conformado por un único Access point configurado a 2.437GHz con seguridad WEP y una estación.

El propósito de evaluación en este escenario es determinar cómo operan los dispositivos que se verifican al realizar un monitoreo monocanal o tradicional.

Figura 4-1 Escenario 1

Para implementar el escenario se utilizaron los siguientes equipos:

- Access Point D-Link DIR-619L
- Tarjeta Inalámbrica Intel laptop Sony Vaio
- AirPcap Nx Adapter

Tabla 17 Direccionamiento MAC Escenario 1

Dispositivo	INTERFAZ	MAC	FUNCION
STA	Intel	00:1B:77:F3:A2:DC	Estación
AP	Inalámbrica	00:24:01:37:00:86	Punto de Acceso

Ya diseñado el primer escenario base procedemos con la configuración.

Configuración de Equipos AP

Para realizar la implementación del escenario disponemos del Access Point D-Link DIR-619L, dicho equipo se lo configura a través del panel de configuración web. En el panel de configuración inalámbrica ingresamos el SSID RADIUS correspondiente a nuestra LAN, seleccionamos el canal 6 y la seguridad WEP.

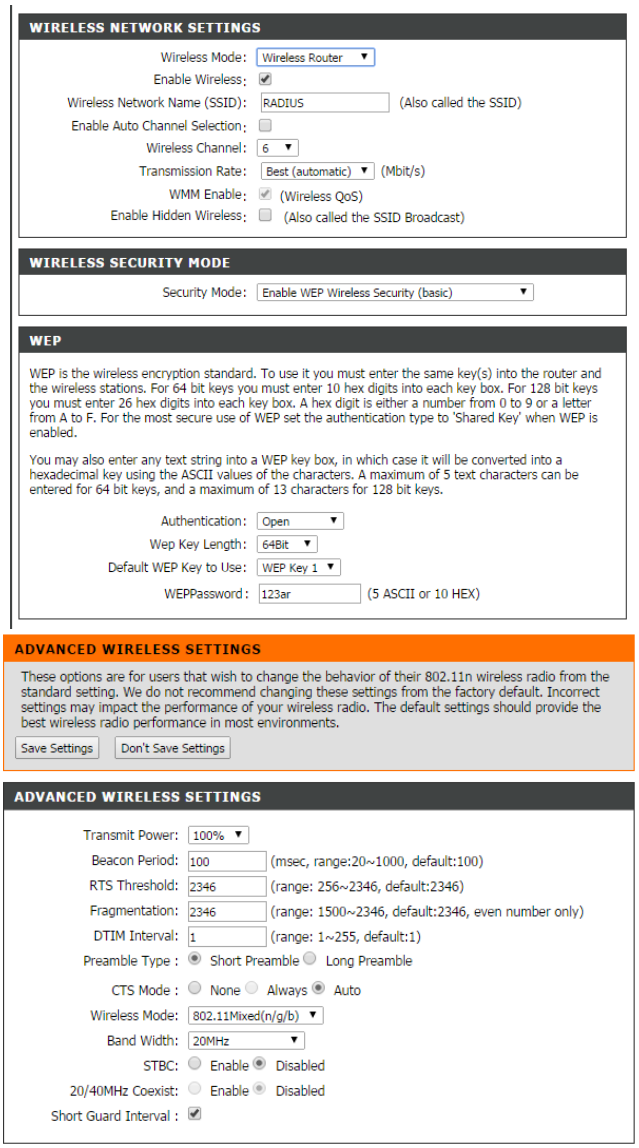


Figura 4-2 Configuración AP D-Link DIR-691L.

Configuración Commview.

Una vez configurado el equipo Access point se configura en la estación el programa de monitorización Commview seleccionando el canal 6 para

monitoreo de nuestra red o a su vez se configura desde el panel de control AirPcap el canal y los parámetros a ser monitoreados mediante la tarjeta.

Como referencia de la tarjeta seleccionada para monitoreo, Commview muestra en la parte superior de la ventana el nombre de la tarjeta desde la cual se mantiene sniffeando la red.

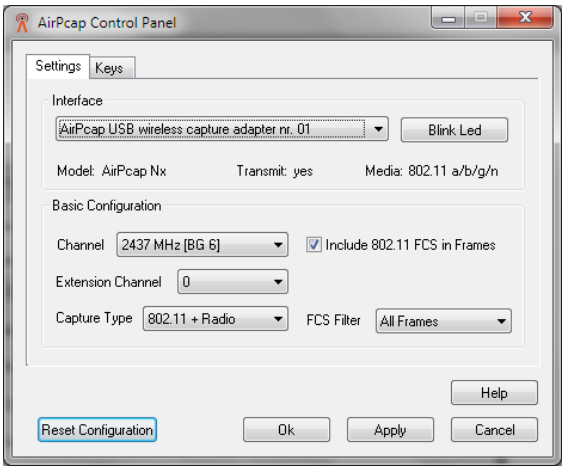


Figura 4-3 Configuración AirPcap.

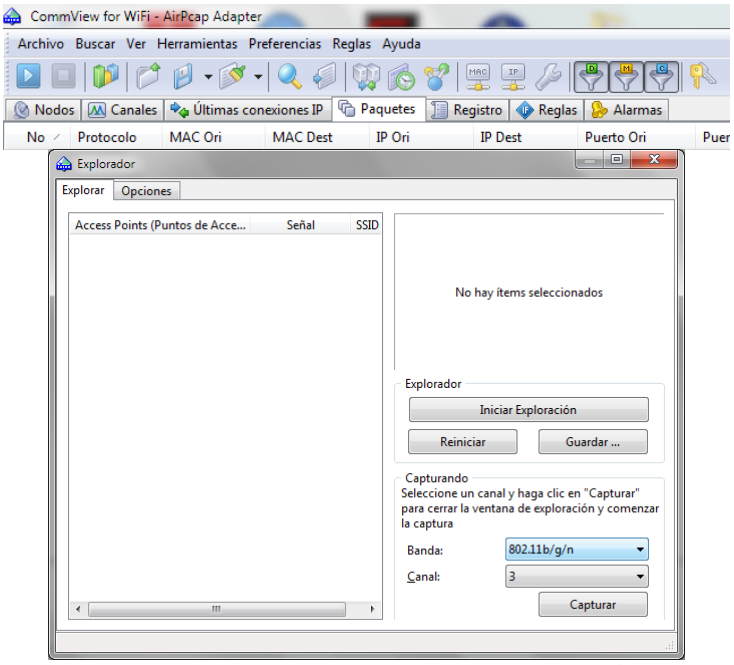


Figura 4-4 Commview opciones de análisis.

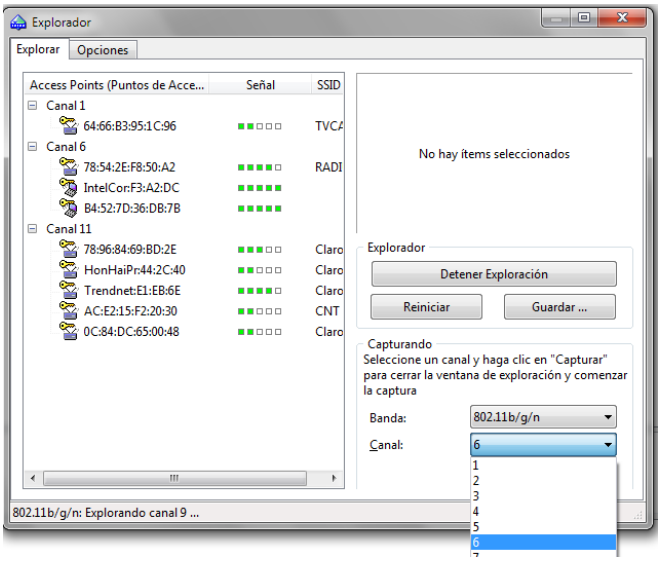


Figura 4-5 Captura Commview.

Finalmente se procede a asociar la estación inalámbrica a la red generada.

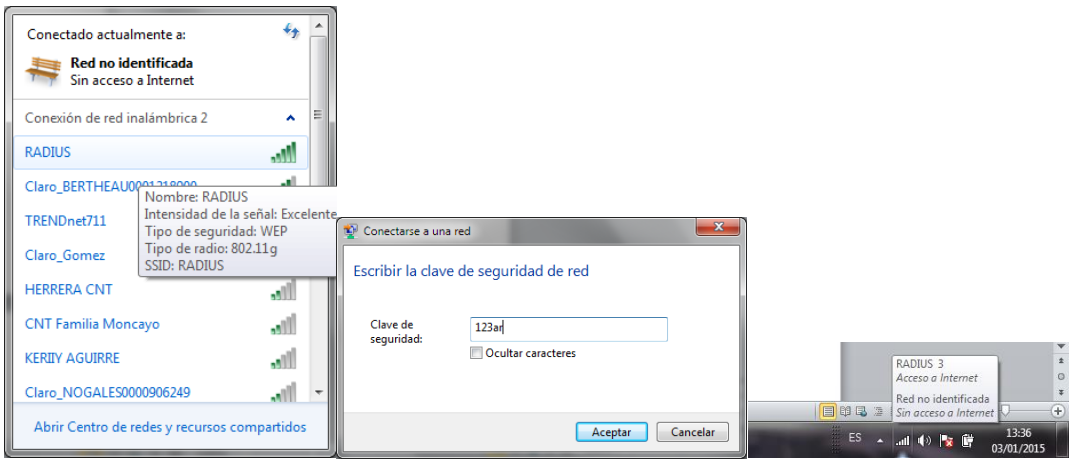


Figura 4-6 Asociación a Red Inalámbrica.

Verificación de Canal en inSSIDer.

Para el análisis de tráfico las herramientas de monitoreo son de gran importancia, como primer paso se procede a verificar el uso de los canales inalámbricos mediante el programa inSSIDer.

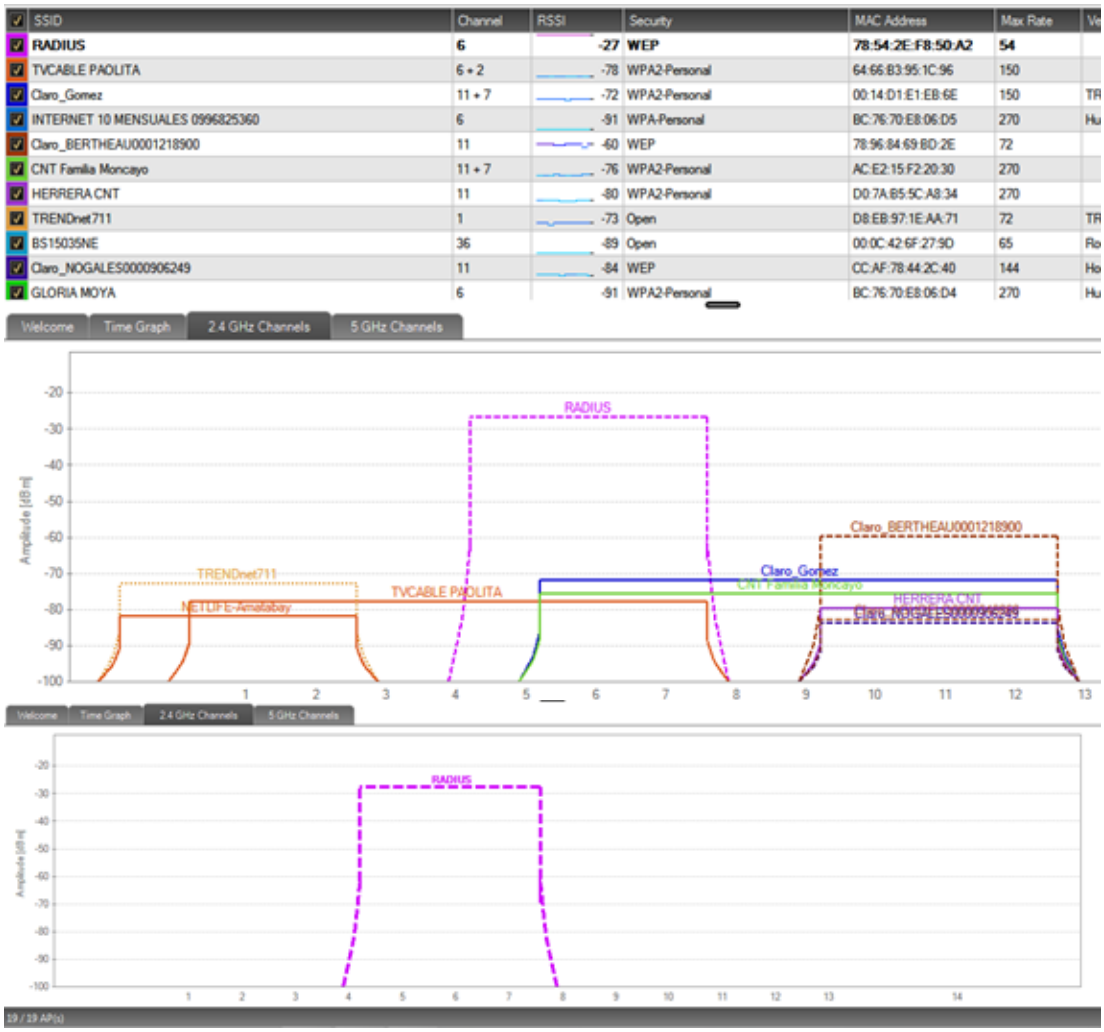


Figura 4-7 Configuración canal Access Point.

En este escenario se verifica que existen redes aledañas solapadas a bajas potencias como es el caso de las redes inalámbricas TVCABLE PAOLITA, Claro Gómez y CNT Familia Moncayo las mismas que se encuentran operando en estándar ieee802.11n, este se deduce debido a la representación gráfica de su ancho de banda a través de Inssider.

Tabla 18 Resumen valores redes aledañas.

SSID	RSSI (dBm)	Channel
TVCABLE PAOLITA	-78	6+2
Claro_Gomez	-72	11+7
CNT Familia Moncayo	-76	11+7

Una vez verificado los canales y la intensidad de señal de los mismos procedemos mediante Commview al monitoreo de la red. Commview dispone una herramienta similar a inSSIDer que permite realizar un barrido de canales y desplegar las estaciones y Access point que se encuentran operando en un mismo canal. Esta opción se genera al dar clic en el botón play y posteriormente en Iniciar Exploración.

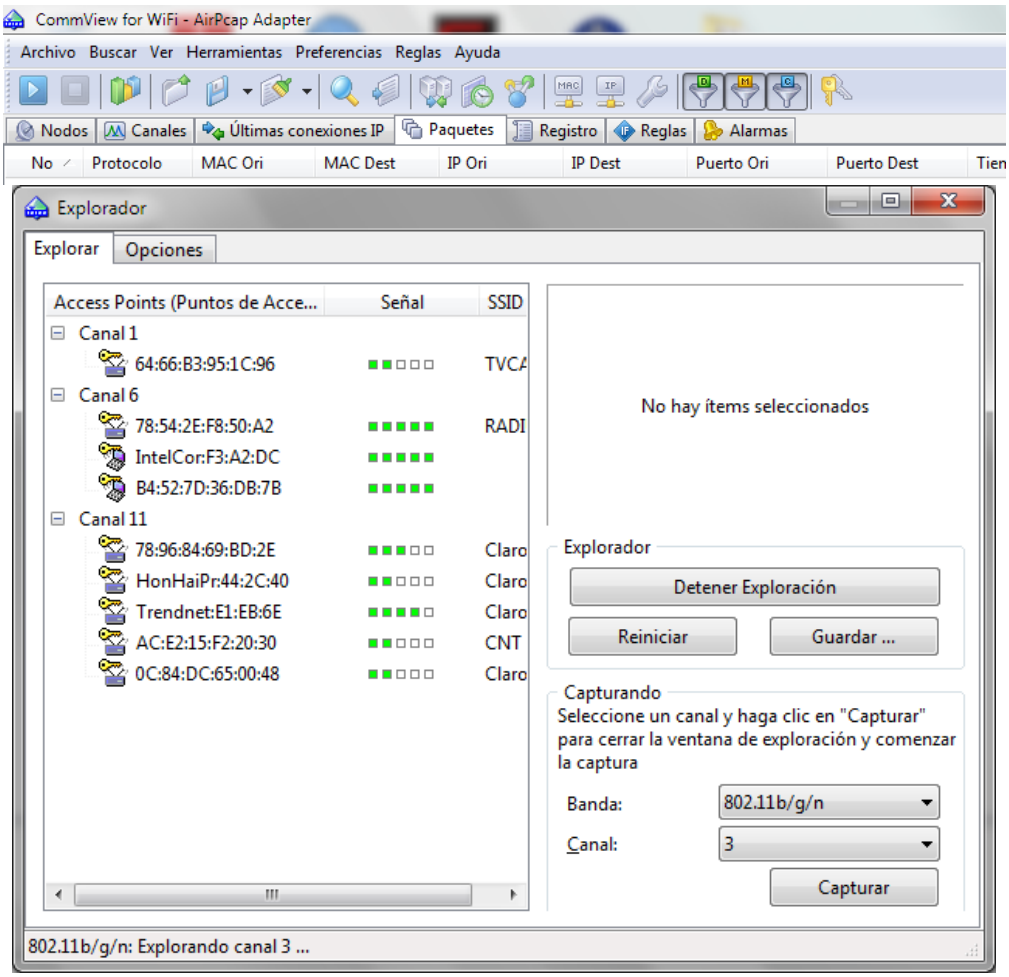


Figura 4-8 Captura con Commview

En la figura previa, Commview muestra al canal 6 con los dispositivos que se encuentran operando como son 78:54:2e:f8:50:a2, IntelCor:f3:a2:dc y el equipo b4:52:7d:36:db:7b, lo cual comparado con el escenario planteado se ve la adición del equipo b4:52:7d:36:db:7b y que puede ocupar cierto tiempo del canal si este se encuentra en pleno uso del mismo.

Para poder verificar cómo se comportan los equipos en la red inalámbrica Commview únicamente permite la selección de monitoreo para un solo canal, es decir se aplica el método de monitoreo monocanal y a través de las opciones como Nodos, Paquetes y Canales se puede verificar tanto el tramado y las estadísticas de paquetería para el escenario.

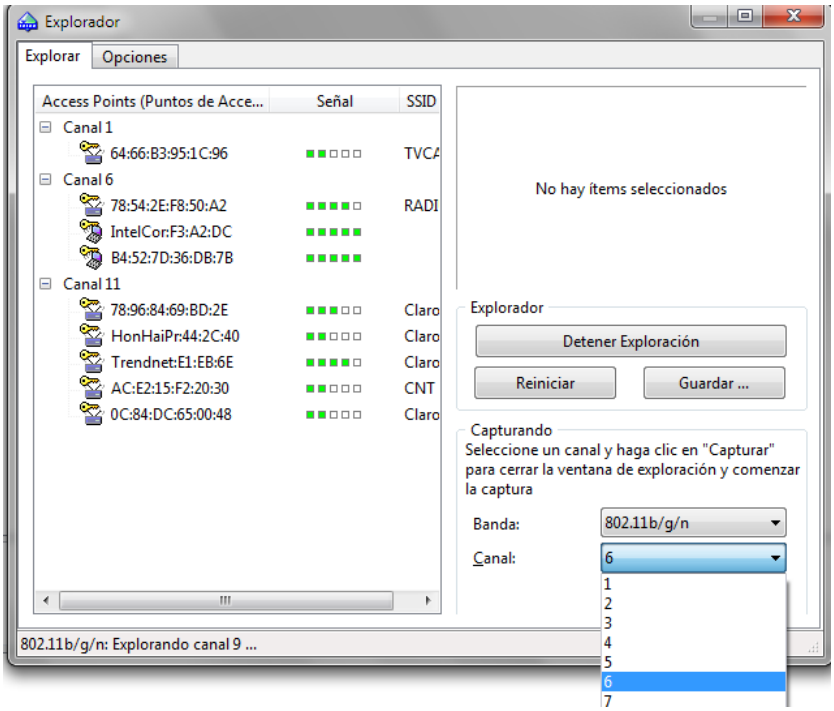
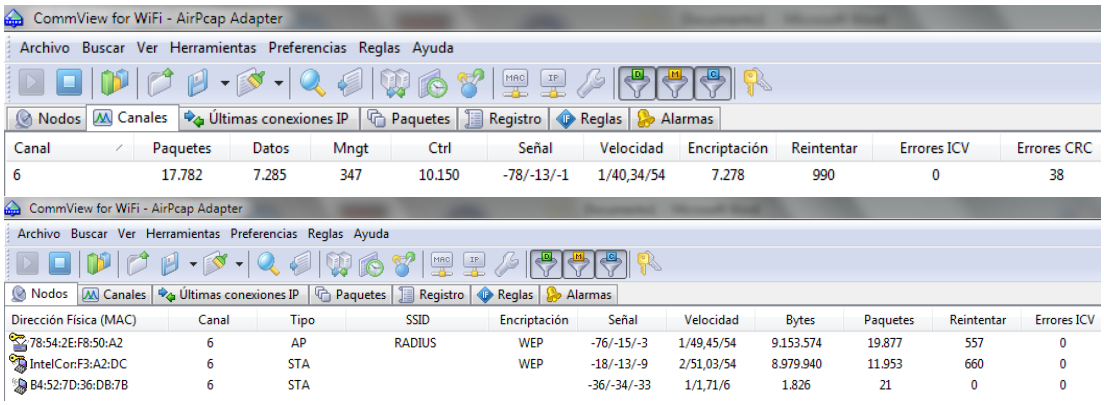


Figura 4-9 Cambio de canal.



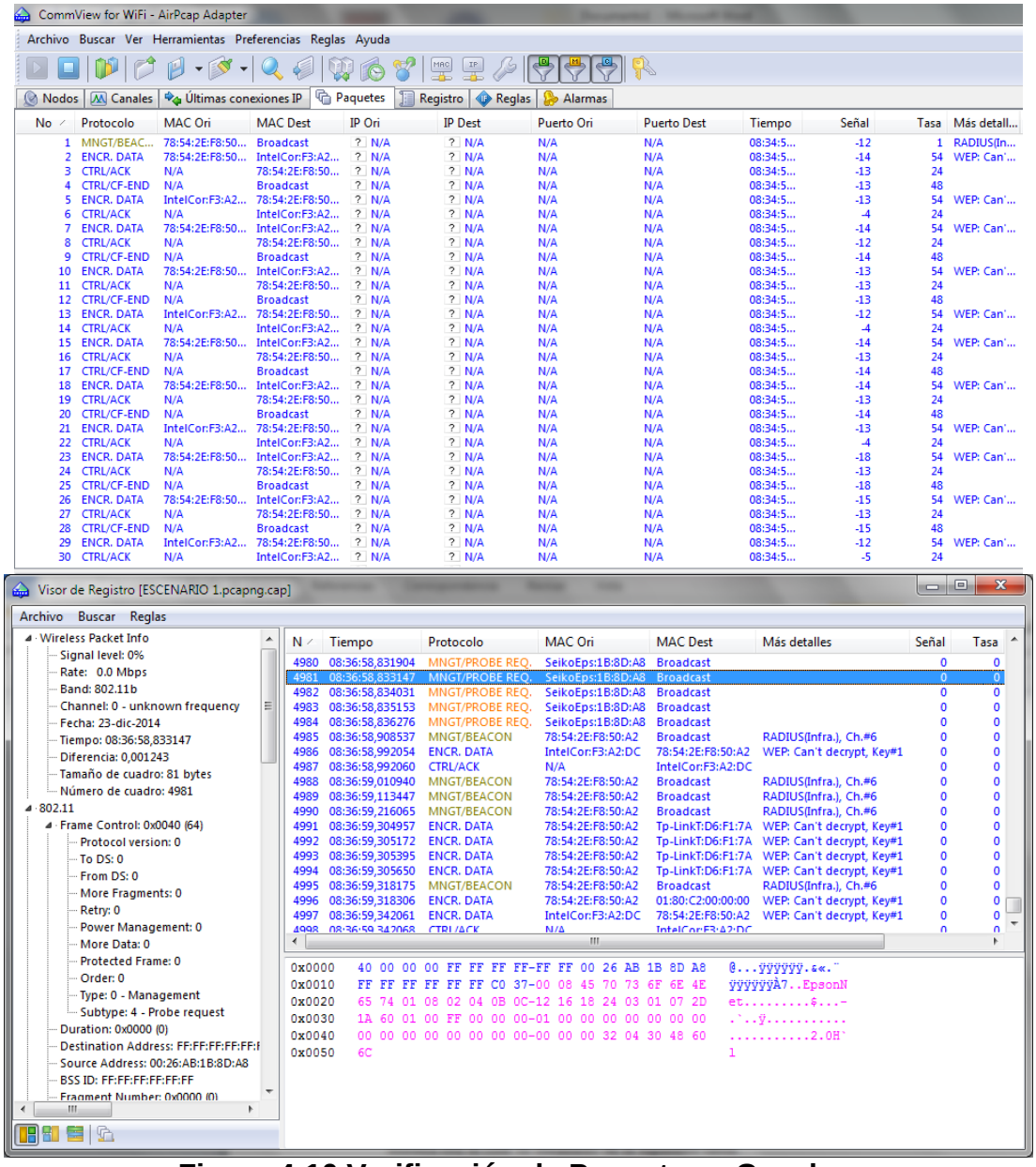


Figura 4-10 Verificación de Paquetes y Canales.

En las figuras anteriores nos muestran el resumen general del comportamiento de nuestra red el cual es detallado en la siguiente tabla.

Tabla 19 Resumen Escenario 1.

Dispositivo	MAC	SEÑAL (dBm)	VELOCIDAD (Mbps)	Trafico (MB)
STA	00:1B:77:F3:A2:DC	-13	51.03	9.153
AP	78:54:2E:F8:50:A2	-15	49.45	8.979

Para poder verificar el tramado, Commview permite que los datos capturados sean registrados en un formato compatible para poder ser analizados mediante herramientas como Wireshark a través de la opción *Guardar Registros de Paquetes como*.

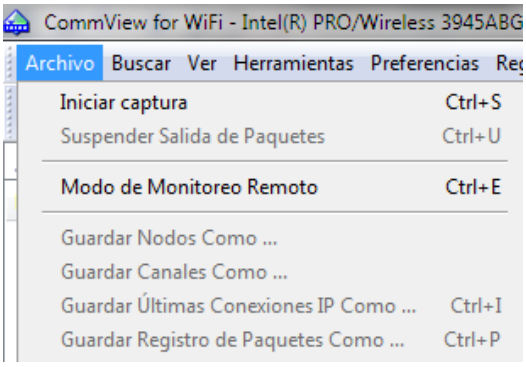


Figura 4-11 Guardado de datos Commview.

Una vez exportado los datos a Wireshark procedemos con el análisis de las tramas registradas en Commview.

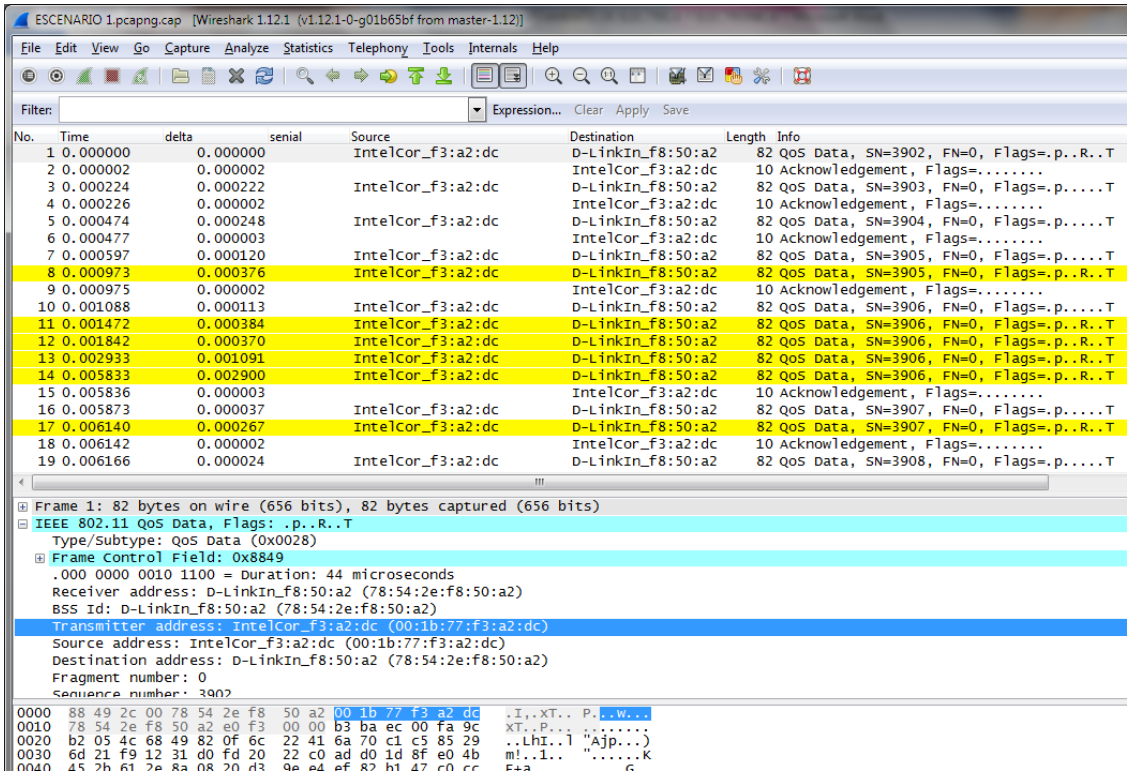


Figura 4-12 Paquetes en Wireshark.

Wireshark permite el uso de filtros que permite analizar de mejor manera las tramas capturadas, estos filtros son establecidos en base a los tipo de tramas ieee802.11.

Tabla 20 Comando de filtros trama de Management.

FRAME	SUBTIPO	FILTRO WIRESHARK
Management		wlan.fc.type eq 0
	Association Request	wlan.fc.type_subtype eq 0
	Association Response	wlan.fc.type_subtype eq 1
	Reassociation Request	wlan.fc.type_subtype eq 2
	Reassociation Response	wlan.fc.type_subtype eq 3
	Probe Request	wlan.fc.type_subtype eq 4
	Probe Response	wlan.fc.type_subtype eq 5
	Beacon	wlan.fc.type_subtype eq 8
	ATIM	wlan.fc.type_subtype eq 9
	Dissasociation	wlan.fc.type_subtype eq 10
	Authentication	wlan.fc.type_subtype eq 11
	Deauthentication	wlan.fc.type_subtype eq 12
	Action	wlan.fc.type_subtype eq 13

Tabla 21 Comando de filtros trama de Data.

FRAME	SUBTIPO	FILTRO WIRESHARK
Data		wlan.fc.type eq 2
	Data+CF ACK	wlan.fc.type_subtype eq 33
	Data+CF Poll	wlan.fc.type_subtype eq 34
	Data+CF ACK+CF Poll	wlan.fc.type_subtype eq 35
	Null Data	wlan.fc.type_subtype eq 36
	Null Data+CF ACK	wlan.fc.type_subtype eq 37
	Null Data+CF Poll	wlan.fc.type_subtype eq 38
	Null Data+CF ACK+CF Poll	wlan.fc.type_subtype eq 39
	CF Poll QoS Data	wlan.fc.type_subtype eq 40
	QoS Data+CF ACK	wlan.fc.type_subtype eq 41
	QoS Data+CF Poll	wlan.fc.type_subtype eq 42
	QoS Data+CF ACK+CF Poll	wlan.fc.type_subtype eq 43
	Null QoS Data	wlan.fc.type_subtype eq 44
	Null QoS Data+CF ACK	wlan.fc.type_subtype eq 46
	Null QoS Data+CF ACK+CF Poll	wlan.fc.type_subtype eq 47

Tabla 22 Comando de filtros trama de Control.

FRAME	SUBTIPO	FILTRO WIRESHARK
Control		wlan.fc.type eq 1
	Block ACK Request	wlan.fc.type_subtype eq 24
	Block ACK	wlan.fc.type_subtype eq 25
	Power Save Poll	wlan.fc.type_subtype eq 26
	Request To Send	wlan.fc.type_subtype eq 27
	Clear To Send	wlan.fc.type_subtype eq 28
	ACK	wlan.fc.type_subtype eq 29
	CF-End	wlan.fc.type_subtype eq 30
	CF-End ACK	wlan.fc.type_subtype eq 31

Adicional a estos filtros, Wireshark permite la aplicación de filtrado por colores con el fin de que el administrador de red pueda utilizarlos para identificar de mejor manera procesos como asociación, autenticación, Desautenticación de estaciones dentro de la red de acuerdo al propósito de análisis que se tenga. Este tipo de filtros se lo configura desde la pestaña View en Coloring Rules.

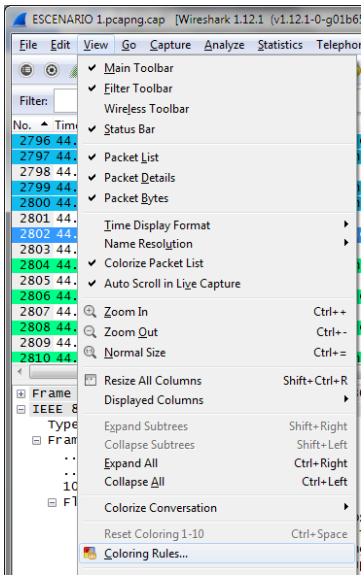


Figura 4-13 Configuración de Coloring Rules

En nuestro caso hemos distribuidos los filtros según la siguiente figura.

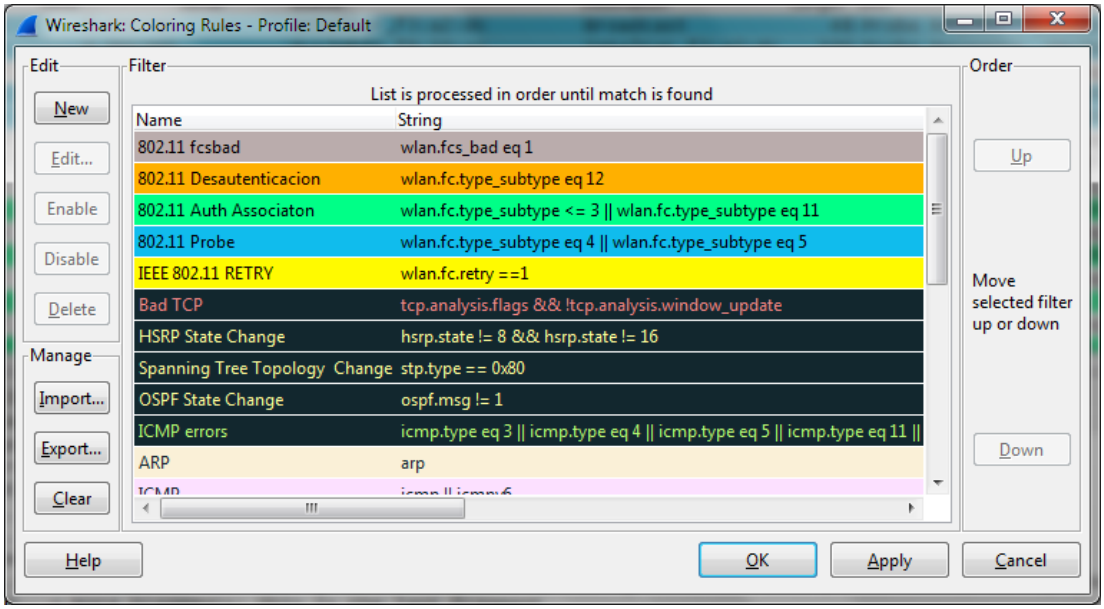


Figura 4-14 Configuración de Coloring Rules.

Por defecto Wireshark suele ya disponer aplicado ciertos filtros pero lo que se hace para añadir filtros es generar en New colocando el nombre que se le va a dar al filtro y los colores tanto del fondo como de las letras que aparecerán en el tramado al ser aplicado dicho filtro. Y son aplicados a las capturas al dar clic en el botón Coloring Packet List.

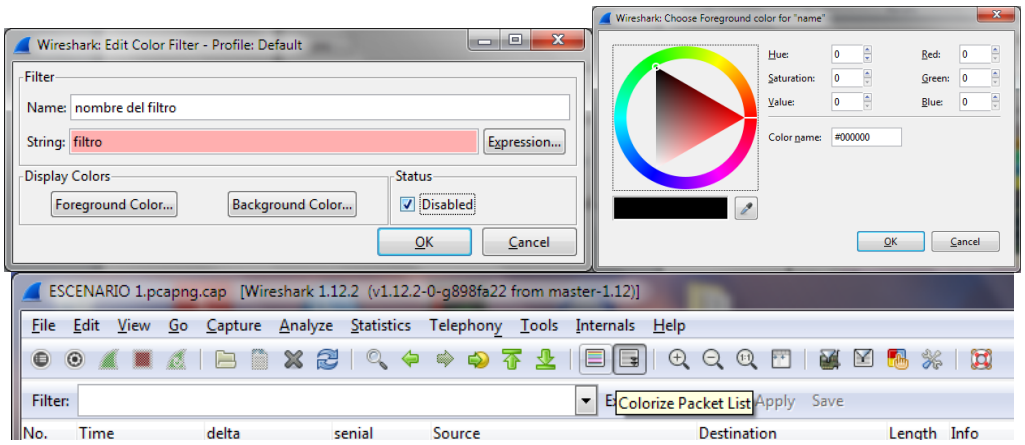


Figura 4-15 Selección de Colores.

Una vez aplicado los filtros indicados procedemos a determinar el comportamiento de la red planteada, mediante el monitoreo monocanal por lo cual procederemos con el filtrado.

Filtro: wlan.fc.type_subtype eq 1 or wlan.fc.type_subtype eq 3 or wlan.fc.type_subtype eq 5 or wlan.fc.type_subtype eq 8

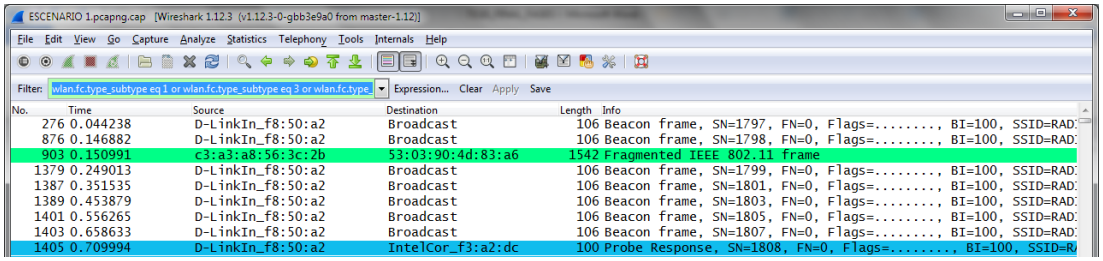


Figura 4-16 Filtrado de puntos de acceso Wireshark

En primera instancia, si requerimos identificar la cantidad de puntos de acceso presentes en un entorno de red, las tramas probe response al igual que las tramas beacon son utilizadas ya que son enviadas por los puntos de acceso ante la petición de las estaciones o para el caso de las tramas beacon se muestran periódicamente en un intervalo especificado en la configuración de los puntos de acceso siempre y cuando estos equipos muestren habilitados la propagación de dichas tramas.

Exportación a Excel.

Ya filtrado la paquetería es posible exportar el archivo filtrado con un formato compatible para análisis en Excel.

Para efectuar esta exportación se selecciona File, Export Packet dissection y as CSV (Comma Separated Values Packet summary) file; posteriormente nos pide guardar el archivo con el nombre deseado.

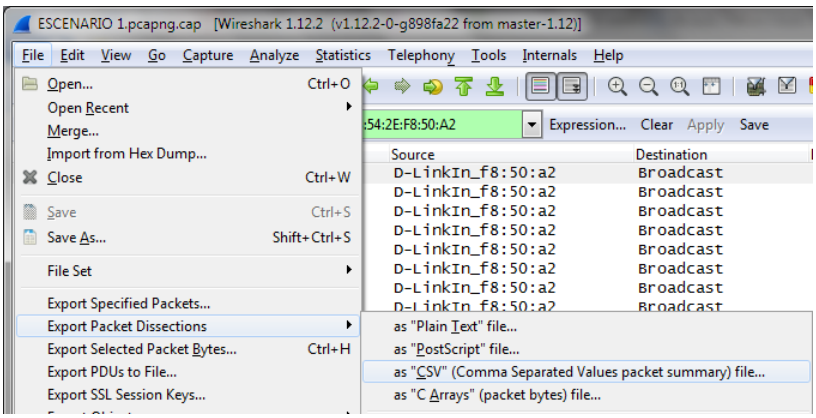


Figura 4-17 Exportación de Paquetes a Excel.

Una vez generado el archivo, desde Excel nos dirigimos a la pestaña datos y seleccionamos el ícono desde texto.

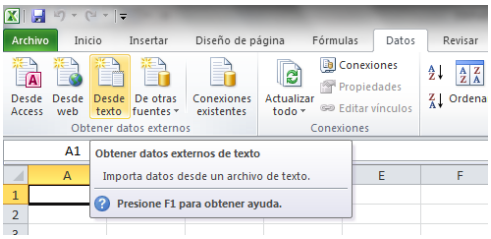


Figura 4-18 Selección de Datos.

Posteriormente aparece una pantalla mostrando archivos de texto o a su vez todos los archivos de la carpeta que se desea seleccionar.

Seleccionamos el archivo generado que para este caso nos aparece con icono de una hoja en blanco con el nombre de ESCENARIO 1 APS. Posteriormente aparece una serie de tres pasos mostrados a través de ventanas en Excel. En la primera ventana se marca la opción Delimitados para poder separar la información extraída desde Wireshark en forma de celdas de Excel. Adicionalmente, en la parte inferior se muestra el formato de nuestro archivo generado y se visualizan los datos de nuestra captura separados por comas.

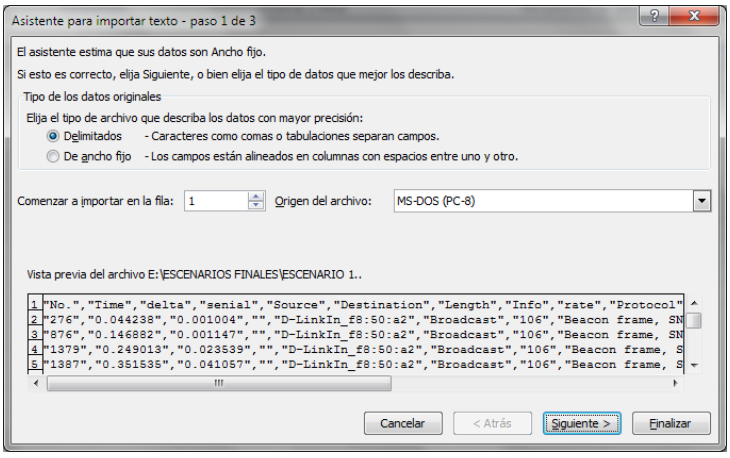


Figura 4-19 Delimitaciones.

La segunda ventana se selecciona la opción coma, para delimitar las columnas en base a las comas que aparecen en la parte inferior de la ventana.

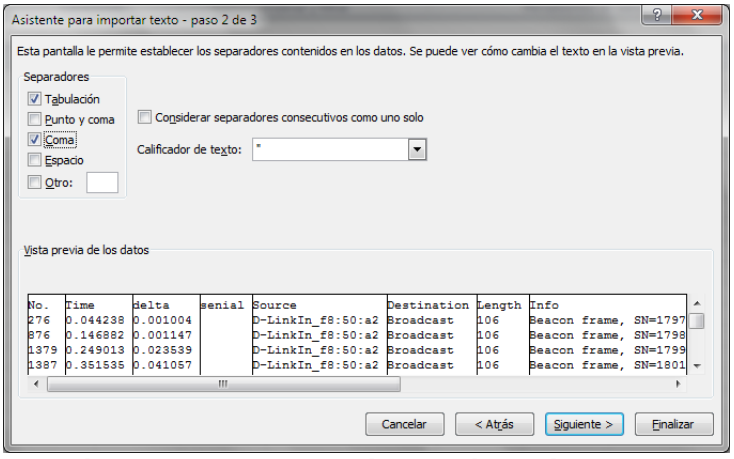


Figura 4-20 Separaciones de Columnas.

Finalmente en la última ventana se debe verificar que se encuentre seleccionada la opción General que permite convertir datos numéricos en números y texto en texto.

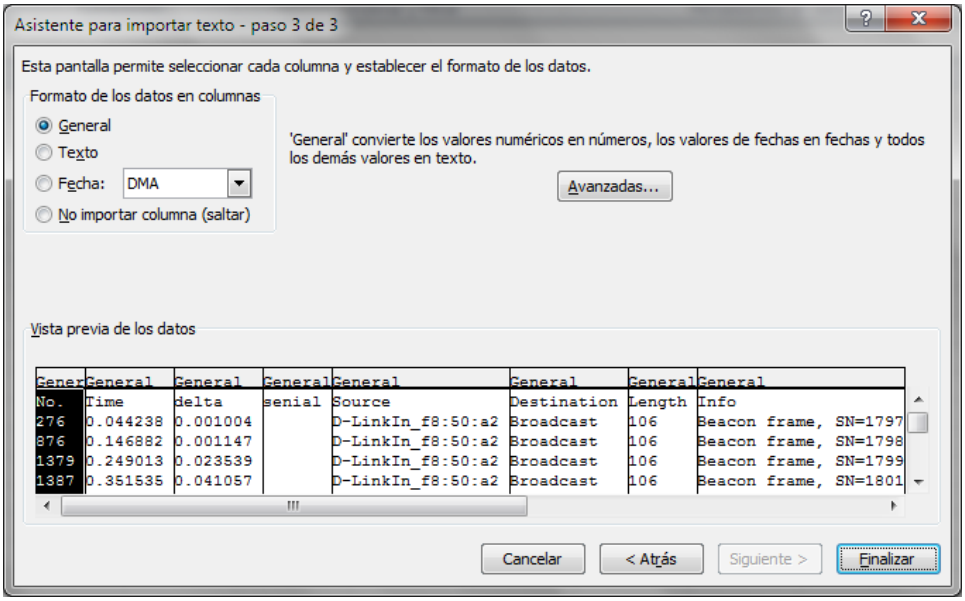


Figura 4-21 Conversión de valores.

Una vez importado en Excel podemos filtrar el archivo importado para evitar ítems duplicados y poder verificar la cantidad de puntos de acceso presentes en el escenario real. Para lograr el filtrado en Excel primero

seleccionamos uno de los títulos generados al importar el archivo en la parte superior de las columnas y nos dirigimos hacia la pestaña Datos en esta pestaña verificamos la opción Filtro en la cual nos aparecerá un botón en cada columna que permite la aplicación de filtros en base a los diferentes valores presentes en las columnas.

Con el fin de retirar datos duplicado de la columna Source nos dirigimos a Datos y damos clic en Quitar duplicados y posteriormente nos aparecerá una ventana con las columnas a las que se le puede aplicar este filtro; en nuestro caso dejamos seleccionado únicamente Source.

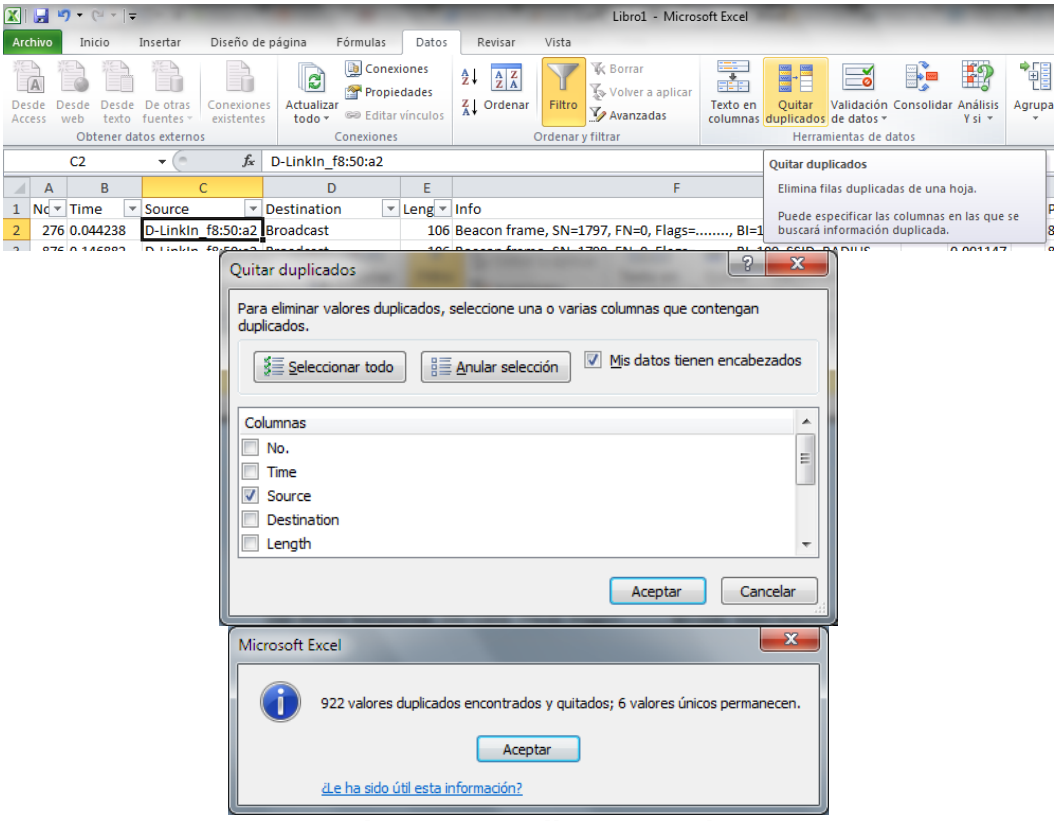


Figura 4-22 Filtros Excel

Y aplicado el filtro en Excel nos muestra un mensaje con la cantidad total de ítems duplicados y restantes por lo cual en nuestro escenario verificamos que existe un total de 6 puntos de acceso.

Tabla 23 Puntos de acceso Escenario1

PUNTO DE ACCESO	MAC ADDRESS
1	D-LinkIn_f8:50:a2
2	c3:a3:a8:56:3c:2b
3	1b:7b:c4:bd:2e:17
4	c4:b8:8c:71:58:4f
5	af:d7:a7:13:b8:b7
6	ad:90:5f:50:f2:13

Por otro lado con el fin de verificar las estaciones presentes en el ambiente de red de igual forma se aplican los filtros específicos.

Filtro: !(wlan.fc.type_subtype eq 1 or wlan.fc.type_subtype eq 3 or wlan.fc.type_subtype eq 5 or wlan.fc.type_subtype eq 8)

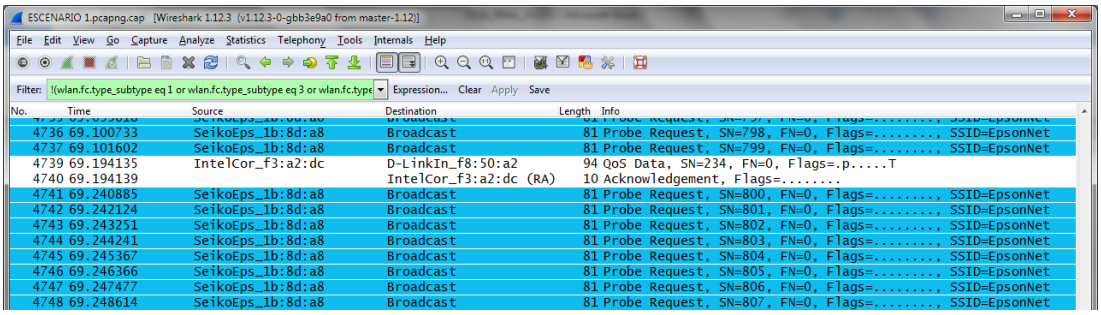


Figura 4-23 Filtrado por estaciones Wireshark

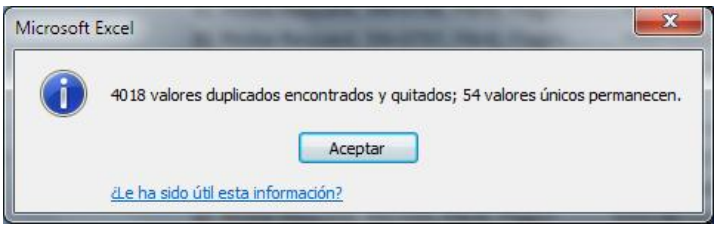


Figura 4-24 Resumen Filtro Excel

De igual manera que en los pasos detallados de filtrado en Excel previamente, procedemos a aplicar el filtrado para las estaciones el mismo que nos da un total de 54 estaciones un valor que es relativo ya que en el filtrado se presentaron dispositivos que se muestran como puntos de acceso que envían otro tipo de tramas por lo cual se comparó entre estaciones y

puntos para que no exista inconvenientes y determinar el número exacto de estaciones teniendo un total de 51 estaciones que operan en el canal 6.

Este resultado implica que pese a que se planteó un escenario base, cada uno de los dispositivos mostrados en el filtrado, utilizan el canal y dependerá mucho nuestra red de los protocolos de control y administración como RTS/CTS.

Para verificar que cantidad de tráfico que se genera de los dispositivos que no forman parte de nuestro escenario se requiere de la aplicación de filtros en los cuales se excluyan nuestros dispositivos.

Filtro: !(wlan.addr eq 00:1B:77:F3:A2:DC or wlan.addr eq 78:54:2E:F8:50:A2) and wlan.fc.type eq 0

Filtro: !(wlan.addr eq 00:1B:77:F3:A2:DC or wlan.addr eq 78:54:2E:F8:50:A2) and wlan.fc.type eq 1

Filtro: !(wlan.addr eq 00:1B:77:F3:A2:DC or wlan.addr eq 78:54:2E:F8:50:A2) and wlan.fc.type eq 2

Filtro: wlan.fc.retry eq 1 and (wlan.addr eq 00:1B:77:F3:A2:DC or wlan.addr eq 78:54:2E:F8:50:A2)

Tabla 24 Tráfico Generado Escenario 1

TRAMA	TOTAL BYTES	%	EQUIPO ESCEN1 BYTES	%	OTRO EQUIPO BYTES	%
MNGT	158157	13.3	98182	62	59975	37,92
CTRL	40428	3,4	10980	27,1	29448	72,8
DATA	986843	83,2	962593	97,5	24250	2,4
TOTAL	1185428	100	1071755	90.4	113673	9,6
RETRY	191349	16,14	153882	14,35	37467	1,78

De la tabla anterior verificamos que el 90.4% de tráfico es generado por la comunicación de los equipos de nuestro escenario de igual manera se verifica que el 72.8% de tramas de control son generadas desde equipos externos a nuestra red.

El filtrado ayudo a comprobar la cantidad de paquetes retransmitidos en el cual se verifica que 16.14% del total de paquetes fue retransmitido y el

14,35% de ese tráfico fue generado por los equipos que conforman nuestro escenario. Adicionalmente el tiempo que se mantuvo monitoreando el escenario fue 1 minuto 14 segundos.

Cabe mencionar que el archivo exportado desde Commview hacia Wireshark presenta únicamente información a nivel de capa MAC descartando las propiedades que posee AirPcap como es la adición de información de capa física como velocidad, nivel de señal

4.1.2. ESCENARIO 2

El segundo escenario se encuentra conformado por tres Access point configurados en el canal 1, 6 y 11 con seguridad WPA y dos estaciones.

El propósito de evaluación en este escenario es verificar cómo se comporta la red mientras se envía tráfico de una estación a otra tomando en cuenta la seguridad WPA implementada finalizando con el análisis de la paquetería y análisis estadístico obtenido de los programas de monitorización. Este hecho es válido gracias a la implementación de la monitorización multicanal ya que el monitoreo tradicional no permitiría verificar los cambios de canal que efectúa la estación dentro del escenario.

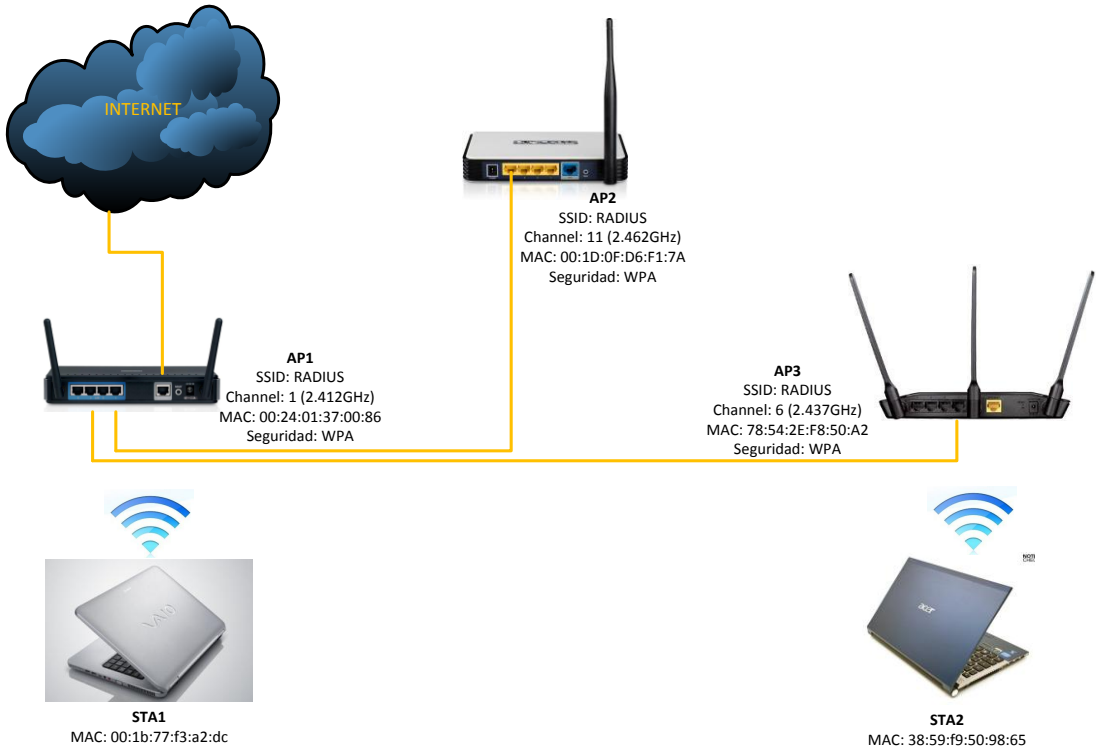


Figura 4-25 Esquema Escenario 2.

Para implementar el escenario se utilizaron los siguientes equipos:

- Access Point D-Link DIR-619L
- Access Point D-Link DIR 615
- Access Point TP-Link TL-WR542G
- Tarjeta Inalámbrica Intel laptop Sony Vaio
- Tarjeta Inalámbrica laptop Acer
- AirPcap Nx Adapter

Tabla 25 Direccionamiento MAC Escenario 2.

Dispositivo	INTERFAZ	MAC	FUNCION
STA1	Intel	00:1B:77:F3:A2:DC	Estación
STA2	Acer	38:59:F9:50:98:65	Estación
AP1	Inalámbrica	00:24:01:37:00:86	Punto de Acceso
AP2	Inalámbrica	00:1D:0F:D6:F1:7A	Punto de Acceso
AP3	Inalámbrica	78:54:2E:F8:50:A2	Punto de Acceso

Configuración de Equipos.

Para realizar la implementación del escenario disponemos del Access point D-Link Dir-615 (AP1), dicho equipo se lo configura a través del panel de configuración web en la sección Configuraciones. Una vez ubicados en las configuraciones inalámbricas habilitamos la opción Wireless, ingresamos el SSID: RADIUS, seleccionamos el modo de compatibilidad de estándares ieee802.11, seleccionamos el canal 1. Finalmente para la configuración de seguridad aplicamos la seguridad WPA, seleccionamos el modo de cifrado TKIP o AES e ingresamos la contraseña.

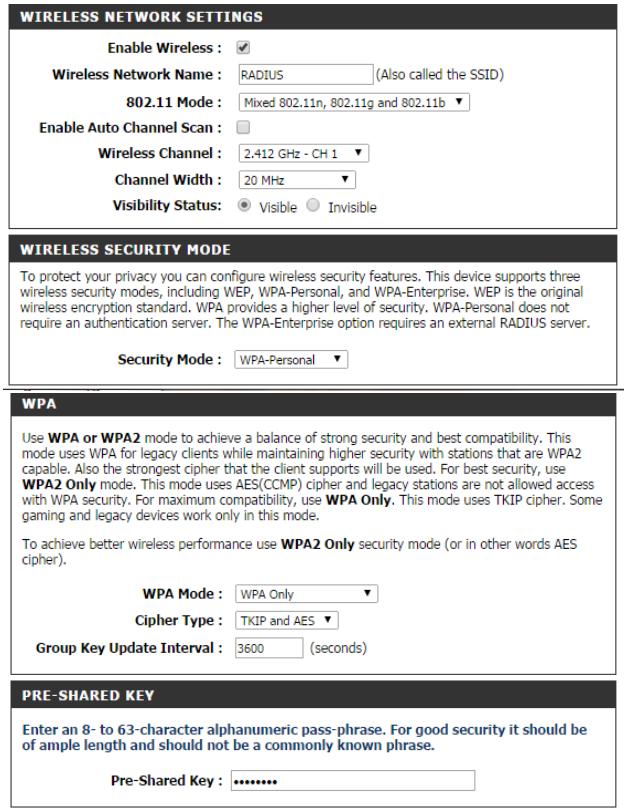


Figura 4-26 Configuración AP1.

Ya configurado los parámetros inalámbricos hemos seleccionado a este equipo para que actúe de servidor DHCP para los equipos de nuestra red y debemos asegurar que la ip a ser utilizada por nuestro equipo se mantenga fija por lo cual la ip 192.168.0.1 será exclusiva para el servidor DHCP, este tipo de opciones se configuran desde el panel principal la opción NETWORK SETTINGS.

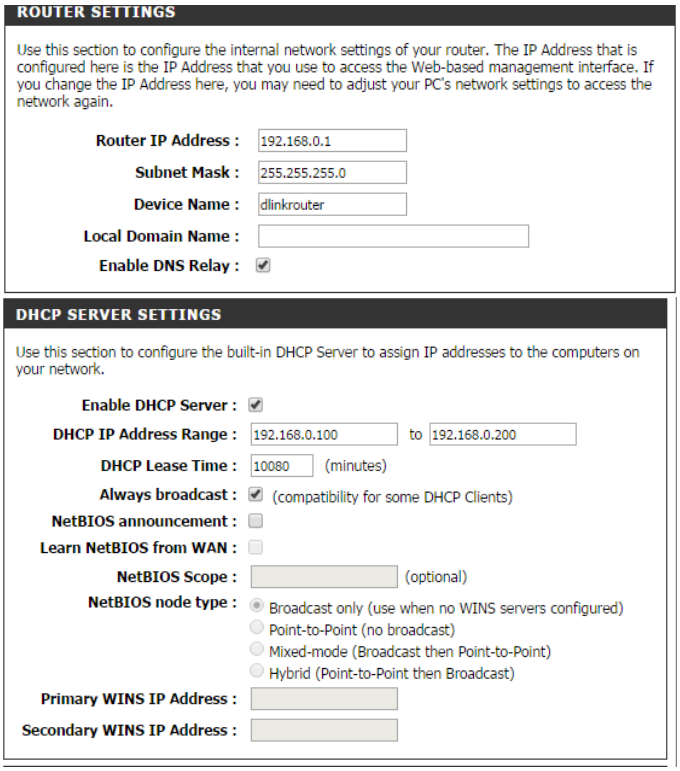


Figura 4-27 Configuración DHCP AP1.

Continuando con el procedimiento de configuración el equipo D-Link DIR-619L (AP3), se lo configura a través del panel de configuración web.

En el panel de configuración inalámbrica seleccionamos el modo de operación del equipo en Access Point, ingresamos el SSID: RADIUS correspondiente a nuestra WLAN, seleccionamos el canal 6 y habilitamos la seguridad WPA con cifrado Auto y algoritmo de autenticación PSK.

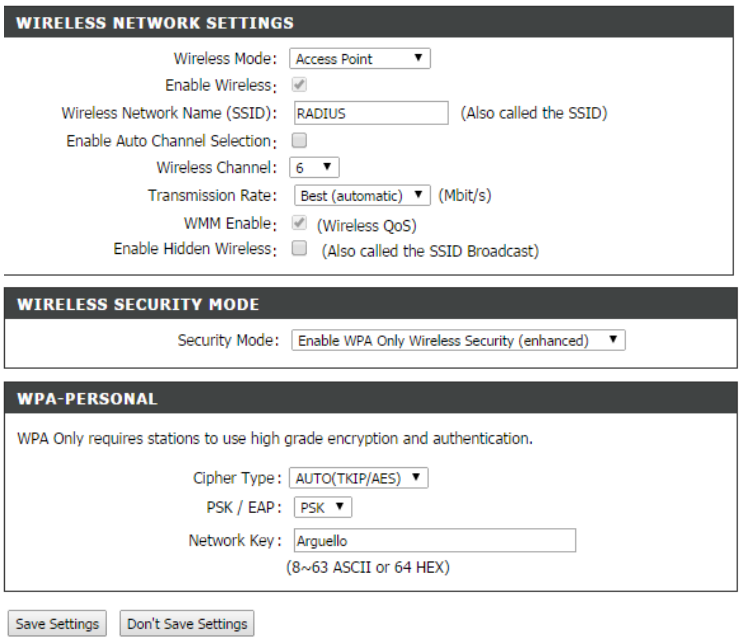


Figura 4-28 Configuración AP3.

Finalmente para el equipo dejamos configurado la Ip estática 192.168.0.2 ya que dicha IP no debe variar dentro del escenario y proporcionará conectividad entre los APs verificando de igual manera que el DHCP se encuentre desactivado para no causar inconvenientes dentro de nuestra red.

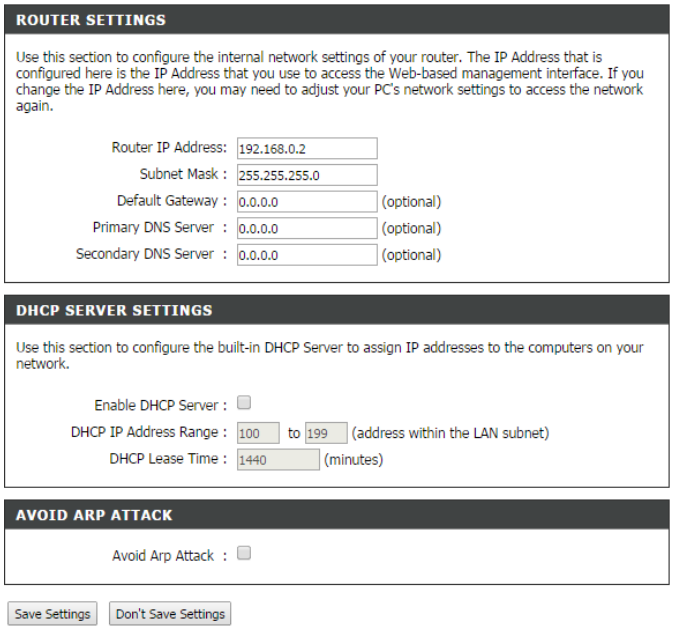


Figura 4-29 Configuración AP3.

Continuando en la configuración, para el equipo TP-Link TL-WR542G (AP2) ingresamos al panel de configuración vía web. Nos ubicamos en la opción Wireless y procedemos a configurar el SSID: RADIUS, seleccionamos el canal 11, el estándar 802.11g.

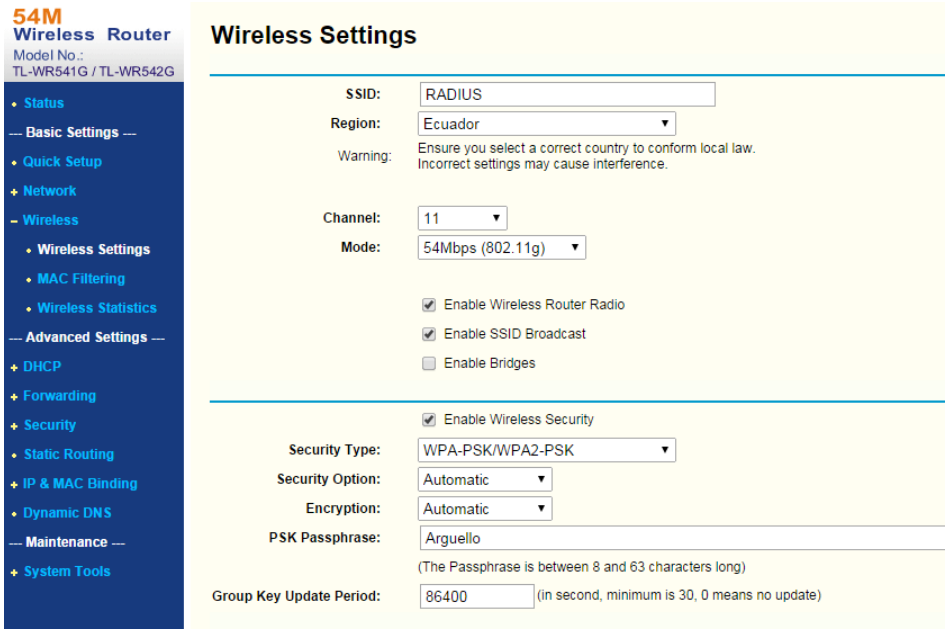


Figura 4-30 Configuración AP2.

Una vez configurado la parte inalámbrica verificamos que el equipo posea una IP estática diferente a los dos Access point restantes, por lo cual nos ingresamos en la opción Network LAN y se procede a fijar la IP a 192.168.0.3.

Figura 4-31 Configuración AP2.

Finalmente procedemos a desactivar la opción de DHCP para que el equipo pueda trabajar como punto de acceso en la red.

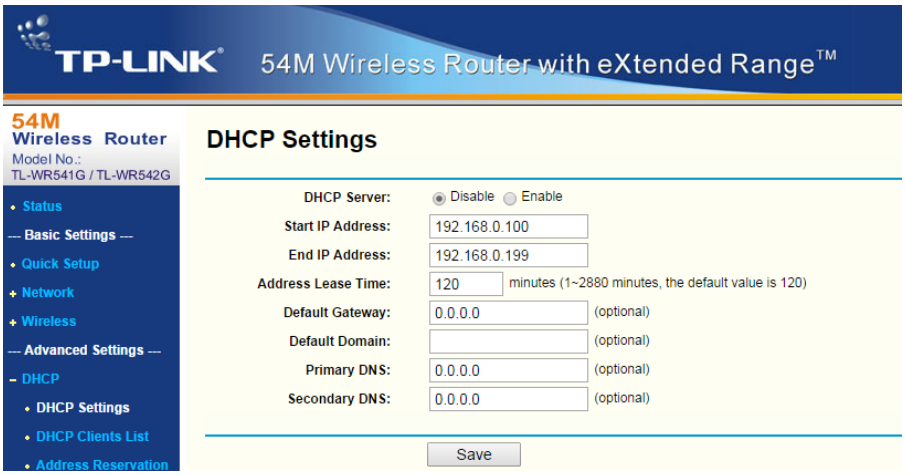


Figura 4-32 Configuración DHCP.

Configuración AirPcap

Una vez configurado los Access Point se configura en la estación Intel (STA1) los parámetros de captura de las tarjetas AirPcap para el monitoreo multicanal, cabe detallar que la opción de Capture Type: 802.11+Radio permitirá adicionar a las tramas capturadas, detalles físicos como radiofrecuencia, potencia, ruido y modulación.

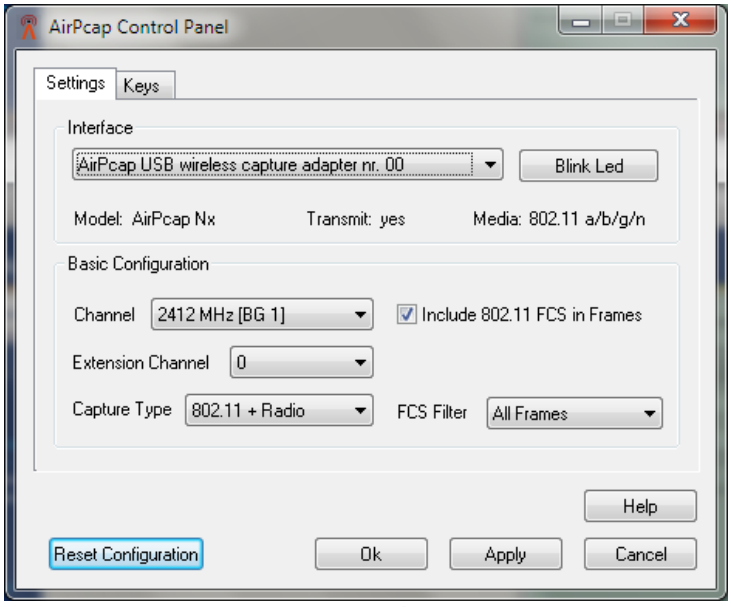


Figura 4-33 Configuración tarjeta AirPcap 1.

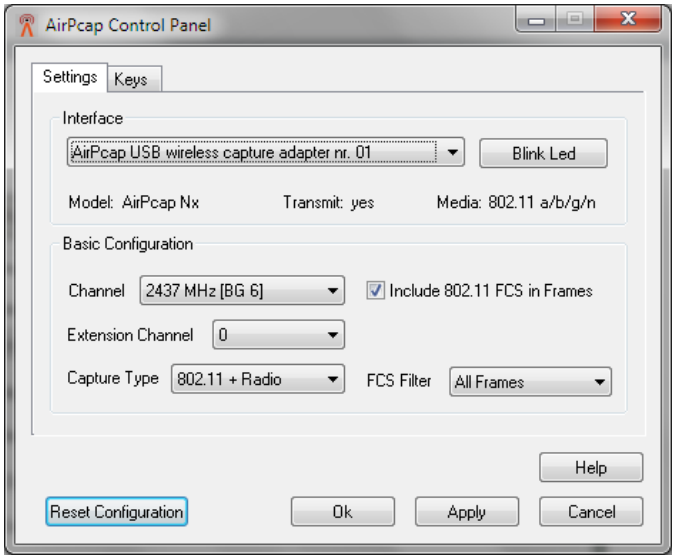


Figura 4-34 Configuración tarjeta AirPcap 2.

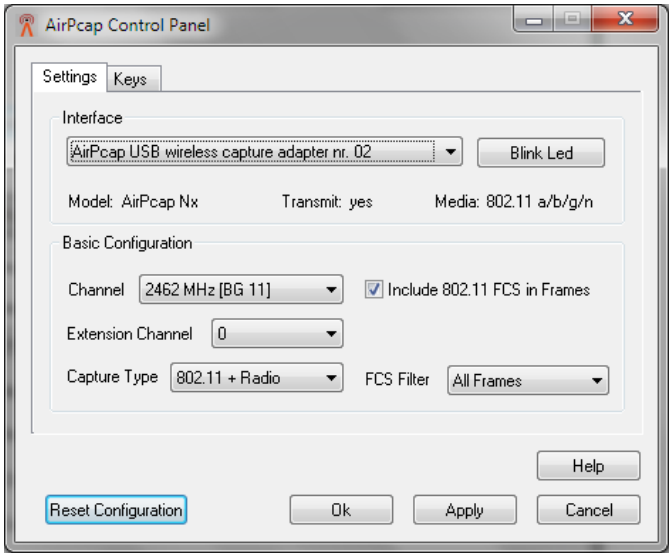


Figura 4-35 Configuración tarjeta AirPcap 3.

Configuración D-ITG.

Una vez configurado las tarjetas de captura los equipos presentan instalados en máquinas virtuales con Ubuntu 12.04 LTS el programa D-ITG para verificar estadísticas de tráfico como Bitrate, Delay, Jitter y Packetloss los cuales son de importancia para evaluación del rendimiento de red pero requiere que disponga sincronismo entre el emisor y receptor para que no exista variación en los resultados lo cual se lo consigue mediante un servidor NTP que en este caso es local y se encuentra instalado en la estación Intel. Para lograr el sincronismo la IP del servidor debe mantenerse constante en

el servidor por lo cual se procede a verificar la IP asignado a la estación Intel.

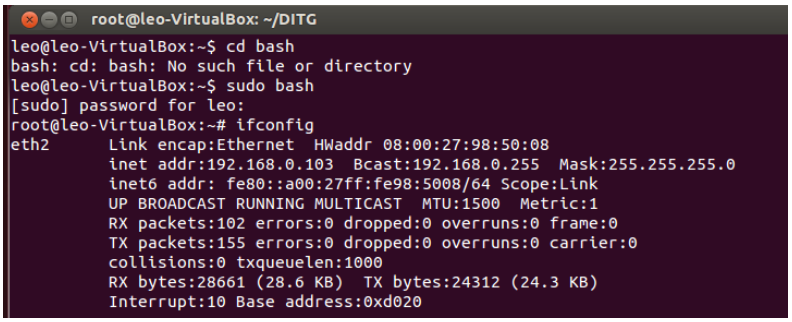


Figura 4-36 Interface Ubuntu D-ITG.

Como se puede verificar en la figura anterior la IP asignada es 192.168.0.103 de la interfaz Eth2, dicha interfaz se asocia mediante bridge a la interfaz física WLAN de la estación Intel. Una vez verificada la IP que nos servirá para sincronizar al cliente procedemos a verificar que el servidor NTP local se mantenga levantado para lo cual utilizamos desde la Shell de Ubuntu el comando NTPQ.

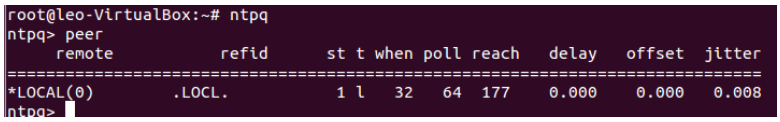


Figura 4-37 Configuración Servidor NTP.

La figura anterior muestra que se encuentra levantado el servidor NTP y lo muestra mediante *LOCAL.

A continuación para sincronizar la estación Intel con su cliente la estación Acer se debe tomar en cuenta que el servidor NTP dentro de una máquina virtual debe sincronizar de igual forma al sistema operativo sobre el que se encuentra en este caso es Windows 7. Para lograr sincronizar una máquina con Windows 7 se debe configurar el reloj, por lo cual damos clic en la pestaña donde se encuentre mostrada la hora y se presiona sobre Cambiar la configuración de fecha y hora. Inmediatamente nos aparece una ventana sobre la cual nos dirigimos en la pestaña Hora de Internet y seleccionamos el botón Cambar la configuración; aquí nos aparecerá una

nueva ventana sobre la cual se coloca la dirección IP del servidor NTP y se sincroniza al presionar el botón Actualizar ahora.

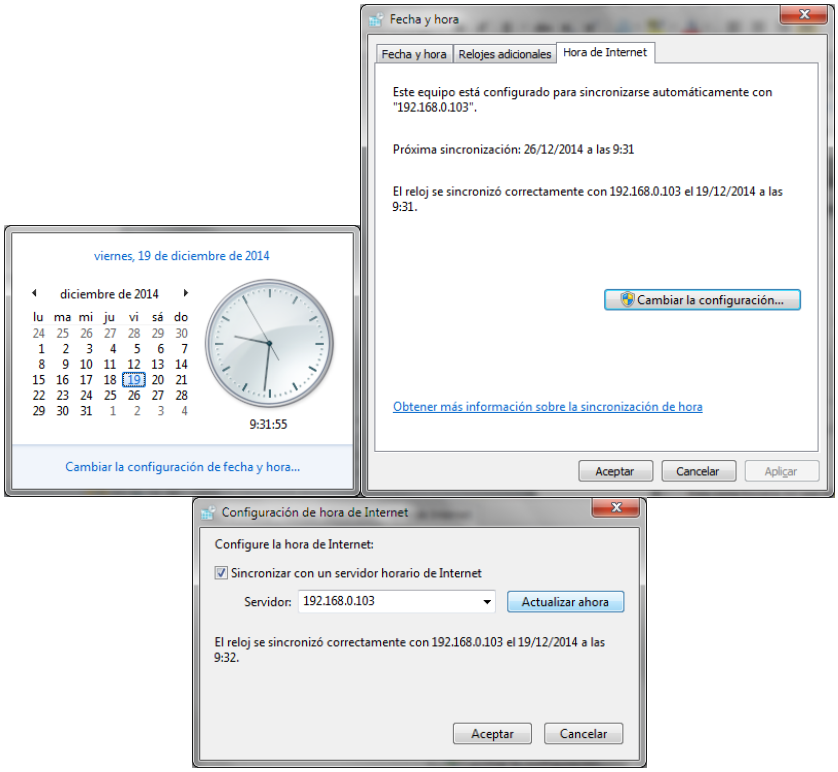


Figura 4-38 Configuración NTP en STA.

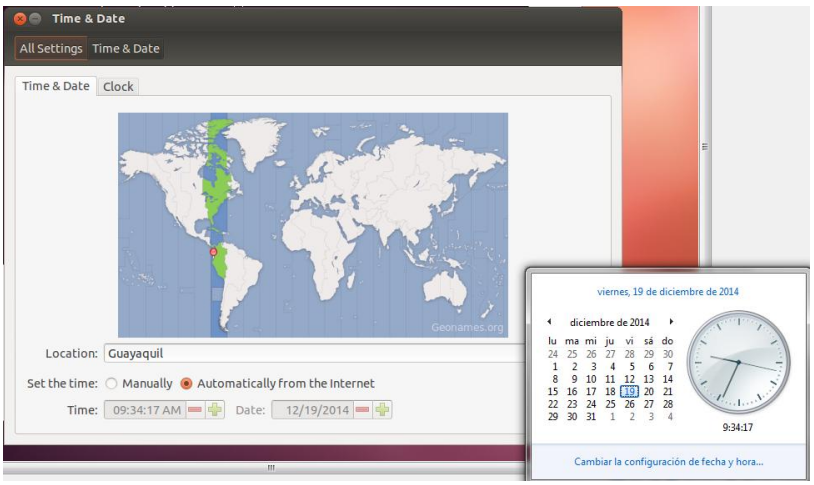


Figura 4-39 Verificación de Hora.

Para verificar que los host virtual y físico se encuentran sincronizados, se verifica la hora en ambos host fijándose específicamente en el segundero.

Ya sincronizado la estación Intel procedemos al cliente (estación Acer) la misma que debe ser configurada primero su host físico y posteriormente el

host virtual. La estación Acer de igual manera corre una máquina virtual Ubuntu 12.04LTS instalada sobre VirtualBox de windows7.

Para configurar el cliente en Ubuntu se abre la terminal Shell de comandos únicamente se utiliza el cliente NTP para Ubuntu mediante el comando ntpdate.

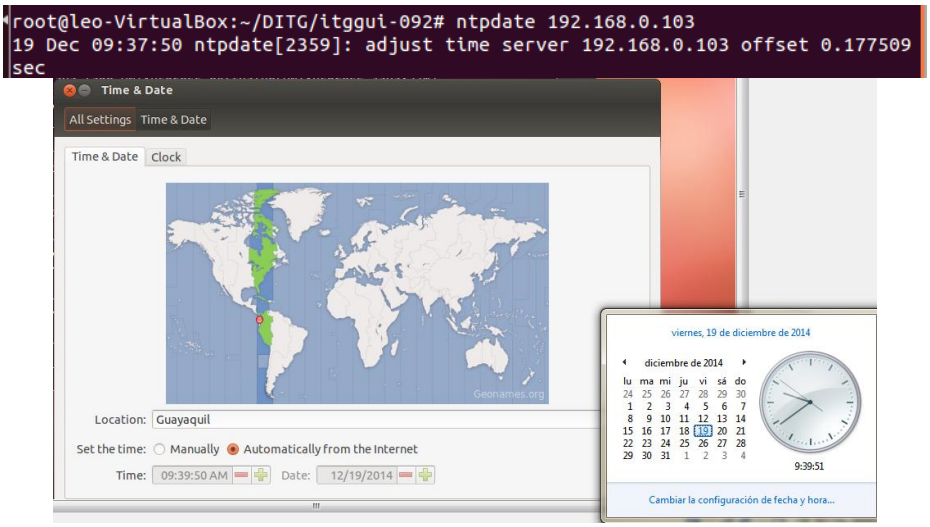


Figura 4-40 Configuración NTP Ubuntu.

Ya sincronizados tanto el cliente como el servidor NTP se puede proceder con el análisis de tráfico desde DITG lo cual se detallara en la sección de Análisis. Adicionalmente, para el proceso de tráfico se requerirá la IP del cliente así como del servidor de Ubuntu la cual se despliega a través de comando Ifconfig y se deberá verificar la IP asignada sobre la interfaz eth2 conectada a la interfaz inalámbrica del host físico configurada en VirtualBox.

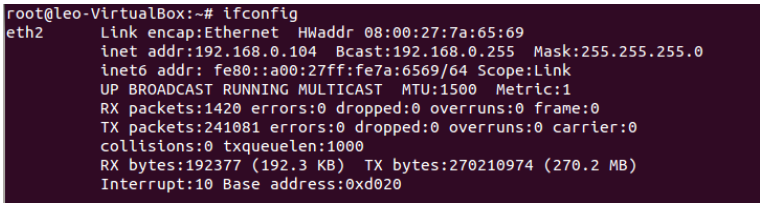


Figura 4-41 Ifconfig Ubuntu.

En el escenario el equipo Intel (STA1) actúa como monitor de red y como servidor DITG para el análisis de tráfico y se tiene implementado en cada Access Point la seguridad WPA con método de autenticación

Como primer paso se procede a verificar el uso de los canales inalámbricos mediante el programa inSSIDer.

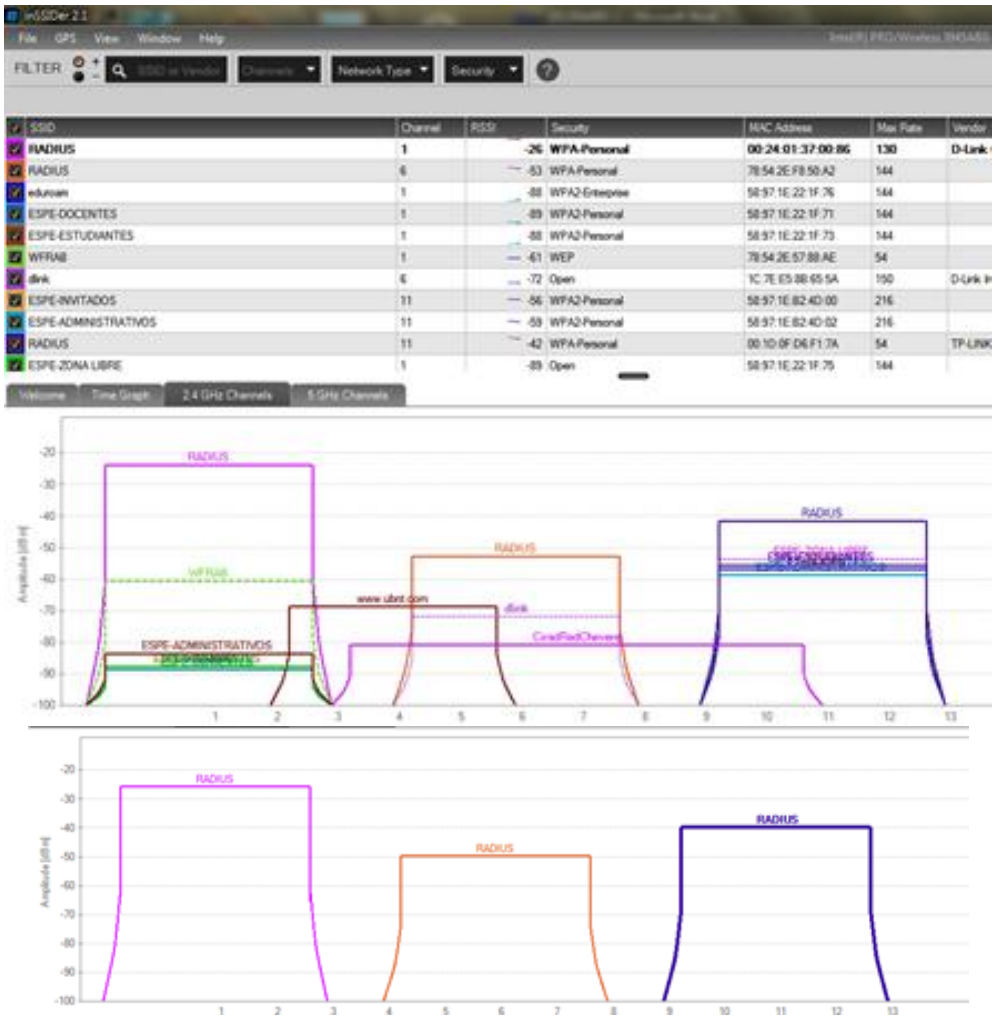


Figura 4-42 Configuración canales AP Escenario 3.

En este escenario se verifica la existencia de varias redes inalámbricas tanto solapadas como de co-canal a diferentes potencias pero el detalle importante de nuestra red RADIUS es poder verificar que cada punto de acceso configurado se encuentra operando en canales no solapados. Adicionalmente se muestra los niveles de cada punto de acceso medido desde la estación Intel, estos niveles se muestran en base a las tarjetas de

red de cada estación por lo cual veremos diferente intensidad de señal si la misma red es verificada desde la estación Acer (STA2) ya que dicha estación se ubica más cerca al Punto de Acceso D-Link DIR-619L (AP3).

Tabla 26 Configuración Canal APs.

SSID	RSSI (dBm)	Channel
RADIUS AP1	-26	1
RADIUS AP2	-53	6
RADISU AP3	-42	11

Para comprobar gráficamente los niveles de señal medidos desde la estación Acer se realizó la captura de datos desde InSSIDer.

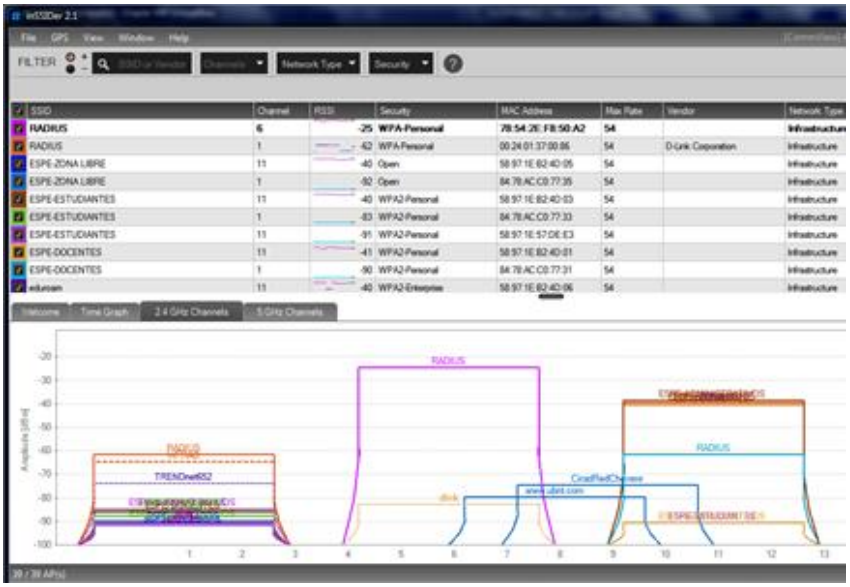


Figura 4-43 Configuración APs.

De la gráfica anterior se puede verificar efectivamente que la señal varió dando como respuesta que el Punto de Acceso D-Link es el que posee mayor intensidad de señal y al mismo que se encuentra conectada inicialmente la estación Acer.

Una vez verificado los canales y la intensidad de señal de los mismos, el siguiente paso es verificar cual es el comportamiento de red ante la presencia de gran cantidad de tráfico por lo cual a través del programa D-

ITG procedemos con la generación del mismo y mediante Wireshark la captura de tramas.

Para la implementación de monitoreo multicanal Wireshark presenta en su nueva versión la selección individual o colectiva de interfaces de red como una forma mejorada de monitoreo de interfaces; por otro lado AirPcap al disponer varias tarjetas genera una interfaz virtual conocida como Multi-Channel Aggregator que asimila ser una interfaz por la cual se recibe todo el tráfico de red monitoreado por cada tarjeta AirPcap individual y de modo que Wireshark pueda identificarla como una interfaz independiente.

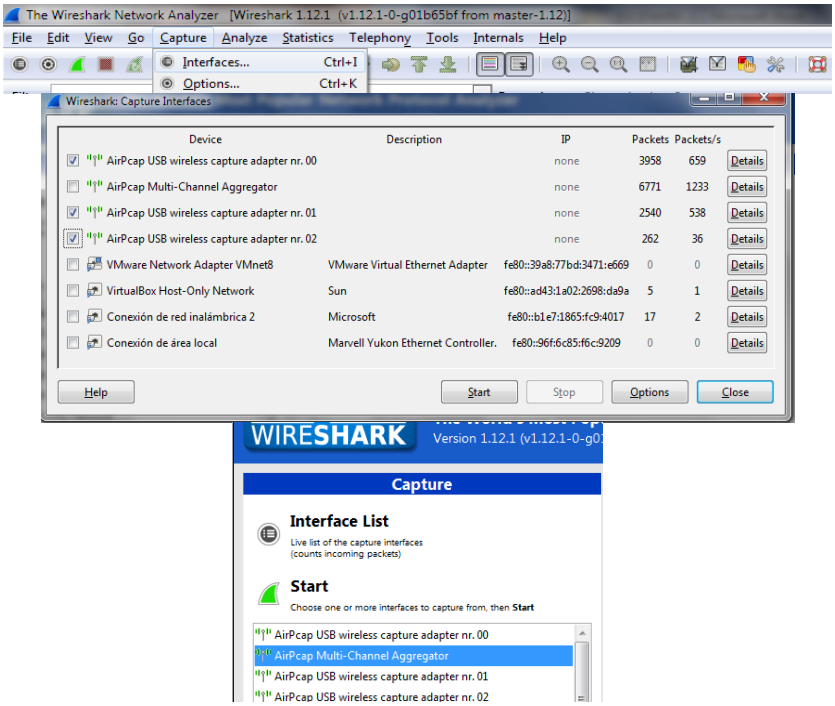


Figura 4-44 Selección de Tarjeta Virtual.

Para el monitoreo multicanal se optó por la selección de la interfaz virtual AirPcap Multi-Channel Aggregator.

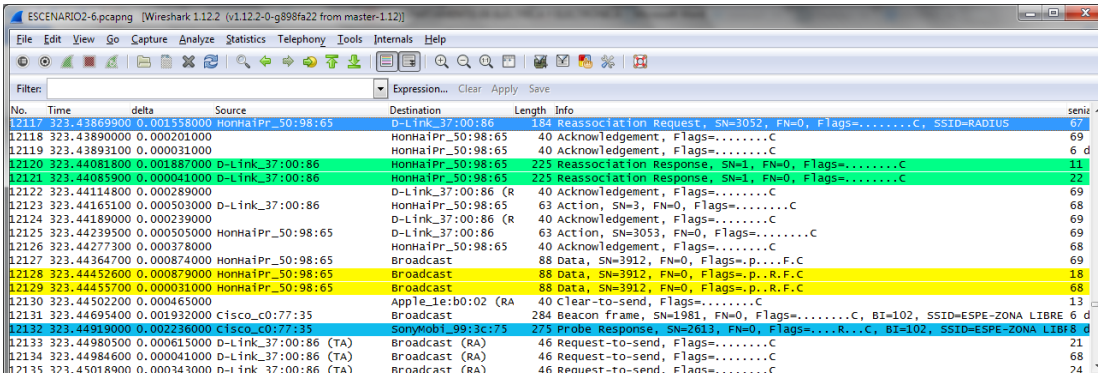


Figura 4-45 Captura de Paquete en Wireshark.

Para poder configurar DITG se debe tomar en cuenta que las estaciones deberán mantenerse sincronizadas dentro de la red ya que si se muestran retardos los datos pueden resultar incorrectos. Adicionalmente se debe considerar que los resultados pueden ser variables ya que no se trabaja con D-ITG instalado directamente en un host físico sino a través de máquinas virtuales instaladas en cada estación. Teniendo en cuenta dichos detalles se procede con el proceso de generación de tráfico.

Lo primero en efectuar para el envío de tráfico es el sincronismo entre servidor y cliente. Posteriormente en la estación Intel se procede a levantar el servidor DITG el cual deberá registrar el tráfico receptado en un archivo el cual contendrá las estadísticas al finalizar el envío de tráfico. Para dar apertura al programa en Ubuntu se utiliza el comando java –jar ITGUI.jar el cual mostrará la interfaz gráfica del programa. En nuestro escenario se ha efectuado una serie de pruebas en las cuales lo único a considerarse es el cambio del nombre del archivo de registros que se muestra en la pestaña Settings ya que de no efectuarse el mismo el archivo será reescrito.

```
root@leo-VirtualBox:~/DITG/itggui-092# java -jar ITGGUI.jar
```

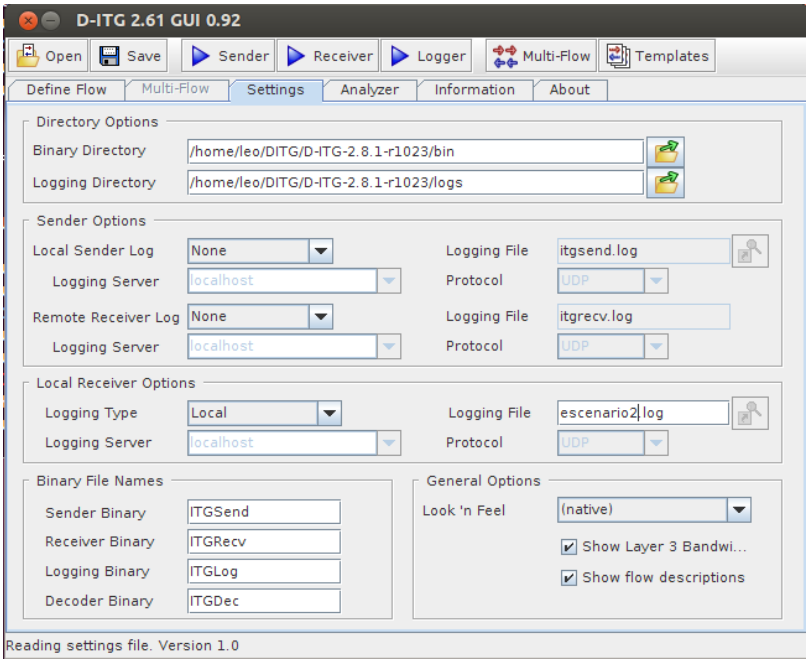


Figura 4-46 Modo gráfico D-ITG Servidor.

Del lado del cliente la configuración del emisor se efectúa en base al administrador según el tipo de tráfico que desea evaluar ya que D-ITG dispone varias opciones de tipo de tráfico para que sea enviados; en nuestro caso al ser un escenario mayormente relativo al comportamiento de los paquetes ieee802.11 se consideró conveniente proporcionar tráfico UDP constante que son los más usados para envío de tráfico de voz y video. Una de las características que proporciona la interfaz gráfica de D-ITG es que muestra el ancho de banda a obtener mediante la modificación de parámetros como Number y Size. Para el escenario y los siguientes escenarios a evaluarse se proponen el envío de un tráfico de 8224kb/s. El tiempo que durará el tráfico es también de importancia y se seleccionó un tiempo de 5minutos para poder efectuar las pruebas de roaming entre cada punto de acceso con la estación Acer.

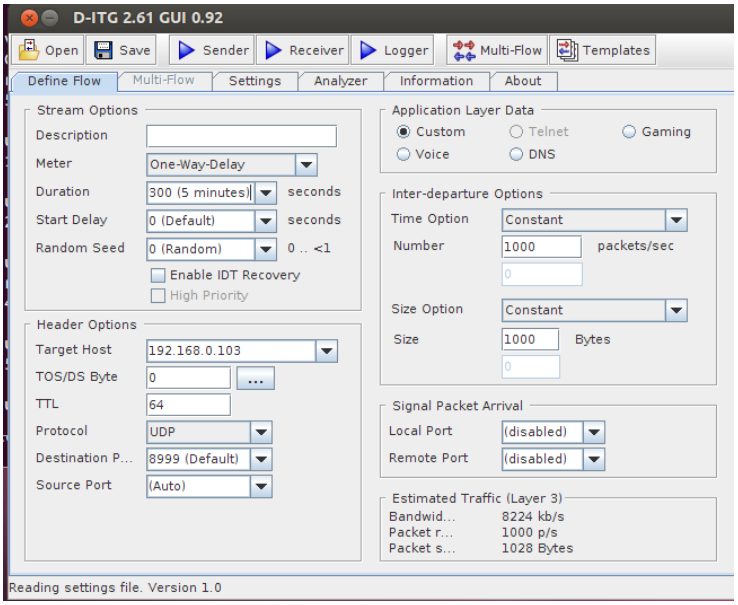


Figura 4-47 Configuración D-ITG.

Ya configurado el tráfico se procede a enviarlo, en el servidor se presiona el botón Receiver mientras que en el emisor se presiona el botón Sender; inmediatamente en cada equipo al dar clic en la pestaña Information mostrará el establecimiento de conexión entre el cliente y servidor DITG.

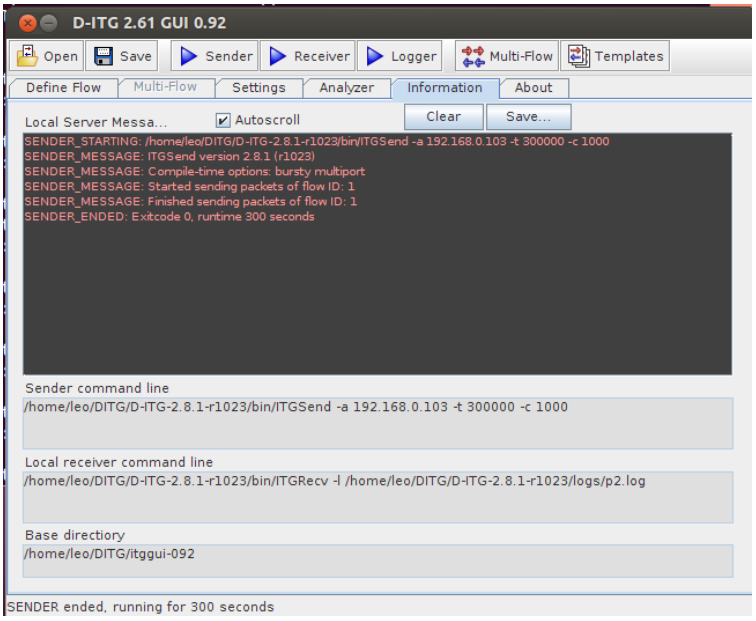


Figura 4-48 Conexión entre Servidor y Cliente D-ITG.

Para poder generar las estadísticas del escenario se utiliza ITGDec que es el encargado de codificar los datos para obtener las estadísticas del

escenario. Hay que tomar en cuenta que el archivo de registro generado desde la captura debe ser copiado hacia la carpeta bin que se encuentra dentro del fichero donde fue instalado D-ITG, una vez con el archivo copiado desde el terminal de comandos de Ubuntu se ubica en la carpeta y se aplica el comando ITGDec

Comando: *root/DITG/bin: **./**ITGDec "nombre del archivo de registro de datos" –b 500 –j 500 –d 500 –p 500*

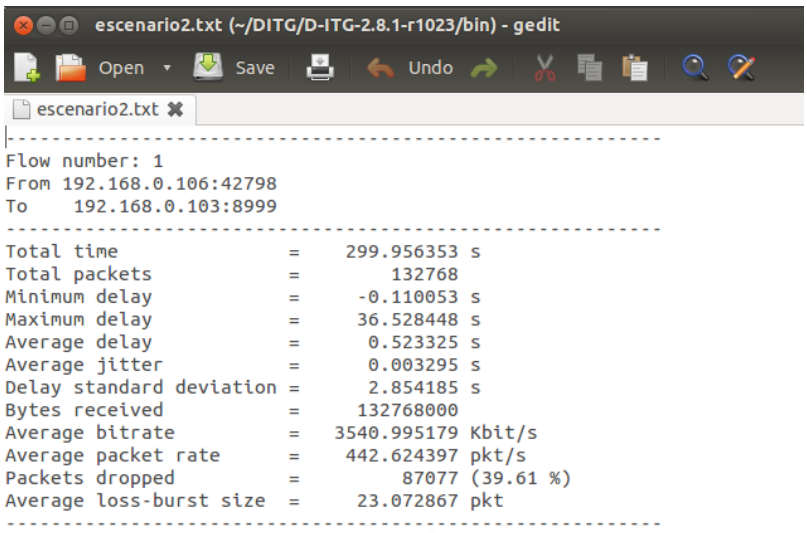


Figura 4-49 Visualización resultados D-ITG.

Para el escenario se realizó un total de 5 pruebas las mismas que se presentan registradas en la siguiente tabla.

Tabla 27 Resultado de Pruebas Escenario 2.

Prueba	Paquetes	Bitrate (Kb/s)	Delay (ms)	Jitter (ms)	Packetloss (%)
1	132768	3540,99	523,35	3,295	39,61%
2	179788	5996,45	96,79	2	14,51%
3	19900	513,80	6840	16,35	90,52
4	127000	3371,39	1441	3,2	38,70%
5	185841	4952,33	127	2,1	9,17%

De lo verificado en la tabla los resultados varían mucho tomando en cuenta que se tuvo como referencia un ancho de banda de 8Mbps y ninguna de las pruebas se muestra sin pérdidas esto debido principalmente a la

cantidad de redes presentes en el escenario y el proceso de movimiento de la estación cliente por lo cual al realizar la comparación entre los datos obtenidos y el tráfico inicial se verifica que la prueba 2 y 5 dan una perspectiva real del comportamiento de la red es decir el rendimiento de la red es de 61,9% en la prueba 5 y 74,95% en la prueba 1; estas cifras son realizadas en base al Bitrate conseguido considerando a 8Mbps como 100%.

Se debe considerar que en D-ITG se puede generar las gráficas de los parámetros principales como Bitrate, Jitter, Delay y Packetloss, esto de igual manera se realiza una vez generado los archivos del mismo nombre a través del comando ./ITGDec, Posteriormente los archivos son copiados a la carpeta ITGPlot del fichero donde se encuentra instalado D-ITG. Finalmente a través de la consola de comandos se ubica en la carpeta y se procede a graficar los archivos.

Commando: *root/DITG/src/ITGPlot#. /ITGPlot bitrate*

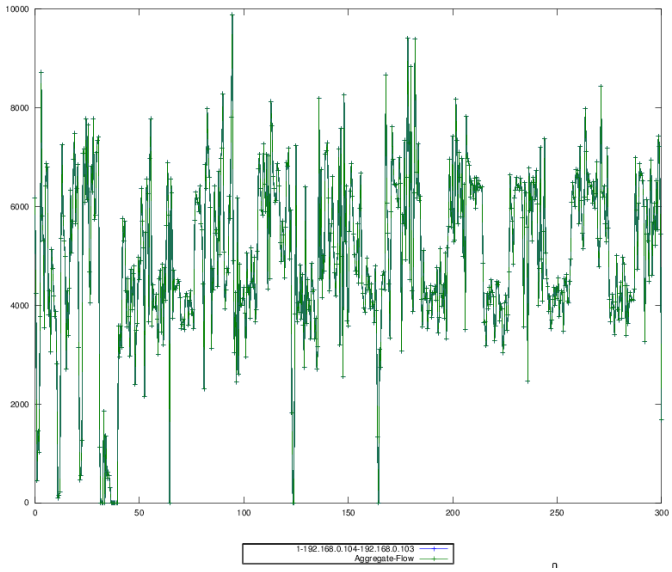


Figura 4-50 Gráfica de Bitrate.

En el gráfico anterior se verifica que la cantidad de datos transferidos o Bitrate es muy irregular y se ve que alrededor de 4200 paquetes se envían por cada segundo.

Commando: *root/DITG/src/ITGPlot#. /ITGPlot delay*

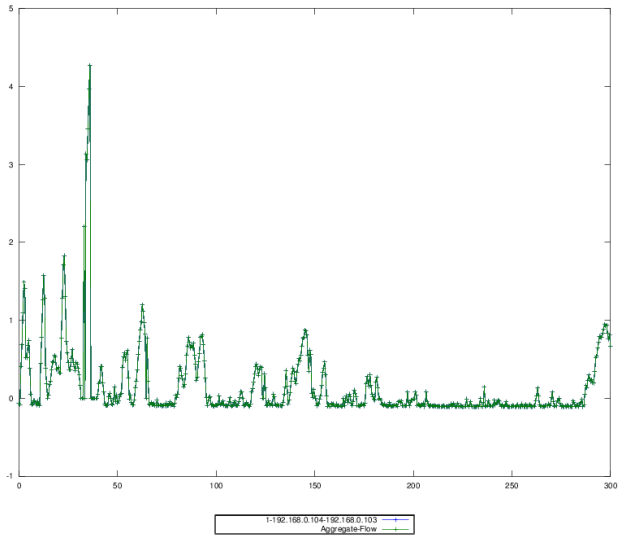


Figura 4-51 Delay Escenario 2.

El retraso en el presente escenario se ve de igual manera variable durante la transferencia de los datos verificándose un pico aproximadamente a 35s de tráfico.

Comando: *root/DITG/src/ITGPlot#. /ITGPlot jitter*

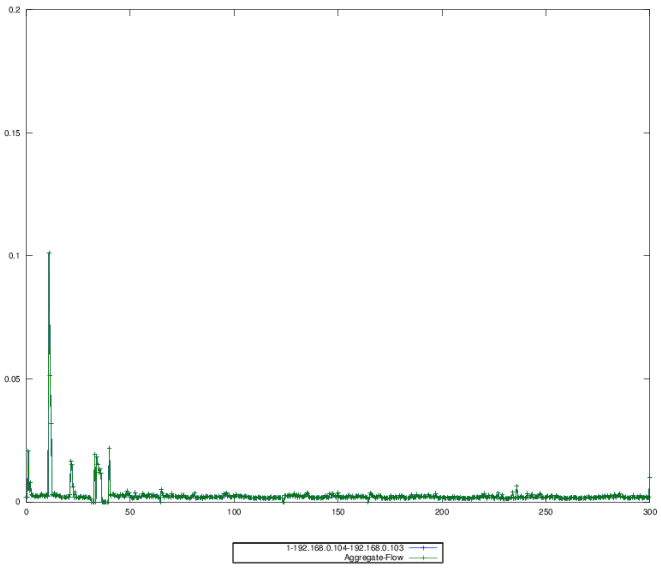


Figura 4-52 Jitter Escenario 2.

El jitter del escenario se verifica en los primeros 50s que existe la mayor variación que puede ocurrir por congestión de la red o pérdida de sincronización. Aquí se verifica un jitter de 1ms a los 10s.

Comando: *root/DITG/src/ITGPlot#. /ITGPlot Packetloss*

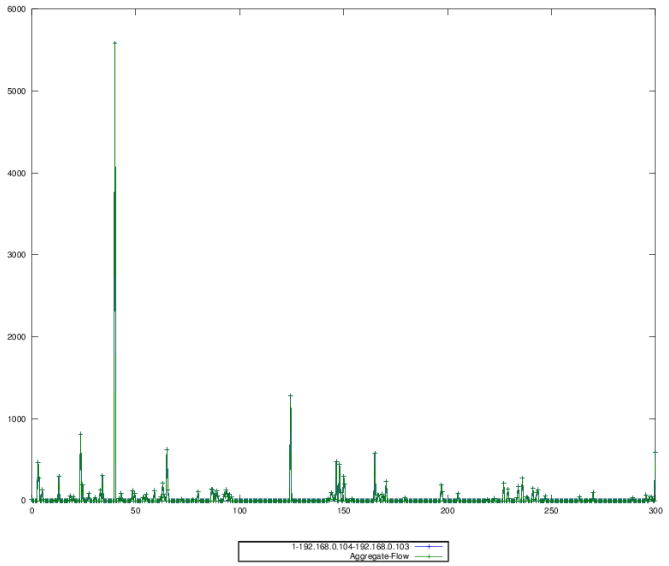


Figura 4-53 Packetloss.

Finalmente Packetloss nos confirma que el escenario presenta una baja pérdida de paquetes mostrándose un pico de 5700 paquetes a los 45s.

Como se conoce en Wireshark se puede verificar el tráfico de red en torno al tipo de trama requerido y los equipos a evaluarse.

La ventaja más importante del monitoreo multicanal implementado en este escenario es que nos permite verificar el tráfico de los equipos configurados en canales diferentes y obtener un detalle de como estaciones y puntos de acceso se comportan al mostrarse configurados en canales no solapados como el 1, 6 y 11.

Filtro1: *wlan.addr eq 78:54:2E:F8:50:A2 and wlan.fc.type_subtype eq 8*

Filtro2: *wlan.addr eq 00:1D:0F:D6:F1:7A and wlan.fc.type_subtype eq 8*

Filtro3: *wlan.addr eq 00:24:01:37:00:86 and wlan.fc.type_subtype eq 8*

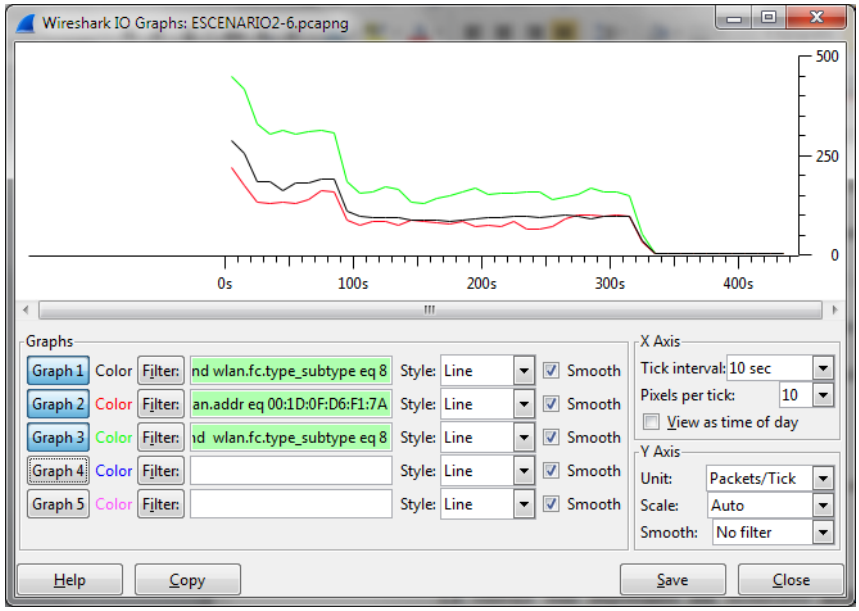


Figura 4-54 Tramas Beacon AP Escenario 2.

La gráfica anterior muestra el comportamiento de las tramas beacon generadas desde los APs, se verifica que durante los primeros 100s de monitorización se presentan mayor cantidad de tramas tipo beacon a diferencia de los 200s posteriores en los que se ve una estabilización de tramas a un promedio de 70 tramas para AP3; 70 tramas para AP2 y 130 tramas para AP1.

Adicionalmente para verificar la transferencia de datos entre STA1 y STA2 de igual manera podemos aplicar filtros y visualizar el comportamiento del tráfico.

Filtro: *wlan.sa eq 38:59:f9:50:98:65 and wlan.da eq 00:1b:77:f3:a2:dc*

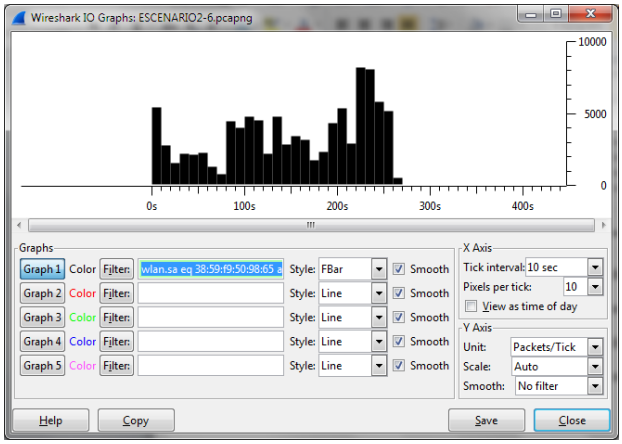


Figura 4-55 Transferencia de Datos entre STA1 y STA2.

Finalmente para mostrar un análisis general del comportamiento de la red utilizamos el programa SteelCentral Packet Analyzer que presenta estadísticas en base al tráfico capturado.

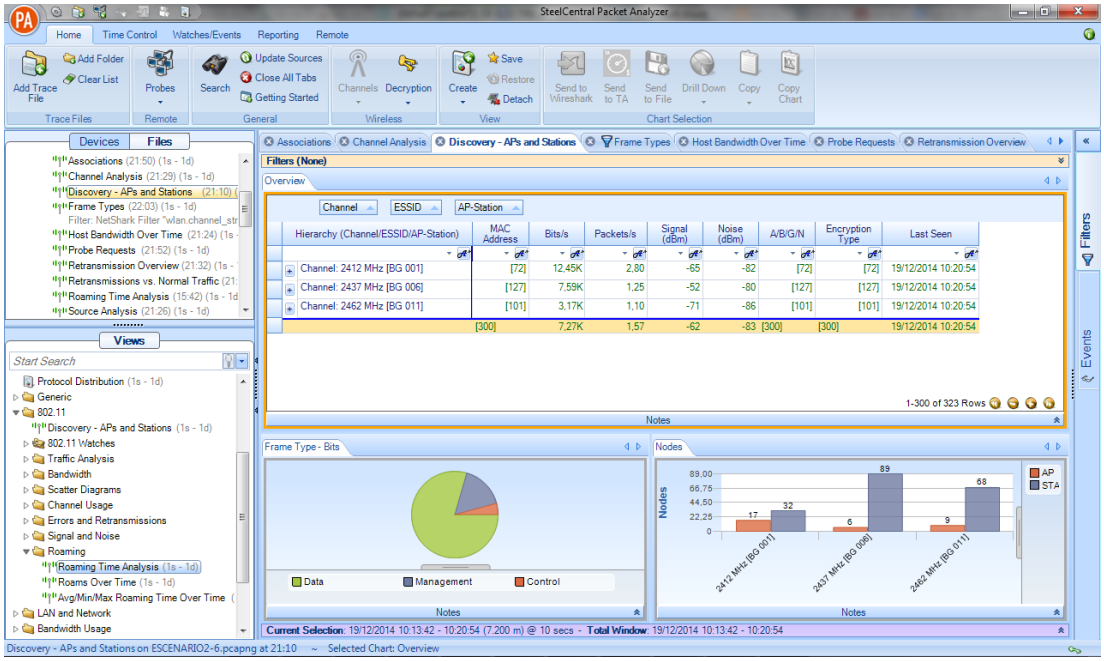


Figura 4-56 Estadísticas Escenario 2.

Para los administradores de red las características del programa hacen que se convierta en una herramienta altamente efectiva para análisis de tráfico IEEE802.11 ya que permite verificar información relevante como la cantidad de tráfico retransmitido, cantidad de tráfico según el tipo de trama, uso del canal que presenta en base a la cantidad de dispositivos presentes entre otras.

Para el uso de la herramienta lo que podemos efectuar es la importación del archivo a ser analizado a través de la pestaña Home y selección de Add Trace File.

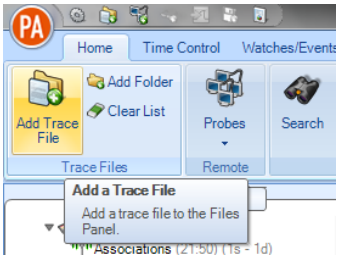


Figura 4-57 Importación de Archivo .pcap

Se selecciona el archivo a ser analizado

Posteriormente nos mostrara en la ventana izquierda superior del programa los archivos seleccionados

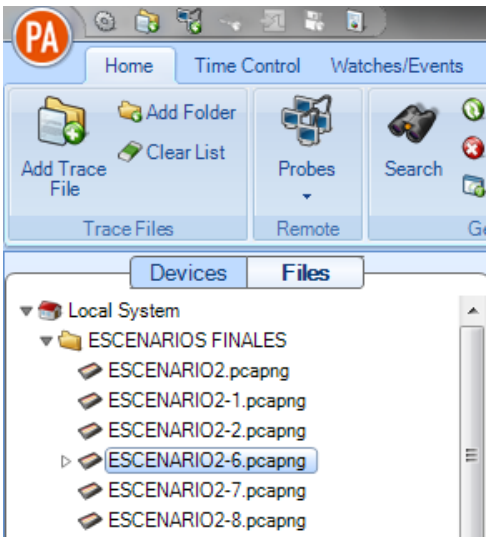


Figura 4-58 .pcap de los Escenarios capturados.

Para procesar la información en la ventana inferior izquierda del programa se muestran las opciones que pueden ser seleccionadas para el análisis de tráfico inalámbrico.

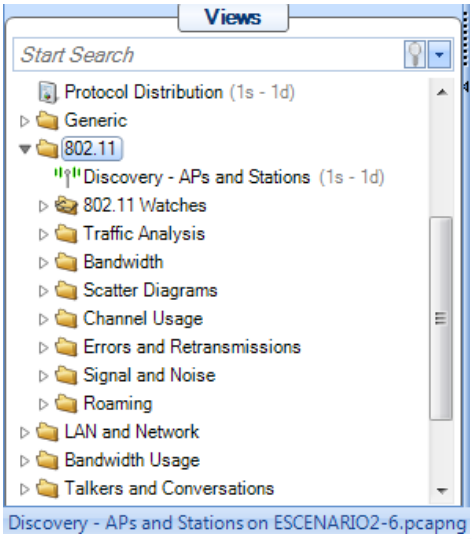


Figura 4-59 Opciones de selección.

Al seleccionar las opciones disponibles se mostraran ventanas de procesamiento de los archivos en la ventana derecha.

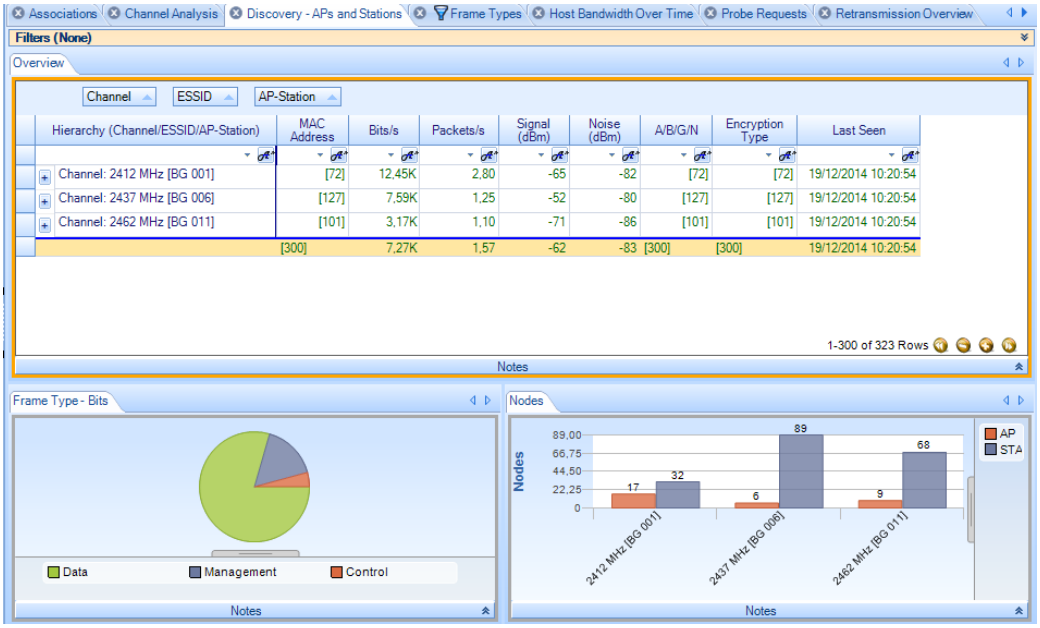


Figura 4-60 Detalle de visualización.

Cada opción seleccionada nos aparecerá inmediatamente en la ventana donde se muestran los archivos a analizarse.

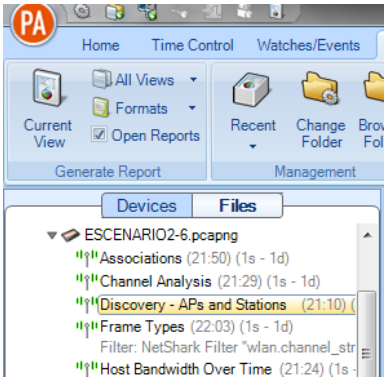


Figura 4-61 Visualización de Opciones en Escenario.

Finalmente las opciones de reportes nos permitirán registrar los datos analizados y los cuales pueden exportarse en 6 tipos de formatos.

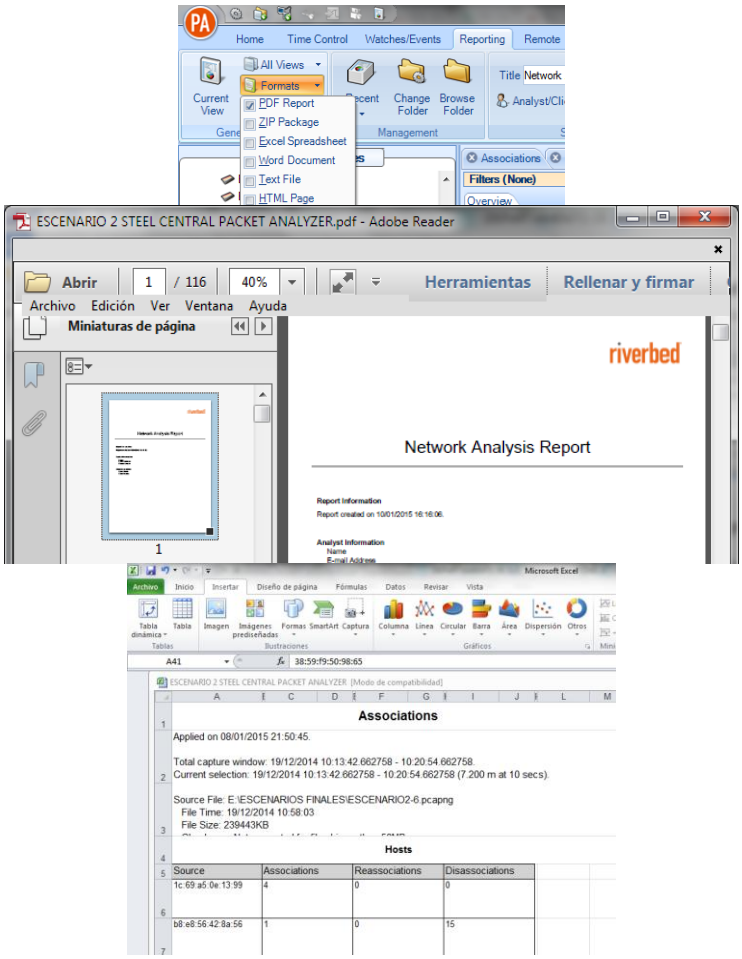


Figura 4-62 Reportaría en diferentes Formatos.

Para continuar con el análisis se consideró gráficos estadísticos y tablas importantes.

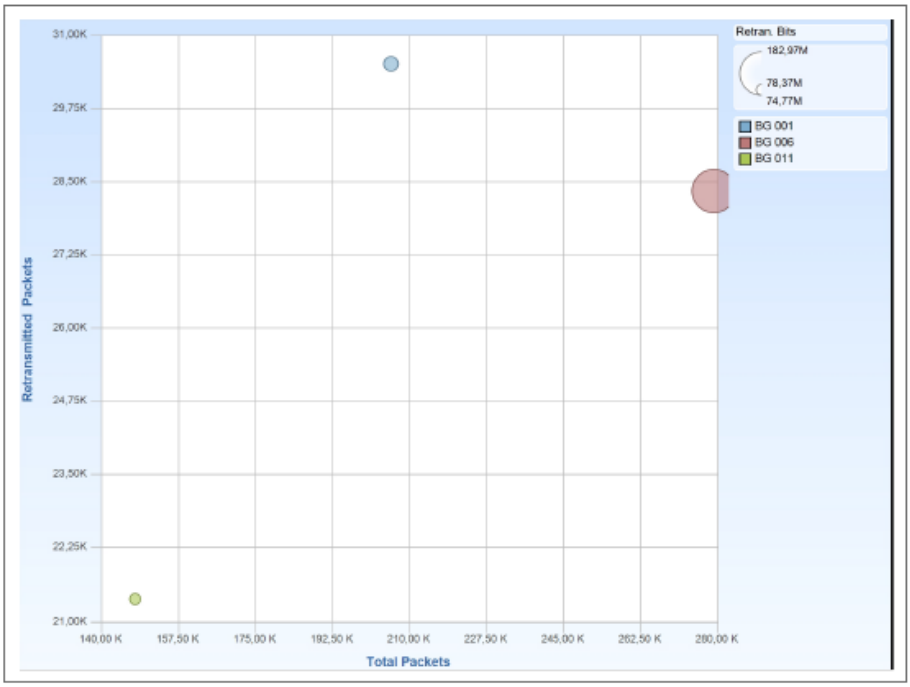


Figura 4-63 Retrasmisiones Vs. Paquetes por canal.

Tabla 28 Retransmisión Vs. Paquetes por canal.

Channel	Total Packets	Bits	Retran. Packets	Retran. Bits	Bytes
BG 001	205736	422988376	30517	110649208	52873547
BG 011	147609	282361896	21370	74766936	35295237
BG 006	279055	813551192	28343	182965616	101693899

La tabla precedente es una de las más importantes ya que muestra la cantidad de paquetes a nivel global por canal y cuantos paquetes en total fueron retransmitidos independientemente del tipo de paquete IEEE802.11. Para el escenario se verifica que el canal 1 correspondiente al AP1 D-Link DIR-615 es en el que se verifica mayor cantidad de retransmisiones en tanto que el AP3 modelo D-Link DIR-619L es en el que se verifica menor cantidad de retransmisiones.

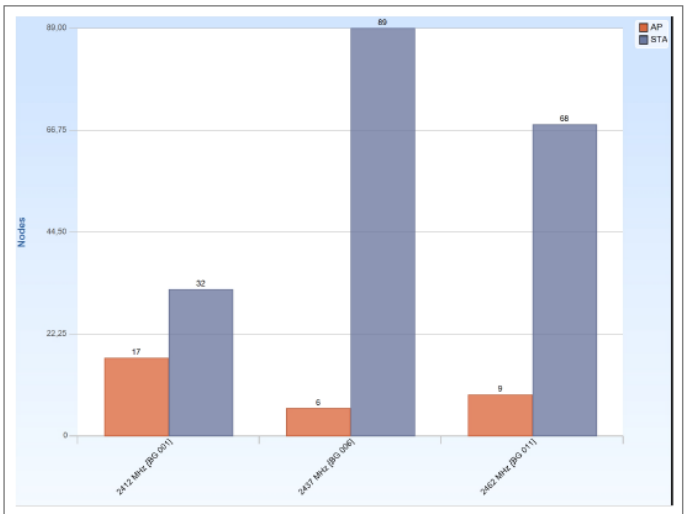


Figura 4-64 Nodos.

Por otro lado se verifica que en el ambiente global de red se determina la presencia de 80 estaciones operando en el canal 6, en tanto que la mayor cantidad de puntos de acceso se encuentran configurados en el canal 1 con un total de 17 puntos de acceso.

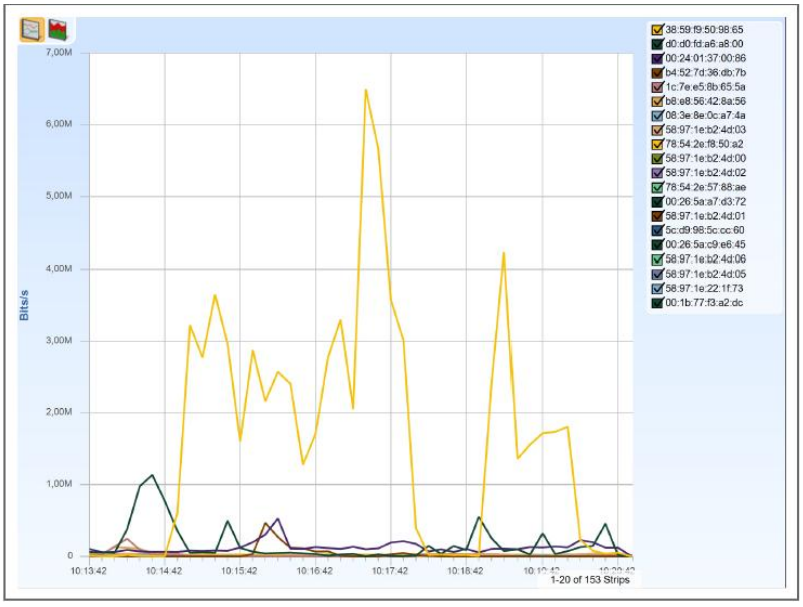


Figura 4-65 Tráfico de cada Host.

La estación STA2 es la que lleva la mayor cantidad de tráfico transmitido en la red verificándose un pico de aproximadamente 6,5Mbps

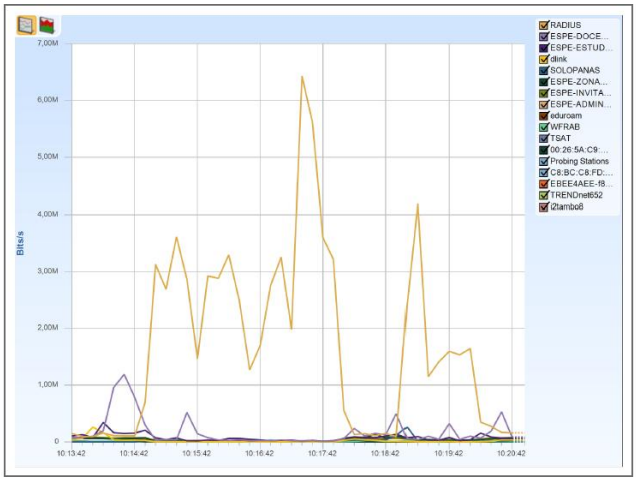


Figura 4-66 Tráfico de cada Red.

Del ambiente de red de igual manera se verifica que la mayor cantidad de tráfico de red se encuentra presente en el SSID RADIUS.

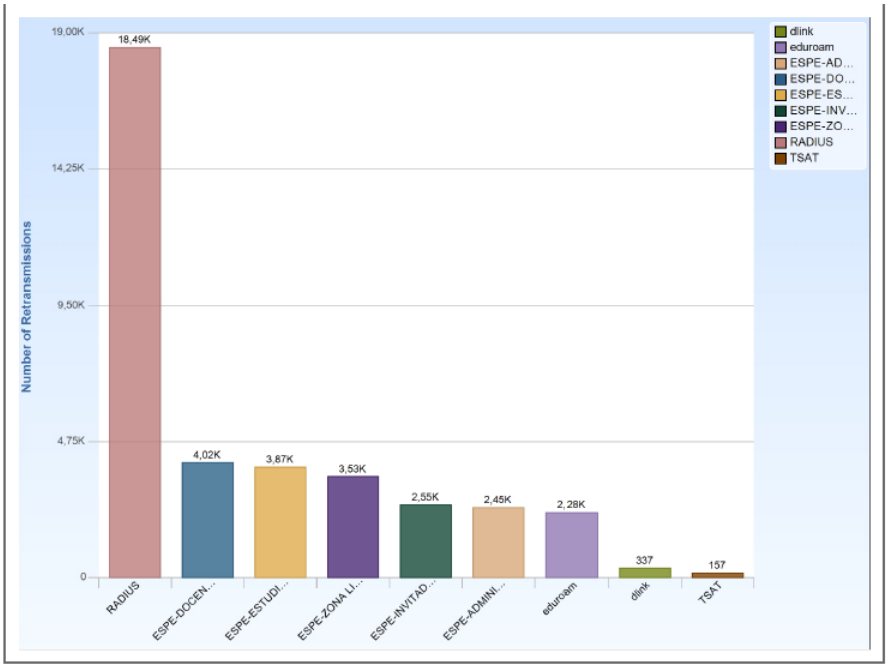


Figura 4-67 Retrasmisión por AP.

Tabla 29 Retrasmisión AP RADIUS.

Retransmissions by AP	
RADIUS	18494

De igual manera la mayor cantidad de retransmisiones se verifica en la red RADIUS.

Tabla 30 Asociaciones.

Networks			
Network	**Associations**	**Reassociation**	**Disassociations**
RADIUS	0	3	0

Nuestro escenario ùnicamente presenta 3 reasociaciones las mismas que como se verifico con el filtrado en wireshark corresponde a la estación STA2.

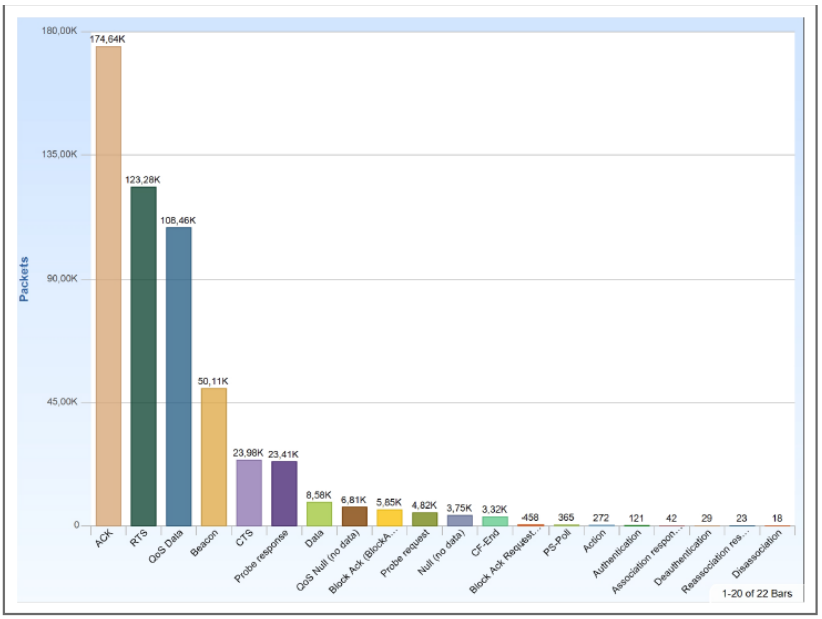


Figura 4-68 Ancho de Banda por Subtipo de paquetes.

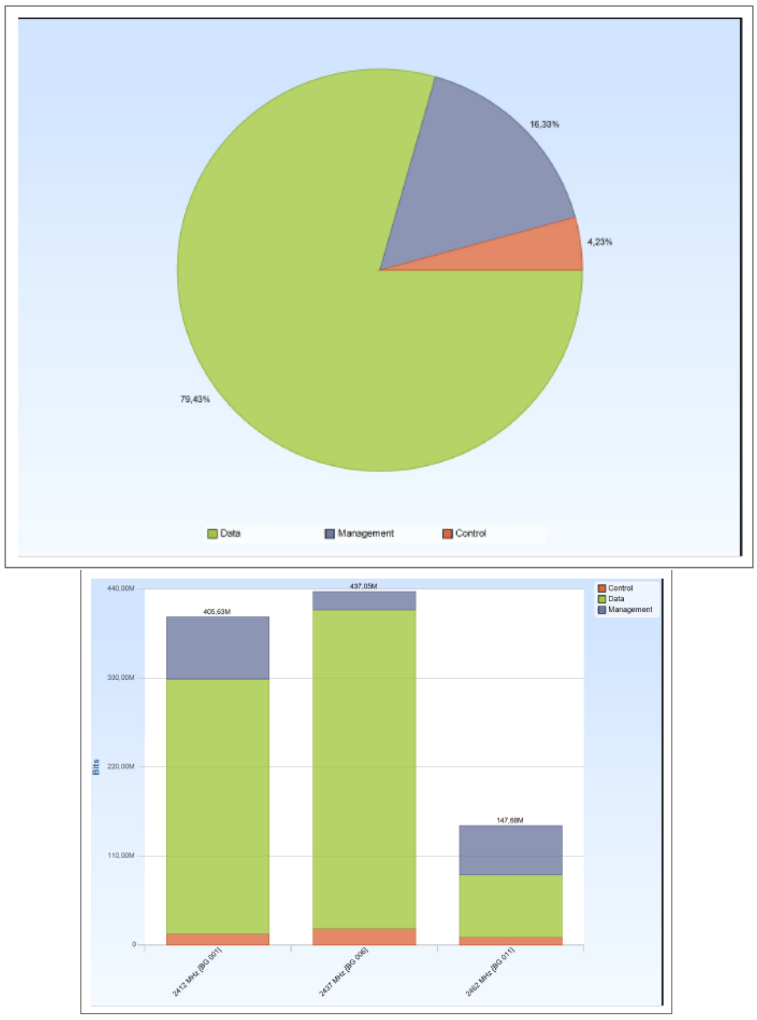


Figure 11 - Channel Type - Bits

Figura 4-69 Tipo de Frames.

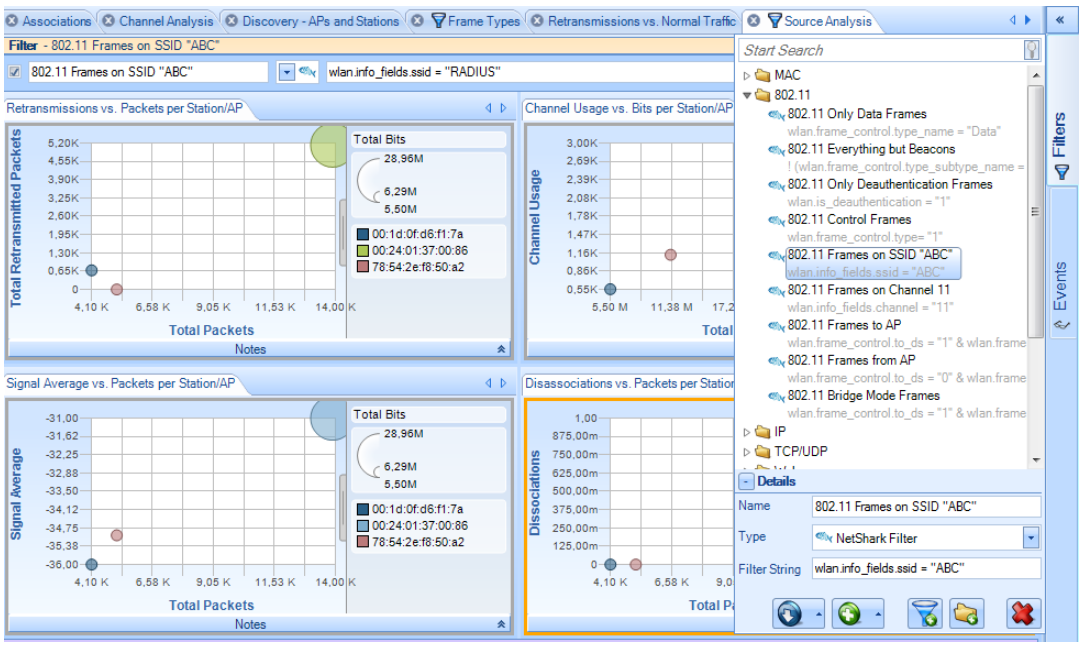
Independientemente de la cantidad de paquetes la cantidad de bits de datos es la mas alta dentro de la red. Esto puede ser confuso pero de hecho se valida que la mayor cantidad de paquetes son originados por tramas ACK las cuales tienen tamaño reducido de bits alrededor de 40bytes por trama ACK.

Tabla 31 Paquetes por tipo de Trama.

Channel Type - Packets	
2412 MHz [BG 001]-Control	100705
2412 MHz [BG 001]-Data	54929
2412 MHz [BG 001]-Management	37942
2437 MHz [BG 006]-Control	158944
2437 MHz [BG 006]-Data	57595
2437 MHz [BG 006]-Management	11111
2462 MHz [BG 011]-Control	72238
2462 MHz [BG 011]-Data	15072
2462 MHz [BG 011]-Management	29809

Con el fin de obtener a mayor detalle información global del comportamiento de nuestro escenario SteelCentral Packet Analyzer presenta la opción de Source análisis y filtros que son de gran ayuda para el análisis. Es así que una vez generados los procesos de la opción Source Analysis verificamos en la parte derecha de la ventana más grande la opción Filter la cual se aplica directamente sobre el proceso que se encuentra en análisis.

Filtro: *wlan.info_fields.ssid = "RADIUS"*



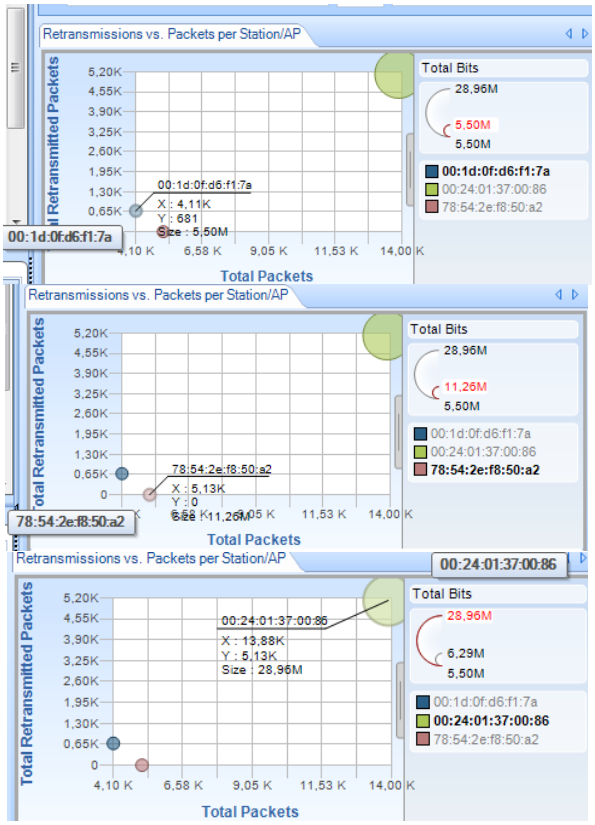


Figura 4-70 Filtro, Retransmisión Vs. Paquetes por AP.

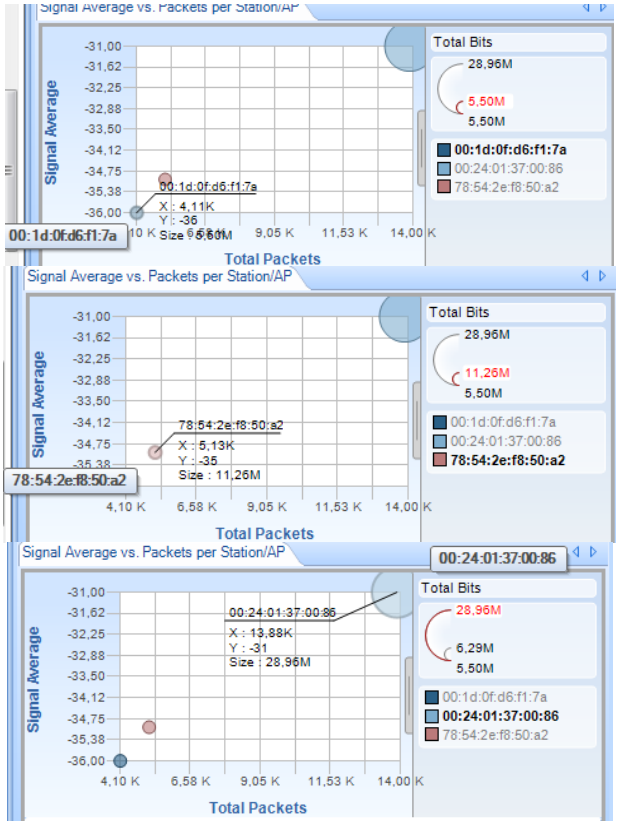


Figura 4-71 Filtro, Señal promedio Vs. Paquetes por AP.

Tabla 32 Resumen Señal y Retransmisiones.

RADIUS				
PUNTOS DE ACCESO	**TOTAL PACKET**	**TOTAL BITS**	**SIGNAL AVERAGE**	**RETRANSMISSION**
00:24:01:37:00:86 (AP1)	13880	28,95M	-31dBm	5130
00:1D:0F:D6:F1:7A (AP2)	4110	5,5M	-36dBm	681
78:54:2E:F8:50:A2 (AP3)	5130	11,26M	-35dBm	0

Como se puede verificar si enfocamos el análisis a los equipos de la red RADIUS podemos visualizar datos relevantes a través del programa Cace Pilot como el nivel de señal promedio, la cantidad de paquetes y la cantidad de retransmisiones generadas.

Como detalle importante las tarjetas AirPcap mediante la información de radiotap agregan información de parámetros físicos al configurar la opción de Capture Type en la cual fue seleccionada Radio.

De la parte teórica se conoce que AirPcap tiene tres tipos de formatos de capturas, Radio+802.11, PPI+802.11 y 802.11. Las dos primeras opciones muestran la misma información de parámetros físicos por lo cual se seleccionó la opción Radio+802.11 para el análisis de red.

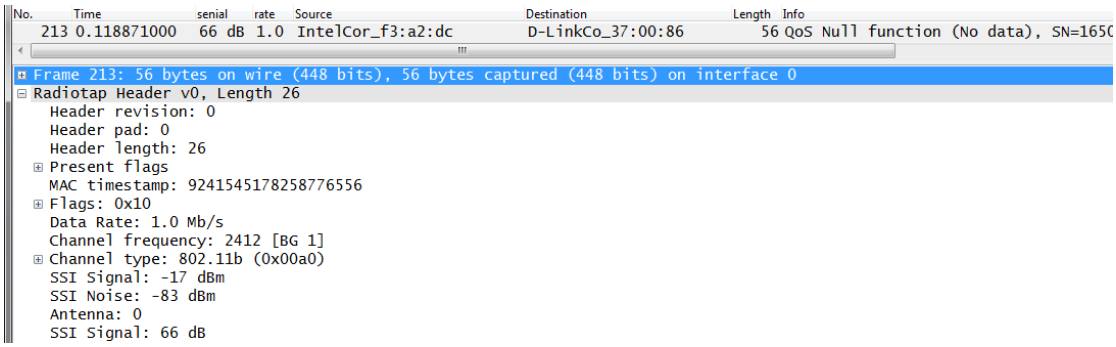


Figura 4-72 Información Radiotap

4.1.3. ESCENARIO 3

El escenario se encuentra conformado por dos Access point configurados en el canal 1 y canal 6 manteniendo la seguridad WPA y autenticación PSK.

El propósito de evaluación en este escenario es verificar la calidad de canal que muestra la red en base al análisis de las tramas IEEE802.11 y parámetros estadísticos obtenidos mediante la aplicación del programa DITG así como resultados de Steel Central Packet Analyzer.

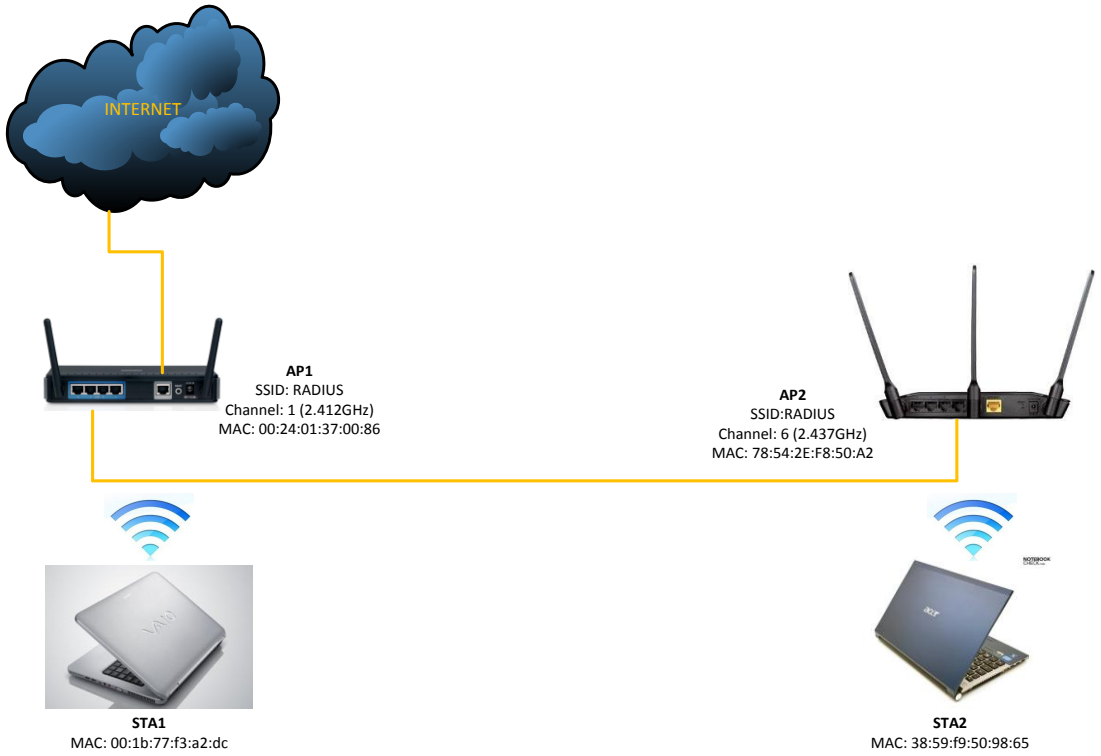


Figura 4-73 Esquema Escenario 3.

Tabla 33 Direccionamiento MAC Escenario 3.

Dispositivo	INTERFAZ	MAC	FUNCION
STA1	Intel	00:1B:77:F3:A2:DC	Estación
STA2	Acer	38:59:F9:50:98:65	Estación
AP1	Inalámbrica	00:24:01:37:00:86	Punto de Acceso
AP2	Inalámbrica	78:54:2E:F8:50:A2	Punto de Acceso

El escenario plantea como objetivo verificar el comportamiento de la red al disponer de dos puntos de acceso configurados en diferentes canales no

solapados tomando en cuenta que dos equipos de la red se mantienen transfiriendo datos. Para el análisis del ambiente de red procedemos a verificar mediante inSSIDer el uso de los canales.

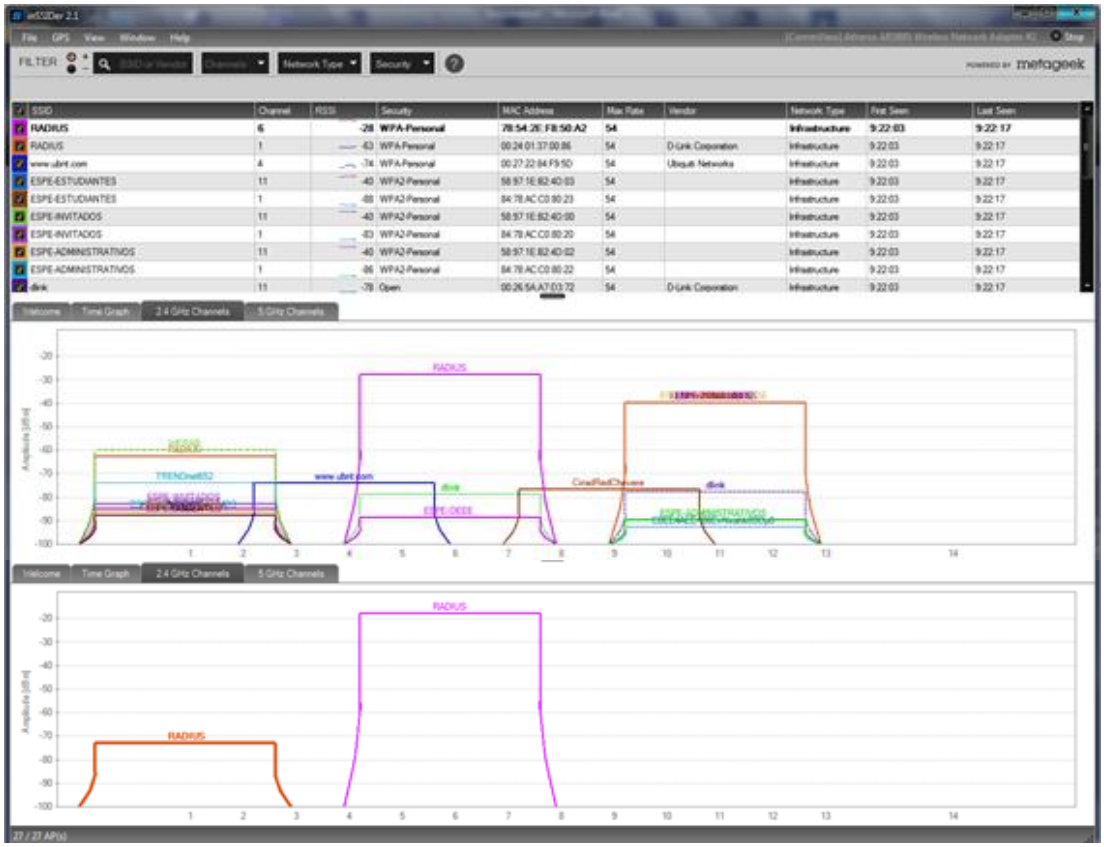


Figura 4-74 Configuración de Canales AP.

En la figura anterior podemos verificar la configuración de la red inalámbrica en los canales 1 y 6, los mismos que se muestran con gran cantidad de redes co-canal y solapadas que se mantiene con el uso de los canales, la captura se verifica realizada desde la estación Acer (STA2) y se verifica la red inalámbrica www.ubnt.com que solapa con gran intensidad de señal los canales 1y 6 lo que puede incurrir en un grado de pérdidas en la transmisión de datos entre STA1 y STA2.

Tabla 34 Configuración de los canales AP.

SSID	RSSI (dBm)	Channel
RADIUS AP1	-63	1
RADIUS AP2	-28	6
www.ubnt.com	-74	4

Ya verificado los canales procedemos a verificar el comportamiento de red ante la presencia de gran cantidad de tráfico por lo cual a través del programa D-ITG procedemos con la generación del mismo tomando en cuenta que Wireshark debe encontrase levantado y realizando capturas en modo multicanal.

Para el monitoreo multicanal se optó por la selección de la interfaz virtual AirPcap Multi-Channel Aggregator.

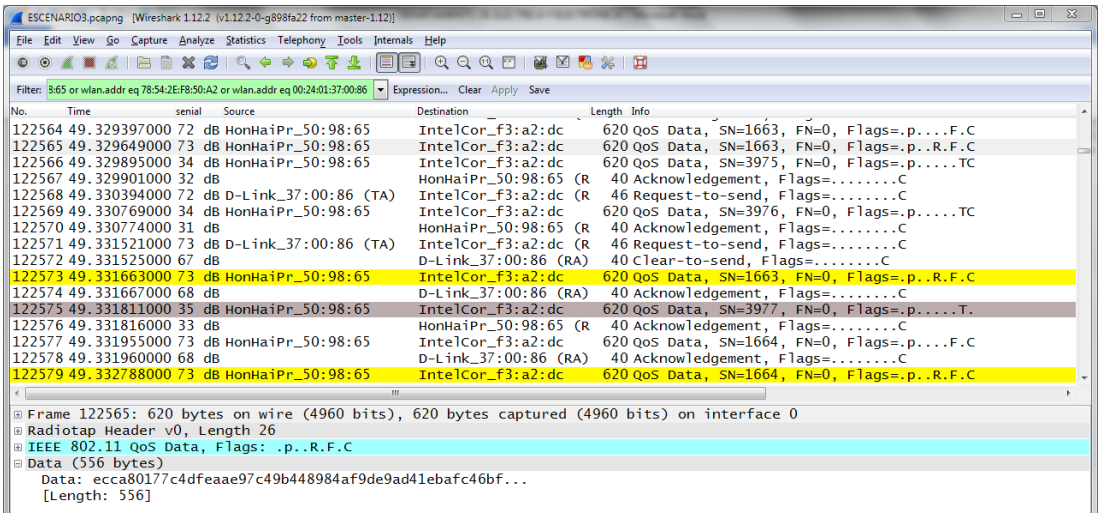


Figura 4-75 Captura de Paquetes en Wireshark.

Para levantar D-ITG tanto en transmisor como en receptor, sincronizamos el servidor NTP configurado en STA1 con la estación STA2. Una vez efectuado el proceso levantamos en STA1 el servidor DITG.

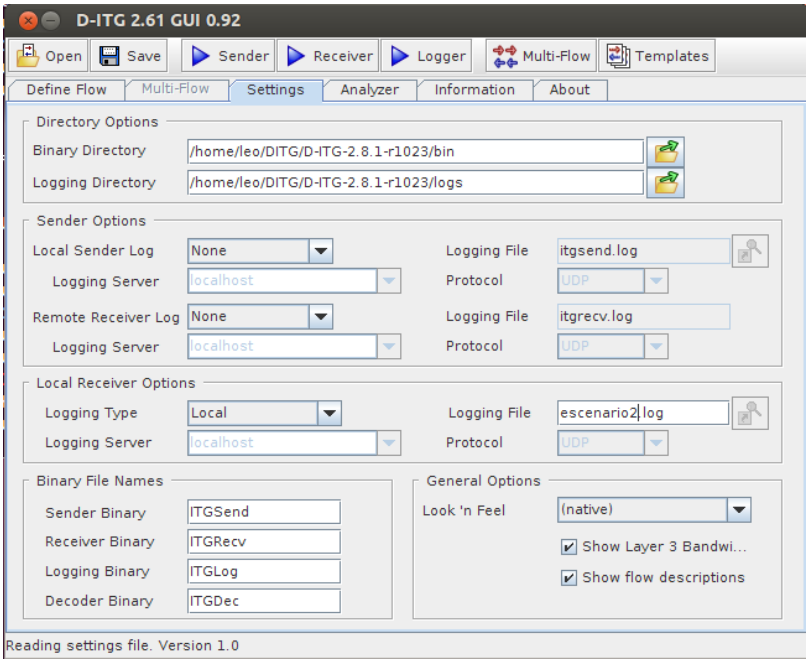


Figura 4-76 Configuración D-ITG Servidor.

Del lado del cliente se procede a configurar el envío de 8224kb/s de tráfico UDP constantes durante 1 minuto.

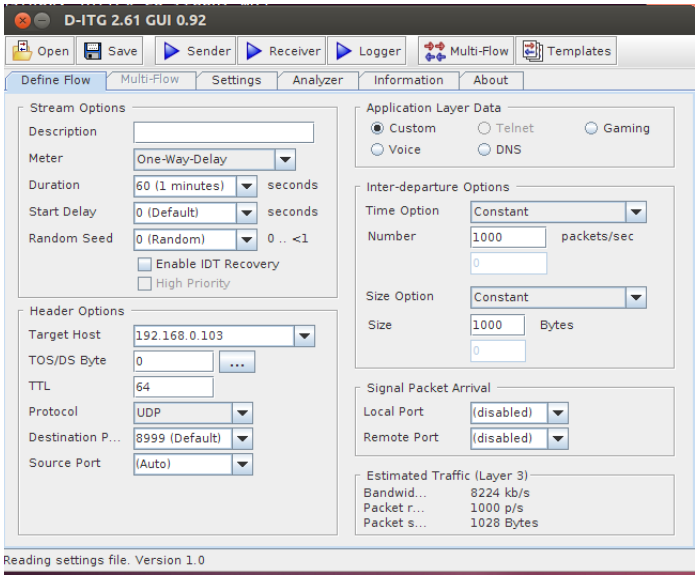


Figura 4-77 Configuración D-ITG Cliente.

Una vez enviado el tráfico se procede a generar las estadísticas del escenario.

Comando: *root/DITG/bin: /ITGDec "nombre del archivo de registro de datos" –b 500 –j 500 –d 500 –p 500*

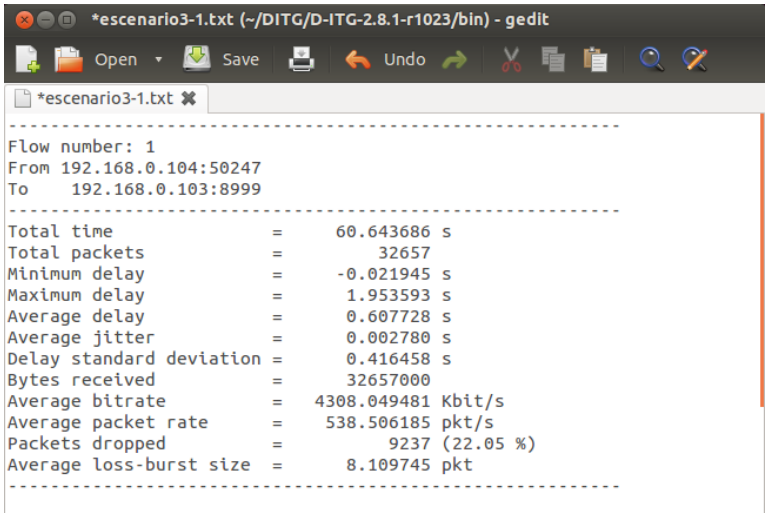


Figura 4-78 Resultado D-ITG.

Para el escenario se realizó un total de 3 pruebas las mismas que se presentan registradas en la siguiente tabla.

Tabla 35 Pruebas Escenario 3.

Prueba	Paquetes	Bitrate (Kb/s)	Delay (ms)	Jitter (ms)	Packetloss
1	32657	4308,05	607	2,7	22,05%
2	28651	3728,65	934	3,17	29,10%
3	30974	4057,51	710	2,79	25,53%
Media	30760,67	4031,4	750,3	2,89	25,56%

En las pruebas realizadas se verifica una constante pérdida de paquetes esto debido a gran cantidad de redes presentes en el escenario y el solapamiento de varias redes por lo cual al sacar los valores promedio se tiene un porcentaje de pérdida de 25,56% y un Bitrate de 4031,4Kb/s dando un rendimiento de red del 50%; cifras que fueron realizadas en base al Bitrate promedio conseguido considerando a 8224Kb/s como 100%.

A continuación verificamos las gráficas generadas con D-ITG.

Commando: *root/DITG/src/ITGPlot#. /ITGPlot bitrate*

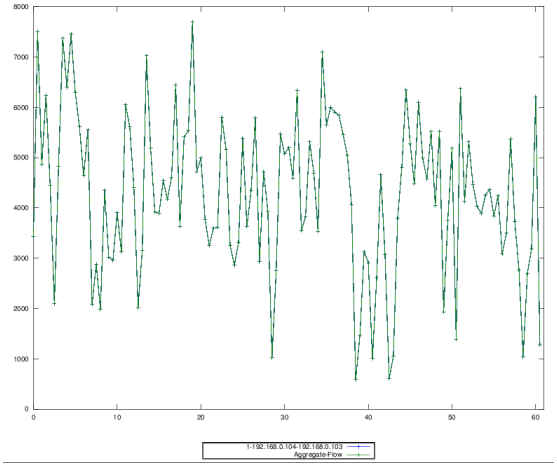


Figura 4-79 Bitrate Escenario 3.

Se puede verificar que la cantidad de datos transferidos varía mucho y se puede verificar picos máximos de alrededor de 7800 y mínimos de 500 este comportamiento se debe como se detalló previamente a la interferencia co-canal y al solapamiento.

Commando: *root/DITG/src/ITGPlot#. /ITGPlot delay*

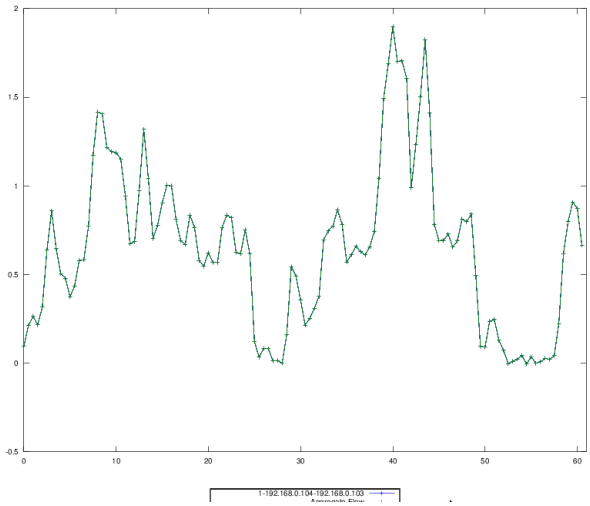


Figura 4-80 Delay Escenario 3.

El retraso de igual forma se verifica muy variable alcanzando pico de 1.9s lo que puede provocar la pérdida de datos.

Commando: *root/DITG/src/ITGPlot#. /ITGPlot jitter*

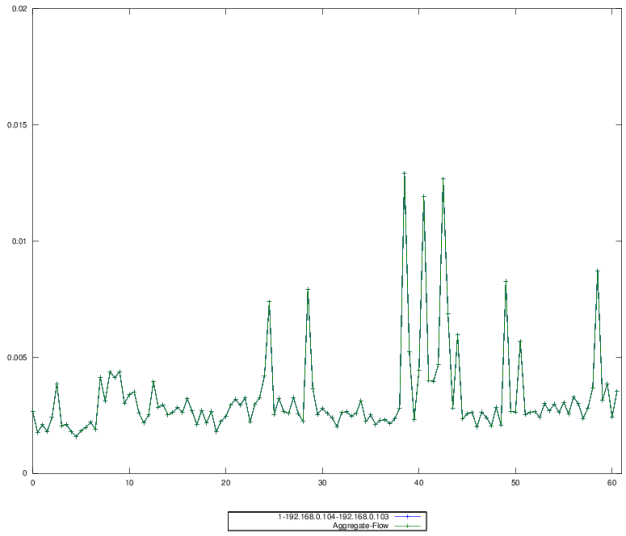


Figura 4-81 Jitter Escenario 3.

El jitter del escenario es muy bueno casi imperceptible en el transcurso de tiempo. El máximo pico se verifica entre los 30y 50s alcanzando un valor aproximado de 12ms

Commando: *root/DITG/src/ITGPlot#. /ITGPlot Packetloss*

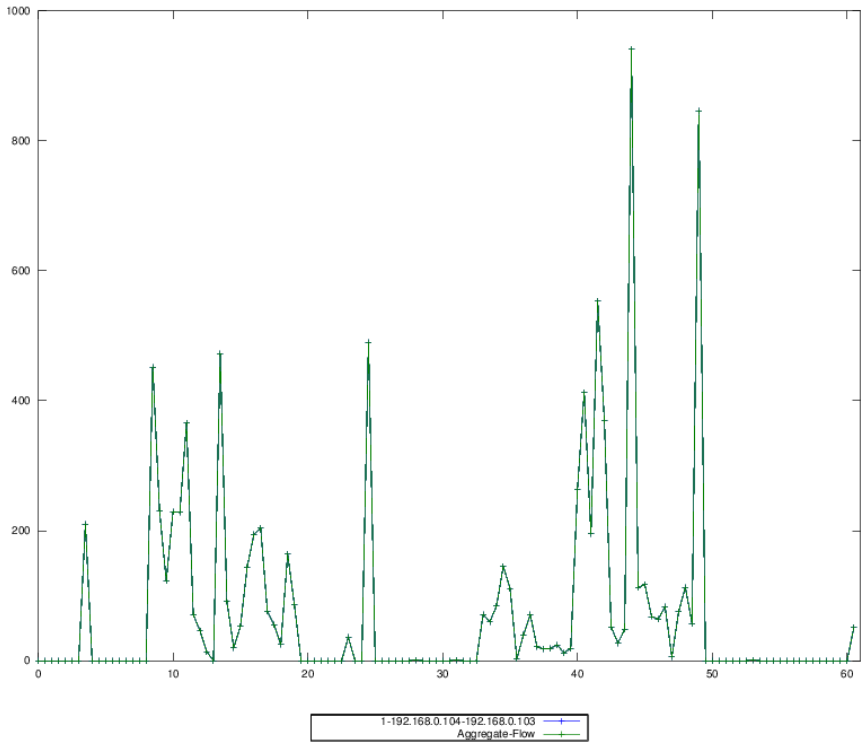


Figura 4-82 Paquetes descartados.

Packetloss nos confirma pérdidas considerables de paquetes que en el transcurso del tiempo varían entre valores aproximados de 200 a 950 paquetes. Hay que tomar en cuenta que el tamaño de los paquetes no es constante y pueden ser muy variables.

Analizando mediante estadísticas por completo el ambiente de red utilizamos SteelCentral Packet Analyzer

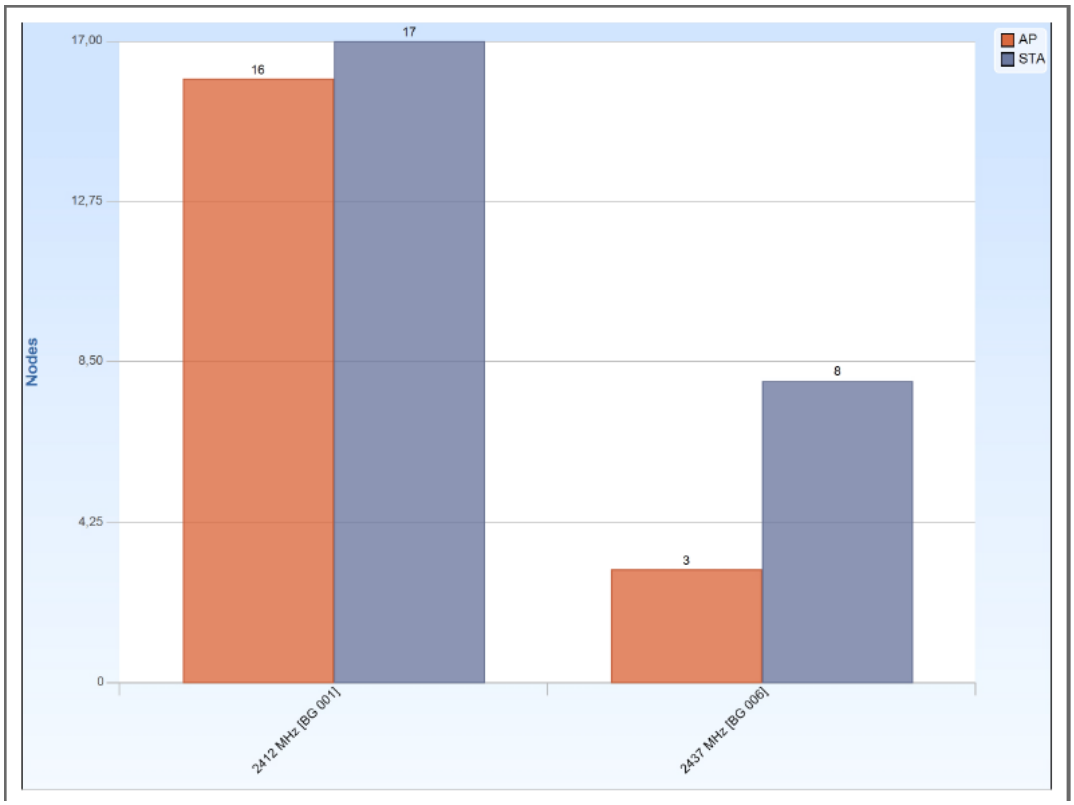


Figura 4-83 Nodos Escenario 3

Tabla 36 Nodos Escenario 3

Name	Value
2412 MHz [BG 001]-AP	16
2412 MHz [BG 001]-STA	17
2437 MHz [BG 006]-AP	3
2437 MHz [BG 006]-STA	8

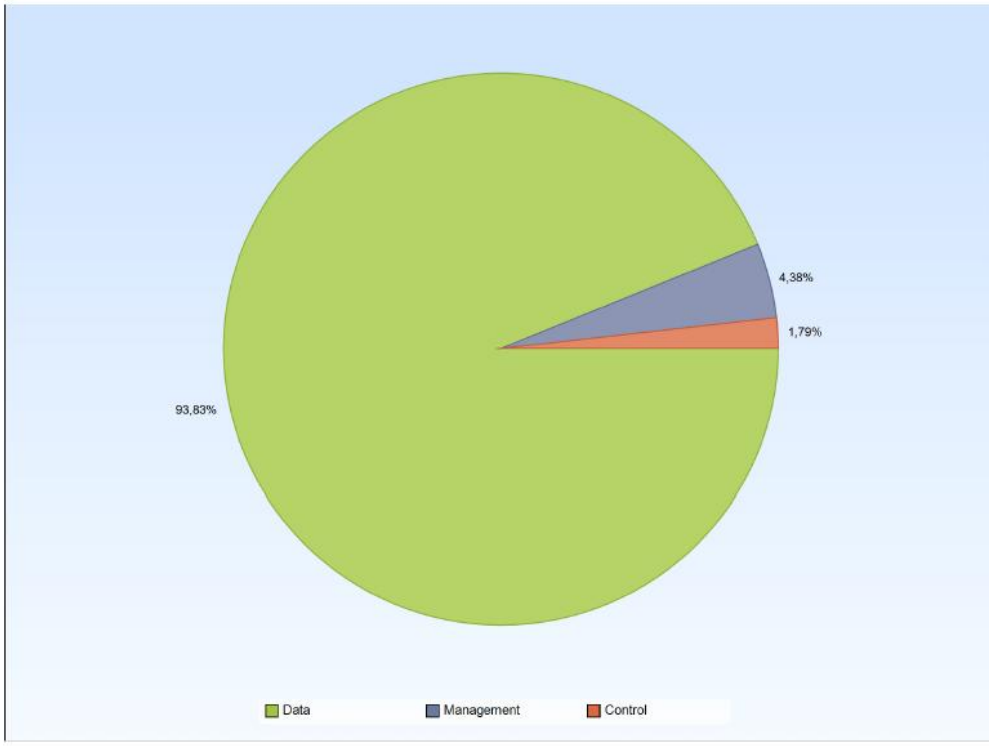


Figura 4-84 Bits según tipo de trama

Tabla 37 Bits según tipo de trama

Name	Value	%
Data	610845816	93,83
Management	28547200	4,38
Control	11636320	1,79

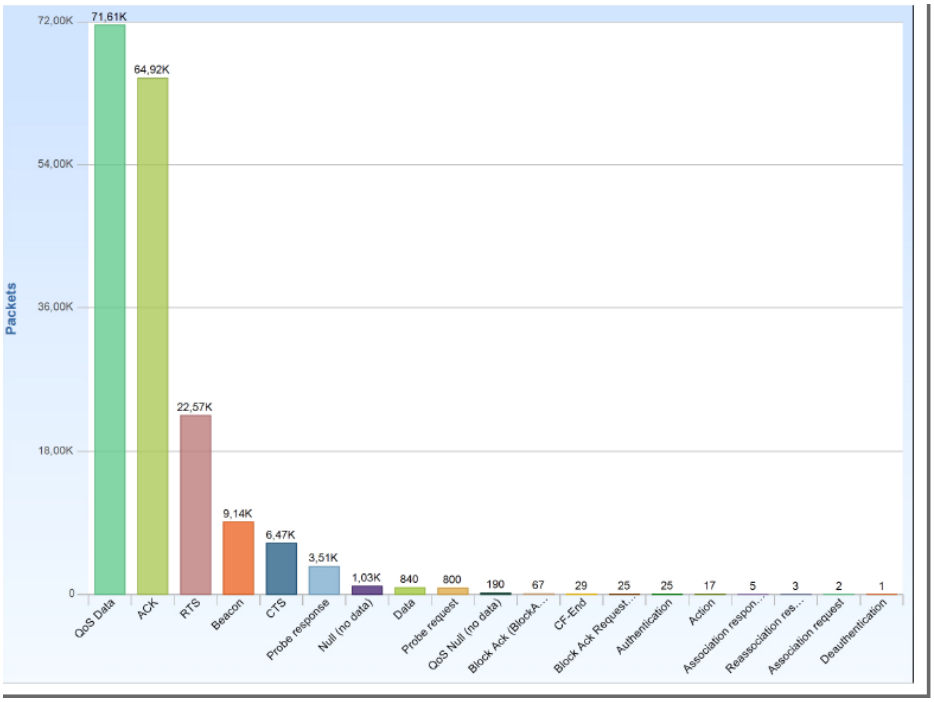


Figura 4-85 Paquetes según subtipo de trama

Tabla 38 Paquetes según subtipo de trama

Subtype	Packets
QoS Data	71612
ACK	64921
RTS	22568
Beacon	9139
CTS	6473
Probe response	3513
Null (no data)	1032
Data	840
Probe Request	800
QoS Null (no data)	190
Block Ack (BlockAck)	67
CF-End	29
Block Ack Request (BlockAckReq)	25
Authentication	25
Action	17
Association response	5
Reassociation response	3
Association Request	2
Deauthentication	1

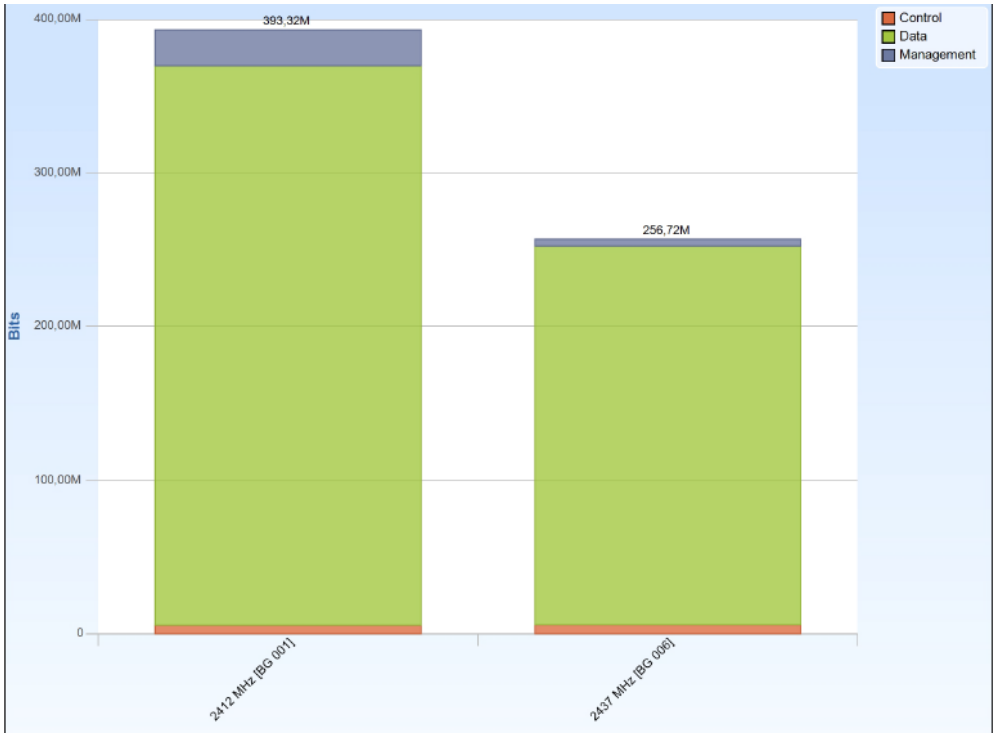


Figura 4-86 Bits por tipo de trama

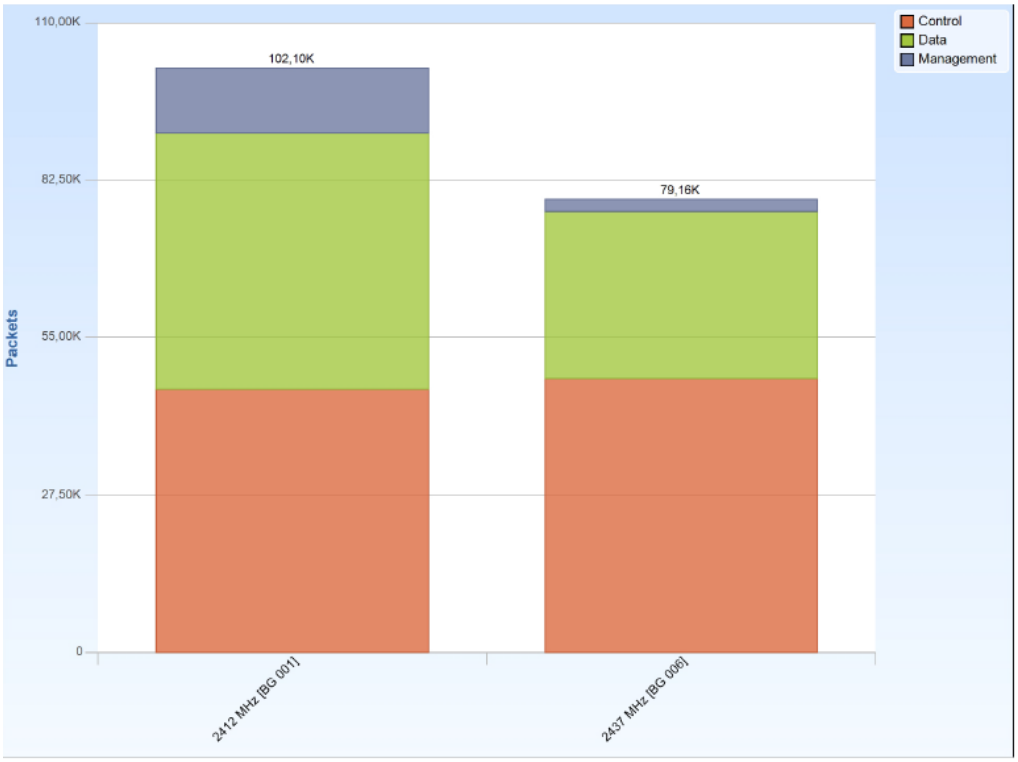


Figura 4-87 Paquetes por tipo de trama

Tabla 39 Paquetes según tipo de trama

Type	Packets
2412 MHz [BG 001]-Control	46102
2412 MHz [BG 001]-Data	44661
2412 MHz [BG 001]-Management	11336
2437 MHz [BG 006]-Control	47981
2437 MHz [BG 006]-Data	29013
2437 MHz [BG 006]-Management	2169

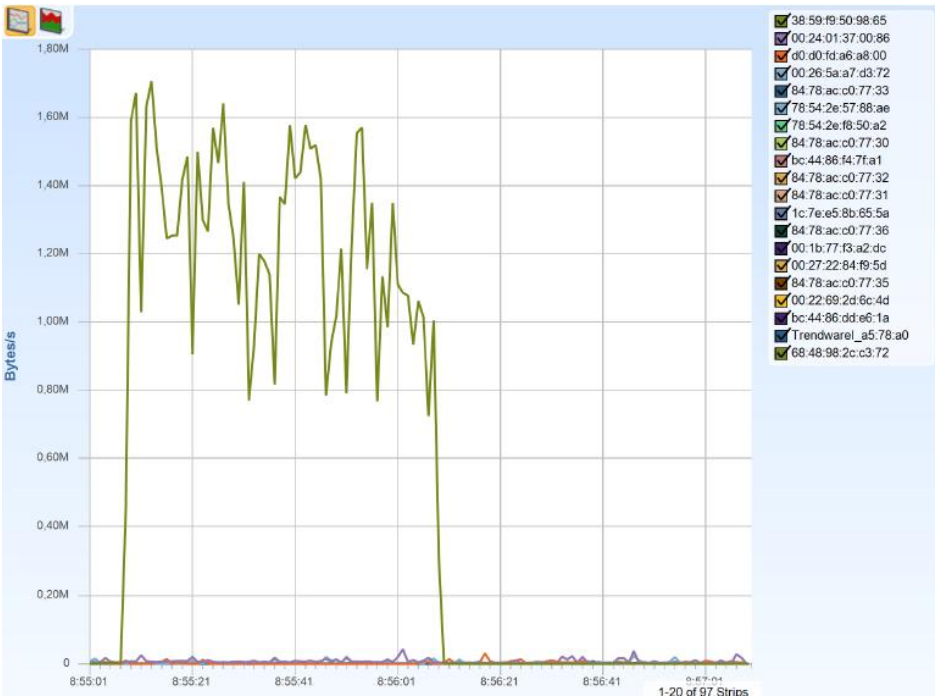


Figura 4-88 Bytes por segundo

De la gráfica anterior se verifica que la mayor cantidad de tráfico se genera desde la estación 38:59:f9:50:98:65.

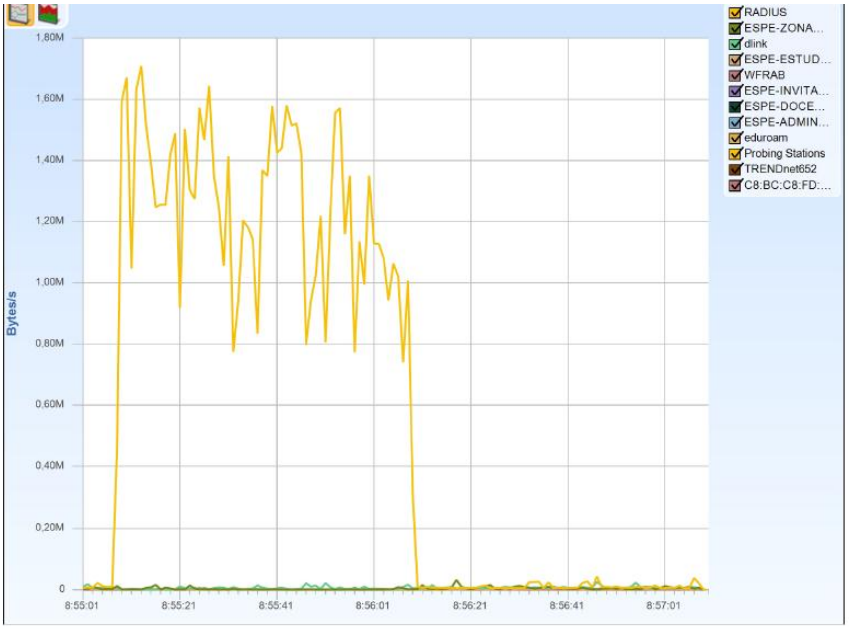


Figura 4-89 Bytes por segundo

De igual manera se verifica en la figura anterior que la red inalámbrica RADIUS es la que más tráfico se genera.

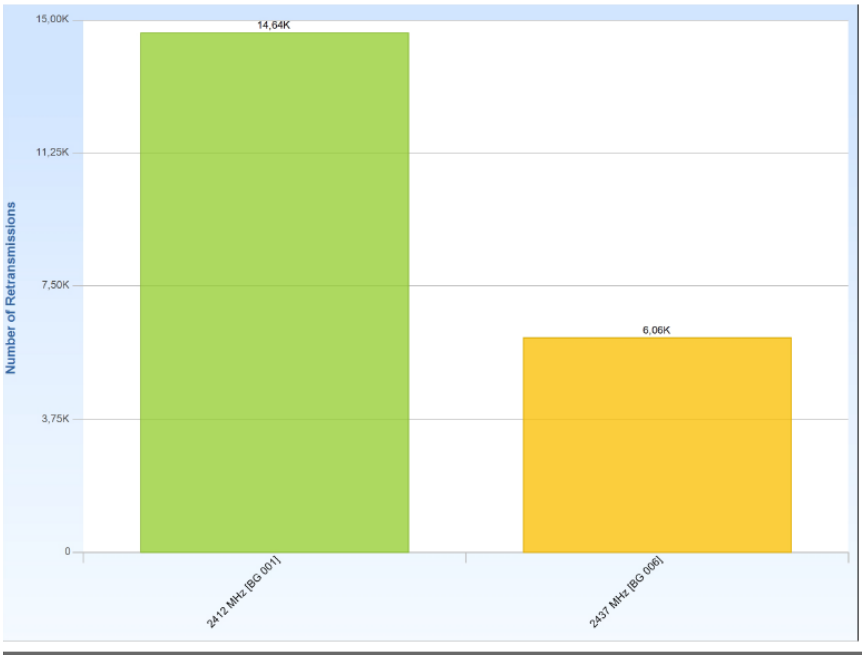


Figura 4-90 Retransmisiones por canal

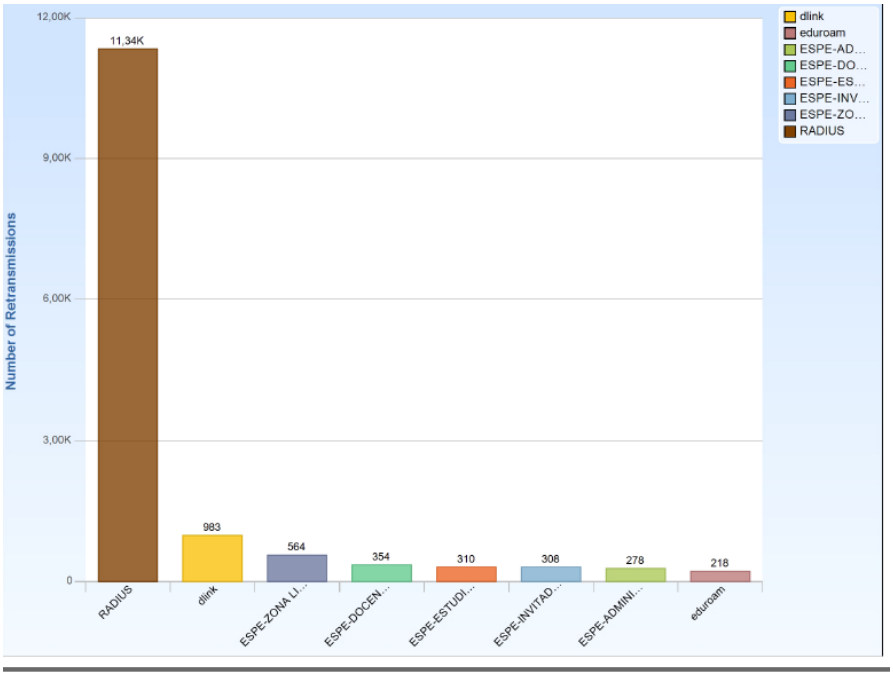


Figura 4-91 Retransmisiones por SSID

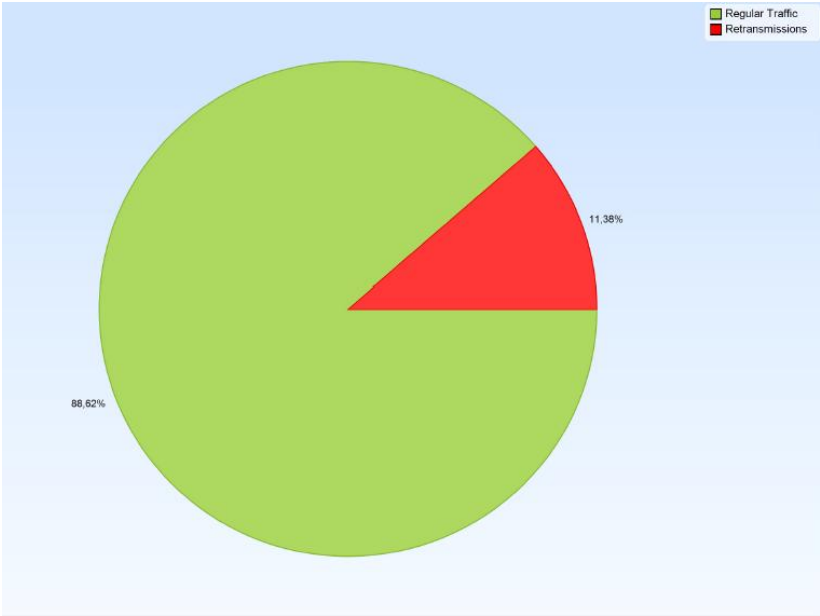


Figura 4-92 Tráfico Retransmitido

Tabla 40 Trafico Retransmitido

Traffic	Packets	%	Bits	%
Other Traffic	161141	88,62	500149128	76,82
Retransmissions	20702	11,38	150880208	23,18

Tabla 41 Promedio De nivel señal según SSID

ESSID	Signal Avg (dBm)	Noise Avg (dBm)
RADIUS	-26	-83
WFRAB	-59	-82
DLink	-72	-83
TRENDnet652	-74	-82

Tabla 42 Resumen Escenario 3

Hierarchy (Channel/ESSID/AP-Station)	MAC Address	Bits/s	Packets/s	Signal (dBm)	Noise (dBm)
Channel: 2412 MHz [BG 001]	[57]	52,65K	7,44	-60	-81
Channel: 2437 MHz [BG 006]	[17]	114,27K	14,14	-49	-85

4.2. FASE 2

Una vez verificado a nivel global una red, el administrador puede enfocarse en el análisis específico de un canal con el fin de comprobar procesos como autenticación o asociaciones, roaming de estaciones hacia un punto de acceso específico para lo cual escenarios como los detallados en la fase 1 nos ayudarán para cumplir con este propósito.

4.2.1. Autenticación WEP

En el caso específico del escenario 1 se mencionó que dicho escenario proporciona seguridad WEP, por lo cual en primera instancia el monitoreo monocanal nos ayuda a cumplir con el propósito de análisis.

A continuación se muestra la secuencia necesaria para que sea asociada una estación.

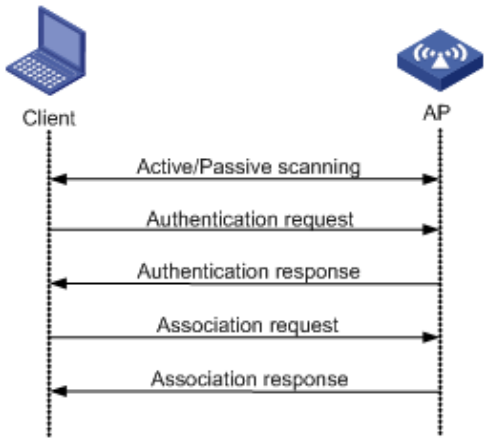
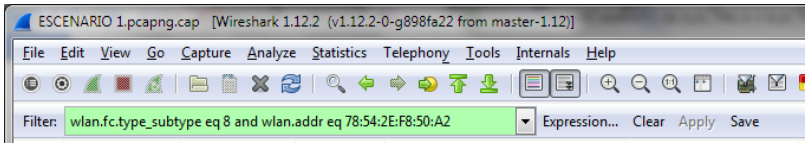


Figura 4-93 Asociacion estación WEP Open System

Análisis en Wireshark

Durante el proceso de escaneo una estación puede obtener datos de los APs circundantes a asociarse en base a un método pasivo o activo. El primer método la estación obtiene datos de los APs al escuchar las tramas beacon enviadas periódicamente y permite el ahorro de energía en las estaciones.

Para verificar el comportamiento en nuestro escenario de las tramas beacon enviadas desde el AP se utilizó un filtro del punto de acceso y tipo de trama.



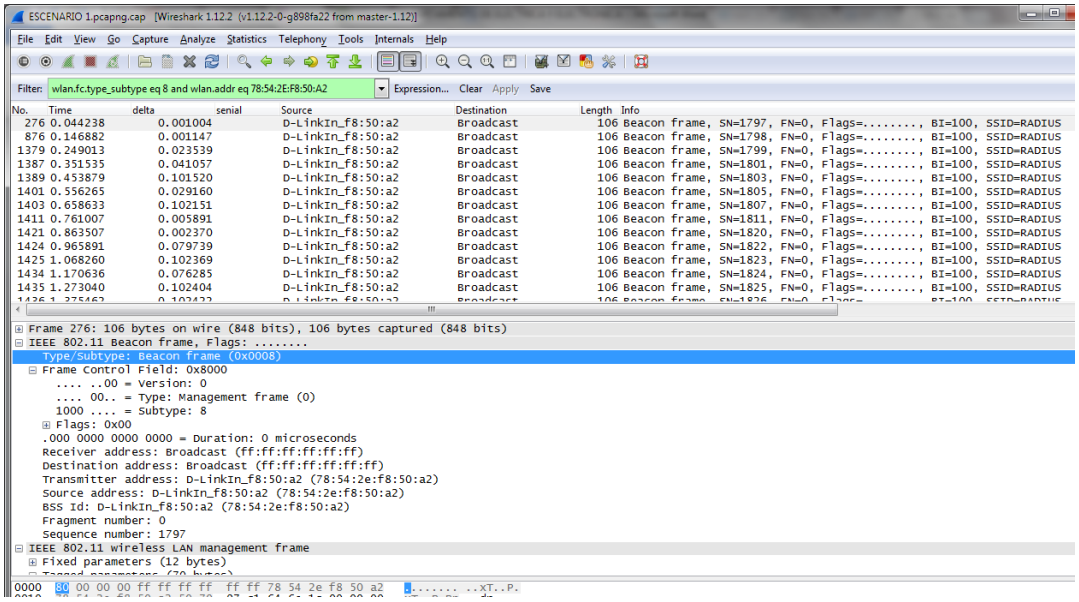


Figura 4-94 Filtrado trama Beacon.

Para poder verificar el tiempo que toma el envío de cada trama beacon; la paquetería aplicada con el filtro en Wireshark puede ser exportado a un formato compatible con Excel para su posterior análisis.

En nuestro escenario se configuro el AP para que se envíe cada 100ms tramas de este tipo pero en realidad al verificar el escenario a través del cálculo de los valores como tamaño del paquete y tiempo medio del paquete se tiene que para este tipo de equipo D-Link DIR-619L, el período promedio en que se enviarán tramas beacon al escenario implementado es de 73ms y el tamaño de cada trama es 106 Bytes.

Adicionalmente en Wireshark se puede obtener gráficas de los datos capturados seleccionando en la pestaña Statistics IO Graph que permiten visualizar de mejor forma el comportamiento de las tramas a evaluarse por el administrador de red. Para el escenario se verifico el comportamiento de las tramas beacon.

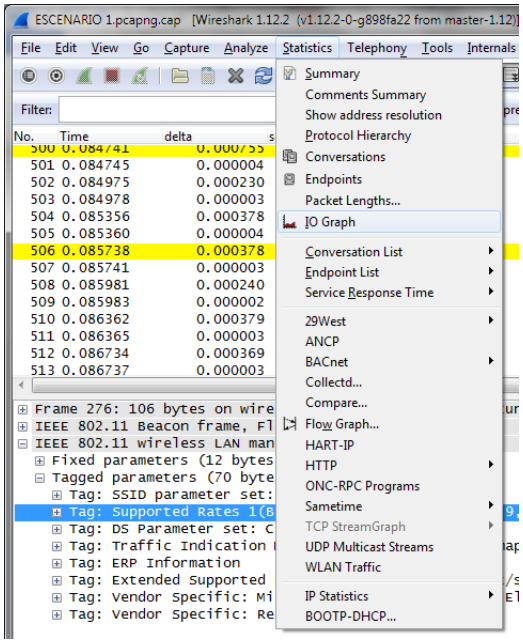


Figura 4-95 Configuración IO Graph.

Para detallar a mayor profundidad una trama beacon es la encargada de enviar a la red los parámetros inalámbricos de conexión para la red WLAN, es decir las características configuradas en el AP para nuestra red.

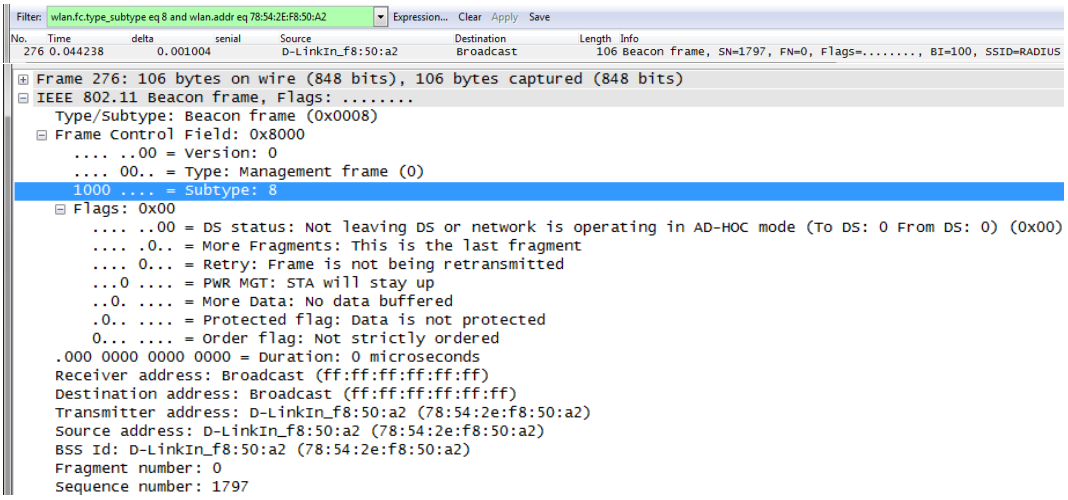


Figura 4-96 IEEE Beacon.

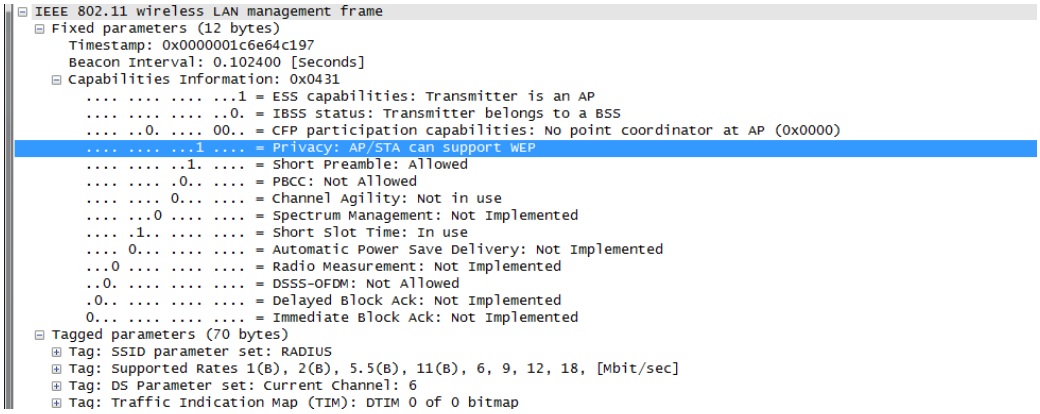


Figura 4-97 Trama 276 Encapsulamiento.

En la trama 276 se verifica los detalles de la red en el encapsulamiento Wireless LAN Management Frame en el cual se especifica que la red se mantiene configurado seguridad WEP y la velocidades de soporte del equipo varían entre 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48 y 54 Mbps y el canal de operación que es el 6.

Por otro lado para inicializar la asociación de la estación a la red tenemos el método de escaneo activo consistente en que una estación periódicamente busque un AP disponible en base a dos modos el primero que consiste en tener una trama tipo Probe Request con SSID nulo y que es enviado por cada canal soportado por la tarjeta inalámbrica de la estación. Posteriormente cada AP que recepta el paquete Probe Request responde con un paquete Probe Response con la información de la red inalámbrica. Finalmente la estación o cliente se asocia con el AP de mayor fuerza de señal.

Para poder verificar el comportamiento de las tramas Probe Request se aplicó el filtro: *!(wlan_mgt.ssid eq RADIUS)and wlan.fc.type_subtype eq 4 and wlan.addr eq 00:1b:77:f3:a2:dc*

Mismo que permite discriminar los SSID con RADIUS al anteponer el signo de admiración y verificar cómo se comporta la estación cuando desconoce un SSID.

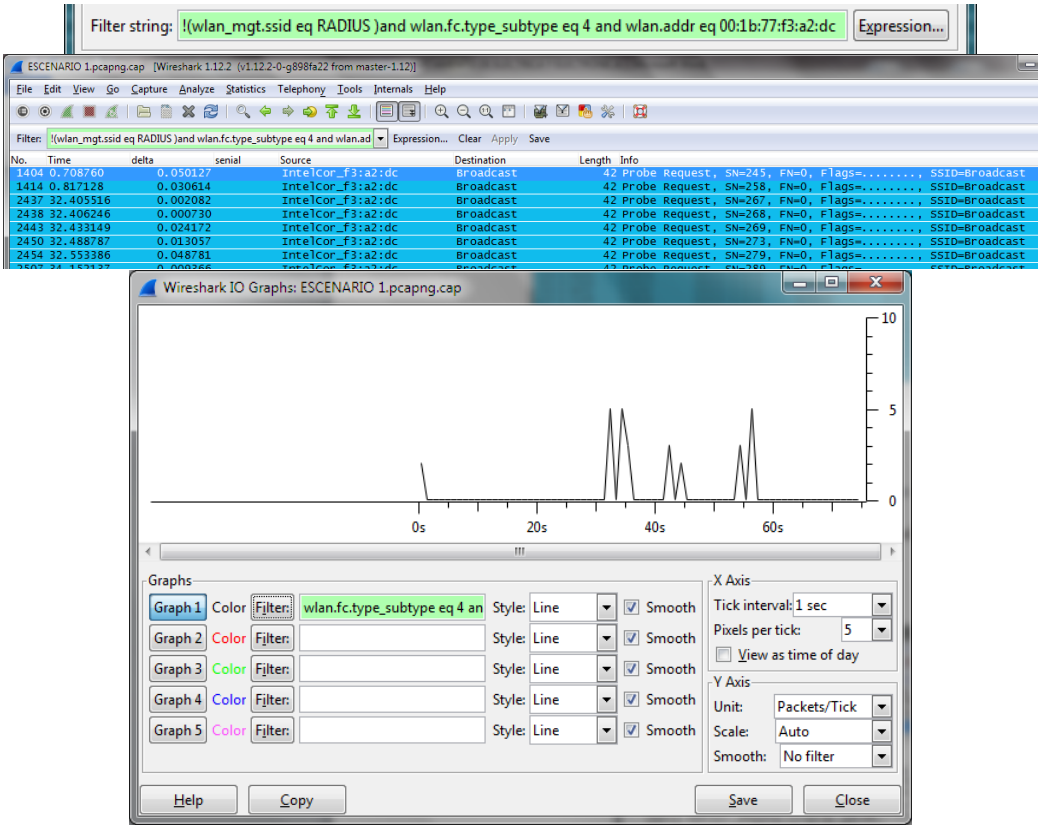


Figura 4-98 Filtro, Paquetes y Grafico Probe Request Escenario 1.

Dado que el monitoreo únicamente es aceptado en un solo canal podemos ver en nuestra red la estación 00:1B:77:F3:A2:DC genera alrededor de 3 a 5 tramas cada 10s las cuales son variables en cuanto a su duración.

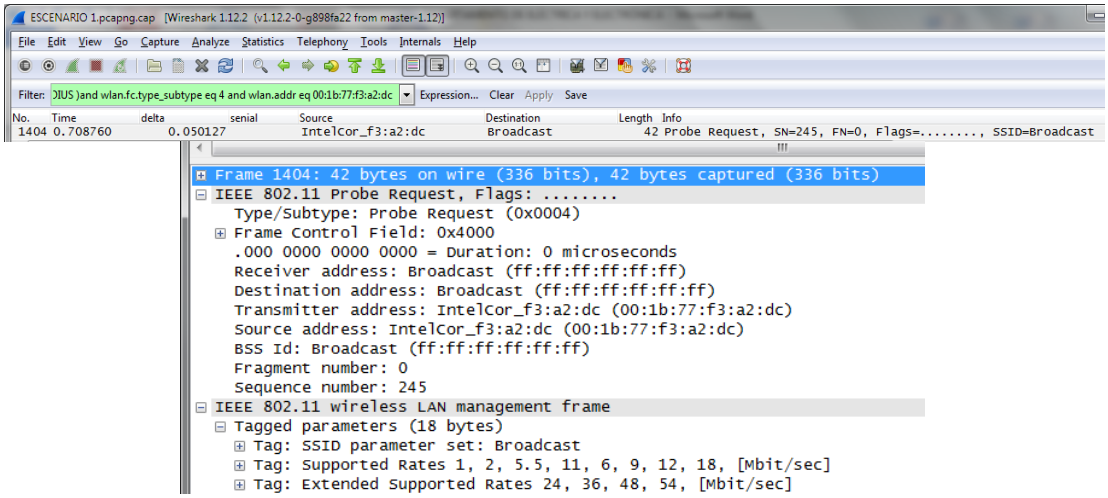


Figura 4-99 Frame Probe Request.

En base a la figura anterior podemos verificar que las tramas Probe Request tiene un tamaño de 42 bytes y se verifica el BSSID como Broadcast (ff:ff:ff:ff:ff:ff) verificando lo mencionado en el modo de escaneo activo.

El segundo modo de conexión de una estación es cuando esta tiene conocimiento del SSID requerido, es decir cuando la estación tiene ya registrado una red inalámbrica y envía una trama unicast Probe Request la cual es respondida por el AP especificado mediante la trama Probe Response.

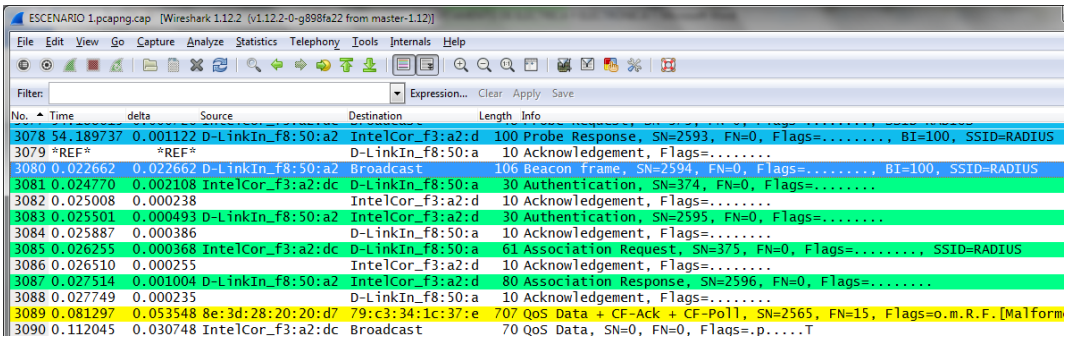


Figura 4-100 Probe Response.

Para asegurar la conexión inalámbrica, el cliente es autenticado previo a la asociación con el AP; en el escenario planteado el método de autenticación es mediante sistema abierto que es conocido por ser el más simple y mediante el cual cualquier cliente puede ser autenticado. Se basa en dos pasos que son el envío de la petición de autenticación desde el cliente y la respuesta de autenticación exitosa del lado del AP.

En nuestro escenario se verifica como primer paso que la estación escucha la trama beacon 3080 la cual tiene una duración de 22,6ms, posteriormente se inicia el proceso de autenticación desde la trama 3081 hasta la trama 3084 las cuales duran 3,22ms finalmente la estación termina asociándose al ser enviado el ACK de confirmación por parte del AP en la trama 3088 transcurriendo en total 27 ms.

De esta manera verificamos que el tipo de asociación efectuada en este escenario es exitosa y fue realizada mediante el método pasivo de autenticación abierta.

4.2.2. Roaming

A continuación con el fin de verificar el proceso de roaming de una estación se procede a verificar el tramado en cuanto a Re Asociaciones.

Enfocándonos en la implementación del escenario 3 descrito en la fase 1 podemos proceder a depurar el tráfico no necesario para el análisis e ir enfocándonos canal por canal de los puntos de acceso involucrados.

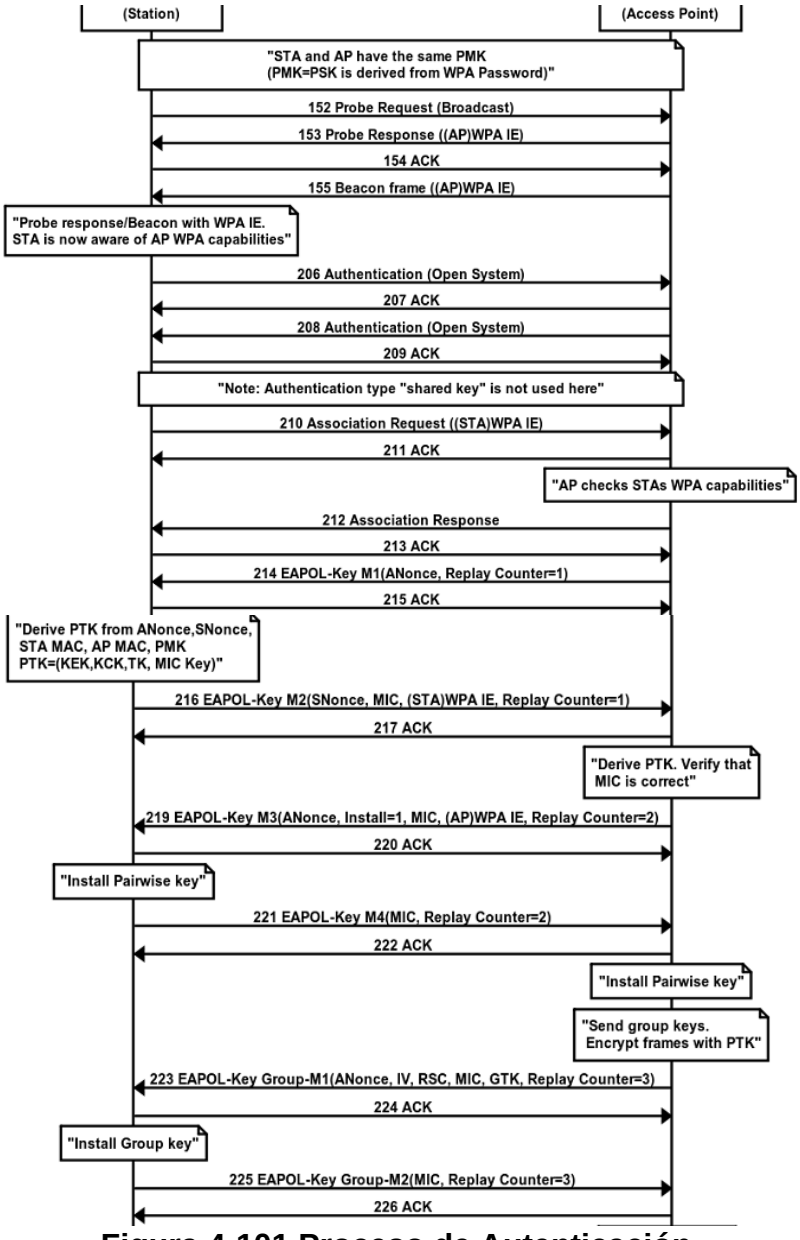


Figura 4-101 Proceso de Autenticación.

Análisis en Wireshark.

Como en este caso necesitamos verificar cual fue el proceso para realizar el roaming por parte de la estación Acer (STA2) aplicamos el uso de filtros disponibles en Wireshark.

Filtro: *wlan.addr eq 38:59:f9:50:98:65 and wlan.fc.type_subtype eq 2*

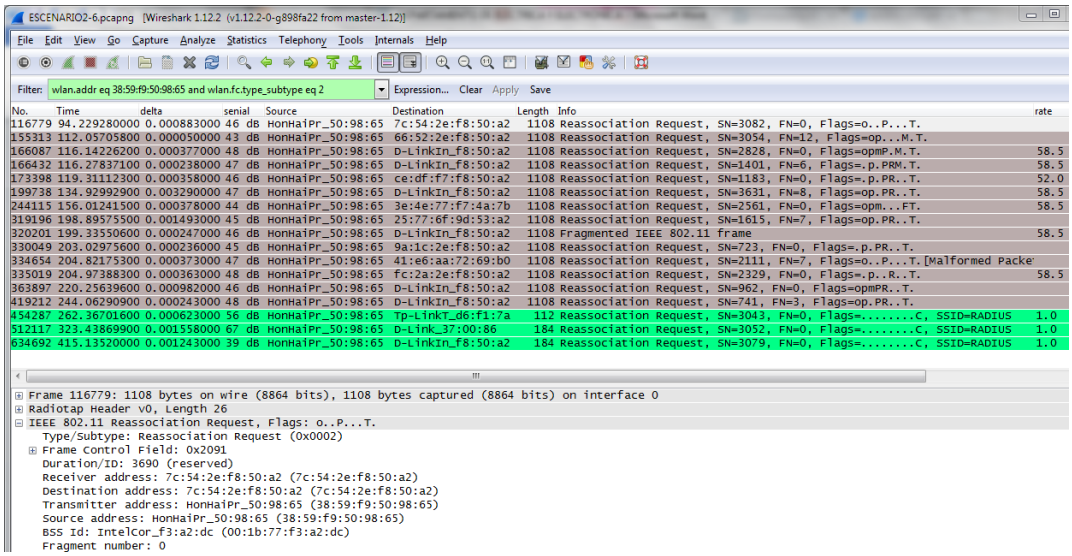


Figura 4-102 Frame Reasociación.

La figura anterior muestra tres solicitudes de Reasociación enviadas correctamente desde la estación HonairPr_50:98:65 (STA2) por lo cual verificamos que el comportamiento de la estación es en principio una asociación hacia el punto de acceso Tp_Link_d6:f1:7a (AP2), la segunda asociación es hacia el punto de acceso D-Link_37:00:86 (AP1) para finalizar asociado al punto de acceso D-Link_f8:50:a2 (AP3). Para poder verificar el proceso de asociación es necesario verificar con un filtro en el cual únicamente se muestren los equipos de nuestro escenario y de ese modo verificar los procesos que toma la estación y comprobar el origen y destino de la estación por cada Reasociación.

Filtro: *wlan.addr eq 00:1b:77:f3:a2:dc or wlan.addr eq 38:59:f9:50:98:65 or wlan.addr eq 78:54:2E:F8:50:A2 or wlan.addr eq 00:1D:0F:D6:F1:7A or wlan.addr eq 00:24:01:37:00:86*

Primero para el análisis de tráfico se debe tomar en cuenta los números de secuencia de las tramas enviadas por la estación Acer (STA2) y del punto de acceso a asociarse.

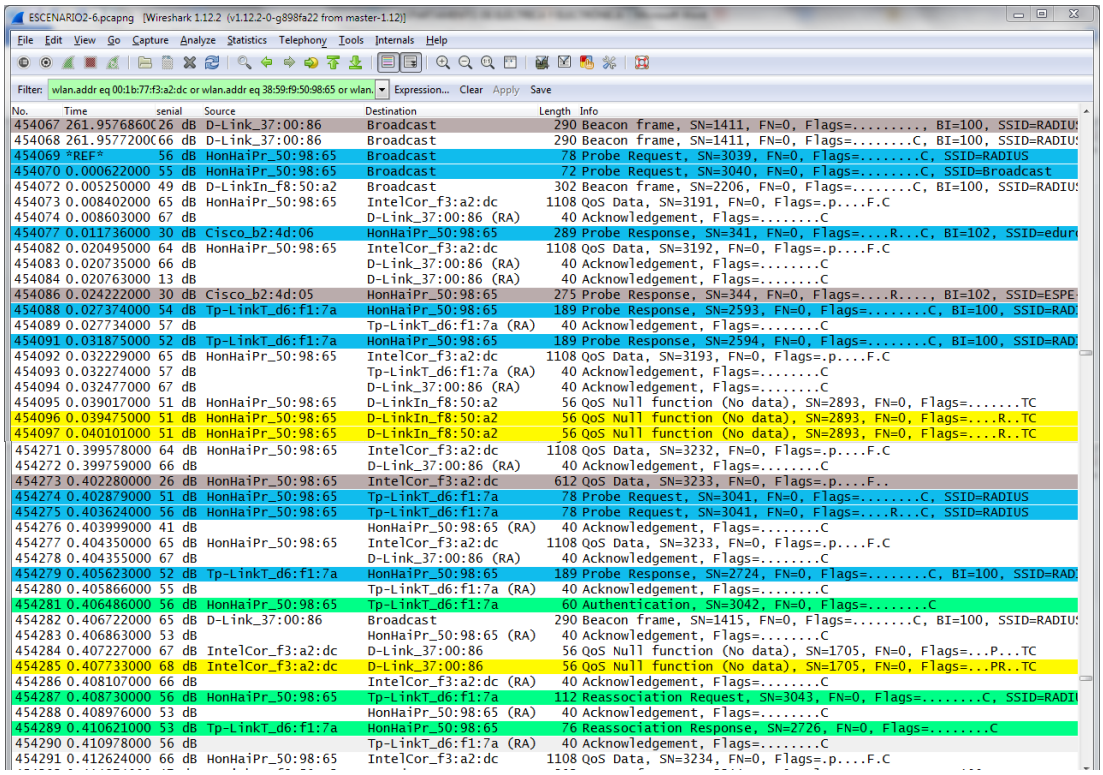


Figura 4-103 Asociación STA 2 con AP2.

De las gráficas anteriores se muestra que la estación Acer (STA2) lleva dos procesos el primero que es el envío de tráfico de D-ITG hacia la estación Intel (STA1) con números de secuencia SN=3193 y el segundo que es el proceso de asociación con el punto de acceso TP-Link (AP2) con número de secuencia SN=3039.

En el proceso de Reasociación se verifica en la tramas #454070 que se envía un Probe Request desde la estación STA2 con destino broadcast, inmediatamente a este petición se verifica las respuestas de los Access point circundantes y se observa en el registro una trama beacon por parte del equipo D-link_f8:50:a2 (AP3), las tramas Probe Response por parte del equipo Cisco_b2:4d:06 y del equipo Tplink_d6:f1:7a (AP2). Luego en la elección de equipo la trama #454274 es enviada por STA2 hacia el AP2 confirmando su elección y se puede verificar adicionalmente que el nivel de

señal registrado es de 51dB y es mayor a las intensidades de señal de los otros dos APs mencionados previamente que son 30dB y 49dB. Dando como resultado en la autenticación de la estación. Al tomar en cuenta que la estación intenta reasociarse mientras la estación se encontraba con el envío de tráfico, se verifico una duración de 411ms de tiempo transcurrido hasta verificar la trama #454289 correspondiente al Reassociation Response enviado por STA2, un tiempo que es considerablemente alto, pero como nuestro escenario se planteó la seguridad WPA; se requería que una vez re asociado se intercambien los mensajes de seguridad para asociarse por completo al nuevo AP en este caso AP2. Nuevamente para verificar la el Handshake de autenticación se aplica un nuevo filtro Wireshark.

Filtro: *(wlan.addr eq 00:1b:77:f3:a2:dc or wlan.addr eq 38:59:f9:50:98:65 Or wlan.addr eq 78:54:2E:F8:50:A2 or wlan.addr eq 00:1D:0F:D6:F1:7A Or wlan.addr eq 00:24:01:37:00:86) and eapol*

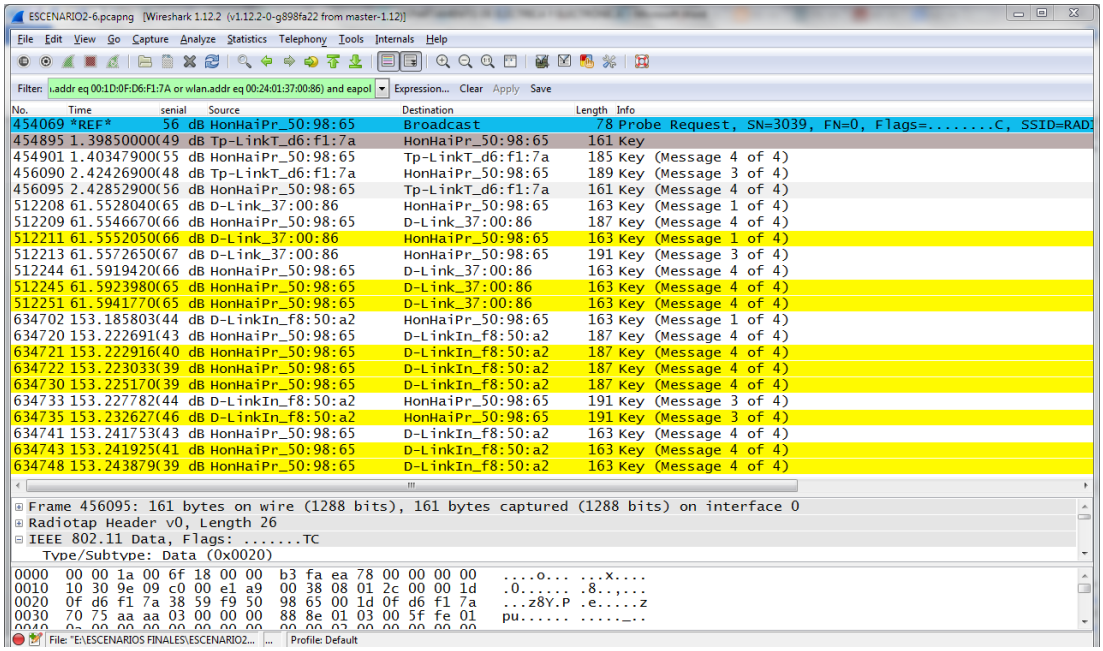


Figura 4-104 Autenticación PSK.

Con el fin de verificar el proceso de autenticación de la estación STA2 en AP2 se analiza a detalle los mensajes de intercambio psk.

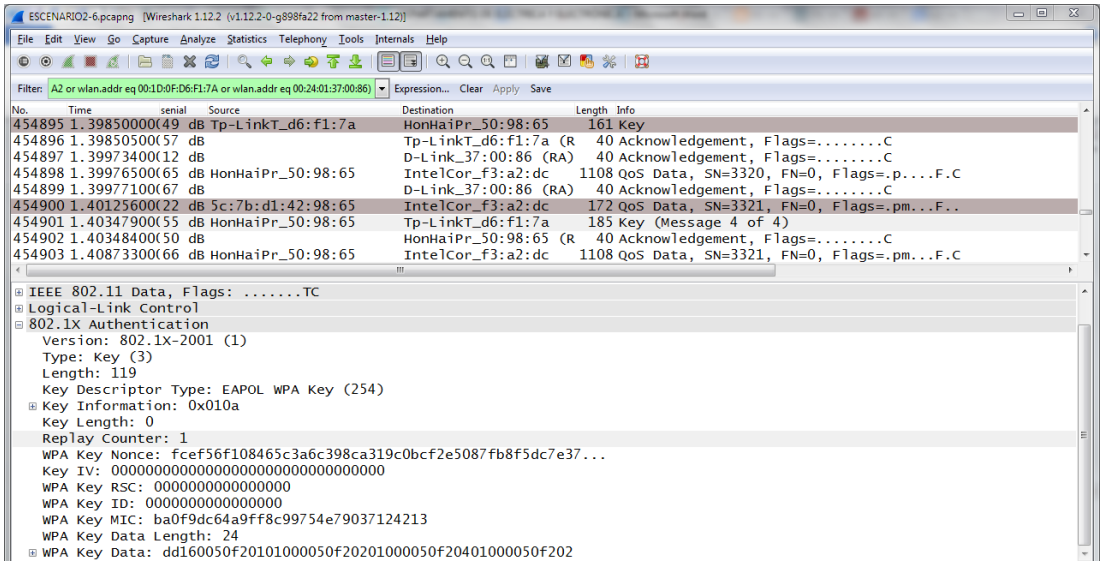
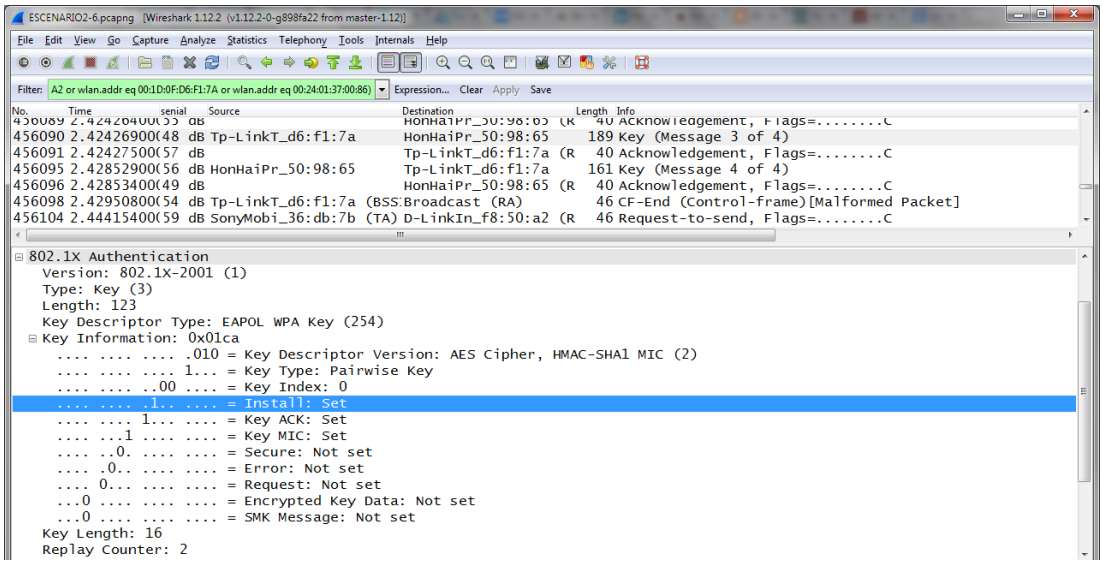


Figura 4-105 Trama #454895 Escenario 2.

Para el primer mensaje la trama #454895 han transcurrido 1,39s desde el proceso de Reasociación, dicha trama tiene información incompleta sin embargo STA2 logra recibirla verificándose la respuesta en la trama 454901 en el cual se incluye el counter=1 que corresponde a la fase de verificación de MIC reflejado en la trama con el nombre de WPA Key MIC.



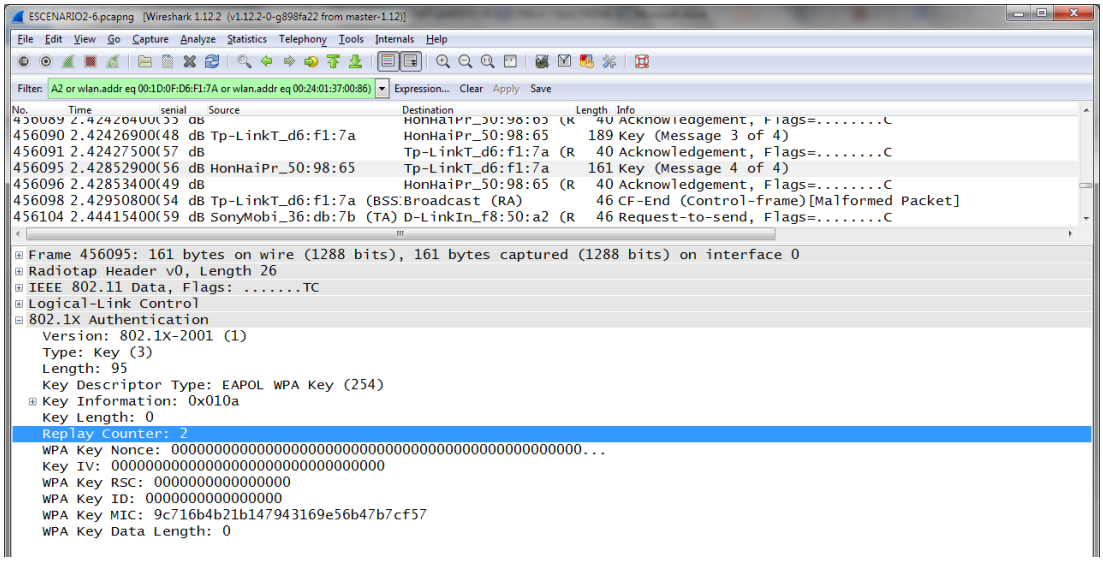


Figura 4-106 Autenticación Trama #456090.

Se continúa con el proceso de autenticación a partir de la trama #456090 la cual activa el flag Install con el fin de compartir la clave entre la estación STA2 y AP2 culminando exitosamente en la trama #456096 luego de transcurridos 2,43s en total para la Reasociación mientras se mantenía el envío de información de STA2 hacia STA1.

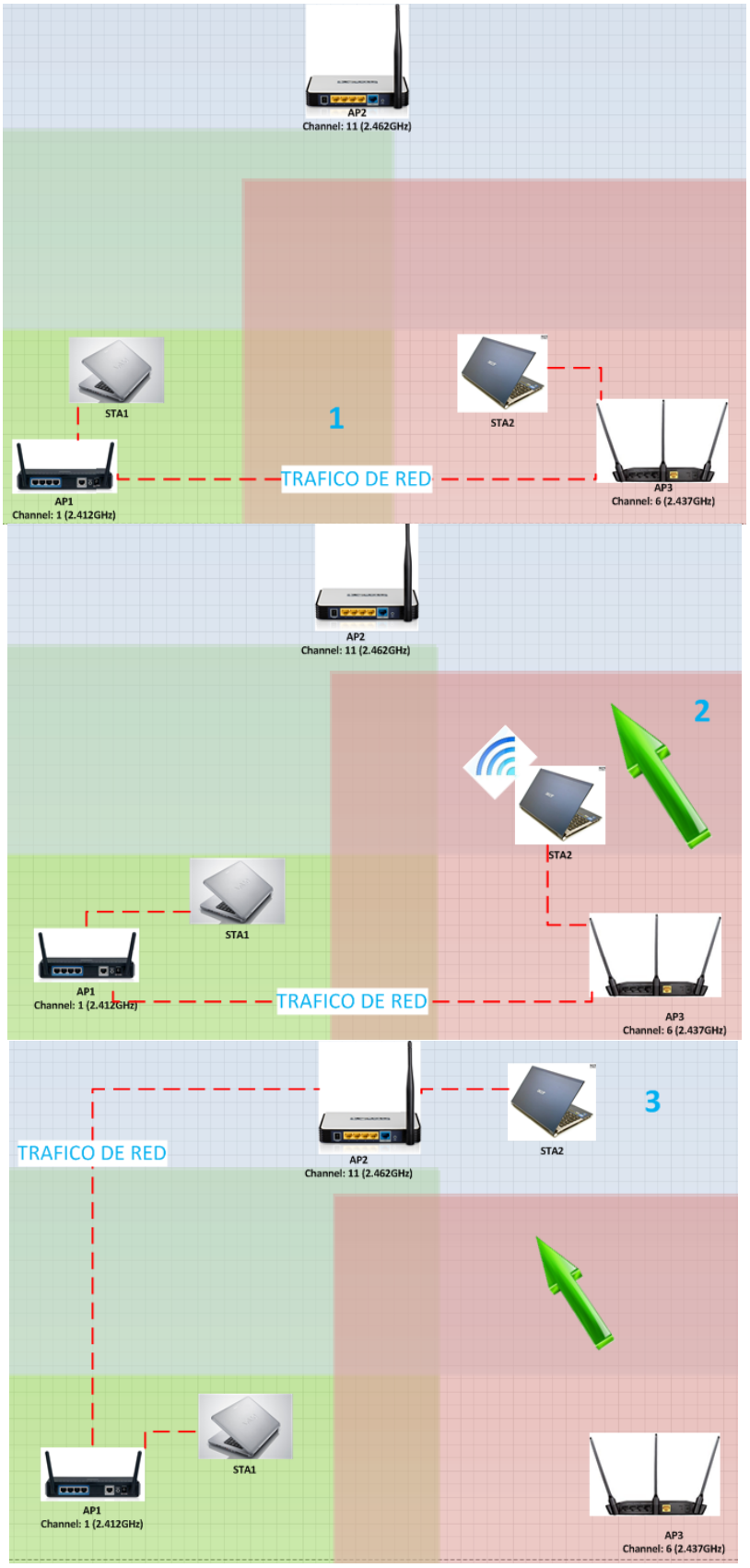


Figura 4-107 Recorrido Roaming Escenario 2.

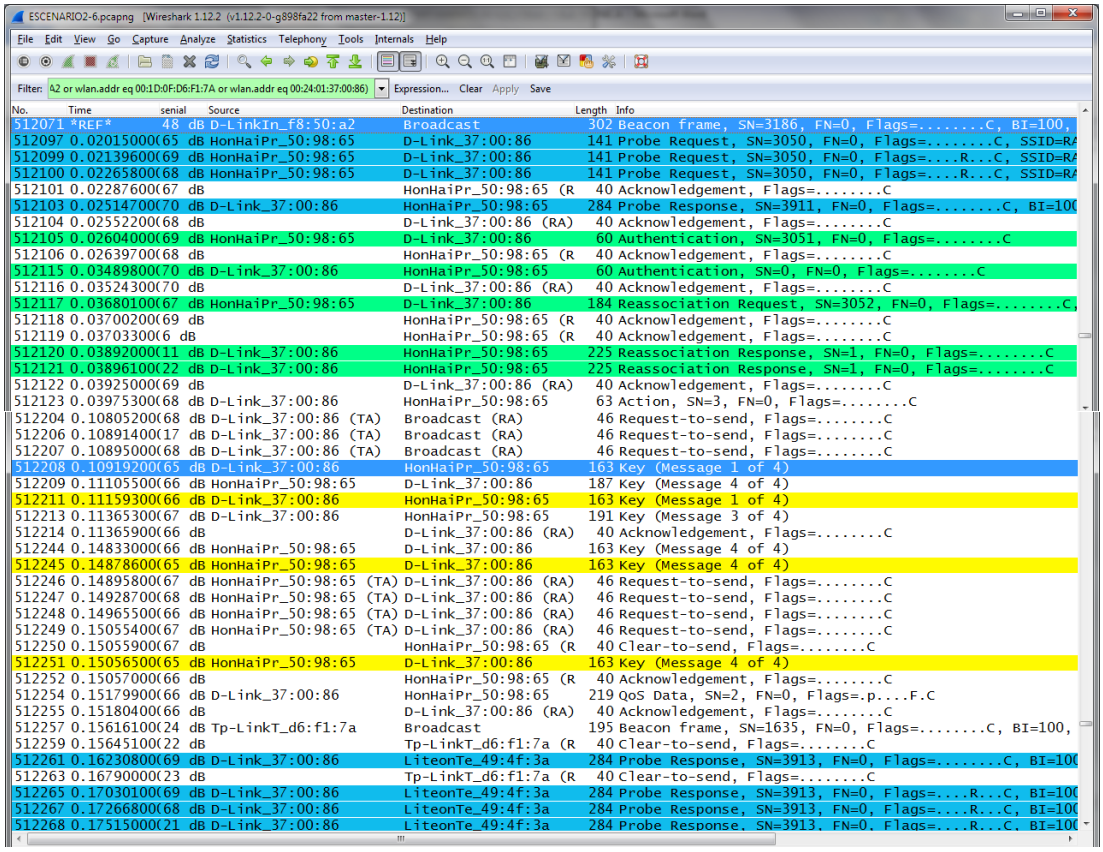


Figura 4-108 Trama #512071 Roaming Proceso 2.

Continuando con el análisis a partir de la trama #512071 se lleva un segundo proceso de roaming en el cual STA2 se dirige desde AP2 hacia AP1. Al igual que en el análisis anterior se aplica la opcion Set Time Parameter (toggle) dando click derecho en la trama que el analizador considere de referencia.

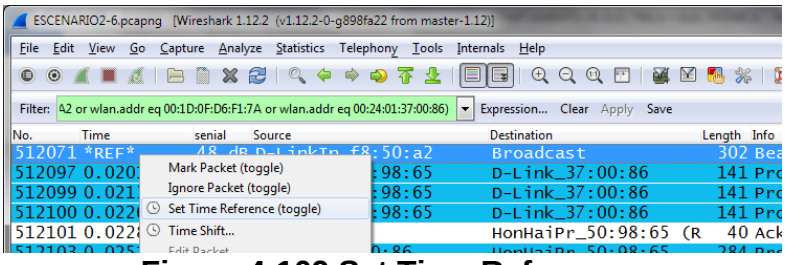


Figura 4-109 Set Time Reference.

Para esto proceso a diferencia del primer análisis se verifica que el proceso roaming desde AP2 modelo TP-Link TL WR542G hacia el AP1 D-Link DIR-615 se realiza la Reasociación transcurridos los 150ms un tiempo

relativamente bajo en comparación con el obtenido de 2.4s cuando la estación móvil enviaba datos hacia la estación STA1.

Finalmente culminando los procesos de roaming de la estación STA2 se tiene la Reasociación hacia AP3 desde AP1.

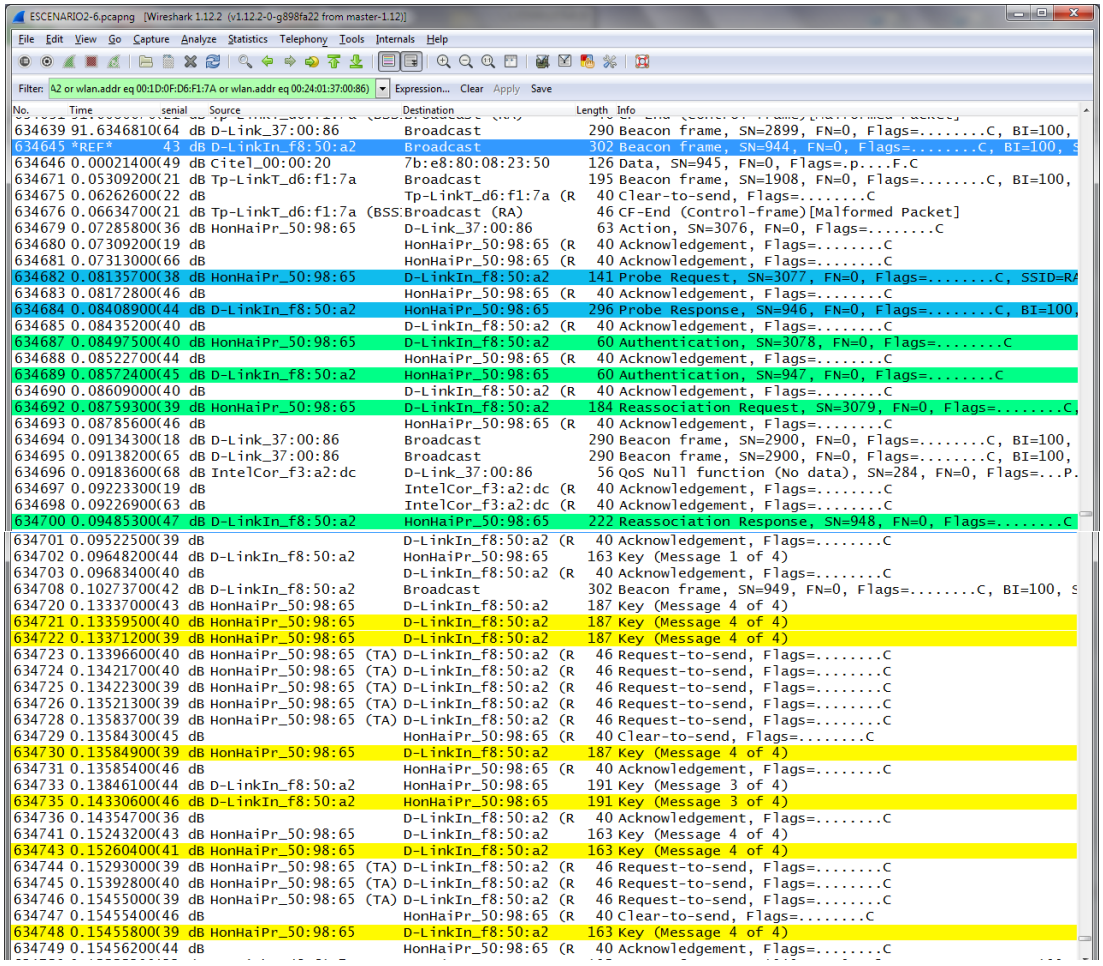


Figura 4-110 Roaming Proceso 3.

La figura anterior muestra un tiempo total de 154ms en que STA2 va desde AP1 D-Link DIR-615 hacia AP3 D-Link DIR-619L.

Tabla 43 Resumen Proceso Roaming.

Proceso	Origen	Destino	Tiempo total
1	AP3 DLink DIR-619L	AP2 Tplink TL WR542g	2,46s
2	AP2 Tplink TL WR542g	AP1 DLink DIR-615	150ms
3	AP1 DLink DIR-615	AP3 DLink DIR-619L	154ms

De lo verificado durante los procesos de roaming el proceso en el cual la estación STA2 transfería tráfico hacia la estación STA1 fue muy alto para que se efectúe por completo teniendo un tiempo muy alto en comparación de los procesos en los cuales ya no se verifico tráfico entre las estaciones. Este hecho se debe principalmente a las tramas de gestión IEEE802.11 debido a que se necesita que tanto la trama Clear to Send y Request to Send sea de la estación STA2 o de AP2 se sincronicen mientras el resto de APs así como la estación STA1 intentan enviar datos a STA2.

4.3. FASE 3

Dentro de esta fase podremos analizar diferentes escenarios, con los cuales podremos verificar comportamientos de escenarios implementados en los cuales con una visión más amplia analizaremos diferentes aspectos como Calidad de Servicio (QoS), Interferencia, Seguridad, etc.

4.3.1. Autenticación RADIUS

Para empezar con el análisis en esta fase realizaremos la implementación de un escenario donde tendremos un dispositivo (STA) que va intentar conectarse a un Punto de Acceso (AP) y éste está conectado hacia un servidor RADIUS en donde se va a verificar la autenticidad del usuario que quiere acceder a nuestra red.

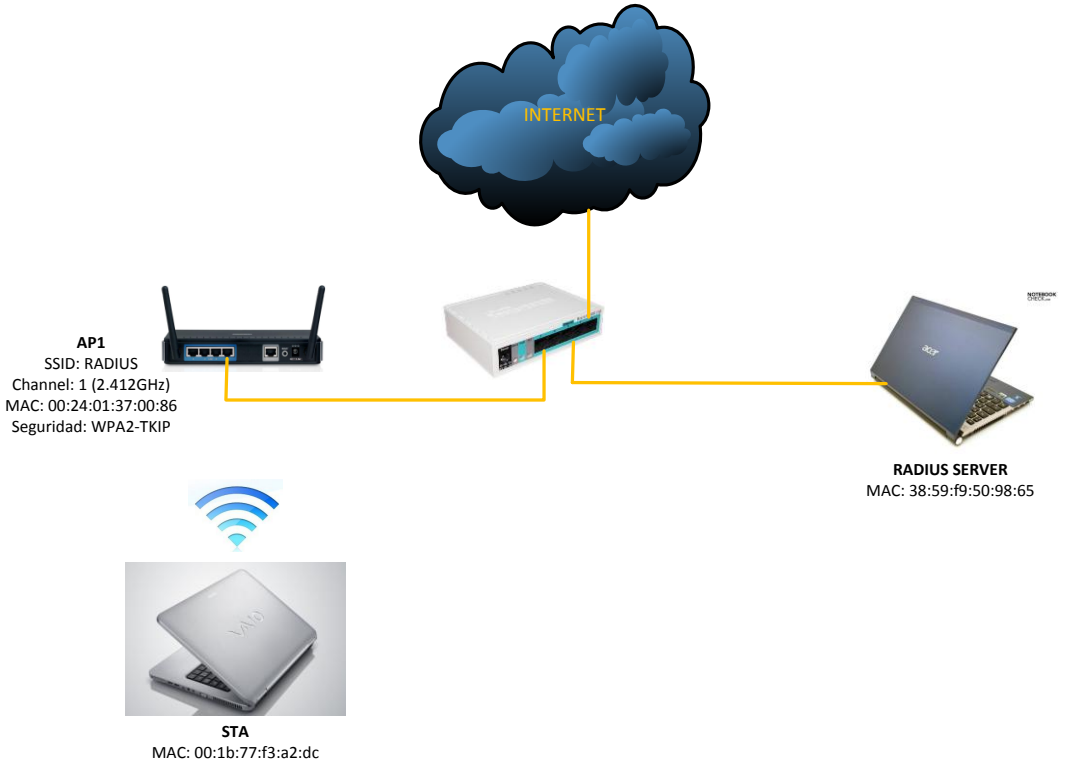


Figura 4-111 Escenario Autenticación RADIUS.

Configuraremos la Red Inalámbrica de nuestro AP D-LINK, mismo que se configura de acuerdo a la figura.

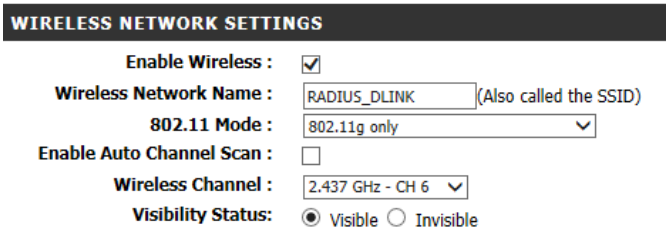


Figura 4-112 Parámetros de Estándar IEEE 802.11 D-LINK

Configuración Equipos de Red.

De acuerdo al escenario tendremos que configurar la Interface del AP con una IP estática ya que nuestro AP tendrá salida hacia el Internet por medio de un Router Mikrotik.

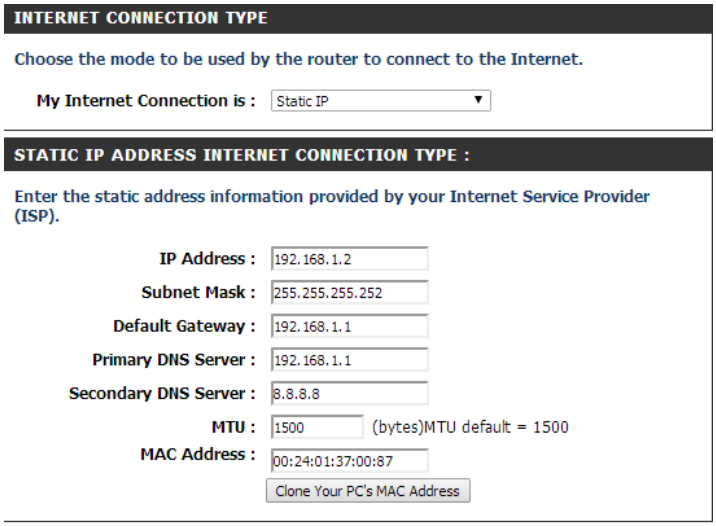


Figura 4-113 Configuración WAN D-LINK.

Realizamos la configuración DHCP para la asignación dinámica de nuestro AP hacia los usuarios que deseen conectarse a la red.

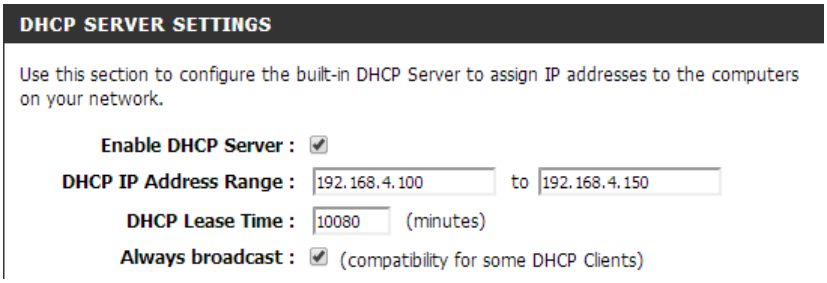


Figura 4-114 Configuración DHCP D-LINK.

Configuramos la autenticación por servidor RADIUS, habilitamos el modo de seguridad WPA-Enterprise, modo WPA22 Only y cifrado TKIP. Para la conexión con el servidor de autenticación ingresaremos la IP configurada en el servidor, el puerto de conexión y la clave compartida.

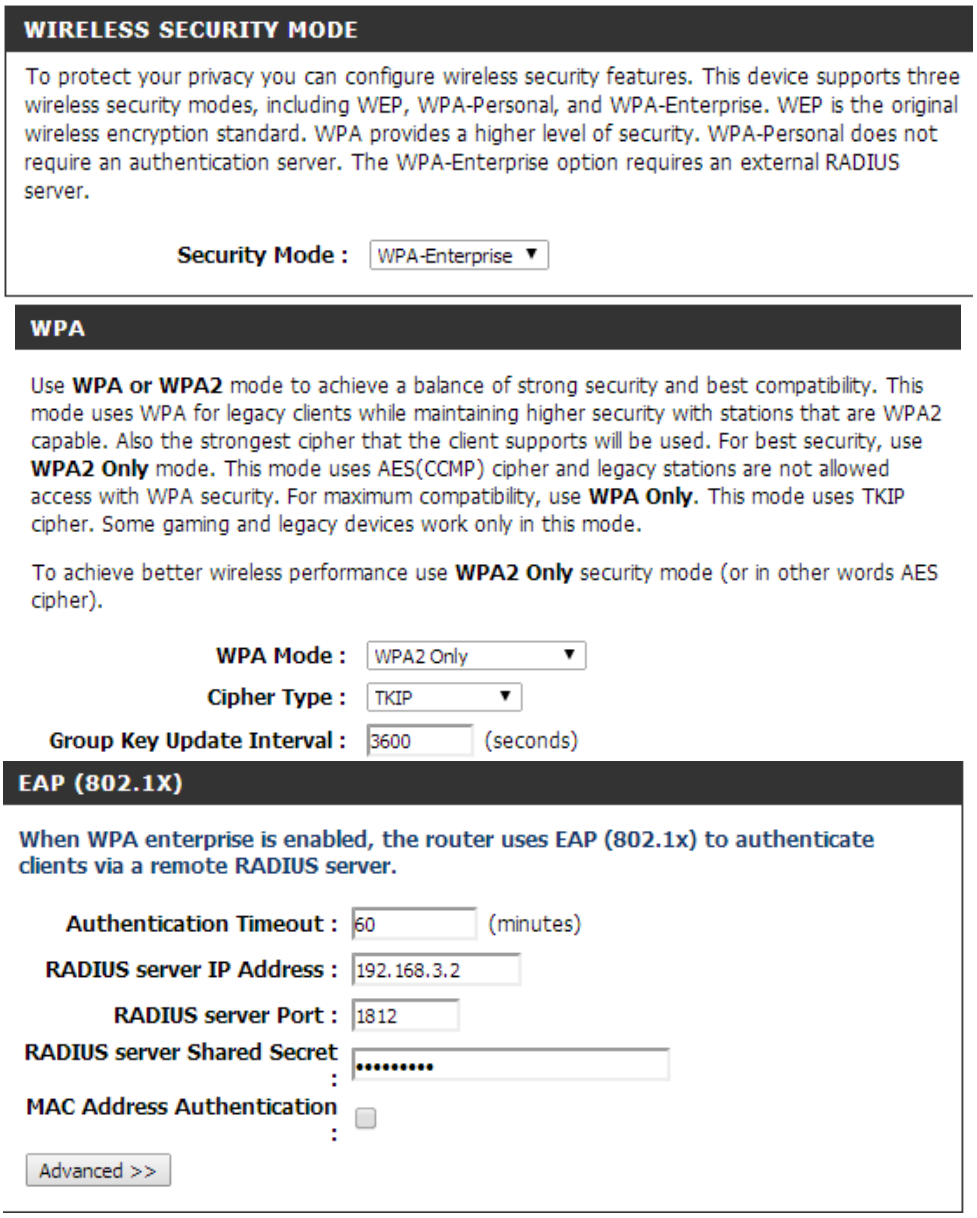


Figura 4-115 Configuración de Seguridad IEEE 802.11 D-LINK.

Esta configuración de seguridad, tiene como objetivo representar una red corporativa que utiliza un sistema de seguridad fuerte en donde cada usuario tiene un acceso exclusivo a la red.

Configuraremos el Router Mikrotik

De acuerdo a lo mostrado en las gráficas, para poder tener una conexión hacia el AP y la salida al internet con el NAT respectivo.

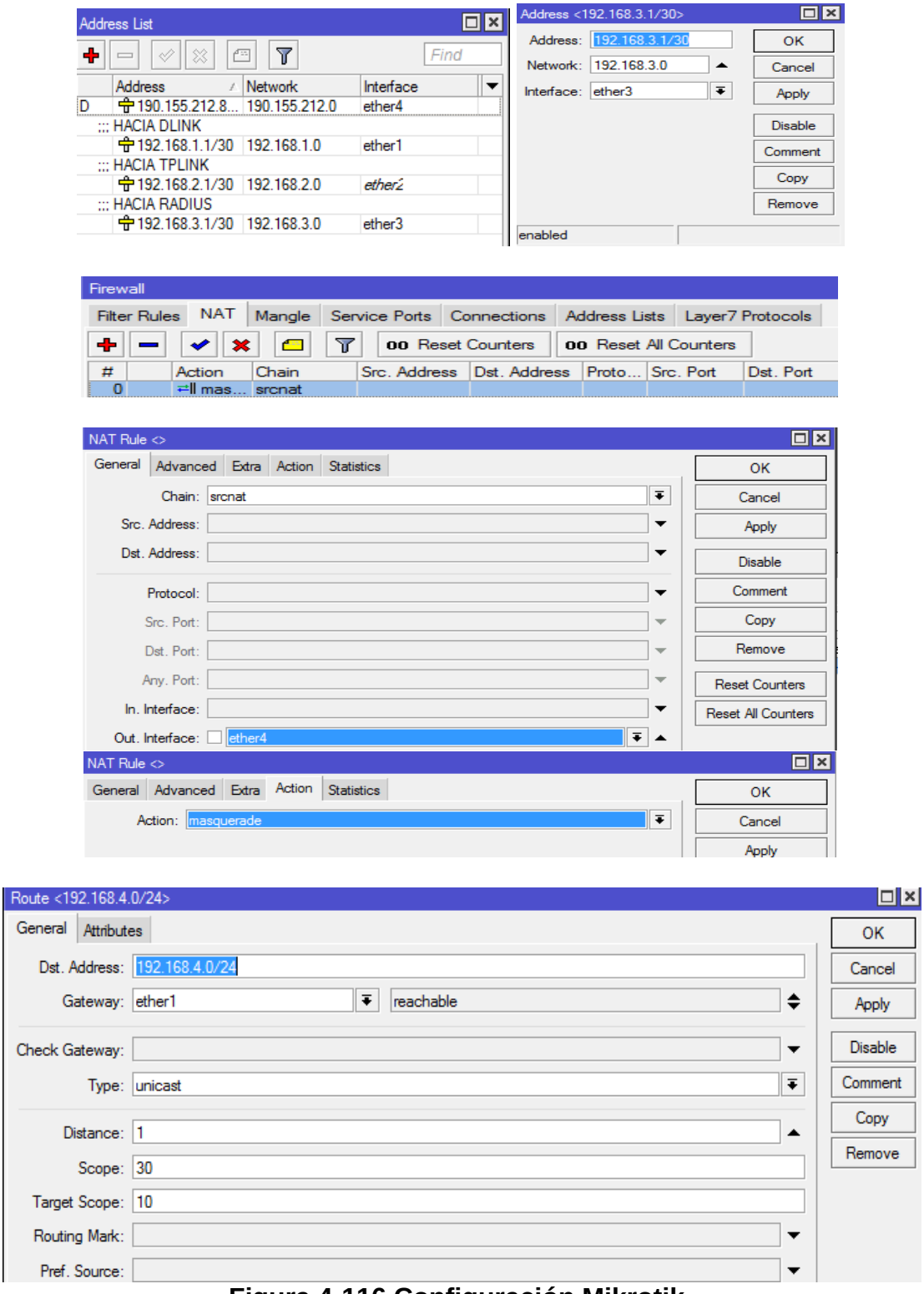


Figura 4-116 Configuración Mikrotik.

Una vez realizado la configuración del AP y del Router Mikrotik, procederemos a instalar el servidor RADIUS sobre Windows y realizaremos su respectiva configuración.

Figura 4-117 Instalación RADIUS.

Figura 4-118 Icono RADIUS.

En el menú de configuración de RADIUS, seleccionamos Edit Radius Client.conf, es aquí donde configuraremos la IP del servidor con la que se va a conectar para poder hacer la autenticación entre el usuario y el AP.

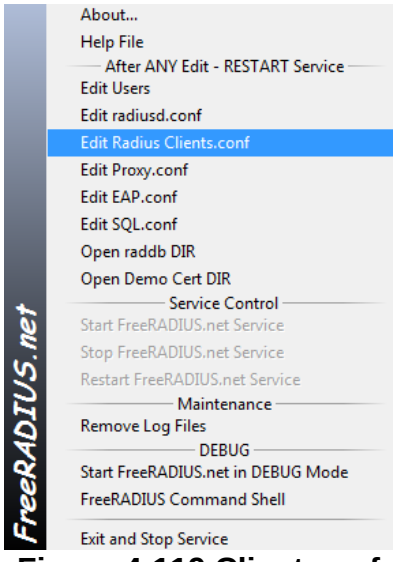


Figura 4-119 Client.conf

client 192.168.1.2/24 {

secret = 12345678

shortname = RADIUS }

client 192.168.2.2/24 {

secret = 12345678

shortname = RADIUS }

Posterior a esto debemos ingresaremos los usuarios y las claves de cada uno de las persona que se autenticarán a la red, esto lo realizamos editando el archivo user.conf.

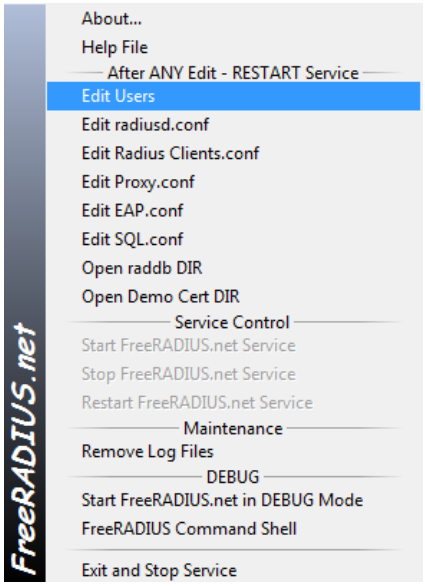


Figura 4-120 Edit Users.

Para poder añadir un nuevo usuario ingresamos lo siguiente:

user1 user-password = "user1"

Finalmente ponemos iniciamos el servicio de RADIUS dando clic en Start FreeRADIUS.net in DEBUG Mode.

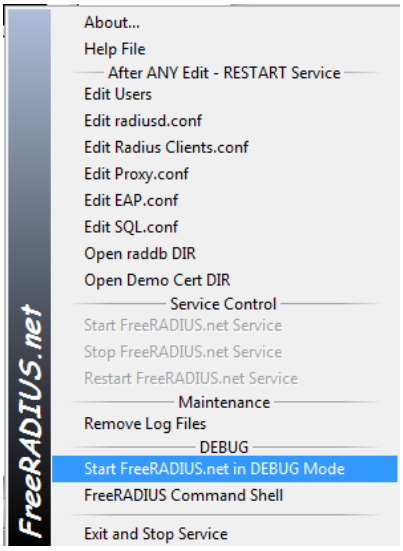


Figura 4-121 Inicio de servicio.

Verificación Wireshark.

Una vez realizada las configuraciones respectivas para este escenario procederemos a realizar la conexión de una estación en este caso una laptop a nuestra red, iniciaremos un sniffer desde la Estación para ver el proceso de autenticación, adiciona tendremos una tarjeta AirPcap Nx conectada para poder capturar el tráfico monocanal que podemos constatar en este escenario, adicional procederemos a analizar lo que ocurre al momento de que la estación intenta hacer esta conexión dentro de nuestro escenario. Podremos verificar la secuencia de las tramas que se tiene al momento de realizar la conexión.

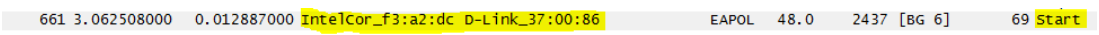


Figura 4-122 Trama 661 Start.

Podemos verificar que la Estación está iniciando una comunicación con el AP y se inicia una comunicación EAPOL, adicional podemos verificar el canal en el cual se está realizando esta conversación (BG 6 2437) y podemos verificar las MAC de los dispositivos involucrados. Continuando con el proceso de autenticación podemos verificar que se realiza un requerimiento de identidad desde el AP hacia la Estación y de la misma manera se tiene una respuesta de identidad desde la Estación hacia el AP.

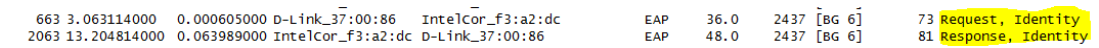
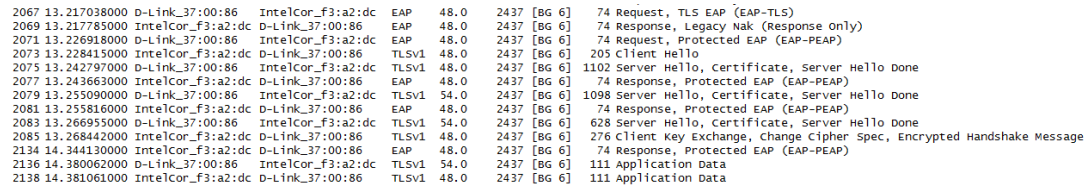


Figura 4-123 Requerimiento y Respuesta



2067	13.217038000	D-Link_37:00:86	IntelCor_f3:a2:dc	EAP	48.0	2437	[BG 6]	74	Request, TLS EAP (EAP-TLS)
2069	13.217785000	IntelCor_f3:a2:dc	D-Link_37:00:86	EAP	48.0	2437	[BG 6]	74	Response, Legacy Nak (Response Only)
2071	13.226918000	D-Link_37:00:86	IntelCor_f3:a2:dc	EAP	48.0	2437	[BG 6]	74	Request, Protected EAP (EAP-PEAP)
2073	13.228415000	IntelCor_f3:a2:dc	D-Link_37:00:86	TLSv1	48.0	2437	[BG 6]	205	Client Hello
2075	13.242797000	D-Link_37:00:86	IntelCor_f3:a2:dc	TLSv1	48.0	2437	[BG 6]	1102	Server Hello, Certificate, Server Hello Done
2077	13.243663000	IntelCor_f3:a2:dc	D-Link_37:00:86	EAP	48.0	2437	[BG 6]	74	Response, Protected EAP (EAP-PEAP)
2079	13.255090000	D-Link_37:00:86	IntelCor_f3:a2:dc	TLSv1	54.0	2437	[BG 6]	1098	Server Hello, Certificate, Server Hello Done
2081	13.255816000	IntelCor_f3:a2:dc	D-Link_37:00:86	EAP	48.0	2437	[BG 6]	74	Response, Protected EAP (EAP-PEAP)
2083	13.266955000	D-Link_37:00:86	IntelCor_f3:a2:dc	TLSv1	54.0	2437	[BG 6]	628	Server Hello, Certificate, Server Hello Done
2085	13.268442000	IntelCor_f3:a2:dc	D-Link_37:00:86	TLSv1	48.0	2437	[BG 6]	276	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2134	14.344130000	IntelCor_f3:a2:dc	D-Link_37:00:86	EAP	48.0	2437	[BG 6]	74	Response, Protected EAP (EAP-PEAP)
2136	14.380062000	D-Link_37:00:86	IntelCor_f3:a2:dc	TLSv1	54.0	2437	[BG 6]	111	Application Data
2138	14.381061000	IntelCor_f3:a2:dc	D-Link_37:00:86	TLSv1	48.0	2437	[BG 6]	111	Application Data

Figura 4-124 Proceso de Autenticación.

De acuerdo a lo verificado en la captura de paquetes realizado con la ayuda de Wireshark podemos tener una visión de la secuencia que realiza un usuario que quiere conectarse desde una Estación hacia uno de nuestros APs de la institución, como podemos ver se tiene una comunicación y un proceso de autenticación entre la estación y el AP, el mismo que se comunica con el servidor RADIUS para validar la información de autenticación que el cliente o usuario ingresa para poder registrarse en la red.

4.3.2. Calidad de Servicio.

El presente escenario es basado en el escenario 3 de la fase 1, se encuentra conformado por 2 AP configurados en canal 1 y canal 6 manteniendo la seguridad WPA y autenticación PSK, el propósito de evaluación de este escenario es poder verificar la calidad de canal que muestra la red en base al análisis de las tramas IEEE 802.11 y parámetros estadísticos obtenidos mediante la aplicación D-ITG así como resultados de reportes obtenidos de Steel Central Packet Analyzer.

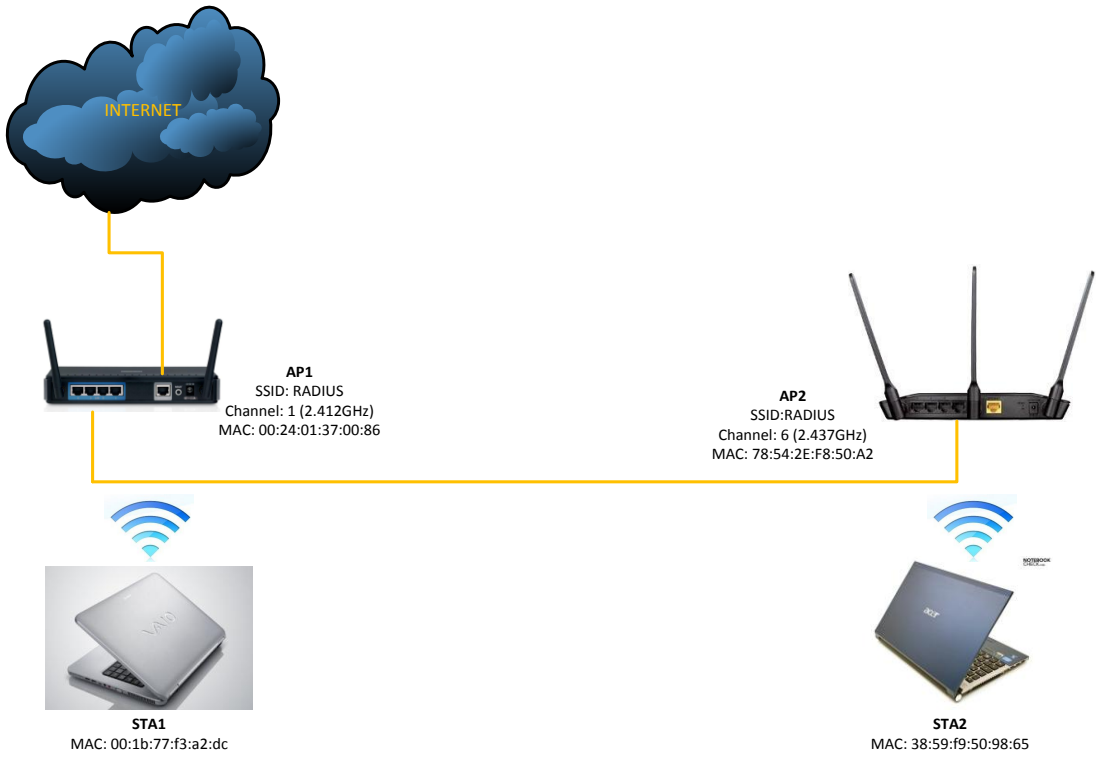


Figura 4-125 Escenario Verificación Calidad de Servicio.

Los equipos usados para la implementación de este escenario son los siguientes:

- Access Point D-Link DIR-619L
- Access Point D-Link DIR-615
- Tarjeta Inalámbrica Intel laptop Sony Vaio
- Tarjeta Inalámbrica laptop Acer
- AirPcap Nx Adapter

Tabla 44 Direccionamiento MAC

Dispositivo	INTERFAZ	MAC	FUNCION
STA1	Intel	00:1B:77:F3:A2:DC	Estación
STA2	Hacer	38:59:F9:50:98:65	Estación
AP1	Inalámbrica	00:24:01:37:00:86	Punto de Acceso
AP2	Inalámbrica	78:54:2E:F8:50:A2	Punto de Acceso

Como tendremos la presencia de un generador y receptor de flujo de tráfico D-ITG, procederemos a configurar un servidor NTP, para poder tener un sincronismo tanto en las Estaciones como en el servidor D-ITG montado

sobre Windows, con esta sincronización evitaremos tener inconsistencias de tiempo al momento de capturar el tráfico generado en el escenario.

Verificación Canal inSSIDer

Para poder iniciar con el análisis en este escenario realizaremos la inspección de la configuración de los canales de los APs, que con la ayuda de inSSIDer podemos verificar gráficamente en que canal se encuentran nuestros equipos configurados, mismos que deben estar configurados en el canal 1 y canal 6. Con esta herramienta podemos verificar también la intensidad de la señal de la red, el tipo de autenticación, la dirección MAC del AP, parámetros valiosos para poder obtener información de nuestra red.

Figura 4-126 Configuración de Canales AP.

Ya verificado los canales procedemos a determinar el comportamiento de red en presencia de gran cantidad de tráfico generado desde el programa D-ITG, tomando en cuenta que Wireshark debe encontrase levantado y realizando capturas en modo multicanal. Para el monitoreo multicanal se optó por la selección de la interfaz virtual AirPcap Multi-Channel Aggregator.

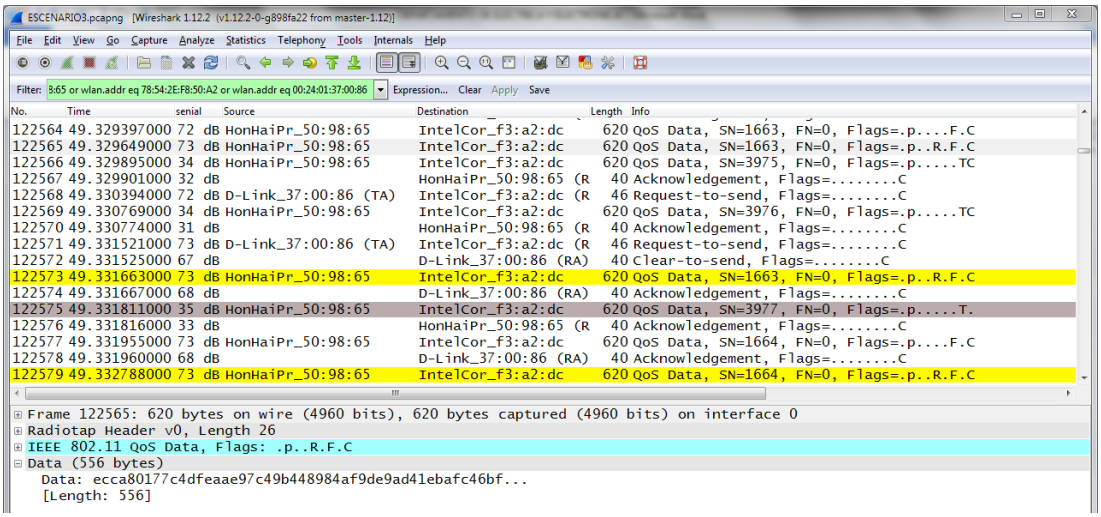


Figura 4-127 Captura de Paquetes en Wireshark.

Dentro de Wireshark podemos aplicar diferentes filtros para poder asociar información de nuestro interés y con esto verificar el comportamiento de nuestra red.

Filtro: *wlan.sa eq 38:59:f9:50:98:65 and wlan.da eq 00:1b:77:f3:a2:dc*

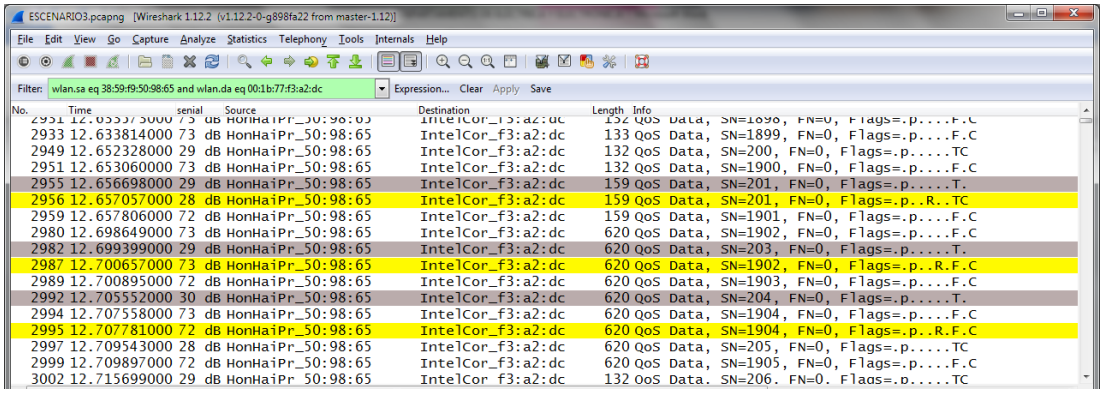
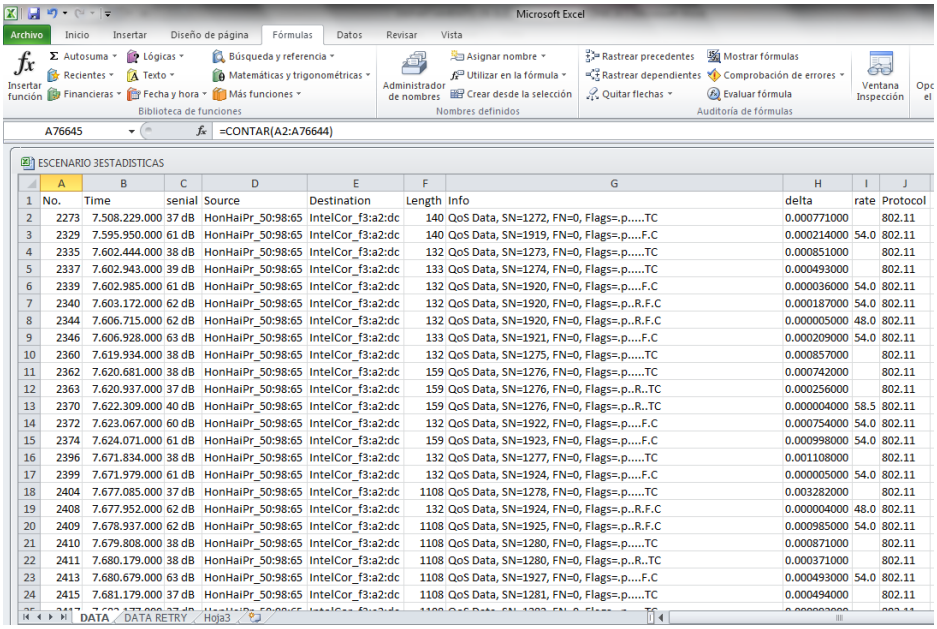


Figura 4-128 Filtro en Wireshark.

Mediante la aplicación del filtro en Wireshark, podemos obtener la comunicación cliente HonairPr_50:98:65 (STA2) servidor IntelCor_f3:a2:dc (STA1) para verificar de mejor manera la calidad del canal durante el envío de tráfico.



	A	B	C	D	E	F	G	H	I	J
1	No.	Time	senial	Source	Destination	Length	Info	delta	rate	Protocol
2	2273	7.508.229.000	37 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	140	QoS Data, SN=1272, FN=0, Flags=.p.....TC	0.000771000		802.11
3	2329	7.595.950.000	61 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	140	QoS Data, SN=1919, FN=0, Flags=.p....F.C	0.000214000	54.0	802.11
4	2335	7.602.444.000	38 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1273, FN=0, Flags=.p.....TC	0.000851000		802.11
5	2337	7.602.943.000	39 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	133	QoS Data, SN=1274, FN=0, Flags=.p.....TC	0.000493000		802.11
6	2339	7.602.985.000	61 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1920, FN=0, Flags=.p....F.C	0.000036000	54.0	802.11
7	2340	7.603.172.000	62 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1920, FN=0, Flags=.p..R.F.C	0.000187000	54.0	802.11
8	2344	7.606.715.000	62 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1920, FN=0, Flags=.p..R.F.C	0.000005000	48.0	802.11
9	2346	7.606.928.000	63 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	133	QoS Data, SN=1921, FN=0, Flags=.p....F.C	0.000209000	54.0	802.11
10	2360	7.619.934.000	38 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1275, FN=0, Flags=.p.....TC	0.000857000		802.11
11	2362	7.620.681.000	38 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	159	QoS Data, SN=1276, FN=0, Flags=.p.....TC	0.000742000		802.11
12	2363	7.620.937.000	37 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	159	QoS Data, SN=1276, FN=0, Flags=.p..R..TC	0.000256000		802.11
13	2370	7.622.309.000	40 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	159	QoS Data, SN=1276, FN=0, Flags=.p..R..TC	0.000004000	58.5	802.11
14	2372	7.623.067.000	60 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1922, FN=0, Flags=.p....F.C	0.000754000	54.0	802.11
15	2374	7.624.071.000	61 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	159	QoS Data, SN=1923, FN=0, Flags=.p....F.C	0.000998000	54.0	802.11
16	2396	7.671.834.000	38 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1277, FN=0, Flags=.p.....TC	0.001108000		802.11
17	2399	7.671.979.000	61 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1924, FN=0, Flags=.p....F.C	0.000005000	54.0	802.11
18	2404	7.677.085.000	37 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	1108	QoS Data, SN=1278, FN=0, Flags=.p.....TC	0.003282000		802.11
19	2408	7.677.952.000	62 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	132	QoS Data, SN=1924, FN=0, Flags=.p..R.F.C	0.000004000	48.0	802.11
20	2409	7.678.937.000	62 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	1108	QoS Data, SN=1925, FN=0, Flags=.p..R.F.C	0.000985000	54.0	802.11
21	2410	7.679.808.000	38 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	1108	QoS Data, SN=1280, FN=0, Flags=.p.....TC	0.000871000		802.11
22	2411	7.680.179.000	38 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	1108	QoS Data, SN=1280, FN=0, Flags=.p..R..TC	0.000371000		802.11
23	2413	7.680.679.000	63 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	1108	QoS Data, SN=1927, FN=0, Flags=.p....F.C	0.000493000	54.0	802.11
24	2415	7.681.179.000	37 dB	HonHaiPr_50:98:65	IntelCor_f3:a2:dc	1108	QoS Data, SN=1281, FN=0, Flags=.p.....TC	0.000494000		802.11

Figura 4-129 Datos de filtrado en Excel.

Ya procesado en Excel las tramas, se verifica un total de 76643 paquetes y un total de 17759 reintentos.

Tabla 45 Tráfico enfocado a la red RADIUS

SSID	Total Bytes	Total Packets
RADIUS	76,710,406	74,525

Tabla 46 Tráfico por host transmisor red RADIUS

Source MAC	Total Bytes	Total Packets
38:59:f9:50:98:65	75,738,664	82,307
00:24:01:37:00:86	969,877	10,81
78:54:2e:f8:50:a2	370,286	1,452
00:1b:77:f3:a2:dc	52,251	528

Tabla 47 Trafico por host receptor red RADIUS

Destination MAC	Total Bytes	Total Packets
00:1b:77:f3:a2:dc	75,818,709	77,616
38:59:f9:50:98:65	542,656	35,634
00:24:01:37:00:86	522,201	33,591
78:54:2e:f8:50:a2	280,173	12,581

Tabla 48 Nivel de señal y ruido por host

Source	Signal Avg (dBm)	Noise Avg (dBm)
IntelCorpo_f3:a2:dc	-14	-81
D-Link_37:00:86	-19	-81
b4:52:7d:36:db:7b	-32	-82
38:59:f9:50:98:65	-36	-84
78:54:2e:f8:50:a2	-40	-86

Tabla 49 Retransmisiones por host

Source	Total Bits	Total Packets
38:59:f9:50:98:65	140,619,688	16,34
00:24:01:37:00:86	1,480,728	554
00:1b:77:f3:a2:dc	183,512	238
78:54:2e:f8:50:a2	31,408	17

Tabla 50 Paquetes Estación STA1

Hierarchy (Subtype)	Bits/s	Total Bits	Packets/s	Total Packets
Subtype: Data	27,28	6,984	0,01	3
Subtype: Probe Request	22,69	5,808	0,06	15
Subtype: Probe response	280,22	71,736	0,14	35
Subtype: QoS Data	2,37M	605,641,264	274,7	70,324
Subtype: QoS Null (no data)	144,38	36,96	0,6	154
Subtype: RTS	9,17K	1,174,240	57,34	7,339

Tabla 51 Paquetes estación STA2

Hierarchy (Subtype)	Bits/s	Total Bits	Packets/s	Total Packets
Subtype: Block Ack (BlockAck)	45,42	5,632	0,18	22
Subtype: Data	174,19	43,2	0,18	44
Subtype: Probe Request	32,42	8,04	0,04	9
Subtype: Probe response	305,13	75,672	0,13	32
Subtype: QoS Data	2,44M	604,195,088	283,07	70,202
Subtype: QoS Null (no data)	58,06	7,2	0,24	30
Subtype: RTS	15,71K	1,947,680	98,17	12,173

Las tablas anteriores muestran el comportamiento del canal en si ya que las estaciones se comunicaban a través de la red RADIUS la cual presenta para el caso de STA2 82000 paquetes enviados y la retransmisión de 16 paquetes ocupando un ancho de banda de 2.44Mbps. Adicionalmente l nivel promedio de señal para STA2 es de -36dBm nivel de señal bueno tomando que STA2 está asociado a AP2 mismo que muestra un nivel de señal de -40dBm.

En el caso de la estación receptora STA1 se verifica que de 1452 paquetes enviados por dicha estación se retransmitieron 238 paquetes considerándose un valor elevado respecto a STA1. Finalmente al verificar la cantidad de datos enviados por segundo en STA1 y STA2 el promedio es de 2Mbps.

En este escenario al igual que los escenarios implementados en la Fase 1 podemos verificar las tramas que son enviadas a nivel del canal y verificar tramas como Beacon, adicional verificamos que en los intentos efectuados con el generador de tráfico se tiene datos un tanto similares teniendo como premisa que el escenario no está bajo la presencia de un canal o AP que tenga interferencia en los canales de nuestros equipos configurados.

En este escenario hemos usado las herramientas inSSIDer, Wireshark y SteelCentral Packet Analyzer, en donde verificamos la configuración de los canales de los APs, generamos tráfico y sacamos una estadística del comportamiento del canal en diferentes pruebas realizadas y en Wireshark podemos verificar las tramas 802.11 que son involucradas como de la asociación, re asociación de las Estaciones en los APs.

4.3.3. WDS

El presente escenario está conformado por 2 Access Point conectados inalámbricamente y configurados en 2437 GHz y dos estaciones que se

conectan a los Access Point de acuerdo al esquema que se detalla a continuación, para poder tener acceso a la red implementada.

El propósito de la evaluación de este tipo de escenarios es poder verificar cómo se comporta una red en donde sus Punto de Acceso se conectan inalámbricamente, en un sistema WDS haciendo a un AP que opere como estación (D-Link DIR-619L) y el otro AP como Bridge (AP TP-Link), se puede verificar que efecto produce esta conexión a nivel de Calidad de servicio (QoS) para poder unir los dos AP en la red. El adaptador AirPcap NX estará conectado en una estación donde se estará capturando el tráfico de la red.

Figura 4-130 Escenario WDS.

Dentro de este escenario usaremos los siguientes dispositivos para poder implementar el diagrama expuesto anteriormente.

- Access Point D-Link DIR-619L
- Access Point TP-Link WR541G

- Tarjeta Inalámbrica Intel Laptop Sony Vaio
- Tarjeta Inalámbrica Atheros Laptop Acer
- AirPcap Nx Adapter

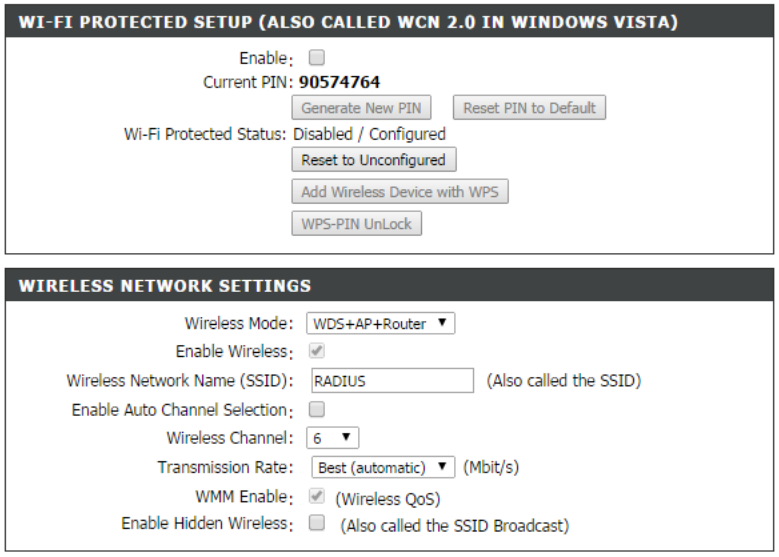
Tabla 52 Direccionamiento MAC Escenario 6.

Dispositivo	INTERFAZ	MAC	FUNCION
AP1	Inalámbrica	78:54:2E:F8:50:A2	Punto de Acceso
AP2	Inalámbrica	00:1D:0F:D6:F1:7A	Punto de Acceso
STA	Intel	00:1B:77:F3:A2:DC	Estación
STA	Atheros	38:59:F9:50:98:65	Estación

Configuración Equipos de Red.

Para poder realizar el análisis del presente escenario debemos configurar los Puntos de Acceso en el mismo canal para poder conectarlos inalámbricamente entre sí, las estaciones se conectarán a los Puntos de Acceso correspondientes y se tendrá conexión en la red y el medio de transporte de los paquetes será el aire.

Para poder confirmar la configuración de los equipos podemos ingresarnos a la administración de los AP y verificar dicha configuración adicional usaremos inSSIDer para verificar gráficamente la configuración de los canales de los AP.



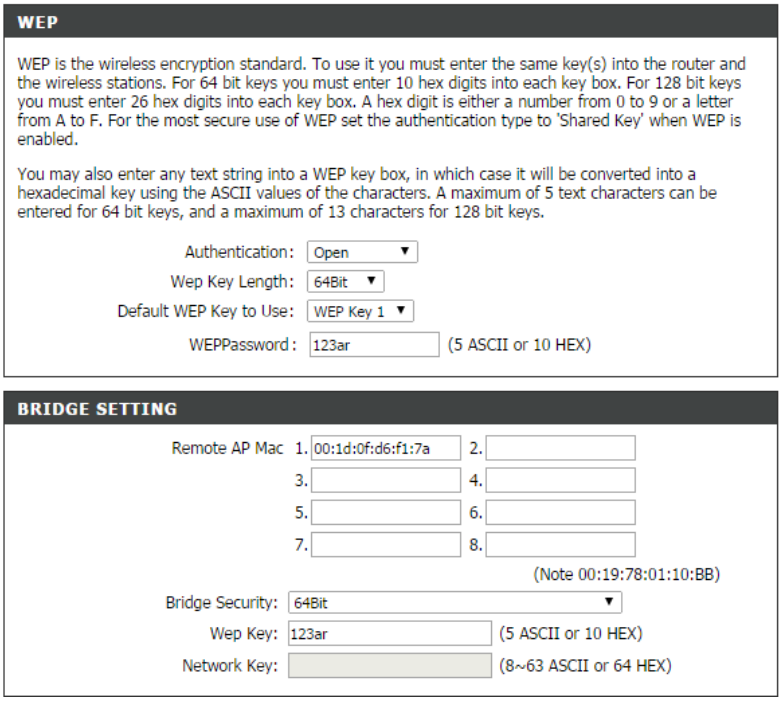
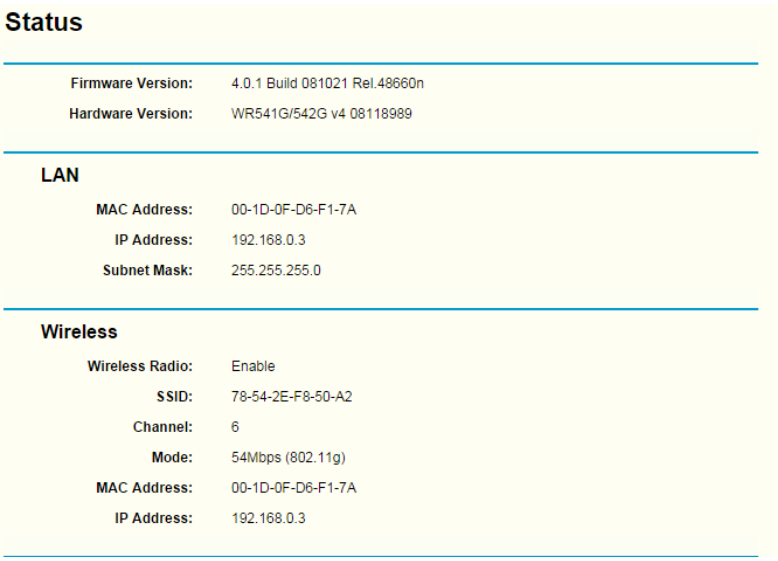


Figura 4-131 Configuración AP D-Link DIR-619L.



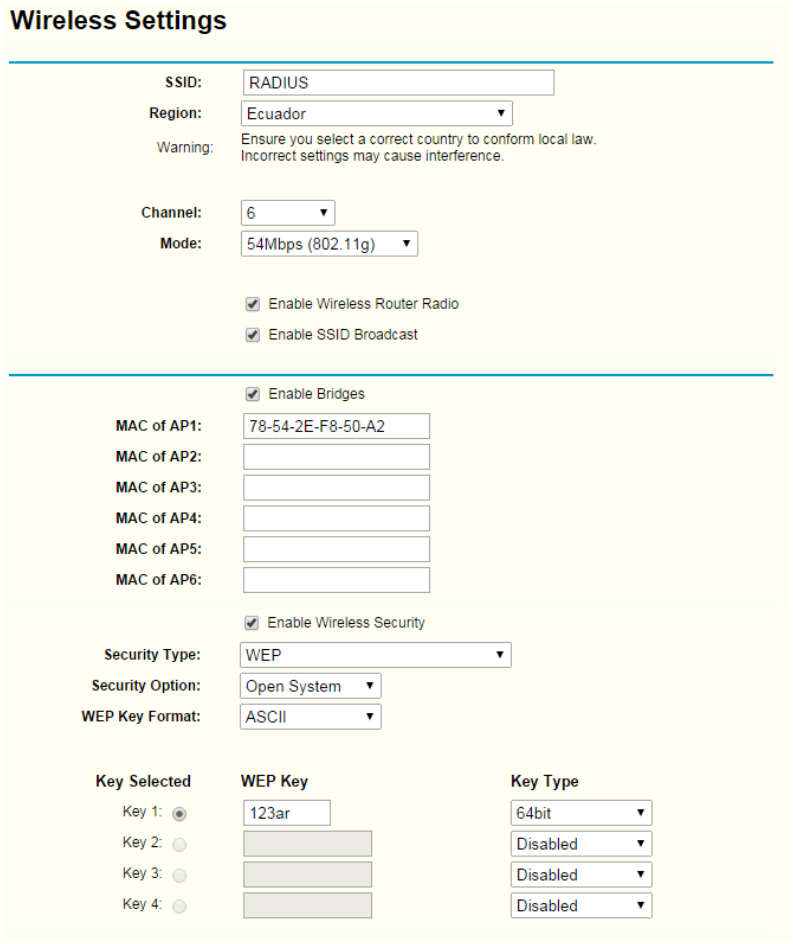


Figura 4-132 Configuración AP TP-Link.

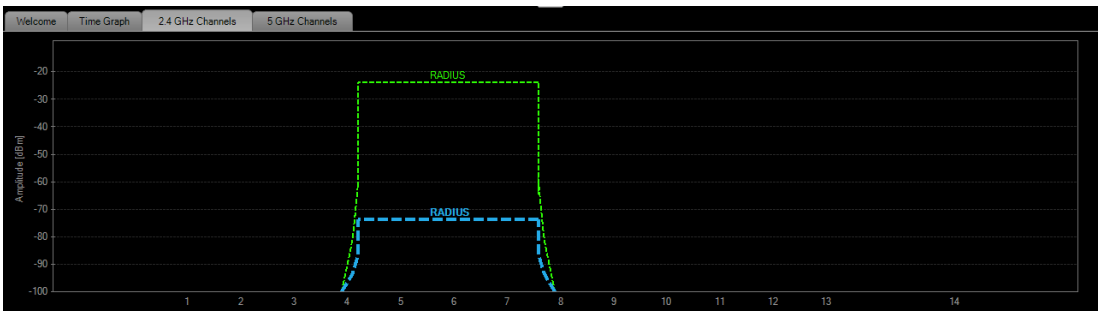


Figura 4-133 Canales AP Escenario WDS.

En la figura podemos verificar que los AP están configurados en el canal 6 (2437 GHz).

Con la generación de tráfico realizada desde el servidor D-ITG, podemos realizar un sin número de pruebas y verificar el comportamiento que se presenta en el escenario teniendo un medio de comunicación inalámbrico, en la tabla podremos verificar los valores de las pruebas realizadas y

podemos verificar que en este medio inalámbrico se tiene porcentajes de pérdida de paquetes que es característico por el medio de comunicación.

Tabla 53 Pruebas Escenario 6.

Test	Tiempo (s)	Packets	Bitrate promedio (Kbit/s)	Delay Promedio (s)	Jitter Promedio (s)	Paquetes descartados (%)
1	62.0826	33092	4264.24	0.5628	0.0017	18.49
2	60.3134	34195	4535.63	0.2187	0.0016	15.53
3	60.2569	34566	4589.14	0.3438	0.0018	16.06

A continuación podremos ver las tablas de resumen de la generación de tráfico realizado desde D-ITG, y las gráficas obtenidas de la tasa promedio, el retardo y el jitter como el porcentaje de paquetes perdidos, esto valores debemos tener en cuenta que se trata de los paquetes que son dirigidos desde una estación a otra, por ende estamos probando y analizando todo el canal tanto entre la comunicación de los AP como la comunicación de los APs a las Estaciones.

```
Total time                =     62.082696 s
Total packets             =         33092
Minimum delay             =     -0.005771 s
Maximum delay             =      3.881310 s
Average delay             =      0.562826 s
Average jitter            =      0.001798 s
Delay standard deviation  =      0.705958 s
Bytes received            =      33092000
Average bitrate           =   4264.247803 Kbit/s
Average packet rate       =    533.030975 pkt/s
Packets dropped           =          7509 (18.49 %)
Average loss-burst size   =      5.053163 pkt
```

Figura 4-134 Resultados Prueba 1.

```
Total time                =     60.313447 s
Total packets             =         34195
Minimum delay             =     -0.018315 s
Maximum delay             =      0.584590 s
Average delay             =      0.218758 s
Average jitter            =      0.001616 s
Delay standard deviation  =      0.167543 s
Bytes received            =      34195000
Average bitrate           =   4535.638628 Kbit/s
Average packet rate       =    566.954828 pkt/s
Packets dropped           =          6287 (15.53 %)
Average loss-burst size   =      3.518187 pkt
```

Figura 4-135 Resultados Prueba 2.

```
Total time                =     60.256949 s
Total packets             =         34566
Minimum delay             =      0.025529 s
Maximum delay             =      0.878199 s
Average delay             =      0.343837 s
Average jitter            =      0.001801 s
Delay standard deviation  =      0.170346 s
Bytes received            =      34566000
Average bitrate           =   4589.147054 Kbit/s
Average packet rate       =    573.643382 pkt/s
Packets dropped           =          6615 (16.06 %)
Average loss-burst size   =      3.722566 pkt
Error lines               =             0
```

Figura 4-136 Resultados Prueba 3.

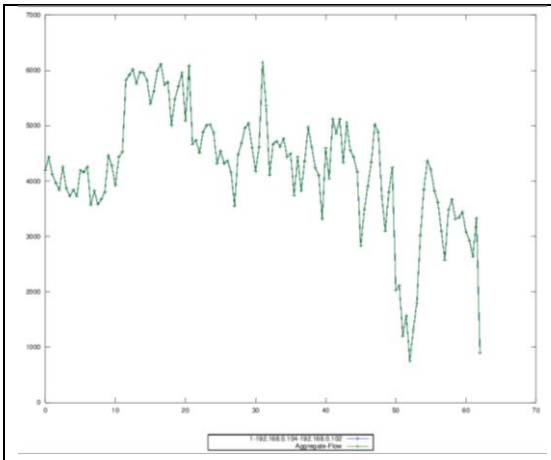


Figura 4-137 Bitrate Prueba 1.

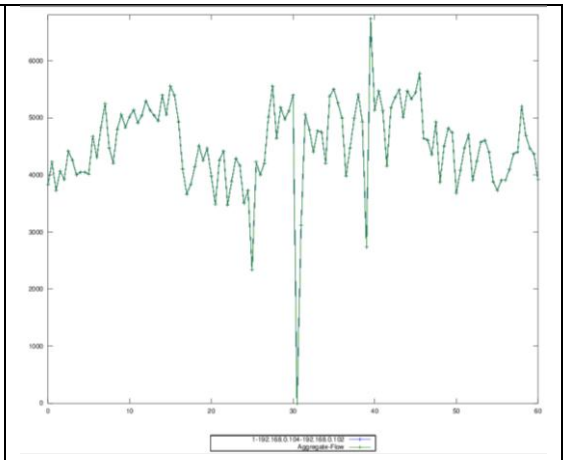


Figura 4-138 Bitrate Prueba 2.

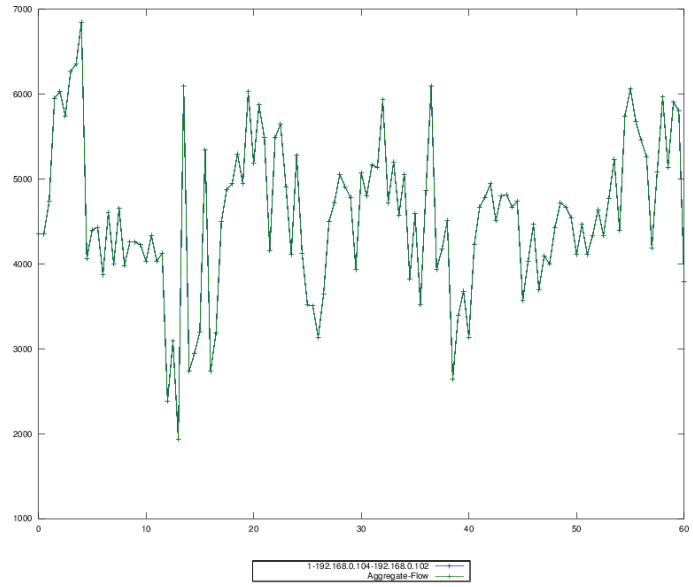


Figura 4-139 Bitrate Prueba 3.

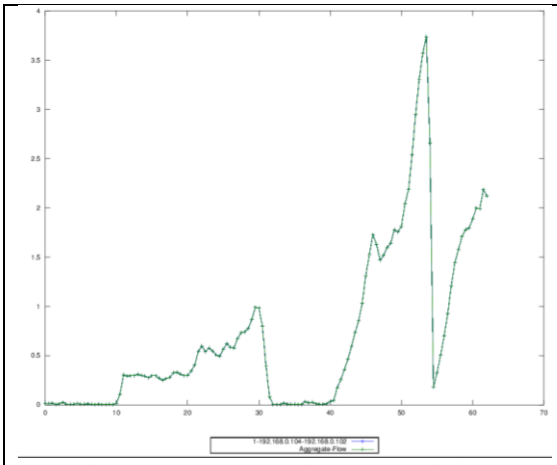


Figura 4-140 Delay Prueba 1.

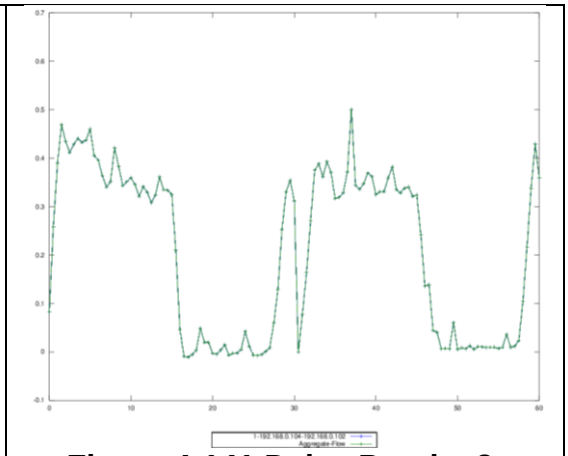


Figura 4-141 Delay Prueba 2.

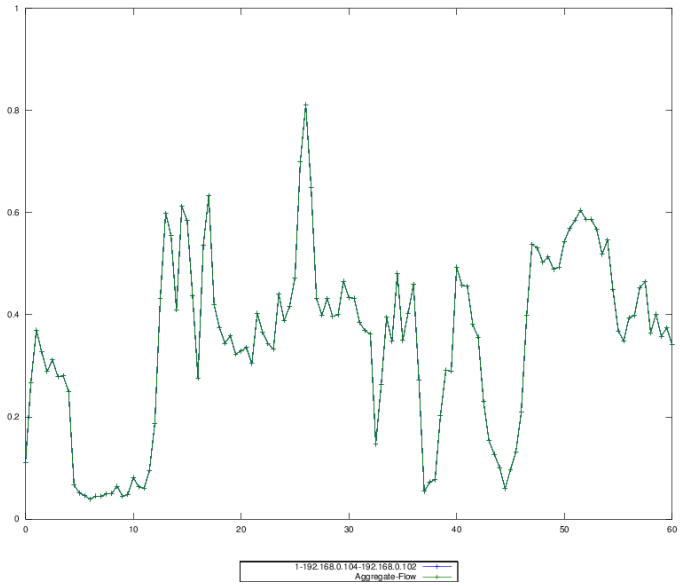


Figura 4-142 Delay Prueba 3.

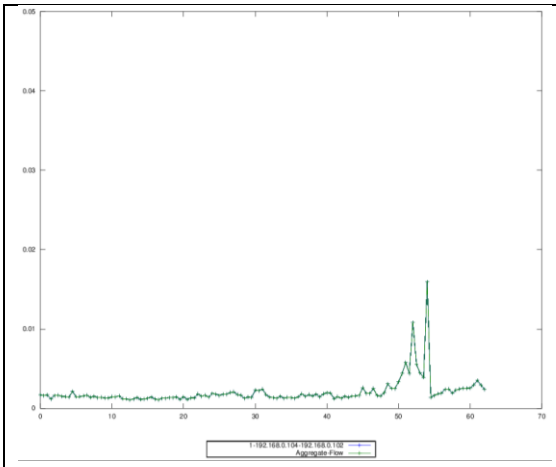


Figura 4-143 Jitter Prueba 1.

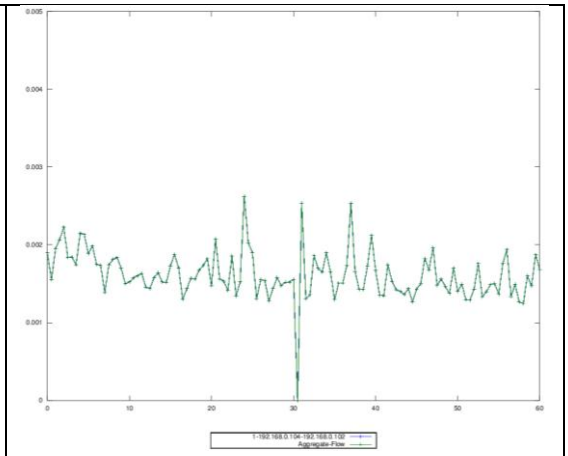


Figura 4-144 Prueba 2.

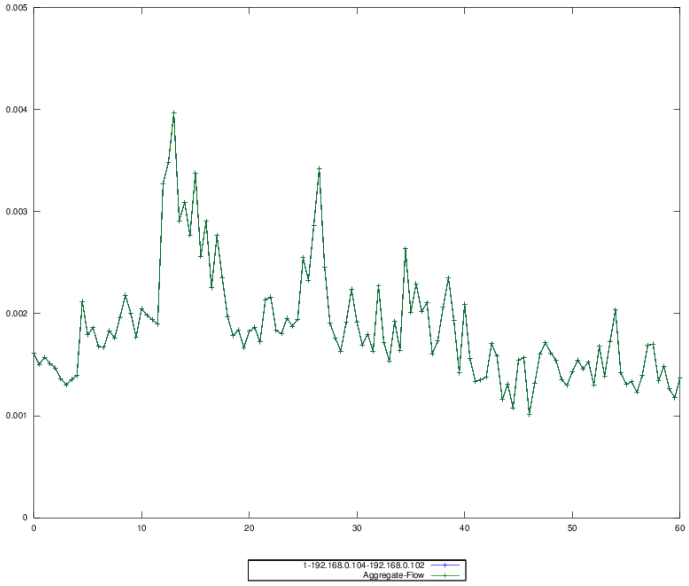


Figura 4-145 Prueba 3.

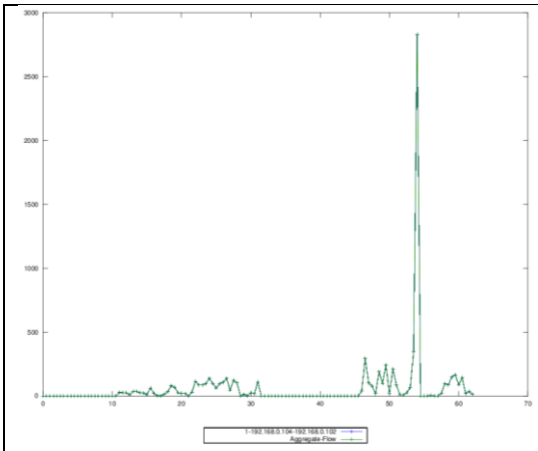


Figura 4-146 Packetloss Prueba 1.

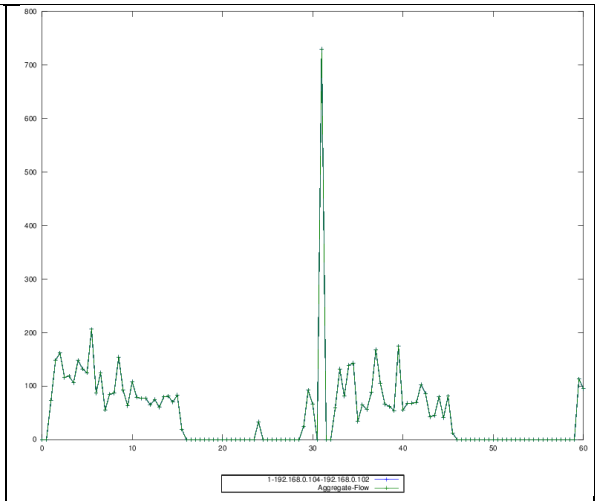


Figura 4-147 Packetloss Prueba 2.

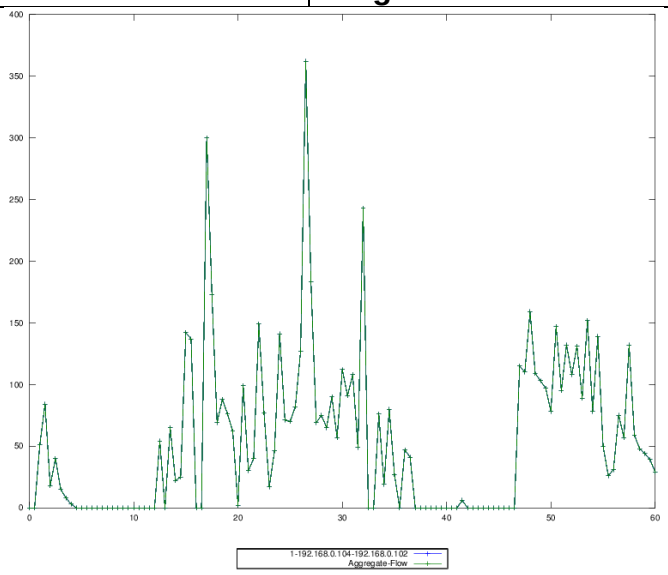


Figura 4-148 Packetloss Prueba 3.

Con los datos obtenidos en este escenario, luego de haber realizado la generación de paquetes podemos verificar ciertos valores que nos permiten conocer el estado y comportamiento de nuestra red Inalámbrica al momento de tener una comunicación entre las estaciones.

El Delay el jitter y el Bitrate promedio en las pruebas realizadas son similares, teniendo como resultado que el medio no tiene presencia de interferencia, por lo que el comportamiento de la comunicación entre los AP es buena, lo que podemos verificar es que se tiene una pérdida de paquetes pero este valor en las pruebas empleadas son similares, dichos valores son normales en comparación con un escenario con presencia de interferencia

ya que el medio por el que se están dirigiendo los paquetes es el aire y por las características de las antenas de los equipos se pude tener esta pérdida de paquetes, normal en un medio inalámbrico.

Lo importante es que no se tiene presencia de tiempos de latencia altos, lo que hace que el paquete llegue a su destino en un tiempo considerablemente corto en comparación cuando se tiene un ambiente con interferencia que lo analizaremos a continuación.

4.3.4. Interferencia

Para poder tratar este tema vamos a tratar dos escenarios sumamente similares pero que a la final nos daremos cuenta que el canal por el que los APs se conectan afecta en cada uno de ellos y más si se tiene la presencia de un AP que interfiere en los canales que nuestros equipos están configurados.

El primer escenario está conformado por 3 Access Point conectados mediante Ethernet y configurados en 2412 GHz, 2422 GHz y 2437 GHz respectivamente, y dos estaciones que se conectan a los Access Point de acuerdo a la Esquema que se detalla a continuación, para poder tener acceso a la red implementada.

El propósito de evaluación en este escenario es poder verificar cómo se comporta una red inalámbrica con varios Puntos de Acceso los mismos que tienen la presencia de interferencia que produce el Punto de Acceso conectado en medio de sus extremos. Adicional a esta interferencia que se presenta, se puede verificar que efecto produce este parámetro a nivel de QoS en dicho escenario.

El adaptador AirPcap NX estará conectado en una estación donde se estará capturando el tráfico de la red.

El análisis se lo realizará únicamente con la obtención de los resultados de la generación de paquetes de D-ITG.

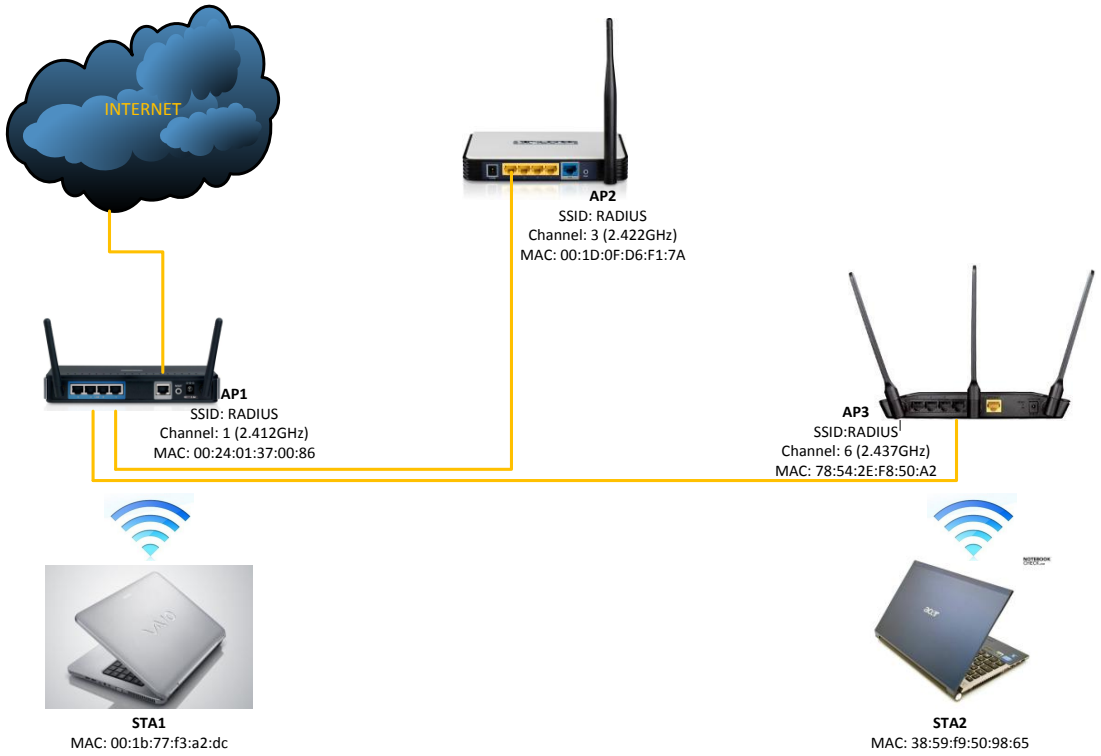


Figura 4-149 Escenario Interferencia Ethernet.

En la implementación del siguiente escenario se usarán los siguientes equipos:

- Access Point D-Link DIR-615
- Access Point D-Link DIR-619L
- Access Point TP-Link WR541G (Interferencia)
- Tarjeta Inalámbrica Intel Laptop Sony Vaio
- Tarjeta Inalámbrica Atheros Laptop Acer
- AirPcap Nx Adapter

Tabla 54 Direccionamiento MAC Escenario Interferencia Ethernet.

Dispositivo	INTERFAZ	MAC	FUNCION
AP1	Inalámbrica	00:24:01:37:00:86	Punto de Acceso
AP2	Inalámbrica	00:1D:0F:D6:F1:7A	Punto de Acceso
AP3	Inalámbrica	78:54:2E:F8:50:A2	Punto de Acceso
STA1	Intel	00:1B:77:F3:A2:DC	Estación
STA2	Atheros	38:59:F9:50:98:65	Estación

Verificación de canales inSSIDer

En base a los escenarios expuestos anteriormente, se ha indicado como configurar cada uno de los Puntos de Acceso, por tal motivo no se realizará esta explicación nuevamente, se debe configurar cada uno de los Puntos de Acceso de acuerdo al Diagrama presentado anteriormente, se usa la herramienta InSSIDer para poder confirmar en que canal se encuentran configurados nuestros equipos (RADIUS), con esto podemos confirmar que se tengas los 3 Puntos de acceso configurados en sus respectivos canales y que uno de ellos esté interfiriendo el canal de los otros 2.

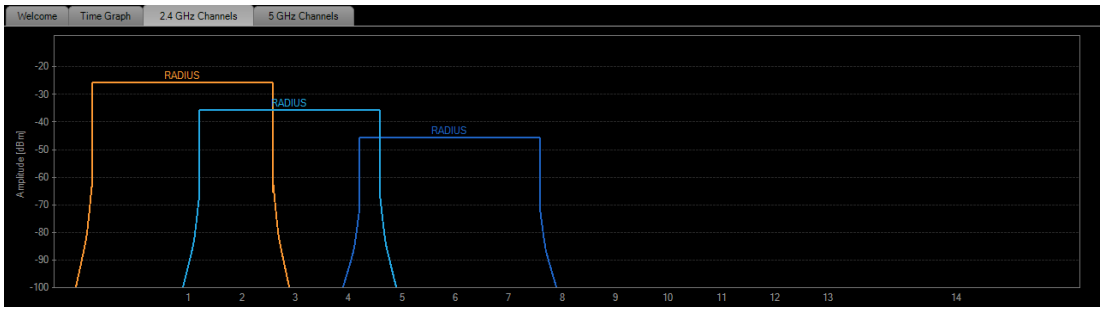


Figura 4-150 Canales AP Escenario 5.

En la Figura podemos verificar que nuestros equipos están configurados en el canal 1, 3 y 6 siendo el equipo configurado en el canal 3 AP2 (TP-Link) es quien produce interferencia a los otros dos AP.

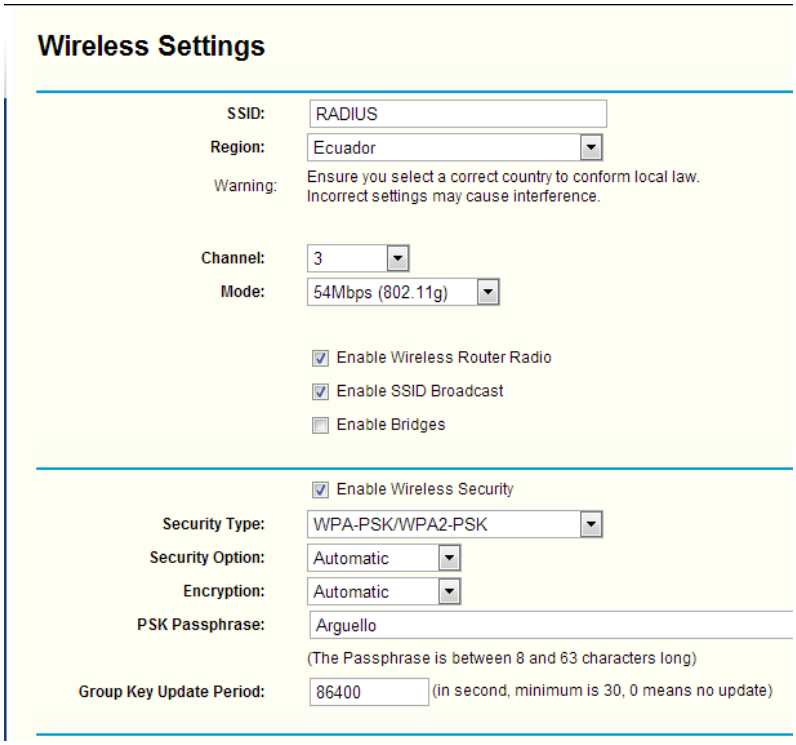


Figura 4-151 Configuración AP TP-Link (AP de Interferencia).

Generación Tráfico D-ITG.

Se procede a configurar el generador de tráfico D-ITG para poder enviar paquetes desde una estación configurada como servidor a otra configurada como cliente, se realizan 4 pruebas del mismo escenario para poder verificar el comportamiento y se tiene los siguientes valores colocados en la tabla.

Tabla 55 Pruebas Escenario 5.

Test	Tiempo (s)	Packets	Delay Promedio (s)	Jitter Promedio (s)	Bitrate promedio (Kbit/s)	Paquetes descartados (%)
1	228.5859	30450	5.0032	0.0136	1065.68	80.21
2	59.9500	41654	0.0347	0.0021	5558.49	1.65
3	59.9698	40240	-0.1840	0.0019	5368.02	3.32
4	60.5653	31017	1.1360	0.0029	4096.99	23.95

```
Total time                =    228.585956 s
Total packets             =         30450
Minimum delay             =     -0.358173 s
Maximum delay             =     21.998762 s
Average delay             =      5.003205 s
Average jitter            =      0.013612 s
Delay standard deviation  =      5.700336 s
Bytes received            =      30450000
Average bitrate           =   1065.682268 Kbit/s
Average packet rate       =    133.210283 pkt/s
Packets dropped           =        123377 (80.21 %)
Average loss-burst size   =     17.455716 pkt
```

Figura 4-152 Resultados Prueba 1

```
Total time                =     59.950005 s
Total packets             =         41654
Minimum delay             =     -0.037026 s
Maximum delay             =      0.542858 s
Average delay             =      0.034772 s
Average jitter            =      0.002152 s
Delay standard deviation  =      0.078035 s
Bytes received            =      41654000
Average bitrate           =   5558.498285 Kbit/s
Average packet rate       =    694.812286 pkt/s
Packets dropped           =           699 (1.65 %)
Average loss-burst size   =     17.475000 pkt
```

Figura 4-153 Resultados Prueba 2

```
Total time                =     59.969877 s
Total packets             =         40240
Minimum delay             =     -0.230697 s
Maximum delay             =      0.401030 s
Average delay             =     -0.184062 s
Average jitter            =      0.001939 s
Delay standard deviation  =      0.060316 s
Bytes received            =       40240000
Average bitrate           =   5368.028352 Kbit/s
Average packet rate       =    671.003544 pkt/s
Packets dropped           =          1381 (3.32 %)
Average loss-burst size   =     32.116279 pkt
```

Figura 4-154 Resultados Prueba 3

```
Total time                =     60.565343 s
Total packets             =         31017
Minimum delay             =     -0.144954 s
Maximum delay             =      2.464382 s
Average delay             =      1.136046 s
Average jitter            =      0.002955 s
Delay standard deviation  =      0.709795 s
Bytes received            =       31017000
Average bitrate           =   4096.996528 Kbit/s
Average packet rate       =    512.124566 pkt/s
Packets dropped           =          9769 (23.95 %)
Average loss-burst size   =      8.487402 pkt
```

Figura 4-155 Resultados Prueba 4

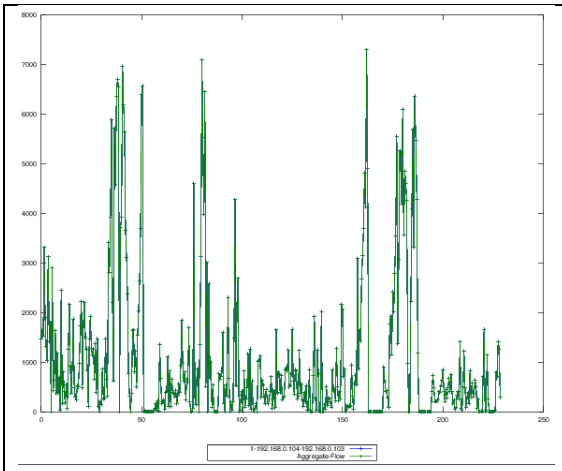


Figura 4-156 Bitrate Prueba 1

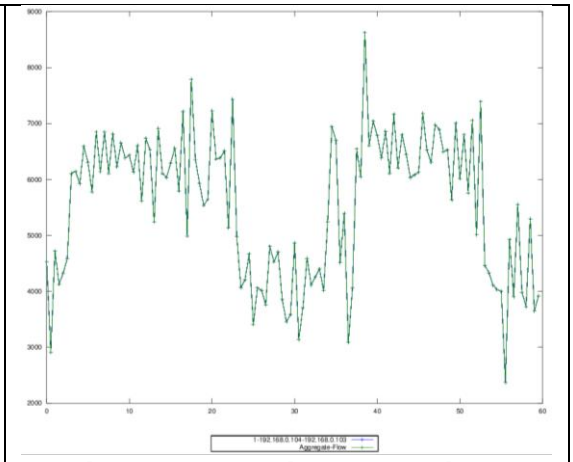


Figura 4-157 Bitrate Prueba 2

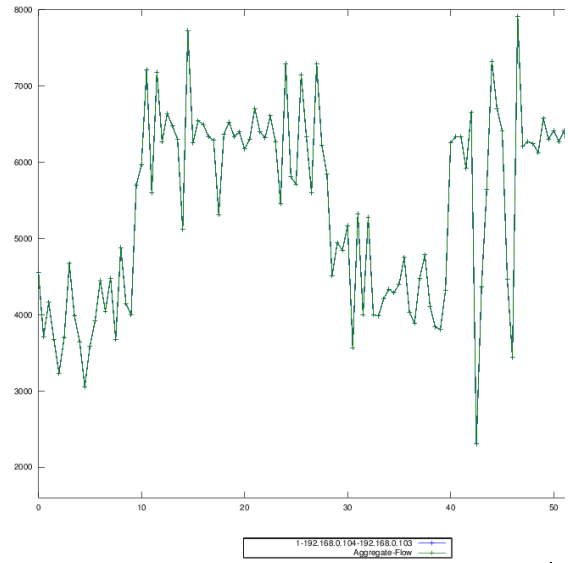


Figura 4-158 Bitrate Prueba 3

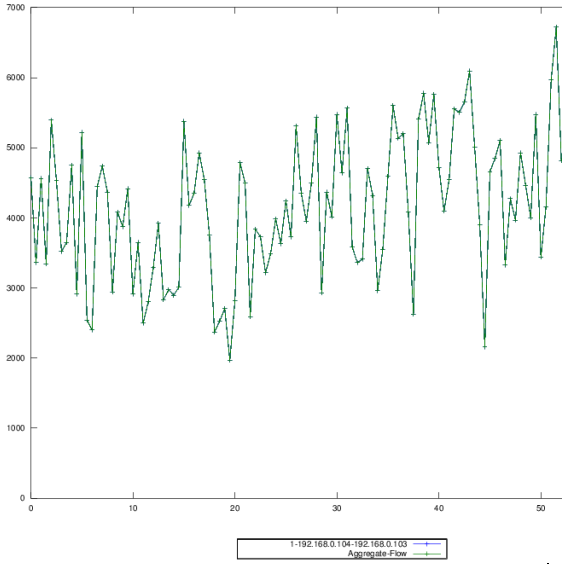


Figura 4-159 Bitrate Prueba 4

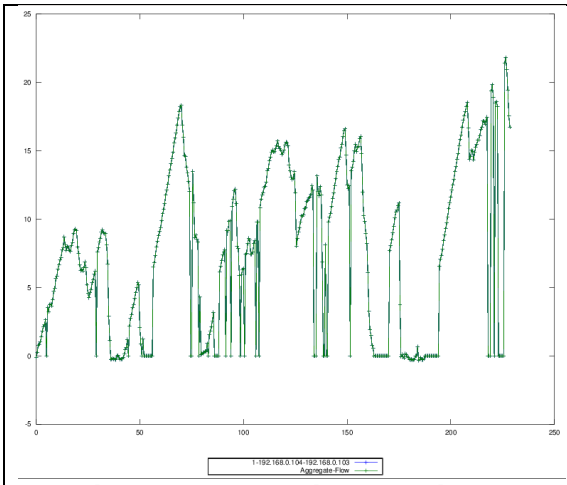


Figura 4-160 Delay Prueba 1

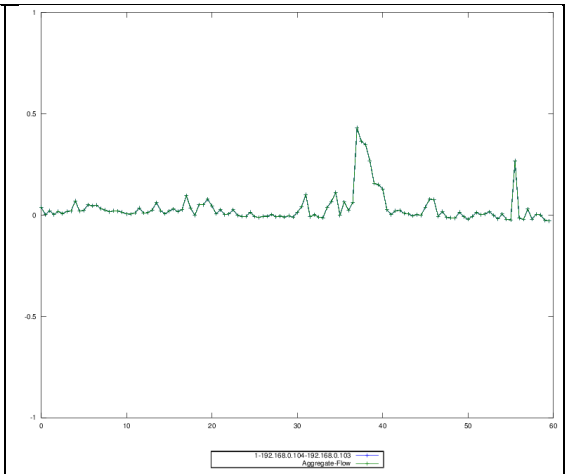


Figura 4-161 Delay Prueba 2

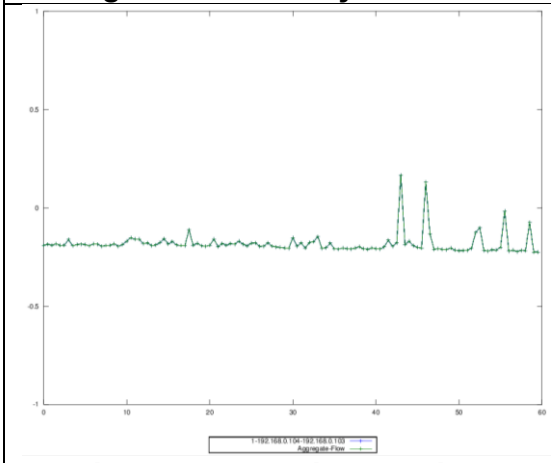


Figura 4-162 Delay Prueba 3

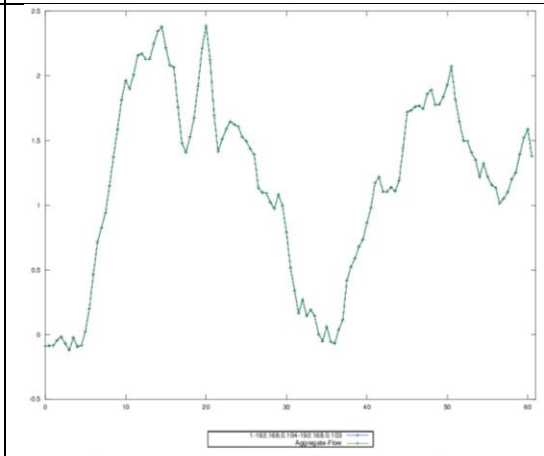


Figura 4-163 Delay Prueba 4

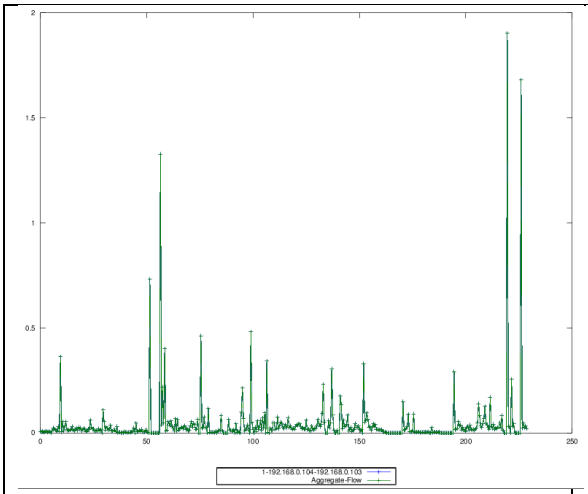


Figura 4-164 Jitter Prueba 1

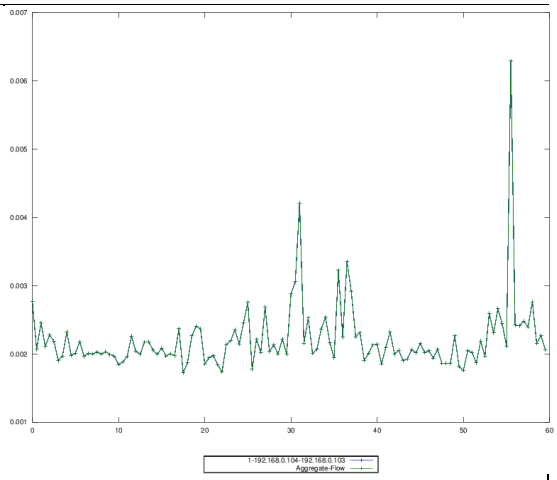


Figura 4-165 Jitter Prueba 2

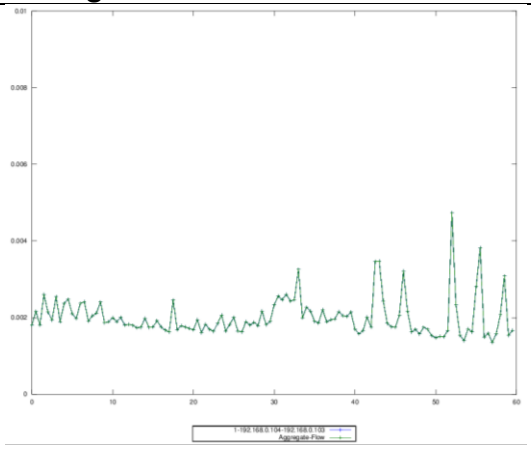


Figura 4-166 Jitter Prueba 3

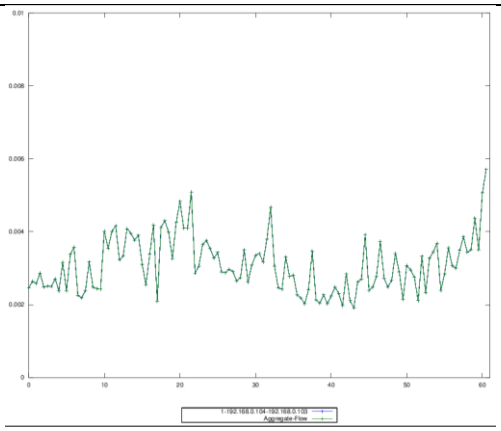


Figura 4-167 Jitter Prueba 4

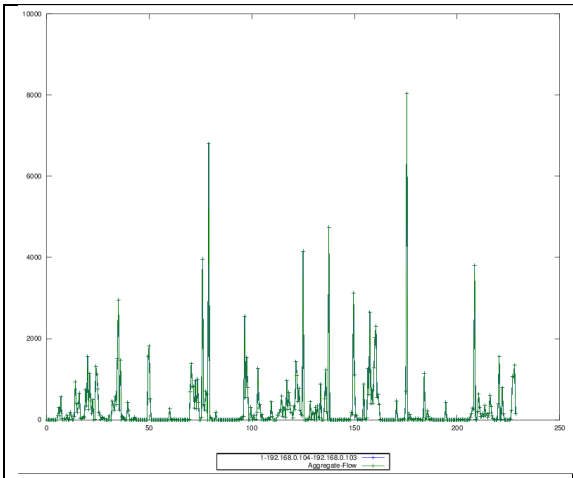


Figura 4-168 Packetloss Prueba 1

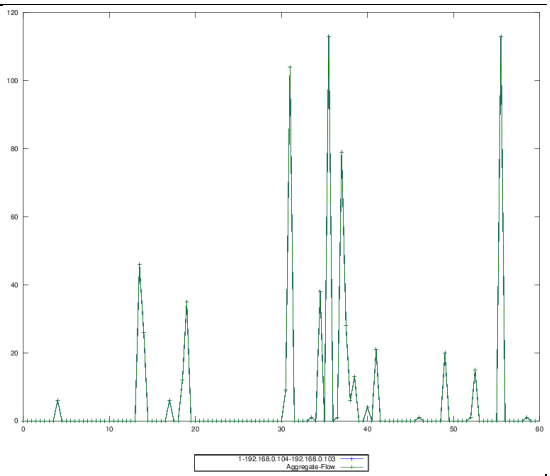


Figura 4-169 Packetloss Prueba 2

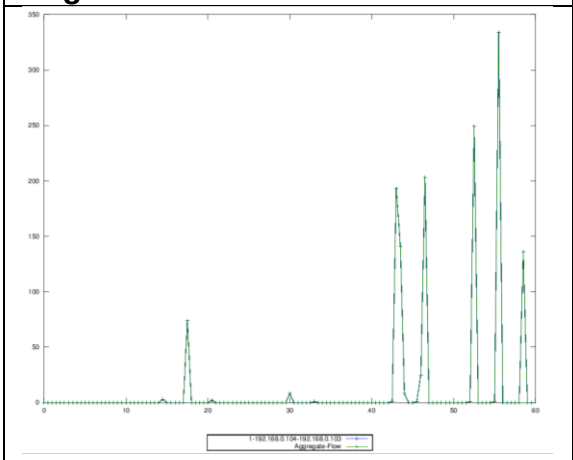


Figura 4-170 Packetloss Prueba 3

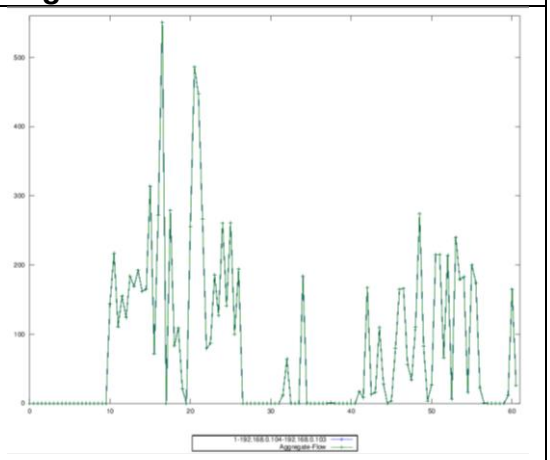


Figura 4-171 Packetloss Prueba 4

Con los datos obtenidos en este escenario podemos decir que al momento de realizar las pruebas se ve un comportamiento no uniforme, esto se debe a la interferencia que se presenta en el escenario, se puede verificar que la latencia en las diferentes pruebas realizadas no es similar y esto se debe a que los paquetes se pierde en el camino desde el emisor hacia el receptor, por tal motivo podíamos indicar que la Calidad de Servicio(QoS) en este escenario no es óptima ya que vamos a perder paquetes en nuestra red, tal como se verifica en la tabla de resumen de las pruebas realizadas y en las gráficas de Latencia (Delay).

Los porcentajes de pérdida de paquetes obtenidos en las diferentes pruebas muestran valores diferentes siendo el mismo escenario, con esto confirmamos que la presencia del Punto de Acceso configurado en el canal 3, mismo que está realizando una interferencia entres los 2 Puntos de

Acceso provoca que la comunicación entre las Estaciones no sea óptima por tal motivo los paquetes son dropeados o descartados en el medio de comunicación, adicional existen otras redes inalámbricas que también provocan interferencia en la comunicación entre los AP1 y AP3.

Por otro lado tendremos otro escenario el cual está conformado por 2 Access Point conectador inalámbricamente y un Access Point que será el encargado de realizar interferencia en el escenario, están configurados en 2412 GHz, 2422 GHz y 2437 GHz respectivamente y dos estaciones que se conectan a los Access Point de acuerdo a la Esquema que se detalla a continuación, para poder tener acceso a la red implementada.

El propósito de evaluación en este escenario es poder verificar cómo se comporta una red inalámbrica con varios Puntos de Acceso los mismos que tienen la presencia de interferencia que produce el Punto de Acceso conectado en medio de sus extremos. Adicional a esta interferencia que se presenta, se puede verificar que efecto produce este parámetro a nivel de QoS en dicho escenario.

El adaptador AirPcap NX estará conectado en una estación donde se estará capturando el tráfico de la red.

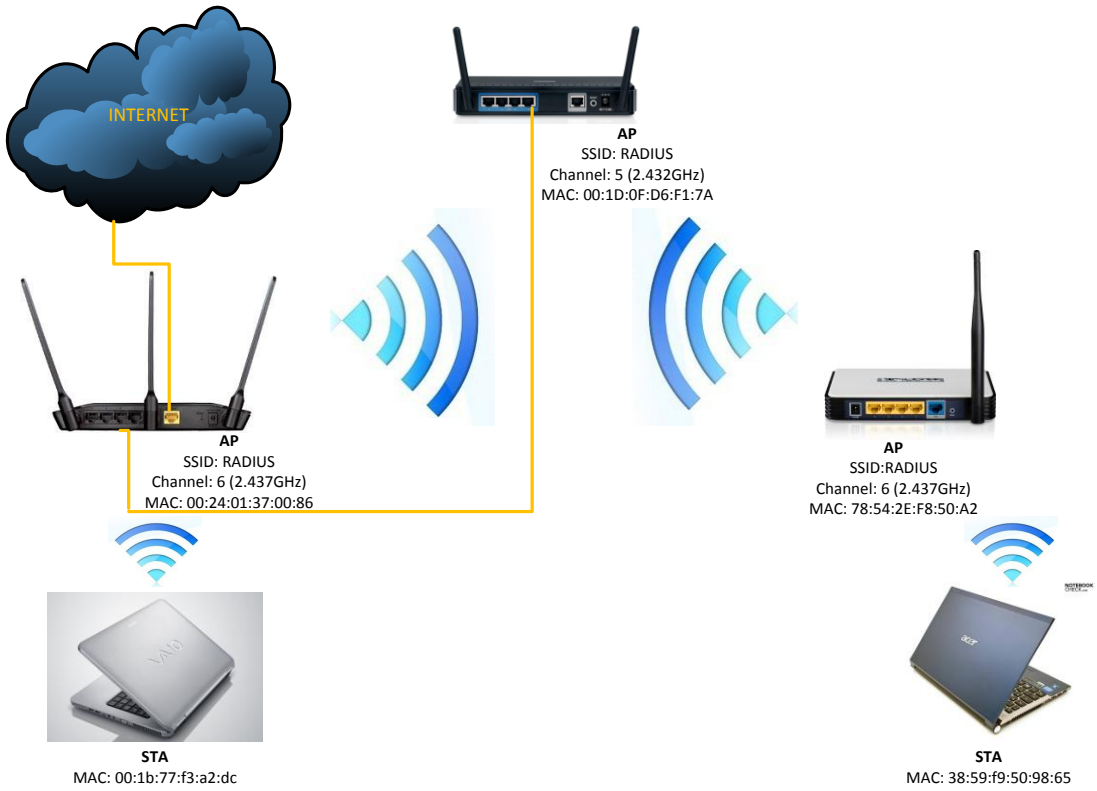


Figura 4-172 Escenario Interferencia Wifi.

Se ocuparan los siguientes equipos para poder implementar el presente escenario:

- Access Point D-Link DIR-615L
- Access Point D-Link DIR-615 (Interferencia)
- Access Point TP-Link WR541G
- Tarjeta Inalámbrica Intel Laptop Sony Vaio
- Tarjeta Inalámbrica Atheros Laptop Acer
- AirPcap Nx Adapter

Tabla 56 Direccionamiento MAC Escenario 7.

Dispositivo	INTERFAZ	MAC	FUNCION
AP	Inalámbrica	00:24:01:37:00:86	Punto de Acceso
AP	Inalámbrica	00:1D:0F:D6:F1:7A	Punto de Acceso
AP	Inalámbrica	78:54:2E:F8:50:A2	Punto de Acceso
STA	Intel	00:1B:77:F3:A2:DC	Estación
STA	Atheros	38:59:F9:50:98:65	Estación

En el presente escenario se procede a configurar los Puntos de Acceso de la misma manera que se configuraron en el escenario anterior, adicional a esto se configura otro equipo AP (D-Link DIR-615) el mismo que hará de interferencia en el escenario, para poder con esto verificar las diferencias que se tiene al momento de conectar en un ambiente por cable o inalámbricamente dos equipos AP. Se puede verificar la configuración de los equipos ingresando a la administración de los mismos.

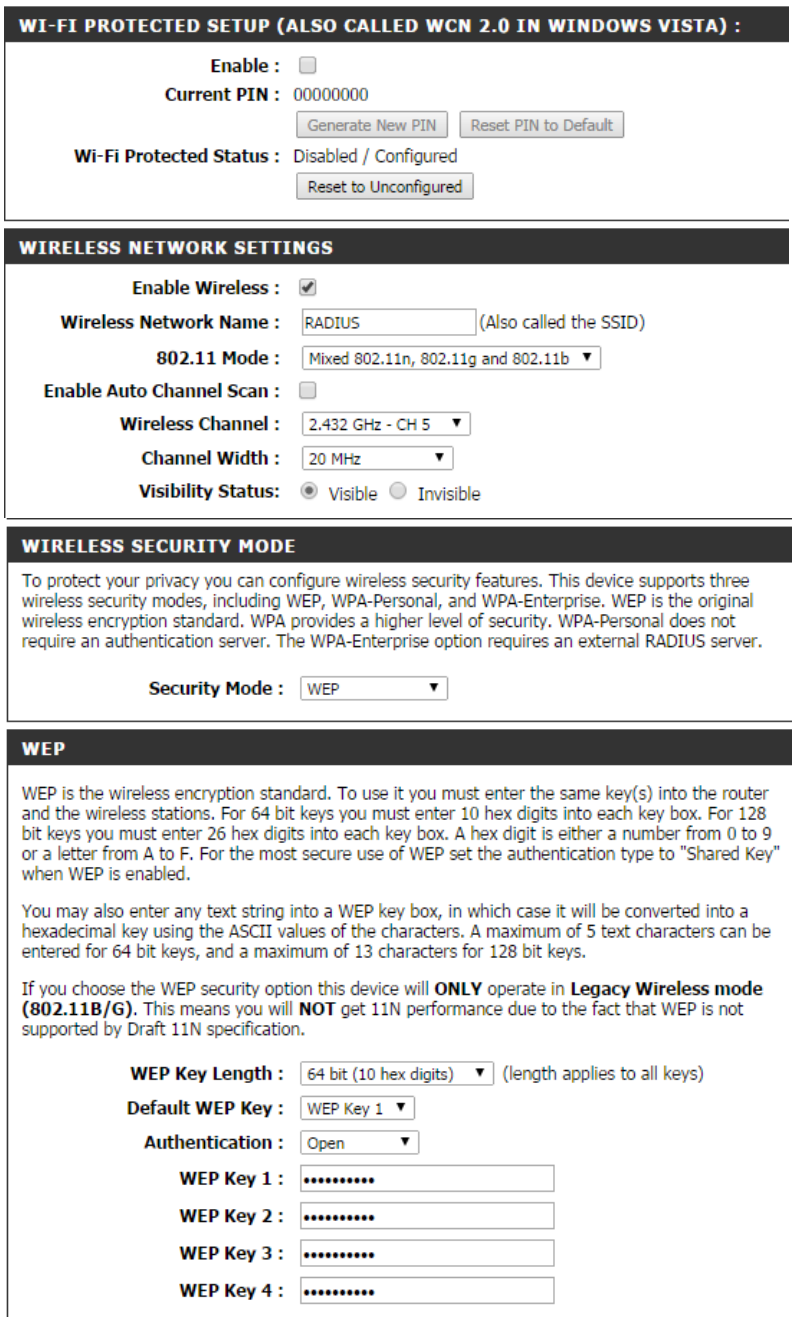


Figura 4-173 Configuración AP D-Link DIR-615 (AP Interferencia).

Configuración AirPcap

De la misma manera se procede a colocar las tarjetas AirPcap Nx en la Laptop para poder capturar el tráfico multicanal que se presenta en el escenario, por la presencia de los equipos que se encuentran configurados en canales diferentes (5 y 6). Esto lo podemos configurar en el Panel de Control de la tarjeta como se podrá verificar a continuación

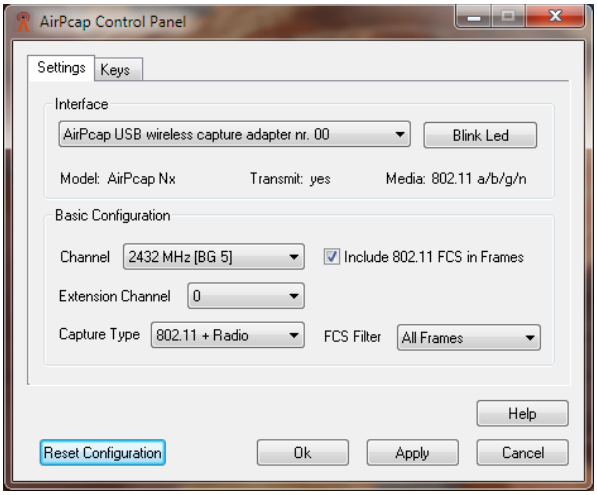


Figura 4-174 Configuración Tarjeta AirPcap Nx 1

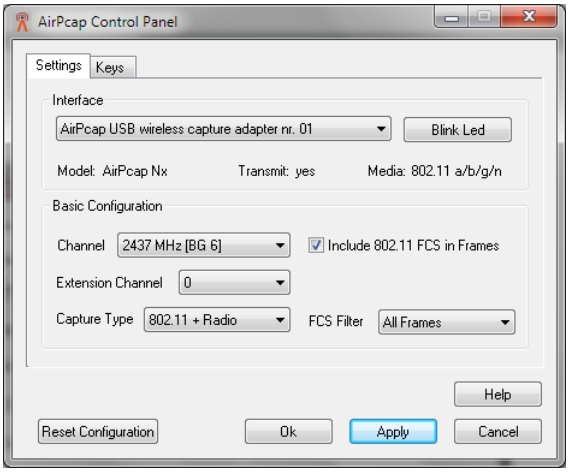


Figura 4-175 Configuración Tarjeta AirPcap Nx 2.

Verificación del Canal inSSIDer.

De la misma manera podemos verificar la configuración de los AP usando el software inSSIDer, en el que verificamos que nuestros equipos se encuentran configurados en el canal 5 y canal 6, siendo el equipo

configurado en el canal 5 el que realiza la interferencia a los otros dos equipos provocando que estos no tengan una buena comunicación.

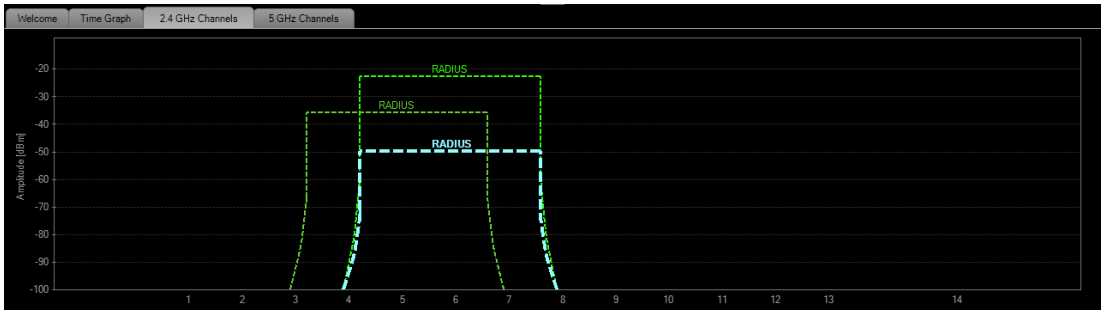


Figura 4-176 Canales AP Escenario Interferencia.

Tabla 57 Pruebas Escenario Interferencia

Test	Tiempo (s)	Packets	Delay Promedio (s)	Jitter Promedio (s)	Bitrate promedio (Kbit/s)	Paquetes descartados (%)
1	61.2421	13458	2.3159	0.0076	1758.00	67.25
2	62.1621	11426	3.2560	0.0092	1470.47	71.20
3	59.9658	29779	0.1817	0.0020	3972.79	11.19
4	60.2353	32682	0.2999	0.0021	4330.57	19.96
5	65.5092	15034	2.3691	0.0056	1835.95	64.15

```
Total time                =     61.242198 s
Total packets             =        13458
Minimum delay             =     0.093516 s
Maximum delay             =     6.646145 s
Average delay             =     2.315967 s
Average jitter            =     0.007647 s
Delay standard deviation  =     1.701596 s
Bytes received            =     13458000
Average bitrate           =  1758.003526 Kbit/s
Average packet rate       =   219.750441 pkt/s
Packets dropped           =        27634 (67.25 %)
Average loss-burst size   =    18.300662 pkt
```

Figura 4-177 Resultados Prueba 1.

```
Total time                =     62.162140 s
Total packets             =        11426
Minimum delay             =    -0.035233 s
Maximum delay             =    10.451693 s
Average delay             =     3.256018 s
Average jitter            =     0.009248 s
Delay standard deviation  =     2.619715 s
Bytes received            =     11426000
Average bitrate           =  1470.477046 Kbit/s
Average packet rate       =   183.809631 pkt/s
Packets dropped           =        28244 (71.20 %)
Average loss-burst size   =    12.950023 pkt
```

Figura 4-178 Resultados Prueba 2.

```
Total time                =     59.965843 s
Total packets             =        29779
Minimum delay             =     0.022274 s
Maximum delay             =     0.786982 s
Average delay             =     0.181797 s
Average jitter            =     0.002067 s
Delay standard deviation  =     0.185696 s
Bytes received            =     29779000
Average bitrate           =  3972.794979 Kbit/s
Average packet rate       =   496.599372 pkt/s
Packets dropped           =         3751 (11.19 %)
Average loss-burst size   =     3.413103 pkt
```

Figura 4-179 Resultados Prueba 3.

```
Total time                =     60.235395 s
Total packets             =        32682
Minimum delay             =    -0.041645 s
Maximum delay             =     1.042117 s
Average delay             =     0.299948 s
Average jitter            =     0.002190 s
Delay standard deviation  =     0.204753 s
Bytes received            =     32682000
Average bitrate           =  4340.570855 Kbit/s
Average packet rate       =   542.571357 pkt/s
Packets dropped           =         8148 (19.96 %)
Average loss-burst size   =     3.244922 pkt
```

Figura 4-180 Resultados Prueba 4.

```
Total time                =     65.509229 s
Total packets             =        15034
Minimum delay             =     0.012838 s
Maximum delay             =    19.984432 s
Average delay             =     2.369198 s
Average jitter            =     0.005684 s
Delay standard deviation  =     3.951032 s
Bytes received            =     15034000
Average bitrate           =  1835.955053 Kbit/s
Average packet rate       =   229.494382 pkt/s
Packets dropped           =        26902 (64.15 %)
Average loss-burst size   =    11.706701 pkt
Error lines               =            0
```

Figura 4-181 Resultados Prueba 5.

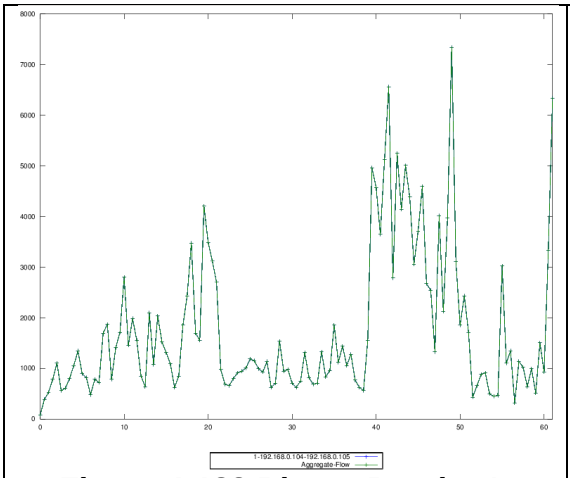


Figura 4-182 Bitrate Prueba 1.

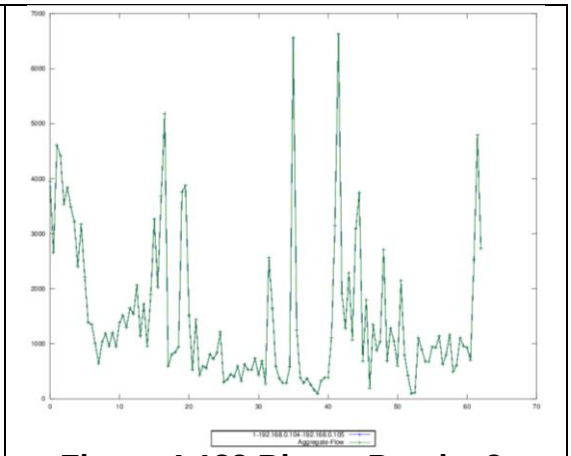


Figura 4-183 Bitrate Prueba 2.

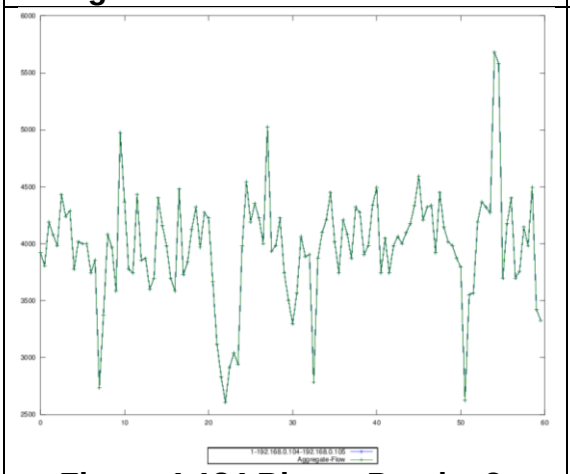


Figura 4-184 Bitrate Prueba 3.

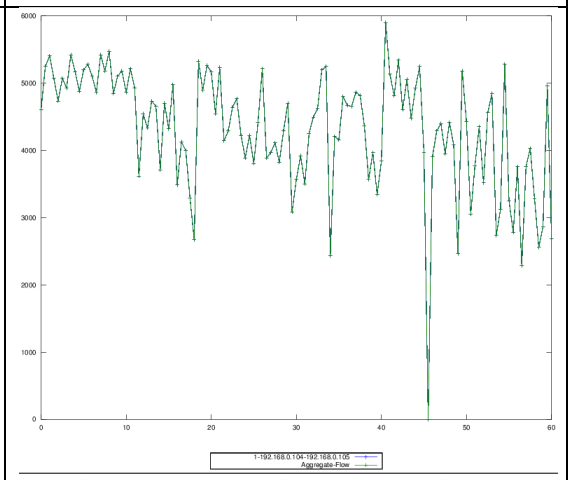


Figura 4-185 Bitrate Prueba 4.

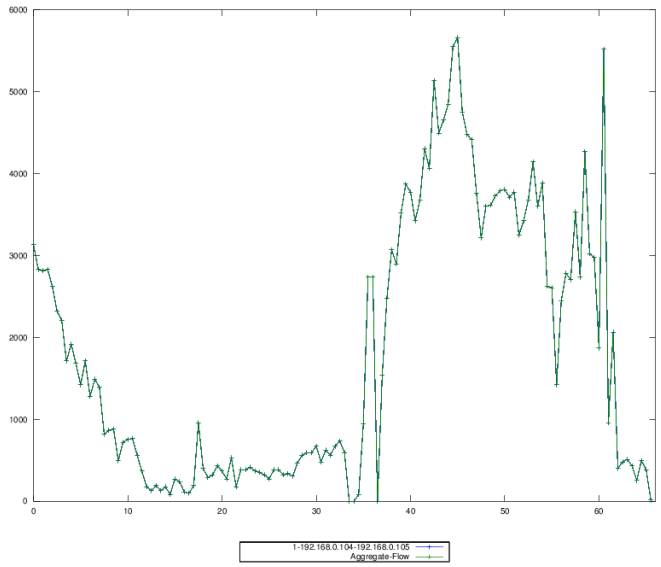


Figura 4-186 Bitrate Prueba 5.

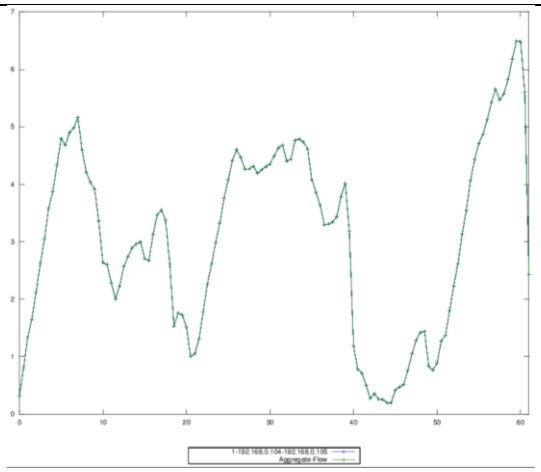


Figura 4-187 Delay Prueba 1.

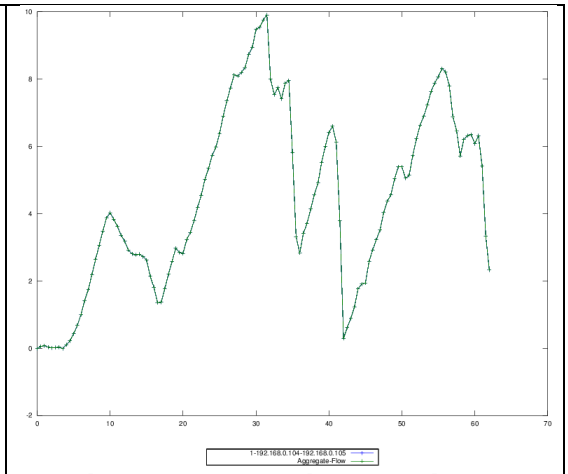


Figura 4-188 Delay Prueba 2.

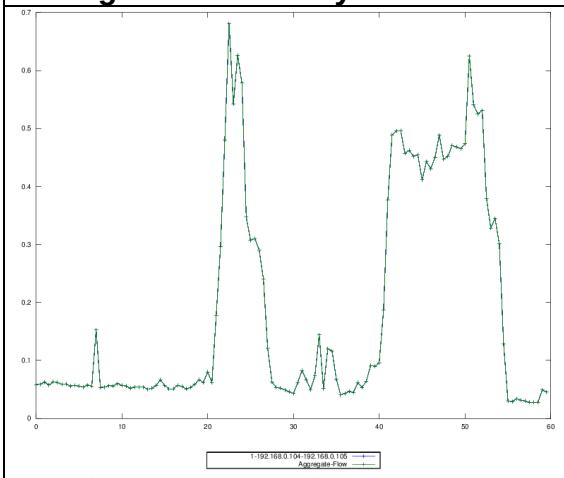


Figura 4-189 Delay Prueba 3.

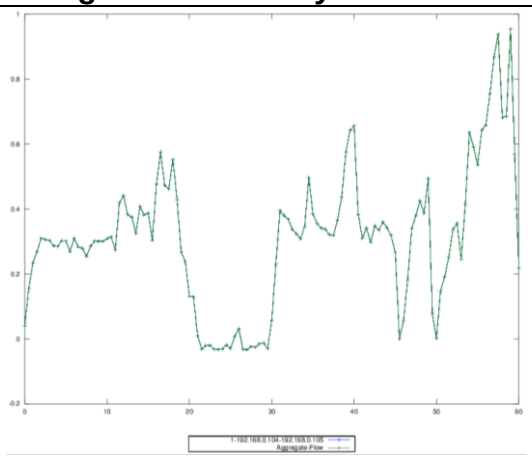


Figura 4-190 Delay Prueba 4.

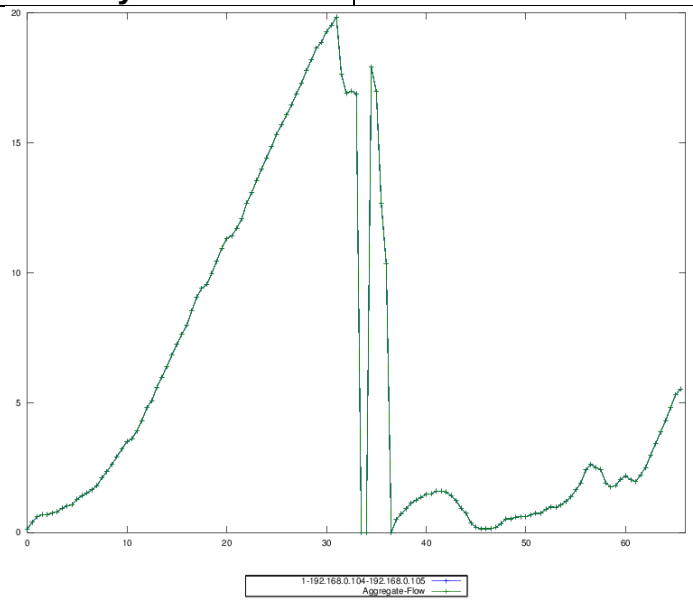


Figura 4-191 Delay Prueba 5.

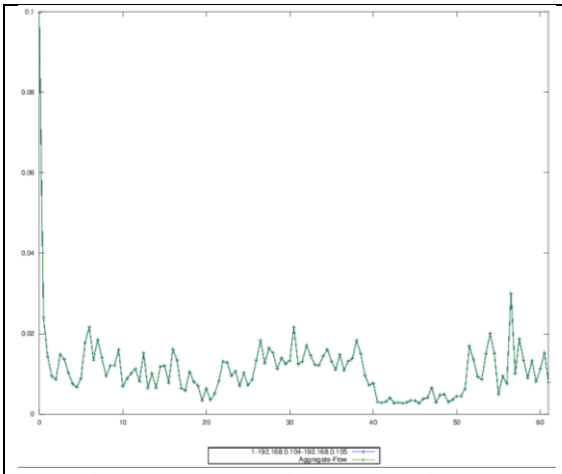


Figura 4-192 Jitter Prueba 1.

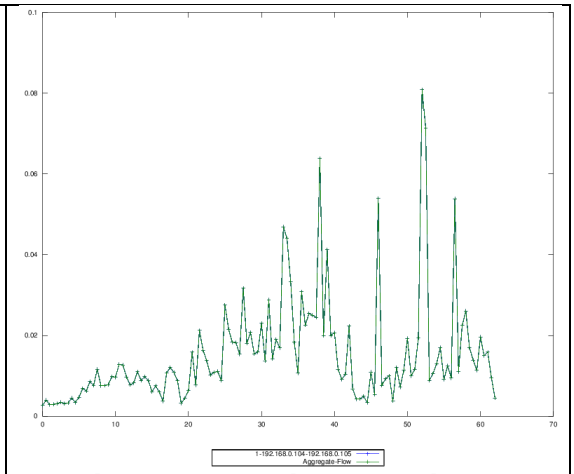


Figura 4-193 Jitter Prueba 2.

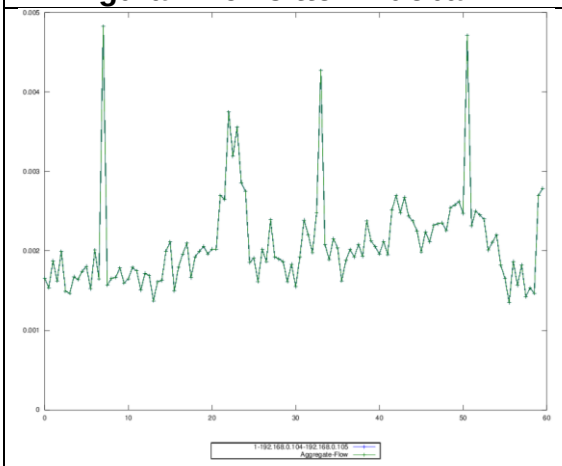


Figura 4-194 Jitter Prueba 3.

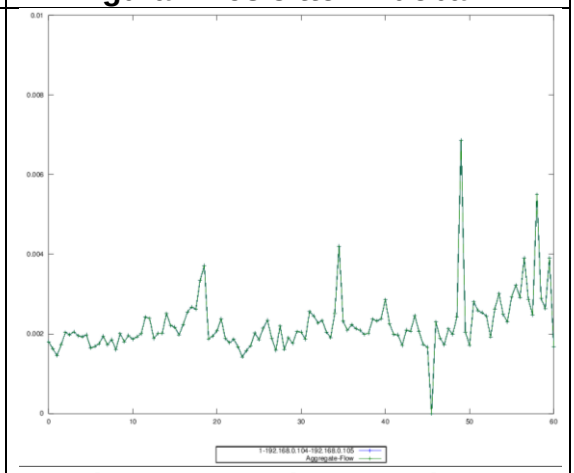


Figura 4-195 Jitter Prueba 4.

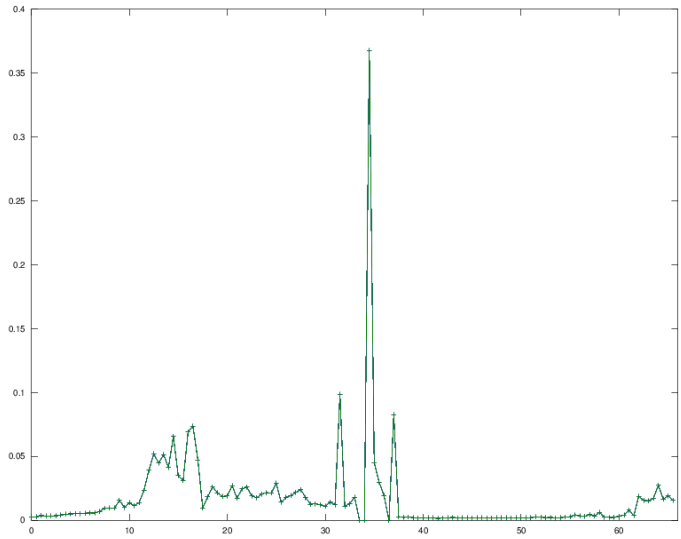


Figura 4-196 Jitter Prueba 5.

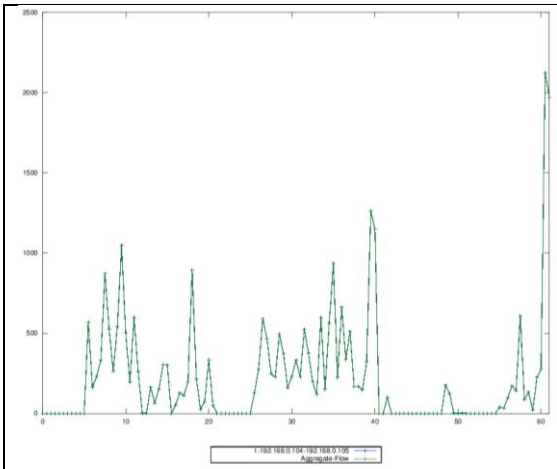


Figura 4-197 Packetloss Prueba 1.

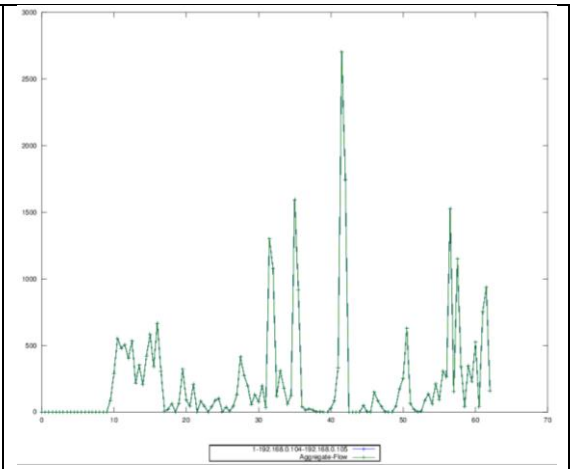


Figura 4-198 Packetloss Prueba 2.

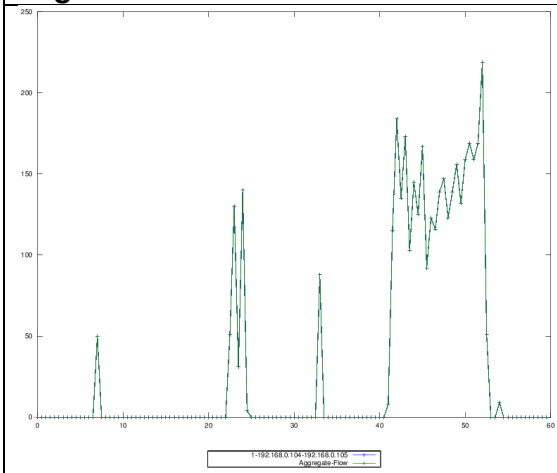


Figura 4-199 Packetloss Prueba 3.

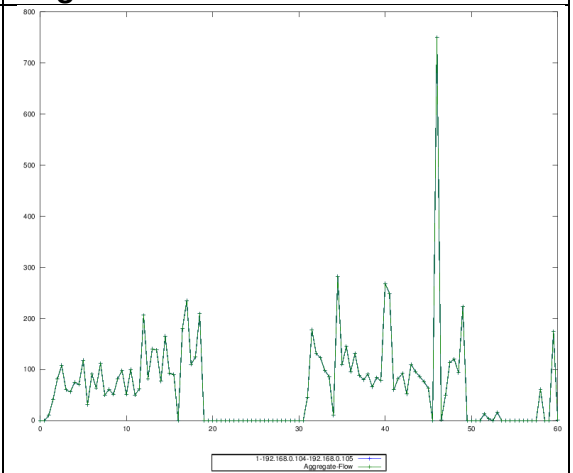


Figura 4-200 Packetloss Prueba 4.

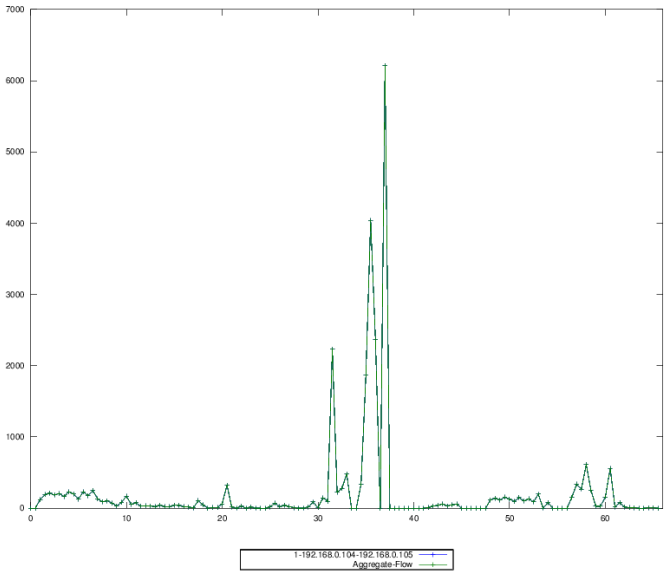


Figura 4-201 Packetloss Prueba 5.

Tal y como se pudo constatar en el escenario anterior, cuando se tiene un equipo que provoca interferencia en nuestra red, constatamos que el

retardo y el jitter son variables en el mismo escenario, esto se da por la influencia del equipo que genera interferencia, por tal motivo los equipos que están conectados inalámbricamente tienen tiempos más altos de envío de paquetes que son enviados desde las Estaciones.

La pérdida de paquetes de la misma manera es un valor no constante ni similar en las diferentes pruebas realizadas. Estas pérdidas de paquetes en un ambiente inalámbrico se lo verifica mayor por el mismo hecho del canal por el cual tienen que pasar los datos generados en las estaciones.

4.3.5. Falso AP

El escenario lo conforman 3 equipos Access point físicos con seguridad WPA y autenticación PSK y un softap con autenticación abierta.

El propósito de este escenario es comprobar el comportamiento de una estación móvil que se asocia al softap y verificar mediante monitoreo que puede extraer como información útil el softap a partir de la estación móvil.

Figura 4-202 Rogue AP

El escenario se encuentra implementado por los siguientes equipos:

- Access Point DLink DIR-619L
- Access Point D-link DIR-615
- Access Point Tplink TL-WR542g
- Tarjeta Inalámbrica Intel laptop Sony Vaio
- Tarjeta Inalámbrica laptop Hacer
- Tarjeta USB Wireless DLink DWA110
- Smartphone Xperia Z
- AirPcap Nx Adapter

Tabla 58 Tabla de direccionamiento

Dispositivo	INTERFAZ	MAC	FUNCION
STA1	Intel	00:1B:77:F3:A2:DC	ESTACION
STA2	Acer	38:59:f9:50:98:65	ESTACION
STA3	Sony	B4:52:7D:36:DB:7B	ESTACION
AP1	Inalámbrica	00:24:01:37:00:86	PUNTO DE ACCESO
AP2	Inalámbrica	00:1D:0F:D6:F1:7A	PUNTO DE ACCESO
AP3	Inalámbrica	78:54:2E:F8:50:A2	PUNTO DE ACCESO
AP4	Inalámbrica	00:1b:11:bc:95:0f	PUNTO DE ACCESO

Este escenario se destaca principalmente por disponer de un softap generado desde una máquina virtual Ubuntu instalada en STA2 y añadida una tarjeta tipo USB DLink DWA 110.

Configuración Falso AP

Para llevar a cabo el levantar el softap debemos tener preinstalado en nuestra máquina virtual un servidor DHCP para Ubuntu (Isc-dhcp-server), un servidor dns (bind9), el modo monitor activado en la tarjeta USB y la suite de Aircrack que permite generarlo. El servidor dhcp isc-dhcp-server utiliza el archivo dhcp.conf quien contiene las configuraciones del mismo para el escenario se implementó la red 192.168.5.0/24 y como Gateway la ip 192.168.5.1.

Comando: #gedit etc/dhcp/dhcp.conf

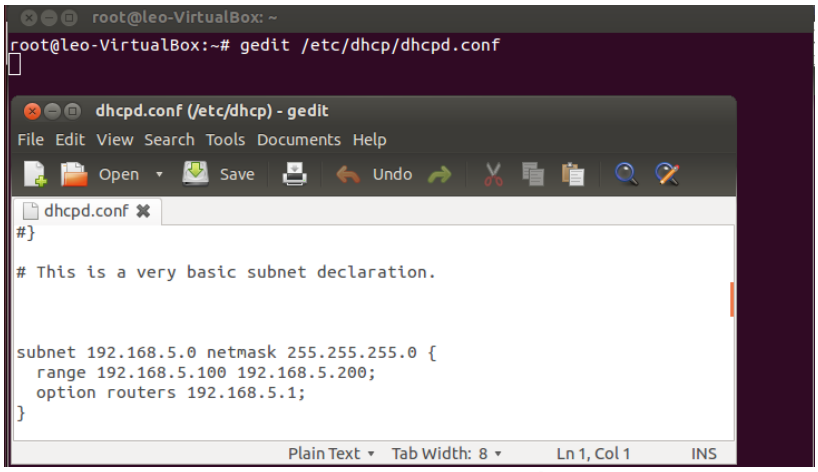


Figura 4-203 Configuración DHCP

Ya configurado el servidor colocamos a la tarjeta inalámbrica USB reconocida en Ubuntu como wlan0 en modo monitor para lo cual mediante airmon de Aircrack-ng es utilizado mostrando un mensaje al habilitarse el modo monitor y generando una interfaz con el nombre de mon0 para dicho propósito.

Comando: #airmon-ng start wlan0

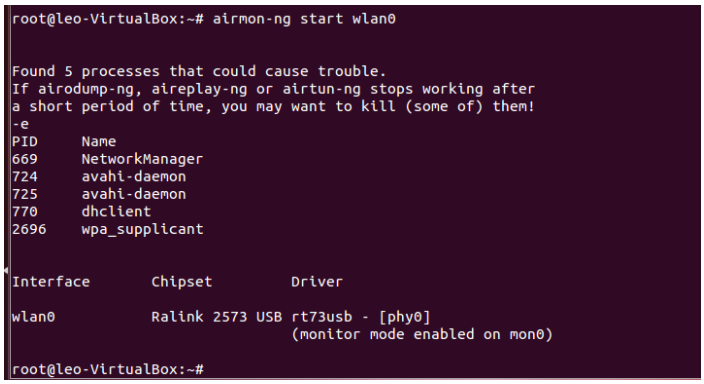


Figura 4-204 Tarjeta modo Monitor

Para comprobar la interfaz creada se aplica en el Shell de comando de Ubuntu iwconfig.

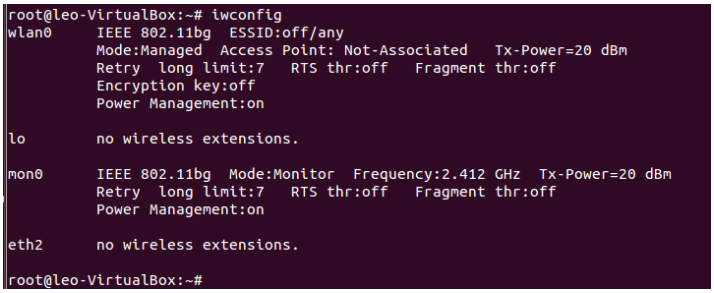


Figura 4-205 Comprobación Tarjeta Monitor

Posteriormente se levanta el softap utilizando airbase y la interfaz en modo monitor generada previamente. El momento de aplicar airbase por defecto se genera la nueva interfaz at0 sobre la cual se propaga el anuncio de la red a generarse con el nombre de InternetGratis. Como detalle adicional al utilizar –c 9 y no especificar contraseñas indica al softap que la autenticación será open System y se trabajará sobre el canal 9

Comando: airbase-ng –c 9 –essid InternetGratis –v mon0

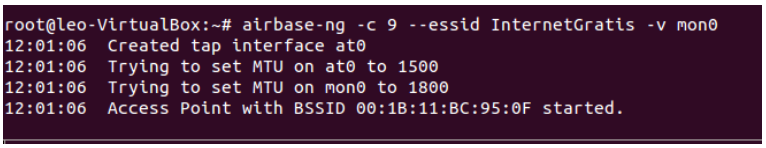


Figura 4-206 Generación Softap

Con el fin de que las estaciones que se asocien a la red generada configuramos la ip de Gateway sobre la interfaz at0 y especificamos a dicha interfaz para que proporcione dhcp a las estaciones mediante la edición del archivo isc-dhcp-server

Comando: #Ifconfig at0 192.168.5.1 netmask 255.255.255.0 up

Comando: #gedit /etc/default/isc-dhcp-server

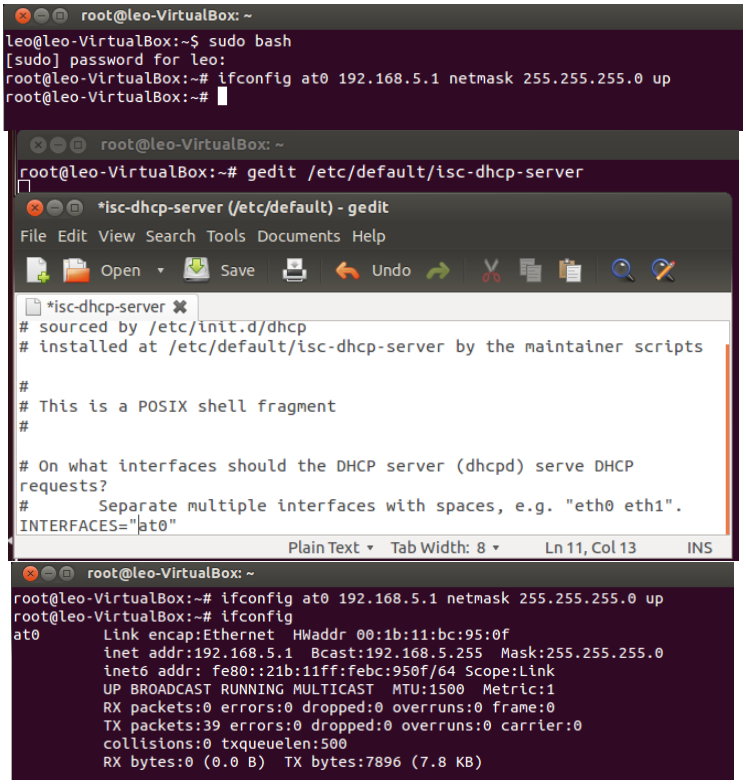


Figura 4-207 Configuración interfaz inalámbrica SoftAP

Se procede a levantar el servidor dhcp sobre la interfaz at0, si se presenta el mensaje Can't PID significa que no se pudo levantar el servidor dhcp por desconocimiento de ruta en la creación del proceso de Ubuntu el cual puede ser corregido mediante la corrección de ruta.

Comando: #dhcpd at0

Comando: #ln –s /var/run/dhcp-server/dhcp.pid var/run/dhcp.pid

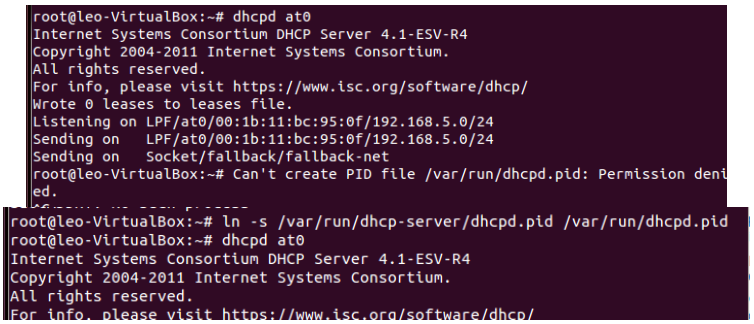


Figura 4-208 Aplicación DHCP a interfaz inalámbrica

Finalmente para que las estaciones tengan acceso a internet a través del softap aplicamos reglas de nat y levantamos el servidor dns bind9

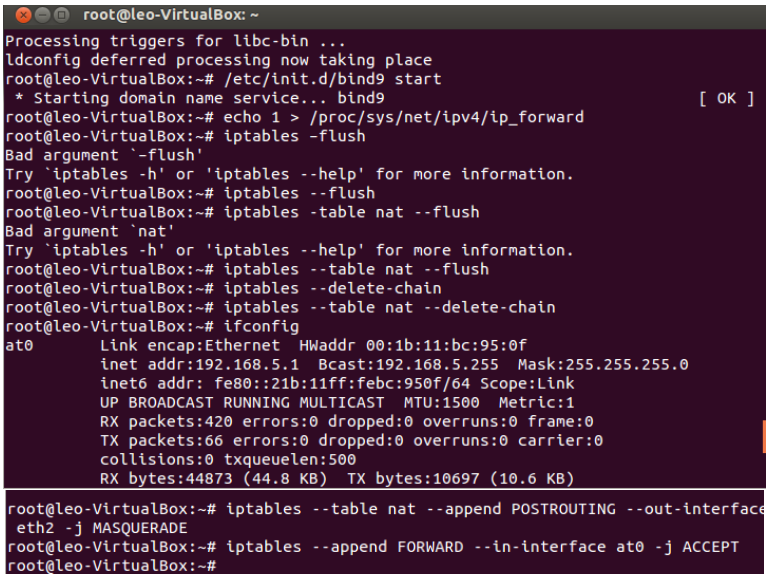


Figura 4-209 Reglas NAT y Servidor DNS

Finalmente para lograr la captura del tramado se configuran las tarjetas AirPcap en los canales 1, 6 y 11 para cubrir todo el espectro de frecuencias de IEEE802.11 de 2.4Ghz.

El escenario tiene como propósito mostrar el tipo de ataque que podría generarse hacia una estación al verificarse en el análisis un equipo no perteneciente a la red con un SSID diferente y con autenticación open System. Esto para un administrador de red es un grave problema debido a que muchos hackers utilizan esta técnica con el fin de obtener datos relevantes de las estaciones de una empresa como claves de autenticación o el uso de una MAC válidos para lograr autenticarse en una red inalámbrica corporativa.

Para el escenario airbase genera el punto de acceso falso y de igual forma cuando un equipo trata de asociarse a la estación muestra la dirección física del equipo y de igual forma ofrece la ip mediante el servidor dhcp.

Para visualizar este tipo de inconvenientes mediante Wireshark verificamos el comportamiento de uno de los equipos de red; por lo general los usuarios que disponen Smartphone o tablets no conocen los riesgos que

puede implicar para una empresa el asociarse a equipos no pertenecientes a la red y son los que más huecos de seguridad proveen a un atacante.

Por lo cual nos enfocaremos al análisis de paquetería.

Para verificar este tipo de ataque hay que tomar en cuenta la localidad donde se encuentra ubicada la red, es decir si estamos dentro de una zona residencial o en una zona corporativa, esto debido a que las redes Wifi se han proyectado en gran cantidad y hoy en día domicilios, escuelas, universidad entre otros sitios disponen de esta tecnología.

Lo primero en realizar es un barrido de frecuencias mediante un analizador de redes Wifi como es el caso de Wifi Analyzer.

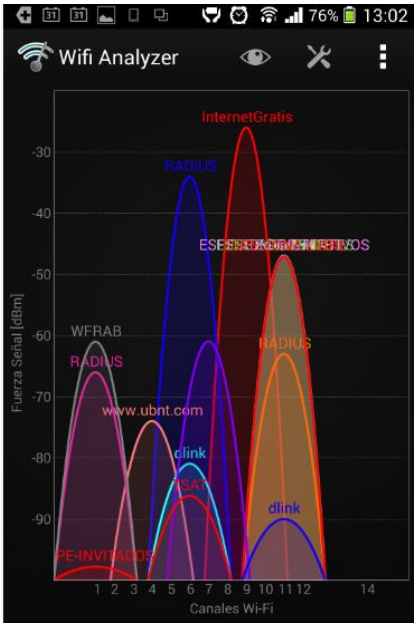


Figura 4-210 Escaneo de redes Wifi Analyzer

De la figura anterior se verifica a simple vista una red con buena señal y un SSID muy particular para ser una red empresarial InternetGratis y adicionalmente se verifica que interfiere en la red RADIUS en el canal 9.

Figura 4-211 Escaneo de redes desde Smartphone

De la gráfica anterior se verifica las redes aledañas y se comprueba que la red InternetGratis no dispone seguridad por lo cual es un candidato altamente riesgoso para nuestra red.

Análisis Wieshark

En el análisis desde Wireshark nos enfocamos en uno de los equipos que pertenecen a nuestra red en este caso utilizaremos la MAC b4:52:7d:36:db:7b (STA3) y el filtro de asociación.

Filtro: wlan.fc.type_subtype <=1 or wlan.addr eq b4:52:7d:36:db:7b

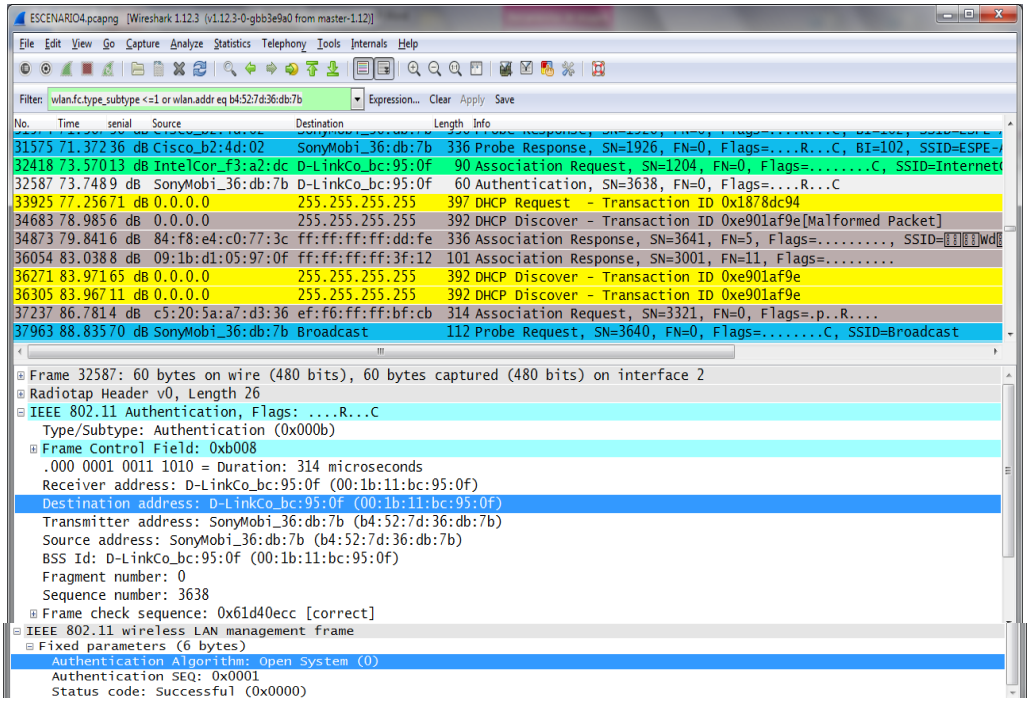


Figura 4-212 Autenticación a falso AP

La gráfica anterior muestra un comportamiento inusual en el monitoreo mediante AirPcap y Wireshark, ya que en primera instancia se verifica una autenticación desde las estación STA3 hacia el AP falso y se muestran una serie de mensajes DHCP. Adicionalmente en las tramas se verifica que se hace la petición de asociación desde STA1.

Dado el caso de lograrse la asociación con el falso Ap el tramado de sistema abierto tiene una secuencia respectiva pero en el caso del falso Ap únicamente presenta la autenticación y negociación de la ip. Cabe recalcar que las tarjetas AirPcap tiene pre configurados los canales de monitoreo y en el caso específico de identificar tramas de equipos cercanos los mostrara a través del canal de la tarjeta AirPcap y no mediante el canal del AP. Ya capturado el canal será mostrado en la información que acarrea la parte de administración en las tramas beacon.

Figura 4-213 Conexión STA3 hacia Rogue AP

Ya asociado se verifica que STA3 logró conectarse hacia la red del falso AP. Finalmente el atacante podrá verificar la dirección MAC y verificará que se asoció una estación.

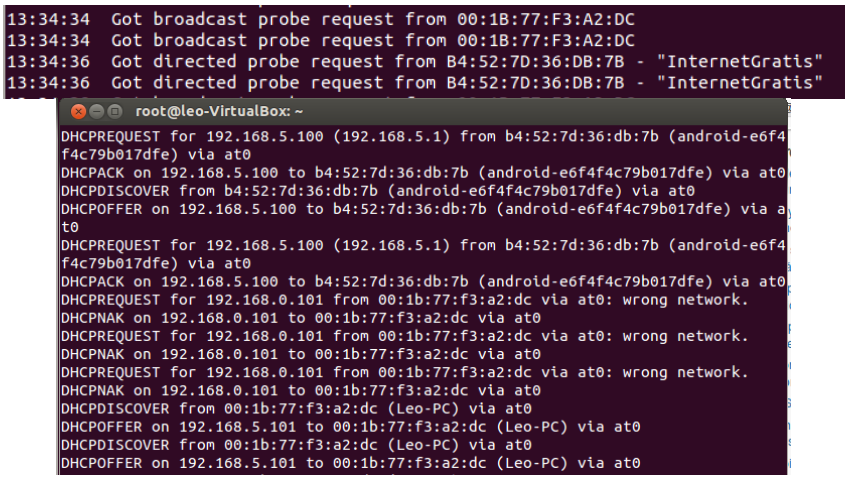


Figura 4-214 Airbase asociacion equipos

Adicionalmente el administrador de red puede verificar la MAC infiltrada y puede ver cómo se comporta el equipo dentro de la red para el caso específico el falso AP muestra la MAC 00:1b:11:bc:95:0f.

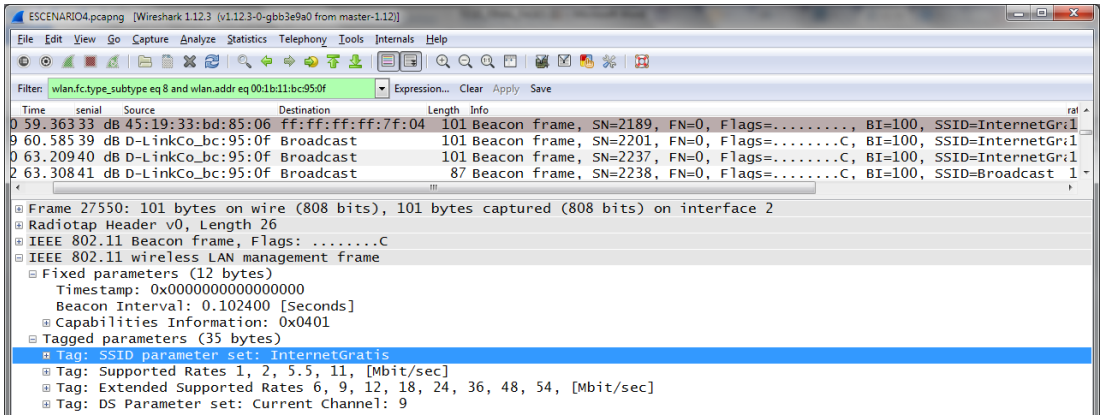


Figura 4-215 Beacon Falso Ap

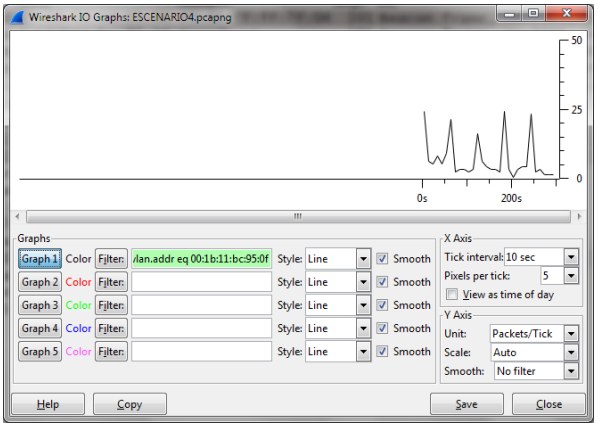


Figura 4-216 Periodo de tramas Beacon.

4.3.6. Monitoreo temporal y análisis de red con gráficas de Wireshark.

Una vez analizado las características de varios escenarios y tener presente la necesidad que tiene un administrador de red de poder conocer el estado de infraestructura, podremos pensar en la idea de encontrar la manera de realizar un análisis gráfico y en tiempo real de los datos que estamos capturando.

Adicional a la herramienta Cascade Pilot en la cual podemos sacar datos y visualizarlos gráficamente de acuerdo a las necesidades que filtramos podemos realizar este mismo análisis con las herramientas gráficas que nos presenta Wireshark.

Dentro de este módulo de Wireshark debemos colocar los filtros y podemos visualizar los datos en un máximo de 5 graficas diferenciándolas por colores, esto lo realizaremos teniendo ya el archivo capturado de paquetes en Wireshark (.pcap), En tiempo real podemos también realizar esta actividad y de la misma manera debemos colocar los filtros para poder tener la información que como administradores de la red es de nuestro interés.

Para poder visualizar las gráficas en Wireshark de un archivo previamente capturado debemos realizar los siguientes pasos.

Abrir el archivo .pcap previamente capturado, una vez realizado esto en el menú principal vamos a escoger las opción Statistics y vamos a

seleccionar IO Graph, se nos abre una ventana de acuerdo a la mostrada a continuación.

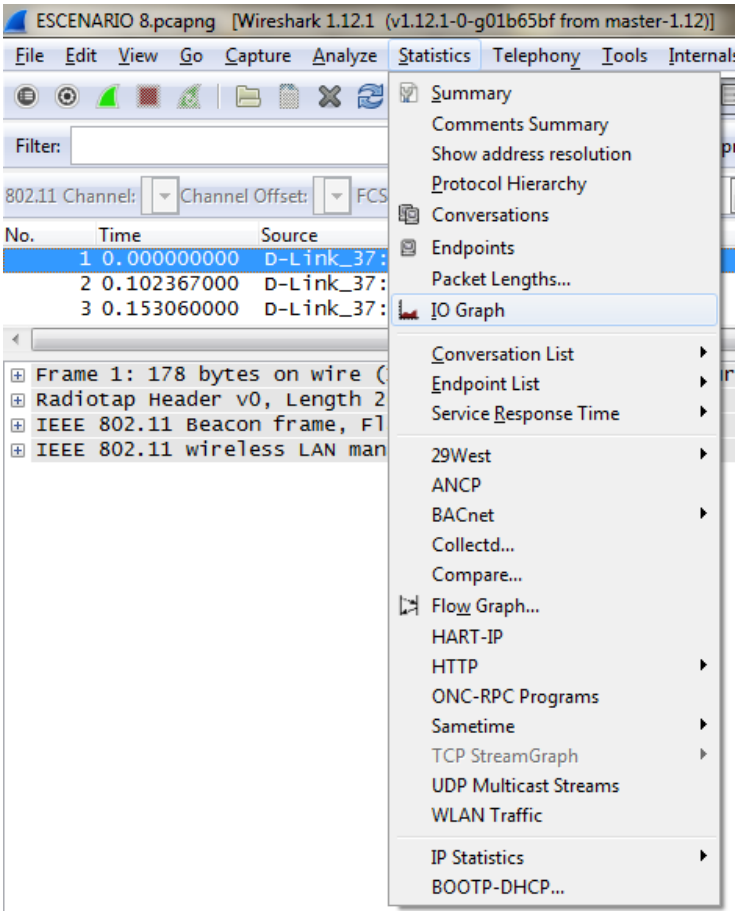


Figura 4-217 Selección IO Graph

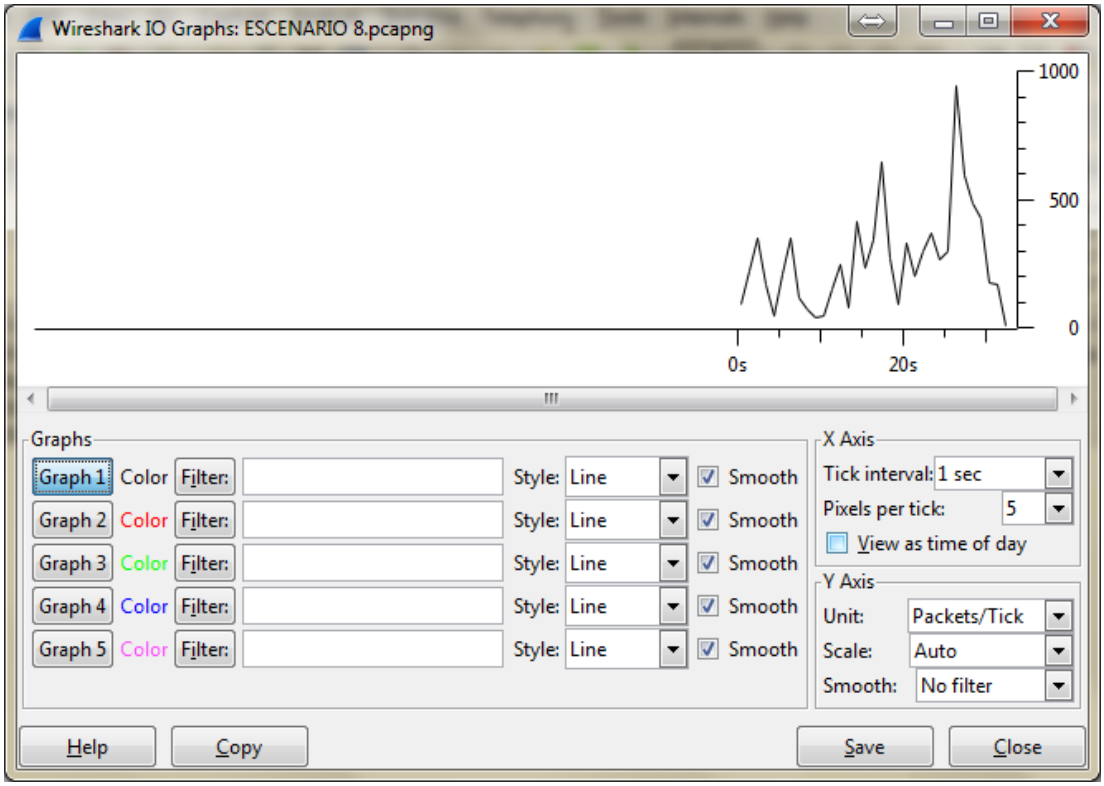


Figura 4-218 IO Graph.

Dentro de esta pantalla colocaremos los filtros respectivos dependiendo del interés de búsqueda del administrador, en nuestro caso vamos a realizar un filtro para poder verificar las tramas de control, administración y de datos, posteriormente realizaremos la validación de otras tramas como beacom o autenticación. También podemos cambiar los parámetros de la visualización de la gráfica como la resolución de los ejes X y Y o poder escoger el estilo de la gráfica a realizarse.

Los filtros se los colocan de acuerdo a la figura:

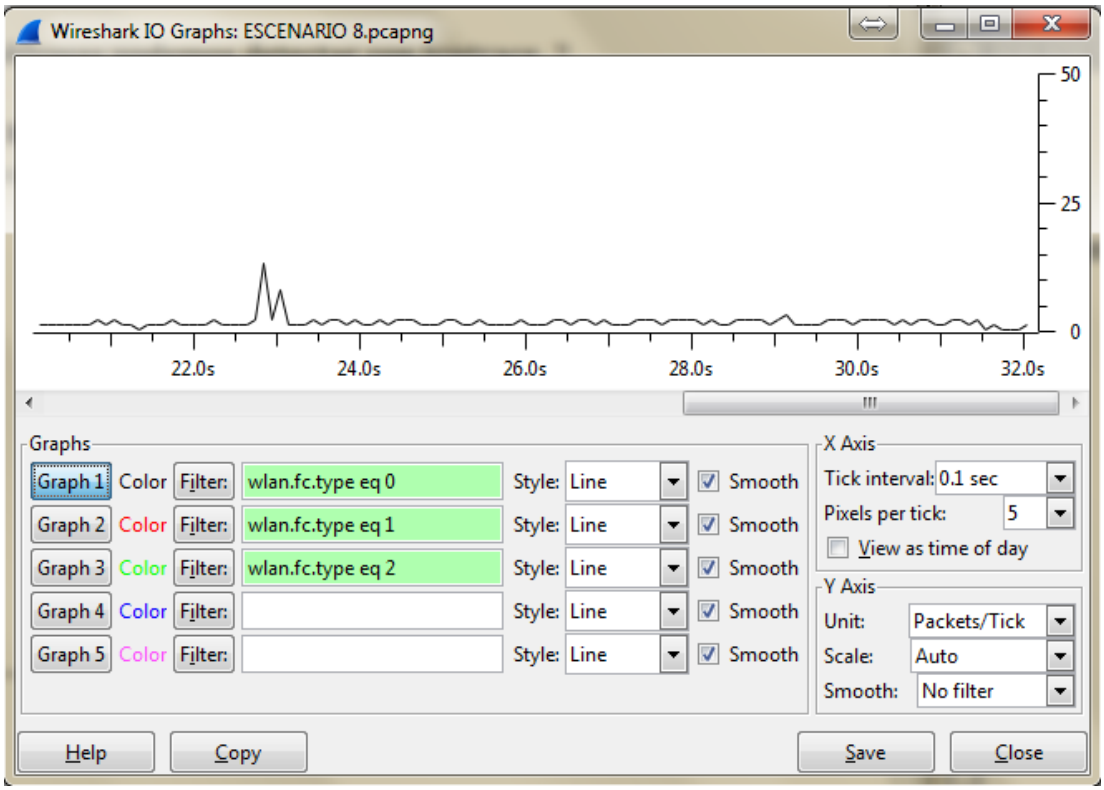


Figura 4-219 Filtros en gráficas Wireshark Management.

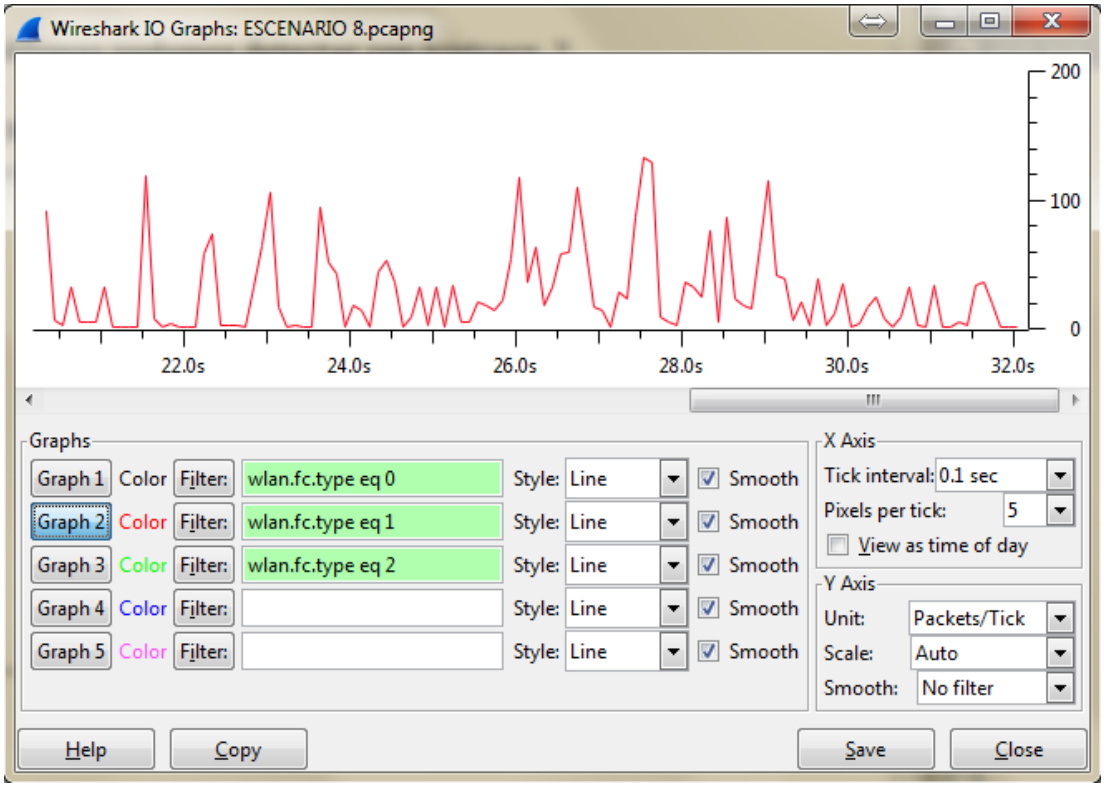


Figura 4-220 Filtros en gráficas Wireshark Control.

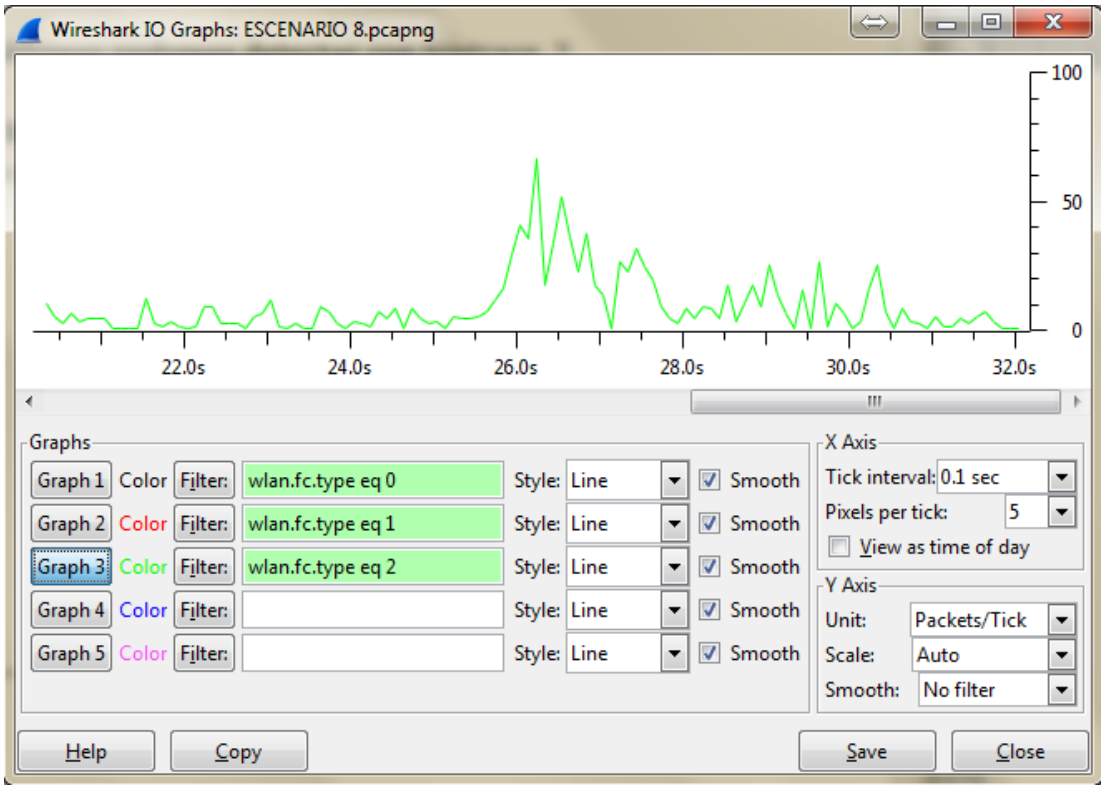


Figura 4-221 Filtros en gráficas Wireshark Data.

En la siguiente Figura vamos a poder visualizar gráficamente filtros ejecutados como Association Request (Graph 1- Negro), Association Response (Graph 2 - Rojo), Reassociation Request (Graph 3 - Verde), Reassociation Response (Graph 4 - Azul), Beacon (Graph 5 - Rosado)

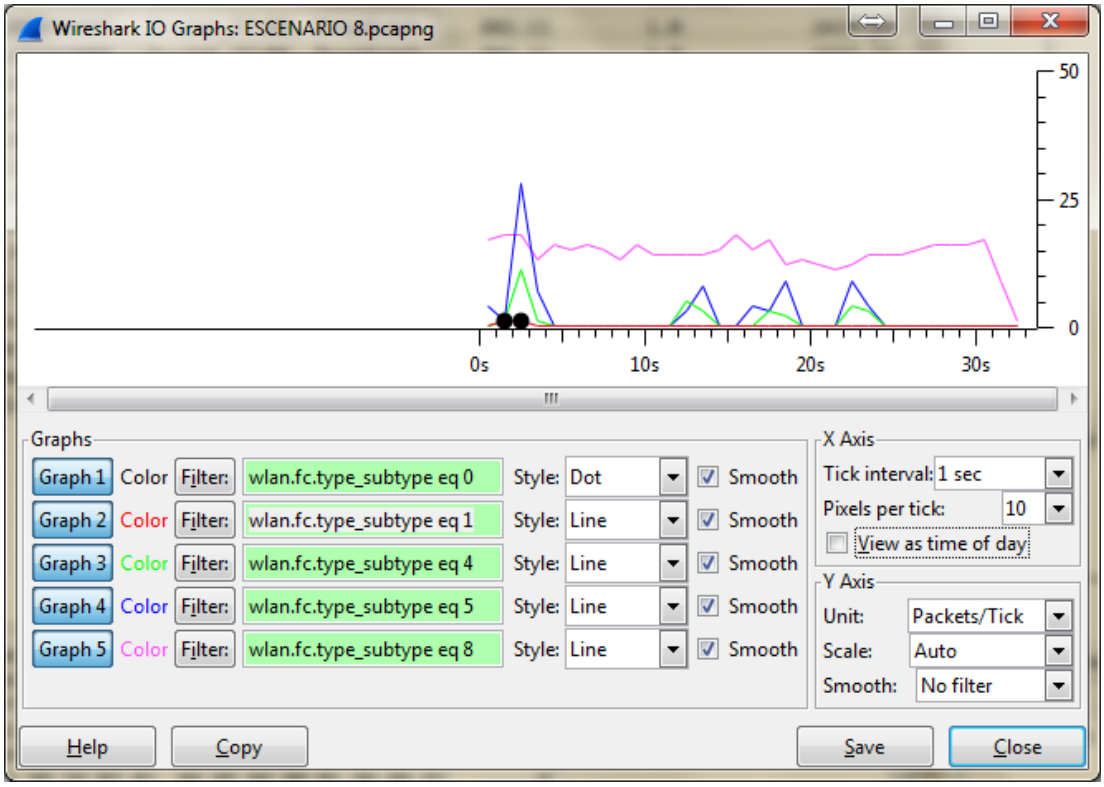


Figura 4-222 Filtros Tramas.

En la gráfica 1 podemos visualizar las tramas de Association Request que se producen a lo largo de la captura de paquetes de la misma manera la gráfica 2 de color rojo veremos las respuestas a estas peticiones, verificando que se tiene los picos similares dándonos a entender que los requisitos de asociación fueron respondidos a las estaciones.

De la misma manera podemos verificar la gráfica 5 de color rosado, en la cual filtramos los paquetes beacon y observamos que a lo largo de la captura de paquetes visualizamos que esta trama es la que más valor tiene por lo que en nuestro escenario las redes están enviando esta información a los dispositivos para que los puedan ver y posterior conectarse o asociarse a una red.

En este tipo de gráficas podemos colocar los mismos filtros que colocamos a nivel de la línea de comando de Wireshark. Sin embargo la apreciación de los datos y el análisis es un poco más complicado de realizarlo.

De la misma manera existe otro módulo de Wireshark denominado Wireshark 2 Preview la cual nos permite abrir el archivo de captura de paquetes y realizar el proceso similar al realizado en IO Graph, obteniendo la siguiente figura.

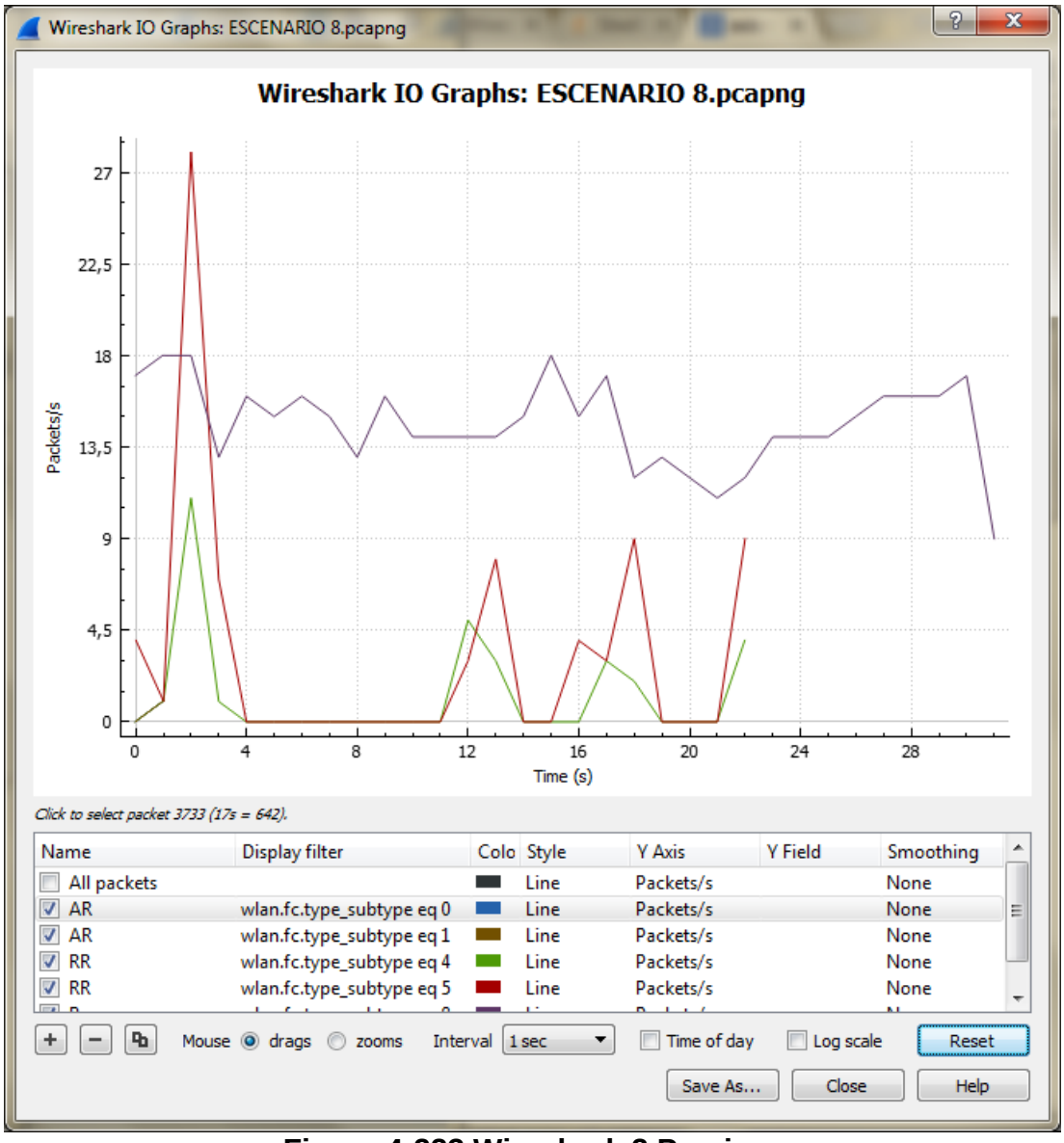


Figura 4-223 Wireshark 2 Preview.

Para pode capturar el tráfico en tiempo real en este mismo módulo podemos visualizar el tráfico que el canal en este caso las tarjetas están capturando, de la misma manera debemos colocar el filtro a filtrar y dar clic en la interface y podremos visualizar el tráfico de red. En los dos casos podemos guardar la imagen en un formato PDF para poder usarla como un reporte de ser necesario.

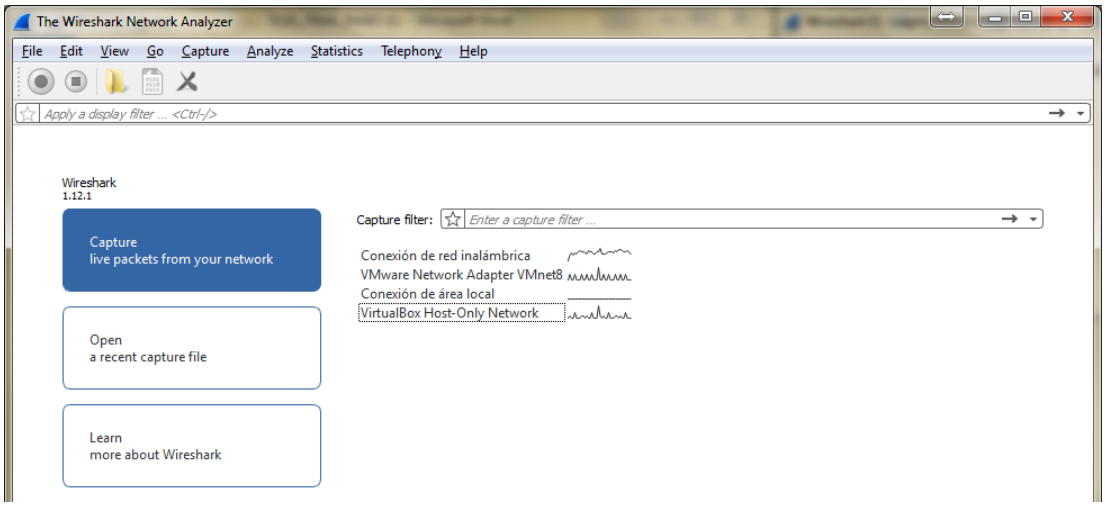


Figura 4-224 Wireshark Preview.

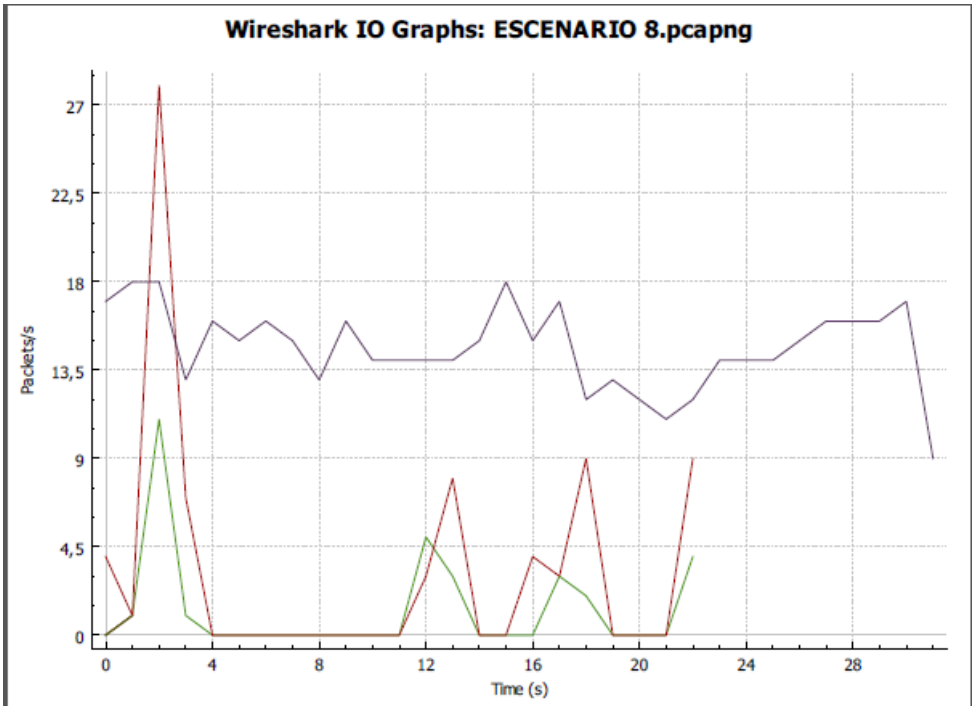


Figura 4-225 Gráfica generada en PDF.

En relación a las otras herramientas analizadas como Cascade Pilot no podemos realizar el análisis en tiempo real del comportamiento de los paquetes capturados, adicional en todos los casos el monitoreo que se realiza no es en tiempo real ya que siempre va a existir un tiempo mientras se captura el paquete y se lo va almacenando en la data de Wireshark o de la misma manera si se hace la gráfica en IO Graph.

De las herramientas que hemos ocupado inSSIDer es una de las herramientas que nos ayudan a verificar un comportamiento simple y que a una primera mano nos damos cuenta de la configuración del canal de nuestros APs, que en la mayoría de los casos podría ser el problema para que nuestra red tenga problemas, por el hecho de que estos APs estén sufriendo interferencias por otros APs propios de la red o de redes aledañas a nuestro entorno físico.

CAPITULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se investigó que el estándar IEEE802.11 logra conectividad a través de señales de frecuencia infrarroja (ISM) con la cual genera conexiones de 1 a 2Mbps. Posteriormente sus estándares a, b, g y n dan una mejora en la velocidad de conexión a través del procesamiento de señales análogas a digitales; es decir, que en la parte práctica hablamos del uso de moduladores para adaptar la señal a las frecuencias del estándar. En la actualidad la versión más reciente del estándar es el IEEE802.11ac que genera velocidades de hasta 7Gbps en la banda de 5Ghz.
- La implementación de escenarios de prueba permiten conocer a profundidad los componentes que conforman el estándar IEEE 802.11 y sus diferentes variaciones, tanto en velocidad, seguridad y alcance.
- Las tramas de Administración son las que nos proporcionan mayor información de la red analizada, contiene parámetros como ESSID, MAC, potencia de transmisión las mismas que son enviadas en broadcast a todas las estaciones (Beacon), esto puede convertirse en un punto de vulnerabilidad de una red inalámbrica ya que pueden aparecer falsos AP que hagan que las estaciones se conecten y envíen información valiosa y que otros los pueden utilizar para realizar ataques a la red.
- Las técnicas de monitoreo pasivas son las técnicas más usadas en un entorno de red que se necesita conocer su funcionamiento y en el caso de la implementación de la presente tesis se concluye que realizar un monitoreo de los paquetes de red o realizar snifing es la más efectiva ya que se realiza una recolección de diferentes protocolos en los cuales analizamos diferentes aspectos como direcciones MAC (capa 2), direcciones IP (capa 3).

- Las tarjetas usadas en el presente proyecto son orientadas a un entorno Windows, pero nos presenta diferentes beneficios ya que lo podemos emplear en su funcionalidad de multicanal y de esta manera se logró comprobar la compatibilidad con diferentes dispositivos que el mercado tiene a disposición de los usuarios.
- Se realizaron pruebas para verificar el comportamiento de las tarjetas tanto en monocanal como en multicanal, y se verificó que cuando se está solo monitoreando el tráfico no importa el número de tarjetas con as que censemos el tráfico del entorno, ya que estaos haciendo un monitoreo pasivo.
- Se implementaron diferentes escenarios, los mismos que se fueron divididos en fases para facilidad de aprendizaje y de análisis.
- En la primera fase de estudio se plantearon escenarios en los cuales se familiarizó con las herramientas y los parámetros para poder realizar un monitoreo monocanal y uno multicanal.
- En la Segunda fase se plantearon escenarios en los cuales nos centramos en un canal específico para tener un estudio de nuestro entorno de red y verificar el comportamiento de nuestros equipos y los diferentes parámetros que involucran tener una buena conexión de red.
- Una tercera fase nos permitió implementar escenarios de aplicaciones que un administrador de red puede encontrarse en la vida práctica, mismos que se analizaron con diferentes herramientas y mostrando diferentes técnicas de analizar la información obtenida.
- De las herramientas usadas en la implementación y análisis de la presente tesis se puede indicar que existen varias herramientas que ayudar a un administrador de red a obtener detalladamente sus dispositivos administrados. Se usó inSSIDer el cual es compatible con Windows el mismo que nos ayuda a verificar de una manera sencilla y práctica la configuración de nuestros dispositivos AP. Cascade Pilot que nos facilitó con el análisis de la red creando diferentes reportes estadísticos los cuales son realizados en base a la paquetería obtenida al realizar un sniffing el mismo que se lo ejecutó con Wireshark.

- La generación de tráfico realizada con D-ITG ayudó para poder realizar la implementación y análisis de escenarios donde el interés del administrador se centra en verificar la calidad del canal y el comportamiento de la red cuando se tiene la presencia de un equipo que produce interferencia.
- En relación a los valores de señal y ruido que se obtienen tanto en los reportes de Cascade Piloto como los valores que se pueden visualizar en las tramas de la captura de paquetes de Wireshark podemos como administradores de red tener una idea de la calidad de la señal y el servicio que estamos proporcionando y la distancia a la cual nos presentamos del AP.
- El uso de seguridad dentro de una red inalámbrica es de mucha importancia para poder cubrir vulnerabilidades externas a la red. El uso de un servidor de autenticación como RADIUS es de gran ayuda para evitar este tipo de vulnerabilidades ya que los usuarios para poder tener conectividad en la red deberá autenticarse y así podemos tener un mayor control de nuestra red.
- Al monitorear el tráfico de red con una sola tarjeta AirPcap solo podemos cubrir el canal al cual ha sido configurado, pero al momento de colocar 2 o más tarjetas para actuar como monitores de tráfico podemos abarcar un espacio mucho más grande y con esto poder realizar un barrido más completo de las señales y los paquetes que se transmiten en nuestra red así los equipos estén configurados en diferentes frecuencias.
- Se verificó el comportamiento de un dispositivo al momento de realizar Roaming en el cual una de las tarjetas estará configurada en un canal y la otra en otro distinto y podremos visualizar lo que ocurre cuando el dispositivo asociado a un AP pierde señal y se conecta automáticamente a otro AP que presenta una mejor señal, todos estos valores los verificamos en la captura de tramas capturadas y analizadas con Wireshark usando los filtros y con la generación de reportes desde Cascade Pilot.

- Al tener presente un tráfico multicanal van a existir paquetes que se van a perder, esto se debe a la existencia de una cantidad muy grande de paquetes que están circulado por la red y que las herramienta de análisis no son capaces de capturar en su totalidad ya que se tiene un tiempo muy corto para poder capturar todos los paquetes involucrados.
- En la implementación de Escenarios con presencia de Interferencia se obtuvo tiempos de Delay y jitter muy diferentes en las diferentes pruebas realizadas, esto se debe a que por el canal sea este cableado o inalámbrico se pierden paquetes por la presencia de factores externos al ambiente o al medio de comunicación entre los AP.
- Para tener un control de nuestra red y poder conocer el motivo de algún comportamiento extraño debemos conocer los equipos y MAC de los equipos que se asocian, con esto a la presencia de un dispositivo externo será mucho más fácil identificar el inconveniente o si estamos presentes a una vulnerabilidad de red.
- Wireshark una aplicación libre y una de las más usadas a nivel de análisis y estudio para verificar el comportamiento de una red. Con el uso de filtros se pudo obtener información detallada de las tramas y con esto se pudo identificar el comportamiento de los diferentes escenarios y de los equipos involucrados.
- SteelCentral Packet Analyzer es una herramienta pagada que nos permite visualizar mediante filtros información de nuestro interés, estos datos los podemos visualizar de manera estadística y generar reportes.

5.2. Recomendaciones

- Como recomendaciones dentro de este proyecto se puede mencionar que existen diferentes programas que nos ayudan para poder realizar un análisis de la red en cualquier entorno que lo estemos implementando. Lo importante es saber aprovechar al máximo las características de cada uno de ellos y poder sacar las mejores conclusiones sobre el

comportamiento de la red para poder ofrecer un servicio óptimo y eficiente.

- De acuerdo a la posibilidad económica que tenga el administrador o la empresa que desee realizar el análisis de su red en los diferentes aspectos, podríamos ver la posibilidad de adquirir un software de los analizados ya que en su mayoría son pagados por su gran diversidad de herramientas que nos presta para poder hacer el análisis como SteelCentral Packet Analyzer.
- Una de las incertidumbres más grandes que se puede presentar al momento de querer analizar una red inalámbrica es el saber en qué lugar se debe colocar el monitor, cerca del AP o cerca del cliente, para poder tener una respuesta a esta incertidumbre debemos analizar dos temas importantes y saber qué es lo que estamos buscando con este análisis, si buscamos niveles de servicio para el cliente o el AP, con esta aclaración del panorama podremos colocar el monitor en la posición correcta y poder realizar un análisis mucho más real de la necesidad que nuestra red presenta.
- Plantearse el motivo por el cual se necesita conocer el estado de la red inalámbrica, ya que con este criterio podemos saber la ubicación de los equipos de monitoreo y conocer los nivele de servicio dependiendo el criterio del administrador, sea este basado en el nivel de servicio al cliente o al Access Point.
- La implementación de las aplicaciones como el Rogue Ap muestran lo insegura que puede ser una red inalámbrica IEEE802.11 por lo cual los administradores de red deberían enfocar en primera instancia a capacitar a los usuarios para que tengan presente los riesgos que implicaría para una empresa los diferentes tipos de ataques inalámbricos. En el caso específico del rogué Ap el atacante puede obtener la MAC de un equipo de red válido y tratar de generar tramas con esta trama para obtener mayor detalle de configuraciones de la red inalámbrica con la idea principal de producir daños en la infraestructura de red.

REFERENCIA BIBLIOGRÀFICA

Aguero Calvo, R. (s.f.). *Redes Inalámbricas/Redes de Acceso Celular.* Obtenido de http://www.tlmat.unican.es/siteadmin/submaterials/987.pdf

Alessio Botta, W. d. (28 de OCTUBRE de 2013). *D-ITG MANUAL.* Obtenido de http://traffic.comics.unina.it/software/ITG/manual/D-ITG-2.8.1-manual.pdf

Alfon. (11 de 05 de 2011). *daboweb Análisis de capturas de red con CACE Pilot Personal Edition.*

Bedoya, K., & Medina, A. (2010). Tecnologías Inalámbricas. *Administración de redes*, 4.

Berg, J. (2011). *Radiotap*. Obtenido de http://www.radiotap.org/

Bernal, I. (2005). Comunicaciones Inalámbricas Estandar IEEE 802.11. *Comunicaciones Inalámbricas.* Quito.

Bernal, I. (Noviembre de 2005). *IEEE 802.11 MAC.* Obtenido de http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Inalambricas/CLASES/802-11ParteIb.pdf

Borja Meino, F. (2011). *ANÁLISIS DE TRÁFICO CON WIRESHARK.*

Broadcom. (2015). *BCM4330*. Obtenido de http://www.broadcom.com/products/Wireless-LAN/802.11-Wireless-LAN-Solutions/BCM4330

CACE Technologies. (2009). *Per Packet Information Header Specification*. Obtenido de http://www.cacetech.com/documents/PPI%20Header%20format%201.0.10.pdf

Cace Technologies. (s.f.). *AirPcap.* Obtenido de http://www.cacetech.com/documents/AirPcap%20Nx%20Datasheet.pdf

Chiu, S. H. (s.f.). Seguridad en Redes Inalámbricas 802.11. *Seguridad en Redes Inalámbricas 802.11*.

Cisco Networking Academy. (s.f.). *Fundamentals of Wireless LANs*. Obtenido de https://es.scribd.com/doc/73328010/Fundamentals-of-Wireless-Lan-1

Distech. (s.f.). *Distech Intel Pro/Wireless 3945ABG PCIe mini card*. Obtenido de http://disctech.com/Intel-Pro-Wireless-3945ABG-PCIe-mini-card

Dlink. (2014). *DIR-615.* Obtenido de http://www.dlinkla.com/dir-615

Dlink. (2014). *DWA-110*. Obtenido de http://www.dlinkla.com/dwa-110

D-Link. (s.f.). *Wireless N 300 Router DIR-619*. Obtenido de http://www.dlinkmea.com/site/index.php/site/productDetails/503

Frenzel, Carrasco, Monachesi, & Chaile. (2010). *Edutecne Física de las Ondas Radioeléctricas dentro del Estándar IEEE802.11b.* Obtenido de http://www.edutecne.utn.edu.ar/wlan_frt/fis_ondas_rad_IEEE802-11b.pdf

Gallegos León, J., & Ruiz Delgado, J. M. (2011). Analizadores de protocolos. *Manual de Wreshark*.

García Galende, O. (s.f.). *IEEE 802.11 Equipos y sistemas de transmisión*. Obtenido de Sistema de Transporte de Datos: http://www.microalcarria.com/descargas/documentos/Wireless/Redes_Inalambricas_802.11b.pdf

Gimenez, R. A. (2008). *Analisis de la seguridad en redes.* Valencia: Universidad de Valencia.

IEEE STANDARS ASSOCIATION. (2012). *standards.ieee.org.* Obtenido de http://standards.ieee.org/about/get/802/802.11.html

Medellin. (s.f.). *Academia.edu ADMINISTRACIÓN Y SEGURIDAD DE REDES.* Obtenido de http://www.academia.edu/7365349/Unidad_V_Monitoreo

Metageek, I. (2014). *inSSIDer*. Obtenido de http://www.inssider.com/inssider4/es/

Metro Mexico. (2006). *metrologicmexico.* Obtenido de http://www.metrologicmexico.com/contenido1/informacion_tecnica/estandares_inalambricos.php

Modem Help UK Atheros AR5B95 11bgn PCIe Mini-Card Reference Design. (s.f.). Obtenido de http://www.modem-help.co.uk/Atheros/AR5B95-11bgn-PCIe-Mini-Card-Reference-Design.html

Navarro Gavira, S. (2005). *Algoritmos Cross-Layer para la Optimización de las prestaciones del TCP en redes Wireless Ad-hoc.* Obtenido de http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F07+-+Capitulo+2.pdf

Nigel. (2013). *What are RadioTap Headers?* Obtenido de http://wifinigel.blogspot.com/2013/11/what-are-radiotap-headers.html

Riverbed. (s.f.). *SteelCentral Packet Analyzer Personal Edition*. Obtenido de http://es.riverbed.com/products/performance-management-control/network-performance-management/packet-analysis.html

SCOS Software. (s.f.). *AirPcap*. Obtenido de http://www.airpcap.nl/airpcap-nx.htm

SERVERCOMP Computing Systems. (s.f.). *servercomp*. Obtenido de http://www.servercomp.com/index.php/es/redes-informaticas-en-girona-barcelona-lloret-de-mar-blanes-tossa-de-mar-vidreres-malgrat-de-mar-granollers-sabadell-mataro-badalona-manresa-terrassa-figueres-olot-banyoles/wifi-redes-inalambricas-lloret-de-mar-tossa

Sons, J. W. (2005). Hacking Techniques in Wireless Networks. *Hacking Techniques in Wireless Networks*.

Sons, J. W. (2005). *Hacking Techniques in Wireless Networks.* Obtenido de http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524695

Stalings, W. (2002). *Wireless Communications and Networks.* Prentice Hall.

Stalings, W. (2004). *Comunicaciones y Redes de Computadores.* Madrid: Prentice Hall Pearson Educacion.

TamoSoft. (1998). *Tama Soft*. Obtenido de http://www.tamos.com/products/commview/

Tanenbaum, A. (2003). *Redes de computadoras.* Mexico: Prentice Hall Pearson Education.

TP-LINK. (s.f.). *Router inalámbrico eXtended Rang de 54 Mbps (Producto Descontinuado)*. Obtenido de http://www.tp-link.com/ar/products/details/?model=TL-WR541G

Wheelers Lane Technology College. (s.f.). Familia IEEE 802.11. En *Redes de Área Local Inalámbrica.*

Wikipedia. (s.f.). *Espectro ensanchado por salto de frecuencia*. Obtenido de http://es.wikipedia.org/wiki/Espectro_ensanchado_por_salto_de_frecuencia

Wikipedia. (s.f.). *Espectro ensanchado por secuencia directa*. Obtenido de http://es.wikipedia.org/wiki/Espectro_ensanchado_por_secuencia_directa

Wikipedia. (s.f.). *IEEE 802.11*. Obtenido de http://es.wikipedia.org/wiki/IEEE_802.11#802.11n

Yunquera Torres, J. J. (s.f.). *bibing.us.es .* Obtenido de http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FPortada.pdf

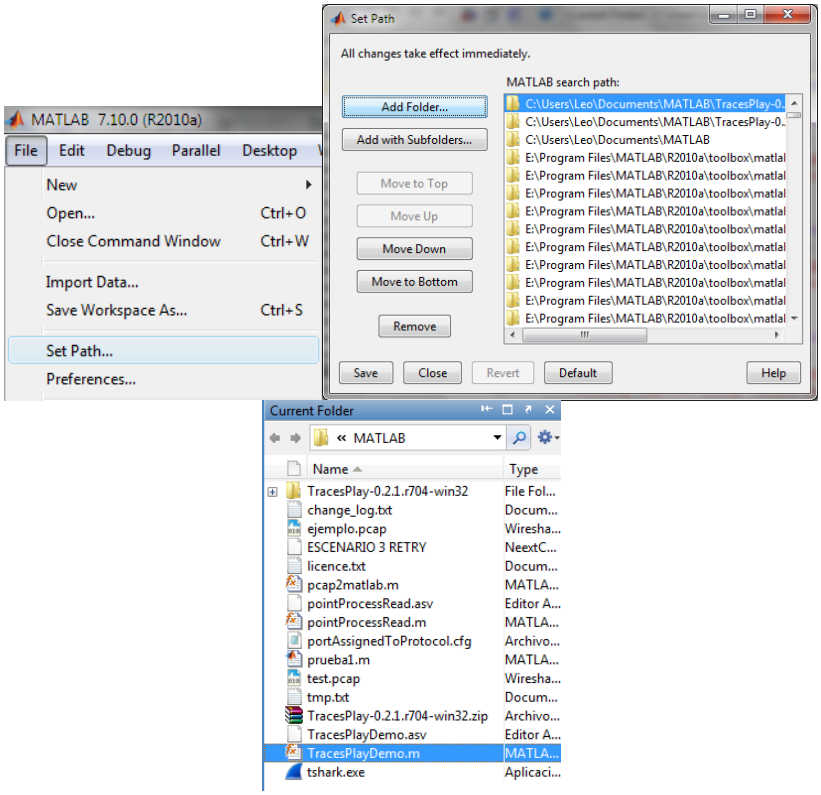
ANEXOS

Matlab es una herramienta de análisis matemático que puede ser utilizada para aplicar monitoreo. Este hecho es posible gracias a la programación que permite Matlab por lo general usuarios de internet comparten funciones específicas para realizar diferentes procesos en este caso la captura o filtrado de archivos .pcap desde Matlab.

Se verifico dos tipos de procesos uno mediante la adición de librerías y otro mediante la aplicación de funciones.

La primera forma nos comparte TracesPlay que es un plugin que se añade a Matlab para poder obtener matrices con información numérica sobre tiempos, tamaños entre otras cosas.

Para añadir este plugin a través de File la opción Set Path nos envía a una ventana la cual nos permite añadir la carpeta donde se encuentran los plugin del programa una vez guardados se podrán usar como una función más de Matlab.



Con el fin de utilizar esta librería la misma página de Traces Play comparte las opciones disponibles necesarias para poder realizar análisis de tráfico.

Presentaremos algunos de ellos mediante la siguiente tabla.

Opcion	Definicion
-o	**Configure el tipo de campo a ser leido**
-r (file name)	**Antecede al nombre del archivo a ser utilizado para análisis**
-n	**Se utiliza para analizar un rango de paquetes**
-w (file_name)	**Escribe los datos sobre un archive CSV**
-version	**Fecha de compilación del programa**
-a	**Muestra fechas**
-c	**Escribe el encabezado al archivo**
-h	**Despliega una pequeña ayuda**
-ss	**print on screen protocol information (value of protocol fields)**
-f	**Habilita filtros**

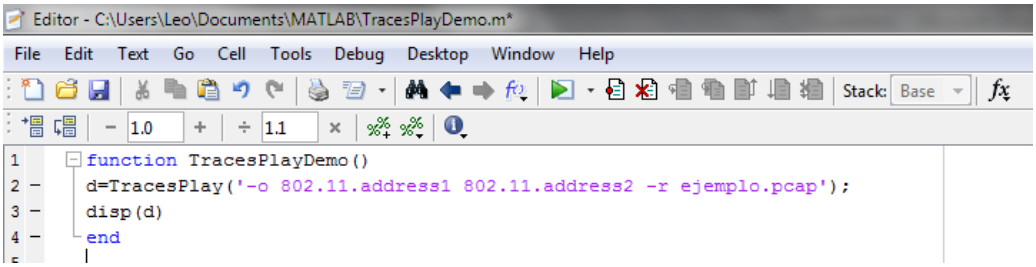
De igual forma los campos soportados son variados entre los que se destacan

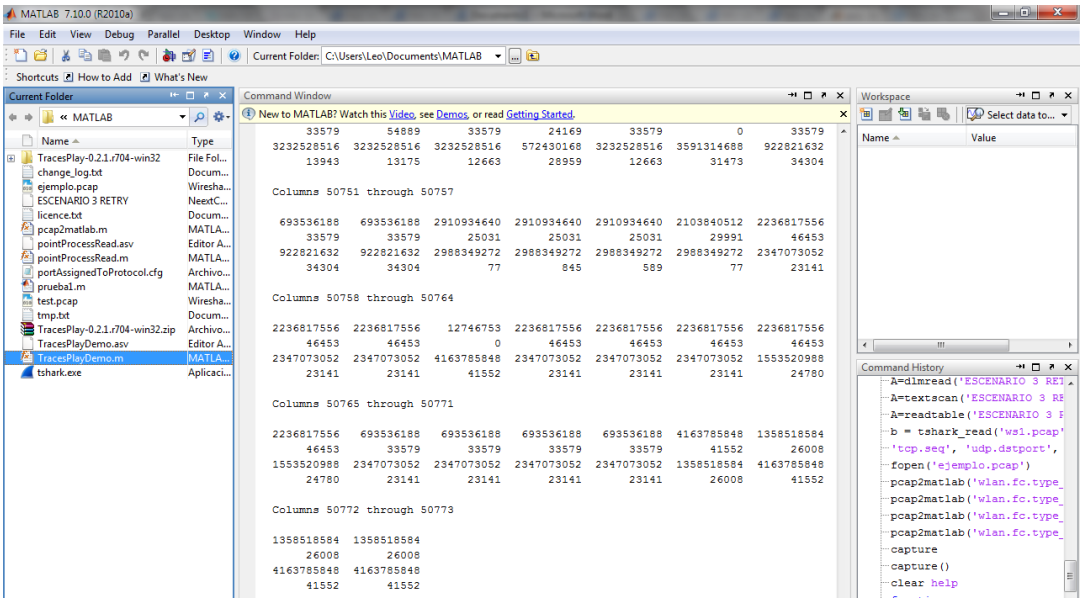
- 802.11.fc
- 802.11.fc.pro_ver
- 802.11.fc.type
- 802.11.fc.subtype
- 802.11.fc.to_ds
- 802.11.fc.from_ds
- 802.11.fc.moreflag
- 802.11.fc.retry
- 802.11.fc.power_mgt
- 802.11.fc.more_data
- 802.11.fc.wep
- 802.11.fc.order
- 802.11.duration_id
- 802.11.address1
- 802.11.address2

- 802.11.address3
- 802.11.address4
- 802.11.da
- 802.11.sa
- 802.11.ra
- 802.11.ta
- 802.11.bssid
- 802.11.bar_control
- 802.11.block_ack
- 802.11.block_ack_bitmap
- 802.11.seq_control
- 802.11.qos_control
- 802.11.seq_control
- 802.11.fra_control
- RADIOTAP.version
- RADIOTAP.pad
- RADIOTAP.len
- RADIOTAP.present
- RADIOTAP.mactime
- RADIOTAP.flags
- RADIOTAP.datarate
- RADIOTAP.channal_requency
- RADIOTAP.channal_flags
- RADIOTAP.hop_set
- RADIOTAP.hop_pattern
- RADIOTAP.dbm_ant_signal
- RADIOTAP.dbm_ant_noise
- RADIOTAP.lock_quality
- RADIOTAP.tx_attenuation
- RADIOTAP.db_tx_attenuation
- RADIOTAP.dbm_tx_power

- RADIOTAP.anntenna
- RADIOTAP.db_ant_signal
- RADIOTAP.db_ant_noise
- RADIOTAP.channal_plus

Para aplicar un ejemplo de uso de la función se puede utilizar la función utilizando los comandos disponibles en Matlab



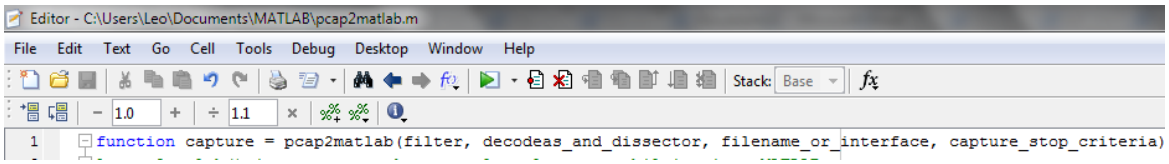


http://tracesplay.sourceforge.net/index.html

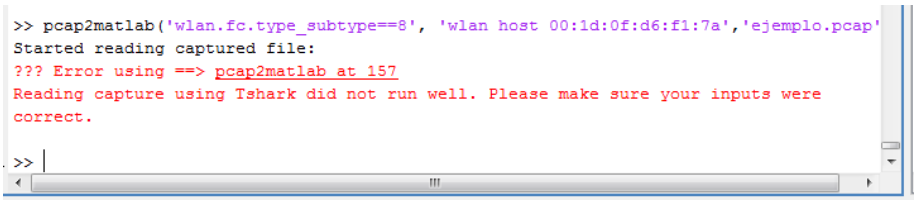
La segunda forma de análisis es implementada por el usuario Alon Geva que implemento una función compatible con las opciones que dispone tshark para monitoreo.

Básicamente en esta función necesita tres parámetros de entrada un filtro, el disector utilizado para lectura que básicamente es los tamaños de paquetes que utiliza un programa de monitoreo para contener la información

capturada, el archivo o interfaz de la cual se debe realizar la captura o análisis y finalmente el parámetro de salida que se utilizaría en caso de presentarse el monitoreo desde la interfaz.



A continuación se muestra un ejemplo de uso de la función desde el workspace de Matlab.



Debe considerarse tres cosas para aplicar la función la primera es que se tenga instalado tshark, la segunda es que se disponga de los comandos utilizados en tshark y la tercera es que el archivo a ser analizado debe estar en formato .pcap y compartido en la carpeta donde se analizan los archivos .m de Matlab.

En las pruebas a pesar de cumplir con los parámetros requeridos y seguir las indicaciones que muestra la función insertadas dentro de la misma no se pudo completar el análisis la cuasa que mostro la función es debido al disector insertado que en el caso del ejemplo fue wlan host MAC 00:1d:0f:d6:f1:7a.

Se comparte la función encontrada en los anexos así como la respectiva fuente de consulta:

http://www.mathworks.com/matlabcentral/fileexchange/44265-pcap2matlab---importing-network-protocol-analyzer-capabilties-into-matlab

function capture = pcap2matlab(filter, decodeas_and_dissector, filename_or_interface, capture_stop_criteria)

% pcap2matlab() imports network protocol analyzer capabilties into MATLAB.

%

% capture = pcap2matlab(filter, decodeas_and_dissector,filename_or_interface, capture_stop_criteria)

% allows to perform direct network live captures as well as *.pcap files reading from the MATLAB

% workspace. The output variable is a MATLAB structure, one entry for each captured packet,

% comprising the content of the packet fields that were requested by the input arguments.

% The function is based on the TShark network protocol analyzer (see http://www.wireshark.org/docs/man-pages/tshark.html

% for more information) and can operate in two modes:

% 1. Capture mode in which it starts listening on the requested network interface, capturing

% packets based on some predefined criteria (i.e. filter) and output the relevant packet fields

% based on the decodeas and dissector input arguments.

% 2. Read mode in which it reads an already existing pcap file, extract packets based on some

% predefined criteria (i.e. filter) and output the relevant packet fields based on the

% decodeas and dissector input arguments.

% The function currently supports PC 32/64-bit as well as Linux 32/64-bit platforms.

% Other platforms might be easily added in the future.

%

% Input arguments:

% * filter – A TShark format capture filter argument (tshark -f flag like 'net 10.10.10.4 and src port 12001')

```
    %                   or a display filter argument (tshark –Y flag like
'ip.src==10.10.10.4 and udp.srcport==12001')
    %             depending on the selected mode of operation (i.e. capture or
read).
    %                              For more information please revert to
http://wiki.wireshark.org/CaptureFilters and
    %          http://wiki.wireshark.org/DisplayFilters.
    %   * decodeas_and_dissector – This input argument can be one of the
following things:
    %             1.  A MATLAB structure whose field names are the requested
packet field names to capture
    %              whereas the content of each field, of this structure, comprises
the byte offsets to
    %              capture for this specific field. The content of the structure can
be one of the following:
    %                (a) A MATLAB decimal vector specifying the byte offsets to
capture. For example:
    %
    %                        decodeas_and_dissector.sn = [43 44 45 46]
    %                        decodeas_and_dissector.timestamp: [47:54]
    %
    %                 will instruct the function to capture 2 fields named "sn" and
"timestamp" with byte offsets
    %                 43-46 and 47-54 respectively. The offset is calculated from
the very first byte (offset 0)
    %                 of the packet including the layer 2 portion (starting from the
MAC destination address in
    %                 the case of an Ethernet frame). The returned value will be a
decimal number representing
    %                 the total decimal value of these aggregated byte offsets.
    %                      (b) A string comprising the offset bytes to capture in
hexadecimal representation. For example:
```

```
%
%                       decodeas_and_dissector.sn = '43:46'
%                       decodeas_and_dissector.timestamp: '47:54'
%
%               will instruct the function to capture 2 fields named "sn" and "timestamp" with byte offsets
%               43-46 and 47-54 respectively. The offset is calculated from the very first byte (offset 0)
%               of the packet including the layer 2 portion (starting from the MAC destination address in
%               the case of an Ethernet frame). The returned value will be a string comprising the entire
%               content of these byte offsets (if only a single byte offset is required the colon can be
%               removed. For example: decodeas_and_dissector.sn = '43').
%               (c) Same as (b) with additional '/' character followed by specific BIT offsets to be extracted
%               from the specified byte offsets (specified before the '/'). For example, the dissector lines:
%
%                       decodeas_and_dissector.firstflag = '43/0:1'
%                       decodeas_and_dissector.secondflag = '45/6'
%
%               will instruct the function to capture MSB bits 0:1 from byte offset 43 in the 'firstflag'
%               field and bit 6 from byte offset 45 in the 'secondflag' field. The returned value is a
%               decimal number of the value of the extracted bits.
%
%           2.  A one-dimensional cell of strings comprising the TShark decodeas expression (TShark
```

```
%               -d flag) (not mandatory but if appears must be the first one) as
well as additional
%               TShark dissector expressions (TShark -e flag). Each dissector
expression will
%               results in a matching field in the output captured struct.
%               For example: the following cell of strings
%
{'tcp.port==8888,http';'frame.number';'frame.time';'tcp.length';'tcp.srcport'}
%                 will instruct the function to decode the captured packet with
TCP port 8888 as http.
%                  Then, extracting the following 4 fields from each captured
packet: frame.number,
%                 frame.time, tcp.length and tcp.srcport to the output capture
struct:
%
%                                   capture =
%                                   1x97 struct array with fields:
%                                       framenumber
%                                       frametime
%                                       tcplength
%                                       tcpsrcport
%
%       For more information on TShark's decodeas and dissection fields
options please refer to:
%       http://www.wireshark.org/docs/man-pages/tshark.html
%    * filename_or_interface – This input argument can be one of two
things:
%           1.  An integer number that identifies the network interface from
which to start
%                 capturing (TShark -i flag). Setting this input argument to an
integer number will
%               automatically set the function to work in capture mode.
```

```
%           2.  A filename string that identifies the pcap file to read. Setting this input argument
%               to a filename string will automatically set the function to work in read mode.
%   * capture_stop_criteria – Relevant for capture mode only (should not be assigned when working in
%           read mode). Sets the capture 'stop capturing' criteria (TShark -a/-c flags). This input
%         argument can be one of the following things:
%           1. A numeric number that sets the total number of packets to capture (TShark -c flag).
%           2. A string that identifies the capture stop criteria (TShark -a flag).
%           3. A cell array combining a few legal capture stop criteria arguments such as
%           {'duration:10',100} that will stop capturing after 10 sec or 100 packets whichever
%           comes first.
%         For more information on TShark's stop capturing criteria options please refer to:
%         http://www.wireshark.org/docs/man-pages/tshark.html.
%
%   Alon Geva
%   $Revision: 1.03 $  $Date: 25/04/2014 01:52:53 $

    OS = computer;
    WSdissector_FLAG = iscell(decodeas_and_dissector);
    capture_FLAG = ~ischar(filename_or_interface);

    switch OS
       case {'PCWIN','PCWIN32','PCWIN64'}
    %       os_cmd = 'dos';
```

```
            separator_char = ';';
        case {'GLNXA64','GLNX86'}
    %       os_cmd = 'unix';
            separator_char = '\;';
    end

    if ~isempty(filter)
        capture_filter_str = [' -f "' filter '"'];
        read_filter_str = [' -Y "' filter '"'];
    else
        capture_filter_str = '';
        read_filter_str = '';
    end

    capture_stop_str = [];
    if exist('capture_stop_criteria','var')
        if iscell(capture_stop_criteria)
            for idx=1:numel(capture_stop_criteria),
                if isnumeric(capture_stop_criteria{idx})
                    capture_stop_str = [capture_stop_str ' -c ' num2str(capture_stop_criteria{idx})];
                else
                    capture_stop_str = [capture_stop_str ' -a ' capture_stop_criteria{idx}];
                end
            end
        else
            if isnumeric(capture_stop_criteria)
                capture_stop_str = [' -c ' num2str(capture_stop_criteria)];
            else
                capture_stop_str = [' -a ' capture_stop_criteria];
            end
```

```
        end
    end

    if (capture_FLAG) % capture mode
        fprintf(['Started capturing from network interface #' int2str(filename_or_interface) ':\n']);
    %       eval(['status=' os_cmd '("tshark -i ' int2str(filename_or_interface) capture_stop_str ' -w tmp.pcap' capture_filter_str '");'])
        eval(['status=system("tshark -i ' int2str(filename_or_interface) capture_stop_str ' -w tmp.pcap' capture_filter_str '");'])

        assert(~status,'Capture using Tshark did not run well. Please make sure your inputs were correct.')
        read_filename = 'tmp.pcap';
    else
        read_filename = filename_or_interface;
    end

    if (~WSdissector_FLAG) % using MATLAB defined disssector
        fprintf('Started reading captured file:\n');
        if (capture_FLAG)
            eval(['status=system("tshark -r ' read_filename ' -F k12text -w tmp.txt");'])
        else
            eval(['status=system("tshark -r ' read_filename ' -F k12text' read_filter_str ' -w tmp.txt");'])
        end
        assert(~status,'Reading capture using Tshark did not run well. Please make sure your inputs were correct.')

    else
```

```
        usingdecodeas_FLAG                                          =
~isempty(regexp(decodeas_and_dissector{1},'==','ONCE'));
        if usingdecodeas_FLAG
            decodeas_str = [' -d ' decodeas_and_dissector{1}];
        else
            decodeas_str = '';
        end

        FieldsofDissector                                           =
decodeas_and_dissector(1+usingdecodeas_FLAG:end);
        SizeofDissector = max(size(FieldsofDissector));
        WSdissector_str = [];
        for idx=1:SizeofDissector,
            WSdissector_str = [WSdissector_str ' -e ' FieldsofDissector{idx} ' '];
        end

        if (capture_FLAG)
            eval(['status=system(''tshark -r ' read_filename decodeas_str ' -T
fields -E separator=' separator_char  WSdissector_str ' > tmp.txt '');'])
        else
            eval(['status=system(''tshark -r ' read_filename decodeas_str ' -T
fields -E separator=' separator_char  WSdissector_str  read_filter_str ' >
tmp.txt '');'])
        end
        assert(~status,'Reading capture using Tshark did not run well. Please
make sure your inputs were correct.')
    end

    FILEREADBLOCKSIZE = 10000; % MUST be a multiple of 5 derived
from K12text file format.

    fprintf('Started importing to MATLAB:\n');
```

```
    if (~WSdissector_FLAG) % using MATLAB struct defined disssector

        % dissecting k12text file
        fid = fopen('tmp.txt');
        n = 0;
        while ~feof(fid)
            n = n + sum( fread( fid, 16384, 'char' ) == char(10) );
        end
        n = n / 4;
        fclose(fid);

    %     dissector_base_FLAG = 10*ones(1,);
    %     if (isfield(decodeas_and_dissector,'base'))
    %         switch decodeas_and_dissector.base
    %             case {'dec'}
    %                 dissector_base_FLAG = 10;
    %             case {'hex'}
    %                 dissector_base_FLAG = 16;
    %             otherwise
    %                     assert('Currently the only supported dissector bases are
DEC and HEX');
    %         end
    %                                                 decodeas_and_dissector      =
rmfield(decodeas_and_dissector,'base');
    %     end

        FieldsofDissector = fieldnames(decodeas_and_dissector);
        SizeofDissector = max(size(FieldsofDissector));

        dissector_weights = cell(SizeofDissector,1);
        capture_template = struct();
```

```
        capture_template.frametime = 0;
        dissector_base_FLAG = 10*ones(1,SizeofDissector); % default is
decimal base dissection

        for idx=1:SizeofDissector,
            capture_template.(FieldsofDissector{idx}) = 0;
%setfield(capture,FieldsofDissector(idx),[]);
            if ischar(decodeas_and_dissector.(FieldsofDissector{idx}))
                dissector_base_FLAG(idx) = 16;
            end

            switch dissector_base_FLAG(idx)
                case {10}
                    dissector_weights{idx,1} =
256.^(length(decodeas_and_dissector.(FieldsofDissector{idx}))-1:-1:0);
                    decodeas_and_dissector.(FieldsofDissector{idx}) =
decodeas_and_dissector.(FieldsofDissector{idx}) + 1; %+1 added on 15/1/14
to make the offset of the first byte 0
                case {16}
                    tmp =
decodeas_and_dissector.(FieldsofDissector{idx});tmp_colon = find(tmp ==
':');tmp_slash = find(tmp == '/');

                    if isempty(tmp_slash)
                        TMP_SLASH_FLAG = 0;
                        tmp_slash = length(tmp);
                    else
                        TMP_SLASH_FLAG = 1;
                    end

                    if (isempty(tmp_colon))
                        TMP_COLON_FLAG = 0;
```

```
            elseif (length(tmp_colon) == 2)
                TMP_COLON_FLAG = 2;
            elseif (tmp_colon < tmp_slash)
                TMP_COLON_FLAG = -1;
            else
                TMP_COLON_FLAG = +1;
            end

            % part A
            if (TMP_COLON_FLAG == -1) || (TMP_COLON_FLAG == 2)%~(isempty(tmp_colon)) && (isempty(tmp_slash))
                decodeas_and_dissector.(FieldsofDissector{idx}) = hex2dec(tmp(1:tmp_colon(1)-1)) : hex2dec(tmp(tmp_colon(1)+1:tmp_slash-1));
                decodeas_and_dissector.(FieldsofDissector{idx}) = reshape([decodeas_and_dissector.(FieldsofDissector{idx})*2+1;decodeas_and_dissector.(FieldsofDissector{idx})*2+2],1,length(decodeas_and_dissector.(FieldsofDissector{idx}))*2);
            else
                decodeas_and_dissector.(FieldsofDissector{idx}) = hex2dec(tmp(1:tmp_slash-1));
                decodeas_and_dissector.(FieldsofDissector{idx}) = reshape([decodeas_and_dissector.(FieldsofDissector{idx})*2+1;decodeas_and_dissector.(FieldsofDissector{idx})*2+2],1,length(decodeas_and_dissector.(FieldsofDissector{idx}))*2);
            end
            % part B
            if (TMP_SLASH_FLAG)
                if (TMP_COLON_FLAG == +1)
                    decodeas_and_dissector.(FieldsofDissector{idx}) = {decodeas_and_dissector.(FieldsofDissector{idx}),
```

```
hex2dec(tmp(tmp_slash+1:tmp_colon(1)-
1))+1:hex2dec(tmp(tmp_colon(1)+1:end))+1};
                elseif (TMP_COLON_FLAG == 2)
                    decodeas_and_dissector.(FieldsofDissector{idx})          =
{decodeas_and_dissector.(FieldsofDissector{idx}),
hex2dec(tmp(tmp_slash+1:tmp_colon(2)-
1))+1:hex2dec(tmp(tmp_colon(2)+1:end))+1};
                else
                    decodeas_and_dissector.(FieldsofDissector{idx})          =
{decodeas_and_dissector.(FieldsofDissector{idx}),
hex2dec(tmp(tmp_slash+1:end))+1};
                end
            end
        end
    end



    %    for idx=1:SizeofDissector,
    %                        capture_template.(FieldsofDissector{idx})   =   0;
%setfield(capture,FieldsofDissector(idx),[]);
    %        if ischar(decodeas_and_dissector.(FieldsofDissector{idx}))
    %            dissector_base_FLAG(idx) = 16;
    %        end
    %        switch dissector_base_FLAG(idx)
    %            case {10}
    %                                                dissector_weights{idx,1}   =
256.^(length(decodeas_and_dissector.(FieldsofDissector{idx}))-1:-1:0);
    %                        decodeas_and_dissector.(FieldsofDissector{idx}) =
decodeas_and_dissector.(FieldsofDissector{idx}) + 1; %+1 added on 15/1/14
to make the offset of the first byte 0
    %            case {16}
```

```
    %                                                                   tmp     =
decodeas_and_dissector.(FieldsofDissector{idx});tmp_colon  =  find(tmp  ==
':');tmp_slash = find(tmp == '/');
    %               if ~(isempty(tmp_colon)) && (isempty(tmp_slash))
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
hex2dec(tmp(1:tmp_colon-1)) : hex2dec(tmp(tmp_colon+1:end));
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
reshape([decodeas_and_dissector.(FieldsofDissector{idx})*2+1;decodeas_a
nd_dissector.(FieldsofDissector{idx})*2+2],1,length(decodeas_and_dissector.
(FieldsofDissector{idx}))*2);
    %               elseif (isempty(tmp_slash))
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
hex2dec(tmp(1:end));
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
reshape([decodeas_and_dissector.(FieldsofDissector{idx})*2+1;decodeas_a
nd_dissector.(FieldsofDissector{idx})*2+2],1,length(decodeas_and_dissector.
(FieldsofDissector{idx}))*2);
    %               else %tmp_slash not empty
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
hex2dec(tmp(1:tmp_slash-1));
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
reshape([decodeas_and_dissector.(FieldsofDissector{idx})*2+1;decodeas_a
nd_dissector.(FieldsofDissector{idx})*2+2],1,length(decodeas_and_dissector.
(FieldsofDissector{idx}))*2);
    %                   if (isempty(tmp_colon))
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
{decodeas_and_dissector.(FieldsofDissector{idx}),
hex2dec(tmp(tmp_slash+1:end))+1};
    %                   else
    %                       decodeas_and_dissector.(FieldsofDissector{idx}) =
{decodeas_and_dissector.(FieldsofDissector{idx}),
```

```
hex2dec(tmp(tmp_slash+1:tmp_colon-
1))+1:hex2dec(tmp(tmp_colon+1:end))+1};
    %                 end
    %             end
    %       end
    %    end

      capture(1:n) = capture_template;

      fid = fopen('tmp.txt');
      dstlineidx = 0;

      while (~feof(fid))%~isempty(line{1})

        linestr = textscan(fid,'%s',FILEREADBLOCKSIZE);


        for srclineidx = 1:5:length(linestr{1}),

          line = linestr{1}{srclineidx+1};
          dstlineidx = dstlineidx + 1;

          capture(dstlineidx).frametime = str2double(line(1:2))* 3600 + ...
            str2double(line(4:5))* 60 + ...
            str2double(line(7:8))* 1 + ...
            str2double(line(10:12))* 1e-3 + ...
            str2double(line(14:16))* 1e-6;

          % packet_bytes
          line = linestr{1}{srclineidx+4};
          packet_tokens   =   regexp(line,'([0-9a-fA-F]{2})','tokens');
          tmp             =   [packet_tokens{:}];
```

```
            packet_bytes_10                                          =
hex2dec(reshape([tmp{:}],2,length(packet_tokens))');
            packet_bytes_16                                          =
[tmp{:}];%reshape([tmp{:}],2,length(packet_tokens))';

    %           switch dissector_base_FLAG
    %               case {10}
    %                                                   packet_bytes      =
hex2dec(reshape([tmp{:}],2,length(packet_tokens))');
    %               case {16}
    %                                                   packet_bytes      =
[tmp{:}];%reshape([tmp{:}],2,length(packet_tokens))';
    %           end

            for idx=1:SizeofDissector,
                switch dissector_base_FLAG(idx)
                    case {10}
                        capture(dstlineidx).(FieldsofDissector{idx})     =
dissector_weights{idx,1}                                                 *
packet_bytes_10(decodeas_and_dissector.(FieldsofDissector{idx}));
                    case {16}
                        if
~iscell(decodeas_and_dissector.(FieldsofDissector{idx}))
                            packet_bytes_extracted                       =
decodeas_and_dissector.(FieldsofDissector{idx});
                            capture(dstlineidx).(FieldsofDissector{idx})     =
packet_bytes_16(packet_bytes_extracted(packet_bytes_extracted           <=
length(packet_bytes_16)));
                        else % iscell TRUE
                            packet_bytes_extracted                       =
decodeas_and_dissector.(FieldsofDissector{idx});
```

```
                    capture(dstlineidx).(FieldsofDissector{idx})          =
packet_bytes_16(packet_bytes_extracted{1}(packet_bytes_extracted{1}    <=
length(packet_bytes_16)));
                    tmp                                                   =
dec2bin(hex2dec(capture(dstlineidx).(FieldsofDissector{idx})),8*length(packet
_bytes_extracted{1})/2);
                    capture(dstlineidx).(FieldsofDissector{idx})          =
dec2hex(bin2dec(tmp(packet_bytes_extracted{2})));
                end
            end

    %                       capture(dstlineidx).(FieldsofDissector{idx})  =
dissector_weights{idx,1}                                                  *
packet_bytes(decodeas_and_dissector.(FieldsofDissector{idx}));
            end
        end
    end


    else % using WS defined disssector

        % reading WS dissected text file
        fid = fopen('tmp.txt');
        n = 0;
        while ~feof(fid)
            n = n + sum( fread( fid, 16384, 'char' ) == char(10) );
        end
        fclose(fid);


        capture_template = struct();
```

```
        for idx=1:SizeofDissector,
            p = find(FieldsofDissector{idx} == '.');
            if ~isempty(p)
                FieldsofDissector{idx} = [FieldsofDissector{idx}(1:p-1)
FieldsofDissector{idx}(p+1:end)];
            end
            capture_template.(FieldsofDissector{idx}) = 0;
%setfield(capture,FieldsofDissector(idx),[]);
        end

        capture(1:n) = capture_template;

        fid = fopen('tmp.txt');
        dstlineidx = 0;

        while (~feof(fid))%~isempty(line{1})
            linestr = textscan(fid,'%s',FILEREADBLOCKSIZE,'delimiter','\n');

            for srclineidx=1:length(linestr{1}),
                line = linestr{1}{srclineidx};
                dstlineidx = dstlineidx + 1;

                main_parser = textscan(line,'%s','delimiter',';');
                Sizeof_main_parser = size(main_parser{1},1);

                for idx=1:min(SizeofDissector,Sizeof_main_parser),
                    switch (FieldsofDissector{idx})
                        case {'framenumber'}
                            capture(dstlineidx).framenumber =
str2double(main_parser{1}{idx});

                        case {'frametime'}
```

```
                    datetime_parser = textscan(main_parser{1}{idx},'%s');
                    capture(dstlineidx).frametime                    =
str2double(datetime_parser{1}{4}(1:2))* 3600 + ...
                        str2double(datetime_parser{1}{4}(4:5))* 60 + ...
                        str2double(datetime_parser{1}{4}(7:end))* 1;
                otherwise
                    if isempty(main_parser{1}{idx})
                        capture(dstlineidx).(FieldsofDissector{idx}) = 0;
                    elseif ~isempty(regexp(main_parser{1}{idx},'0x','ONCE'))
                        capture(dstlineidx).(FieldsofDissector{idx})     =
hex2dec(main_parser{1}{idx}(3:end));
                    else
                        capture(dstlineidx).(FieldsofDissector{idx})     =
str2double(main_parser{1}{idx});
                    end
                end
            end
        end
    end

    % deleting the temporary k12text file
    fclose all;
    delete('tmp.txt');
```

FECHA DE ENTREGA:

En la ciudad de Sangolquí, firman en constancia de la entrega del presente proyecto de Grado titulado "**HERRAMIENTES Y TÉCNICAS DE MONITORIZACIÓN DE TRÁFICO IEEE 802.11 A B G N MULTICANAL**", en calidad de Autores el Sr. Milton Leonardo Arguello Ramos y el Sr. Andrés Alejandro Vaca Villarreal, estudiantes de la carrera de Ingeniería Electrónica en Redes y Comunicación de Datos, y recibe por parte del Departamento de Eléctrica y Electrónica el Director de Carrera de Redes y Comunicación de Datos, el Señor Dr. Nikolai Espinosa.

---	---
Milton Leonardo Arguello Ramos	Vaca Villarreal Andrés Alejandro
1719303057	1719280818

Dr. Nikolai Espinosa
DIRECTOR DE LA CARRERA DE INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS