ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

ANÁLISIS DE TRÁFICO DE DATOS EN LA CAPA DE ENLACE DE UNA RED LAN, PARA LA DETECCIÓN DE POSIBLES ATAQUES O INTRUSIONES SOBRE TECNOLOGÍAS ETHERNET Y WiFi 802.11

VERÓNICA DEL ROCÍO OCHOA VILLALBA

SANGOLQUÍ – ECUADOR

2011

CERTIFICACIÓN

Certificamos que el presente proyecto titulado:

"ANÁLISIS DE TRÁFICO DE DATOS EN LA CAPA DE ENLACE DE UNA RED LAN, PARA LA DETECCIÓN DE POSIBLES ATAQUES O INTRUSIONES SOBRE TECNOLOGÍAS ETHERNET Y WiFi 802.11"

Ha sido desarrollado en su totalidad, por la Señorita: VERÓNICA DEL ROCÍO OCHOA VILLALBA, bajo la dirección de:

Ing. Carlos Romero	Ing. Gonzalo Olmedo, PHD
DIRECTOR	CO-DIRECTOR

RESUMEN

El presente proyecto tiene como finalidad detectar ataques que afecten la integridad/seguridad de la información de una Empresa u otros por medio del Análisis de Tráfico de Datos cursado en la Capa de Enlace en redes LAN sobre tecnologías Ethernet y WiFi 802.11. La información proporcionada por la capa MAC son: direcciones de origen/destino (MAC/IP); tramas 802,11.

Entre los ataques más comunes que pueden ejecutarse a nivel de la Capa de Enlace en redes LAN Inalámbricas están: ARP/MAC_Spoofing, DoS, Man_in_the_Midle(sniffing) o ataques pasivos como el Análisis de Tráfico. Para contrarrestar estos ataques existen protocolos de seguridad como: WEP, WPA (personal), WPA2 (empresarial), y mecanismos de detección y protección

El análisis de tráfico de datos se realiza bajo el Comportamiento Normal de la Red haciendo uso de software libre como son: WIRESHARK y COMMVIEW para el monitoreo y captura de paquetes. La red inalámbrica analizada corresponde a las Red WiFi de la ***Biblioteca Alejandro Segovia***: ***ESPE-WIFI-ZONA BIBLIO PISO 1***. Los resultados obtenidos del análisis del tráfico capturado proporcionan información de direcciones MAC/IP, tramas de administración, datos y control. Con esta información es posible ejecutar uno de los tipos de ataques indicados, los ataques pueden tener como objetivo analizar cuál sería el comportamiento de la Red frente a uno de estos ataques, o en su defecto atacar y afectar la Red analizada.

De éste análisis se puede concluir que el uso de mecanismos de seguridad implementados en una Red LAN (Ethernet/Inalámbrica) son necesarios y deben involucrar aspectos como: Protocolos de Seguridad, Mecanismos de Monitoreo/Detección, entre otros.

DEDICATORIA

A DIOS, por sus bendiciones y por haberme regalado una familia maravillosa; a mis Padres: Isabelita y Kléver, en especial a mi ***Madre*** por ser mi apoyo, ejemplo, y fortaleza en todo momento, por sus palabras de aliento en situaciones difíciles y tristes, por su amor, cariño y ternura incondicional, por no sólo ser Madre sino también mi Mejor Amiga. A mi Papi, que a pesar de la distancia siempre me ha apoyado y con sus palabras de amor ha estado presente durante esta etapa de vida universitaria.

A mis hermanos: Roberto, Hernán, Edgar, Jessy y Geovannia, mi ñaña política; mis loquitos bellos, por su amor, cariño y complicidad. A mi angelito bello Anthony, ya que su llegada y presencia a nuestro hogar ha sido motivo de alegría y felicidad. A todos mis familiares por su apoyo incondicional en todo momento.

A los Ingenieros, por brindarnos sus conocimientos, ayuda y tiempo; por hacernos partícipes de sus experiencias para prepararnos y proyectarnos como profesionales en el ambiente laboral.

Por último a lo más lindo que encontrado en la Universidad y Trabajo, Mis Amig@s, ya que con ustedes el día a día estudiantil y laboral es grato, lleno de experiencias y alegrías.

Verónica R. Ochoa V.

AGRADECIMIENTO

A Dios, por sus bendiciones y guía; a mis Padres, por su amor incondicional y constante, porque son la razón de ser quién soy; a mis hermanos, por su cariño y fuerzas para seguir adelante; a mis familiares por apoyarme en todo momento.

A los Ingenieros: Carlos Romero y Gonzalo Olmedo, por guiarme y brindarme sus conocimientos en la realización, ejecución y culminación del presente proyecto.

Gracias!!!

PRÓLOGO

Dada la necesidad de comunicarse e intercambiar información, el uso de redes a nivel mundial ha incrementado; este proyecto busca determinar los posibles ataques e intrusiones que pueden afectar a la red de manera que puedan ser detectados a nivel de capas inferiores para optimizar el trabajo de la misma antes de llegar al usuario final, enfocando el análisis en determinar cuan seguro es el tráfico de datos en la Capa de Enlace, para Redes LAN, con tecnologías Ethernet y WiFi 802.11

Las redes LAN son un medio compartido que tiene una serie de reglas que rigen el acceso a dicho medio; sin embargo la LAN más difundida, es la Ethernet así como WiFi 802.11. Ethernet es una familia de tecnologías de interconexión de redes que se define en los estándares 802.2 y 802.3, que a la vez definen los protocolos de Capa 2.

Una de las tecnologías más prometedoras y discutidas es la de poder comunicar computadores mediante tecnología inalámbrica. El estándar IEEE 802.11 se basa en el mismo marco de estándares que Ethernet, esto garantiza un nivel de interoperatividad y asegura una implantación sencilla de las funciones y dispositivos de interconexión Ethernet/WLAN. Por otra parte; la seguridad de las redes sufre constantemente amenazas las cuales de manera general pueden ser: Pasiva, Activa.

De lo anteriormente indicado, el contenido general del proyecto hace referencia a:

- Redes LAN: Ethernet, WiFi 802.11
- Capa de Enlace de Datos (Ethernet, WiFi 802.11)
- Seguridad: Protocolos de seguridad, ataques, vulnerabilidades, mecanismos de detección y recuperación.
- Análisis de Tráfico: Comportamiento General de la Red.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

ARP _ Address resolution protocol: Protocolo de red que permite a un host descubrir la dirección en hardware de un nodo con su dirección IP.

Autenticación: Proceso de identificación de un equipo o usuario. El estándar 802.11 define dos métodos de autenticación: Abierto y Cerrado (llave).

Backend: Sistemas de servidores también denominados “posteriores” que proporcionan servicios tales como: acceso a una base de datos, la gestión de red y el almacenamiento centralizado de archivos.

Beacon: Paquete (trama) que transmite un AP (punto de acceso) para anunciar su disponibilidad y características.

BSS: Topología básica de una LAN 802.11., en el caso de conexión de únicamente 2 estaciones se denomina **IBSS** (BSS independiente), que a menudo se denomina: Ad Hoc.

Cabecera: información que identifica a otra que le sigue y que define una serie de características y/o propiedades comunes a toda la información hasta el final, o bien hasta que encuentre otra cabecera que informe de nuevas características.

Colisión: Ocurre cuando dos dispositivos intentan transmitir simultáneamente, teniendo que proceder a una retransmisión posterior en diferentes instantes de tiempo.

Cracker: Persona que accede a sistemas informáticos para sabotearlos.

DHCP _ Dynamic Host Configuration Protocol: Protocolo para la configuración automática de los parámetros de red. La información se almacena en un servidor DHCP al que los equipos, al encenderse solicitan dichos parámetros de configuración.

ESSID: Uno de los dos tipos de SSID, el mismo que se emplea en Redes Wireless en modo Infraestructura.

Ethernet: Stándar de redes de computadoras de área local con acceso al medio muy utilizado por su aceptable velocidad y coste de implementación.

FCC _ Federal Communications Commission: Agencia que regula las telecomunicaciones y el espectro radioeléctrico en USA, incluye entre sus funciones la de certificar los dispositivos cumplan sus normas de interferencia electro-magnéticas.

Feedback: Introducción de una parte de la señal de salida de un dispositivo de vuelta a su entrada.

Gateway: Dispositivo de comunicación entre dos o más redes LAN y remotas, actúa como medio (camino) para permitir la comunicación. También realiza la conversión de protocolos en los niveles superiores.

Hacker: Persona que se dedica a entrar en sistemas violando la seguridad de los mismos. A diferencia de "***cracker***" su objetivo es "***entrar***" al sistema, más que causar daño al mismo.

Handoff: Sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente.

IEEE _ Instituto de Ingenieros Electrónicos y Electricistas: Asociación técnico-profesional mundial dedicada a la estandarización, que desarrolla entre otras cosas, la serie de normas 802.x para redes de área local LAN.

Infrarrojos: Señales electromagnéticas (microondas) utilizado para sistemas de red local inalámbrica.

Interfaz: Punto de frontera en el que se definen características y procedimientos físicos y lógicos para el intercambio de información.

ISM _ Industrial, Scientific and Medical: Banda de frecuencias empleada en Norteamérica para las comunicaciones inalámbricas.

Latencia: Es el tiempo o lapso necesario para que un paquete de información se transfiera de un lugar a otro. La latencia, junto con el ancho de banda, son determinantes para la velocidad de una red.

MAC _ Media Access Control: Protocolo de radiofrecuencia (en redes wireless), corresponden al nivel de Enlace en el modelo OSI.

MAU: Unidad de acceso a múltiples estaciones. Núcleo central en una red de área local de tipo anillo de señales.

Modulación: Proceso de variar características (amplitud, frecuencia y fase) de la onda portadora de acuerdo con valores instantáneos de la información a transmitir

Monomodo: Se denomina así a la fibra óptica cuyo núcleo es muy fino, lo que hace que se transmita solamente un portador o “modo” de la señal luminosa, permitiendo transmitir gran ancho de banda a grandes distancias.

Multimodo: Se denomina así a la fibra óptica cuyo núcleo es grande (50 micras), permitiendo múltiples caminos a la señal luminosa. Su alto valor de dispersión hace que este tipo de fibras ópticas tengan un valor reducido para el ancho de banda y la distancia de transmisión.

ODFM: Técnica de modulación FDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio.

PDU: Unidad de datos de protocolo.

Polling: Elección de uno entre varios terminales, por un controlador para permitir la transmisión de tráfico hacia/desde todos los terminales de una línea multipunto de manera ordenada.

Puerto: Lugar donde la información entra o sale de un ordenador, o ambas cosas. En Internet, es el número que se muestra en una URL, después de una coma justo después del Nombre de Dominio. Cada servicio en un servidor de Internet *escucha* en un número de puerto particular

Redundancia: Parte del total de información en un mensaje, que puede eliminarse sin pérdida de información esencial.

Repetidores: Componente de un sistema de comunicaciones que amplifica o regenera señales para compensar las pérdidas.

Roaming: Capacidad de cambiar de un área de cobertura a otra sin interrupción en el servicio o pérdida en conectividad. Permite a los usuarios seguir utilizando sus servicios de red inalámbrica cuando viajan fuera de la zona geográfica en la que contrataron el servicio.

SSID: Código (código de máximo 32 caracteres alfanuméricos) incluido en los paquetes de una red WiFi para identificarlos como parte de esa red.

TKIP: Algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes wireless.

Tramas: unidad de envío de datos. La trama cuenta con una cabecera (control de protocolos), datos (información a transmitir) y una cola (chequeo de errores).

Velocidad de transmisión: Capacidad de transmisión de un medio de comunicación en cualquier momento. Mide la cantidad de información por unidad de tiempo.

CAPÍTULO 1

REDES DE ÁREA LOCAL

1.1 VISIÓN GENERAL

La tendencia de las *redes de área local LAN* implica el uso de medios de transmisión o conmutación compartidos para lograr altas velocidades de transmisión de datos en distancias relativamente cortas. Conceptos como medios de transmisión, topologías y técnicas de control de acceso al medio surgen por sí mismos. El cable coaxial (en banda base y banda ancha) ha sido uno de los medios de transmisión usados con más frecuencia; sin embargo las actuales redes LAN hacen uso de par trenzado (apantallado o no) o fibra óptica así como también del medio inalámbrico (microondas o infrarrojo), para el par trenzado se hace uso de esquemas de codificación eficientes para lograr velocidades de transmisión altas a través del medio. Normalmente se usa cuatro topologías: bus, anillo, árbol o estrella.

La industria de las redes LAN en cuanto a comunicación de datos se refiere, ha sido la que mayor crecimiento ha tenido; esto se debe a que las empresas en su afán de automatizarse han escogido esta tecnología que les brinda facilidad de compartir recursos tanto de hardware como de software, sus altas velocidades aseguran a las empresas un incremento en su eficiencia y productividad.

Por otra parte, mientras que las redes MAN pueden ser tanto públicas como privadas, las redes LAN por lo general son propiedad de una organización que utiliza la red para interconectar equipos como PC’s personales, impresoras y otros dispositivos; además tienen muchas ventajas para los usuarios de computadoras como son: acceso compartido a dispositivos, aplicaciones, intercambio de

archivos entre usuarios conectados y la comunicación entre usuarios vía correo electrónico y demás aplicaciones.

1.1.1 Aplicaciones de las redes LAN

Las redes LAN constituyen la base de casi todas las redes de comunicación de datos comerciales, por tanto, a medida que se ha ampliado el campo de aplicaciones de las LAN también ha crecido lo que se exige de ellas en términos de volumen de transmisión de datos y confiabilidad.

La aplicación más extendida de las redes LAN es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. Por otra parte, algunas de las áreas de aplicación generales más importantes de este tipo de redes son [1]:

- **Redes LAN de computadores personales**

Una configuración de red LAN común es aquella que consta de computadores personales. Con frecuencia, algunos gerentes administradores adquieren PC’s personales para aplicaciones departamentales como hojas de cálculo, herramientas de gestión de proyectos y acceso a Internet; esto debido al bajo costo del sistema.

Este conjunto de procesadores departamentales no cubren todas las necesidades de un organismo ya que muchos de los programas usados para sus actividades diarias son demasiado grandes para una PC, requiriendo por tanto, de un proceso centralizado y al mismo tiempo que sea accesible para distintos usuarios. Los miembros del equipo de un proyecto u organismo necesitan compartir trabajo e información, resultando eficiente el uso de la tecnología digital para hacerlo.

Recursos caros como una impresora láser puede ser compartida por todos los usuarios de la red LAN, esta puede ser a nivel de edificio; además la red puede servir de nexo entre servicios de red corporativos mayores. Un servidor de comunicaciones puede dar acceso controlado a estos recursos. Por otra parte, el coste de conexión a la red será menor que el del dispositivo conectado, esto

sugiere que la velocidad de la red puede estar limitada ya que el coste es superior cuanto mayor sea la velocidad.

♦ **Redes de respaldo y almacenamiento**

Las redes de respaldo (<< backend >>) conectan grandes sistemas como computadoras centrales, supercomputadores y dispositivos de almacenamiento masivo en un espacio reducido con una transferencia elevada de datos en un número limitado de dispositivos.

Características:

- *Alta velocidad*: para satisfacer la de demanda de volumen de tráfico, precisan velocidades de 100 Mbps o más.
- *Interfaz de alta velocidad*: se usa interfaces de entrada/salida en paralelo de alta velocidad debido a las operaciones de transferencia de datos. El enlace físico entre la estación y la red debe ser de alta velocidad.
- *Acceso distribuido*: permite que varios dispositivos compartan el medio mediante un acceso eficiente y fiable.
- *Distancia limitada*: las redes de respaldo se emplean en salas de computadoras.
- *Número limitado de dispositivos*: es el número de computadoras principales o dispositivos de almacenamiento. Están en el orden de las decenas.

Se puede observar que algunos de los requisitos para redes de salas de computadores son contrarios a los de las LAN de PC's; además se requieren altas velocidades para poder trabajar adecuadamente lo que implica generalmente la transferencia de bloques de datos de gran tamaño.

♦ **Redes LAN troncales**

El uso de aplicaciones y computadores personales provoca la necesidad de una estrategia flexible para el uso de redes LAN. El soporte de comunicaciones de datos entre oficinas precisa de un servicio de red capaz de cubrir distancias e interconectar equipos situados en uno o varios edificios.

El uso de una única LAN presenta varios inconvenientes, aunque es posible desplegar una sola LAN para interconectar todos los equipos de procesamiento de datos necesarios en una oficina. Los inconvenientes de usar una única LAN pueden ser:

- *Fiabilidad:* una interrupción del servicio podría provocar un trastorno importante para los usuarios.
- *Capacidad*: la red LAN se podría saturar si el número de dispositivos de la red crece con el tiempo.
- *Coste*: una única LAN no es óptima para los numerosos requisitos de interconexión y comunicación. Las redes que admiten conexiones de muy bajo coste no son adecuadas para satisfacer los requisitos globales.

Las LAN se distinguen de otro tipo de redes por las siguientes tres características:

1. Tamaño,
2. Tecnología de transmisión, y
3. Topología.

1.1.2 Topologías y medios de transmisión

Hay varias maneras de conectar dos o más computadoras en red. La manera en que están conectadas no es arbitraria, sino que siguen estándares físicos llamados topologías; dependiendo de la topología será la distribución física de la red y dispositivos conectados a la misma, así como también las características de ciertos aspectos de la red como: velocidad de transmisión de datos y confiabilidad del conexionado.

Las topologías usuales en redes LAN son bus, árbol, anillo y estrella. La topología bus es un caso especial de la topología en árbol, con un solo tronco y sin ramas.

Topologías

- **Topología en bus**

Figura. 1.1. Topología en bus

Consiste en un solo cable al cual se le conectan todas las estaciones de trabajo. Los nodos que componen la red quedan unidos entre sí linealmente uno a continuación del otro. El cableado usado en esta topología presenta menos problemas logísticos ya que los cables no se acumulan [2].

Ventajas

- Es barata. Apta para oficinas medianas y chicas.
- El retardo en la propagación de la información es mínimo, debido a que los nodos de la red no deben amplificar la señal

Desventajas

- Si se tiene demasiadas computadoras conectadas a la vez la eficiencia baja notablemente.
- El fallo en una parte del cableado detendría el sistema total o parcialmente en función del lugar en que se produzca. Es difícil encontrar y diagnosticar las averías.

- La posibilidad de interceptar la información por usuarios no autorizados es alta; ya que la información en una topología en bus recorre de manera bidireccionalmente hasta hallar su destino.
- Es posible que dos computadoras intenten transmitir al mismo tiempo provocando una “colisión” y produciéndose un reintento de transmisión.

Es la topología tradicionalmente usada en redes Ethernet.

♦ **Topología en árbol**

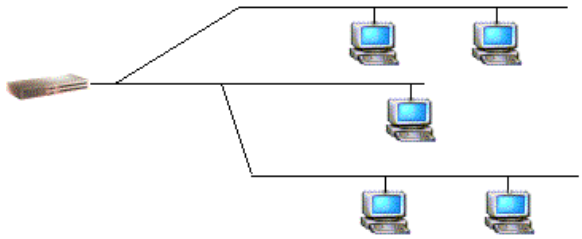


Figura. 1.2. Topología en árbol

Esta topología es una generalización del tipo bus, el árbol tiene su primer nodo en la raíz y se expande hacia fuera utilizando ramas en donde se conectan las demás terminales. Uno o más cables comienzan en el punto raíz y cada uno de ellos puede presentar ramificaciones, las mismas pueden disponer de ramas adicionales dando lugar a un esquema más complejo [2].

Ventajas

- Esta topología permite que la red se expanda y al mismo tiempo asegura que nada más exista una ruta de datos entre dos terminales cualesquiera
- A cada estación en el bus se le asigna una dirección o identificador única, incluyéndose en la cabecera la dirección destino de la trama.

Desventajas

- La transmisión desde una estación se puede recibir en las demás estaciones, siendo necesario usar un método para indicar a quién va dirigida la transmisión.

- Si dos estaciones transmiten simultáneamente sus señales se superpondrán y serán erróneas.

Para dar solución a estos inconvenientes, las estaciones transmiten datos en bloques pequeños llamados tramas; cada una de ellas consta de una porción de los datos que una estación determinada desea transmitir. Cada trama posee una cabecera que contiene información de control.

♦ **Topología en anillo**

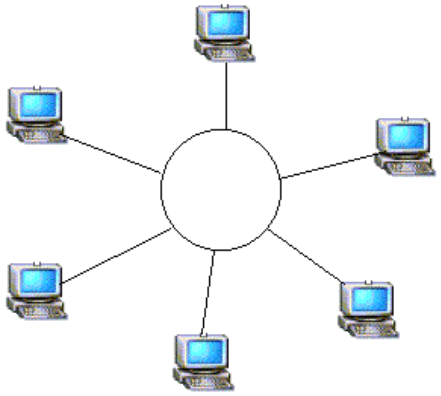


Figura. 1.3. Topología en anillo

Consiste en conectar linealmente entre sí todos los ordenadores en un bucle cerrado. La información se transfiere en un solo sentido a través del anillo mediante un paquete especial de datos llamado testigo que se transmite de un nodo a otro hasta alcanzar el nodo destino [2].

El cableado de esta topología es más complejo, no sólo por el coste, sino también por la necesidad de emplear dispositivos MAU (unidades de acceso multiestación) usados para implementar físicamente el anillo.

Ventajas

- En caso de una avería, esta topología deriva partes de la red mediante los MAU's aislando las partes defectuosas del resto de la red
- No es necesario detener toda la red para añadir nuevas estaciones ya que los MAU's aíslan las partes a añadir hasta que se hallan listas.

Desventajas

- Es cara, una placa de red llega a costar lo que una estación de trabajo.

Dos buenos ejemplos de red en anillo serían Token-Ring y FDDI (fibra óptica)

♦ **Topología en estrella**

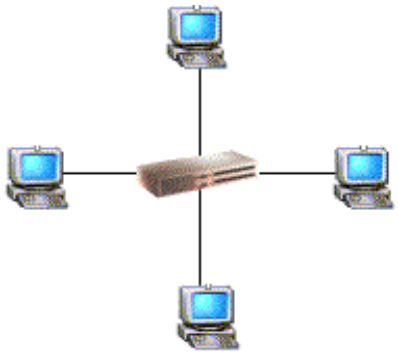


Figura. 1.4. Topología en estrella

En este esquema todas las estaciones están conectadas a un concentrador (HUB) con cable por computadora, es decir existe un punto central [2].

Ventajas

- Su gran modularidad le permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red.
- La ausencia de colisiones en la transmisión y dialogo directo de cada estación con el servidor.
- En caso de añadir otra estación, no es necesario interrumpir la actividad de la red realizándose la operación casi inmediatamente

Desventajas

- Su punto vulnerable es el nodo central, si éste falla, toda la red fallaría.
- Baja transmisión de datos.

La topología en estrella es empleada en redes Ethernet y ArcNet.

Medios de transmisión

La elección de la topología depende de varios factores como fiabilidad, capacidad de expansión, rendimiento y elección del medio de transmisión. La elección del medio de transmisión viene determinada por una serie de factores y restringida por la topología de la red LAN.

Existen otros aspectos que desempeñan un papel importante a la hora de determinar el medio de transmisión, entre los que están:

- *Capacidad:* debe soportar el tráfico de red esperado.
- *Fiabilidad:* debe satisfacer los requisitos de disponibilidad.
- *Tipos de datos soportados:* ajustados a la aplicación.
- *Alcance del entorno:* debe proporcionar servicio a la gama de entornos requeridos.

♦ **Medios magnéticos – ópticos**

Los disquetes, zips y en general los medios removibles los podemos llevar de un sitio a otro.

♦ **Par trenzado**

El ancho de banda depende del grosor y de la distancia; así el grosor del cable es de 1 mm y la velocidad está en el orden de 10 – 100 Mbps.

El cable par trenzado se divide en categorías, así tenemos:

- **STP (**apantallado**):** 2 pares de hilo recubierto por malla.
- **UTP (**no apantallado**):** 4 pares de hilos.
  Categoría 3: van de 4 en 4 (8 hilos), alcanzando 30 Mbps.
  Categoría 5: más retorcido y mejor aislante (teflón) alcanzando 100 Mbps [3].

Figura. 1.5. Par Trenzado (Cable UTP)

- **Cable coaxial**

Existen de dos impedancias:

- **75 ohmios:** banda ancha, utilizado en TV, distintos canales, 300 MHz.
- **50 ohmios:** banda base, utilizado en Ethernet, un canal
  10 BASE 5: coaxial grueso, 500 metros, 10 Mbps, conector “N”.
  10BASE 2: coaxial fino, 185 metros, 10 Mbps, conector “BNC” [3]

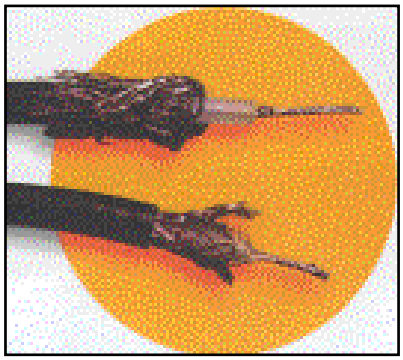


Figura. 1.6. Cable Coaxial

- **Fibra óptica**

Sus características son:

- Se necesita una fuente de luz (láser o LED).
- Se transmite por fibra y se capta por foto diodo.
- La topología típica es el anillo.
- Alcanza un ancho de banda de 30000 GHz.

- Se necesita repetidores cada 30 Km.
- No hay interferencias.
- Pesa 8 veces menos que el cable par trenzado [3]

Figura. 1.7. Fibra Óptica [2]

Así; la topología en bus ha hecho uso del cable coaxial en banda base, principalmente en el caso de los sistemas Ethernet. La topología en estrella ha trabajado sobre par trenzado o fibra óptica; aprovecha de la distribución natural del cableado de los edificios, es usada para distancias cortas y puede ofrecer velocidades elevadas a un número pequeño de dispositivos.

La topología en anillo puede ser usada para proporcionar enlaces de muy alta velocidad sobre distancias largas.

♦ **Cable usado según norma**

Tabla. 1.1. Cable según norma [3]

Categoría	Velocidad	Donde se usa
1	No entra dentro de los criterios de la norma	
2	Hasta 1 MHz	Para telefonía
3	Hasta 16 MHz	Ethernet 10Base-T
4	Hasta 20 MHz	Token-Ring, 10Base-T
5	Hasta 100 MHz	100Base-T, 10Base-T

1.1.3 Arquitecturas de protocolos de redes LAN

En el modelo OSI las diferencias entre las redes LAN, MAN y WAN se presentan en las 3 capas inferiores que son: capa física, de control de acceso al medio y de control de enlace lógico.

Para las redes LAN, las tres primeras capas que forman la arquitectura cumplen las siguientes funciones [4]:

- **Capa física**

- Codificación y decodificación de señales.
- Generación y eliminación de preámbulo.
- Transmisión y recepción de bits.

- **Control de acceso al medio (MAC)**

- Ensamblado de datos en tramas con campos de direccionamiento y detección de errores.
- Desensamblado de tramas, reconocimiento de direcciones y detección de errores.
- Control de acceso al medio de transmisión LAN

- **Control de enlace lógico (LLC)**

- Interfaz con las capas superiores y control de errores y de flujo. Cada capa toma las tramas y le añade una serie de datos de control antes de pasar a la siguiente capa.
- Control de errores (retransmisión de tramas erróneas) y de flujo.
- Especifica el tipo de servicio ofrecido a la capa superior: servicio sin conexión y sin asentimiento, servicio sin conexión y con asentimiento, servicio con conexión.

Por encima de la capa física se encuentran las funciones asociadas a los servicios ofrecidos a los usuarios LAN. Estas funciones se asocian en la capa 2 de OSI, algunas de estas funciones se agrupa en la capa LLC (control de enlace

lógico) como también en la capa MAC (control de acceso al medio). El motivo de la división se debe a:

- La gestión del acceso al medio compartido no se encuentra en la capa 2 de control de enlace de datos tradicional.
- Para un mismo LLC, están disponibles varios MAC.

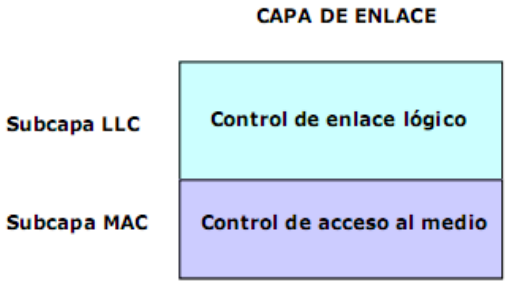


Figura. 1.8. Capa de Enlace

Además, los datos de nivel superior se pasan hacia abajo hacia el nivel LLC a la que añaden una cabecera de información de control dando lugar a la **PDU (***unidad de datos de protocolo LLC***).**

PDU es la información que se usa para el funcionamiento del protocolo LLC. La PDU LLC se pasa a la capa MAC; la misma que añade información al principio y al final de cada paquete formando una trama MAC; esta información sirve para el funcionamiento del protocolo MAC [1].

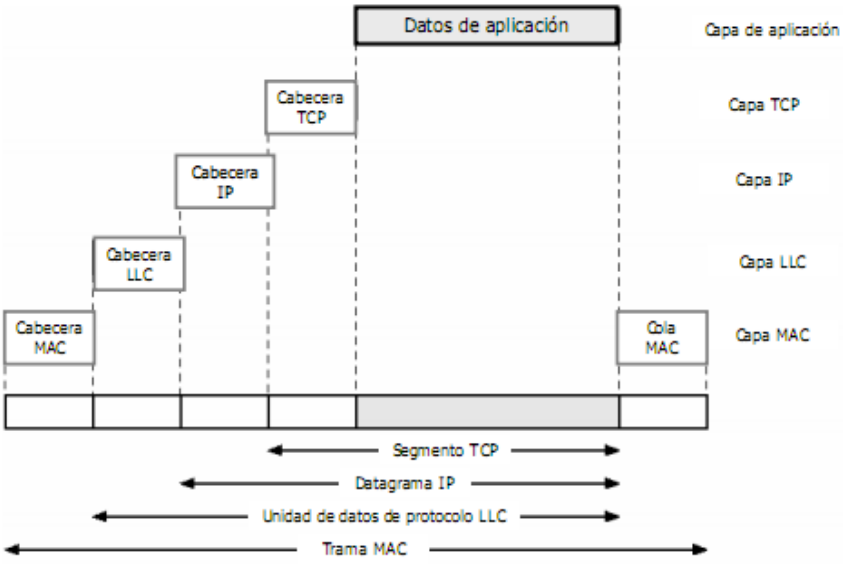


Figura. 1.9. Protocolos LAN en contexto

1.1.4 Conmutadores

Hay varias maneras de conectar dos o más computadoras en red. La manera en que están conectadas no es arbitraria, sino que siguen estándares físicos llamados topologías; dependiendo de la topología será la distribución física de la red y dispositivos conectados a la misma.

Los conmutadores se utilizan para unir los segmentos físicos de una red y permiten la circulación de datos entre estos segmentos. Trabajan en el nivel 2 del modelo OSI y dirigen el tráfico según la dirección del nivel 2 (MAC de Ethernet).

La configuración de los conmutadores es automática, sus funciones son las de escuchar el tráfico en cada puerto Ethernet y descubrir el puerto al que está conectado cada dispositivo para enviar el tráfico directamente a dicho puerto. El hecho de no necesitar una configuración predeterminada resulta ventajoso al momento de instalar una red; por otra parte el proceso de conmutación se realiza a nivel de hardware a la velocidad que permite el cable sin prácticamente periodo de latencia.

Inicialmente los conmutadores unían segmentos con varios dispositivos, actualmente se conecta un solo dispositivo a cada puerto. El tener un sólo dispositivo activo por puerto evita se produzcan colisiones mejorando el rendimiento de la red y los dispositivos pueden funcionar a dúplex completo. Además, el tráfico en la red incluye mensajes de difusión que se copian en todos los puertos lo que repercute considerablemente en las redes grandes; la forma de reducir el tráfico de difusión es proporcionando un conmutador para cada puerto para posteriormente conectarlo a un enrutador los mismos que no transmiten difusiones. Otra manera de reducir el tráfico de difusión es utilizando redes VLAN, ya que la difusión de un miembro de esta red sólo va a los otros miembros de la misma VLAN reduciendo el tráfico de difusión [5].

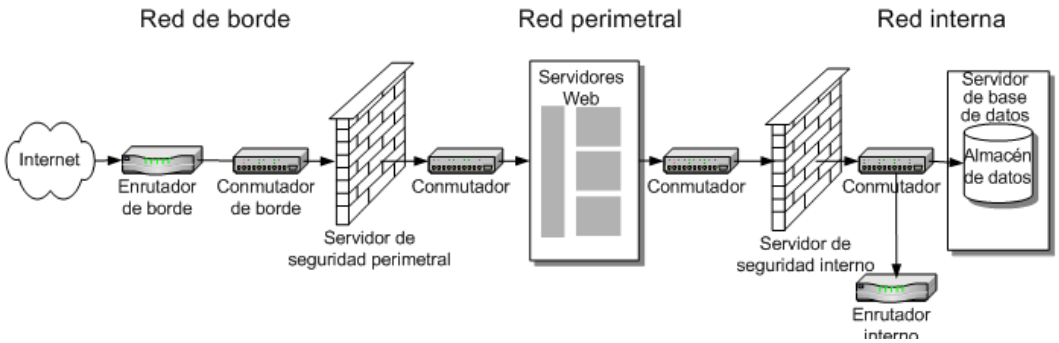


Figura. 1.10. Arquitectura de conmutación multinivel

Características

Las características fundamentales propias de los conmutadores son las siguientes:

- **STP (Spanning Tree Protocol, protocolo del árbol de expansión)**

El protocolo STP se utiliza para calcular la mejor ruta entre conmutadores cuando existen varios conmutadores y varias rutas en la red. Esto es necesario para evitar el envío de datos por varias rutas a la vez lo que redunda en duplicación de los datos. En conmutadores pequeños este protocolo no suele estar disponible, pero para redes grandes es importante que los conmutadores admitan este protocolo.

- **Compatibilidad con VLAN**

Las redes VLAN sirven para segmentar la red en grupos de equipos con necesidades de comunicación similares, de manera que se reduce el tráfico en la red. Los conmutadores pequeños no son compatibles con las redes VLAN; si las redes son pequeñas esto no es importante, pero si las redes son de gran tamaño es importante la compatibilidad entre conmutadores y redes VLAN.

- **Conectividad de vínculo ascendente**

Los vínculos ascendentes se usan para conectar conmutadores en una red. Mientras que todos los conmutadores pueden conectarse mediante vínculos

Ethernet ordinarios, los conmutadores de gama alta admiten vínculos de mayor velocidad que utilizan protocolos troncales diseñados para conexión entre conmutadores.

- **Consolidación**

La incorporación de otras funciones en el conmutador puede reducir los costos y mejorar la administración; es decir los conmutadores (pequeños) pueden incluir un enrutador y un servidor de seguridad e incluso un modem de banda ancha. Los conmutadores superiores también pueden incorporar un módulo enrutador denominado conmutador de nivel 3, así como otras funciones de equilibrio de carga y servidor de seguridad.

Clases de centros conmutados

- **Conmutador de almacenamiento y envío (store and forward switch)**

El conmutador acepta una trama sobre una línea de entrada, la almacena temporalmente y después los encamina hacia la línea de salida correspondiente. Este tipo de conmutador implica un retardo entre la emisión y recepción, pero mantiene la integridad completa de la red

- **Conmutador rápido (cut through switch)**

El conmutador aprovecha que la dirección de destino se encuentra al comienzo de la trama MAC para retransmitir la trama entrante sobre la línea de salida tan pronto como sabe la dirección de destino. El conmutador de tipo rápido permite el mayor rendimiento posible, aunque a riesgo de propagar tramas erróneas dado que no es capaz de comprobar el campo CRC antes de efectuar la retransmisión [1].

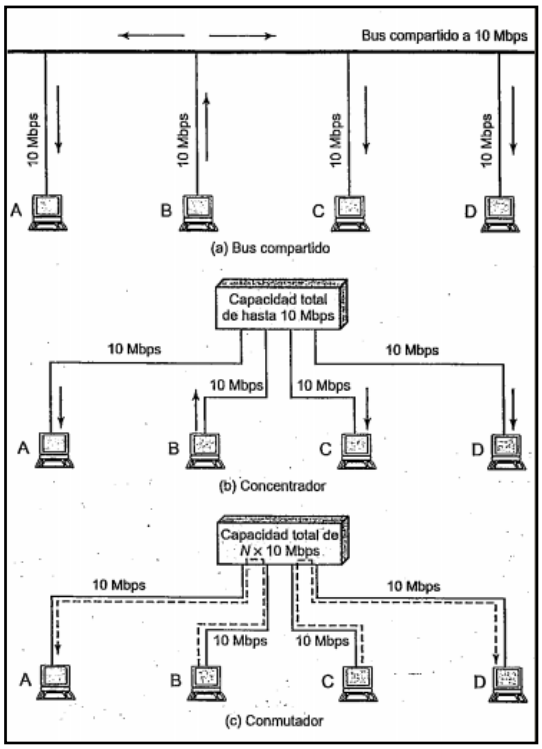


Figura. 1.11. Conmutadores y concentradores en una LAN

1.2 REDES LAN: ETHERNET

Las redes LAN de alta velocidad más ampliamente utilizadas en la actualidad son las basadas en Ethernet y fueron desarrolladas por el comité de estándares IEEE 802.3.

Tabla. 1.2. Características de algunas redes LAN de alta velocidad [1]

	Fast Ethernet	***Gigabit Ethernet***	***Canal de Fibra***	***LAN Inalámbrica***
Velocidad de Datos	100 Mbps	1 Gbps, 10 Gbps	100 Mbps, 3.2 Gbps	1 Mbps, 54 Mbps
Medio de Transmisión	UTP, STP, fibra óptica	UTP, cable apantallado, fibra óptica	Fibra óptica, cable coaxial, STP	Microondas: 2.4 GHz 5 GHz

Método de Acceso	CSMA/CD	Conmutado	Conmutado	CSMA/Sondeo
Estándar	IEEE 802.3	IEEE 802.3	Asociación del canal de fibra	IEEE 802.11

1.2.1 Especificaciones IEEE 802.3 10 Mbps (Ethernet)

El comité IEEE 802.3 ha definido varias configuraciones físicas las mismas que tienen limitantes y ventajas; por tanto; la normalización responde a la evolución de la tecnología, mientras que su limitante se encuentra en la variedad de opciones que el proveedor dispone y que a la vez debe satisfacer la mayoría de necesidades. Así; las alternativas definidas son [1]:

- **10BASE5:** especifica el uso de cable coaxial de 50 ohmios, señalización digital Manchester y la longitud máxima del segmento de cable se fija en 500 metros la misma que se puede extender por medio de repetidores. La normalización permite un máximo de cuatro repetidores en el camino entre dos estaciones cualesquiera ampliándose así la longitud efectiva del medio hasta 2.5 Km.

- **10BASE2:** similar a 10BASE5, excepto que utiliza un cable más fino que admite tomas de conexión para distancias más cortas que el cable 10BASE5.

- **10BASE-T:** hace uso del par trenzado no apantallado en una topología en estrella. Dada la alta velocidad y baja calidad de transmisiones, características propias de este tipo de cable; la longitud de cada enlace se restringe a 100 metros. Como alternativa se puede hacer uso de un enlace de fibra óptica para alcanzar una longitud máxima de 500 metros.

- **10BASE-F:** se basa en tres especificaciones: una topología en estrella pasiva para la interconexión de estaciones y repetidores con segmentos de hasta 1 Km de longitud, un enlace punto a punto que puede ser usado para conectar estaciones o repetidores separados hasta 2 Km.

Tabla. 1.3. Alternativas para el medio de transmisión en la capa física IEEE 802.3 a 10 Mbps [1]

	10 BASE5	***10 BASE2***	***10 BASE-T***	***10 BASE-FP***
Medio de Transmisión	Cable coaxial (50 Ohm)	Cable coaxial (50 Ohm)	Par trenzado no apantallado	Par de fibra óptica a 850 nm
Técnica de Señalización	Banda base (Manchester)	Banda base (Manchester)	Banda base (Manchester)	Manchester On / Off
Topología	Bus	Bus	Estrella	Estrella
Long. Máx. Seg.	500	185	100	500
Nodos por segmento	100	30	-----	33
Diámetro del cable (mm)	10	5	0.4 a 0.6	62.5 / 125 um

1.2.2 Especificaciones IEEE 802.3 100 Mbps (Fast Ethernet)

Fast Ethernet es un conjunto de especificaciones desarrolladas por el Comité IEEE 802.3 con el propósito de proporcionar una red LAN de bajo costo compatible con Ethernet que funcione a 100 Mbps, de esta manera, la designación genérica para estos estándares es 100BASE-T.

La siguiente figura (Figura 1.12) muestra la terminología utilizada en las distintas especificaciones así como el medio usado. Todas las opciones 100BASE-T usan el protocolo MAC y el formato de la trama IEEE 802.3. [1]

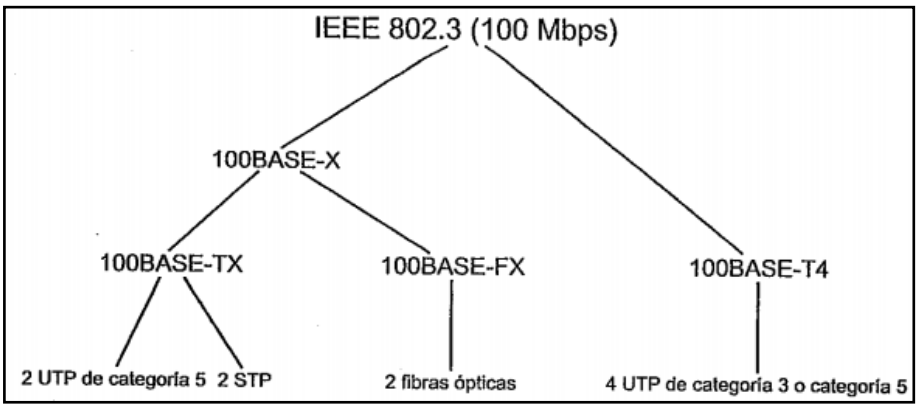


Figura. 1.12. Opciones 100 BASE-T en IEEE 802.3

- **100BASE-X:** los 100 Mbps se consiguen en un solo sentido utilizando un único enlace (par trenzado ó fibra óptica individual). Para que esto suceda, en todos los medios se necesita un esquema de codificación de señal efectivo y eficiente; inicialmente se definió para FDDI denominado 4B/5B-NRZI [1].

  El esquema 100BASE-X incluye dos especificaciones para el medio físico:

  - ***100BASE-TX:*** utiliza dos pares de cable de par trenzado, uno para transmisión y otro para recepción; se permiten tanto STO como UTP de categoría 5. Usa el esquema de señalización MLT-3.

  - ***100BASE-FX:*** utiliza dos fibras ópticas, una para transmitir y otra para recibir. Para este tipo de especificación es necesario el uso de un método para convertir la secuencia de grupos de código 4B/5B-NRZI en señales ópticas, a este proceso se le denomina *modulación en intensidad*. Así; un 1 binario se representa por un haz de luz, y, un 0 binario se representa por la ausencia de pulso de luz o, en su defecto uno de muy baja intensidad.

- **100BASE-T4:** ofrece una velocidad de transmisión de datos de 100 Mbps a través de cable de tipo 3 de baja calidad con la posibilidad de reutilizar las instalaciones existentes de este tipo de cable en edificios de oficina. Esta especificación puede usar también el cable tipo 5. 100BASE-T4 no transmite

una señal continua entre paquetes lo que le hace útil para sistemas alimentados por baterías.

La secuencia de datos a transmitir en 100BASE-T4 se debe dividir en tres secuencias distintas, así cada una tendrá una velocidad de transmisión efectiva de 33.3 Mbps. Esta especificación usa 4 pares trenzados, 3 pares para transmitir datos, 3 pares para recibir datos y 2 pares son configurados para una transmisión bidireccional. 100BASE-T4 no usa el esquema de codificación NRZ, en su lugar hace uso del esquema de señalización ternario 8B6T.

- **Funcionamiento Full-Duplex:** una red tradicional Ethernet es *semi-duplex* en donde una estación puede transmitir una trama o recibirla, pero no las dos simultáneamente. Por su parte, en el modo de funcionamiento *Full-Duplex* la estación puede transmitir y recibir al mismo tiempo de manera que una Ethernet a 100 Mbps en *full-duplex* alcanzaría, teóricamente, una velocidad de 200 Mbps.

  Las estaciones conectadas para funcionar en modo *full-duplex* deben tener tarjetas adaptadoras *full-duplex* en lugar de las semi-duplex tradicionales; además el punto central en la topología en estrella no puede ser solo un repetidor multipuesto sino un concentrador conmutado. En este caso, cada estación constituye un dominio de colisión separado, por lo cual las colisiones no se producen y el algoritmo CSMA/CD no es necesario.

1.2.3 GIGABIT Ethernet

Para finales de 1995, el comité IEEE 802.3 empezó a investigar estrategias para transmitir paquetes con formato Ethernet a velocidades del orden de Gigabits por segundo; en este caso Gigabit Ethernet adopta la estrategia seguida por Fast Ethernet [1].

En Gigabit Ethernet se define un nuevo medio y una especificación para la transmisión, se ha adoptado el protocolo CSMA/CD así como el formato de

tramas usado por Ethernet a 10 Mbps y 100 Mbps. Es compatible con 10 BASE-T y 100 BASE-T lo que facilita la migración.

La Figura 1.13 muestra una aplicación típica de Gigabit Ethernet, en la cual el conmutador a 1 Gbps proporcionará la conectividad entre los servidores centrales y concentradores de alta velocidad. Cada concentrador se conecta a la línea troncal mediante un enlace a 1 Gbps y conecta a los servidores de cada concentrador ofreciendo enlaces a 100 Mbps para a estaciones de trabajo, servidores y otros concentradores a 100 Mbps.

Por otra parte, el crecimiento de la demanda de tecnología Gigabit Ethernet se debe a que las organizaciones adoptan cada vez más 100 BASE-T lo que implica enormes cantidades de tráfico en las líneas troncales.

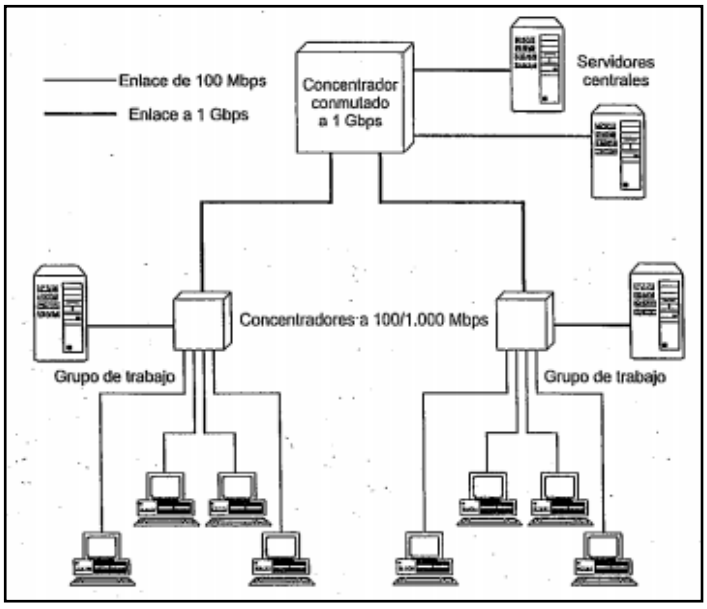


Figura. 1.13. Configuración para GIGABIT Ethernet (ejemplo)

La especificación actual IEEE 802.3 a 1 Gbps define las siguientes alternativas en la capa física:

- **1000BASE-SX:** usa longitudes de onda pequeñas proporcionando enlaces dúplex de 275 m usando fibras multimodo de 62.5 μm, ó hasta 550 m con fibras multimodo de 50 μm. Las longitudes de onda se encuentran en el intervalo comprendido entre 770 y 860 nm.

- **1000BASE-LX:** usa longitudes de onda mayores proporcionando enlaces dúplex de 550 m usando fibras multimodo de 62.5 μm o 50 μm, ó de 5 Km con fibras monomodo de 10 μm. Las longitudes de onda se encuentran en el intervalo comprendido entre 1.270 y 1.355 nm.

- **1000BASE-CX:** proporciona enlaces de 1 Gbps entre dispositivos localizados dentro de una habitación (armario de conexiones) utilizando latiguillos de cobre (cables de par trenzado de menos de 25 m con un apantallamiento especial). Cada enlace consiste en dos pares trenzados apantallados, cada uno en un sentido.

- **1000BASE-T:** utiliza 4 pares no apantallados tipo 5 para conectar dispositivos separados hasta 1.000 m

1.2.4 Ethernet de 10 Gbps

El incremento en el tráfico de Internet e Intranets ha sido motivo de estudio de Ethernet con capacidad de 10 Gpbs, algunos de los factores que ha promovido este nuevo estudio son [1]:

- Incremento en el número de conexiones de red.
- Incremento en la velocidad de conexión de cada estación final; por ejemplo; usuarios de líneas analógicas de 56 kbps migrando hacia soluciones DSL y modem de cable, o usuarios de 10 Mbps migrando hacia 100 Mbps.
- Incremento en el despliegue de aplicaciones demandantes de ancho de banda, como el video de alta calidad.
- Incremento en el hospedaje de web y el tráfico de las aplicaciones de hospedaje

A medida que la demanda de ancho de banda crezca, Ethernet de 10 Gbps podrá ser desplegada a lo largo de toda la red interconectando agrupaciones centralizadas de servidores, redes troncales y proporcionando cobertura para toda un área. Además, esta tecnología permite que tanto los proveedores de servicio de internet (ISP) como los de servicios de red (NSP) puedan ofrecer enlaces a un costo reducido entre encaminadores y conmutadores adyacentes.

Por otra parte, esta tecnología permite la construcción de redes MAN y WAN que conecten redes LAN geográficamente dispersas. Es así que Ethernet empieza a competir con ATM y otras tecnologías de transmisión de área amplia en los cuales los requisitos del cliente es el transporte de datos y de TCP/IP., Ethernet a 10 Gbps proporciona un valor agregado sobre el transporte ofrecido por ATM tanto para usuarios finales como para proveedores del servicio; como:

- No se requiere una conversión costosa y demandante de ancho de banda entre paquetes Ethernet y celdas ATM. La red es Ethernet extremo a extremo.
- La combinación de IP y Ethernet ofrece calidad de servicio y capacidades para establecer políticas de tráfico que se aproximan a las que brinda ATM de manera que tanto usuarios como proveedores tienen a su disposición una tecnología de ingeniería de tráfico avanzada.
- Ethernet de 10 Gbps abarca un amplio campo de interfaces ópticas estándares (longitud de onda y distancias) optimizando su funcionamiento y coste para aplicaciones LAN, MAN o WAN.

Las distancias máximas de los enlaces cubren un intervalo de aplicaciones desde 300 m hasta 40 Km, los enlaces funcionan exclusivamente en modo full-duplex usando diversos medios físicos de fibra óptica.

La especificación en Ethernet a 10 Gbps define las siguientes alternativas en la capa física:

- **10GBASE-S (corta):** diseñada para transmisiones de 850 nm sobre fibras multimodo, puede alcanzar distancias de hasta 300m.

- **10GBASE-L (larga):** diseñada para transmisiones de 1.310 nm sobre fibras monomodo, puede alcanzar distancias de hasta 10 Km.

- **10FGBASE-E (extendida):** diseñada para transmisiones de 1.550 nm sobre fibras monomodo, puede alcanzar distancias de hasta 40 Km.

- **10GBASE-LX4:** diseñada para transmisiones de 1.310 nm sobre fibras monomodo o multimodo que puede alcanzar distancias de hasta 10 Km. Este

medio utiliza multiplexación por división de longitud de onda (WDM) para multiplexar el flujo de bits sobre cuatro ondas de luz.

1.3 REDES LAN: INALÁMBRICA

Una LAN inalámbrica es una red en donde un usuario móvil puede conectarse a una LAN a través de enlaces de radiofrecuencia sin cables. La norma IEEE 802.11 especifica las tecnologías WLAN.

Una *red de área local inalámbrica* (**WLAN**) cubre un área equivalente a la red local de una empresa con un alcance aproximado de cien metros, permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí [6].

Figura. 1.14. Red Inalámbrica sencilla

Quiénes necesitan WLAN

Todas aquellas aplicaciones en donde haya limitaciones para la instalación de infraestructura de cableado ya sea de cobre o de fibra son usuarios naturales de esta tecnología inalámbrica. Estas limitaciones se pueden deber a:

- Necesidad de un rápido despliegue en edificios sin cableado; por ejemplo una compañía se muda a un nuevo edificio.
- Dificultades para instalar cableado por razones de acceso, estética, o asepsia (Ejm: un quirófano)

- Movilidad de los usuarios finales, por ejemplo operarios controladores de stock de un depósito con sus laptops o handhelds conectadas la red.
- Dispersión de usuarios con distancias mayores a 100m (máxima normalizada por IEEE 802.3 para Ethernet), ejemplo, un campus universitario o un country.

En el caso proveedores de servicio de internet; se evaluará económicamente la posibilidad de WLAN frente a otras opciones de llegada a los clientes como par de cobre para acceso dial-up o ADSL por coaxial usando Cable Modem. En estos casos, aparte del costo de los elementos de cada red en sí misma, hay otros factores importantes como el mejor retorno de inversión de WLAN debido a la facilidad de despliegue y su menor costo de mantenimiento e instalación.

1.3.1 Especificaciones

La familia de especificaciones ***802.11*** para una WLAN fue desarrollada por un grupo de trabajo internacional del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Actualmente hay cuatro especificaciones en la familia: ***802.11, 802.11a, 802.11b*** y ***802.11g***. Todas ellas usan el protocolo Ethernet y CSMA/CA para compartir el acceso, la norma aprobada más reciente es la ***802.11g*** que ofrece transmisión inalámbrica sobre cortas distancias hasta 54 Mbps comparada con los 11 Mbps de la 802.11b. Estas dos normas operan en la banda no licenciada de 2.4 GHz y son compatibles entre sí. La norma ***802.11b*** (a menudo llamada Wi-Fi) es retrocompatible con la 802.11 que es la primera de toda esta familia de normas.

La norma ***802.11a*** aplica a sistemas ATM y se usa en puntos de acceso de concentración, opera en frecuencias entre 5 GHz - 6 GHz y mediante su multiplezado OFDM se alcanzan velocidades de hasta 54 Mbps, pero se usa comúnmente velocidades de 6 Mbps, 12 Mbps y 24 Mbps. Por trabajar en otra frecuencia no es compatible con las otras normas pero es útil para el caso de que la interferencia en 2,4 GHz sea elevada.

1.3.2 Tecnologías

- **WiFi (*IEEE 802.11*)**

Con el respaldo de WECA (Wireless Ethernet Compatibility Alliance) ofrece una velocidad máxima de 54 Mbps en una distancia de varios cientos de metros.

- **HiperLAN2 (*High Performance Radio LAN 2.0*)**

Estándar europeo desarrollado por ETSI (*European Telecommunications Standards Institute*). HiperLAN2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros y transmite dentro del rango de frecuencias de 5150 y 5300 MHz [7].

Las LAN inalámbricas se clasifican generalmente de acuerdo con la técnica de transmisión usada. Las actuales se encuentran en las siguientes categorías:

- **Redes LAN de infrarrojos**

Una celda individual en un LAN IR está limitada a una sola habitación dado que la luz infrarrojo no es capaz de atravesar muros opacos, por lo cual las comunicaciones ópticas inalámbricas en la banda infrarroja del espectro son de uso común en hogares, como en el control remoto de numerosos dispositivos

Ventajas

- Puede alcanzar velocidades de datos extremadamente altas. El espectro de los infrarrojos no está regulado internacionalmente.
- La luz infrarroja se refleja difusamente por los objetos de color, se usa esta reflexión para proporcionar cobertura a toda una habitación.
- Las comunicaciones infrarrojas pueden ser aseguradas contra escuchas de forma más sencilla que las de microondas.

- En cada habitación de un edificio puede funcionar una instalación de infrarrojos aislada sin interferencias permitiendo la construcción de grandes redes LAN infrarrojas.
- Utiliza equipos relativamente baratos y simples, usa modulación en intensidad.

Desventajas

Varios entornos de interior sufren una radiación infrarroja de fondo debido a la luz solar como a la artificial, esta radiación se manifiesta en forma de ruido en el receptor obligando el uso de transmisores de alta potencia que limitan el alcance de la señal.

Técnicas de transmisión

Un ***haz dirigido*** puede utilizarse para crear enlaces punto a punto, donde el alcance depende de la potencia de emisión y el grado de enfoque. Un enlace de datos IR dirigido puede alcanzar distancias de hasta kilómetros utilizando este tipo de enlace en la interconexión de edificios a través de puentes o dispositivos encaminadores entre los que haya línea de visión.

En una ***configuración omnidireccional*** existe una estación base aislada que se encuentra en la línea de visión del resto de estaciones que conforman la LAN; por lo general esta estación se ubica en el techo y actúa como un repetidor multipunto. El transmisor del techo difunde una señal omnidireccional que es recibida por el resto de transceptores IR en la zona

En una configuración de ***difusión*** todos los transmisores IR están enfocados hacia un punto en un techo reflectante. La radiación IR que alcanza el techo es reflejada omnidireccionalmente y recogida por todos los receptores en la zona [1].

♦ **Redes LAN de espectro expandido**

En la mayoría de los casos estas LAN operan en las bandas ISM que no necesitan licencia FCC para su uso en los E.E.U.U. Estas LAN hacen uso de la tecnología de transmisión de espectro expandido

Configuración

Este tipo de redes LAN hacen uso de una disposición de celdas múltiples en donde las celdas adyacentes utilizan diferentes frecuencias dentro de la misma banda para evitar interferencias. Si se usa una topología basada en un concentrador, éste puede controlar el acceso actuando como un repetidor multipunto. Por otra parte cada estación puede difundir usando una antena omnidireccional de tal forma que el resto de estaciones en la celda pueda recibir.

Otra función importante de un concentrador es el traspaso automático de las estaciones móviles

Cuestiones de transmisión

Una red LAN inalámbrica puede ser utilizada sin requerir una licencia para la transmisión. Por ejemplo, en los Estados Unidos, la FCC ha autorizado dos aplicaciones dentro de la banda ISM que pueden operar sin licencia, como son:

- Sistemas basados en espectro expandido que pueden funcionar hasta a 1 vatio, y;
- Sistemas de potencia reducida que pueden funcionar hasta a 0.5 vatios.

Dada que esta banda fue incorporada por la FCC, su uso para las redes LAN inalámbrica de espectro expandido se ha vuelto popular

♦ Redes LAN de microondas de banda estrecha

Esta tecnología hace referencia al uso de una banda de frecuencias de microondas de radio para la transmisión de la señal, siendo esta banda relativamente estrecha. Algunos de estos productos funcionan a frecuencias en donde es necesaria la licencia FCC, y otras en algunas bandas ISM.

Tabla. 1.4. Comparación de las tecnologías de redes LAN Inalámbricas [1]

	Infrarrojos		Espectro expandido		Radio
	Infrarrojos difusos	Infrarrojos de haz directo	Salto de frecuencia	Secuencia directa	Microondas de banda estrecha
Velocidad (Mbps)	1-4	1-10	1-3	2-50	10-20
Movilidad	Estacionario/móvil	Estacionario con LOS	Móvil	Estacionario/móvil	
Alcance (m)	15-60	25	30-100	30-250	10-40
Detectabilidad	Despreciable		Pequeña		Alguna
Longitud de onda/frecuencia	λ: 800-900 nm		902-928 MHz 2,4-2,4835 GHz 5,725-5,85 GHz		902-928 MHz 5,2-5,775 GHz 18,825-19,205 GHz
Técnica de modulación	ASK		FSK	QPSK	FS/QPSK
Potencia radiada	—		<1 W		25 mW
Método de acceso	CSMA	Anillo con paso de testigo, CSMA	CSMA		Reserva, ALOHA, CSMA
Necesidad de licencia	No		No		Sí a menos que sea ISM

1.3.3 Topologías

- ***Red Malla***

Conceptualmente una LAN es una topología de todos contra todos. En el caso de una Ethernet sobre cable, esta interconexión libre se dibuja como un BUS troncal de transmisión sobre la cual todos los usuarios “cuelguan” sus dispositivos y, debido al protocolo CSMA/CA todos pueden comunicarse entre sí con la única limitación de las colisiones producidas cuando dos o más estaciones envían datos simultáneamente.

- ***Red Punto-Multipunto o de Concentración***

En caso que la cantidad de colisiones sean las suficientes para afectar el normal desempeño de la red, se debe pasar a una topología de concentración de las comunicaciones ubicando en el centro un dispositivo con la inteligencia y capacidad de administrar estas comunicaciones adecuadamente y restringiendo las colisiones a un conjunto de dispositivos determinado (llamado dominio de colisión). Estos dispositivos deben entonces conmutar las comunicaciones y/o encaminarlas convenientemente entre un punto central y varios (Multipuntos), estas operaciones son realizadas por Switches (para la conmutación) si es una

sola red LAN o se utilizan Routers (para el encaminamiento) si hay que conectar varias redes LAN entre sí.

- ***Comunicaciones Punto a Punto***

Para el caso de interconexiones entre redes LAN, es posible que las mismas se encuentren alejadas lo suficiente para considerarlas "***puntos diferentes***" en este caso es necesario realizar enlaces punto a punto, en el caso de que estos enlaces punto a punto sean dentro de una misma red no es necesario encaminar con Routers sino que se utilizan "puentes" entre estos dos puntos denominados "Bridges".

1.3.4 Requisitos para las redes LAN Inalámbricas

Algunas de los requisitos son:

- Alta capacidad
- Cobertura de pequeñas distancias
- Conectividad total de las estaciones conectadas
- Capacidad de difusión

Otras necesidades específicas para redes LAN Inalámbricas; son [8]:

- **Rendimiento:** El uso del protocolo MAC debe ser eficiente para maximizar la capacidad.
- **Número de Nodos:** pueden dar soporte a muchos nodos mediante el uso de varias celdas.
- **Conexión a la LAN Troncal:** se da la interconexión con estaciones situadas en una LAN troncal cableada. Se da soporte a las LAN Inalámbricas con infraestructura por medio de Módulos de control que conectan ambos tipos de LAN, a los usuarios nómadas y a las LAN Inalámbricas ad hoc.
- **Área de Servicio:** La superficie de cobertura tiene un diámetro típico entre 100 y 300 metros.
- **Consumo de Batería:** Cuando los usuarios móviles usan adaptadores sin cable necesitan una batería de larga vida.

- **Robustez en la transmisión y seguridad:** El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.
- **Funcionamiento de red ordenada:** Es probable que dos o más redes operen en alguna zona donde sea posible la interferencia entre ellas, esto obstaculiza el funcionamiento del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.
- **Funcionamiento sin licencia:** Los usuarios prefieren trabajar sobre LAN inalámbricas que no necesitan de una licencia para la banda de frecuencia usada por la red.
- **Traspasos (***Handoff***)/Itenerancia (***roaming***):** El protocolo MAC usado debería permitir a las estaciones móviles desplazarse de una celda a otra.
- **Configuración dinámica:** Los aspectos de direccionamiento MAC y de gestión de red de la LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

1.3.5 Configuraciones

- **Red AD-HOC**

Conocidas también como ***Redes sin Infraestructura***. El termino ***ad hoc*** aunque podría ser interpretado con connotaciones negativas (“improvisado” o “desorganizado”), en el contexto de las redes inalámbricas hace referencia a redes flexibles en las cuales todas las estaciones ofrecen servicios de encaminamiento para permitir la comunicación de estaciones que no tienen conexión inalámbrica directa.

En relación a las redes cableadas, las redes Ad Hoc presentan cambios de topología frecuente e impredecible debido a la movilidad de sus estaciones. Estas características impiden la utilización de protocolos de encaminamiento desarrollados para redes cableadas y crean nuevos retos de investigación que permitan ofrecer soluciones de encaminamiento eficientes que superen problemas como topología dinámica, recursos de AB, batería limitada, seguridad reducida.

Las Redes *ad-hoc* están formadas por hosts móviles que pueden estar conectados entre sí arbitrariamente y de manera dinámica. Es decir, no hay ningún elemento fijo y la topología de la red puede adoptar múltiples formas siendo igual de funcional. En este tipo de redes, todos los nodos funcionan como ruteadores y se ven involucrados en el descubrimiento y mantenimiento de rutas.

Algunos ejemplos de uso de las redes Ad-Hoc son: Operaciones de emergencia de búsqueda y rescate, convenciones y análisis de datos en terrenos catastróficos

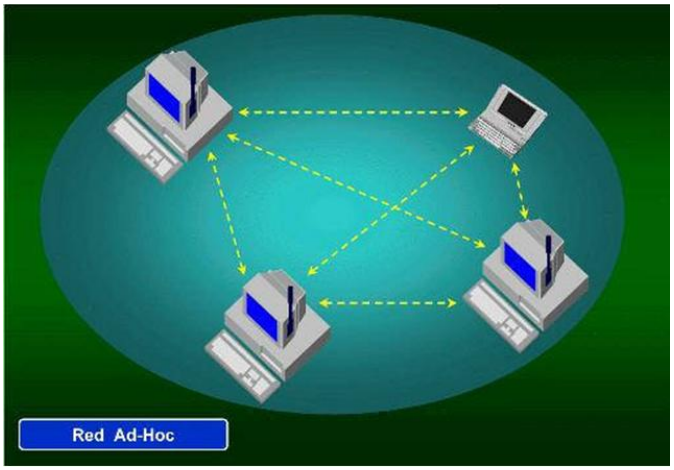


Figura. 1.15. LAN Inalámbrica Ad – Hoc [8]

- **Red Infraestructura**

En el modo de ***infraestructura*** cada estación se conecta a un ***Punto de Acceso*** (***AP***) a través de un enlace inalámbrico. La configuración formada por el AP y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula, cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits). *En el modo infraestructura el* ***BSSID corresponde al AP de la dirección MAC***.

Así, el nodo puede moverse libremente pero si sale fuera del rango de su enlace debe conectarse a otro para asegurar que la información llegue a su destino; de esa forma se podrán ir añadiendo más AP a medida que sean necesarios. La gestión está centralizada en un AP, así los datos que un host emite llegan al AP y éste los transfiere a los otros miembros de la red.

De ésta forma se economiza el ancho de banda, también es posible conectar AP entre sí (por cable o WiFi) para aumentar el alcance de la red WiFi (el rango que cubre un AP es de 25 y 100 metros). Esta topología resulta ideal para permitir el acceso a Internet o a una red local a los ordenadores inalámbricos itinerantes.

Ejemplo de este tipo de redes es la Red de telefonía móvil formada por numerosas estaciones y antenas dispersas por todas las ciudades.

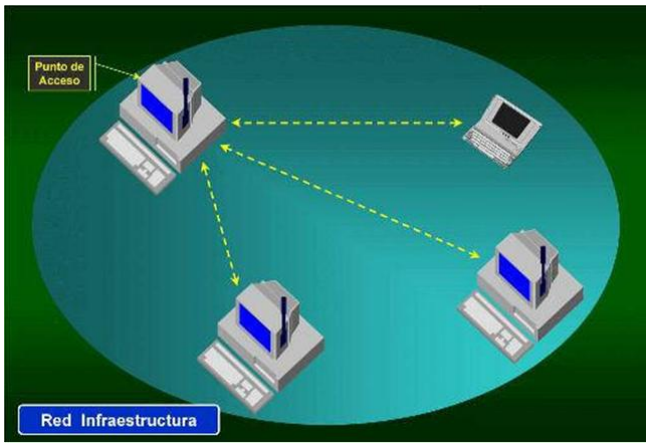


Figura. 1.16. LAN Inalámbrica con Infraestructura

1.3.6 Beneficios

Las redes LAN inalámbricas (WLAN) ofrecen diversas ventajas sobre las redes LAN convencionales (Ethernet, Token-Ring, fibra óptica) porque pueden ser móviles. Los beneficios son evidentes para computadoras portátiles y computadoras de escritorio dado que el usuario puede verdaderamente trasladarse de un punto a otro y permanecer conectado a la red LAN y a sus recursos.

La red puede establecerse sin incurrir en los gastos y las exigencias de colocar cables e instalar conectores en paredes, además, las redes inalámbricas son flexibles dado que las máquinas de escritorio pueden cambiarse de lugar sin ningún trabajo de infraestructura. Esto resulta particularmente útil al instalar sitios temporales o al trabajar en lugares "fijos" que periódicamente cambian de ubicación tales como: las empresas que se trasladan a otra oficina más grande cuando exceden la capacidad de sus instalaciones actuales.

La disponibilidad de la norma IEEE 802.11(que define el Control de Acceso al Medio y las características de la Capa Física, específicas para LAN Inalámbricas), las únicas soluciones de redes inalámbricas disponibles eran dispositivos de diseño original y baja velocidad. Esta norma estableció un sistema de 2Mbps en 1997. La ampliación IEEE 802.11b aprobada en 1999 aumentó la velocidad a 11 Mbps., esto ofrece aproximadamente la misma gama de rendimiento que una tarjeta Ethernet de 10 Mbps. La norma IEEE 802.11a está siendo considerada y podría aumentar la velocidad hasta 25 Mbps o más [8].

1.3.7 Dispositivos

- **Adaptadores de Red Inalámbricos**

Estos son las interfaces que conectarán los equipos de los usuarios (PC, Notebooks, etc.) a la estructura de red. Estos elementos tienen distintos modelos según la forma en que se conectarán al equipo del usuario. Hay tres dispositivos internos para conectarse a los buses PCMCIA, PCI y COMPACTFLASH y uno externo para conectarlo al conector USB del equipo usuario.

- **Punto de Acceso Inalámbrico**

Este dispositivo permite a los equipos que poseen Adaptadores de Red Inalámbricos conectarse entre sí. Además permite comunicarse con otros Puntos de Acceso con el fin de ampliar la cobertura de la LAN. Esta última función se asocia a una funcionalidad como Bridge, además de conectar equipos de usuarios se pueden conectar switches o routers pertenecientes a la infraestructura de red cableado de cobre o fibra preexistente.

- **Punto de Acceso de Red Inalámbrico con funciones de Router**

Cuando es necesario unir una LAN con otra LAN (Internet por ejemplo), es mandatorio utilizar este dispositivo que será el encargado de interpretar las direcciones de origen y destino de las comunicaciones internas o externas y encaminarlas convenientemente.

- **Antenas**

Si bien cada uno de los dispositivos WLAN anteriores poseen un dispositivo irradiante básico que le permite comunicarse con otros dispositivos cercanos, es posible que las distancias entre los usuarios sea tal en donde deba utilizar antenas con características especiales.

Normalmente el tipo de antena a utilizar se elije según la topología de los puntos a unir; por ejemplo para una topología punto a punto se usa una antena direccional que concentre la potencia en un determinado sentido, para una topología Punto-Multipunto se usa una antena omnidireccional en el centro geográfico de la red y antenas direccionales apuntando a este centro en los puntos circundantes.

- **Amplificadores**

Si la potencia irradiada por las Antenas no alcanza a cubrir adecuadamente la dispersión de usuarios de la red, es necesario agregar Amplificadores para la señal de transmisión.

1.3.8 Aplicaciones

- **Ampliación de las redes LAN**

Una red LAN inalámbrica evita el coste de la instalación del cableado y facilita las tareas de traslado y otras modificaciones en la estructura de la red; sin embargo el uso de cableado estructurado ya existente en las construcciones, minimizó el uso de redes LAN inalámbricas.

Actualmente, es frecuente combinar el uso de redes LAN inalámbricas con cableadas en una empresa. Así, una LAN inalámbrica puede estar conectada con una LAN cableada en el mismo recinto, denominándose a ésta aplicación ***ampliación o extensión de redes LAN*** [1]***.***

La Figura 1.17 muestra la configuración de una LAN inalámbrica de ***celdas únicas en la cual todas*** los sistemas finales inalámbricos se encuentran en el dominio de un único módulo de control.

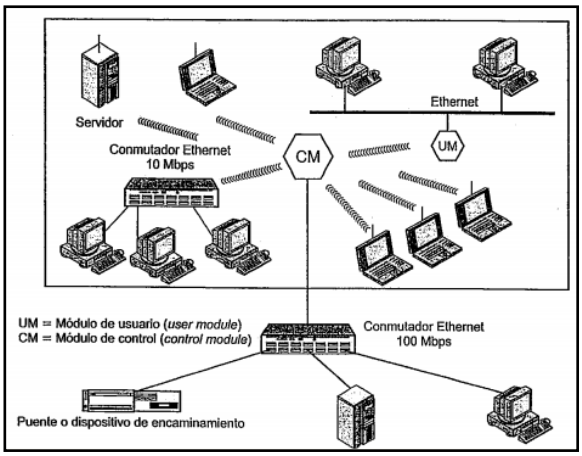


Figura. 1.17. LAN inalámbrica de celda única

En esta configuración existe una LAN troncal cableada que conecta varios servidores, estaciones de trabajo y uno o más puentes o dispositivos de encaminamiento para la comunicación con otras redes. Adicional, se observa que existe un ***CM*** (*módulo de control*) y un ***UM*** (módulo de usuario).

El ***módulo de control*** funciona como interfaz con la LAN inalámbrica, incluye funciones propias de un dispositivo de encaminamiento para conectar a la troncal la LAN inalámbrica. Los ***módulos de usuario*** como hubs y otros controlan varias estaciones fuera de una LAN cableada que a la vez pueden formar parte de una LAN inalámbrica. La Figura 1.18 muestra la configuración de una LAN inalámbrica de ***celda múltiple*** en la cual existen varios módulos de control (CM) interconectados por una LAN cableada. Cada módulo da servicio a varios sistemas finales inalámbricos dentro de su rango de transmisión. Ejemplo de este tipo de configuración es una LAN de infrarrojos, en donde la transmisión se encuentra limitada a una sola habitación por lo que se necesita una celda en cada habitación de un edificio de oficinas que precise de soporte inalámbrico [1].

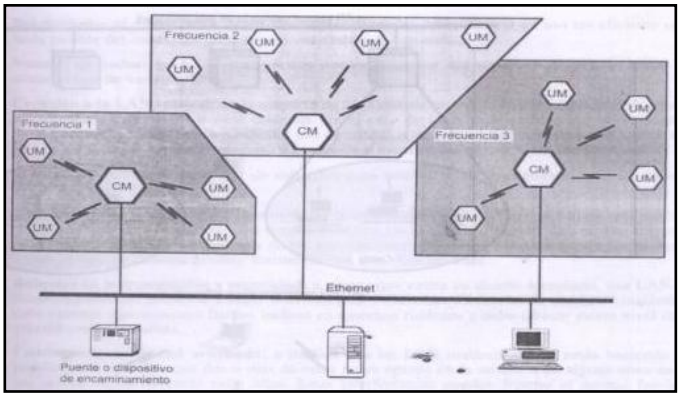


Figura. 1.18. LAN inalámbrica de celda múltiple

- **Interconexión entre edificios**

Otra aplicación es la conexión de redes LAN situadas en edificios vecinos, la red LAN puede ser cableada o inalámbrica. En esta aplicación se hace uso de un enlace punto a punto inalámbrico entre los dos edificios; los dispositivo utilizados son, por lo general, puentes o dispositivos de encaminamiento.

El enlace punto a punto no es en sí una LAN, pero ésta aplicación se usa en las LAN Inalámbricas. La combinación del Punto de Acceso y el Puente permite llevar a cabo el enlace entre dos áreas inalámbricas cuando resulta imposible o demasiado caro realizar esta unión mediante un cable [8].

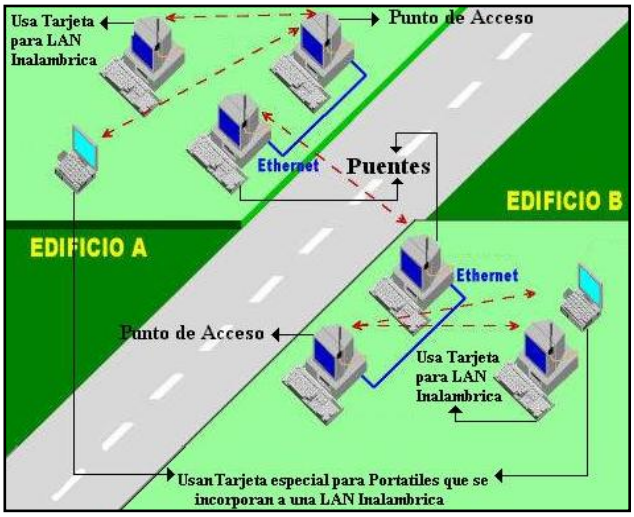


Figura. 1.19. Conexión entre dos edificios

- **Acceso nómada**

Permite un enlace no guiado entre un centro o servidor de LAN y un terminal de datos móvil con antena (computador portátil). En este caso el usuario puede desplazarse con la computadora portátil y conectarse con servidores de LAN inalámbricos desde distintos lugares. La Figura 1.20 muestra esta aplicación [8].

Figura. 1.20. Tarjeta de LAN inalámbrica especial para portátiles

CAPÍTULO 2

CAPA DE ENLACE DE DATOS

La Capa de Enlace de Datos proporciona un medio para intercambiar datos a través de medios locales comunes. La Capa de Enlace de Datos realiza dos servicios básicos [9]:

- Permite a las capas superiores acceder a los medios usando técnicas como tramas.
- Controla como los datos se ubican en los medios y son recibidos desde los medios usando técnicas como control de acceso a los medios y detección de errores.

Como en cada una de las capas OSI, existen términos específicos para esta capa como:

- ***Trama:*** el PDU de la capa de enlace de datos
- ***Nodo:*** la notación de la Capa 2 para dispositivos de red conectados a un medio común.
- ***Medios / medio (***físico***):*** los medios físicos para la transferencia de información entre dos nodos.
- ***Red (***física***):*** dos o más nodos conectados a un medio común.

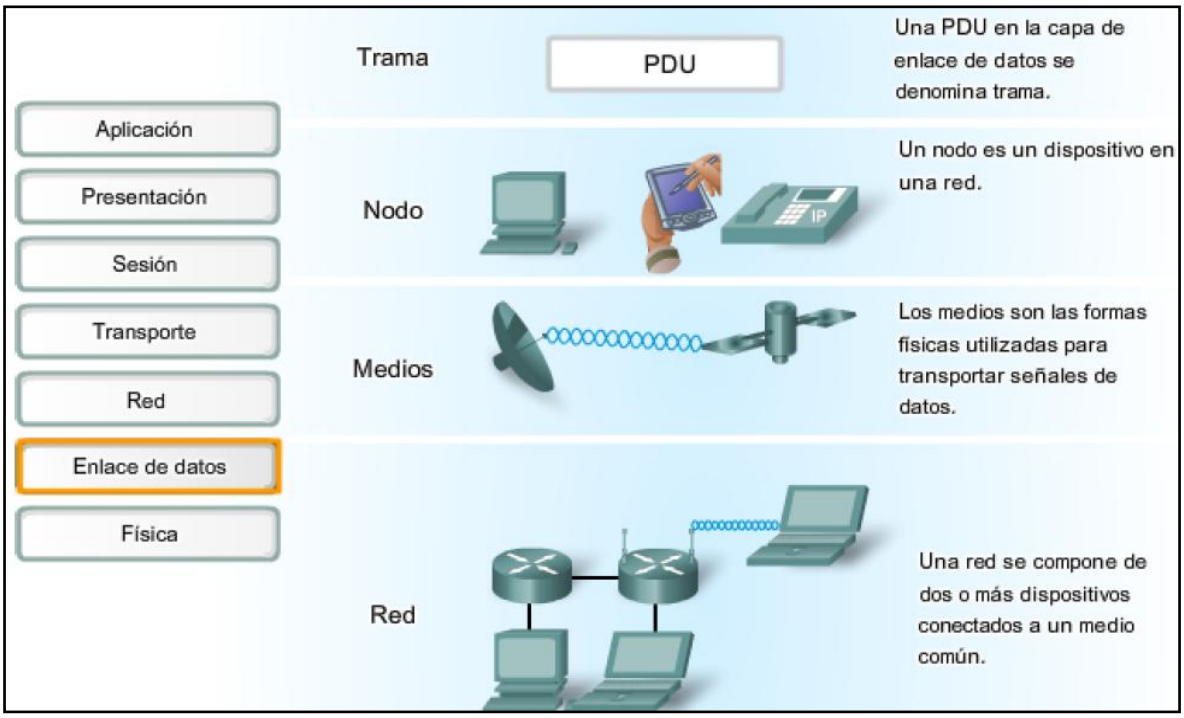


Figura. 2.1. Términos de la Capa de Enlace de Datos

La Capa de Enlace de Datos es responsable del intercambio de tramas entre nodos a través de los medios de una red.

Funciones de la Capa de Enlaces de Datos

- Proveer servicios de interfaz a la capa de red
- Tratamiento con errores de transmisión
- Regulación de flujo de datos

2.1 ETHERNET

Ethernet opera en las dos capas inferiores del modelo OSI: la *Capa de Enlace de Datos* y la *Capa Física* [10]

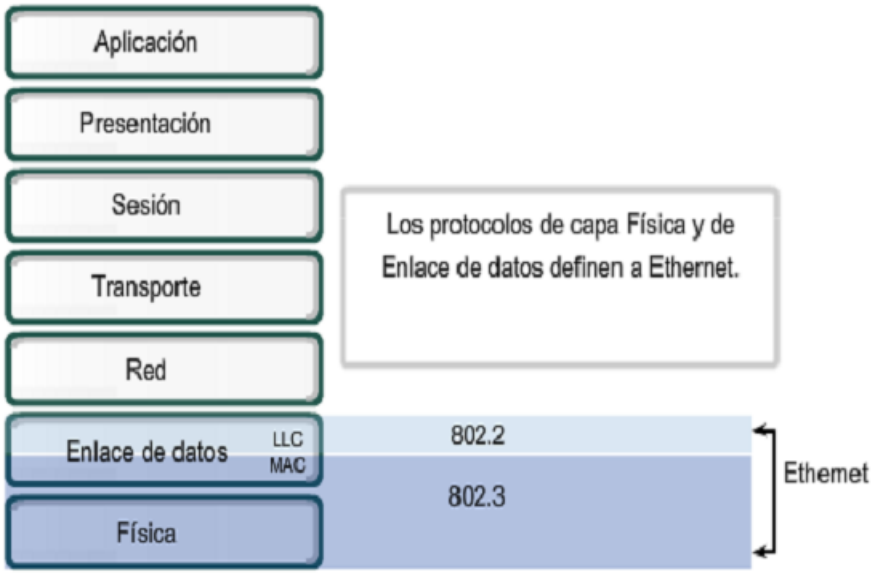


Figura. 2.2. Ethernet - Capa de Enlace de Datos

Subcapas de Enlaces de Datos

Para que exista una gran variedad de funciones en la red, la capa de Enlace de Datos se divide en dos subcapas:

- La subcapa superior (LLC) define los procesos de software que proveen servicios a los Protocolos de capa de red.
- La subcapa inferior (MAC) define los procesos de acceso a los medios realizados por el hardware.

Separar la capa de Enlace de Datos en subcapas permite a un tipo de trama definida por la capa superior, acceder a diferentes tipos de medios definidos por la capa inferior; tal es el caso de varias tecnologías LAN, como la Ethernet.

2.1.1 Capa MAC

El control de acceso al medio ***MAC,*** es la subcapa de Ethernet inferior de la capa de Enlace de Datos. El hardware implementa, por lo general, el control de acceso al medio en la tarjeta de interfaz de red (NIC).

2.1.1.1 Estándar IEEE 802.3

El estándar IEEE 802.3 es extenso y se subdivide en diferentes sub-estándares, por tanto los componentes del IEEE 802.3 se nombran de acuerdo a las siguientes convenciones [11]:

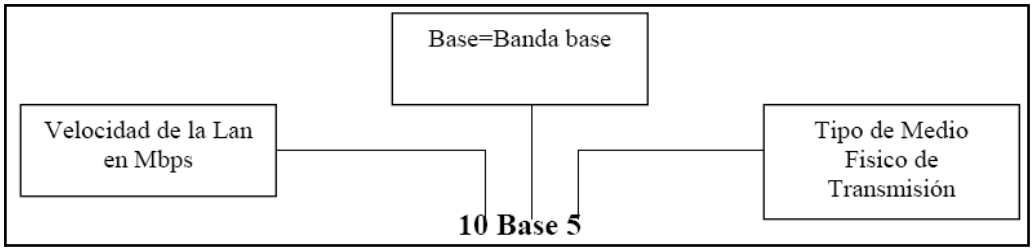


Figura. 2.3. Convenciones del estándar IEEE 802.3

Tabla. 2.1. Diferentes capas físicas del estándar IEEE 802.3

Denominación	***Cable***	***Pares***	***Full Duplex***	***Conectores***	***Distancia***
10 BASE5	Coaxial grueso	1	No	'N'	500 m
10 BASE2	RG 58 (coaxial fino)	1	No	BNC	185 m
10 BASE - T	UTP categ. 3	2	Sí	RJ – 45	100 m
10 BASE - T	UTP categ. 5	2	Sí	RJ – 45	150 m
100 BASE - TX	UTP categ. 5	2	Sí	RJ – 45	100 m
100 BASE - TX	STP	2	Sí	9 pin D sub.	100 m

100 BASE – T4	UTP categ. 3	4	No	RJ – 45	100 m
1000 BASE - CX	STP	2	Sí	8 pin HSSDC o, 9 pin D sub	25 m
1000 BASE – T (prev. Mar. 99)	UTP categ. 5	4	Sí	RJ – 45	100 m

Tabla. 2.2. Cableado con Fibra Óptica

Medio	***Ventana***	***Luz***	***Fibra***	***Conectores***	***Distancia***
10 BASE - FL	Primera	Normal	62.5 / 125	ST	2 Km
100 BASE - FX	Segunda	Normal	62.5 / 125	SC	2 Km
100 BASE – SX (propuesto)	Primera	Láser	62.5 / 125 50 / 125	SC o, ST	500 m 500 m
1000 BASE – SX	Primera	Láser	62.5 / 125 50 / 125	SC	275 m 550 m
1000 BASE – LX	Segunda	Láser	62.5 / 125 50 / 125 9 / 125	SC	550 m 550 m 5 Km

Codificación

Codificación Manchester es una variación de la codificación Manchester básica, un bit 1 se indica mediante la ausencia de una transición al comienzo del intervalo, un bit 0 se indica mediante la presencia de una transición al inicio del intervalo. Este esquema ofrece mejor inmunidad al ruido [11].

Tabla. 2.3. Codificación

Tipo de Red	*Velocidad (Mbps)*	*Codificación*	*Número de Pares*	*Frecuencia Señalización*	*Categoría mín. de UTP*
1 BASE - 5	1	Manchester	1	2	2
Token Ring	4	Manchester Diferencial	1	8	3
10 BASE-T	10	Manchester	1	20	3
100BASE – T4	100	8B / 6T	3	25	3
100BASE – T2	100	PAM 5*5	2	25	2
100 VG-AnyLAN	100	5B / 6B	4	30	3
Token Ring	16	Manchester Diferencial	1	32	3
ATM	25.6	4B / 5B	1	32	3
FDDI, 100 BASE – X	100	4B / 5B	1	125	5
1000BASE-TX	1000	PAM 5*5	4	125	5
ATM	155.52	NRZ	1	155.52	5
1000 BASE - X	1000	8B / 10B	1	1250	-

Protocolo de Subcapa MAC del 802.3 (trama) [11]

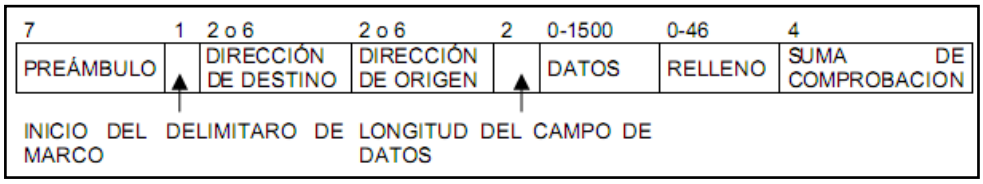


Figura. 2.4. Trama de la subcapa MAC 802.3

- ***Preámbulo:*** cada uno de los cuales contiene el patrón de bits 10101010. La codificación Manchester de este patrón produce una onda cuadrada de 10 MHz permitiendo que el reloj de recepción se sincronice con el de transmisión
- ***Inicio de Marco:*** contiene 10101011 para indicar el inicio del marco.
- ***Dirección origen y destino:*** el bit de orden mayor de la dirección de destino es 0 para direcciones ordinarias; 1 para direcciones de grupo o multidifusión. La dirección que es únicamente 1 está reservada para difusión.
- ***Longitud:*** cuántos bytes están presentes en el campo de datos de un mínimo de 0 a un máximo de 1500.
- ***Relleno:*** para determinar si es un marco válido o es basura. Para que sea válido debe tener al menos 64 bytes para evitar que una estación complete la transmisión de un marco corto antes de que el primer bit llegue al extremo más alejado del cable.
- ***Suma de comprobación:*** redundancia cíclica, de esta manera se determina que los datos se reciben correctamente

El correcto funcionamiento de CSMA/CD requiere que el tiempo de ida y vuelta entre dos estaciones cualesquiera de la red no supere el tiempo que tarda en emitirse la trama permitida. Este tiempo depende de la velocidad de la red que a su vez fija una distancia máxima entre las estaciones. Velocidad de la red, tamaño de trama mínimo, tiempo de ida y vuelta y distancia máxima, son parámetros que están relacionados entre sí, de la siguiente manera:

Tabla. 2.4. Relación de Parámetros

Velocidad (Mbps)	*Tamaño de trama mínimo*	*Tiempo de ida y vuelta*	*Distancia máxima*
10	512 bits	51.2 ms	4000 m
100	512 bits	5.12 ms	412 m
1000	4096 bits	4.096 ms	330 m

Las distancias que se indican en la Tabla 2.4 son para casos óptimos; ya en la práctica, la distancia depende de varios factores tal como el número de repetidores intermedios o el tipo de cable utilizado.

2.1.1.2 Encapsulación de datos

La encapsulación de datos proporciona tres funciones:

- Delimitación de trama
- Direccionamiento
- Detección de errores

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibir la misma. Cuando se forma una trama, la capa MAC agrega un encabezado y un tráiler a la PDU de Capa 3. La utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y la agrupación de bits en el nodo receptor.

El proceso de entramado ofrece delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama. Este proceso ofrece una sincronización entre los nodos transmisores y receptores.

El proceso de encapsulación también posibilita el direccionamiento de la capa de Enlace de datos. Cada encabezado Ethernet agregado a la trama contiene la dirección física (dirección MAC) que permite que la trama se envíe a un nodo de destino.

Una función adicional de la encapsulación de datos es la detección de errores

2.1.1.3 Control de acceso al medio

La subcapa MAC (Figura. 2.5.) controla la colocación y retiro de tramas en los medios. Como su nombre lo indica, se encarga de administrar el control de acceso al medio, esto incluye el inicio de la transmisión de tramas y la recuperación por fallo de transmisión debido a colisiones [10].

Topología lógica

La topología lógica subyacente de Ethernet es un bus de multiacceso. Esto significa que todos los nodos (dispositivos) en ese segmento de la red comparten el medio y además reciben todas las tramas transmitidas por cualquier nodo de dicho segmento.

Debido a que todos los nodos reciben todas las tramas, cada nodo debe determinar si debe aceptar y procesar una determinada trama. Esto requiere analizar el direccionamiento en la trama provisto por la dirección MAC. Ethernet ofrece un método para determinar cómo comparten los nodos el acceso al medio. El método de control de acceso a los medios para Ethernet clásica es el Acceso múltiple con detección de portadora con detección de colisiones (CSMA/CD).

Figura. 2.5. Subcapa MAC

2.1.2 Capa LLC

El subnivel LLC gestiona la comunicación de enlace de datos y define el uso de puntos de interfaz lógicos llamados puntos de acceso al servicio (SAP, Service Access Points). Otros equipos pueden hacer referencia y utilizar los SAP para transferir información desde el subnivel LLC hacia los niveles superiores del modelo OSI. La categoría 802.2 define estos estándares.

2.1.2.1 Estándar IEEE 802.2

El estándar IEEE 802.2 describe la parte superior de la Capa de Enlace de Datos que usa el protocolo LLC.

LLC proporciona control de errores y control de flujo (cabecera con secuencia y acuse), además especifica puntos de acceso al servicio (SAP). Ofrece varios servicios como:

- Sin conexión no confirmado
- Con conexión
- Sin conexión confirmado

2.1.2.2 Identificación de protocolos

Es necesario definir como se entienden entre sí las entidades LLC, es decir, definir el protocolo LLC entre entidades pares; este entendimiento se logra

mediante la inclusión de información de control de protocolo LLC en las LLC_PDU intercambiadas y mediante el orden en que son pasadas.

Algunas LLC_PDUs son consideradas *comandos* u *órdenes,* otras *respuestas* y otras definidas de ambas formas. Sus diferentes clases se conocen por los valores que toma el campo de control de la unidad de datos. Debido a que hay tres posibles tipos de operación; existen tres tipos de protocolo [9].

Protocolo para operación Tipo 1: *SIN CONEXION*

Es un protocolo sencillo ya que no requiere secuencia, control de flujo ni retransmisiones. La subcapa MAC realiza los chequeos para detección de errores pero la información proporcionada a LLC no provoca ninguna acción por parte de este. Las estaciones que son capaces de operar con este protocolo se llaman ***LLC_Clase_I***. Al ser un servicio orientado a *No Conexión*, todas las LLC_PDU son no numeradas.

Con este tipo de servicio, si se producen errores o entregas desordenadas, los niveles altos son los encargados de corregirlos si es necesario.

Protocolo para operación Tipo 2: *CON CONEXION*

Estos protocolos son usados cuando se presume que la comunicación va a ser duradera y necesita alta fiabilidad. Las estaciones que los soportan son: estaciones ***LLC_Clase_II*** y ***LLC_Clase IV*** obligadas a poder comunicarse con estaciones ***LLC_Clase_I*** y ***LLC_Clase_III*** por tanto, deben incorporar protocolos de *operación tipo 1*.

Ambos tipos de estaciones son bastante complejas ya que tienen que construir las LLC_PDU tanto para los servicios No orientados a conexión como para los Orientados a conexión.

Protocolo para operación Tipo 3: *SIN CONEXIÓN Y CON RECONOCIMIENTOS*

Este protocolo no necesita un proceso previo de establecimiento de conexión, sin embargo corrige errores. El subnivel MAC opera normalmente realizando los chequeos para la detección de errores y los descartes que deba de hacer mientras, que la información que pasa al LLC produce el envío en sentido opuesto de una LLA_AC y el reenvío en caso de error. Las estaciones capaces de operar con este protocolo y los protocolos de tipo 1 son conocidos como ***LLC_Clase_III***, mientras que si operan con los *tres tipos* son ***LLC_Clase_IV***.

La Figura. 2.6 muestra las LLC_PDUs disponibles en cada tipo de estaciones para protocolos tipos 1, 2 y 3

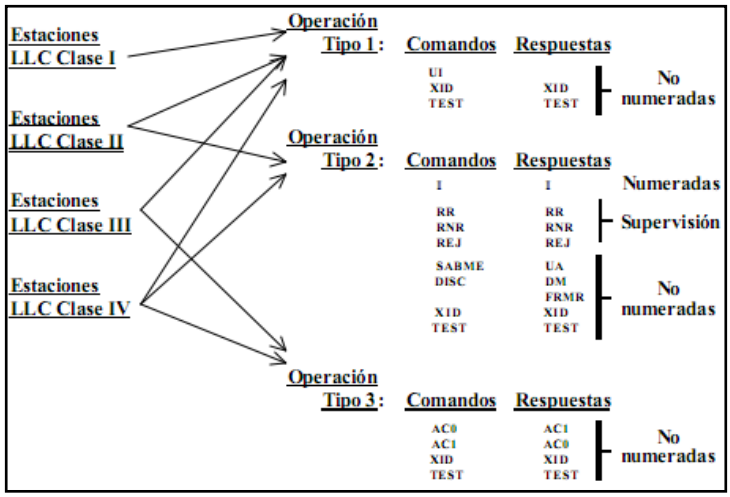


Figura. 2.6. Subcapa MAC

2.1.2.3 Control de flujo

El control de flujo es la solución más simple al problema que se genera cuando las velocidades de transmisión o de aceptación de datos del emisor y del receptor son diferentes. Con un buen control de flujo se puede regular la cadencia (frecuencia) con la que se envía las tramas en la red, es por tanto, un sistema que regula el tráfico de la red. Las técnicas de control de flujo normalmente necesitan información de feedback (retroalimentación) intercambiable entre emisor y receptor. Lo más común es que no se transmitan tramas al receptor hasta que

éste no haya dado su permiso para que les sean transmitidas, cuando lo haga, expresará cuantas tramas está dispuesto a recibir que se conceda un nuevo permiso.

Gestión de Enlace de datos

Cuando se tienen dos ordenadores unidos por una línea punto a punto la gestión de enlace es muy simple. El problema se suscita cuando se tienen múltiples ordenadores que comparten el canal, en especial cuando los servicios estén orientados a la conexión puesto que habrá que gestionar el quién, cuándo, cómo y con quién. Algunos sistemas de gestión de enlace requieren la definición de una estación primaria que lleve el peso de la gestión haciendo que el resto sean secundarias. Se crea un sistema de sondeo o POLLING por el que la estación primaria pregunta a las secundarias por sus necesidades de transmisión estableciendo, de este modo, un mecanismo de permisos para gestionar la utilización del enlace. En las LAN lo normal es que las estaciones sean todas iguales desde el punto de vista de la funcionalidad en el nivel de enlace, es decir, que todos los nodos de la red tienen los mismos derechos de transmisión estableciéndose una competición por el acceso al medio.

2.2 WIFI: 802.11

Separar la capa de Enlace de Datos en subcapas permite a un tipo de trama definida por la capa superior acceder a diferentes tipos de medios definidos por la capa inferior.

2.2.1 Estándares

El estándar 802.11 es el primer estándar y permite un ancho de banda de 1 a 2 Mbps. El estándar original se ha modificado para optimizar el ancho de banda de estándares 802.11a, 802.11b y 802.11g denominados estándares físicos (802.11), o para especificar componentes de mejor manera con el fin de garantizar mayor seguridad o compatibilidad.

2.2.1.1 802.11a

El estándar 802.11a conocido también como ***WiFi 5,*** admite un ancho de banda superior (rendimiento total máximo: 54 Mbp, en la práctica es de 30 Mpbs).

El estándar 802.11a tiene en teoría un flujo de datos máximo de 54 Mbps, cinco veces el del 802.11b y sólo a un rango de 30 metros aproximadamente. El estándar 802.11a se basa en la tecnología llamada OFDM (multiplexación por división de frecuencias ortogonales), transmite en un rango de frecuencia de 5 GHz y utiliza 8 canales no superpuestos [7].

Es por esto que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de "***banda dual***".

Tabla. 2.5. Flujo de datos – Rango; 802.11a

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

2.2.1.2 802.11b

Ofrece un rendimiento total máximo de 11 Mpbs (6 Mpbs en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.

El estándar ***802.11b*** permite un máximo de transferencia de datos de 11 Mbps en un rango de 100 metros aproximadamente en ambientes cerrados y de más de 200 metros al aire libre (o incluso más que eso con el uso de antenas direccionales) [7].

Tabla. 2.6. Flujo de datos – Rango; 802.11b

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
11 Mbit/s	50 m	200 m
5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

2.2.1.3 802.11c

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

2.2.1.4 802.11d

El estándar ***802.11d*** es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

2.2.1.5 802.11e

El estándar ***802.11e*** está destinado a mejorar la calidad del servicio en el nivel de la *capa de enlace de datos*. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.

2.2.1.6 802.11f

El ***802.11f*** es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de

acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como ***itinerancia***

2.2.1.7 802.11g

El estándar ***802.11g*** ofrece un ancho de banda elevado en el rango de frecuencia de 2,4 GHz. Es compatible con el estándar 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b con excepción de algunos dispositivos más antiguos [7].

Permite un máximo de transferencia de datos de 54 Mbps en rangos comparables a los del estándar 802.11b. Además, y debido a que el estándar 802.11g utiliza el rango de frecuencia de 2.4 GHz con codificación OFDM, es compatible con los dispositivos 802.11b.

Tabla. 2.7. Flujo de datos – Rango; 802.11g

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

2.2.1.8 802.11h

El estándar ***802.11h*** tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la h de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.

2.2.1.9 802.11i

El estándar ***802.11i*** está destinado a mejorar la seguridad en la transferencia de datos (administrar, distribuir claves, implementar el cifrado y la autenticación).

Este estándar se basa en el *AES* (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.

2.2.1.10 802.11r

El estándar ***802.11r*** se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.

2.2.1.11 802.11j

El estándar ***802.11j*** es para la regulación japonesa, lo que el 802.11h es para la regulación europea.

2.2.2 Capa MAC

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas, ya que debe de tenerse en cuenta las dos topologías de una red inalámbrica [12]:

• ***Ad-Hoc:*** Varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utilizan en grupos de trabajo, reuniones, conferencias, etc.

• ***Basadas en Infraestructura:*** La red inalámbrica se crea como una extensión a la red existente basada en cable. Los elementos inalámbricos se conectan a la red cableada por medio de un punto de acceso o un PC Bridge, siendo estos los que controlan el tráfico entre las estaciones inalámbricas y las transmisiones entre la red inalámbrica y la red cableada.

Además de los dos tipos de topología diferentes se debe tener en cuenta:

- Perturbaciones ambientales (**interferencias**)
- Variaciones en la **potencia** de la señal
- **Conexiones y desconexiones** repentinas en la red
- **Roaming**. Nodos móviles que van pasando de celda en celda.

A pesar de todo ello la norma IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas ayudando a la fabricación en serie de chips.

Trama MAC 802.11

El protocolo MAC del estándar IEEE 802.11 distingue tres tipos de tramas: ***tramas de control, de datos y de gestión***. Los mensajes de ***gestión*** se utilizan para soportar los servicios de 802.11. Los mensajes de ***control*** se utilizan para la correcta entrega de tramas y los mensajes de ***datos*** transportan la información de los usuarios.

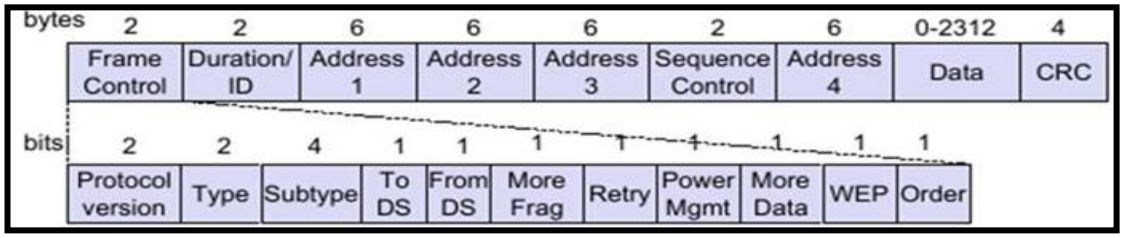


Figura. 2.7. Formato de trama IEEE 802.11

FC: Frame Control:

- Tipo de trama + subtipo:
- Control: ACK, RTS, CTS...
- Gestión Entre estaciones y AP's para acceso a servicios.
- Datos.
- Trama dentro de la BSS ó hacia/desde otra BSS.
- Bit que indica si hay más fragmentos en la secuencia.
- Bit que indica si es retransmisión.
- Cifrado / No cifrado.

D/ID: Duración (CTS, RTS) / ID (conexión).

Direcciones:

- Source Adress.
- Destiniy Adress.
- Transmissor Adress - BSS externos en la misma ESS.
- Receptor Adress - BSS externos en la misma ESS.
- BSSID

SC: Sequence Control

- Controla fragmentos.

Datos: En la práctica <1500 bytes.

- CRC: 32 bits.

Servicios

El estándar IEEE 802.11 ***define nueve servicios MAC*** (Medium Access Control). ***Seis de estos servicios*** están destinados a la transmisión de paquetes entre STA. ***Los tres servicios*** restantes se utilizan para controlar el acceso a la LAN 802.11 y para proporcionar confidencialidad a la transacción de datos [37].

- **Servicios de Transmisión y distribución de los mensajes** [38]

Asociación: Relación Estación-AP (SSID).

Reasociación: Transferencias de asociación entre AP's de la ESS.

Disociación: Fin asociación.

Entrega MSDUs (Unidad de datos del servicio MAC)
- Con confirmación (ACK).
- Fragmentación MAC.
- Entrega en la misma BSS o en otras (Distribución).

DFC: Función de coordinación distribuida:
- SIFS: Intervalo corto.

- DIFS: Intervalo distribuido.

PFC: Función de coordinación puntual:

- Coordinador (Punto de acceso).
- Tiempo dividido en "Supertramas" de dos partes:
- Libre de contienda (PFC).
- Con contienda (DFC).

- **Servicios de Control de acceso y seguridad:**

Autenticación: SSID (Service Set ID) ó técnica de cifrado.

Fin de autenticación.

Privacidad -> Cifrado de datos:

- WEP (Wire Equivalent Privacy) - Vulnerable.
- WPA2 (802.11i) (Wi-Fi Protected Access 2) - Cifrado AES.

Mecanismos de Acceso

• ***Protocolos con arbitraje*** (FDMA - Frequency Division Multiple Access, TDMA - Time Division Multiple Access)

• ***Protocolos de contienda*** (CDMA/CA - Carrier-Sense, Múltiple Access, Collision Avoidance), CDMA (Code Division, Multiple Access) y el CDMA/CD (detección de colision).

2.2.2.1 Protocolos con arbitraje

La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este

mecanismo se llama multiplexación en el tiempo (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

2.2.2.2 Protocolos de acceso por contienda

- **CSMA (Code-division multiple Access / Acceso múltiple por división de tiempo).**

Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia PN. En este esquema se asigna una secuencia PN distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias PN pertenecientes a los demás nodos. Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia PN del destinatario, así se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

- **CSMA/CD (Carrier Sense, Multiple Access, Collision Detection)**

En estos medios de difusión (radio, infrarrojos) no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las LAN alambradas. Se diseñó una variación denominada detección de colisiones (peine) para redes inalámbricas. En este esquema, cuando un nodo tiene una trama que transmitir, lo que hace es generar una secuencia binaria seudoaleatoria corta llamada ***peine*** la cual se añade al preámbulo de la trama. A continuación; el nodo realiza la detección de la portadora, si el canal está libre transmite la secuencia del peine. Por cada ***1*** del peine el nodo transmite una señal durante un intervalo de tiempo corto, por cada ***0*** del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y espera hasta que los otros nodos hayan transmitido su trama. La eficiencia del esquema depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

❖ **CSMA/CA (Carrier-Sense, Múltiple Access, Collision Avoidance).**

Este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3. En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF6 de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI [12].

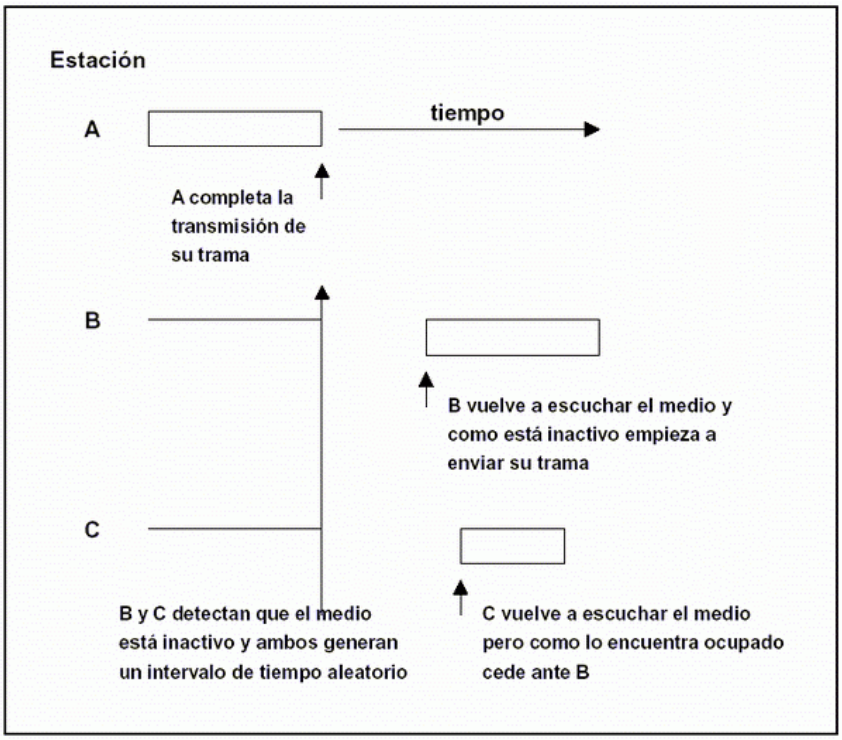


Figura. 2.8. Protocolo CSMA/CA

Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío y, a la capa MAC se le da el estado de canal vacío

para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

El Standard proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible. Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11. En comunicaciones inalámbricas este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido) [12].

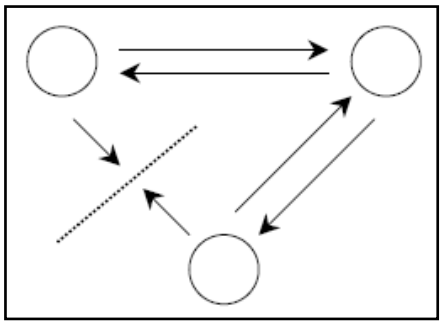


Figura. 2.9. Ejemplo Nodo Escondido

Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión. Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina Reservation-Based Protocol, que es la 2ª subcapa MAC.

Cuando una estación está lista para transmitir, primero envía una solicitud (destino y longitud del mensaje) al punto de acceso (RTS – “request to send”) quien difunde el NAV (Network Allocation Vector) - tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos para que queden informados de que se va a transmitir (y que por lo tanto no transmitan) y cuál va a ser la duración de la transmisión. Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de backoff (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS – “clear to send”) que permite al solicitante enviar su trama

(datos). Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan de nuevo.

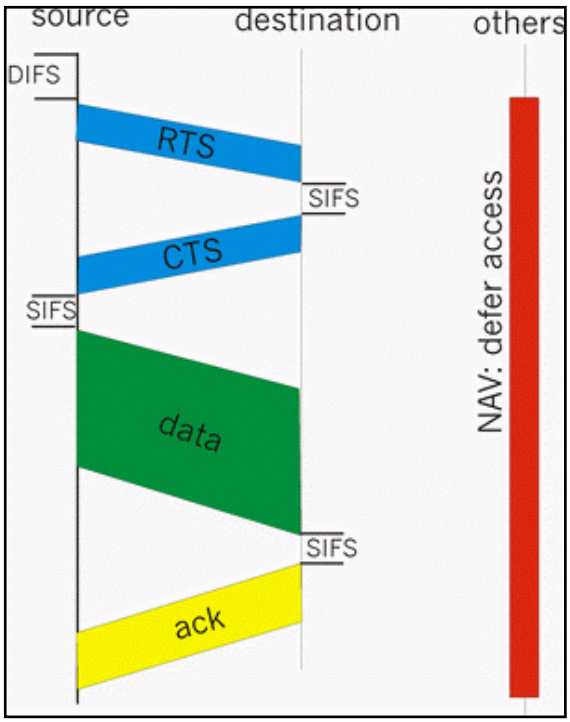


Figura. 2.10. CSMA/CA – Mecanismo de intercambio

Después de que se recibe la trama de los datos se devuelve una trama de reconocimiento (ACK - ACKnowledged) notificando al transmisor que se ha recibido correctamente la información (sin colisiones) [12].

Aún así permanece el problema de que las tramas RTS sean enviadas por varias estaciones a la vez, sin embargo estas colisiones son menos dañinas ya que el tiempo de duración de estas tramas es relativamente corto. Este mismo protocolo también puede utilizarse si no existen dispositivos auxiliares en las redes ad-hoc, en este caso no aparecería la trama NAV.

CAPÍTULO 3

SEGURIDAD. INTRUSIONES EN LA RED

3.1 SEGURIDAD

Seguridad en redes es mantener bajo protección los recursos y la información con que cuenta la red, a través de procedimientos basados en políticas de seguridad que permitan el control de dichos recursos e información.

Las debilidades de las tecnologías inalámbricas y más en concreto de la tecnología Wi-Fi; son la falta de seguridad atribuida más que a la seguridad física, a la seguridad de la información, su integridad y la no accesibilidad a terceros.

3.2 INTRODUCCIÓN A LA SEGURIDAD

Actualmente las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. Tampoco se debe subestimar las fallas de seguridad provenientes del interior mismo de la organización; una de las razones es la propia complejidad de la red con respecto a la dificultad para la detección y corrección de los problemas de seguridad que van apareciendo, como también son las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas.

“Hackers”, “crakers”, y otros términos forman parte del vocabulario ordinario de los usuarios y administradores de las redes. Adicional a las técnicas y herramientas criptográficas, es necesario recalcar la importancia de la protección de los sistemas, poniendo atención y vigilancia continua y sistemática.

3.2.1 Vulnerabilidad

Las vulnerabilidades de un sistema surgen a partir de errores individuales, nuevas y complejas vulnerabilidades surgen de la interacción entre varios componentes como el kernel del sistema, sistemas de archivos, servidores de procesos, entre otros. Estas vulnerabilidades generan problemas de seguridad para la red en cuestión; entre las más conocidas están el “finger username” y la notificación de mensajes de correo a través de “comsat”; además de:

- **Aumento de privilegios**. Los más terribles permiten tomar el control de los programas ejecutados con privilegios de administrador;
- **Generación de error de sistema**. El objetivo de algunos puntos vulnerables es saturar un programa informático para que "se bloquee".

Con estas prácticas el intruso puede obtener información como horarios de trabajo, claves de acceso, nombres de empleados e infiltrarse indirectamente en la organización y/o empresa así como también acceder a la información de manera sencilla: por medio de una conversación, de una llamada telefónica (haciéndose pasar por un empleado de una empresa) ó recibiendo un correo electrónico informando que se ha ganado un premio y se requieren algunos datos para enviar el supuesto premio a al domicilio [13].

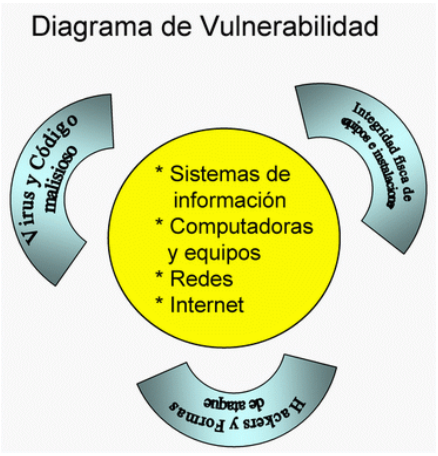


Figura. 3.1. Diagrama de Vulnerabilidad

3.2.2 Amenaza

Las principales amenazas actuales a la seguridad son:

- *Las utilizadas para comprometer la seguridad de los sistemas*; como escanear/explorar otros sistemas para encontrar puertas traseras para obtener acceso no autorizado y los ataques del tipo DoS (Denial of Service).
- *Malware*; como virus informáticos, spyware, troyanos, gusanos, etc.
- *Spammin*; que son sistemas utilizados para enviar correos electrónicos no solicitados

La Figura 3.2.; muestra las diferentes amenazas a las que puede estar expuesta una red [14].

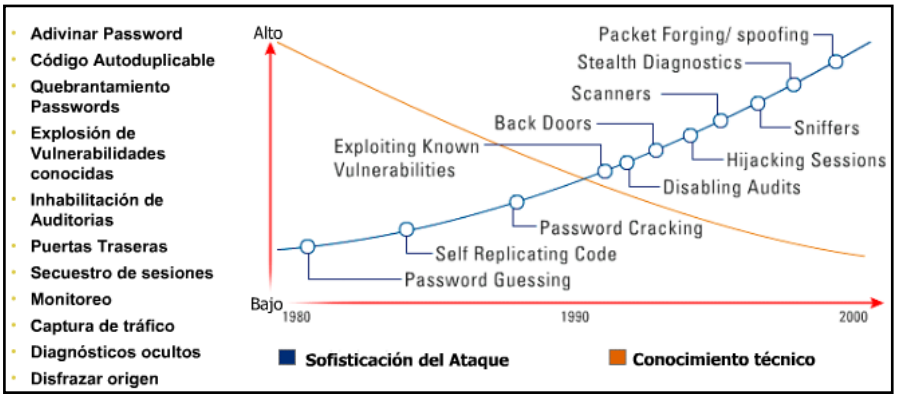


Figura. 3.2. Incremento de las amenazas

3.2.3 Riesgo

La seguridad de red hace referencia a la protección de los recursos de la red, en particular a los sistemas de computación (PCs, servidores, PDAs, etc.) y a la información-datos-conocimiento. Los diferentes riesgos de los recursos de red se pueden identificar en relación a:

- Los sistemas de computación (referente a la disponibilidad-tolerancia a fallos)
- Acceso no autorizado, y
- La información-datos, que tiene que ver con el acrónimo CIA (Confidentiality, Integrity, Availability).

Sin embargo, se puede delimitar las áreas de riesgos:

- Los que tienen que ver con las personas de dentro en relación a las de fuera,
- Los que están relacionados con la red, por ejemplo las escuchas clandestinas
- Lo que tienen que ver con los computadores como las vulnerabilidades de los sistemas, el control de acceso y la seguridad física.

3.3 PRINCIPALES ATAQUES

Cualquier equipo conectado a una red informática puede ser vulnerable a un ataque. Un "**ataque**" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Los ataques se producen en Internet, en su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo; en casos atípicos, son ejecutados por piratas informáticos. Para bloquear estas intrusiones es importante estar familiarizado con los principales tipos de ataques y tomar medidas preventivas [15].

Los ataques pueden ejecutarse por diversos motivos:

- Obtener acceso al sistema;
- Robar información (secretos industriales o propiedad intelectual)
- Recopilar información personal acerca de un usuario;
- Obtener información de cuentas bancarias u organización,
- Utilizar el sistema de un usuario como un "rebote" para un ataque;
- Usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

3.3.1 ATAQUES EN REDES LAN ETHERNET

3.3.1.1 Spoof, spam, sniffers

- ***Spoof***

Se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque es sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basado en el nombre o dirección IP del host suplantado. Adicional, los anillos de confianza basados en estas características son fáciles de falsificar y demasiado abundantes, razón por la cual el spoofing en la actualidad es un ataque no trivial, pero factible contra cualquier tipo de organización [16].

Para el ataque por spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita establecer una comunicación falseada con su objetivo, y evitar que el equipo suplantado interfiera en el ataque.

Es probable que el último punto no sea difícil de conseguir; aunque existen múltiples formas de dejar fuera de juego al sistema suplantado que no son triviales tales como: modificar rutas de red, ubicar un filtrado de paquetes entre ambos sistemas, etc.; lo más fácil en la mayoría de ocasiones es simplemente lanzar una negación de servicio contra el sistema en cuestión.

Otro aspecto importante del ataque, es la comunicación falseada entre dos equipos, no es tan inmediato como el anterior y es donde reside la principal dificultad del spoofing. Un escenario típico del ataque; un pirata envía una trama SYN a su objetivo indicando como dirección origen la de esa tercera máquina que está fuera de servicio y que mantiene algún tipo de relación de confianza con la atacada. El host objetivo responde con un SYN+ACK a la tercera máquina, que simplemente lo ignorará por estar fuera de servicio (si no lo hiciera, la conexión se resetearía y el ataque no sería posible), y el atacante enviará ahora una trama ACK a su objetivo, también con la dirección origen de la tercera máquina. Para que la conexión llegue a establecerse, esta última trama deberá enviarse con el

número de secuencia adecuado; el pirata ha de predecir correctamente este número: si no lo hace, la trama será descartada), y si lo consigue la conexión se establecerá y podrá comenzar a enviar datos a su objetivo, generalmente para tratar de insertar una puerta trasera que permita una conexión normal entre las dos máquinas.

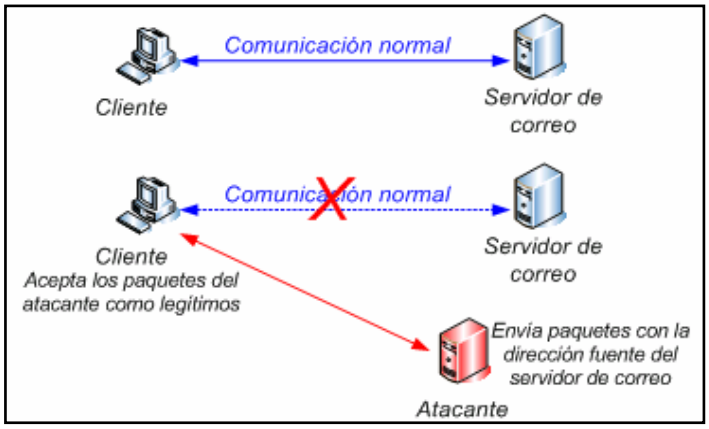


Figura. 3.3. Spoofing de dirección IP

Además de este ataque; existen otros ataques de falseamiento relacionados en mayor o menor medida con este, entre los que destacan el DNS Spoofing, el ARP Spoofing y el Web Spoofing.

- **DNS Spoofing**

Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (resolver con una dirección falsa un cierto nombre DNS), o viceversa (resolver con un nombre falso una cierta dirección IP). Esto se puede conseguir de diferentes formas, modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre, hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como DNS Poisoning); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos.

- **ARP/MAC Spoofing**

ARP Spoofing hace referencia a la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP - MAC) de una víctima de forma que, en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un host o a una puerta de enlace atacante en lugar de hacerlo a su destino legítimo.

El protocolo Ethernet trabaja mediante direcciones MAC. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC, para ello cuando un host quiere comunicarse con una IP emite una trama ARP–Request a la dirección de Broadcast pidiendo la MAC del host destino, primando la IP. El ordenador con la IP solicitada responde con un ARP–Reply indicando su MAC. Los switchs y los host guardan una tabla local con la relación IP-MAC llamada “tabla ARP”. La tabla ARP es sensible a cambios y se actualiza con frecuencia; puede ser falseada por un ordenador atacante que emita tramas ARP–Reply indicando su MAC como destino válido para un a IP específica [17].

La idea es sencilla, y los efectos del ataque pueden ser muy negativos como: negaciones de servicio hasta interceptación de datos, incluyendo algunos Man in the Middle contra ciertos protocolos cifrados.

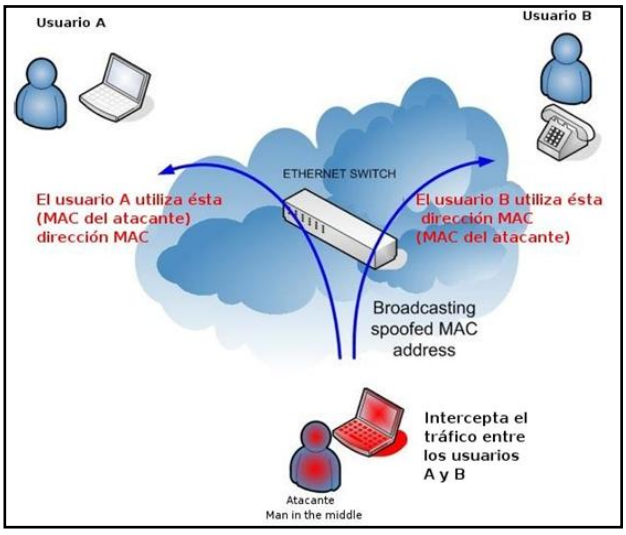


Figura. 3.4. ARP/MAC Spoofing [18]

- **Web Spoofing**

Este ataque permite a un pirata visualizar y modificar cualquier página web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL. Para ello, mediante código malicioso un atacante crea una ventana del navegador correspondiente de apariencia inofensiva en la máquina de su víctima; a partir de ahí, enruta todas las páginas dirigidas al equipo atacado «incluyendo las cargadas en nuevas ventanas del navegador» a través de su propia máquina donde son modificadas para que cualquier evento generado por el cliente sea registrado (esto implica registrar cualquier dato introducido en un formulario, cualquier click en un enlace, etc.).

- ***Spam***

Se llama *SPAM*, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (en algunos casos de manera masiva) que perjudican de alguna o varias maneras al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

La recepción de SPAM, o correo basura, se ha convertido en uno de los principales problemas de la comunicación por correo electrónico [19].

Cómo se producen los ataques Spam

Un Spam se produce de la siguiente manera:

Emisor del ataque (spammer): envía un mismo mensaje masivo a un gran número de direcciones. Hace uso de de cualquier área de Internet desprotegida y mal gestionada.

Máquina atacada: es una máquina desprotegida, y encargada de manera forzada, de procesar la entrega de correo y de emitir informes de error. Se puede afectar de manera simultánea a varias máquinas.

Emisores de fallo de error: son las máquinas atacadas y cualquier otro servidor de correo que esté recibiendo el mensaje de ataque.

Máquina inocente: es una máquina correctamente protegida contra el Spam; sin embargo, es la receptora de los informes de error producidos en el ataque y de las denuncias

Procedimiento del ataque

El proceso de un ataque Spam es el siguiente:

Elaboración del mensaje: El Emisor del ataque prepara un mensaje con un campo ***From***, y también puede añadir un campo ***Reply-to***, ambos generalmente idénticos. Estas direcciones suelen ser y escogidas al azar del estilo *fd34rf@dpto.usal.es* o incluso el mismo ataque utiliza unas direcciones similares en las que sólo cambia/n alguna/s letras.

Ataque a una máquina mal gestionada: con un procedimiento automático, inyectan el mensaje en un servidor desprotegido en Internet con destino a un gran número de direcciones de correo. Muchas de estas direcciones pueden ser incorrectas.

Procesamiento de errores: la máquina atacada debe procesar los errores producidos de las direcciones que son incorrectas. Algunas de las direcciones a las que se envía el Spam, serán aceptadas por sus servidores de correo que las encaminarán al servidor final el cual podrá rechazarlo y enviar un informe a la máquina del responsable de las direcciones de campo *From.*

Informes de error: Estos informes van encaminados a la dirección del campo ***From*** y la máquina responsable de la misma será la verdadera víctima de este tipo de ataques. Pero dado que la dirección del campo From: es incorrecta ésta máquina inocente generará el clásico informe de error:

<<< 550 <j9fyx7429@gugu.usal.es>... User unknown; que, en este caso, se entregará en la cuenta local de postmaster Es decir por cada dirección incorrecta, de las miles implicadas en el ataque, se producirá un informe de error que irá a la máquina inocente. Debemos de pensar que pueden ser miles los errores y que esta máquina ***Receptora de fallos de error*** tendrá que emplear sus recursos en procesarlos. Además el buzón de postmaster de dicha organización se verá inundado de estos errores.

Contenido del correo Spam

A continuación se muestra algunos de los temas más comunes que vienen en el contenido de estos mensajes:

- Información sobre negocios piramidales para conseguir dinero de manera fácil y rápida
- Cadenas de cartas
- Enlaces a páginas Web de tipo pornográfico
- Personas, generalmente niños muy enfermos, a los cuales podemos salvar enviando el correo que nos llega con la información.
- Falsos virus

Tabla. 3.1. correo SPAM [20]

¿Cómo lo hacen?	¿Qué buscan con el *spam*?	¿Quién es el que se beneficia?
Motivando e incitando al comprador con descuentos, promociones y otros beneficios	Vender sus productos y/o servicios	Empresa de e-marketing (generalmente falsa)
• Remedios milagrosos. • Enfermos que se "salvarán" si se reenvía el correo • Falsos Virus y Antivirus • Virus y gusanos • Software Ilegal muy barato • Enlaces a Pornografía Gratis	Conseguir nuevas direcciones electrónicas para la creación de bases de datos.	Los *spammers*
• Supuestos negocios piramidales • Hacer parte de una estafa o lavado de dinero (caso Nigeria 419. ver más adelante)	Negocios fraudulentos	El estafador
Falso requerimiento para actualizar información	Robo de identidad	El estafador

- ***Sniffers***

Un ***sniffer*** es un programa de., para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella [21].

Es algo común que el medio de transmisión (cable coaxial, UTP, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él.

Una vez que la NIC se encuentre en estado promiscuo se necesitarán los privilegios administrativos o de root, así la computadora será capaz de ver

todos los datos transmitidos; en ese momento el programa comienza a hacer una lectura de toda la información entrante al PC por la tarjeta de red. Así, el ***sniffer*** conseguirá observar el equipo de origen, el equipo destino, número de puerto, etc.; de esta manera se puede observar toda la información intercambiada entre dos computadoras [22].

Topología de redes y packet sniffers

La cantidad de tramas que puede obtener un sniffer depende de la topología de red, del nodo donde esté instalado y del medio de transmisión. Por ejemplo [23]:

- **Para redes antiguas con topologías en estrella**, el sniffer se podría instalar en cualquier nodo, ya que lo que hace el nodo central es retransmitir todo lo que recibe a todos los nodos. Sin embargo en las redes modernas en las que solo lo retransmite al nodo destino, el único lugar donde se podría poner el sniffer para que capturara todas las tramas sería el nodo central.
- **Para topologías en anillo, doble anillo y en bus**, el sniffer se podría instalar en cualquier nodo, ya que todos tienen acceso al medio de transmisión compartido.
- **Para las topologías en árbol**, el nodo con acceso a más tramas sería el nodo raíz, aunque con los switches más modernos las tramas entre niveles inferiores de un nodo viajarían directamente y no se propagarían al nodo raíz.

Es importante remarcar el hecho de que los sniffers sólo tienen efecto en redes que compartan el medio de transmisión como en redes sobre cable coaxial, cables de par trenzado (UTP, FTP o STP), o redes WiFi.

El uso de switch en lugar de hub incrementa la seguridad de la red ya que limita el uso de sniffers al dirigirse las tramas únicamente a sus correspondientes destinatarios.

Utilidades

Los principales usos que se le pueden dar son:

- ***Captura automática*** de contraseñas enviadas en claro y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por crackers para atacar sistemas a *posteriori*.
- ***Conversión del tráfico*** de red en un formato entendible por los humanos.
- ***Análisis de fallos*** para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?
- ***Medición del tráfico***, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- ***Detección de intrusos***, con el fin de descubrir hackers. Aunque para ello existen programas específicos llamados IDS (Intrusion Detection System, Sistema de Detección de intrusos), estos son prácticamente sniffers con funcionalidades específicas.
- ***Creación de registros de red***, de modo que los hackers no puedan detectar que están siendo investigados.
- ***Para los desarrolladores***, en aplicaciones cliente-servidor. Les permite analizar la información real que se transmite por la red.

3.3.1.2 Gusanos, virus

Los virus informáticos son programas habitualmente ocultos dentro de otro programa, correo electrónico, pagina web, fichero o volumen. Se ejecutan automáticamente, haciendo copias de sí dentro de otros programas a los que infectan. Esta capacidad de copiarse a sí mismos genera un efecto de propagación exponencial, que además suele conllevar la alteración del funcionamiento del equipo infectado.

- ***Virus***

Los virus informáticos son pequeños programas de computadora que al igual que un virus biológico, infecta equipos de computo y se propaga a través

de la red o utilizando otros medios de transmisión como Memorias, disquetes, discos ópticos, etc.

El crecimiento de las redes y en especial de la Internet ha facilitado la propagación de virus de forma acelerada. Un método de propagación de virus común es el uso de correo electrónico; al abrir un correo infectado por virus puede infectar el equipo y puede ser capaza de reenviarse a otros usuarios de correo utilizando la libreta de direcciones del usuario.

Hay que tomar en cuenta que cualquier medio de intercambio de datos puede ser un medio potencial de propagación de virus. Los medios más comunes pueden ser: Disquetes, DVD, Conexiones LAN, Vía MODEM, CD, Unidades portables (memorias Flash), cintas magnéticas, conexiones a Internet.

Un virus puede causar muchos daños como perdida de datos, evitar que el equipo arranque normalmente (daños en el sector de arranque), formateo de las unidades lógicas.

Un síntoma de infección dentro de la red es que el desempeño de esta baja considerablemente a causa de trafico excesivo provocado por virus.

- ***Gusanos***

Los gusanos pueden ser clasificados de acuerdo con el método de propagación que usan, es decir, por el modo en que se copian a los equipos de las nuevas víctimas, por su método de instalación, de ejecución o de acuerdo a las características comunes a todos los programas maliciosos [24].

Muchos de los gusanos capaces de causar brotes virulentos usan uno o más métodos de propagación y técnicas de infección. Estos métodos son:

- Gusanos de correo electrónico
- Gusanos de sistemas de mensajes instantáneos
- Gusanos de Internet
- Gusanos de IRC

- **Gusanos de correo electrónico**

Los gusanos de correo electrónico se propagan por medio de mensajes infectados. El gusano puede estar en forma de *archivo adjunto* o contener un *enlace a un sitio web infectado*. Sin embargo, en ambos casos el vehículo es el mensaje de correo electrónico.

En el primer caso, mediante un *archivo adjunto*; el gusano se activa cuando el usuario abre los datos adjuntos. En el segundo caso, mediante un *enlace a un sitio web infectado*, el gusano se activa cuando el usuario sigue el enlace que lleva al sitio infectado. Los gusanos de correo electrónico por lo general usan uno de los siguientes métodos para propagarse:

- Conexión directa a los servidores SMTP usando una biblioteca SMTP API contenida en el gusano
- Servicios de MS Outlook
- Funciones MAPI de Windows

Los gusanos de correo electrónico recolectan direcciones en los equipos de las víctimas para seguir propagándose. Los gusanos usan una o más de las siguientes técnicas:

- Escanear la libreta de direcciones locales de MS Outlook
- Escanear la base de datos WAB
- Escanear los archivos que pueden contener direcciones de correo electrónico
- Enviar copias de sí mismo a todos los mensajes del buzón postal del usuario (los gusanos incluso pueden "responder" a mensajes que el usuario todavía no ha abierto)

Mientras estas son las técnicas más usadas, algunos gusanos son capaces hasta de construir nuevas direcciones usando listas de posibles nombres combinadas con nombres de dominio comunes.

- **Gusanos de sistemas de mensajes instantáneos (ICQ y MSN)**

Estos gusanos tienen sólo un método de propagación. Se propagan por medio de sistemas de mensajes instantáneos enviando a todos los contactos locales, enlaces a sitios web infectados. La única diferencia entre estos virus y los de correo electrónico, es la forma en que envían los enlaces.

- **Gusanos de Internet**

Los autores de virus usan otras técnicas para distribuir gusanos de ordenador, incluyendo:

- *Copiar el gusano a los recursos de red compartidos:* el gusano localiza equipos remotos y se copia a sí mismo en los directorios que están abiertos a operaciones de lectura y escritura. Estos gusanos de red escanean todos los recursos de red disponibles, usando los servicios locales de los sistemas operativos y escaneando Internet en búsqueda de equipos vulnerables. A continuación, intentan conectarse a esos equipos y obtener acceso ilimitado a los mismos.
- *Explotar las vulnerabilidades de los sistemas operativos para penetrar a los ordenadores o a las redes*: los gusanos escanean Internet buscando equipos que no han sido parchados, es decir, cuyos sistemas operativos contienen vulnerabilidades críticas aún abiertas. El gusano envía paquetes de datos o solicitudes que pueden instalar el gusano completo o una sección de su código fuente que contiene funciones de downloader. Si este código se instala con éxito, el gusano completo es cargado; una vez que el gusano se instala, empieza a ejecutar su código y el ciclo continúa.
- *Piggy-backing:* usa programas maliciosos en calidad de portador del gusano

Los gusanos que usan servidores Web y FTP pertenecen a otra categoría. La infección se realiza en dos etapas; primero, los gusanos penetran a archivos de servicio en el servidor de archivos, por ejemplo, a páginas web estáticas. Después, los gusanos esperan a que los clientes efectúen alguna acción con los archivos infectados y entonces atacan a los

equipos individuales. Estos equipos-víctimas son luego usados como plataforma de lanzamiento para realizar nuevos ataques.

"Algunos creadores de virus usan gusanos o troyanos para difundir nuevos gusanos. Inicialmente, estos autores identifican estos virus que instalaron puertas traseras (backdoors) en los equipos de las víctimas. En la mayoría de los casos, éstas permiten enviar instrucciones al equipo de la víctima. Los ordenadores zombies que tienen puertas traseras instaladas, pueden usarse para descargar y ejecutar archivos, en este caso, copias de nuevos gusanos."

- **Gusanos de IRC**

Al igual que los gusanos de correo electrónico, usa dos formas de propagarse por los canales de IRC. La primera, envía un enlace que lleve a un sitio infectado; la segunda, envía archivos infectados, es menos efectiva, ya que el destinatario tiene que confirmar la recepción, guardar el archivo y abrirlo para que el gusano penetre al equipo de la víctima.

- **Gusanos de redes de intercambio de archivos (File-sharing o P2P)**

Estos gusanos se copian a sí mismos en una carpeta compartida por lo general ubicada en el equipo local. Una vez que el gusano ha logrado poner una copia de sí mismo en una carpeta compartida bajo un nombre aparentemente inofensivo, la red P2P empieza a funcionar: informa a los otros usuarios acerca del nuevo recurso y proporciona la infraestructura para cargar y ejecutar el archivo infectado.

3.3.2 ATAQUES REDES LAN INALÁMBRICAS

3.3.2.1 Access Point Spoofing

Access Point Spoofing o "Asociación Maliciosa"; en este caso el atacante se hace pasar por un access point y el cliente piensa estar conectándose a una red WLAN verdadera. Ataque común en redes ad-hoc.

El AP furtivo puede “atacar” al cliente Wifi de distintas formas:

• Espiando la conversación
• Enviando contenido falso (ej: exploits)
• Redirigiendo los pedidos a sitios malicioso

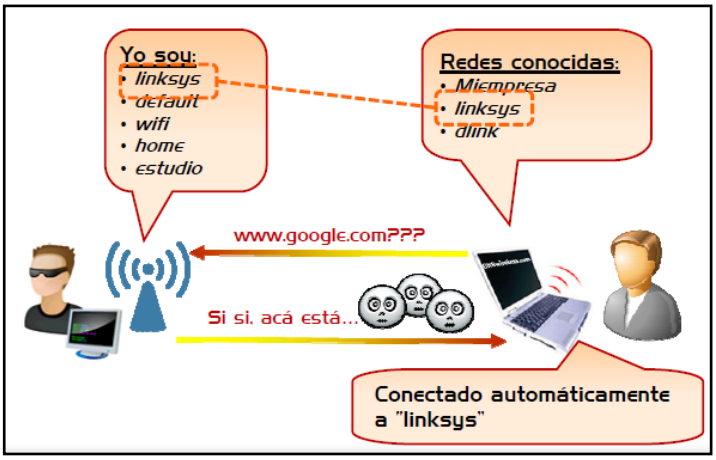


Figura. 3.5. Ejemplo de ataque con AP Spoofing

3.3.2.2 ARP Poisoning

"Envenenamiento ARP", es el ataque al protocolo ARP como el caso del ataque denominado "Man in the Midle". Una computadora invasora X envía un paquete de ARP reply para Y diciendo que la dirección IP de la computadora Z apunta hacia la dirección MAC de la computadora X, y de la misma forma envía un paquete de ARP reply para la computadora Z diciendo que la dirección IP de la computadora Y apunta hacia la dirección MAC de X. Como el protocolo ARP no guarda los estados, las computadoras Y, Z asumen que enviaron un paquete de ARP request solicitando esta información, y asumen los paquetes como verdaderos. A partir de este punto, todos los paquetes enviados y recibidos entre las computadoras Y, Z pasan por X (hombre en medio) [25].

3.3.2.3 WLAN Scáners

WLAN Escáners o "Ataque de Vigilancia", consiste en recorrer un local, área que se desea invadir para descubrir redes WLAN activas en dicho local, así como equipamientos físicos, para un posterior ataque o robo.

3.3.2.4 Wardriving / Warchalking

Se llama de "Wardriving" a la actividad de encontrar puntos de acceso a redes inalámbricas mientras uno se desplaza por la ciudad en un automóvil y haciendo uso de una notebook con una placa de red wireless para detectar señales. Entre los requisitos necesarios para realizar el Wardriving están [26]:

- Automóvil
- Portátil con tarjeta inalámbrica
- Receptor GPS para ubicar un AP

Figura. 3.6. Wardriving

Después de localizar un punto de acceso a una determinada red inalámbrica, algunos individuos marcan el área con un símbolo hecho con tiza en la vereda o la pared, e informan a otros invasores –ésta actividad se denomina "warchalking".

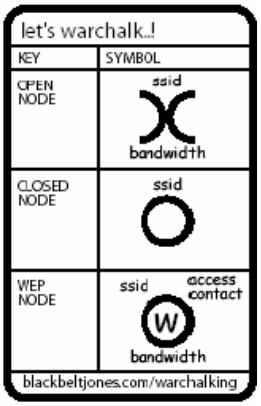


Figura. 3.7. Warchalking

3.3.2.5 Denegación de Servicio (DoS)

Una denegación de servicio (DoS) es un asalto que pueden paralizar o desactivar una WLAN. La posibilidad que se produzca el ataque es algo que las empresas y el despliegue de redes WLAN deben tener en cuenta.

Una forma de ataque DoS es la "fuerza bruta". Esto puede darse de dos formas: Inundación de paquetes que consuma todos los recursos de la red, o una señal de radio fuerte que domine al aire y deshabilite los AP y tarjetas de radio.

Un hacker puede llevar a cabo un ataque basado en DoS mediante el uso de otros equipos de la red para enviar paquetes inútiles al servidor. Esto implica una sobrecarga en la red y uso de ancho de banda asignado a los usuarios legítimos de la red [27].

Las redes inalámbricas son extremadamente vulnerables a los ataques de DoS. Se puede reducir la red a velocidades de arrastre lo cual obliga a dejar de trabajar. Para una compañía que depende de una WLAN, experimentar retrasos puede ser costoso.

Wi-Fi Protected Access (WPA) es vulnerable al tipo de ataque DoS ya que utiliza algoritmos matemáticos para autenticar a los usuarios a la red. Si un usuario está tratando de entrar y envía dos paquetes de datos no autorizados dentro de un segundo, WPA asume que está bajo ataque y se apagará.

Aunque esta característica está diseñada para proteger las violaciones de seguridad, representa una oportunidad de ataque para un hacker; ya que lo único que tienen que hacer es enviar periódicamente tramas de datos causando paros constantes. El hacker puede ser difícil o imposible de encontrar ya que no es necesario usar mucha potencia de transmisión o utilización de la red.

3.3.2.6 Ataques basados en ARP/MAC

Entre los ataques basados en ARP/MAC están [28]:

Man in the Middle (Sniffing): Utilizando ARP Spoofing el atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo.

Secuestro (Hijacking): Utilizando ARP Spoofing el atacante puede lograr redirigir el flujo de tramas entre dos dispositivos hacia su equipo. Así puede lograr colocarse en cualquiera de los dos extremos de la comunicación (previa deshabilitación del correspondiente dispositivo) y secuestrar la sesión.

Denial of service (DoS): Utilizando ARP Spoofing el atacante puede hacer que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

3.4 VULNERABILIDAD EN PROTOCOLOS

El protocolo es abierto en su definición, no hay secretos sobre cómo los datos se transportan en Internet. Siendo abierto, cualquier persona malintencionada puede aprender el protocolo y la implantación particular de un servicio o aplicación sobre él y atacar comunicaciones o transacciones de interés. Esta actividad pasa, y ha dado lugar al sector de los famosos hackers, los piratas informáticos.

3.4.1 PPP

El protocolo PPP para realizar la autenticación hace uso de dos mecanismos como son: PAP y CHAP.

PAP; sólo autentica una vez y deja de funcionar, las contraseñas se envían como texto plano no codificado lo que crea vulnerabilidades. PAP no es un protocolo seguro

CHAP; por su parte realiza comprobaciones cada cierto tiempo para observar si se cuenta con la contraseña correcta. La comprobación es única y aleatoria, lo que evita ataques y autenticaciones no autorizadas.

3.4.2 CSMA / CD

En este protocolo la vulnerabilidad se basa al momento de detectar una colisión durante la transmisión, ya que, si la trama a transmitir fuese menor que el tiempo de vulnerabilidad o su valor máximo; la estación transmisora no podría detectar a tiempo si se ha producido una colisión

3.4.3 RTS / CTS

El acceso al medio es controlado por el uso de diversos tipos de interframe spaces (IFS) o espacio entre tramas, que corresponde a los intervalos de tiempo que una STA necesita esperar antes de enviar datos. Los datos prioritarios como paquetes de RTS/CTS esperarán un período más corto (SIFS) que el tráfico normal.

La vulnerabilidad de este protocolo se presenta cuando el atacante modifica su software para que en cuanto escuche un RTS envié un CTS; se produce una colisión y las unidades se desconectan [29].

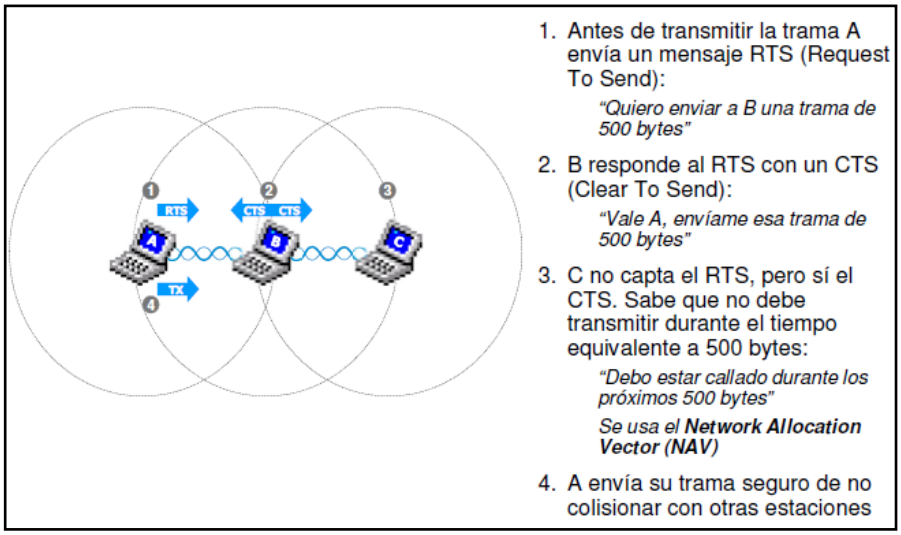


Figura. 3.8. Terminal oculto_ RTS/CTS

3.5 MECANISMOS PROTECCIÓN Y DETECCIÓN

3.5.1 PROTECCIÓN

La mayoría de los problemas de seguridad en redes WLAN son debido al medio de transmisión utilizado, el aire, que es de fácil acceso para los atacantes. Al no poder impedir de ninguna manera que la información que está en el aire sea vista por cualquiera, ésta debe ser protegida por medio de protocolos de encriptación. En la actualidad se utilizan WEP, WPA y WPA2.

La seguridad de los datos se realiza por una compleja técnica de codificación conocida como **WEP** [12] (Wired Equivalent Privacy Algorithm). WEP se basa en proteger los datos transmitidos en el medio RF usando clave de 64 bits y el algoritmo de encriptación RC4 (desarrollado por RSA Security Inc.).

Actualmente WEP está siendo sustituido por un nuevo protocolo: **WPA** [30] (*"WI -FI Protected Access"*). WPA mejora la forma de codificar los datos respecto a WEP, utilizando TKIP (*"Temporal Key Integrity Protocol"*), al mismo tiempo que proporciona autenticación de usuarios mediante 802.1x y EAP.

3.5.1.1 Seguridad WEP (Protocolo de equivalencia con red cableada)

La seguridad de la red es extremadamente importante, especialmente para las aplicaciones o programas que almacenan información valiosa. WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP que codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire.

Cuanto más larga es la clave, más fuerte el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan en cadenas de 10/26 dígitos hexadecimales y 5/13 dígitos alfanuméricos.

La activación del cifrado WEP de 128 bits evitará que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad. Sin embargo, si la clave de seguridad es estática, es posible que un

intruso irrumpa en su red mediante el empleo de tiempo y esfuerzo. Por tanto, se recomienda cambiar la clave WEP frecuentemente; a pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad.

Cifrado

Cuando tenemos activo el cifrado WEP en cualquier dispositivo inalámbrico sea éste un adaptador de red o un AP, estamos forzando que el emisor cifre los datos y el CRC de la trama 802.11, el receptor recoge y la descifra. El cifrado se lleva a cabo partiendo de la clave compartida entre dispositivos que previamente ha sido configurada en cada STA. Un sistema WEP almacena cuatro contraseñas y mediante un índice indica cuál de ellas se va a utilizar en las comunicaciones.

El proceso de cifrado WEP agrega un vector de inicialización (IV) aleatorio de 24 bits concatenándolo con un la clave compartida para generar la llave de cifrado. Al configurar WEP tenemos que introducir un valor de 40 bits (5 dígitos hexadecimales), que junto con los 24 bits del IV obtenemos la clave de 64 bits. El IV podría cambiar en cada trama trasmitida, WEP usa la llave de cifrado para generar la salida de datos que serán los datos cifrados más 32 bits para la comprobación de la integridad, denominada ICV (integrity check value). El valor ICV se utiliza en la STA receptora donde se recalcula y se compara con el del emisor para comprobar si ha habido alguna modificación y tomar una decisión, que puede ser rechazar el paquete [26].

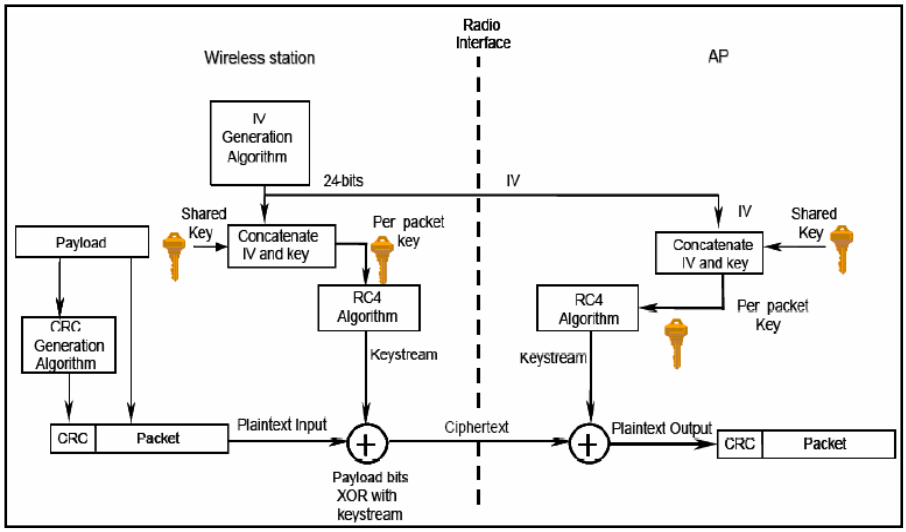


Figura. 3.9. Cifrado en WEP

Para cifrar los datos, WEP utiliza el algoritmo RC4, que consiste en generar un flujo de bits a partir de la clave generada que utiliza como semilla, realiza una operación XOR entre este flujo de bits y los datos que tiene que cifrar. El valor IV garantiza que el flujo de bits no sea siempre el mismo. WEP incluye el IV en la parte no cifrada de la trama, lo que aumenta la inseguridad. La estación receptora utiliza este IV con la clave compartida para descifrar la parte cifrada de la trama [31].

Autenticación

En el sistema WEP se pueden utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida [32].

- **Sistema Abierto:** el cliente WLAN no se tiene que identificar en el AP durante la autenticación. Así, cualquier cliente, independientemente de su clave WEP, puede verificarse en el AP y luego intentar conectarse. La no autenticación ocurre después de la autenticación y la asociación, el sistema WEP puede ser usado para cifrar los paquetes de datos [26].

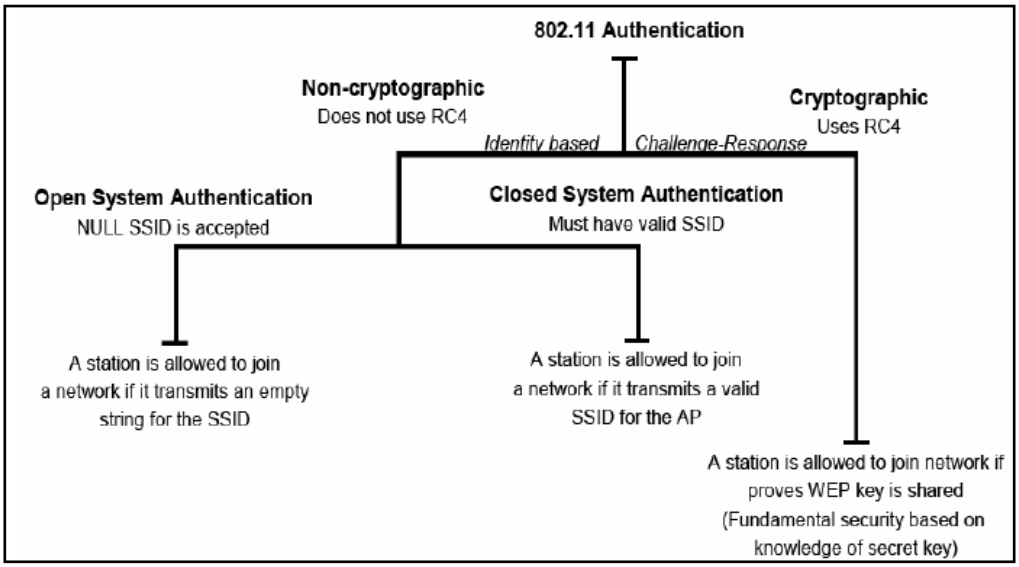


Figura. 3.10. Autenticación en WEP

- **Clave Compartida:** WEP es usado para la autenticación. Este método se puede dividir en cuatro fases:

  1. La estación cliente envía una petición de autenticación al AP.

  2. El AP envía de vuelta un texto modelo.

  3. El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al AP en otra petición de autenticación.

  4. El AP descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el AP envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

Parecería que la autenticación por Clave Compartida es más segura que la autenticación por Sistema Abierto. Sin embargo, es posible averiguar la clave WEP estática interceptando los cuatro paquetes de cada una de las fases de la autenticación con Clave Compartida. Por lo tanto es aconsejable usar la autenticación de Sistema Abierto para la autenticación WEP (nótese que ambos mecanismos de autenticación son débiles) [26].

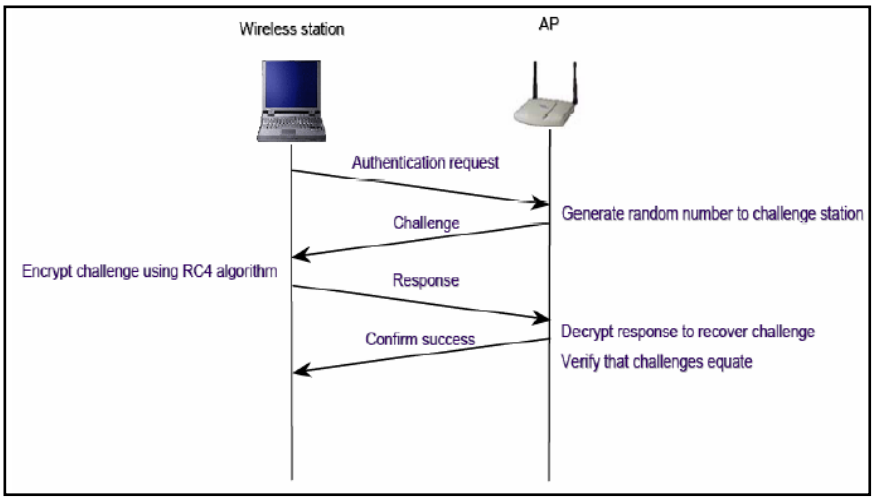


Figura. 3.11. Autenticación en WEP_ Clave compartida

Vulnerabilidades _ Problemas [26]

- **Uso de claves estáticas**
  - No existe ningún mecanismo de gestión de claves
  - Es compartida entre numerosos usuarios por tiempo ilimitado.
  - Se genera mucho tráfico, lo que permite su análisis

- **Vector de inicialización (IV)**
  - Es demasiado corte (hace uso de 24 bits) y se transmiten sin cifrar.
  - Si se repite el IV, se produce la misma secuencia cifrante.
  - Conocida la secuencia, se puede descifrar el tráfico cifrado con ella.
  - RC4 posee una debilidad en su planificación de claves.
  - Se puede realizar ataques que recuperen la clave.

- **Integridad**
  - No existe control criptográfico de la integridad.
  - CRC detecta errores fortuitos
  - Si se cambia algunos bits del paquete y obtener el mismo CRC
  - Se puede cambiar la dirección de destino
- **Configuración**
  - La configuración es predeterminada.
  - Es débil
  - Los valores por defecto de los fabricantes, suelen excluir la seguridad para facilitar el despliegue

- **Autenticación de la STA**
  - Se autentica la STA, no el individuo que ocupa la STA.
  - El cliente no autentica el AP, sólo el AP autentica al cliente

La vida de WEP fue muy corta; esto debido al diseño poco transparente, lo que condujo a ataques muy efectivos a su implantación. Tiempo después de que WEP fuera publicado, el protocolo fue considerado obsoleto, ya que, aunque la

llave tenía una longitud limitada debido a restricciones de exportación, se pudo probar que el protocolo era débil independientemente de ese hecho.

No fueron solo las fallas de diseño las que hicieron que WEP fuera obsoleto, sino también la falta de un sistema de manejo de llaves como parte del protocolo. WEP no tuvo incluido un sistema de manejo de llaves, el sistema de distribución de llaves fue tan simple como teclear manualmente la misma llave en cada dispositivo de la red inalámbrica.

Existen varios ataques y programas para quebrar el WEP (Airsnort, wepcrack, kismac, aircrack, etc). Algunos de los ataques están basados en la limitación numérica de los vectores de inicialización del algoritmo de cifrado RC4, o la presencia de la llamada “debilidad IV” en un datagrama [33].

Posterior a los problemas presentados con WEP, en el 2003 se propone el ***Acceso Protegido a Wi-Fi*** [33] (WPA) y luego queda certificado como parte del estándar IEEE 802.11i, con el nombre de ***WPA2***.

Una mejora notable en el WPA sobre WEP es la posibilidad de intercambiar llaves de manera dinámica mediante un protocolo de integridad temporal de llaves ***TKIP*** (Temporal Key Integrity Protocol). WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de llaves. Si no se usa un servidor de llaves, al protocolo se le conoce como ***PSK*** (Pre-Shared-Key), llamado también WPA o WPA2-Personal. Cuando se emplea un servidor de llaves, al WPA2 se le conoce como WPA2-Corporativo o ***WPA2- Enterprise***. En WPA-Corporativo, se usa un servidor IEEE 802.1X para distribuir las llaves.

3.5.1.2 Seguridad WPA (Wi-Fi Protected Access)

El algoritmo de cifrado conocido para el estándar IEEE 802.11 es **WEP**. Sin embargo, está probado que WEP es inseguro, surgiendo otras alternativas como ***Wi-Fi Protected Access*** (**WPA**), considerado como el estándar recomendado.

WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. Las claves se insertan como dígitos

alfanuméricos, sin restricción de longitud, en la que es recomendable usar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal.

Dentro de WPA, hay dos versiones que utilizan distintos procesos de autenticación. La primera versión es temporal, y se ha aplicado en el último par de años hasta que fueran diseñados y producidos nuevos AP y tarjetas WiFi que soporten los cálculos requeridos por AES. En esta versión se utilizó el protocolo WPA (WiFi Protected Access) basado en el TKIP [34].

- **WPA. Para el uso personal doméstico**

WPA utiliza ***TKIP*** (**Temporal Key Integrity Protocol**) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el IV [35].

TKIP es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP, debido a que las claves están en constante cambio ofreciendo un alto nivel de seguridad para la red. Por otra parte, si las STA de la red usan una “llave previamente compartida”, a este modo se le conoce con el nombre de ***PSK*** (Pre-Shared-Key)

WPA-PSK ó WPA2-Personal, usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que WEP, esta clave hay que introducirla en cada STA y AP de la red inalámbrica. Así, cada STA que se identifique con esta contraseña, accede a la red [35].

Vulnerabilidades

- Clave compartida entre estaciones.
- Si un sistema basa su seguridad en contraseñas, éste es susceptible de sufrir un ataque de fuerza bruta.

- Al momento de establecer el diálogo de autenticación, se establece un tiempo de debilidad en el cual es posible conocer el contenido del paquete de autenticación y conocer su valor cifrado.

➢ **WPA2. Para el uso empresarial/de negocios**

En redes corporativas resulta imprescindible usar mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo; los usuarios de un sistema identificados con usuarios, o la posesión de un certificado digital

Los clientes WPA2 tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del AP. Los sistemas de validación WPA2 pueden ser, entre otros, EAP-TLS, PEAP, EAP-TTLS [35].

EAP **(Protocolo de autenticación extensible)** se emplea para el intercambio de mensajes durante el proceso de autenticación, usa la tecnología de servidor 802.1x para autenticar a los usuarios a través de un servidor **RADIUS** (Servicio de usuario con autenticación remota: Peticionario, autentificador, servidor de autentificación). Esto aporta una seguridad de fuerza industrial para su red [36].

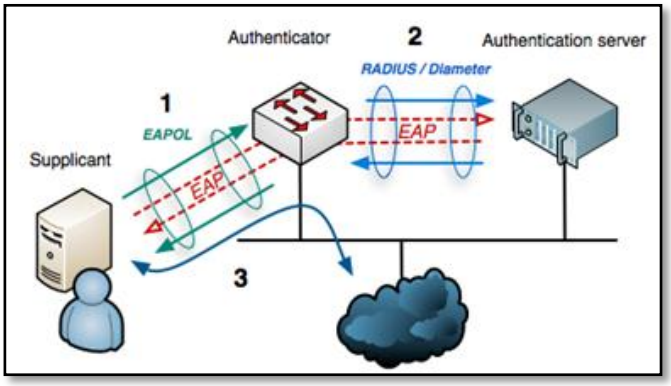


Figura. 3.12. Autenticación 802.1x [39]

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas; entre los que están [40]:

- **EAP-TLS:** Es un sistema de autenticación basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos. TLS (transport Layer Security) es el nuevo estándar que sustituye a SSL (Secure Socket Layer).

- **EAP-TTLS:** El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor.

- **PEAP:** El significado de PEAP se corresponde con Protected EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos.

A diferencia de WPA, WPA2 usa el ***Estándar avanzado de cifrado (AES)*** para el cifrado de los datos, mientras que WPA original emplea TKIP. AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de seguridad de varias agencias del gobierno federal. Además, WPA2 será compatible tanto con la versión para la empresa como con la doméstica [36].

WPA vs. WPA2

WPA2 es la versión certificada de WPA y es parte del estándar IEEE 802.11i. Existen dos cambios principales en WPA2 vs. WPA [33]:

- El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo “Counter-Mode/CBC-Mac” (CCMP), que es considerado criptográficamente seguro.

- El reemplazo del algoritmo RC4 por el “Advanced Encryption Standard (AES)” conocido también como Rijndael.

Recomendaciones

- Si se necesita confidencialidad mediante el cifrado a nivel de enlace: la mejor opción es WPA2 en modo “corporativo” (WPA2-Enterprise”).

- En caso de usarse una solución más simple como la WPA2-Personal, deben tomarse precauciones especiales al escoger una contraseña (PSK).
- El protocolo WEP y sus variantes WEP+, y WEP2, deben ser descartados.

La Figura 3.13., muestra la evolución a partir de la Autenticación WEP [26].

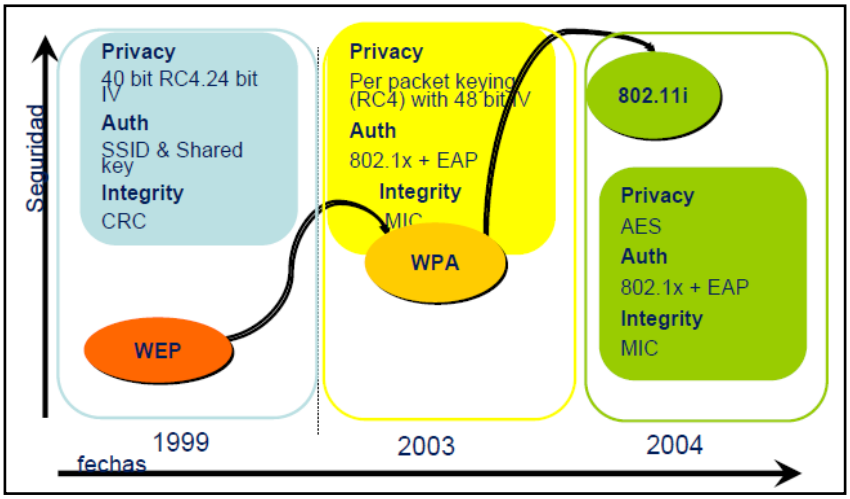


Figura. 3.13. Autenticación en WEP

3.5.2 DETECCIÓN

3.5.2.1 Tripwire, Snort

➢ **Tripwire**

Una forma de detectar ataques locales (y también de red) en su sistema es ejecutar un programa que verifique la integridad de la información almacenada en los ficheros, tal como Tripwire. El programa ***Tripwire*** ejecuta varios cheksums de todos los binarios importantes y ficheros de configuración y los compara con una base de datos con valores de referencia aceptados como buenos; de esta manera detecta cualquier cambio en los ficheros.

Se sugiere instalar Tripwire en un disquete y protegerlo físicamente; de esta forma no se puede alterar Tripwire o modificar su base de datos. Una vez que Tripwire se ha configurado, es aconsejable ejecutarlo como parte de de los deberes habituales de administración para ver si algo ha cambiado.

- **Snort**

Es un sistema para detección de amenazas para un sistema o red, monitoriza distinto tráfico que puede haber desde intrusos o diferentes tipos de ataques; es muy útil para auditar un sistema o mantener un control de éste. La idea no es la de proteger frente a posibles ataques sino dar información sobre estos.

Dentro las características más notables de Snort cabe destacar las siguientes:

- Tiene la función de sniffer para controlar el tráfico de un sistema, red o host.
- Detecta intrusiones.
- Da información sobre puertos con el fin de evitar agujeros de seguridad o anomalías en ellos.
- Tiene un sistema de firmas de ataques actualizable que funciona a partir de patrones de ataques reales.
- Dispositivo de almacenaje mediante logs sobre anomalías detectadas.
- Previene de ataques ddos, backdoors y otros sistemas intrusivos, incluso de escáneres como el conocido Nmap.
- Puede trabajar en distintos sistemas operativos como Windows, Unix y Linux.
- Uso de filtros personalizables mediante la librería libpcap, la misma utilizada por TCPDump.

3.5.2.2 Detectores de vulnerabilidades, Nessus, ISS, SATAN, NMAP

- **NMAP**: escáner para auditorías de seguridad en red. Permite escanear servicios TCP, UDP, ICMP, RPC, etc. así como el S.O de la máquina remota [41].

Soporta la mayoría de sistemas operativos GNU/Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, y más.

- **NESSUS**: Es una herramienta que detecta numerosos fallos de seguridad en base a plugins o módulos externos de pruebas que se van actualizando periódicamente.

  La última versión Nessus 3 soporta plataformas como: Red Hat Enterprise Server, Red Hat Fedora Core, SuSE Linux, Debian, FreeBSD, Solaris, Windows, y Mac OS X

- **SATAN**: Security Administrator's Tool for Analyzing Networks (Herramienta de Administrador de Seguridad para Analizar Redes); es un explorador de puerto con una interfaz de web. Puede ser configurado para hacer comprobaciones ligeras, medias o fuertes en un equipo o una red de equipos [42].

- **ISS**: Internet Security Scanner (Explorador de Seguridad de Internet); es otro explorador basado en el puerto. Es más rápido que SATAN, y por eso podría ser mejor para redes grandes. Sin embargo, SATAN tiende a proporcionar más información.

3.5.2.3 IDS - WIDS.

- **IDS**

Un Sistema de Detección de Intrusos o IDS (***Intrusion Detection System***) es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión. Un IDS escucha sigilosamente el tráfico de la red para detectar actividades anormales o sospechosas y, de este modo, detectar un intento de intrusión

Al detectar un intento de intrusión:

- ***Un IDS Pasivo*** almacena la información y manda una señal de alerta
- ***Un IDS Reactivo*** (I. Prevention S.) trata de responder reprogramando el cortafuegos o reseteando la conexión

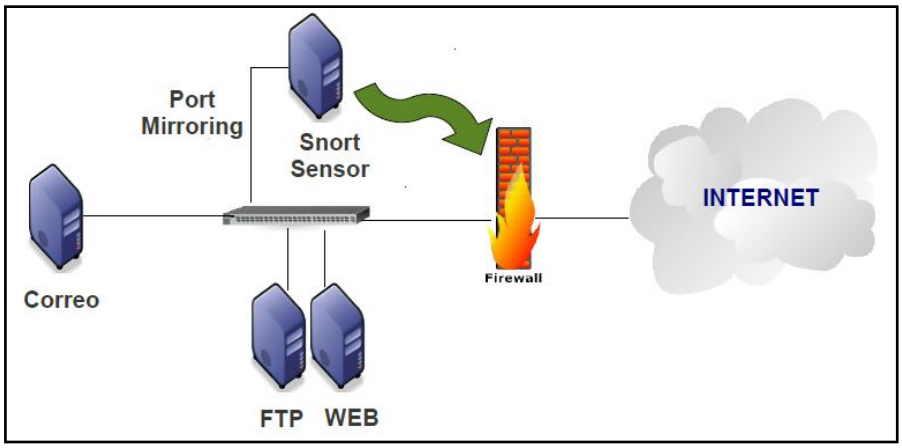


Figura. 3.14. IDS

Clasificación

- **Host - based IDS:** operan en un host para detectar actividad maliciosa en el mismo.
- **Network - based IDS:** operan sobre los flujos de información intercambiados en una red.
- **Knowledge - based IDS:** sistemas basados en Conocimiento.
- **Behavior - based IDS:** sistemas basados en Comportamiento. Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperado de un usuario en el sistema [43].

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un conjunto de actividades anómalas. Si alguien consigue entrar de forma ilegal al sistema, no actuará como un usuario comprometido; su comportamiento se alejará al de un usuario normal. Sin embargo en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Así las intrusiones pueden clasificarse en:

- **Intrusivas pero no anómalas**: denominados Falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, porque dan una falsa sensación de seguridad del sistema.
- **No intrusivas pero anómalas**: denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados.
- **No intrusiva ni anómala**: son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal.
- **Intrusiva y anómala**: se denominan Positivos Verdaderos, la actividad es intrusiva y es detectada.

Los detectores de intrusiones anómalas requieren mucho gasto computacional, ya que se siguen normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal.

Características de IDS

Cualquier sistema de detección de intrusos debería, sea cual sea el mecanismo en que esté basado, debería contar con las siguientes características:

- Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que está siendo observado. Sin embargo, no debe ser una "caja negra" (debe ser examinable desde el exterior).
- Debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.
- En relación con el punto anterior, debe ser resistente a perturbaciones. El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.
- Debe imponer mínima sobrecarga sobre el sistema. Un sistema que relentiza la máquina, simplemente no será utilizado.
- Debe observar desviaciones sobre el comportamiento estándar.

- Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.
- Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo.
- Debe ser difícil de "engañar".

Fortalezas de IDS

- Suministra información muy interesante sobre el tráfico malicioso de la red.
- Poder de reacción para prevenir el daño.
- Es una herramienta útil como arma de seguridad de la red.
- Ayuda a identificar de dónde provienen los ataques que se sufren.
- Recoge evidencias que pueden ser usadas para identificar intrusos.
- Es una "cámara" de seguridad y una "alarma" contra ladrones.
- Funciona como "disuasor de intrusos".
- Alerta al personal de seguridad de que alguien está tratando de entrar.
- Protege contra la invasión de la red.
- Suministra cierta tranquilidad.
- Es una parte de la infraestructura para la estrategia global de defensa.
- La posibilidad de detectar intrusiones desconocidas e imprevistas. Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques.
- Son menos dependientes de los mecanismos específicos de cada sistema operativo.
- Pueden ayudar a detectar ataques del tipo "abuso de privilegios" que no implica realmente ninguna vulnerabilidad de seguridad
- Menor costo de implementación y mantenimiento al ubicarse en puntos estratégicos de la red.
- Dificulta el trabajo del intruso de eliminar sus huellas.

Vulnerabilidades de IDS

- No existe un parche para la mayoría de bugs de seguridad.
- Se producen falsas alarmas.
- Se producen fallos en las alarmas.
- No es sustituto para un buen Firewall, una auditoría de seguridad regular y una fuerte y estricta política de seguridad.

Inconvenientes de IDS

- La alta tasa de falsas alarmas dado que no es posible cubrir todo el ámbito del comportamiento de un sistema de información durante la fase de aprendizaje.
- El comportamiento puede cambiar con el tiempo, haciendo necesario un re-entrenamiento periódico del perfil, lo que da lugar a la no disponibilidad del sistema o la generación de falsas alarmas adicionales.
- El sistema puede sufrir ataques durante la fase de aprendizaje, con lo que el perfil de comportamiento contendrá un comportamiento intrusivo el cual no será considerado anómalo.

➢ **WIDS**

Existen sistemas de monitorización para detectar intrusiones WiFi que son bastante útiles y fiables, las cuales se conocen como ***WIDS (wireless intrusion detection system)***. Estos programas monitorizan el espectro de radio para encontrar la presencia de elementos no autorizados, como pueden ser otros AP o herramientas especiales para vulnerar redes wireless [44].

Las funciones de este sistema de protección es comparar las direcciones MAC que va encontrando con los dispositivos WiFi autorizados que tiene registrados. Algunas herramientas pueden suplantar direcciones MAC legítimas, por lo que también revisa la firma digital del producto y las compara para saber si son fiables.

Métodos de Detección [45]

- **Contención de sesión:** cuando un WIDS identifica un STA no autorizado en la red wireless, tratará de prevenir que la STA acceda a los recursos de la Red. Esta acción se la consigue mediante la realización de un ataque de denegación de servicio sobre un AP o STA ilícito, aprovechando la debilidad de las redes WiFi en la que no se autentican las tramas de administración utilizadas para esta acción.

  Si un mensaje de desconexión es repetido continuamente, la STA ilícita no es capaz de conectarse a la red Wireless, previniendo así una intrusión.

- **WIDS Fingerprinting:** utiliza parámetros y características para la detección como:

  - ✓ *Valores característicos en las tramas*; sobre todo en el código de las tramas de des-autenticación.
  - ✓ *Tiempos de trama*; es la frecuencia (tiempo fijo o variable) con la que se envían las tramas. También se puede enviar en cierta parte del proceso de asociación/autenticación.

- **Puntos de Acceso ilícito:** dentro de los WIDS, es una de las técnicas de detección más potentes y seguras. Se determinan las MAC de los AP admitidos como legítimos en el WIDS, también se puede incluir: el canal y SSID utilizado.

  Si un sensor inalámbrico detecta un AP emitiendo cerca del AP legítimo y no está en su lista de admitidos, emitirá una alerta y puede que responda de manera activa previniendo que los usuarios se conecten a dicho AP. Sí un AP ilícito usa el mismo canal y SSID, los clientes tendrán problemas de conectividad por que los AP interferirán entre sí debido a las tramas Beacon.

3.6 MECANISMOS DE RECUPERACIÓN

Son aquellos que se aplican cuando una violación del sistema se ha detectado para retornar a su funcionamiento correcto. Ejemplos son el uso de copias de seguridad o el hardware de respaldo. Dentro de este grupo se encuentra un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema y el medio utilizado para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros elementos de nuestra red.

3.6.1 Respaldos

Los discos magnéticos fallan en ocasiones y es necesario tener cuidado para garantizar que los datos perdidos debido a esos fallos no se pierdan para siempre. Con este fin, pueden utilizarse programas del sistema para realizar una copia de seguridad de los datos del disco en otro dispositivo de almacenamiento, como por ejemplo un disquete, una cinta magnética, un disco óptico incluso otro disco duro. La recuperación de la pérdida de un archivo individual o de un disco completo puede ser entonces, simplemente, una cuestión de restaurar los datos a partir de la copia de seguridad [46].

Los respaldos pueden consistir en efectuar copias completas del contenido de los discos (flexibles o rígidos). Una técnica muy usada para asegurar la disponibilidad de los datos es realizar respaldos periódicos:

- Hacer con regularidad una o más copias de los archivos y colocarlas en lugar seguro
- Todas las actualizaciones realizadas luego del último respaldo pueden perderse

Otra técnica es pasar todas las transacciones a un archivo, copiándolas en otro disco:

- Genera una redundancia que puede ser costosa

- En caso de fallas en el disco principal, puede reconstruirse todo el trabajo perdido si el disco de reserva no se dañó también

También existe la posibilidad del respaldo incremental:

- Durante una sesión de trabajo los archivos modificados quedan marcados.
- Cuando un usuario se retira del sistema (deja de trabajar), un proceso del sistema efectúa el respaldo de los archivos marcados

3.6.2 Redundancia

La técnica más usada para enmascarar las fallas es la Redundancia. Hay tres tipos de redundancia [47]:

- ***De información***: se agrega información adicional para detectar fallas (código de Hamming, bits de paridad, etc.)

- ***De tiempo***: una acción se puede repetir si es necesario (modelo de transacciones).

- ***Física***: se adicionan equipos o procesos extras para sustituirlo por el componente que falle

3.6.3 BCP, DRP

Los principales beneficios que se obtiene de BCP/DRP son:

- Identifica de forma proactiva los impactos de un trastorno operacional.
- Proporciona una respuesta efectiva que minimiza el impacto en la organización. Mantiene la capacidad para gestionar los riesgos no asegurables.
- Fomenta el trabajo entre equipos.
- Puede mejorar la reputación y ventajas competitivas de las organizaciones en su capacidad para mantener, entregar y recuperarse de un desastre.

3.6.4 Análisis forense

El análisis forense de sistemas pretende averiguar lo ocurrido durante una intrusión. Busca dar respuesta a los interrogantes que normalmente envuelven a todo incidente: quién realizó el ataque, qué activos de información se vieron afectados y en qué grado, cuándo tuvo lugar, dónde se originó y contra qué blancos se dirigió, cómo fue llevado a cabo y por qué [48].

El análisis forense comprende dos fases: la primera, la captura de las evidencias y su protección; la segunda, el análisis de las mismas. Sin embargo, debido a que en los crímenes digitales cada vez resulta más difícil dar respuesta a los interrogantes, especialmente quién realizó el ataque, la investigación forense suele centrarse en averiguar qué fue dañado, cómo fue dañado y cómo arreglarlo.

Durante la fase de recolección de evidencias se captura todo aquello que resulte susceptible de posible análisis posterior y que pueda arrojar luz sobre detalles de muestras de un delito. El análisis de la evidencia es la fase más extensa y delicada, ya que requiere poseer conocimientos avanzados para poder interpretar las pruebas incautadas, cuyo volumen puede llegar a ser inmenso. Dependiendo de la calidad de los datos de registro de actividad se podrá realizar de forma más o menos sencilla el análisis de la evidencia. Igualmente, dependiendo de la información existente se procederá a obtener unos resultados más o menos satisfactorios.

CAPÍTULO 4

ANÁLISIS DE TRÁFICO

4.1 ESCENARIO. GENERACIÓN DE TRÁFICO. PRUEBAS

Modos de Operación de Redes Inalámbricas

El conjunto de estándares 802.11 definen dos modos fundamentales para redes inalámbricas:

- *Ad hoc*: los clientes se conectan entre sí sin ningún punto de acceso.
- *Infraestructura*: los clientes de tecnología inalámbrica se conectan a un punto de acceso. Éste es por lo general el modo predeterminado para las tarjetas 802.11b.

- ***Modo Ad Hoc***

En el modo ad hoc, los equipos clientes inalámbricos se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente. Sin embargo al permitir que los clientes inalámbricos operen en modo ad hoc, no es necesario involucrar un punto de acceso central [49].

Características [50]**:**

- Todos los nodos de una red ad hoc se pueden comunicar directamente con otros clientes.

- Cada cliente inalámbrico en una red ad hoc debería configurar su adaptador inalámbrico en modo ad hoc y usar los mismos SSID y "numero de canal" de la red.
- Una red ad hoc normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca unos de otros.
- En una red ad hoc el rendimiento es menor a medida que el número de nodos crece.
- Para conectar una red ad hoc a una red de área local (LAN) cableada o a Internet, se requiere instalar una Pasarela o Gateway especial.
- El termino latino ad hoc significa "para esto" pero se usa comúnmente para describir eventos o situaciones improvisadas y a menudo espontaneas.

En redes IEEE 802.11 el modo ad hoc se denota como ***Conjunto de Servicios Básicos Independientes*** (***IBSS*** -Independent Basic Service Set).

Tabla. 4.1. Configuración típica de una Red Ad Hoc [51]

Configuración	**Nodo 1**	**Nodo 2**
Modo	*ad hoc*	*ad hoc*
SSID	MI_SSID	MI_SSID
Canal	Debe ser convenido y conocido por todos	Debe ser convenido y conocido por todos
Dirección IP	Normalmente fija	Normalmente fija

Si un nodo está conectado a la red (Ej.: Intranet o Internet) puede extender dicha conexión a otros que se conecten a él inalámbricamente en el modo *ad hoc*, si se le configura para esta tarea.

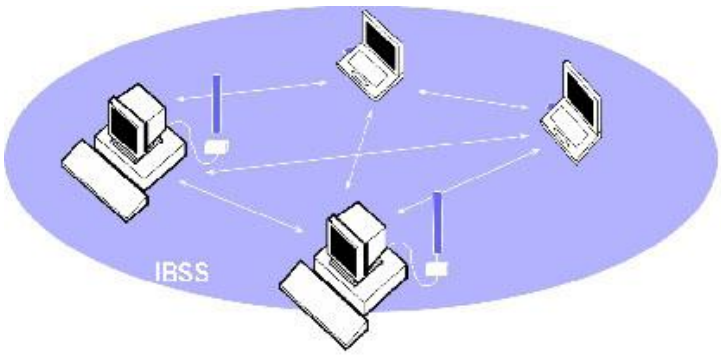


Figura. 4.1. Configuración Ad Hoc Inalámbrica

- ***Modo Infraestructura***

A diferencia del modo *ad hoc* donde no hay un elemento central, en el modo de ***Infraestructura*** hay un elemento de "coordinación" : un *punto de acceso (AP)* o *estación base*.

En redes IEEE 802.11 el modo de infraestructura es conocido como ***Conjunto de Servicios Básicos*** (***BSS*** – Basic Service Set). También se conoce como Maestro y Cliente.

Características:

- Si el AP se conecta a una red Ethernet cableada, los clientes inalámbricos pueden acceder a la red fija a través del AP.
- Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID.
- Para asegurar que se maximice la capacidad total de la red, no se debe configurar el mismo canal en todos los puntos de acceso que se encuentran en la misma área física.
- Los clientes descubrirán (a través del escaneo de la red) cual canal está usando el punto de acceso de manera que no se requiere que ellos conozcan de antemano el número de canal.

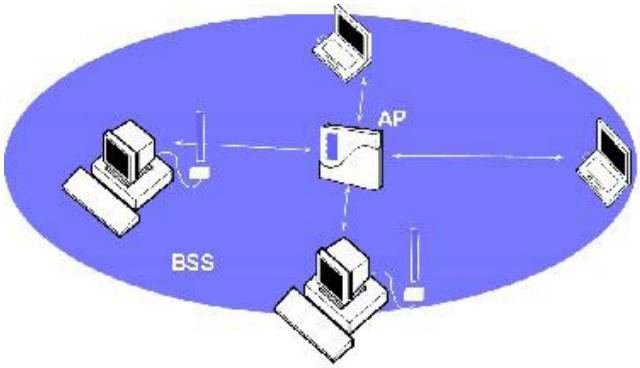


Figura. 4.2. Modo de Infraestructura [50]

A continuación se indica la configuración en modo de Infraestructura en base a diferentes topologías.

- **Estrella:** Esta topología es con mucho, la infraestructura más común en redes inalámbricas. Es la tecnología típicamente usada para un "***hotspot***" (punto de conexión a Internet), por ejemplo en aeropuertos o telecentros. Esta topología es la disposición típica de un ***WISP*** (Wireless Internet Service Provider). A menudo este tipo de redes se combina en árboles o con elementos de otras topologías.

Tabla. 4.2. Configuración en Topología Estrella [51]

Configuración	Punto de acceso / Gateway	Nodo x1
Modo	Infraestructura	Infraestructura
SSID	Defina MI_SSID	Conectar a MI_SSID
Canal	Defina el canal x	Descubre el canal
Dirección IP	Normalmente tiene un servidor DHCP (Si cuenta con características de enrutamiento)	Normalmente toma la IP que se le asigna por DHCP

- **Repetidores:** El uso de repetidores se hace necesario generalmente cuando existen obstrucciones en la línea de vista directa o hay una distancia muy larga para un solo enlace. En una red cableada, el dispositivo equivalente a un repetidor inalámbrico es un concentrador (hub). La configuración del repetidor depende de factores específicos (hardware y software) y es difícil hacer una descripción genérica para este asunto.

La unidad repetidora puede consistir en uno o dos dispositivos físicos y tener uno o dos radios. Un repetidor también puede ser visto como un cliente que cumple funciones de receptor y un punto de acceso de retransmisión. Normalmente, el SSID debería ser el mismo para las tres unidades; además del SSID, el repetidor esta enlazado a una dirección MAC [51].

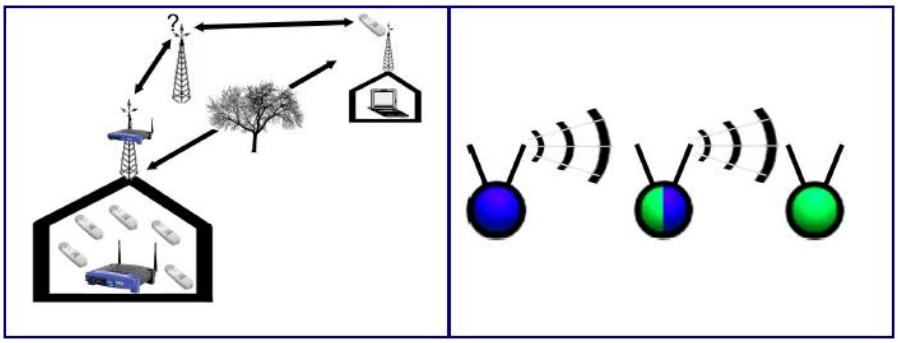


Figura. 4.3. Modo de Infraestructura Inalámbrica con Repetidores

El análisis de la captura de paquetes se realizará en base al Modo de Operación de Infraestructura Inalámbrica.

4.1.1 Captura de paquetes

Para realizar la captura de paquetes se hizo uso de software libre, teniendo en cuenta que el escenario de pruebas se basa en el comportamiento general de la red, para lo cual la captura de paquetes se hizo por medio de WIRESHARK (tramas Ethernet), y COMMVIEW FOR WIFI (tramas 802.11).

Para realizar la captura de paquetes la tarjeta de nuestra máquina debe estar en modo promiscuo. El ***modo promiscuo*** significa que las tarjetas Ethernet operan de modo que el tráfico que reciben viene marcado con su dirección MAC y aceptan el paquete, caso contrario lo rechazan. El modo promiscuo deshabilita este filtro haciendo que la tarjeta acepte todo el tráfico.

4.1.1.1 Captura de paquetes con WIRESHARK

Se verifica las redes inalámbricas disponibles alrededor de nuestro STA; en este caso se selecciona como punto de acceso (AP) de conexión a la red inalámbrica que proporciona el servicio a la ***Biblioteca Alejandro Segovia*** ubicada en ESPE Matriz – Sangolquí _ **ESPE WIFI – ZONA BIBLIO PISO 1** como se muestra a continuación:

Figura. 4.4. Redes inalámbricas disponibles

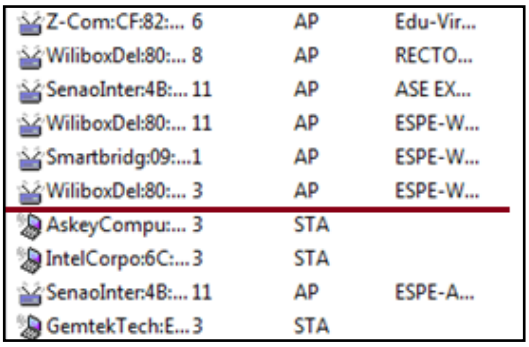


Figura. 4.5. AP seleccionado para conexión [52]

Una vea seleccionada la red inalámbrica procedemos a conectarnos a ella para posteriormente analizar el tráfico de la red por medio del software WIRESHARK que analiza cada trama de Enlace de Datos que se envía o recibe.

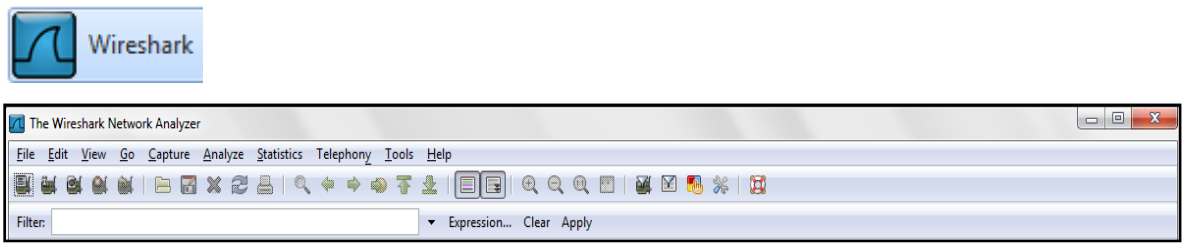


Figura. 4.6. WIRESHARK, analizador de Red [53]

Una vez conectados a la red inalámbrica seleccionada, procedemos a capturar el tráfico de dicha interfaz como se muestra en la Figura. 4.7., Figura. 4.8. [53]:

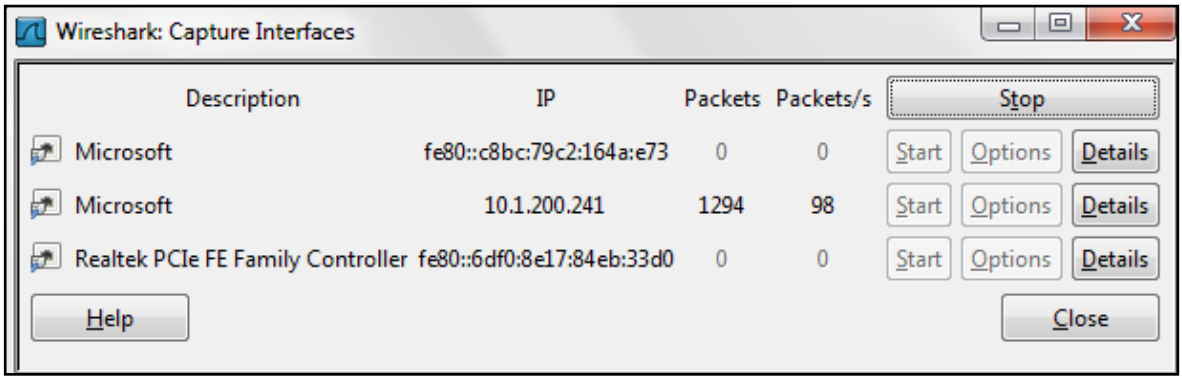


Figura. 4.7. Interfaz disponible para capturar el tráfico.

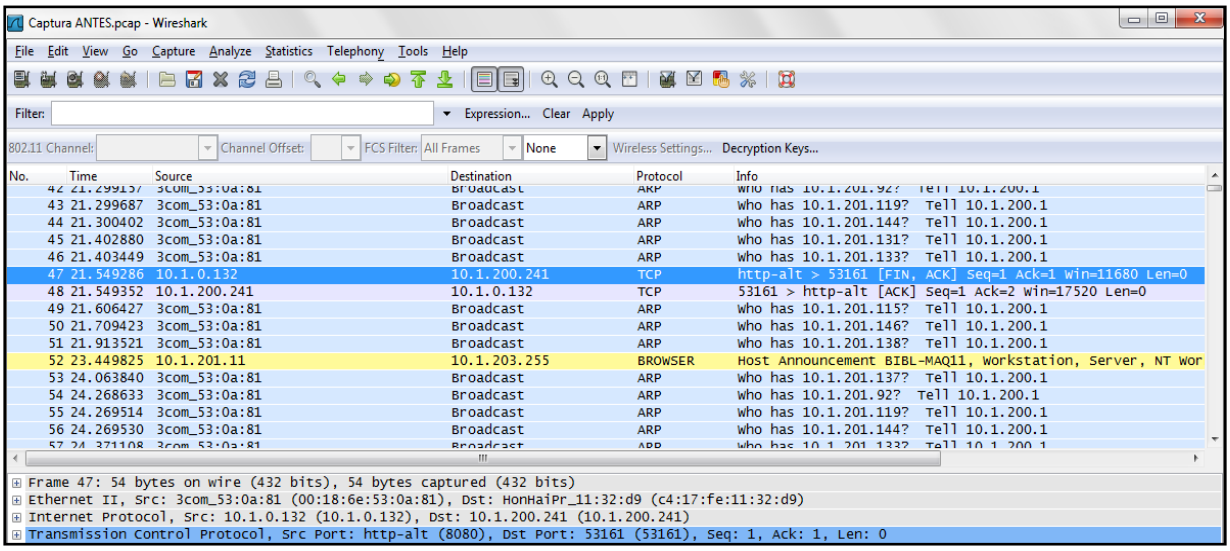


Figura. 4.8. Tráfico capturado

4.1.1.2 Captura de paquetes con COMMVIEW

Para capturar el tráfico de la red inalámbrica a la que estamos conectadas se utilizó también el software COMMVIEW FOR WIFI. Una vez se habilita la aplicación las redes que se encontraban disponibles se bloquean (Figura. 4.9) y empieza la captura de paquetes [52]. Cabe indicar que el acceso a la red inalámbrica se bloquea sólo en el STA en el que está corriendo el software, para el resto de usuarios la activación de éste programa es imperceptible, Figura. 4.10., [53].

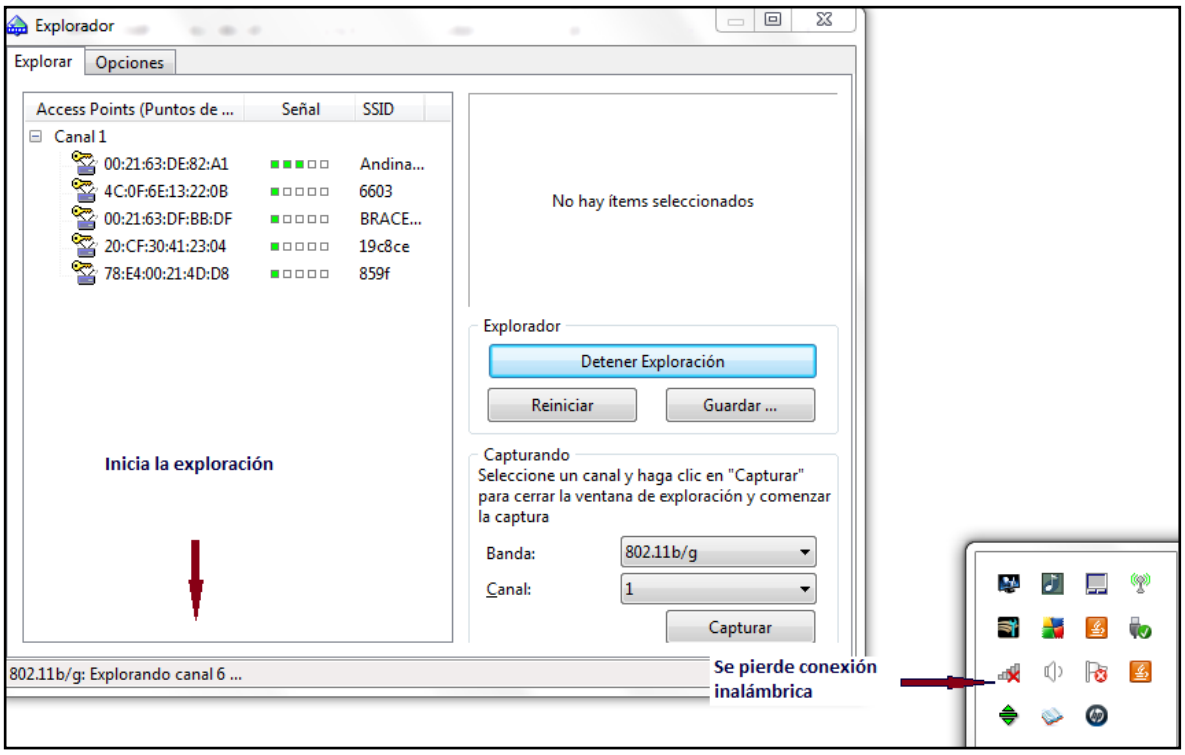


Figura. 4.9. Inicia Commview y se pierde acceso a la conexión inalámbrica

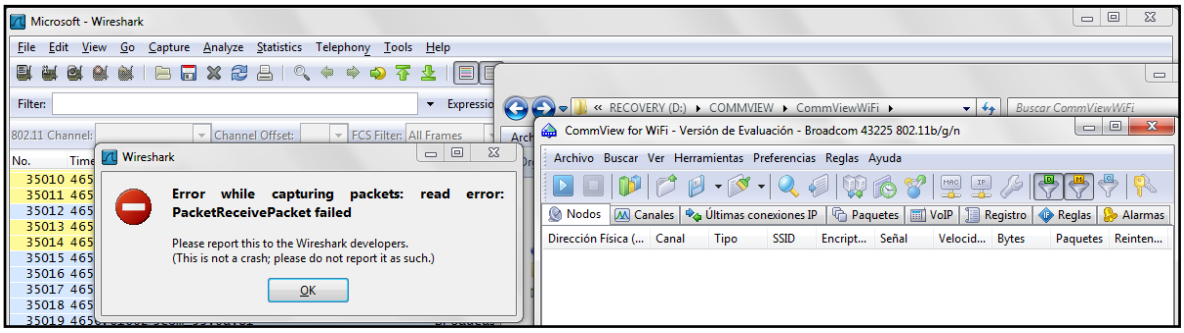


Figura. 4.10. Wireshark identifica la pérdida de conexión

Una vez que se ha ejecutado el programa se ubica la red (AP) cuyo tráfico se desea analizar y se identifica el canal por el cual se ésta transmitiendo los datos/paquetes a analizar para posteriormente proceder a capturar como se indica en la Figura 4.11., [52]:

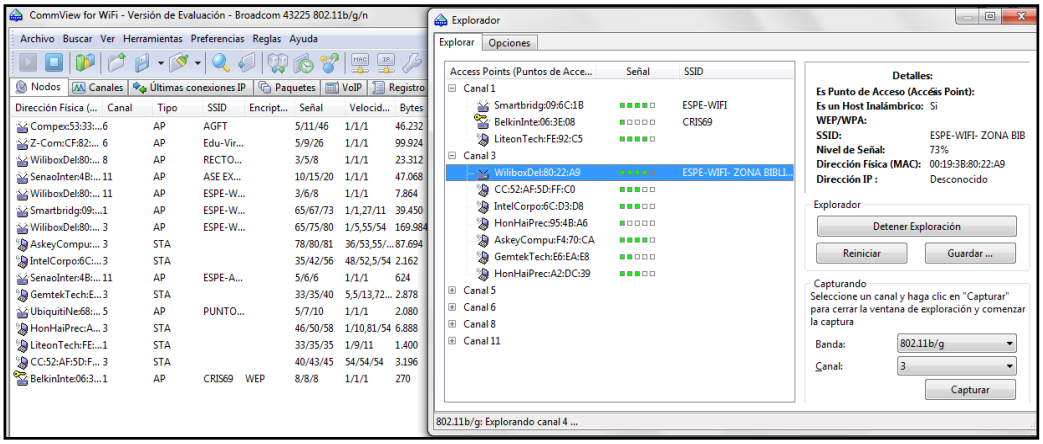


Figura. 4.11. Captura de paquetes de la red inalámbrica ESPE-WIFI-ZONA BIBLIO, canal 3

4.2 ANALISIS DE TRAMAS

4.2.1 Trama MAC

Las tramas MAC contienen la siguiente información [54]:

- ***Cabecera MAC:*** comprende los siguientes campos: control, duración, direccionamiento y control de secuencia.
- ***Cuerpo de trama de longitud variable:*** contiene información específica del tipo de trama.
- ***Secuencia Checksum (FCS):*** contiene un código de redundancia CRC de 32 bits.

Clasificación

- ***Tramas de datos***.
- ***Tramas de control:*** ejemplos de éstas tramas son los reconocimientos (ACK), tramas para multiacceso (RTS / CTS), tramas libres de contienda.

- ***Tramas de gestión:*** son servicios de distribución como: Servicios de Asociación, tramas de *Beacon* o portadora, tramas *TIM* o de tráfico pendiente en el AP.

Campos de la Trama

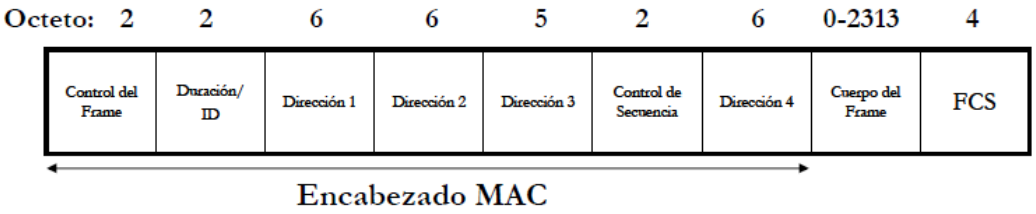


Figura. 4.12. Trama MAC genérica

Los campos que contiene ésta trama, mostrados en la Figura. 4.12 [54] son:

- ***Campo de control***
- ***Duración/ID:*** en tramas de tipo PS (Power Save) para dispositivos con limitaciones de potencia, contiene el AID (identificador) de la estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.
- ***Campo Address (1/4):*** contiene direcciones de 48 bits donde están incluidas las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y destino.
- ***Control de secuencia:*** contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.
- ***Cuerpo de la trama:*** varía según el tipo de trama que se quiere enviar.
- ***FCS:*** contiene el Checksum.

Campos de Control de Trama

Los campos de control de trama tiene el siguiente formato [54]:

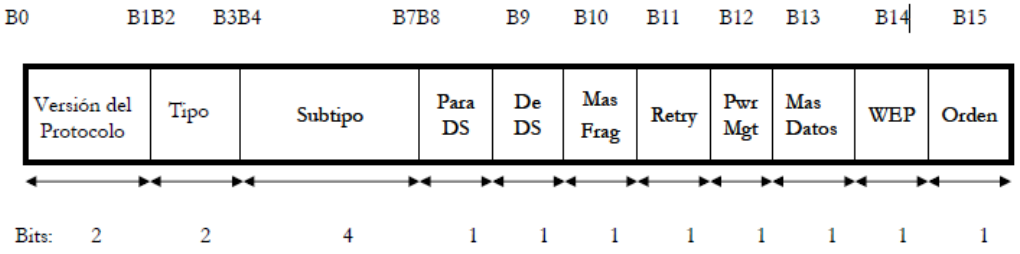


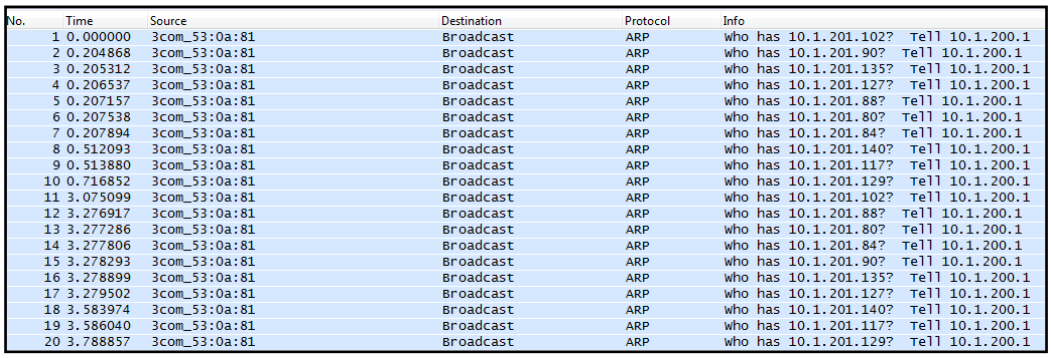
Figura. 4.13. Campos de control de trama

- ***Versión***
- ***Tipo:*** identifica si la trama es del tipo de datos, control o gestión.
- ***Subtipo:*** identifica cada uno de los tipos de tramas de cada uno de éstos tipos.
- ***To DS / From DS:*** identifica si la trama envía o recibe al sistema de distribución. En redes Ad-Hoc el To DS como el From DS están en cero (0). Otro caso contempla el envío entre dos estaciones a través del sistema de distribución, en cuyo caso tanto el To DS como el From DS se coloca en 1.
- ***Fragmentos:*** se activa si se usa fragmentación
- ***Retry:*** se activa si la trama es una retransmisión.
- ***Power Management:*** se active si la estación utiliza el modo de economía de potencia.
- ***More Data:*** se activa si la estación tiene tramas pendientes en un AP.
- ***WEP:*** se activa si se usa el mecanismo de autenticación y encriptación.
- ***Order:*** se utiliza con el servicio de ordenamiento estricto.

4.2.2 Análisis de Tramas bajo el Comportamiento General de la Red

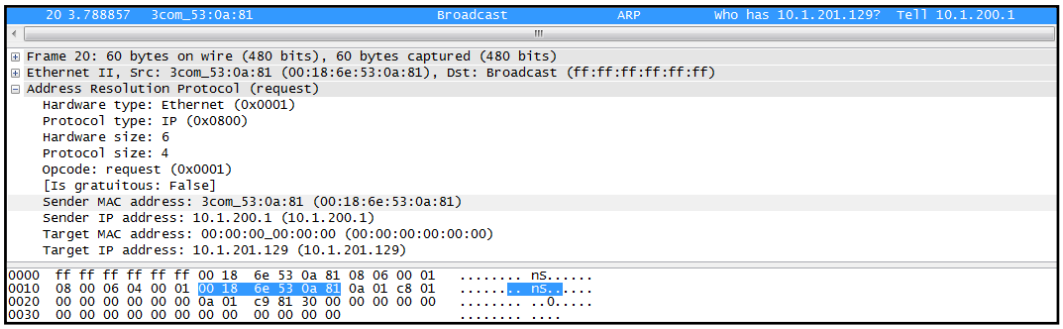
4.2.2.1 Comportamiento de la Red _ Wireshark

Iniciada la captura de paquetes, mediante el protocolo ARP, Wireshark identifica las estaciones que se encuentran alrededor y forman parte de la red Local y desean realizar la conexión, como se muestra a continuación enlas Figuras. 4.14., 4.15. [53].



No.	Time	Source	Destination	Protocol	Info
1	0.000000	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.102? Tell 10.1.200.1
2	0.204868	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.90? Tell 10.1.200.1
3	0.205312	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.135? Tell 10.1.200.1
4	0.206537	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.127? Tell 10.1.200.1
5	0.207157	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.88? Tell 10.1.200.1
6	0.207538	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.80? Tell 10.1.200.1
7	0.207894	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.84? Tell 10.1.200.1
8	0.512093	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.140? Tell 10.1.200.1
9	0.513880	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.117? Tell 10.1.200.1
10	0.716852	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.129? Tell 10.1.200.1
11	3.075099	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.102? Tell 10.1.200.1
12	3.276917	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.88? Tell 10.1.200.1
13	3.277286	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.80? Tell 10.1.200.1
14	3.277806	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.84? Tell 10.1.200.1
15	3.278293	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.90? Tell 10.1.200.1
16	3.278899	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.135? Tell 10.1.200.1
17	3.279502	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.127? Tell 10.1.200.1
18	3.583974	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.140? Tell 10.1.200.1
19	3.586040	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.117? Tell 10.1.200.1
20	3.788857	3com_53:0a:81	Broadcast	ARP	Who has 10.1.201.129? Tell 10.1.200.1

Figura. 4.14. Peticiones ARP



```
20 3.788857  3com_53:0a:81                Broadcast          ARP        Who has 10.1.201.129?  Tell 10.1.200.1
Frame 20: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: 3com_53:0a:81 (00:18:6e:53:0a:81), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
   Hardware type: Ethernet (0x0001)
   Protocol type: IP (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (0x0001)
   [Is gratuitous: False]
   Sender MAC address: 3com_53:0a:81 (00:18:6e:53:0a:81)
   Sender IP address: 10.1.200.1 (10.1.200.1)
   Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
   Target IP address: 10.1.201.129 (10.1.201.129)
0000  ff ff ff ff ff ff 00 18  6e 53 0a 81 08 06 00 01   ........ nS......
0010  08 00 06 04 00 01 00 18  6e 53 0a 81 0a 01 c8 01   ........ nS......
0020  00 00 00 00 00 00 0a 01  c9 81 30 00 00 00 00 00   ........ ..0.....
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Figura. 4.15. Trama ARP Request

En donde:

- Hardware type: medio sobre el cual se trabaja, 1 corresponde al valor asignado al medio, en esta caso: Ethernet.
- Protocol type: tipo de protocolo que es mapeado, IP toma el valor 0x0800.
- Hardware size: Tamaño de dirección de Hardware.
- Protocol size: Tamaño de dirección de protocolo (IP).

- Opcode: Especifica la operación, es decir los valores que puede tomar el campo ARP: request (1), reply (2), RARP request (3) , RARP reply (4).
- Sender MAC: Dirección MAC Origen.
- Sender IP: Dirección IP Origen.
- Target MAC: Dirección MAC destino.
- Target IP: Dirección IP Destino.
- Tipo Trama: Este campo especifica cual es el contenido del resto del paquete, cuando este valor es de 0x0806 nos indica que estamos ante un paquete ARP.

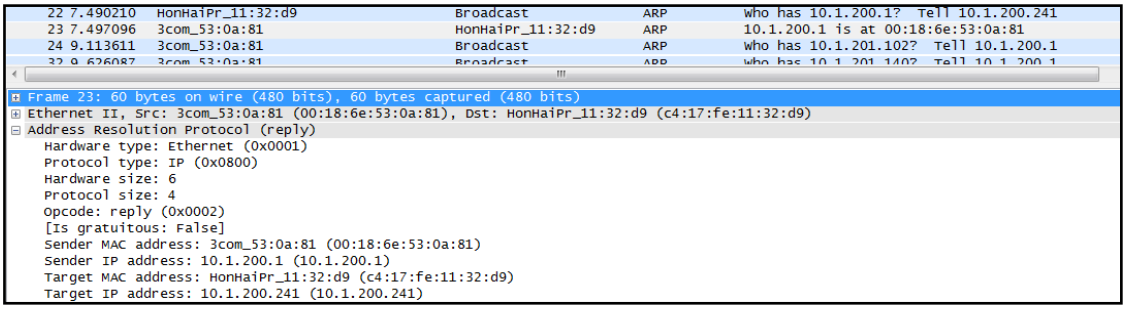


Figura. 4.16. Trama ARP Reply [53]

Como se puede observar, la mayoría de peticiones ARP de los paquetes capturados provienen de la siguiente dirección **MAC**: **00:18:6e:53:0a:81**, cuya dirección **IP** es: **10.1.200.1**.Por otra parte, en la trama ARP Reply se puede observar que la dirección MAC asignada a nuestra STA es: **MAC: c4:17:fe:11:32:d9,** cuya dirección **IP** es: **10.1.200.241**.

Cada una de las tramas capturadas, sean estas ARP, DNS, DHCP, etc., también contiene información de la Capa de Enlace de Datos. Se procede a analizar los datagramas, a continuación se muestra la estructura la trama Ethernet.

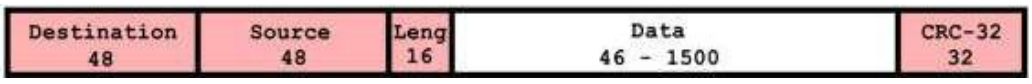


Figura. 4.17. Trama Ethernet

En Ethernet II se muestra la cabecera ***Ethernet II*** que a su vez pertenece a la ***capa de enlace de datos***: **0000 c4 17 fe 11 32 d9 00 18 6e 53 0a 81 08 00**

Parte de la cabecera de la trama Ethernet II es:

Destino, 6 bytes: MAC destino
Origen, 6 bytes: MAC origen
Tipo, 2 bytes 08 00: protocolo que viaja en la parte de datos de la trama en este caso IP. 0×0800.

Dentro de Ethernet II el campo ***Type*** nos informa cual es el tipo de protocolo que está ocupando el formato de la trama, es decir diferencia los distintos tipos de protocolos de capas superiores que puedan ocupar Ethernet, como: ARP, IP, etc.

En Wireshark se observa la siguiente información, Figura. 4,18 [53]:

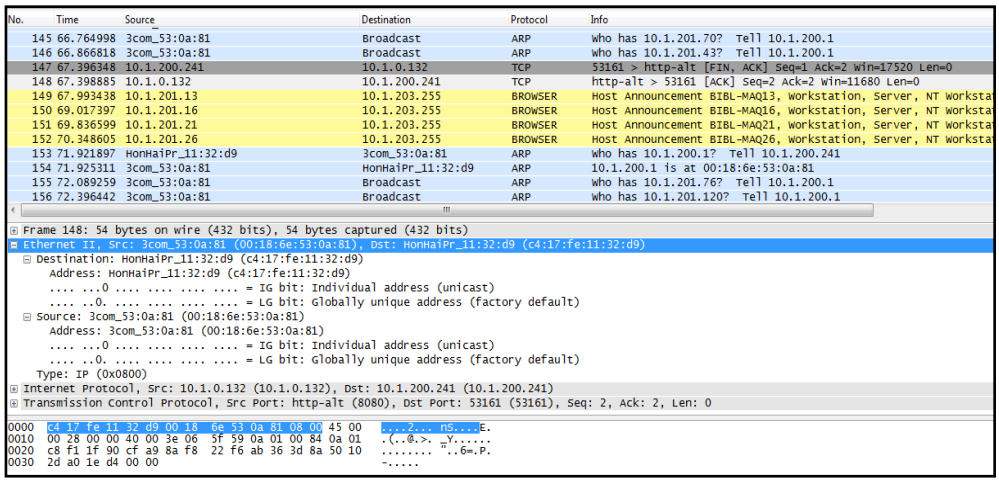


Figura. 4.18. Trama capturada con Wireshark

A partir de la información proporcionada por las peticiones ARP, podemos determinar cuáles son las MAC de origen y destino así como también la dirección IP asignadas a las diferentes estaciones que forman parte de la Red LAN Inalámbrica.

Una vez identificadas las direcciones MAC e IP de cada estación, y haciendo uso de la información proporcionada del tráfico capturado por Wiresark podemos conocer a qué tipo de información está accediendo cada usuario de la Red (estación) y determinar si con ésta información se puede o no causar o realizar

algún tipo de ataque que afecte el correcto funcionamiento de la Red. Como se puede observar las estaciones forman parte de la Red 10.1.200.x

Tabla. 4.3. Direcciones MAC que forman parte de las tramas ARP capturadas _ Wireshark [53]

Encabezado			
Encabezado MAC		Encabezado IP	
MAC Destino	MAC Origen	IP Destino	IP Origen
00:00:00:00:00:00	00:18:6e:53:0a:81	10.1.200.29	10.1.200.1
00:00:00:00:00:00	1c:4b:d6:c5:f5:56	169.254.80.248	0.0.0.0
00:00:00:00:00:00	00:08:a1:96:30:fb	10.1.201.13	10.1.200.2
00:00:00:00:00:00	e8:39:df:25:af:71	10.1.200.1	10.1.200.27
00:00:00:00:00:00	00:23:14:6c:d3:d8	10.1.200.1	10.1.200.98
00:00:00:00:00:00	f0:7b:cb:95:4b:a6	10.1.200.1	10.1.200.17
00:00:00:00:00:00	c4:17:fe:11:32:d9	10.1.200.1	10.1.200.241
00:00:00:00:00:00	f0:7b:cb:95:4b:a6	10.1.200.1	10.1.200.17
00:00:00:00:00:00	cc:52:af:5d:ff:c0	10.1.200.1	10.1.200.20
00:00:00:00:00:00	5c:59:48:ba:38:6a	10.1.200.1	10.1.200.31
00:00:00:00:00:00	00:23:15:4f:03:74	10.1.200.1	10.1.200.30
00:00:00:00:00:00	4c:ed:de:f4:70:ca	10.1.200.1	10.1.200.28
00:00:00:00:00:00	00:26:c7:b9:4f:7a	10.1.200.98	10.1.200.24
00:00:00:00:00:00	00:21:00:e6:ea:e8	10.1.200.1	10.1.200.33
00:00:00:00:00:00	78:e4:00:ab:6d:ea	10.1.200.1	10.1.201.212
00:00:00:00:00:00	c8:bc:c8:db:b2:50	10.1.200.1	10.1.200.25

También se visualiza el tipo de información a la que acceden los usuarios por medio de otros protocolos como: Browser, DHCP, DNS, HTTP, ICMP, IGMP, LLMNR, NBNS, SSDP, TCP, TLS, UDP.

Para el protocolo BROWSER, Figura. 4.19., se tiene la siguiente información proporcionada por Whireshark [53]:

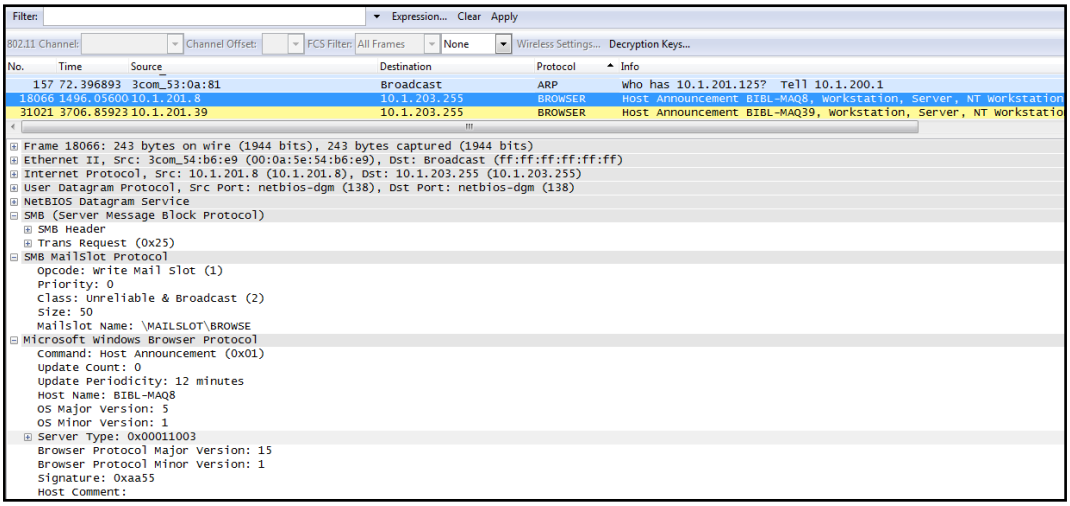


Figura. 4.19. Trama capturada, Protocolo BROWSER

BROWSER es un protocolo desarrollado por Microsoft para su sistema operativo Windows, este protocolo es de uso privativo y no tiene nada que ver con Internet o HTTP.

El ***Browser Protocol*** registra los nombres ***SMB*** (CIFS) o de ***NetBIOS*** de una red, los almacena y los comparte para los demás nodos de la red. Todos estos datos son enviados por parte del computador cliente, el servidor solo registra lo que lee en el campo del protocolo.

El ***servidor*** es un campo conocido como Server Type, en donde se tiene 8 grupos de 4 bits con los que podemos identificar que rol tiene un host en una red, cabe indicar que esto SOLO aplica para los host que usen un sistema operativo que tenga la característica de MailSlot en SMB, principal y casi únicamente Windows.

La información que proporciona éste protocolo es conocer si un host es una ***estación de trabajo*** o es un ***servidor***; es decir se puede conocer si se trata de un equipo en la red, con sistema operativo Windows, que puede tener una impresora conectada y compartida. Con ésta información es posible realizar un ataque.

Tabla. 4.4. Tramas BROWSER capturadas [53]

BROWSER						
Name	**MAC Origen**	**IP Origen**	**IP Destino**	**Estación**	**Servidor**	**Domain Enum**
BIBL - MAQ8	00:0a:5e:54:b6:e9	10.1.201.8	10.1.203.255	X	X	NO
BIBL - MAQ39	00:0a:5e:4d:9e:d4	10.1.201.39	10.1.203.255	X	X	NO
ESPE	00:08:a1:96:30:fb	10.1.200.2	10.1.203.255	…	…	SI
BIBL - MAQ24	00:01:03:e7:d3:ec	10.1.201.24	10.1.203.255	X	X	NO
ESPE	00:0a:5e:51:0b:4d	10.1.201.32	10.1.203.255	…	…	SI
CIRCULACION1-PC	00:21:97:22:5e:2a	10.1.200.156	10.1.203.255	X	X	NO
USUARIO - VAIO	00:26:c7:b9:4f:7a	10.1.200.24	10.1.202.255	X	X	NO
BIBL - MAQ30	00:0a:5e:4d:9e:9d	10.1.201.30	10.1.203.255	X	X	NO
WORKGROUP	00:21:97:22:5e:2a	10.1.200.156	10.1.203.255	…	…	SI
BIBL - MAQ33	00:08:a1:7d:d6:54	10.1.201.33	10.1.203.255	X	X	NO
BIBL - MAQ13	00:0a:5e:4d:9c:08	10.1.201.13	10.1.203.255	X	X	NO
USER-VAIO	00:23:14:6c:d3:d8	10.1.200.98	10.1.203.255	X	X	NO
BIBLIOTECA	00:0a:5e:4d:99:fa	10.1.200.15	10.1.203.255	…	…	SI
USUARIO - PC	00:1f:e2:a2:dc:39	10.1.200.55	10.1.203.255	X	X	NO
ERO - PC	00:21:00:e6:ea:e8	10.1.200.33	10.1.203.255	X	X	NO

Como parte de ésta información se visualiza que los siguientes Host Announcement actúan como estación, servidor y equipo de red; en este caso una impresora:

- **USUARIO – VAIO**
- **USER – VAIO**
- **ERO – PC**

4.2.2.2 Comportamiento de la Red _ Commview

Al hacer uso de Commview se observa que el comportamiento de nuestro STA varía respecto al comportamiento que tenía el STA mientras se hacía uso de Wireshark. Es decir, al ejecutar Commview el STA deja de formar parte de la red WLAN a la que nos conectamos, en este caso, nuestra estación hace el papel de Man in The Middle _ ESCUCHA entre las máquinas que forman parte de la LAN Inalámbrica.

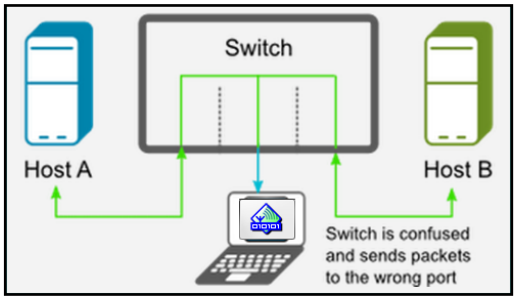


Figura. 4.20. Man in the Middle

Previo a seleccionar el canal del cual se va a capturar los paquetes, se realiza un barrido de todos la STA y AP que se encuentran disponibles alrededor de nuestra STA. Figura. 4.21. [52].

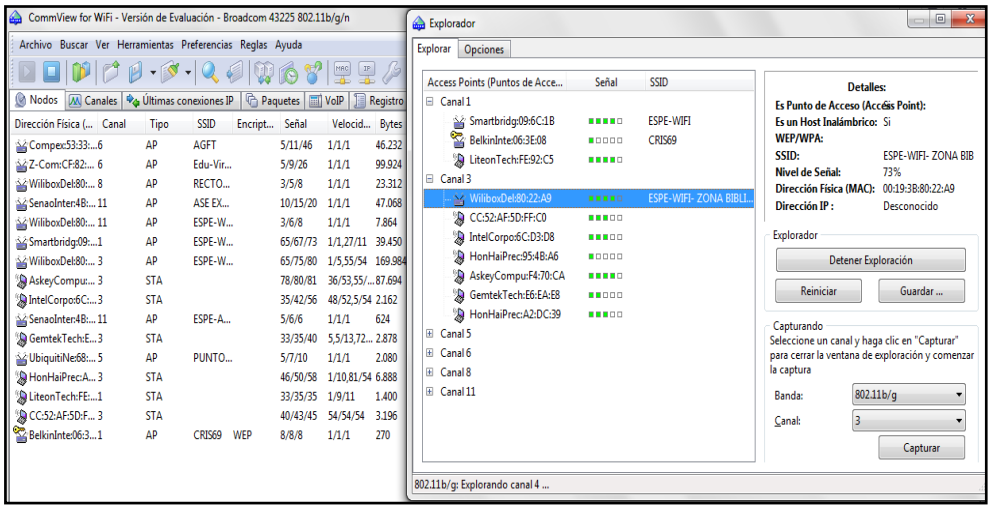


Figura. 4.21. STA y AP disponibles. Selección del canal del cual se capturará los paquetes

Una vez se seleccione el canal a analizar, se procede a capturar los paquetes que atraviesen o circulen por dicho canal como se muestra a continuación en la Figura. 4.22. COMMVIEW [52] muestra que a partir del paquete 11327 los paquetes capturados corresponden sólo al canal 3.

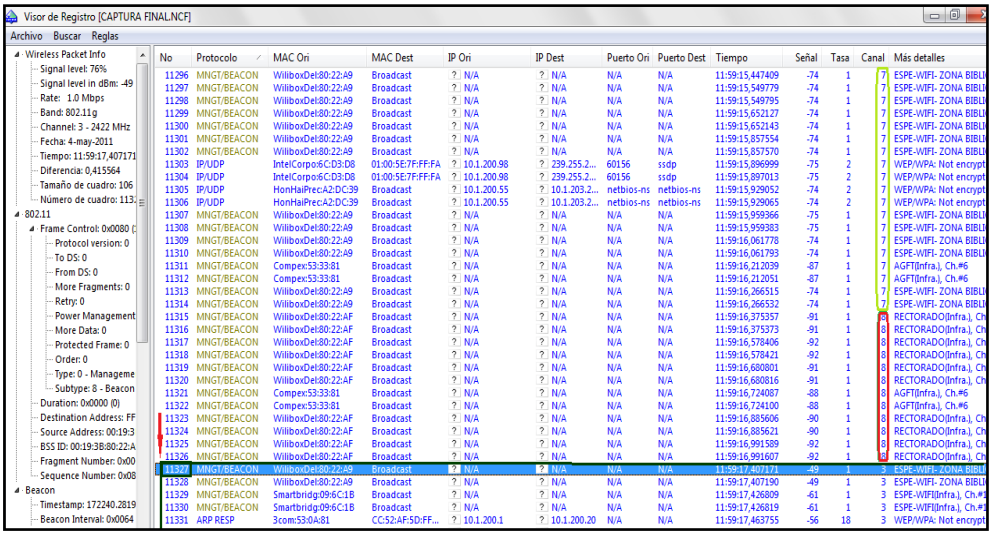


Figura. 4.22. Captura de paquetes del canal 3

Para el presente estudio analizaremos los paquetes capturados en el canal 3, en particular los paquetes que corresponden al AP cuyo **SSID** (nombre) es: ***ESPE-WIFI- ZONA BIBLIO PISO 1*** y su **BSSID** (MAC) es: **00:19:3B:80:22:A9.**

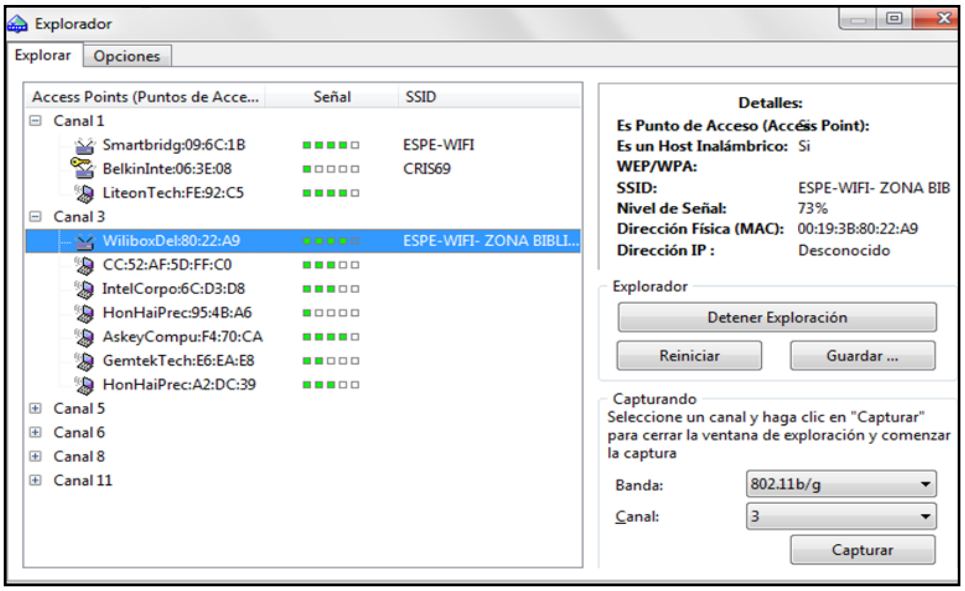


Figura. 4.23. MAC&SSID del AP *ESPE-WIFI- ZONA BIBLIO PISO 1* [52]

Como parte de la información que nos proporciona un AP se tiene:

- *Un nombre* al que llamamos SSID (o essid)
- *Una Dirección MAC* que llamamos BSSID
- *Un modo de distribución*: Infraestructura, Repetidor, Cliente y algún otro más.
- *Seguridad y/o cifrado*: WEP, WAP, WPA2, sin seguridad (OPEN)
- *Clientes*: Las estaciones inalámbricas que se conectan a ellos
- *Enrutamiento*: Capa2 y también los hay de Capa3 (no todos)
- Una *fuerza de la señal* aplicada a cada paquete
- Un *alcance* que depende de factores como la antena, entorno, obstáculos, etc.

Adicional a lo manifestado anteriormente, un AP, envía y recibe:

- *Tramas de Administración:* Beacons, Probes y Request
- *Tramas de Datos:* Cifrados o en "texto plano"
- *Tramas de Control:* RTS, ACK's y CTS

De acuerdo a lo anteriormente expuesto, la información obtenida del AP que analizaremos es:

- *SSID:* **ESPE-WIFI- ZONA BIBLIO PISO 1**
- *BSSID:* **00:19:3B:80:22:A9**
- *Modo de distribución*: **Infraestructura**
- *Seguridad y/o cifrado*: **Sin seguridad (OPEN)**
- *Clientes*: Las estaciones inalámbricas que se conectan a ellos. Varios.
- *Enrutamiento*: Capa2 / Capa3
- *Fuerza de la señal* varía de acuerdo al paquete.

A continuación se muestra la información y análisis de las tramas de Administración, Datos, Control y otras capturadas por medio de COMMVIEW.

TRAMAS DE ADMINISTRACION:

En los paquetes de administración capturados se tiene como información principal obtenida el tipo de trama; es decir si es: Beacon, Probe Request o Response, de Autenticación, Desautenticación, Asociación, Reasociación donde:

- ***BEACON*:** Nos proporciona como información el SSID, el canal actual, tasa de transmisión soportada, otros.

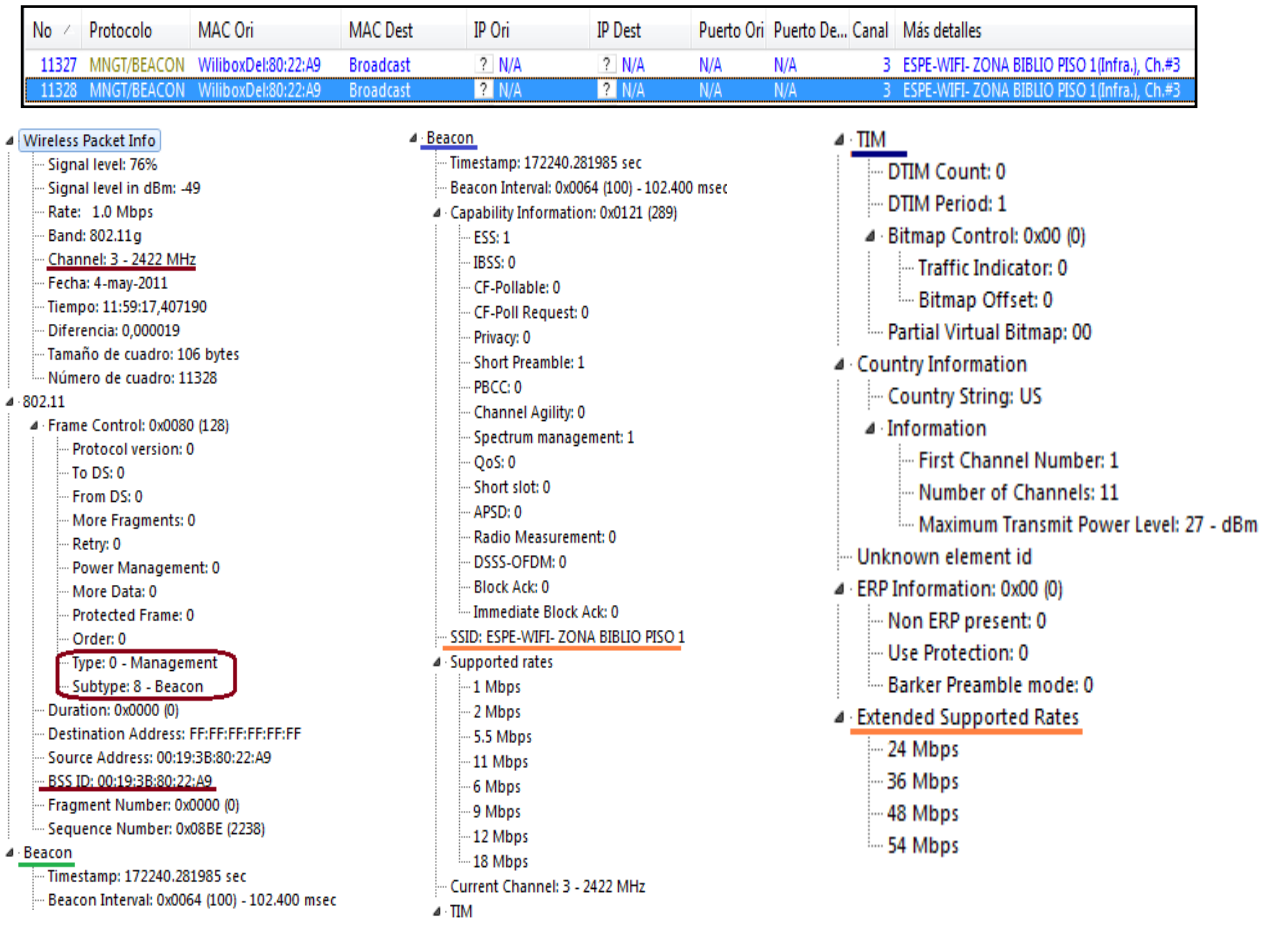


Figura. 4.24. Trama de Administración: Beacon

Análisis

Como se puede observar en la trama capturada, dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa →**To DS**: 0 / **From DS**: 0, de **AP a STA**

- Trama: ***Administración,*** y de
- Subtipo: ***8 – Beacon***, donde 8 →***1000*** que significa ***señalización.***
- BSSID: **00:19:3B:80:22:A9**

BEACON [52]

- Intervalo de señalización: 0x0064 (100) - 102.400 msec
- SSID: **ESPE-WIFI- ZONA BIBLIO PISO 1**
- Tasa de transmisión soportada: desde 1 Mbps hasta 18 Mbps
- TIM: identifica una estación por el ID de asociación que el AP le asignó durante el proceso de asociación, en este caso: *DTIM Count:0 / DTIM Period:1*

Otro SSID que forma parte del canal 3 es ***ESPE-WIFI (Infra)*** cuyos paquetes han sido capturados, se observa que el AP le asignó un TIM con los siguientes valores: *DTIM Count:0 / DTIM Period:2 y DTIM Count:1 / DTIM Period:2*, Figura. 4.25. [52]

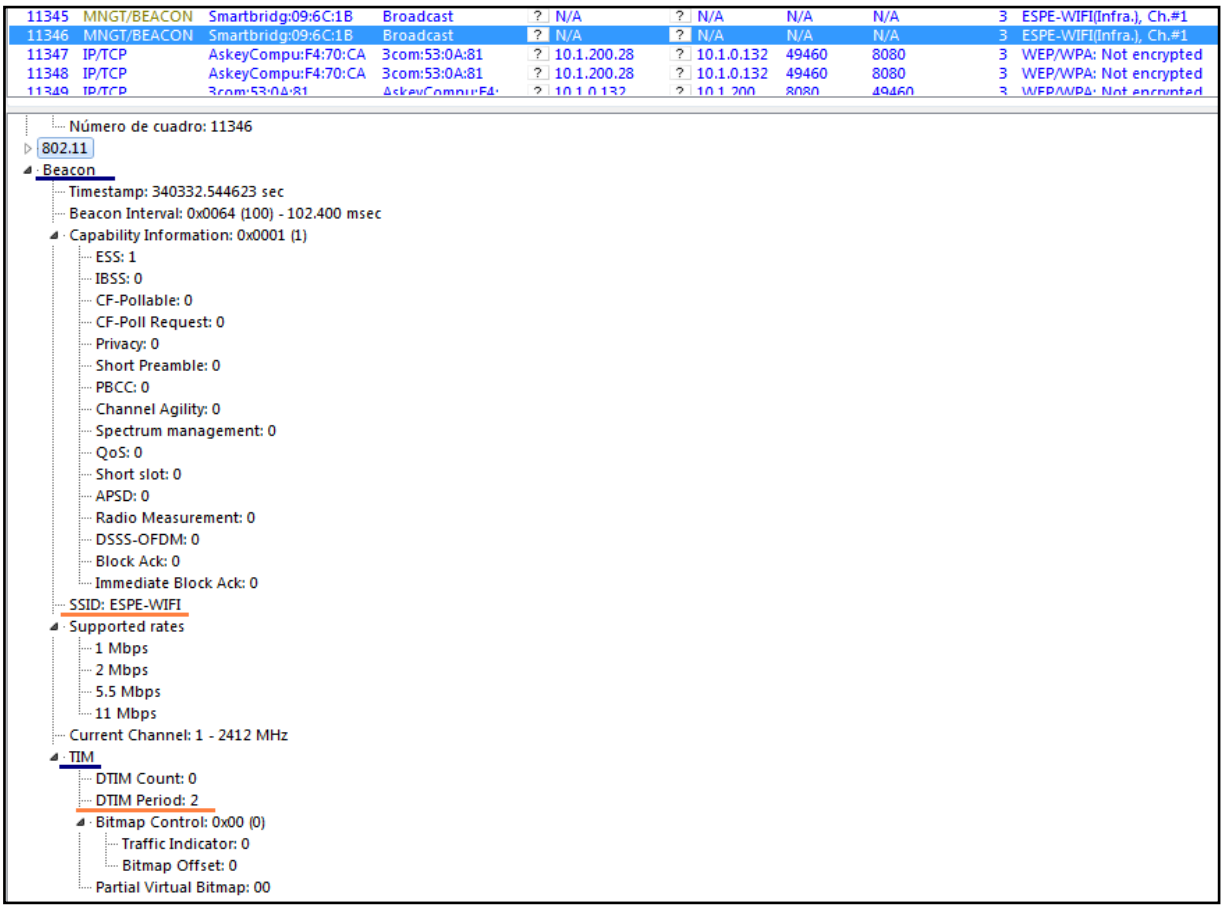


Figura. 4.25. Valores de TIM asignado a SSID ESPE - WIFI

- ***PROBE*:** Es un intercambio de mensajes que típicamente ocurre entre el AP y las estaciones, los más habituales son: Request y Response.

Request: Solicitud de sondeo

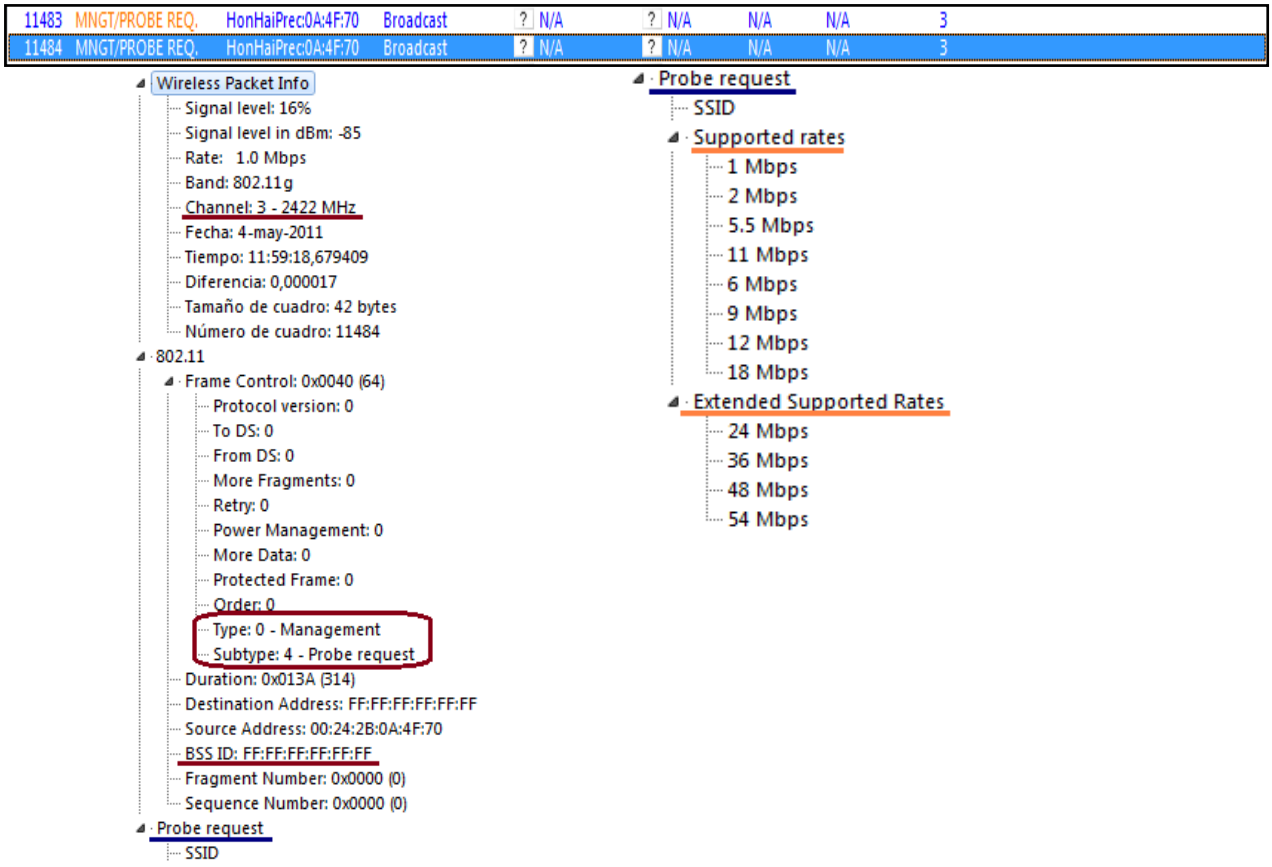


Figura. 4.26. Trama de Administración: Probe Request

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa →**To DS**: 0 / **From DS**: 0, de **STA a AP.**
- Trama: ***Administración***
- Subtipo: ***4-Probe Request***, donde 4 →***0100***, significa ***solicitud de sondeo.***
- BSSID: **FF:FF:FF:FF:FF:FF**

PROBE REQUEST [52]

- SSID: No asignado.
- Tasa de transmisión soportada: desde 1 Mbps hasta 18 Mbps
- Tasa de transmisión soportada Extendida: desde 24 Mbps hasta 54 Mbps.

El STA con MAC: **00:24:2B:0A:4F:70** está solicitando información de nuestro AP analizado. Como se puede observar en la trama capturada la dirección de destino es **FF:FF:FF:FF:FF:FF** que es cuando la NIC de la STA está usando de manera activa su scánner para determinar que AP's están dentro del posible rango de *Asociación.*

Response: Respuesta de sondeo [52]

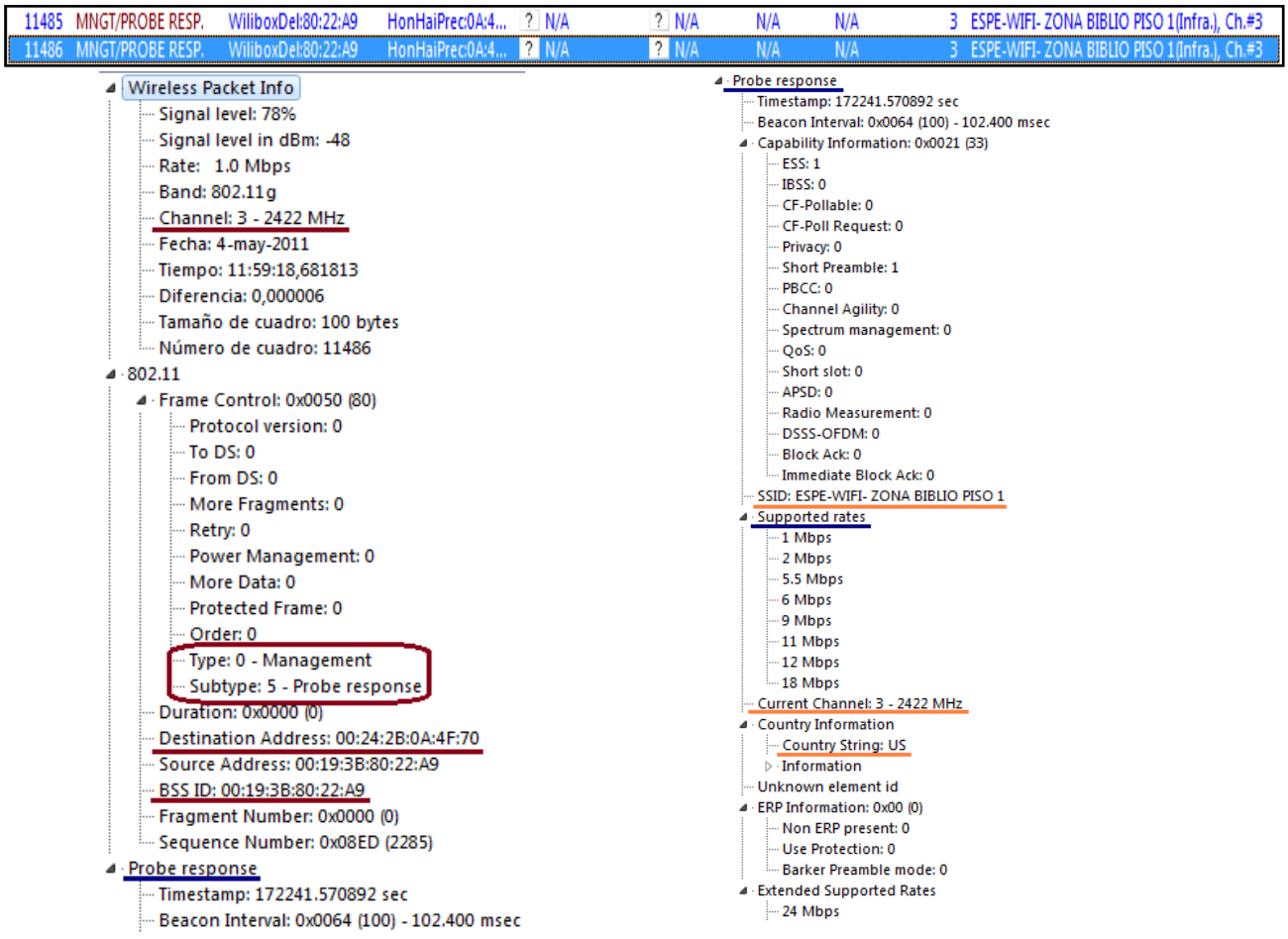


Figura. 4.27. Trama de Administración: Probe Response

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa →**To DS**: 0 / **From DS**: 0, de **AP a STA.**
- Trama ***Administración***
- Subtipo: ***5-Probe Response***, donde 5→***0101*** significa ***respuesta de sondeo.***
- BSSID: **00:19:3B:80:22:A9**

PROBE RESPONSE

- SSID: **ESPE-WIFI- ZONA BIBLIO PISO 1**
- Tasa de transmisión soportada: desde 1 Mbps hasta 18 Mbps
- Tasa de transmisión soportada Extendida: desde 24 Mbps hasta 54 Mbps.

En esta caso, nuestro AP asignado con MAC **00:19:3B:80:22:A9** está entregando (respondiendo) la información qué solicitó el STA con MAC **00:24:2B:0A:4F:70** informándole sobre su SSID, las tasas de transmisión soportadas, el canal y frecuencia en la que está trabajando

- ***AUTENTICACIÓN*:** Implica una serie de intercambios entre las STA y el AP. La autenticación puede variar debido a que pueden existir otros sistemas de autenticación (tipo RADIUS) que también pueden estar presentes.

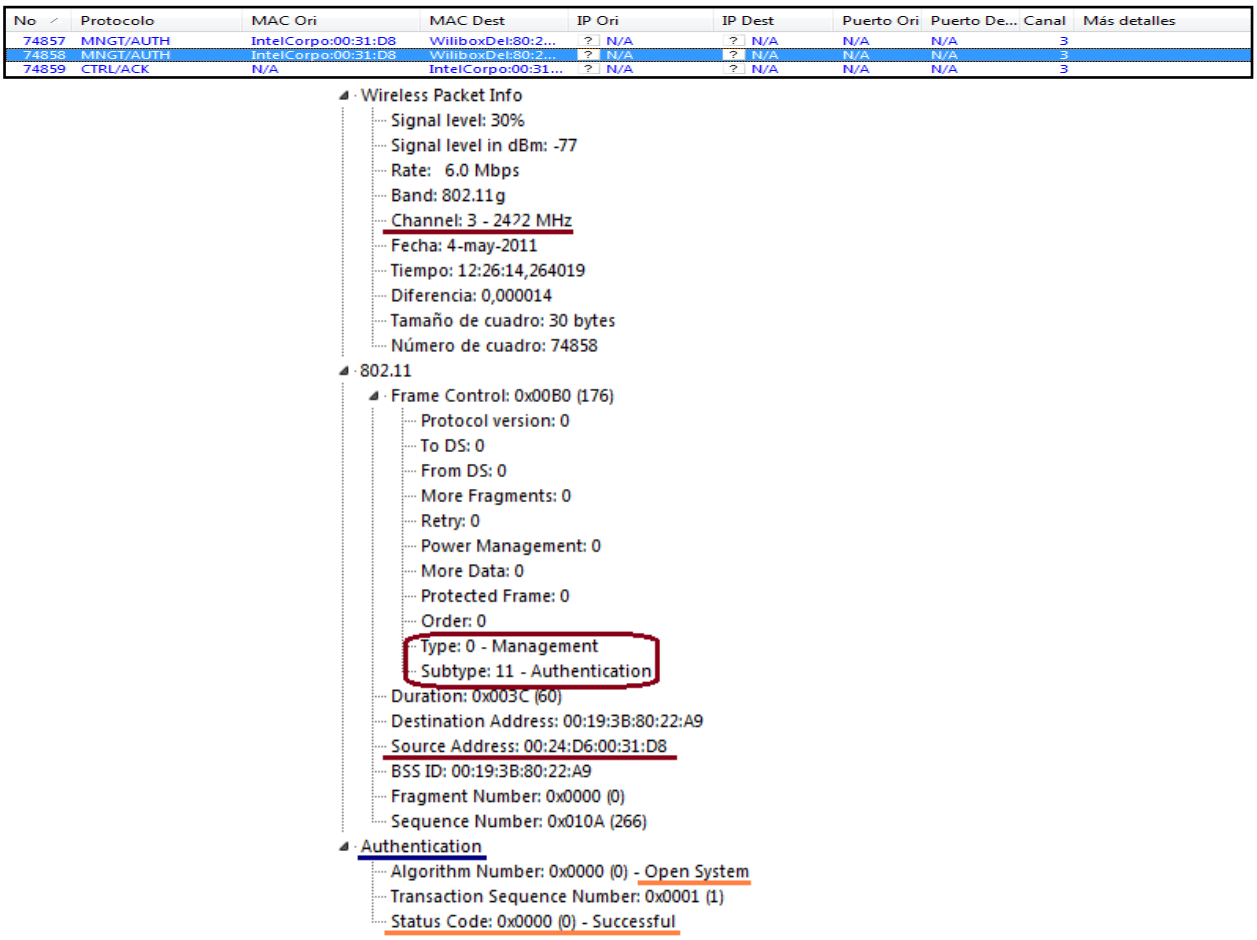


Figura. 4.28. Trama de Administración: Authentication _ STA-AP

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa →**To DS**: 0 / **From DS**: 0, de **STA a AP.**
- Trama: ***Administración***
- Subtipo: ***11-Authentication***, donde 11 →***1011*** es ***Autenticación.***
- BSSID: **00:19:3B:80:22:A9**

AUTHENTICATION

- Sistema abierto
- Exitoso.

El STA con MAC: **00:24:D6:00:31:D8** está solicitando autenticarse con nuestro AP cuya MAC **00:19:3B:80:22:A9.** La siguiente trama de Autenticación es la que realiza nuestro AP analizado con MAC **00:19:3B:80:22:A9** hacia el STA con MAC: **00:24:D6:00:31:D8** que solicitó la autenticación, Figura. 4.29 [52].

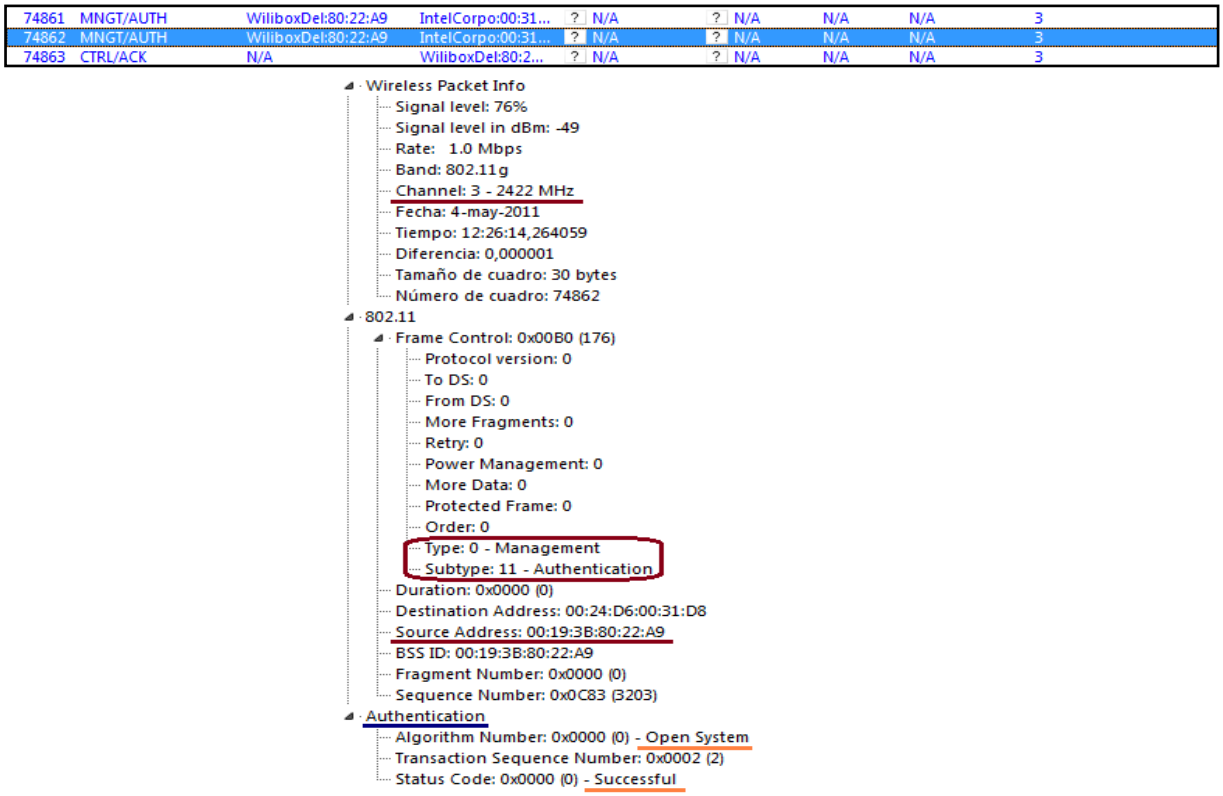


Figura. 4.29. Trama de Administración: Authentication _ AP-STA

- ***ASOCIACIÓN*****:** Es un intercambio de tramas de Administración con Subtipo ***Request / Response*** una vez que la autenticación resultó correcta.

Request: incluye información acerca de las capacidades del dispositivo, tasas de transmisión, QoS, ESSID, y razones y estados de la solicitud de la asociación [52]

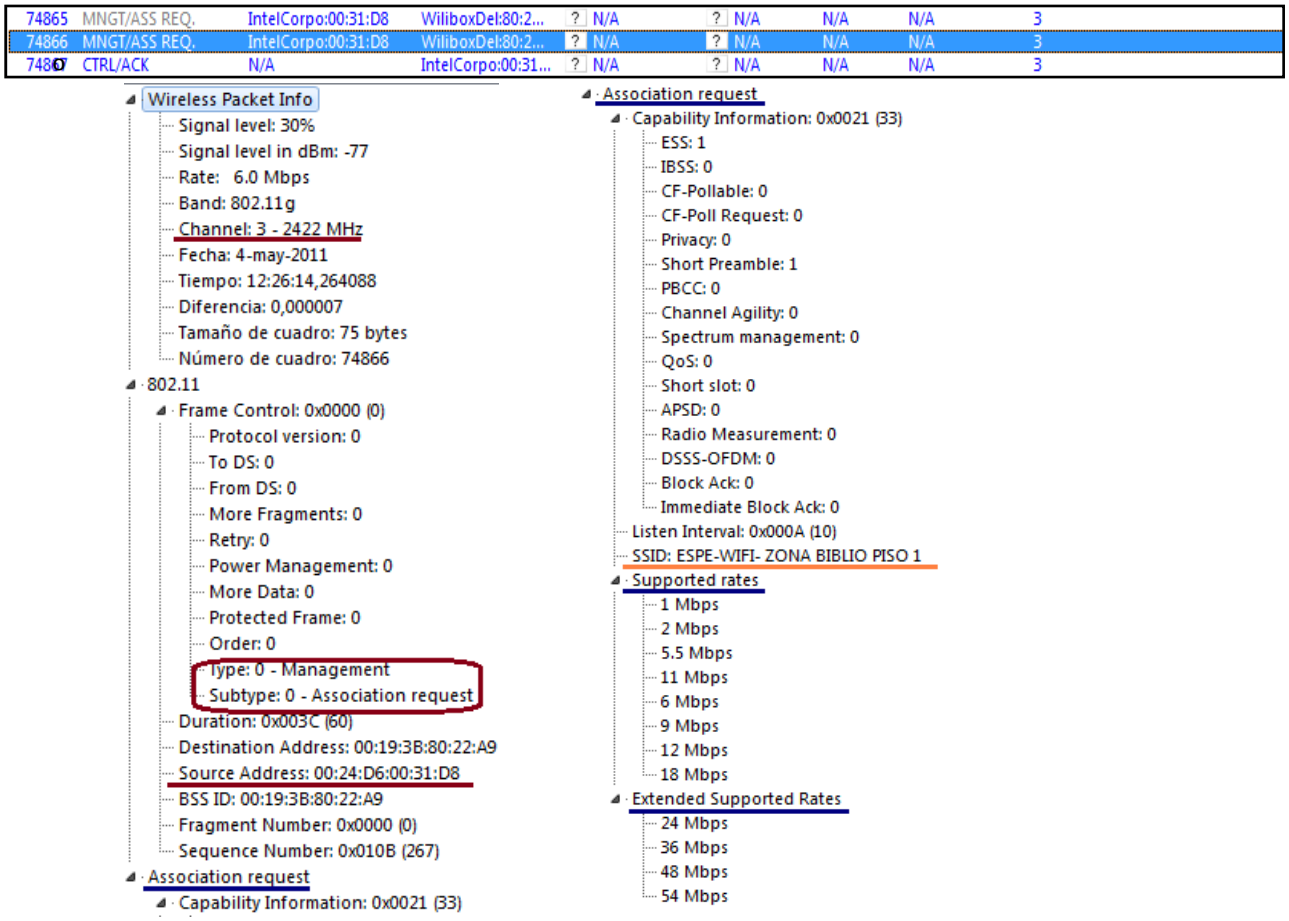


Figura. 4.30. Trama de Administración: Association Request

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa →**To DS**: 0 / **From DS**: 0, de **STA a AP**
- Trama: ***Administración***
- Subtipo: ***0-Association Request***, donde 0 → ***0000*** es ***solicitud de asociac.***
- BSSID: **00:19:3B:80:22:A9**

ASSOCIATION REQUEST

- SSID: **ESPE-WIFI- ZONA BIBLIO PISO 1**
- Tasa de transmisión soportada: desde 1 Mbps hasta 18 Mbps
- Tasa de transmisión soportada Extendida: desde 24 Mbps hasta 54 Mbps.

En esta caso, el STA con MAC: **00:24:D6:00:31:D8** está solicitando asociarse a nuestro AP analizado con MAC **00:19:3B:80:22:A9.**

Response: Respuesta de sondeo [52]

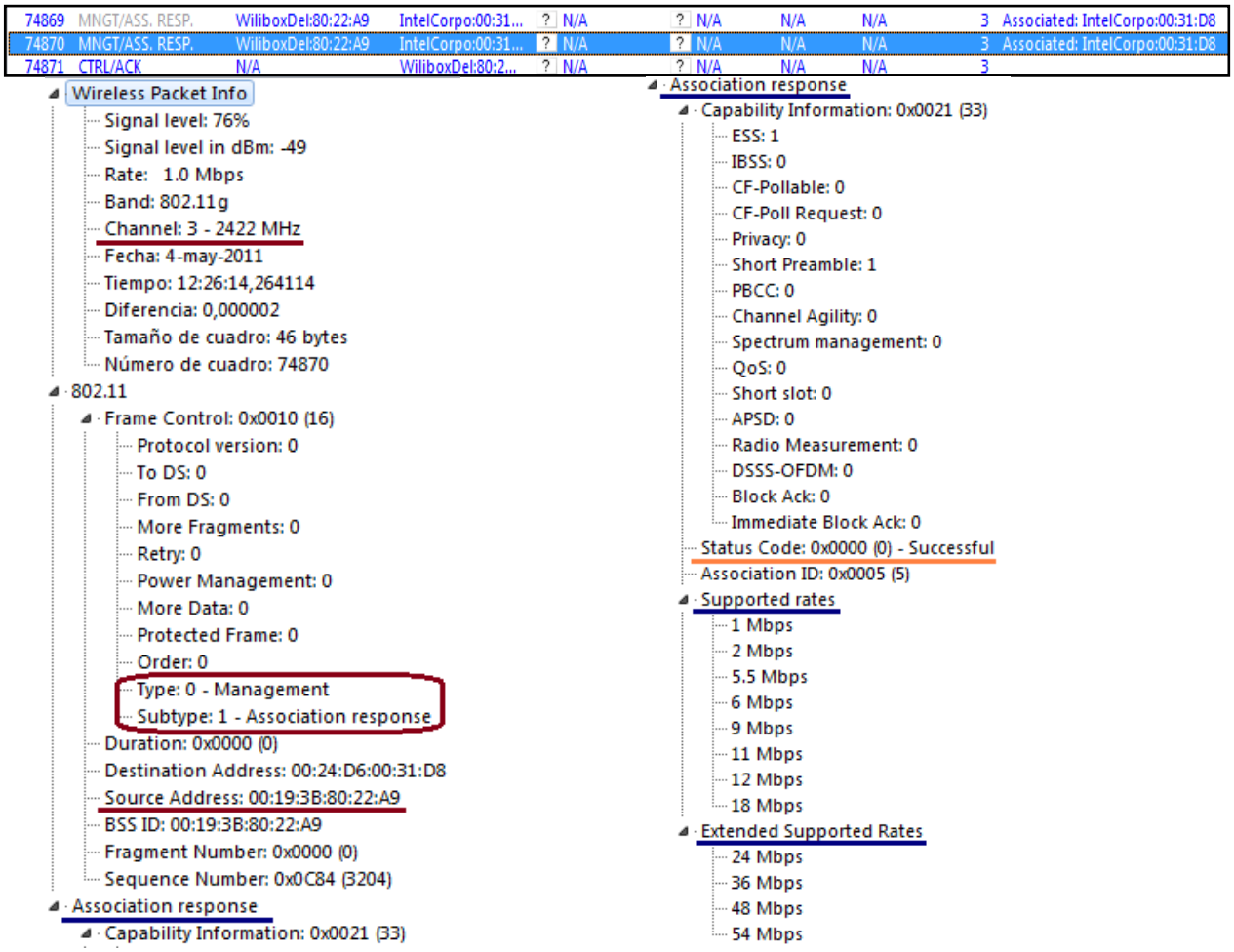


Figura. 4.31. Trama de Administración: Association Response

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa → **To DS**: 0 / **From DS**: 0, de **AP a STA**
- Trama: ***Administración***

- Subtipo: ***1 - Association Response***, donde 1 → ***0001*** es ***respuesta de solicitud de asociación.***
- BSSID: **00:19:3B:80:22:A9**

ASSOCIATION RESPONSE

- Tasa de transmisión soportada: desde 1 Mbps hasta 18 Mbps
- Tasa de transmisión soportada Extendida: desde 24 Mbps hasta 54 Mbps.

En esta caso, nuestro AP asignado con MAC **00:19:3B:80:22:A9** está respondiendo a la solicitud de Asociación que realizó el STA con MAC **00:24:D6:00:31:D8** informándole que su requerimiento fue exitoso.

➢ ***RE-ASOCIACIÓN*:** Un cliente o STA, puede enviar tramas de reasociación tras recibir una disociación; ó enviar tramas de reasociación si ya está conectado a un AP y desea asociarse con otro.

Request [52]

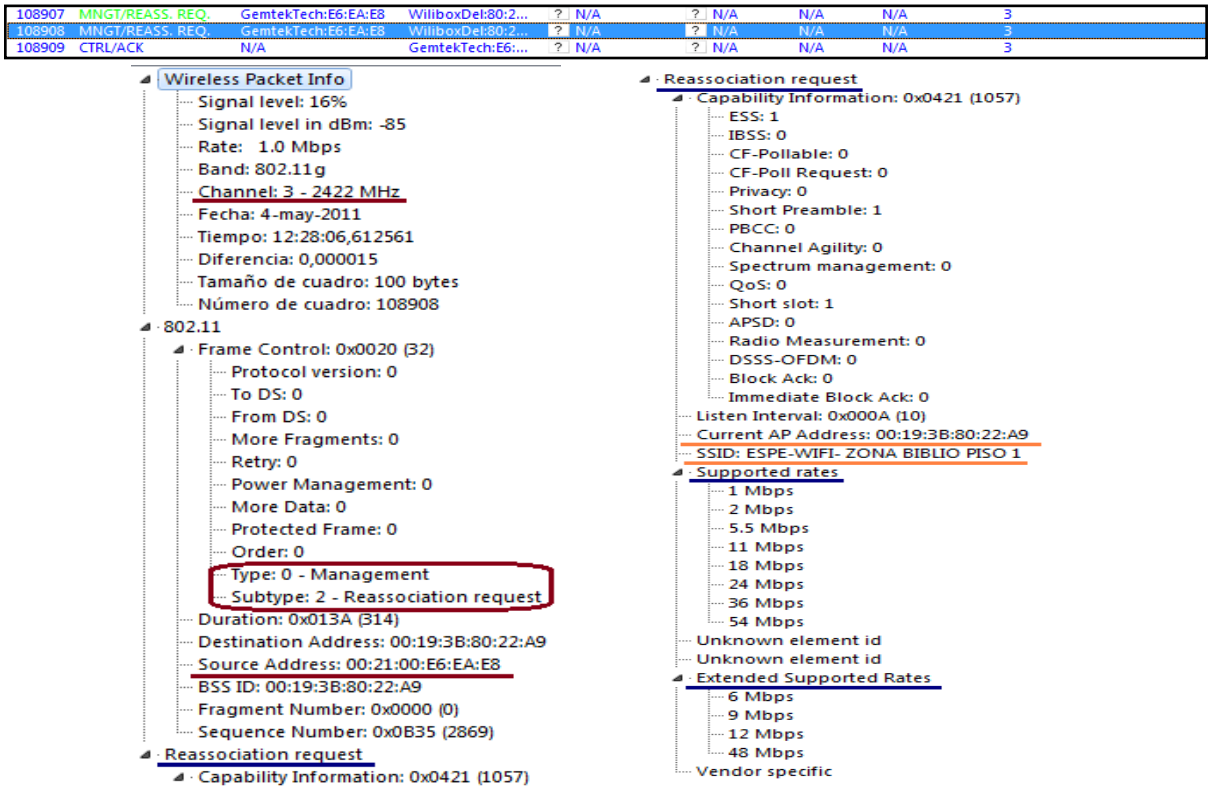


Figura. 4.32. Trama de Administración: Re-Association Request

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa →**To DS**: 0 / **From DS**: 0, de **STA a AP**
- Trama: ***Administración***
- Subtipo: ***2- Association Request***, donde 2 →***0010*** es ***solicitud de re-asociación.***
- BSSID: **00:19:3B:80:22:A9**

RE-ASSOCIATION REQUEST

- SSID: **ESPE-WIFI- ZONA BIBLIO PISO 1**
- Tasa de transmisión soportada: desde 1 Mbps hasta 54 Mbps
- Tasa de transmisión soportada Extendida: desde 6 Mbps hasta 48 Mbps.

En esta caso, el STA con MAC: **00:21:00:E6:EA:E8** está solicitando Re-asociarse a nuestro AP analizado con MAC **00:19:3B:80:22:A9.**

Response [52]***:***

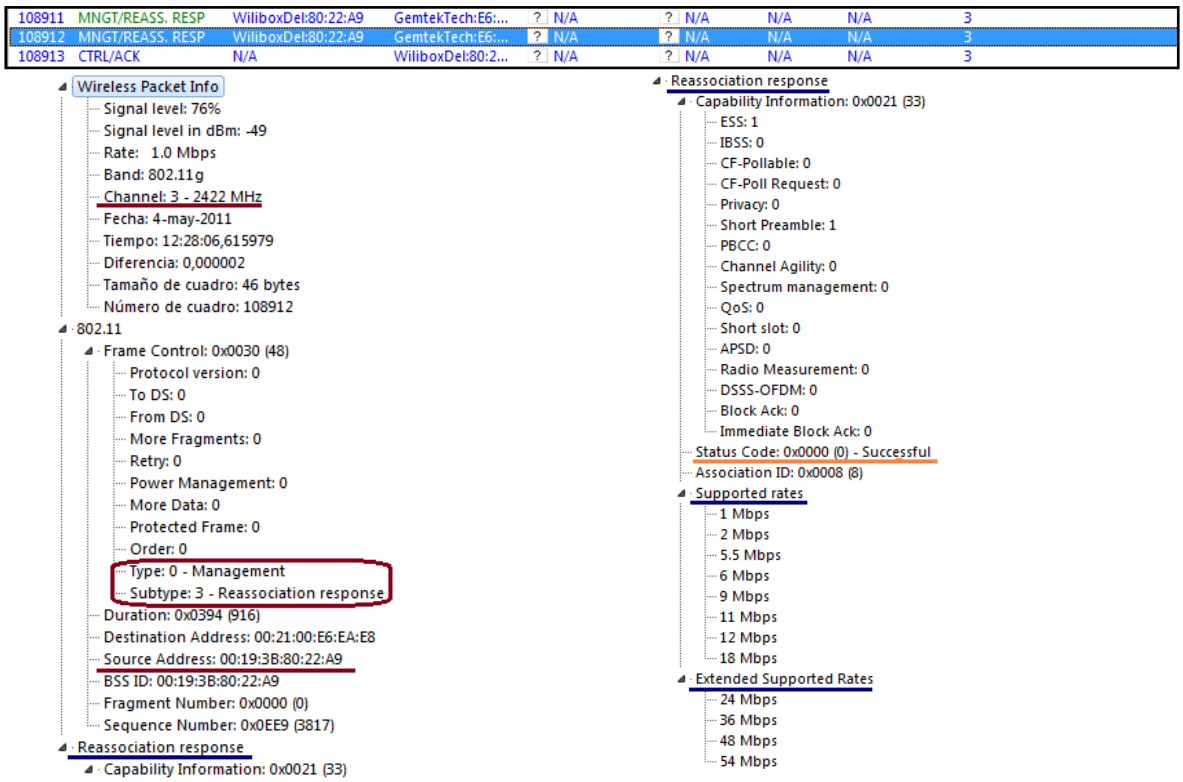


Figura. 4.33. Trama de Administración: Re-Association Response

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa →**To DS**: 0 / **From DS**: 0, de **AP a STA**
- Trama: ***Administración***
- Subtipo: ***3-Association Response***,donde 3 →***0011*** es ***respuesta de re-asociación.***
- BSSID: **00:19:3B:80:22:A9**

RE-ASSOCIATION RESPONSE

- Estado: exitoso
- Tasa de transmisión soportada: desde 1 Mbps hasta 18 Mbps
- Tasa de transmisión soportada Extendida: desde 24 Mbps hasta 54 Mbps.

En esta caso, nuestro AP asignado con MAC **00:19:3B:80:22:A9** está respondiendo a la solicitud de Re-Asociación que realizó el STA con MAC **00:21:00:E6:EA:E8** informándole que su requerimiento fue exitoso.

COMENTARIO

La cantidad de tramas de Administración capturadas durante el monitoreo fueron:

Tabla. 4.5. Tramas de Administración

TRAMA DE ADMINISTRACIÓN	CANTIDAD DE PAQUETES
BEACON	68 378
PROBE REQUEST	1 892
PROBE RESPONSE	6 750
AUTHENTICATION	46
DES-AUTHENTICATION	46
ASSOCIATION REQUEST	6
ASSOCIATION RESPONSE	10
RE-ASSOCIATION REQUEST	2
RE- ASSOCIATION RESPONSE	2

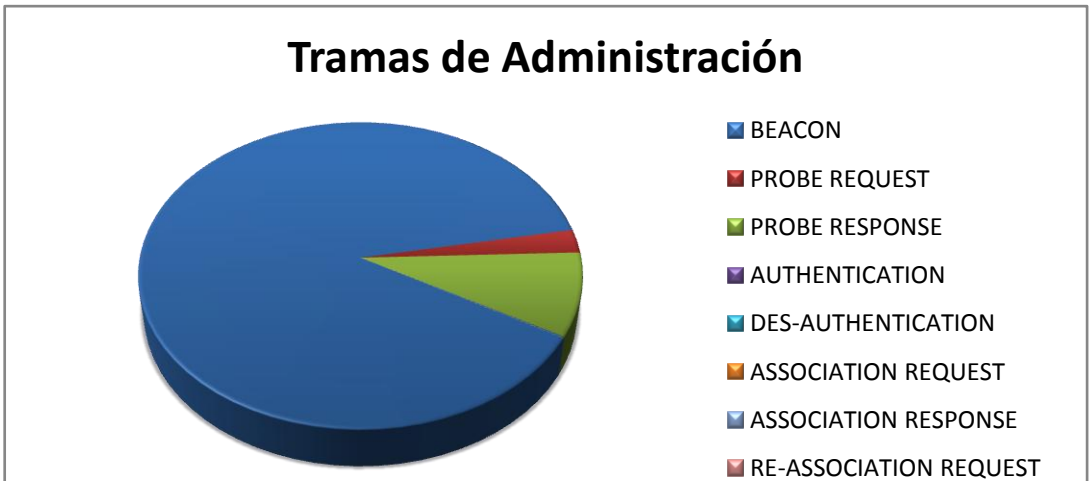


Figura. 4.34. Trama de Administración [52]

TRAMAS DE DATOS:

De acuerdo a los paquetes capturados, se observa que forman parte de las Tramas de Datos los paquetes correspondientes a tramas: ARP (Resp/Req), DATA, IP/TCP, IP/UDP, IP/ICMP, IP/IGMP. Se analiza las tramas ARP y Data.

- **ARP:** proporciona una correspondencia entre las direcciones IP y las direcciones físicas usadas a nivel de enlace.

  Request / Response: Cuando un host recibe una petición ARP (***REQUEST***) dirigida a él, rellena en la trama su dirección física, intercambia las dos direcciones origen con las dos direcciones destino, pone el campo de tipo de operación a 2 (para indicar que es una ***RESPONSE*** ARP) y envía la trama de respuesta.

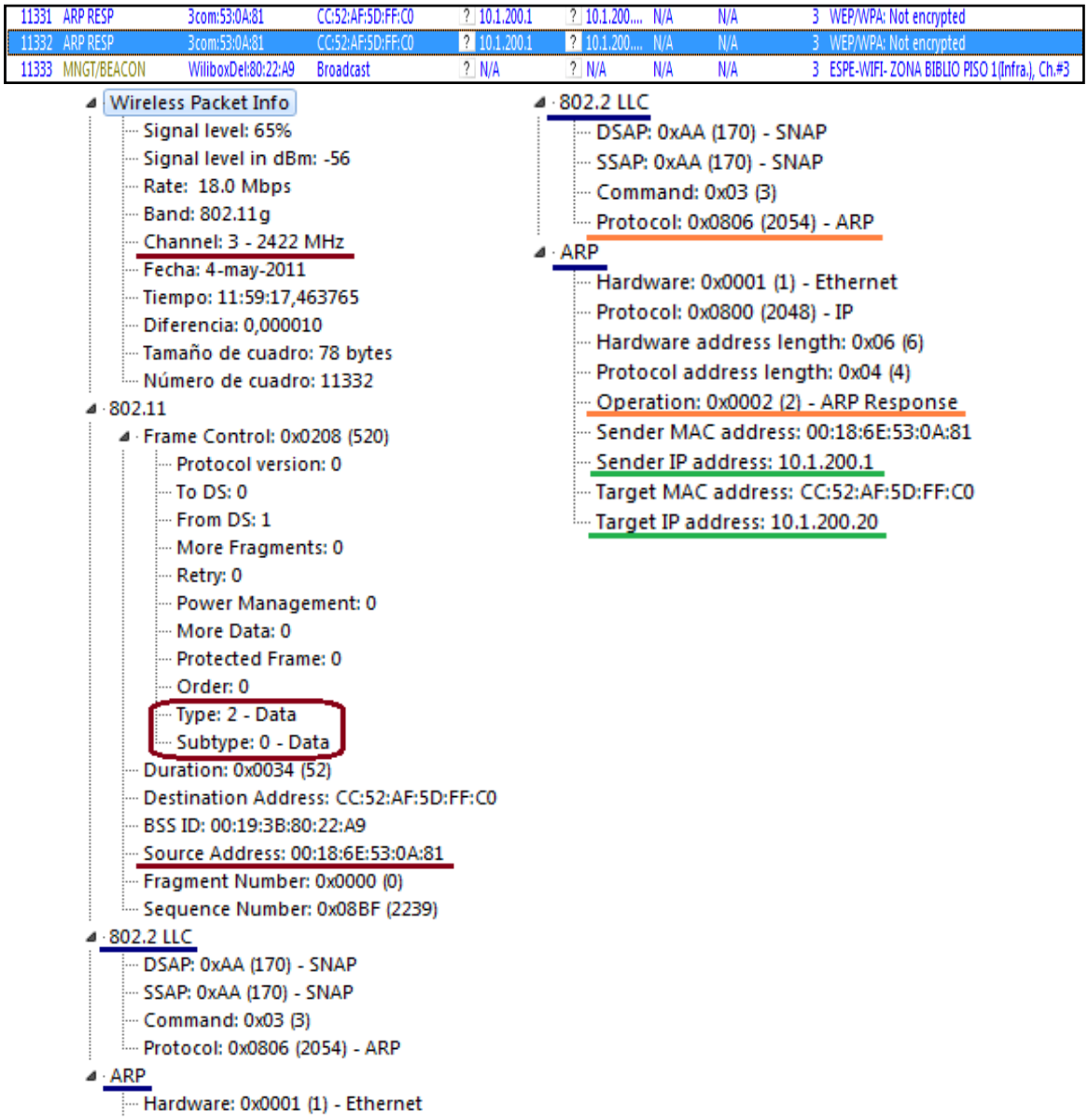


Figura. 4.35. Trama de Datos: ARP Response

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es desde el sistema de distribución → **To DS**: 0 / **From DS**: 1, comunicación entre **AP y STA.**
- Trama: ***Datos***
- Subtipo: ***0-Data***

ARP RESPONSE

- Hardware: Ethernet.
- Operación: **ARP Response - 2**
- Sender MAC / IP: **00:18:6E:53:0A:81 / 10.1.200.1**
- Target MAC / IP: **CC:52:AF:5D:FF:C0 / 10.1.200.20**

Como se puede observar, una vez contestada la petición ARP Request se verifica que el valor asignado al ***Tipo de Operación*** es **2**; que es el valor asignado a una trama ARP Response.

Request [52]***:***

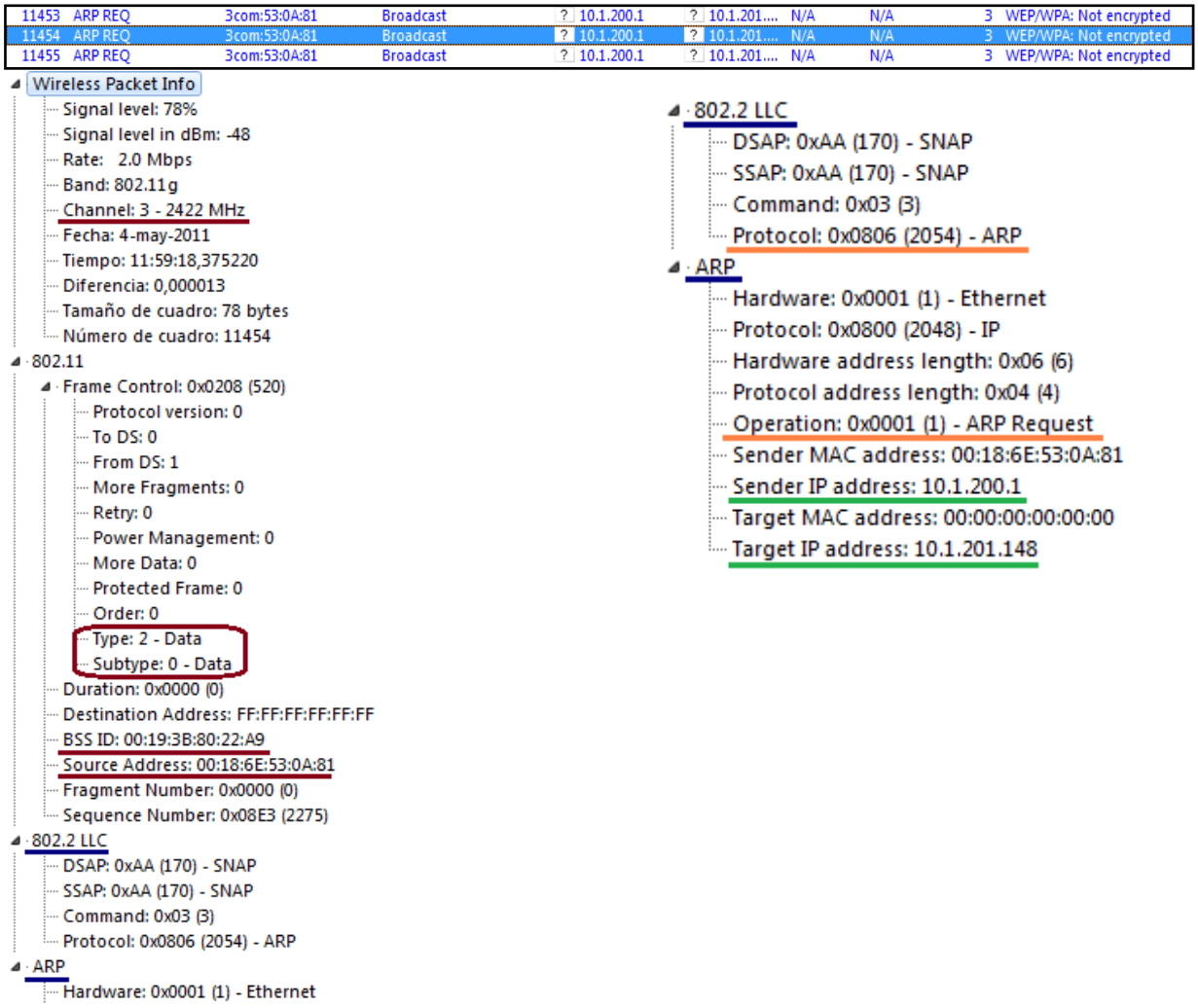


Figura. 4.36. Trama de Datos: ARP Request

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es desde el sistema de distribución → **To DS**: 0 / **From DS**: 1, comunicación entre **AP y STA.**
- Trama: ***Datos***
- Subtipo: ***0-Data***
- BSSID: **00:19:3B:80:22:A9**

ARP REQUEST

- Hardware: Ethernet.
- Operación: **ARP Request** - **1**.
- Sender MAC / IP: **00:18:6E:53:0A:81 / 10.1.200.1**
- Target MAC / IP: **00:00:00:00:00:00 / 10.1.201.148**

ARP Request muestra: IP Origen: **00:18:6E:53:0A:81/10.1.200.1**, IP Destino: **00:00:00:00:00:00/10.1.201.148, *Tipo de Operación:* 1** (valor asignado a ARP Request). La trama capturada muestra que el Host **10.1.200.1** solicita una petición Broadcast ARP para averiguar la MAC de otro host con dirección **10.1.201.148.** De esta manera, el AP (10.1.200.1) como cualquier STA (host) emisor (**10.1.201.148 u otra**) actualizan sus Caches ARP, sus tablas MAC, etc. de forma que en las siguientes conexiones no será preciso enviar peticiones-respuestas ARP ya que ambos conocen sus respectivas MAC.

Tabla. 4.6. Tramas ARP. Direcciones IP asignadas a varios STA que están asociadas a nuestro AP

Target MAC	Target IP
CC:52:AF:5D:FF:C0	10.1.200.20
00:00:00:00:00:00	10.1.201.148
00:00:00:00:00:00	10.1.201.142
00:00:00:00:00:00	10.1.201.83
00:00:00:00:00:00	10.1.201.43
00:00:00:00:00:00	10.1.201.147
00:00:00:00:00:00	10.1.201.91
00:00:00:00:00:00	10.1.201.125

Con la información obtenida de la tabla MAC se podría realizar un ataque en el que se puede ***falsear*** la dirección IP asignada a la MAC, ***falsear*** la MAC asignada a la IP ó ***falsear*** la MAC e IP. En éste último caso el ataque resultaría siempre y cuando la nueva IP asignada a la MAC forme parte de la red WLAN.

➢ **DATA:**

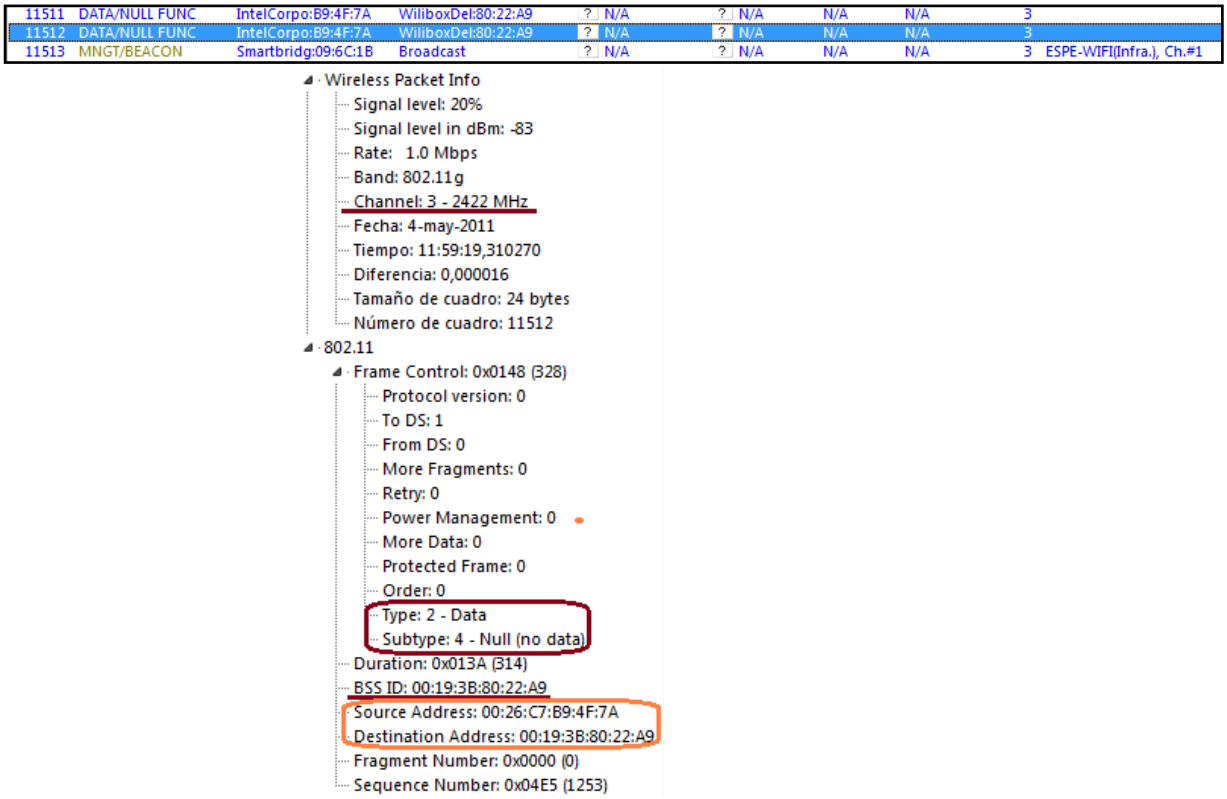


Figura. 4.37. Trama de Datos: DATA

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es hacia el sistema de distribución → **To DS**: 1 / **From DS**: 0, comunicación entre **STA y AP.**
- Trama: ***Datos***
- Subtipo: ***4-Data***
- BSSID: **00:19:3B:80:22:A9**
- Source Address: **00:26:C7:B9:4F:7A**
- Destination Address: **00:19:3B:80:22:A9**

La información proporcionada por la trama DATA nos indica la MAC de un STA conectándose hacia el AP. Con éstas tramas podríamos conocer las MAC de cada uno de los STA que están teniendo una comunicación hacia al AP y escuchar/obtener la información que está manejando cada uno de los usuarios y con ello realizar intrusiones y/o ataques.

Los protocolos ***TCP, UDP, ICMP, IGMP***; son protocolos que forman parte de las capas superiores pero que se forman ***desde*** la Capa de Enlace de Datos hacia arriba. Por lo anteriormente indicado, no se realizará el análisis de éste tipo de paquetes y que también forman parte de las capturas obtenidas en el canal 3.

COMENTARIO

La cantidad de tramas de Datos capturadas durante el monitoreo fueron:

Tabla. 4.7. Tramas de Datos

TRAMA DE DATOS	CANTIDAD DE PAQUETES
ARP REQUEST	1 720
ARP RESPONSE	122
DATA_NULL	1 572

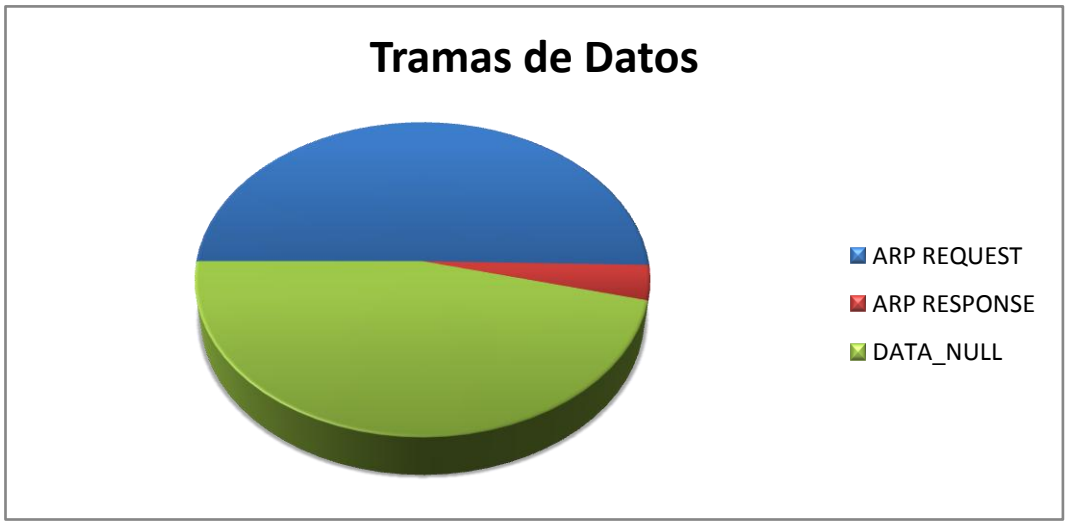


Figura. 4.38. Trama de Datos [52]

TRAMAS DE CONTROL

Se utilizan para colaborar en la entrega de tramas de datos entre estaciones.

- **Trama ACK:** Las ***tramas ACK*** tienen como objetivo confirmar la recepción de una trama. En caso de no llegar la trama ACK el emisor vuelve a enviar la trama de datos, Figura. 4.39 [52].

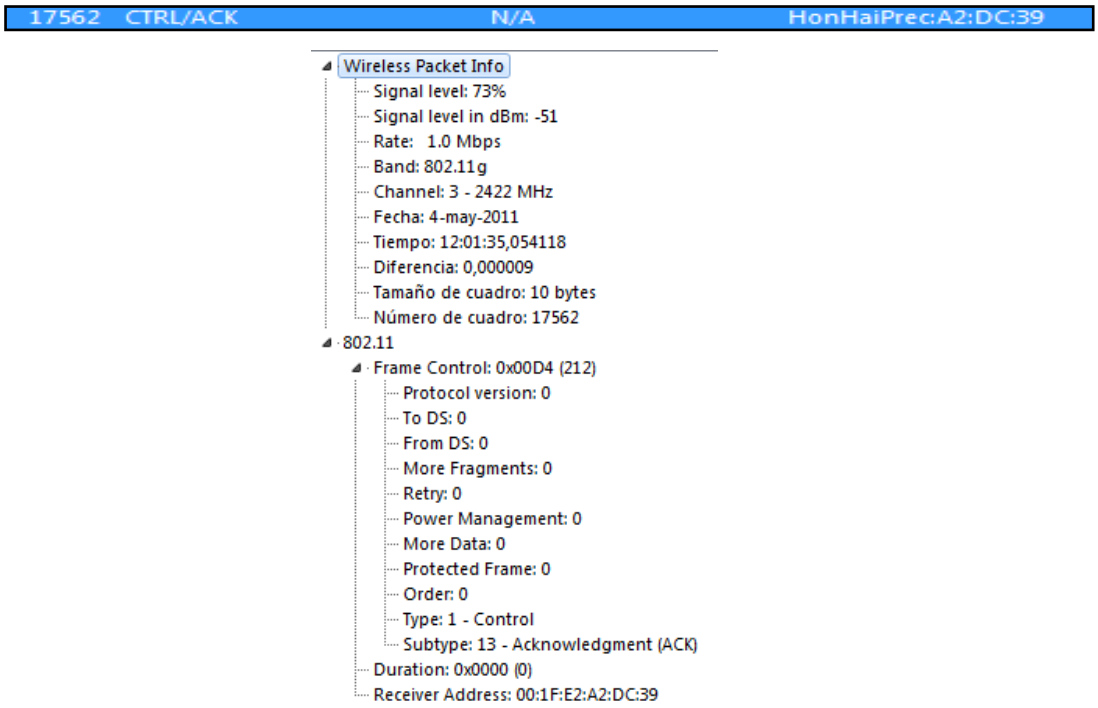


Figura. 4.39. Trama de Control ACK

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa → **To DS**: 0 / **From DS**: 0.
- Trama: ***Control***
- Subtipo: ***13-Acknowledgment***
- Receiver Address: **00:1F:E2:A2:DC:39**

En esta caso, la trama de control confirma la recepción de una trama de datos proveniente de **00:1F:E2:A2:DC:39**

- **Trama CTS:** Las estaciones utilizan las ***tramas CTS*** para responder a una trama RTS para dejar el canal libre de transmisiones. Las tramas CTS contienen un valor de tiempo durante el cual el resto de las estaciones dejan de transmitir el tiempo necesario para transmitir la trama.

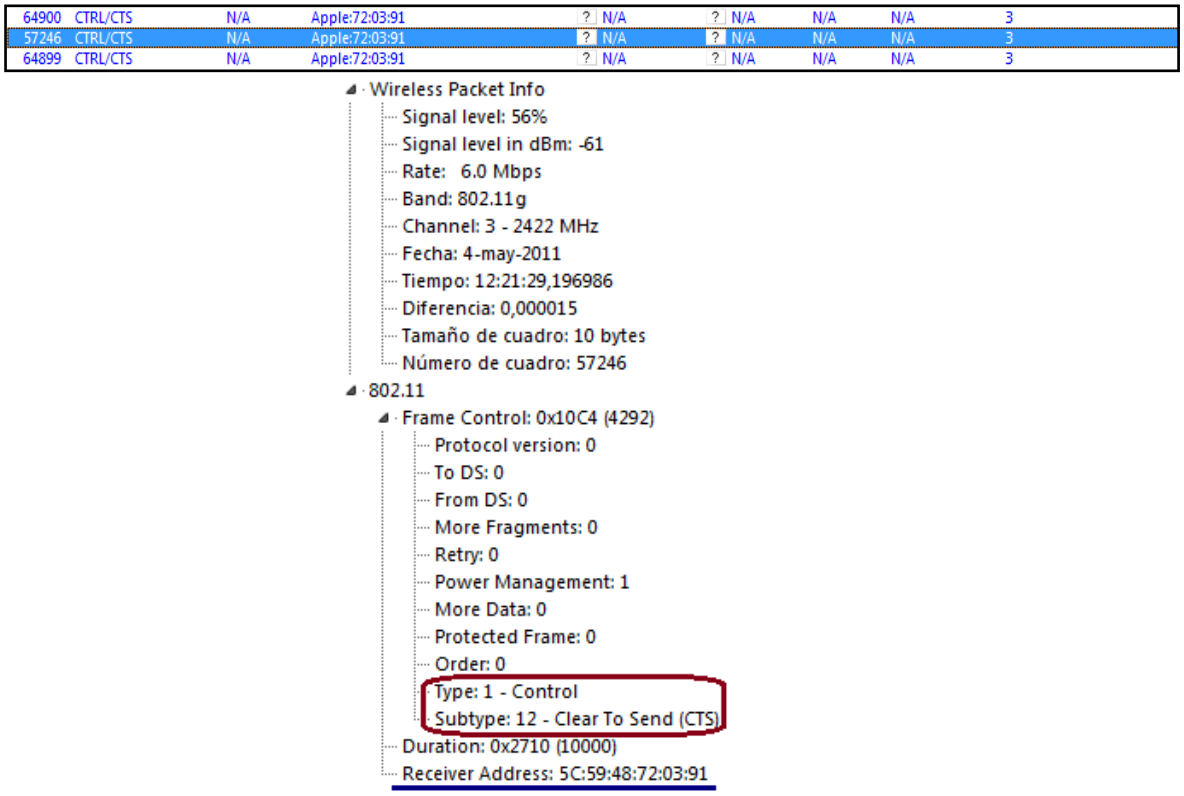


Figura. 4.40. Trama de Control CTS

Análisis

Dentro del Frame de Control que nos proporciona ***802.11*** se verifica que:

- La comunicación es directa → **To DS**: 0 / **From DS**: 0
- Trama: ***Control***
- Subtipo: ***12-Clear to Send***
- Receiver Address: **5C:59:48:72:03:91**

A continuación se muestra la Tabla. 4.8. [52], con información de tramas ACK/CTS.

Tabla. 4.8. Tramas de Control: ACK /CTS.

PACKET	PROTOCOLO	802.11				
		To DS	From DS	Type	SubType	Receiver Address
17556	CTRL / ACK	0	0	1-Control	13-ACK	00:1F:E2:A2:DC:39
17596	CTRL / ACK	0	0	1-Control	13-ACK	00:19:3B:80:22:A9
17626	CTRL / ACK	0	0	1-Control	13-ACK	CC:52:AF:5D:FF:C0
17650	CTRL / ACK	0	0	1-Control	13-ACK	00:21:00:E6:EA:E8
17712	CTRL / ACK	0	0	1-Control	13-ACK	70:F1:A1:FE:92:C5
17780	CTRL / ACK	0	0	1-Control	13-ACK	00:26:C7:B9:4F:7A
17902	CTRL / ACK	0	0	1-Control	13-ACK	00:23:14:6C:D3:D8
18024	CTRL / ACK	0	0	1-Control	13-ACK	00:30:1A:09:6C:1B
22746	CTRL / ACK	0	0	1-Control	13-ACK	4C:ED:DE:F4:70:CA
57246	**CTRL / CTS**	0	0	1-Control	12-CTS	5C:59:48:72:03:91
88560	CTRL / ACK	0	0	1-Control	13-ACK	5C:59:48:72:03:91
106262	CTRL / ACK	0	0	1-Control	13-ACK	00:24:D6:00:31:D8
108142	CTRL / ACK	0	0	1-Control	13-ACK	5C:59:48:72:03:91

Con la información obtenida de los paquetes capturados a nivel de la Capa de Enlace (direcciones MAC/IP, tramas ARP) se puede hacer uso de la misma para efectuar ataques que impliquen el uso de esta información.

Como se dijo en el Capítulo anterior, los ataques a nivel de la Capa de Enlace pueden ser: *Man in the Middle (Sniffing), Secuestro (Hijacking), Denial of service (DoS);* todos ellos basados en ARP/MAC.

COMENTARIO

La cantidad de tramas de Control capturadas durante el monitoreo fueron:

Tabla. 4.9. Tramas de Control

TRAMA DE CONTROL	CANTIDAD DE PAQUETES
CTRL / ACK	4 260
CTRL /CTS	6

Figura. 4.41. Trama de Control

Tabla. 4.10. Tramas de Datos

TRAMAS	CANTIDAD DE PAQUETES
ADMINISTRACION	77 132
DATOS	3 414
CONTROL	4 266

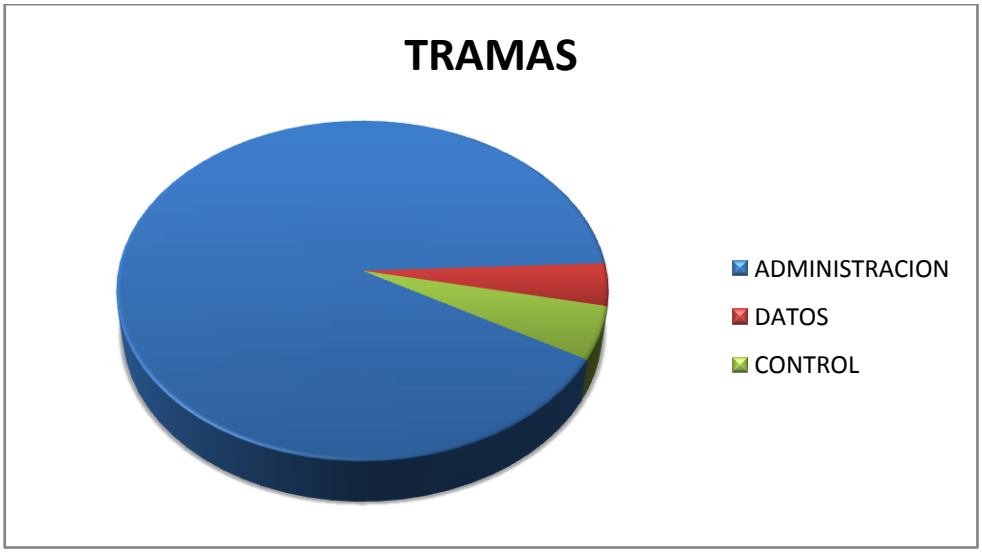


Figura. 4.42. Tramas

4.3 DETERMINACIÓN DE CARACTERÍSTICAS DEL TRÁFICO CAPTURADO

- Al realizar la captura de paquetes por medio de Wireshark, la información que enviaba/recibía nuestro STA con MAC e IP correspondiente, formaba parte de los paquetes capturados.

- Cuando se inicia la captura de paquetes haciendo uso del software Commview for WIFI se observa que la MAC asignada a nuestro STA se oculta, siendo ésta acción imperceptible para el resto de STA. De esta manera nuestro STA pasó de ser una estación que formaba parte de la LAN inalámbrica de la zona a ser un Host oculto que ‘‘escuchaba’’ las conversaciones (comunicaciones) del resto de STA de la LAN inalámbrica.

  Este hecho, al parecer simple e imperceptible, en caso de querer actuar con malicia; se puede hacer uso de el mismo para afectar el correcto desempeño de la Red o en su defecto acceder a información única y personal de un usuario X de la Red.

  Para determinar cuál es el comportamiento de nuestro STA al momento de hacer uso de los dos software, tanto en comportamiento normal (Wireshark) como en comportamiento intrusivo (Commview), se solicitó la colaboración del departamento de redes de la ESPE para que nos ayude con el monitoreo y captura de tráfico de nuestro STA por un tiempo determinado.

- Se procede a analizar el comportamiento de nuestro STA de la siguiente manera, cuando el STA forma parte de la WLAN Inalámbrica haciendo uso de WIRESHARK y cuando el STA oculta su MAC/IP al hacer uso de COMMVIEW.

  Para esto se contó con el apoyo y colaboración de la ***Unidad de Tecnología de Información y Comunicaciones*** _ ***UTIC - ESPE.*** La UTIC es el área encargada de monitorear y analizar el comportamiento de cada una de las sub-redes que forman parte de la Red WLAN de la ESPE. Entre las subredes monitoreadas se encuentran las redes asignadas a las ***Sedes*** de la ESPE (Redes LAN cableadas) entre ellas están: ESPE Matriz – Sangolquí, IASA (Selva Alegre, Santo Domingo), Héroes de Cenepa, Instituto de Idiomas,

etc.; **Redes Inalámbricas** como: ESPE – WIFI, ESPE-WIFI-ZONA-BIBLIO-PISO1, RECTORADO, etc.; entre otras.

La UTIC dispone de herramientas de monitoreo para las Redes LAN Cableadas e Inalámbricas. Para las redes WLAN Inalámbricas, hace uso del software de monitoreo WIRESHARK, por medio del mismo se puede capturar y analizar el tráfico de cada uno de los STA que se conectan a las diferentes Redes Inalámbricas que se encuentran configuradas. Para este caso en particular, nuestro STA se ha conectado a la WLAN Inalámbrica de la Biblioteca Alejandro Segovia ubicada en ESPE Matriz – Sangolquí.

Para capturar el tráfico de nuestro STA, como información proporcionada a la UTIC se indicó la MAC e IP que tomó el STA al momento de conectarse a la WLAN de la Biblioteca cuyo SSID es: **ESPE-WIFI-ZONA-BIBLIO-PISO1.** A continuación se muestra la información descrita anteriormente [55].

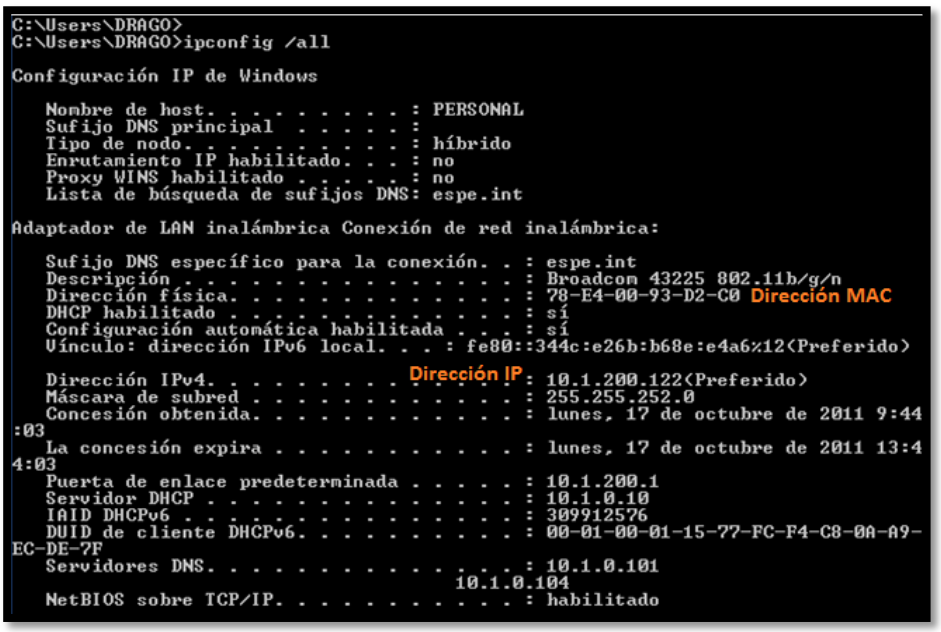


Figura. 4.43. Información proporcionada por el SO de Windows

Con la información indicada, personal de la UTIC configura Wireshark para proceder a capturar el tráfico cursado en nuestro STA. Por otra parte, una vez que nos han indicado que por parte de la UTIC ya observan la MAC e IP del STA, se inicia la captura del tráfico para determinar el comportamiento de la Red WLAN Inalámbrica **ESPE-WIFI-ZONA-BIBLIO-PISO1.**

Captura Wireshark: nos conectamos a la Red: *ESPE-WIFI-ZONA-BIBLIO-PISO1,* iniciamos la captura de paquetes por medio de Wireshark [53].

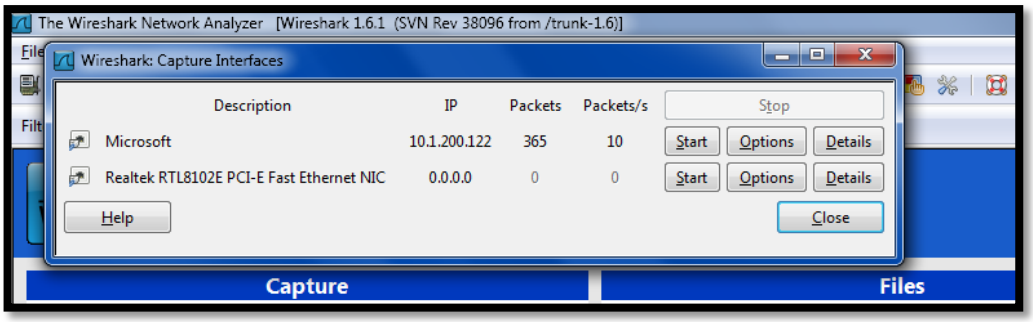


Figura. 4.44. Iniciando captura de paquetes con Wireshark

Como se puede observar, la interfaz por medio de la cuál Wireshark va a realizar la captura de paquetes tiene configurada la IP: **10.1.200.122**

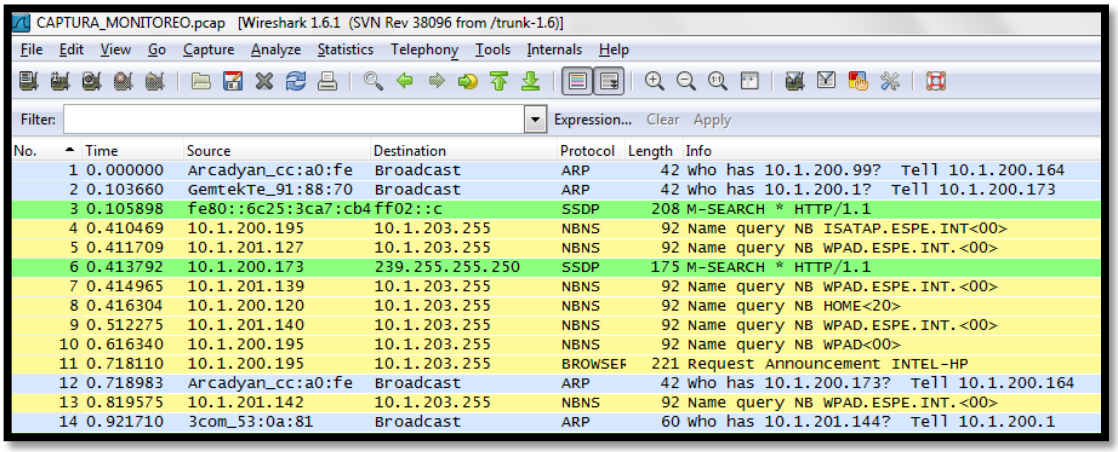


Figura. 4.45. Paquetes capturados con Wireshark

Captura Commview: en este punto lo único que se realiza es iniciar el Commview. Como se explicó anteriormente, cuando se inicia Commview se pierde la conexión a Internet y por lo tanto Wireshark deja de funcionar, como prueba de esto el propio Wireshark envía un mensaje indicando que se ha perdido la conexión a Internet [52,53].

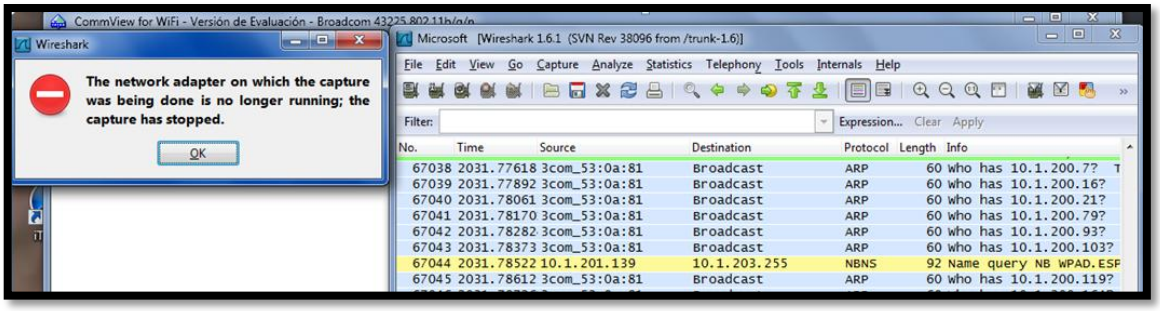


Figura. 4.46. Se inicia Commview y Wireshark pierde conexión

Al iniciar Commview [52], primero se realiza un barrido de los canales disponibles y seleccionamos el AP de la Red Inalámbrica que deseamos "escuchar". En este caso el AP de la Red **ESPE-WIFI-ZONA-BIBLIO-PISO1** se encuentra ubicado en el canal 8, por tanto seleccionamos este canal e iniciamos la captura de paquetes que se encuentran cursando en el mismo.

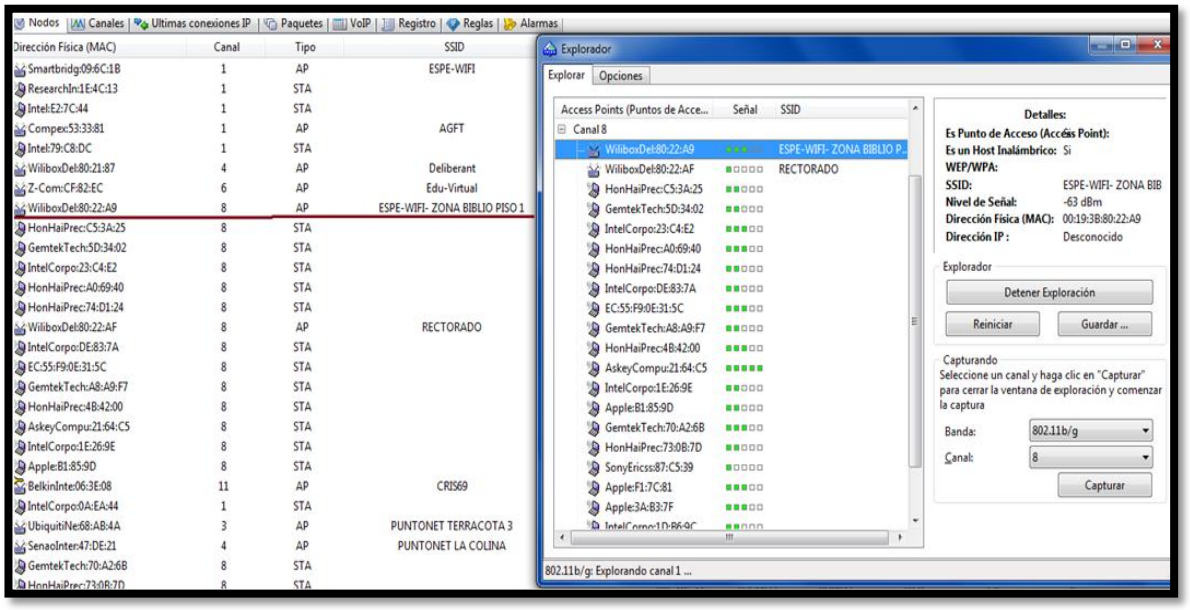


Figura. 4.47. Se inicia Commview, se selecciona el canal 8 en el cual se encuentra el AP: ESPE-WIFI-ZONA-BIBLIO-PISO1

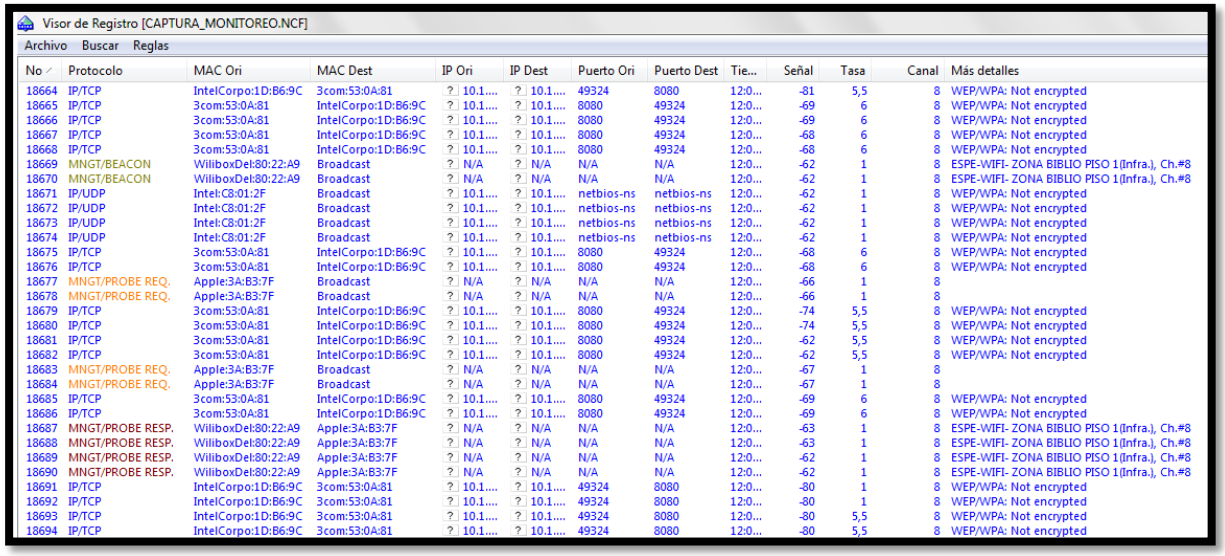


Figura. 4.48. Se inicia la captura de paquetes

***Monitoreo y captura de paquetes UTIC*:** Del lado de UTIC, para monitorear y observar el comportamiento de nuestro STA se configuró Wireshark para que capture el tráfico cursado a través de la IP del STA como IP origen y destino.

A continuación, en la Figura. 4. 49. [52], se muestra al tráfico de paquetes cursado a través de nuestro STA por medio de Wireshark, configurado con IP origen la IP: 10.1.200.122.

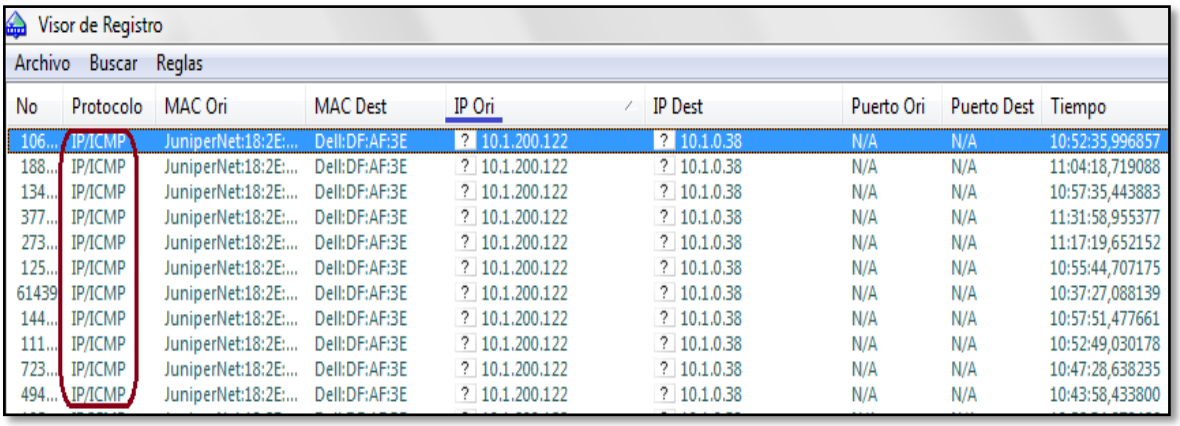


Figura. 4.49. Paquetes con IP Source: 10.1.200.122

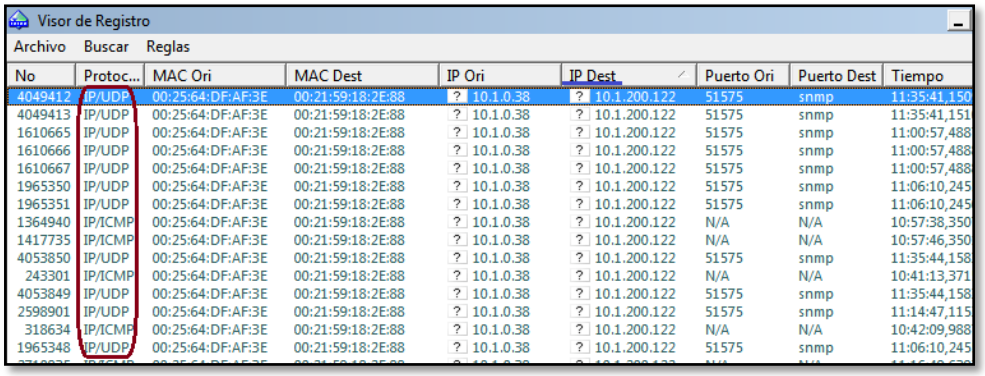


Figura. 4.50. Paquetes con IP Destino: 10.1.200.122

Como se puede observar en los paquetes capturados a través de Wireshark desde la UTIC [53], el comportamiento de nuestro STA durante la sesión establecida al conectarnos a la WLAN Inalámbrica ESPE-WIFI-ZONA-BIBLIO-PISO1 y haciendo uso de WIRESHARK ***es el mismo*** como cuando el STA se desconecta de la Red mientras estaba ejecutándose COMMVIEW. Es decir los paquetes que se visualiza en el monitoreo corresponde a paquetes cuyo protocolo son prácticamente IP/ICMP/UDP en ambos casos.

Por otra parte, el comportamiento del STA en cuestión, visualizado como usuario del mismo es totalmente diferente. Constancia de ello son las pruebas de PING realizadas antes y después de hacer uso de COMMVIEW como software intrusivo de "monitoreo" de la red inalámbrica a la que nos conectamos. A continuación se muestran las pantallas respectivas.

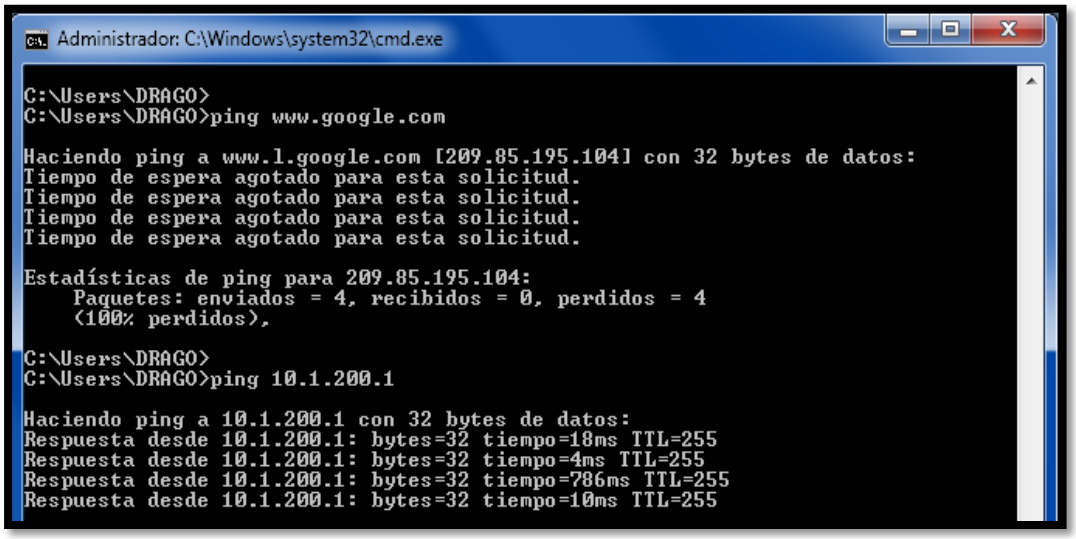


Figura. 4.51. Ping Gateway – Google _ Wireshark

La Figura. 4.51. [55], muestra que se tiene respuesta de ping hacia la IP Gateway mientras se hace uso de Wireshark. También se realiza un ping a la IP de Google, como se observa se tiene como respuesta: ***Tiempo de Espera Agotado***, sin embargo, al realizar la misma prueba de Ping hacia la IP Gateway y hacia Google mientras se hace uso de Commview la respuesta obtenida es***: Destino Inaccesible***, como muestra la Figura. 4.52. y 4.53 [55].

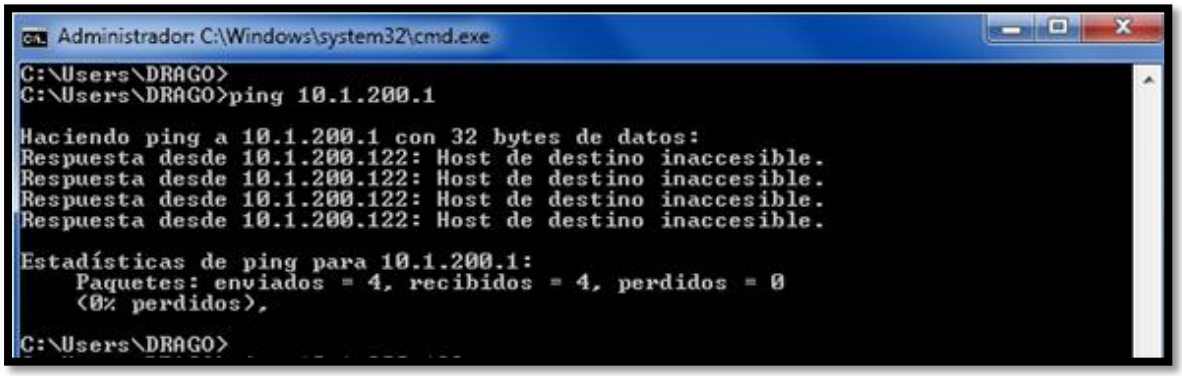


Figura. 4.52. Ping Gateway _ Commview

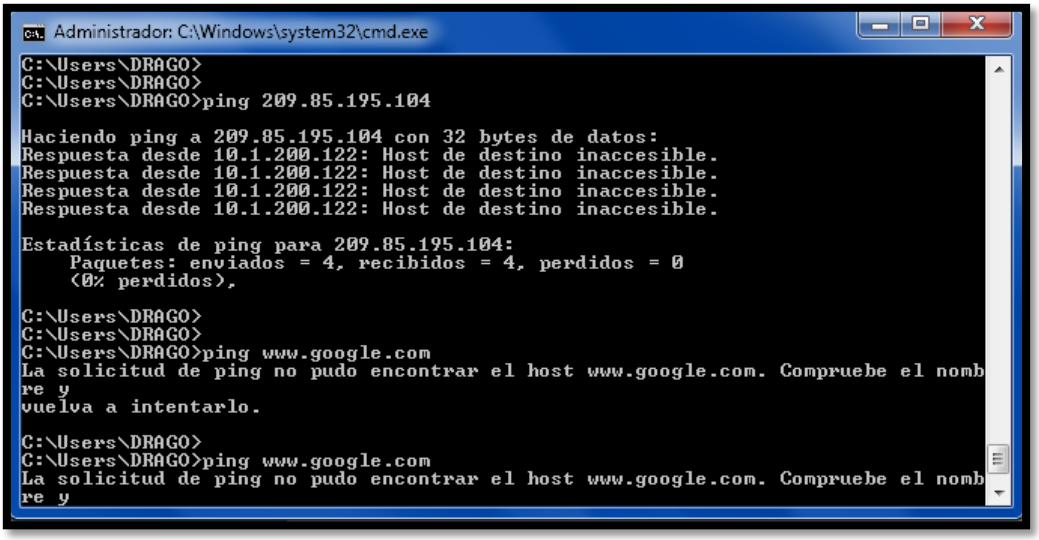


Figura. 4.53. Ping Google _ Commview

- **Número de paquetes capturados:**

La cantidad de paquetes capturados con cada software utilizado fue diferente como se observa en las Figuras 4.54 [53]– 4.55 [52].

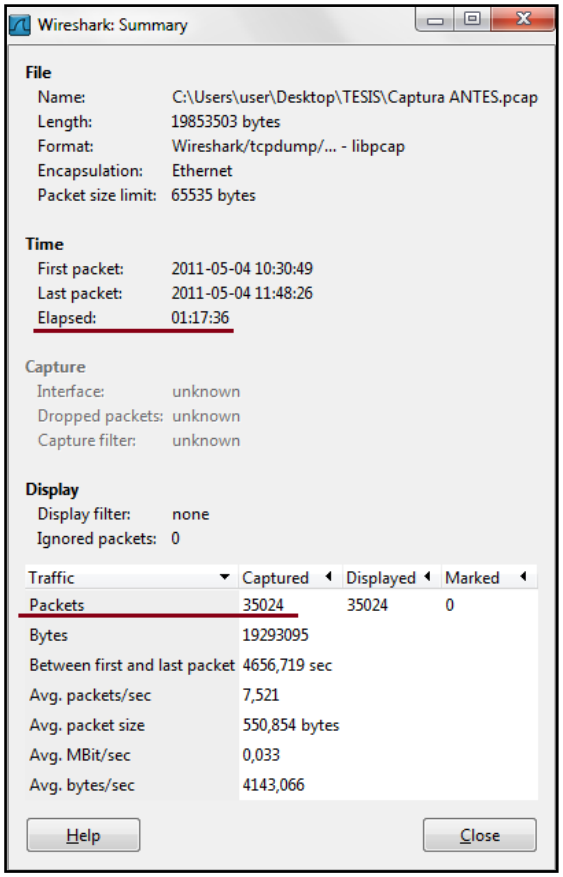
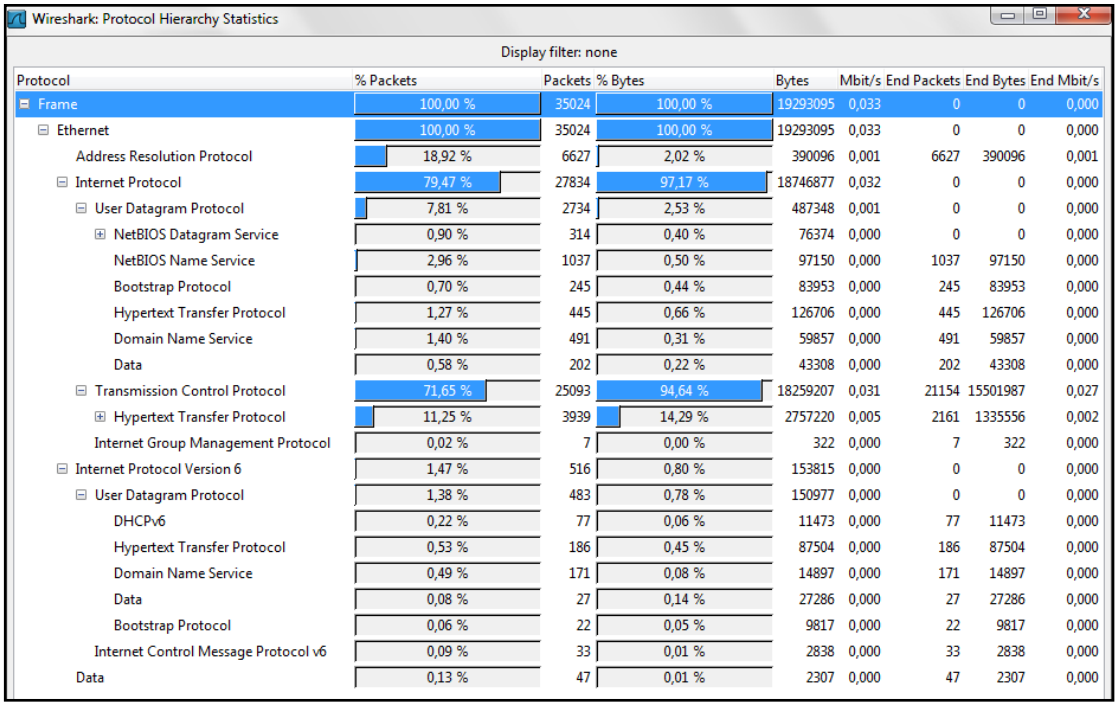


Figura. 4.54. Paquetes capturados, Wireshark

Figura. 4.55. Paquetes capturados, Commview

- **Protocolos**, [53,52].



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	35024	100,00 %	19293095	0,033	0	0	0,000
Ethernet	100,00 %	35024	100,00 %	19293095	0,033	0	0	0,000
Address Resolution Protocol	18,92 %	6627	2,02 %	390096	0,001	6627	390096	0,001
Internet Protocol	79,47 %	27834	97,17 %	18746877	0,032	0	0	0,000
User Datagram Protocol	7,81 %	2734	2,53 %	487348	0,001	0	0	0,000
NetBIOS Datagram Service	0,90 %	314	0,40 %	76374	0,000	0	0	0,000
NetBIOS Name Service	2,96 %	1037	0,50 %	97150	0,000	1037	97150	0,000
Bootstrap Protocol	0,70 %	245	0,44 %	83953	0,000	245	83953	0,000
Hypertext Transfer Protocol	1,27 %	445	0,66 %	126706	0,000	445	126706	0,000
Domain Name Service	1,40 %	491	0,31 %	59857	0,000	491	59857	0,000
Data	0,58 %	202	0,22 %	43308	0,000	202	43308	0,000
Transmission Control Protocol	71,65 %	25093	94,64 %	18259207	0,031	21154	15501987	0,027
Hypertext Transfer Protocol	11,25 %	3939	14,29 %	2757220	0,005	2161	1335556	0,002
Internet Group Management Protocol	0,02 %	7	0,00 %	322	0,000	7	322	0,000
Internet Protocol Version 6	1,47 %	516	0,80 %	153815	0,000	0	0	0,000
User Datagram Protocol	1,38 %	483	0,78 %	150977	0,000	0	0	0,000
DHCPv6	0,22 %	77	0,06 %	11473	0,000	77	11473	0,000
Hypertext Transfer Protocol	0,53 %	186	0,45 %	87504	0,000	186	87504	0,000
Domain Name Service	0,49 %	171	0,08 %	14897	0,000	171	14897	0,000
Data	0,08 %	27	0,14 %	27286	0,000	27	27286	0,000
Bootstrap Protocol	0,06 %	22	0,05 %	9817	0,000	22	9817	0,000
Internet Control Message Protocol v6	0,09 %	33	0,01 %	2838	0,000	33	2838	0,000
Data	0,13 %	47	0,01 %	2307	0,000	47	2307	0,000

Figura. 4.56. Protocolos, Wireshark

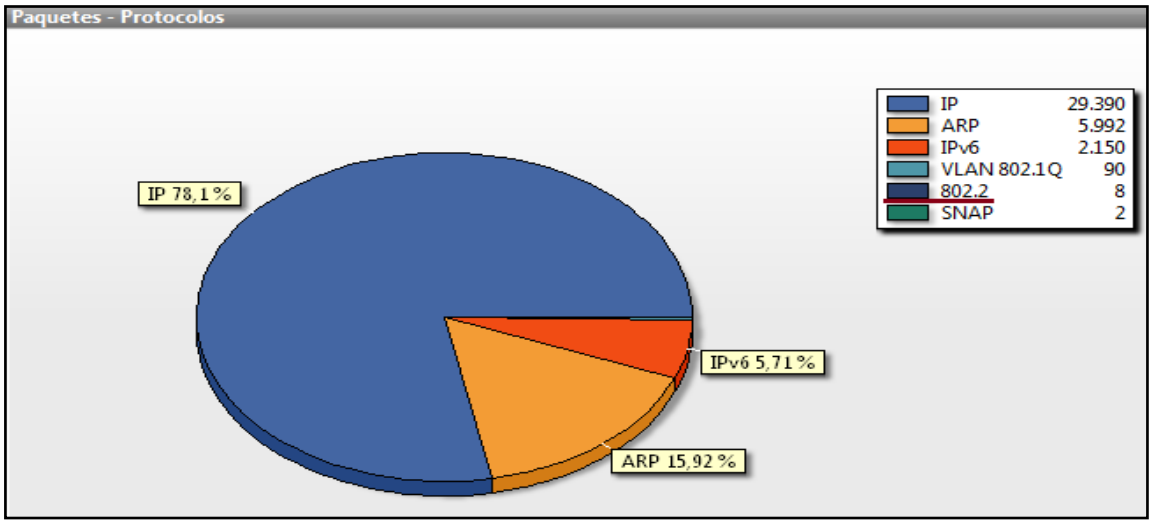


Figura. 4.57. Protocolos, Commview

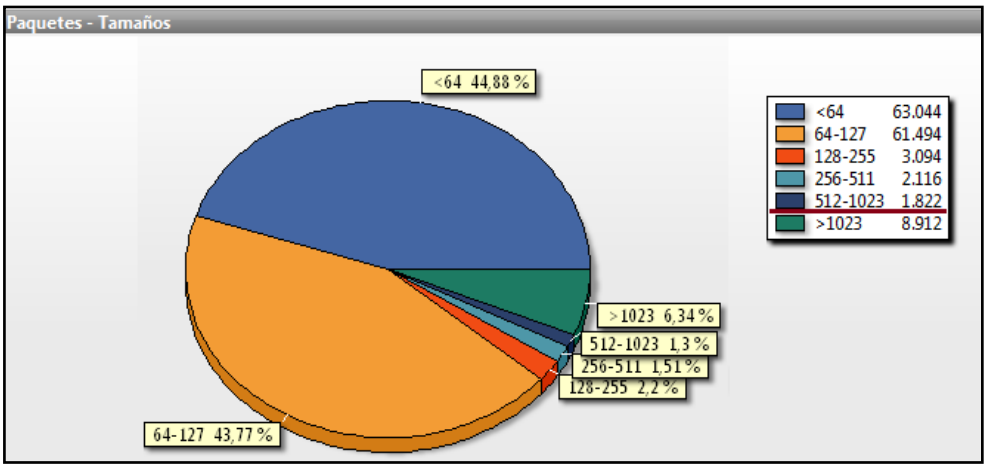


Figura. 4.58. Tamaño de paquetes, Commview

- **Conexiones de AP analizado con otros STA**

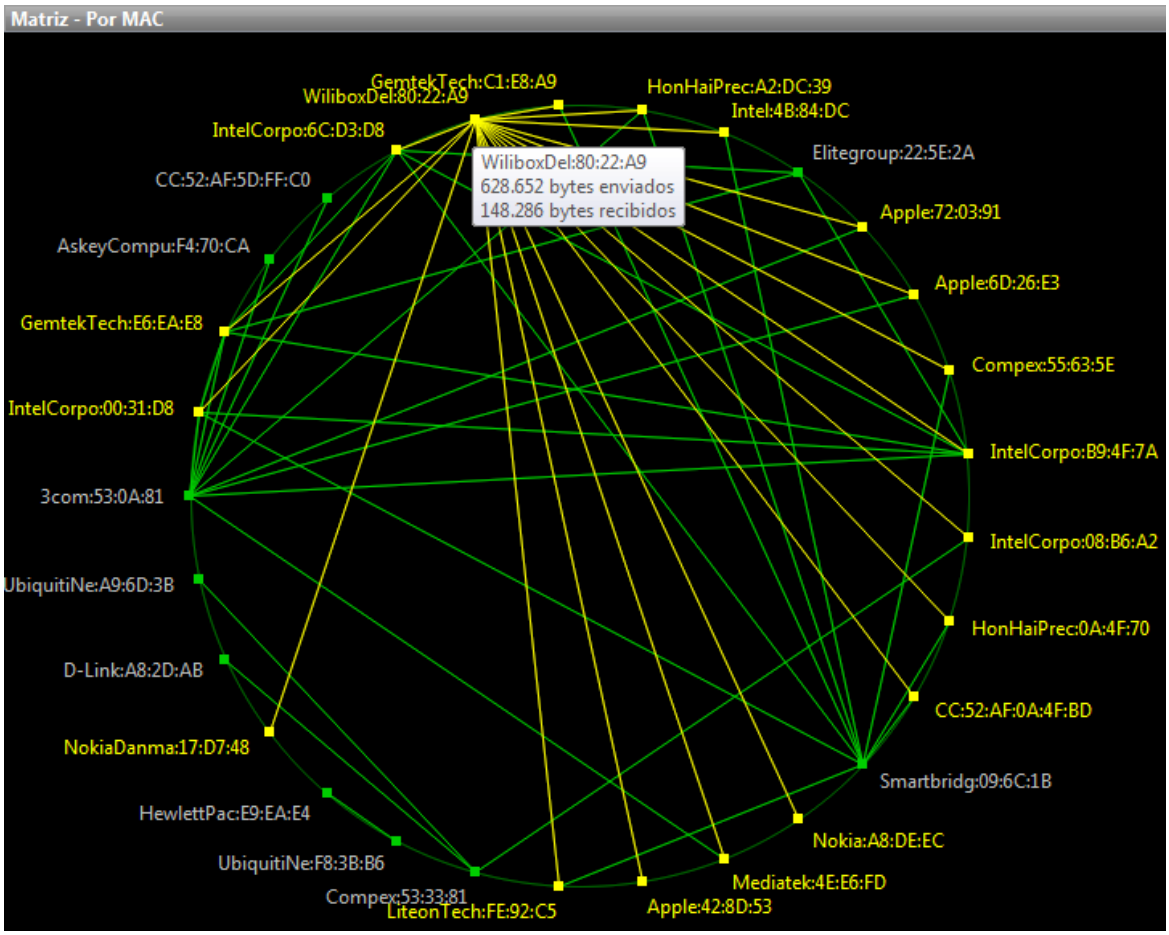


Figura. 4.59. MAC: 00:19:3B:80:22:A9, asignado a AP analizado

A continuación se muestra características propias de los paquetes capturados durante la ejecución de Commview.

- **Beacon**

Se conoce también como ***señalizaciones***. Son tramas que envían periódicamente los puntos de acceso, normalmente lo hace a intervalos regulares y sirve para que los clientes "lo vean" y puedan conectarse al mismo. Se puede "restringir" el envío de beacons, si este es el caso, el cliente debe conocer el ESSID (nombre) para poder realizar los pasos de asociación y autenticación. Es el mecanismo por el que las estaciones pueden enumerar todos los puntos de acceso disponibles [56].

Figura. 4.60. FC de un Beacon

El cuerpo de un beacon contiene información como: Marcas de tiempo, intervalo de señalización, SSID, Tasa de transmisión soportada (1Mb, 11Mb, etc), Frecuencia, y otros como DS, CF, IBSS, TIM, País, patrones y parámetros FH.

Tabla. 4.11. Valores To DS / From DS

TO DS	FROM DS	DESCRIPCION
0	0	Comunicación directa Ad-Hoc, entre dos estaciones.
0	1	La trama viaja DESDE el sistema de distribución, comunicación entre AP y STA
1	0	La trama viaja HACIA el sistema de distribución, comunicación entre las STA y AP.
1	1	Comunicación WDS, entre AP.

- **Probes**

Es un intercambio de mensajes que típicamente ocurre entre el punto de acceso y las estaciones, los más habituales son: Request y Response (Solicitud de Sondeo y Respuesta de Sondeo) [56].

Frame Control de un Probe Request															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	wep					toDS	FromDS	Subtipo				Tipo		Version	
	0					0	0	0	1	0	0	0	0	0	0
¿?					¿?			4				0			

Tipo: 00-> Trama de Administración
Subtipo: 0100 -> Request
FromDS y ToDS 00 -> Dirección STA a STA
Wep: 0 -> No cifrado

Figura. 4.61. FC de un Probe Request

Frame Control de un Probe Response															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	wep					toDS	FromDS	Subtipo				Tipo		Version	
	0					0	0	0	1	0	1	0	0	0	0
¿?					¿?			5				0			

Tipo: 00-> Trama de Administración
Subtipo: 0101 -> Response
FromDS y ToDS 00 -> Dirección STA a STA
Wep: 0 -> No cifrado

Figura. 4.62. FC de un Probe Response

A continuación se muestra un resumen de las tramas de Administración y sus correspondientes FC.

Tabla. 4.12. FC de las tramas de Administración

Tipo (bits 3 y 2)	Valor de FC	Descripción	Subtipo (bits 7-6-5-4)	Descripción del subtipo
00	00 00	Administración	0000	Solicitud de asociación
00	10 00	Administración	0001	Respuesta para la asociación
00	20 00	Administración	0010	Solicitud de reasociación
00	30 00	Administración	0011	Respuesta para la reasociación
00	40 00	Administración	0100	Solicitud de sondeo
00	50 00	Administración	0101	Respuesta de sondeo
00	80 00	Administración	1000	Señalización
00	A0 00	Administración	1010	Disociación
00	B0 00	Administración	1011	Autenticación
00	C0 00	Administración	1100	Desautenticación

- Parte de los paquetes capturados contenían información de protocolos propios de las capas superiores pero que se forman a partir de la Capa de Enlace de Datos.

- Algunos de estos protocolos son: ***IP, ICMP e IGMP*** que forman parte de la Capa de Red; otros como ***TCP, UDP*** forman parte de la Capa de Transporte.

CONCLUSIONES - RECOMENDACIONES

CONCLUSIONES

- Las empresas dependiendo del trabajo a realizar, ubicación, recursos a utilizar, costos de implementación y otras necesidades, pueden optar por implementar una red LAN Ethernet (cableada) o una red LAN Inalámbrica conocida también como redes WiFi. La implementación de redes LAN Ethernet/Inalámbricas varía en base a la velocidad de datos, medio de transmisión, acceso al medio, alcance, movilidad, etc.

- El protocolo de Acceso al medio (Capa MAC) resulta más complejo para una Red LAN Inalámbrica que para una LAN Ethernet. En las redes LAN Ethernet la Capa MAC considera aspectos como: codificación, protocolos, encapsulación. En las redes LAN Inalámbricas, la Capa MAC se basa en las topologías que pueden ser configuradas, esto es: Ad-Hoc o Infraestructura.

- En cuanto a los protocolos de Acceso al Medio _ MAC, Ethernet hace uso de CSMA/CD mientras que a nivel de LLC los protocolos usados son: sin conexión, con conexión, sin conexión con reconocimiento. Por su parte, los mecanismos de acceso al medio usados por WiFi son: Protocolos con arbitraje (FDMA,TDMA) y Protocolos de contienda (CDMA/CA, CDMA, CDMA/CD).

- Dado que el presente trabajo está direccionado a analizar el tráfico de datos cursado en la Capa de Enlace para evitar intrusiones o ataques, se debe tomar en cuenta medidas de seguridad que se puedan aplicar a nivel de la Capa de Enlace ya sea en Redes LAN Ethernet como WiFi. Como parte de la información que contiene una trama MAC están: la Dirección origen, dirección

destino (IP/MAC) la misma que puede ser utilizada como herramienta para acceder a una determinada Red, su información y causar daños a la misma.

- Actualmente existen varios protocolos de seguridad como WEP, WPA y WPA2 que pueden ser implementados en las Redes LAN para prevenir ataques e intrusiones a la Red. Las variantes de WEP, WPA y WPA2, son protocolos diseñados para trabajar con y sin un servidor de manejo de llaves. WPA utiliza TKIP (Temporal Key Integrity Protocol) para la gestión de las claves dinámicas mejorando el cifrado de datos; mientras que en WPA2 los clientes tienen que estar configurados para utilizar un sistema de validación que es independiente del AP. Los sistemas de validación WPA2 pueden ser: EAP-TLS, PEAP, EAP-TTLS.

- A nivel de seguridad se tiene que considerar aspectos como: vulnerabilidades, amenazas, riesgos y ataques. En las redes LAN WiFi los principales ataques a tener en cuenta a nivel de la Capa de Enlace son: ARP/MAC Spoofing, Man in the Midle (contra ciertos protocolos cifrados), sniffer (NIC-tarjeta de Red), ARP Poisoning. Vulnerabilidades en protocolos como: CSMA/CD, RTS/CTS. Para contrarrestar estos ataques se puede hacer uso de mecanismos de monitoreo y detección como IDS (WIDS para redes WiFi)

- Para capturar el Tráfico de Datos en la Capa de Enlace se consideró como escenario de pruebas el Comportamiento Normal de la Red a analizar, en este caso la Red WLAN: ESPE-WIFI-ZONA-BIBLIO-PISO1. Para ello se utilizó herramientas de monitoreo (software) y captura de paquetes como Wireshark y Commview. El análisis del tráfico capturado se basó en la información proporcionada por los paquetes capturados por medio de COMMVIEW, esto debido a que dichos paquetes contienen información propia de la tecnología WiFi 802.11 como tramas de administración, datos y control.

- Del análisis realizado; la información proporcionada por las tramas de administración, datos y control es suficiente como para entender y conocer cuál es el comportamiento habitual de la red en un horario determinado, así como también, cuál es la información a la que acceden cada uno de los usuarios conectados a la misma.

- La cantidad de tramas de administración es mayor que la cantidad de tramas de datos y control. La información proporcionada por las tramas de administración nos ayuda a conocer las características del punto de acceso al cual están conectándose los usuarios de un área determinada, si es posible o no asociarse a un punto de acceso así como también, nos indica si un STA se desconectó de la misma, si solicita conectarse nuevamente, si realizó auntenticación o desauntenticación.

  Por su parte las tramas de datos ARP nos proporciona las direcciones MAC/IP de cada una de las estaciones que forman parte de la WLAN analizada. Esta información es importante ya que se puede determinar una tabla de direcciones ARP, la cual puede ser usada para ejecutar alguno de los ataques basados en ésta información cómo son: ARP/MAC Spoofing(DoS), ARP Poisoning, Man in the Middle (Sniffing)

- Otro dato que nos proporciona cada una de éstas tramas es el tiempo en que se ejecutan y el tiempo que transcurre en presentarse una trama a continuación de otra. Esta información puede resultar eficiente para un atacante, ya que conociendo éstos tiempos puede enviar paquetes con características similares a los capturados en intervalos de tiempo más cortos.

- Aunque la información obtenida durante la captura de paquetes se utilizó para realizar un análisis del comportamiento general de la red, éste tipo de análisis se considera un Ataque pasivo, ya que obtiene información basada en el hecho de examinar el tráfico y sus patrones como: a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

- Para conocer el comportamiento de nuestro STA visto desde un Sistema (software) de monitoreo externo a la Red WLAN analizada, se contó con la ayuda y colaboración de la ***Unidad de Tecnología de Información y Comunicaciones _ UTIC – ESPE***. Para esto, la UTIC hizo uso de WIRESHARK como software de monitoreo y captura de paquetes cursado por nuestro STA al momento de ejecutar los dos software (Wireshark/Commview). Los resultados obtenidos del monitoreo y captura de paquetes del tráfico cursado por nuestro STA solo incluía protocolos IP/ICMP.

- Para prevenir los ataques/intrusiones indicados, se puede usar la encripción a nivel de la Capa de Enlace (WEP, WPA, WPA2) como medida de seguridad sin que esto garantice confidencialidad punto-a-punto. Si se necesita seguridad a nivel de Capa de Enlace se debe evitar el uso de WEP y en su defecto usar WPA2 (IEEE 802.11i). La supresión del SSID y el filtrado mediante direcciones MAC no son métodos de autenticación seguros, es necesario un método de autenticación de más alto nivel, como RADIUS.

RECOMENDACIONES

- Al momento de implementar una Red LAN Etherne/WiFi se recomienda hacer uso de uno de los Protocolos de Seguridad como WEP, WPA ó WPA2 a nivel de la Capa de Enlace, para desde esta capa iniciar un nivel de seguridad y protección de la información cursada en la Red hacia las capas superiores.

- Dependiendo de la información a transmitir en la red, es recomendable aplicar por lo menos, el Protocolo de Seguridad WEP, teniendo en cuenta que los datos de SSID y Clave de encriptación debe ser cambiada de manera periódica para evitar el acceso maliciosa a la Red.

- Dado los ataques a los que está expuesta la información ARP/MAC que proporciona la Capa de Enlace, se recomienda hacer uso de mecanismos de detección y protección contra éstos ataques para evitar posibles intrusiones a la Red que afecten el desempeño y ponga en riesgo la información de la misma.

- Las técnicas de detección de intrusiones se recomiendan como una solución preventiva, más no correctiva, y sobre todo como una segunda línea de defensa que ayuda a mejorar la seguridad de las redes WiFi.

- En base al estudio y características del tráfico analizado en este proyecto, se puede considerar la información proporcionada por el mismo para realizar a futuro un estudio que indique cual sería el comportamiento de una Red Inalámbrica si se ejecutan de manera activa ataques/intrusiones basados en datos ARP y MAC.

ANEXOS

WIRESHARK

Es una herramienta básica para observar los mensajes intercambiados entre aplicaciones, es un analizador de protocolos (packet sniffer). **Un analizador de protocolos** es un elemento pasivo, únicamente observa mensajes que son transmitidos y recibidos desde y hacia un elemento de la red, pero nunca envía él mismo mensajes. En su lugar, un analizador de protocolos recibe una copia de los mensajes que están siendo recibidos o enviados en el terminal donde está ejecutándose [57].

Está compuesto principalmente de dos elementos: una librería de captura de paquetes, que recibe una copia de cada trama de enlace de datos que se envía o recibe, y un analizador de paquetes, que muestra los campos correspondientes a cada uno de los paquetes capturados. Para realizar esto, el analizador de paquetes ha de conocer los protocolos que está analizando de manera que la información mostrada sea coherente.

Es decir, si se captura un mensaje HTTP, el analizador de paquetes ha de saber que este mensaje se encuentra encapsulado en un paquete TCP, que a su vez se encuentra encapsulado en un datagrama IP y éste a su vez en una trama de Ethernet. Un esquema de la integración de Wireshark con el Sistema Operativo del equipo en uso puede verse en la Figura 6.1 [58].

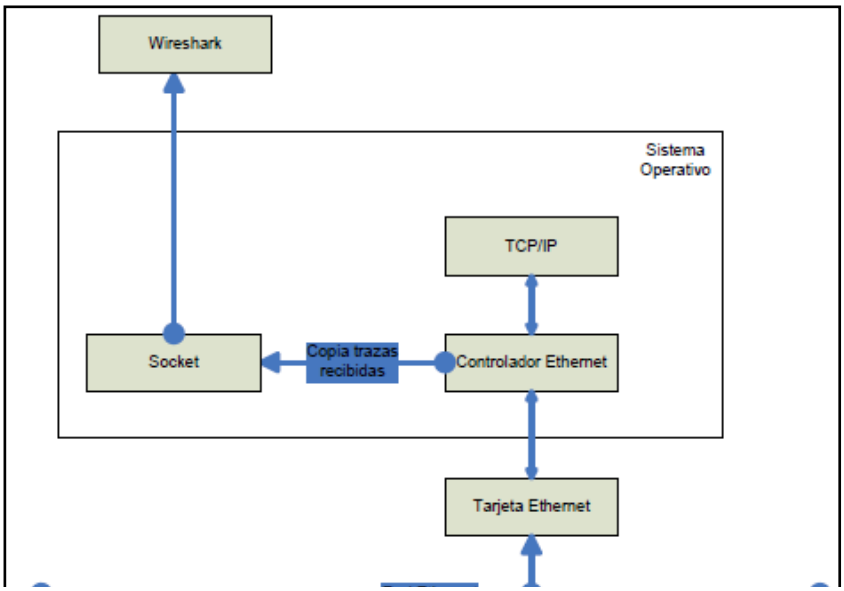


Figura. 6.1. Esquema integración Wireshark con el SO

COMMVIEW FOR WIFI

CommView for WiFi es la versión para conexiones inalámbricas de uno de los sniffers más completos y mejor valorados para Windows, se encarga de capturar los paquetes que circulen por una conexión inalámbrica para testearlos, analizarlos y comprobar el grado de optimización de una red inalámbrica en diversos aspectos.

Se comporta exactamente igual que lo haría un sniffer (utilidad diseñada para capturar el tráfico que viaja por redes de tipología Ethernet) en una red local por tanto capturara tramas, analizara cabeceras, tiene soporte para cerca de 70 protocolos entre ellos: RTP y RTCP, paquete de IP, direcciones IP, sesiones, datagramas, es compatibles con redes 802.11a, 802.11b y 802.11g, etc [59].

CommView for WiFi [60]es útil para los administradores de red por su motor de descifrado, es un sistema capaz de poner a prueba la seguridad de una red, descifrando las claves WEP y WPA definidos en sus puntos de acceso. CommView for WiFi es capaz de reconstruir sesiones TCP, generar estadísticas muy detalladas, monitorizar anchos de banda, exportar direcciones IP, entre otras posibilidades.

Requisitos

- Sistema operativo: Win2000/XP/2003/Vista
- Conexión inalámbrica
- Lista de tarjetas de red compatibles

Características

- Escaneo de más de 70 protocolos.
- Captura de tráfico WLAN 802.11 a/b/g/n
- Descifrado de paquetes WEP y WPA
- Multitud de opciones avanzadas

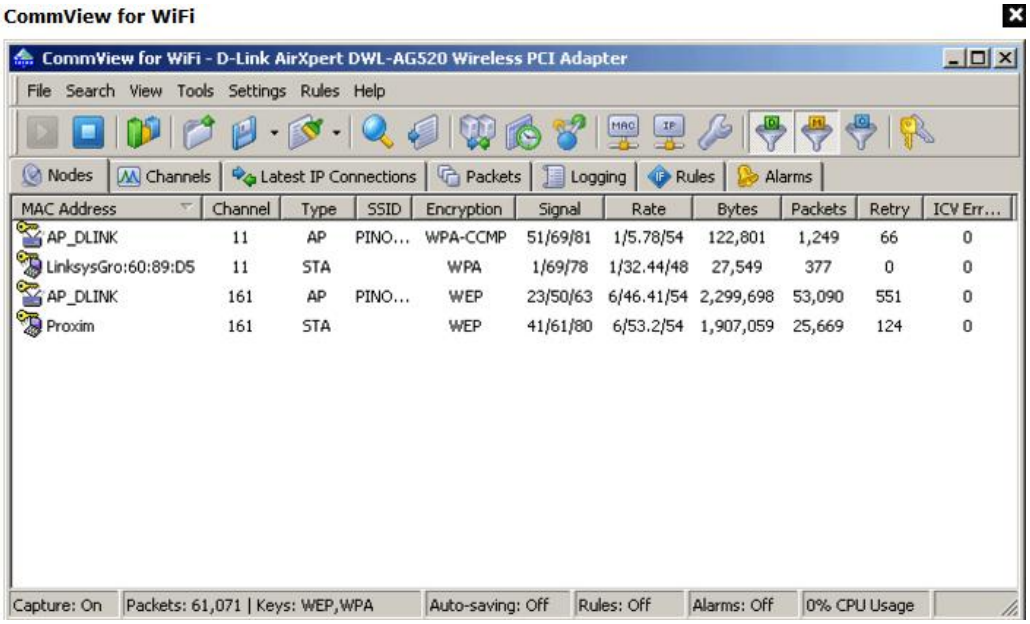


Figura. 6.2. Commview for Wifi

REFERENCIAS BIBLIOGRÁFICAS

[1] Stallings, William, *Comunicaciones y Redes de Computadoras*, Séptima Edición, Pearson Prentice Hall, Madrid, 2004.

[2] http://www.frm.utn.edu.ar/comunicaciones/redes.html.

[3] http://www.forpas.us.es/aula/hardware/dia4_redes.pdf

[4] http://www.mailxmail.com/curso-de-redes-trnasmicion-datos-2/protocolo-lan- arquitectura-topologías

[5] http://www.microsoft.com/spain/technet/recursos/articulos/secmod40.mspx

[6] http://www.canal-ayuda.org/a-informatica/inalambrica.htm

[7] http://es.kioskea.net/contents/wifi/wifiintro.php3

[8] http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/laninalambricas.htm

[9] Archivo_PDF: Capitulo 7[1]

[10] González, Manuel, Ethernet, http://www.monografias.com/trabajos-ppt/ethernet/ethernet.shtml

[11] http://members.multimania.co.uk/baloosoftware/php/docredes/docredes5.pdf

[12] Ponce, Enrique; Molina, Enrique; Mompó, Vicente, Redes Inalámbricas: IEEE 802.11, http://multingles.net/docs/Manual%20-%20Redes%20WiFi%20inalambricas.pdf

[13] http://redesmarisol.blogspot.com/2010_06_01_archive.html

[14] Romero, Claudio, Seguridad en Redes IP, http://www.slideshare.net/thumann/presentacion-4-seguridad-en-redes-ip

[15] http://es.kioskea.net/contents/attaques/attaques.php3

[16] http://www.zonavirus.com/articulos/que-es-el-spoofing.asp

[17] http://msi.wikispaces.com/mo2_mmagliano

[18] http://www.openkiosco.com.ve/popups/vulnerabilidad.html

[19] De las Heras, Jesús Sanz, Ataques de Spam con direcciones falsificadas, http://www.rediris.es/mail/abuso/doc/spam.pdf

[20] http://www.monografias.com/trabajos39/spam-correo-electronico/spam-correo-electronico2.shtml

[21] http://www.fortunecity.es/imaginapoder/artes/368/escuela/telecom/sniffer.htm

[22] http://www.mundocisco.com/2009/08/que-es-un-sniffer.html

[23] http://tutorialesdehacking.mforos.com/1657301/7721675-definicion-de-sniffer

[24] http://www.sekiura.com.py/herramientas/glosario/gusanos-red

[25] http://www.taringa.net/posts/info/9042099/Vulnerabilidades-de-las-redes-WIFI.html

[26] González, Alvaro; Pérez, Pedro, Seguridad en Redes Inalámbricas WiFi, http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf

[27] http://www.esecurityplanet.com/trends/article.php/2200071/Denial-of-Service-a-Big-WLAN-Issue.htm

[28] Arellano, Gabriel; Seguridad en Capa 2; http://www.google.com.ec/url?sa=t&rct=j&q=ataques%20en%20la%20capa%20de%20enlace%2Bseguridades&source=web&cd=3&ved=0CCgQFjAC&url=http%3A%2F%2Fwww.gabriel-arellano.com.ar%2Ffile_download%2F13&ei=Z6KqTvWfIYTGgAfkn_nUDw&usg=AFQjCNERJMsXzZms3kmWpq92rEpPyB2SFA

[29] Agüero, Ramón; Redes Inalámbricas de Área Local y Personal, WLAN: Estándar IEEE 802.11; http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf

[30] http://www.coit.es/descargar.php?idfichero=238

[31] http://dns.bdat.net/seguridad_en_redes_inalambricas/c14.html

[32] http://es.wikipedia.org/wiki/WEP

[33] Escudero, Alberto, Seguridad en Redes Inalámbricas, http://www.eslared.org.ve/tricalcar/12_es_seguridad-inalambrica_guia_v01%5B1%5D.pdf

[34] http://www.virusprot.com/Nt210371.htm

[35] http://dns.bdat.net/seguridad_en_redes_inalambricas/x59.html

[36] http://garelifabrizi.com.ar/hablemosdecomputacion/diferencias-entre-wep-y-wpa-seguridad-wifi

[37] http://wikitel.info/wiki/Capa_de_Control_de_Acceso_al_Medio_(MAC)#Distributed_Coordination_Function_.28DCF.29

[38] http://es.wikipedia.org/wiki/IEEE_802.11

[39] http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi?showall=1

[40] http://dns.bdat.net/seguridad_en_redes_inalambricas/x80.html

[41] http://www.csirtcv.gva.es/es/paginas/herramientas-escaneadoras-y-detectoras-de-vulnerabilidades.html

[42] http://www.gulic.org/almacen/01_www/cosecha/Teresa/Security-HOWTO/Security-HOWTO-latex/Security-HOWTO/node57.html

[43] http://www.segu-info.com.ar/proteccion/deteccion.htm

[44] http://www.ordenadores-y-portatiles.com/intrusion-wifi.html

[45] Asitimbay, Ana María; Técnicas de Detección de Intrusiones como Estrategias de Seguridad en Redes WiFi;

http://www.slideshare.net/UCACUE/tcnicas-de-deteccin-de-instrusiones-como-estrategias-de-seguridad-en-redes-wi-fi

[46] http://sistemasoperativos.angelfire.com/html/5.8.html

[47] Cardinale, Yudith; Tolerancia a Fallas y recuperación; http://ldc.usb.ve/~yudith/docencia/ci-4821/Temas/Tema6-ToleFalyRecupera.pdf

[48] http://www.idg.es/pcworldtech/Analisis-forense.-Como-investigar-un-incidente-de-/art194718-seguridad.htm

[49] http://es.kioskea.net/contents/wifi/wifimodes.php3

[50] http://oscar-carvajal-telecomunicaciones.wikispaces.com/file/view/Marco+Teorico.pdf

[51] Buettrich, Sebastián; Escudero, Alberto; Topología e Infraestructura Básica de Redes Inalámbricas; http://www.it46.se/courses/wireless/materials/es/04_Topologia-Infraestructura/04_es_topologia-e-infraestructura_guia_v01.pdf

[52] Ochoa, Verónica; Commview_Software

[53] Ochoa, Verónica; Wireshark_Software

[54] WLAN, Red Inalámbrica de Área Local; http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/valle_i_lf/capitulo1.pdf

[55] Ochoa, Verónica

[56]http://foro.elhacker.net/hacking_wireless/taller_de_victhor_protocolo_80211_taller_wifi-t261453.0.html

[57] http://www.dea.icai.upcomillas.es/jmatanza/LabComIndAv/3.1.-Intro_Wirehsark.pdf

[58] http://www.dea.icai.upcomillas.es/jmatanza/LabComIndAv/3.1.-Intro_Wirehsark.pdf

[59] http://gratis.portalprogramas.com/Commview-for-WiFi.html

[60] http://www.gratisprogramas.org/descargar/commview-for-wifi-6-1-full-captura-paquetes-de-conexiones-inalambricas/

[61] http://commview-for-wifi.softonic.com/

Sangolquí ___ de Diciembre del 2011

_____

Ing. Edwin Chávez

Director de la Carrera

Ingeniería Electrónica en Telecomunicaciones

_____

Srta. Verónica Ochoa

Autor