ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UNA RED WLAN QUE PERMITA EL ACCESO A LA INTERNET, A LAS PCS DE TODAS LAS AULAS DE LA ESCUELA FISCAL MIXTA "JOSÉ MARÍA VARGAS" UBICADA EN EL BARRIO DE SANTO DOMINGO DE CONOCOTO.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO, EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

VALERIA STEFANIA AGUALONGO MESA
vsam011@hotmail.com

MANUEL ALEJANDRO SALAZAR LÓPEZ
asalazar.consultor.ti@outlook.com

DIRECTOR: ING. CÉSAR GALLARDO
cesar.gallardo@epn.edu.ec

Quito, Febrero 2016

DECLARACIÓN

Nosotros, **VALERIA STEFANIA AGUALONGO MESA** Y **MANUEL ALEJANDRO SALAZAR LÓPEZ**, declaramos bajo juramento que el trabajo aquí descrito es de nuestra total auditoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en el documento.

A través de la presente declaración confiero los derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la ley de propiedad intelectual, por su Reglamento y por la normativa institucional vigente.

VALERIA STEFANIA AGUALONGO MESA

MANUEL ALEJANDRO SALAZAR LÓPEZ

CERTIFICACIÓN

Certifico que el presente trabajo, ha sido desarrollado en su totalidad por: **VALERIA STEFANIA AGUALONGO MESA Y MANUEL ALEJANDRO SALAZAR LÓPEZ** bajo mi supervisión.

ING. CESAR GALLARDO

AGRADECIMIENTO

A ti Dios que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

A mi familia y a todas las personas que de una u otra manera influyeron positivamente en mí para alcanzar esta meta.

Un agradecimiento especialmente al Ing. Cesar Gallardo, por su paciencia, apoyo y motivación para alcanzar esta meta que se ve plasmada en el proyecto de culminación de mi carrera profesional.

A la Escuela José María Vargas por permitir la implementación de este proyecto en la institución que cumple las expectativas de los avances tecnológicos hacia la comunidad educativa.

VALERIA STEFANIA AGUALONGO MESA

AGRADECIMIENTO

A Dios por brindarme la oportunidad de tener una familia maravillosa y gozar de buena salud.

Agradezco a mi familia que están siempre a mi lado apoyándome en mis proyectos personales, laborales y profesionales.

Agradezco al Ing. César Gallardo por su conocimiento y valores instruidos en mi formación como Tecnólogo, a través de su esfuerzo he logrado cumplir exitosamente la elaboración y culminación de este proyecto.

A la Directora de la Escuela José María Vargas, quien brindó su confianza para implementar nuevas tecnologías en su área y ser parte de la solución en su camino de mejora.

A la Escuela Politécnica Nacional por el prestigio otorgado al culminar mis estudios en sus aulas.

MANUEL ALEJANDRO SALAZAR LÓPEZ

DEDICATORIA

Rashel anhelo que sigas mis pasos y logres todo lo que te propongas, este no es un logro personal si no el de todos nosotros, a mis padres, por el apoyo incondicional que me han brindado durante toda la carrera, y a mi querido hermano Cristhian por las palabras de aliento que me supo brindar cuando más necesité.

VALERIA STEFANIA AGUALONGO MESA

DEDICATORIA

A mi familia, que siempre está presente brindándome su apoyo incondicional y gracias a sus valores instruidos cada día puedo cumplir con mis metas.

Esta meta es un logro familiar ya que en el camino de mi formación en la carrera me apoyaron con sus experiencias y consejos.

MANUEL ALEJANDRO SALAZAR LÓPEZ

CONTENIDO

GRÁFICOS

TABLAS

RESUMEN

El objetivo del proyecto es el desarrollo e implementación de una red inalámbrica que será la parte principal de interconectividad para compartir el servicio de internet y recursos tanto de hardware como de software dentro toda la institución.

El primer capítulo contiene un estudio del problema y las posibles soluciones a darse.

En el segundo capítulo contiene estudios teóricos de las redes inalámbricas como por ejemplo la historia, tecnologías existentes, topologías, formas de transmisión, alternativas existentes en cuanto a seguridades.

En el tercer capítulo contiene un análisis técnico de la situación antes de la implementación de la red inalámbrica, así como también requerimientos y características de los equipos que la Institución posee.

En el cuarto capítulo se ha realizado un estudio de los dispositivos Wireless haciendo referencia a sus estándares usados en velocidad de transmisión, alcances y compatibilidad, además se ha tomado una muestra de marcas para realizar un análisis de las tecnologías vigentes en el mercado.

En el quinto capítulo se ejecutará la implementación de la red y las seguridades que permitan obtener una red fiable de ataques y bloquear accesos a la red no autorizados, además de probar la conectividad a la red mediante el uso de sus recursos.

Adicionalmente, se anexado manuales que ayudaran a solventar dudas sobre el manejo de este dispositivo.

PRESENTACIÓN

La utilidad de las redes inalámbricas en el hogar, pequeñas o grandes empresas e instituciones educativas ofrecen ventajas muy considerables.
Con la visión de una red inalámbrica, evitamos considerablemente el instalar cables para conectar los distintos equipos entre si y los portátiles pueden trasladarse de un lado a otro, manteniendo su conexión a la red.

Al conocer la existencia de tantas tecnologías de conexión y transmisión en las redes inalámbricas, en este trabajo se describe y se realiza un análisis de cada una de estas tecnologías, basadas en la norma IEEE 802.11 que constituyen un conjunto de estándares del sector para tecnologías de red de área local inalámbrica (WLAN) compartidas, de los cuales el que utilizamos con mayor frecuencia es IEEE 802.11g y el que está empezando a usarse con regularidad es IEEE 802.11n, también denominados Wi-Fi IEEE 802.11g e IEEE 802.11g que transmiten a 54 Mbps y hasta 600 Mbps en el intervalo de frecuencias ISM(industrial, científico y médico)de banda de 2,4 GHz. Otros dispositivos inalámbricos, como hornos microondas, teléfonos inalámbricos, videocámaras inalámbricas y dispositivos que utilizan otra tecnología inalámbricas denominada Bluetooth, también utilizan ISM de banda.

En condiciones ideales, en situación de proximidad y sin fuentes de atenuación o interferencias, IEEE 802.11g/n funciona a 54 Mbps y hasta 600 Mbps. El estándar IEEE 802.11g/n utiliza frecuencias del intervalo de 2.4 GHz y 5 GHz, incluida la banda de frecuencias ISM de banda C de 5,725 a 5,875 GHz. Esta tecnología de velocidad mayor permite que las redes locales inalámbricas tengan un mejor rendimiento para aplicaciones de videos conferencias y transmisión de información.

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA

La **Escuela José María Vargas** dedicada a formar intelectualmente y moralmente a sus estudiantes, se encuentra al oriente de la ciudad de Quito, como muestra en el Gráfico 1 está en el sector de Conocoto, junto a la autopista General Rumiñahui, institución en la cual la gestión educativa se ha visto afectada por la falta de apoyo tecnológico para instituir la enseñanza diaria.

Gráfico 1.- Ubicación de la Escuela

En el día a día se experimenta un crecimiento acelerado del uso de Internet, el constante desarrollo de la tecnología y la implementación de nuevas plataformas para gestionar aplicaciones en la web, especialmente los diferentes sistemas de validación, corrección y almacenamiento de historiales estudiantiles controlados por el estado, han obligado a las diferentes instituciones educativas de nuestro

país a implementar nuevas tecnologías para optimizar la conexión y transmisión de datos.

Actualmente se experimenta un proceso de implementaciones para estar a la par con las exigencias gubernamentales, pero no todas las instituciones tienen la facilidad para instalar nuevas tecnologías a la medida, como es el caso de la **Escuela José María Vargas**, la misma que no cuenta con la infraestructura adecuada para hacer uso de estas nuevas tecnologías, motivo por el cual genera varios inconvenientes en los diferentes procesos de enseñanza a los alumnos y control de registro académico, basándonos en estos criterios podemos mencionar los siguientes problemas que experimenta la institución:

- Para ingresar datos de diferente índole a las plataformas que posee el Ministerio de Educación, los docentes no cuentan con el servicio de internet en cada aula.
- Para cumplir con los requerimientos distritales de educación, como el registro de notas a plataformas gubernamentales, informes educativos de rendimiento entre otras; los docentes dejan de ejecutar varias tareas importantes relacionadas con el desarrollo intelectual de los estudiantes.
- La institución tiene acceso a Internet, pero solo el Laboratorio de Computación mediante una red de cableado estructurado y equipos con de bajo rendimiento que limitan la eficiencia en las consultas y carga de información.

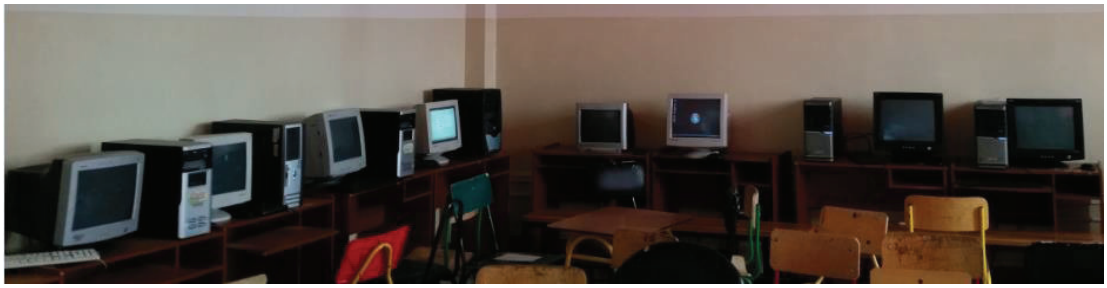


Gráfico 2.- Centro de cómputo

- Los docentes deben recurrir a métodos ineficientes para completar la carga de esta información.

- Los estudiantes no desarrollan destrezas necesarias para el dominio de las herramientas en línea, lo cual condiciona a los estudiantes su conocimiento de nuevas tecnologías para el tratamiento de la información, afectando su formación estudiantil y posteriormente su vinculación laboral.
- El laboratorio de computación experimenta atenuación en la conexión a internet mediante la red de cableado.
- Los estudiantes no desarrollan el dominio de las herramientas en línea la cual permite a los niños y jóvenes tener un mayor espectro. Es decir en la medida que tengan más alfabetización tecnológica les ayudará para el tema del empleo, sobre todo porque estamos en una sociedad de la información y conocimiento.
- Cuenta con un dispositivo inalámbrico que no tiene la suficiente capacidad para abastecer el área hábil de la institución.

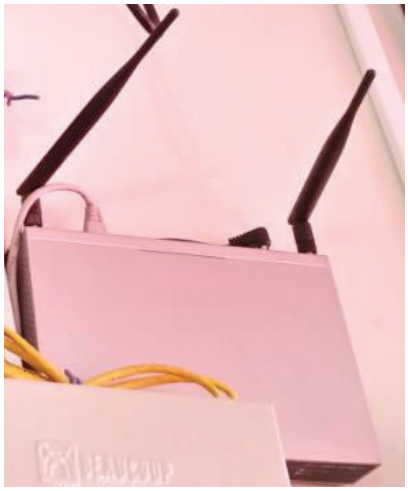


Gráfico 3.- Dispositivo inalámbrico no eficiente

- Por la irregularidad topográfica donde se ubica las instalaciones de la institución, para cada estación situada dentro de las aulas, es inestable hacer uso de una red de cableado estructurado, esto se debe a que es completamente complejo implementar este tipo de red ya que las condiciones de infraestructura dificultan adecuada implementación.

Gráfico 4.- Área 1

Gráfico 5.- Área 2

En consideración a la problemática expuesta, se propone como mejor opción la implementación de una red con acceso inalámbrico (WLAN) la cual permita integrar a un servicio de conexión permanente, compartiendo diferentes servicios.

1.1. NECESIDAD

La **Escuela José María Vargas** a diario presta una enseñanza-aprendizaje con metodologías y tecnologías significativas que desarrollen las destrezas con criterio de desempeño, para formar estudiantes competentes que se involucren en las diferentes actividades productivas y se conviertan en sujetos pro-sociales.

Dentro de una superficie de 1000 m² las aulas están distribuida de forma horizontal y vertical, pero no han sido correctamente ubicadas, por este principal motivo se puede evidenciar que no se alinea a un diseño efectivo y eficiente para montar una red de cableado estructurado.

El conjunto de aulas existentes no poseen una construcción previamente diseñada, con el pasar del tiempo la construcción de aulas no ha sido contralada adecuadamente, basándonos en este criterio se explica este inconveniente. (Ver Anexo 1)

Al percibir la necesidad primordial de usar el servicio de internet se ha optado por entregar un acceso que no sea del uso de una red de cableado estructurado por su irregularidad en la distribución de su espacio físico, afirmando así la necesidad de implementar tecnologías de conectividad inalámbricas para salida hacia el internet, con la que se pretende que los docentes y alumnos puedan acceder al servicio.

Para brindar los beneficios que este tipo de enlace ofrece, es de suma importancia comprender a fondo el estándar a implementarse (802.11 a/b/g/n), ya que esto es una necesidad para la investigación e implementación de redes.

Para realizar una apropiada implementación de una red inalámbrica, es necesario una efectiva planificación de recursos y un correcto criterio de instalación, por lo tanto, se deben tomar en cuenta diferentes elementos asociados con:

- **Cobertura inadecuada.-** dependiendo del entorno donde funcionará, puede afectar los accesos si no se establece una ubicación estratégica para la distribución y disponibilidad del servicio.
- **Flexibilidad.-** la solución de conectividad debe estar en la capacidad de crecer de acuerdo a una proyección de necesidades en el establecimiento.

- **Seguridad.**- controlar con estándares internacionales la conexión de nuevos dispositivos, aspectos que se desarrollaran más adelante en este documento.

1.1.1. CARACTERÍSTICAS DE EQUIPOS DEL CENTRO EDUCATIVO

- Cantidad: 11 estaciones de trabajo.
- Sistema Operativo: Windows XP Service Pack 2
- Equipos integrados por un procesador INTEL Pentium
- Para cada estación se usa 512 Mb de memoria RAM.
- Un disco duro de 40 GB para todos los equipos.
- Monitores de 15" de modelo cónico.

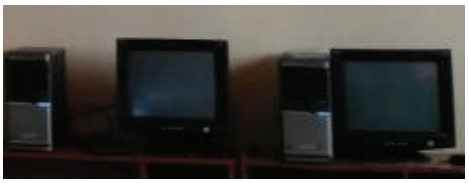


Gráfico 6.- Equipos actuales

1.2. OBJETIVOS DEL PROYECTO

1.2.1. OBJETIVO GENERAL

- Proveer el servicio de acceso a internet a todas las PC's de las aulas de la Escuela José María Vargas de la parroquia de Conocoto, mediante a implementación de una red WLAN.

1.2.2. OBJETIVOS ESPECÍFICOS

- Determinar la situación actual de la Escuela José María Vargas en el barrio Santo Domingo de Conocoto.
- Determinar las diferentes tecnologías existentes en el mercado que permitan interconectar las PC's en una red WLAN.
- Analizar las alternativas tecnológicas y determinar la mejor, que permita dar solución a los problemas detectados.
- Implementar la red WLAN y su conexión a internet.

1.3. ALCANCE

La primordial razón de la implementación es la conexión a internet de ésta manera se mejorará la infraestructura tecnológica, garantizando la conexión permanente, fácil acceso, cumpliendo con el compromiso de conectividad y disponibilidad.

Es necesario tomar en cuenta que el presente proyecto ha considerado seguridad de alto nivel cumpliendo así los estándares establecidos por el gobierno y adicional asegurar el acceso con autorización y autenticación, con el fin de garantizar la estabilidad de la red para la instalación.

1.3.1. INTERCONECTIVIDAD ENTRE ESTACIONES

La interconectividad entre estaciones asegura la disponibilidad de información, a través de una transmisión de 54Mbps y las mismas estarán comunicadas con el objetivo de compartir recursos tanto de hardware y software dentro de la institución.

1.3.2. NESECIDAD DE USO DEL INTERNET

El servicio de internet es una herramienta necesaria para cumplir parte de las tareas habituales, por este motivo cada estación tendrá acceso al internet a través del dispositivo de acceso inalámbrico. Gracias al internet la información se la pueda compartir íntegramente en cualquier lugar.

1.3.3. SERVICIO DINÁMICO PARA DISTRIBUCIÓN DE LA CONEXIÓN AL INTERNET

Una de las características que tiene el dispositivo inalámbrico es el servicio DHCP, el cual se lo puede definir como un protocolo de tipo cliente/servidor en el que generalmente posee una lista de direcciones IP que son asignadas dinámicamente a cada estación que se conecte al dispositivo.

Todo este contenido se desarrollará y describirá especificaciones en el Capítulo 4.

CAPÍTULO 2

FUNDAMENTO TEÓRICO

En estos tiempos se está viviendo la revolución tecnológica, en donde se ha visto un gran avance en las tecnologías inalámbricas. Esta revolución se considera como una importancia similar a la que se dio cuando apareció el Internet. Poco a poco las redes inalámbricas, se están introduciendo en el mercado de consumo gracias a su facilidad de acceso tanto en costos, como también en infraestructura.

2.1. RESEÑA HISTORICA DE LAS REDES

Se considera que la teoría de redes tuvo su inicio con el matemático suizo Leonhard Euler que planteó el curioso problema de los siete puentes sobre el río Pregel de la ciudad prusiana de Kaliningrado: ¿es posible dar un paseo comenzando por cualquiera de las cuatro partes de tierra, cruzando cada puente una sola vez y volviendo al punto de partida? Euler representó cada parte de tierra por un punto y cada puente por una línea, haciendo la siguiente pregunta: ¿se puede recorrer el dibujo sin repetir las líneas?.

Ya en el siglo XX, la teoría de grafos cobró un nuevo impulso gracias a la intervención de especialistas en psiquiatría y antropología social que introdujeron el concepto de análisis de redes sociales en los años treinta del siglo pasado

(Moreno, 1934). Pero el verdadero desarrollo en redes sociales se llevó a cabo con la introducción de medidas destinadas a la obtención de patrones de conexiones sociales que enlazaran conjuntos de actores en psicología para detectar grupos sociales (interrelación de actores) o las posiciones de los actores en la red (detección de actores estructuralmente similares) (Molina, 2001; Rodríguez, 1995). También fue Moreno el introductor de la primera representación gráfica de una matriz de datos para el análisis de patrones psicológicos, el sociograma.

Desde el punto de vista de la abstracción o la información visual, el sociograma presenta ventajas sobre la información meramente numérica o tabular, ya que hace posible transmitir la información estructural de la red de forma sencilla y destacar la relevancia de los distintos actores que la conforman. La introducción generalizada de ordenadores personales en la década de los ochenta facilitó la aplicación de técnicas de agrupamiento de los datos y permitió la reproducción de sociogramas de forma rápida.

2.2. DEFINICIÓN DE REDES DE COMPUTADORAS[1]

Una red informática se define a un conjunto de equipos conectados entre sí, que envían y reciben impulsos eléctricos, ondas electromagnéticas o similares con el fin de transportar datos.

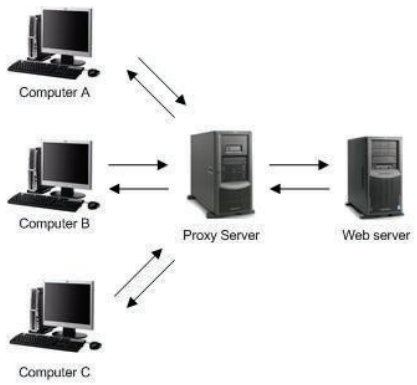


Gráfico 7.- Esquema de una Red de Computadoras[2]

En el gráfico 1 muestra un ejemplo común de una red de computadoras. En esta red, una de las computadoras se denomina servidor. El servidor es por lo general una computadora con mayor capacidad de almacenamiento y velocidad que las otras computadoras, sirve de medio para la comunicación entre las computadoras A, B y C, el cual contiene los programas de administración de la red y almacena datos comunes y particulares de las personas suscritas a la red. El hardware y el software requerido dependen del tipo de red.

[1] (Groth & Skandier, 2005)
[2] (HOME-NETWORK, 2014)

2.3. TOPOLOGÍA DE RED[3]

Es la configuración o forma que adoptan las interconexiones entre equipos. Antes de describir las topologías más comunes, es conveniente aclarar que se puede hablar de topología física y lógica.

Como estén conectados y dispuestos los equipos desde un punto de vista físico y visual y otra cosa en como entiendan esos equipos que están conectados entre sí a un nivel lógico. Por esta razón puede ocurrir que los computadores de una red estén enlazados con un cable formando una estrella y sin embargo se comuniquen entre ellos a través de un bus que pudiera estar localizado en uno de los equipos.

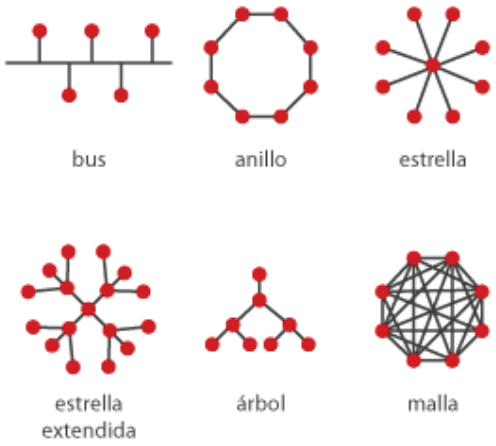


Gráfico 8.- Topologías de red[4]

2.3.1. TOPOLOGÍA EN MALLA[5]

Se utiliza cuando no puede existir ninguna interrupción en las comunicaciones. De modo que, cada equipo tiene sus propias conexiones con los demás equipos. Esto también se refleja en el diseño de Internet, que tiene múltiples rutas hacia cualquier ubicación evidentemente es la topología más cara por la cantidad de cableado y de dispositivos de

[3] (Carmen de Pablos, 2004)
[4] (RengerTH, 2013)
[5] (Pablo Gil Vázquez, 2010)

conexión necesarios. Suele establecerse entre equipos que necesitan conexión ininterrumpida.

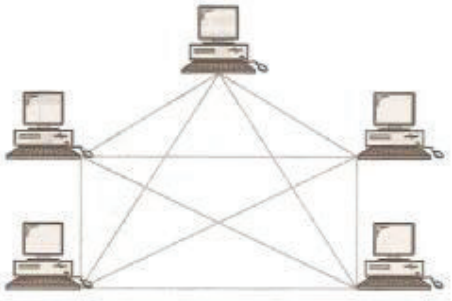


Gráfico 9.- Topología de malla[6]

2.3.2. TOPOLOGÍA EN ESTRELLA

Conecta a todos los equipos a un equipo central mediante una conexión punto a punto.

Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

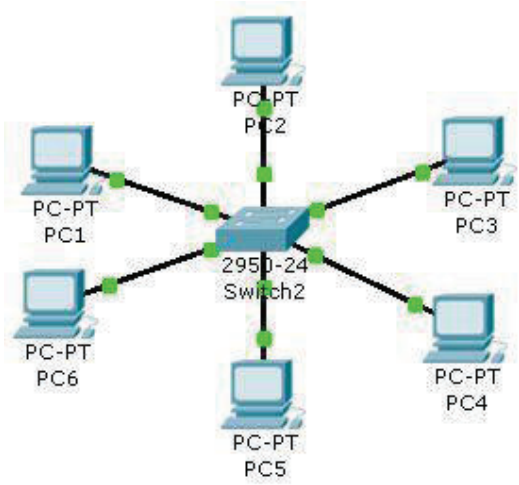


Gráfico 10.- Topología en estrella[7]

[6] (Infoepo11, 2012)
[7] (Fernández, 2012)

2.3.3. TOPOLOGÍA EN BUS

Todos los dispositivos están conectados a un cable central llamado bus o backbone utiliza un único segmento al que todos los equipos se conectan directamente. Su mayor inconveniente es que si un enlace falla, falla toda la red.

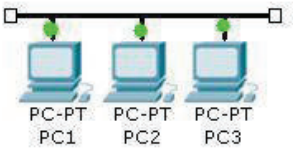


Gráfico 11.- Topología en bus[8]

2.3.4. TOPOLOGÍA EN ANILLO

Esta topología conecta un equipo con el siguiente, y el último con el primero, es decir, se forma un círculo de conexiones punto a punto entre equipos contiguos. El protocolo de comunicaciones debe evitar situaciones conflictivas a la hora de utilizar el medio compartido.

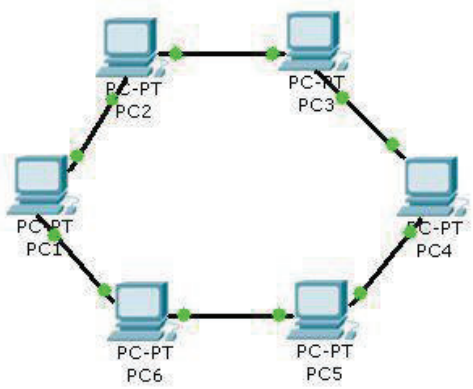


Gráfico 12.- Topología en Anillo[9]

2.3.5. TOPOLOGÍA EN ÁRBOL

Todas las estaciones están conectadas a un ordenador central y se conectan entre ellas a través de los Hubs que haya instalados.

[8] (Fernández, 2012)
[9] (Fernández, 2012)

Gráfico 13.- Topología en árbol[10]

2.4. TIPOS DE REDES

Una red informática tiene distintos tipos de clasificación dependiendo de su estructura o forma de transmisión, entre los principales tipos de redes están los siguientes:

2.4.1. REDES POR ALCANCE[11]

Este tipo de red se nombra con siglas según su área de cobertura: una red de área personal o **PAN (Personal Área Network)** es usada para la comunicación entre dispositivos cerca de una persona; una **LAN (Local Área Network)**, corresponde a una red de área local que cubre una zona pequeña con varios usuarios, como un edificio u oficina. Para un campus o base militar, se utiliza el término **CAN (Campus Área Network)**. Cuando una red de alta velocidad cubre un área geográfica extensa, hablamos de **MAN (Metropolitan Área Network)** o **WAN (Wide Área Network)**. En el caso de una red de área local o LAN, donde la distribución de los datos se realiza de forma virtual y no por la simple direccionalidad del cableado, hablamos de una **VLAN (Virtual LAN)**. También cabe mencionar las **SAN (Storage Área Network)**, concebida para conectar servidores y matrices de discos y las Redes Irregulares, donde los cables se conectan a través de un módem para formar una red.

[10] (Colin, 2010)
[11] (Xavier Hesselbach Serra, 2002)

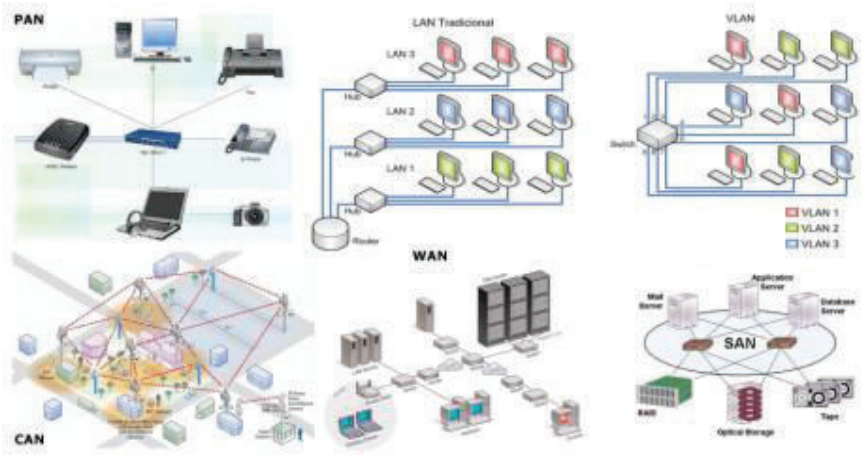


Gráfico 14.- Redes[12]

2.4.2. REDES POR TIPO DE CONEXION

El tipo de red varía dependiendo si la transmisión de datos es realizada por medios guiados como cable coaxial, par trenzado o fibra óptica, o medios no guiados, como las ondas de radio, infrarrojos, microondas u otras transmisiones por aire.

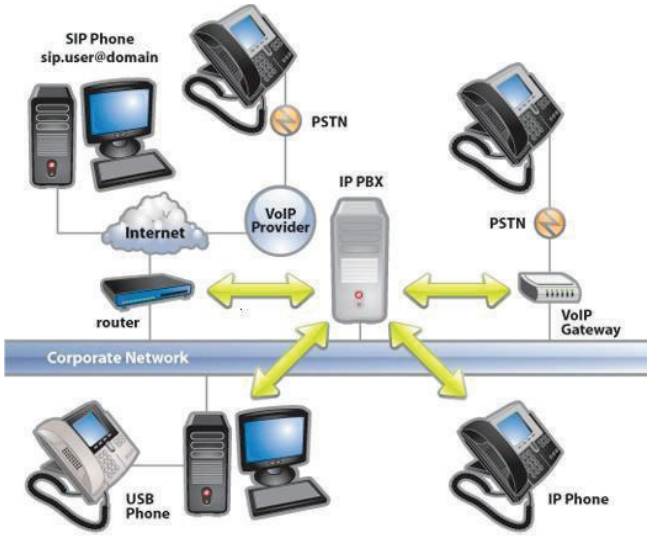


Gráfico 15.- Tipos de conexión[13]

[12] (Henriquez, 2011)
[13] (Orellana, 2011)

2.4.3. REDES POR RELACION FUNCIONAL

Ocurre al solicitar información un cliente o usuario al servidor que le da respuesta se la llama Relación Cliente/Servidor, en cambio cuando en dicha conexión una serie de nodos operan como iguales entre sí, sin cliente ni servidores, hablamos de Conexiones Peer to Peer o P2P.

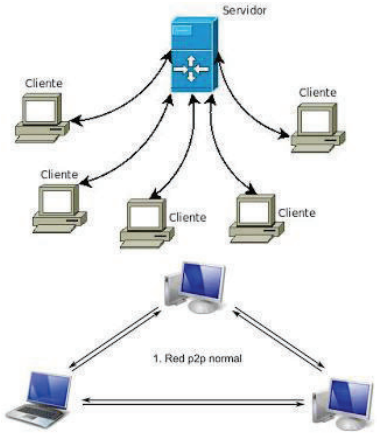


Gráfico 16.- Relación funcional[14]

2.4.4. REDES POR DIRECCIONALIDAD DE DATOS

Al actuar un equipo como emisor en forma unidireccional se llama Simplex, si la información es bidireccional pero solo un equipo transmite a la vez, es una red Half-Duplex o Semi-Duplex, y si ambos equipos envían y reciben información simultáneamente hablamos de una red Full Duplex.

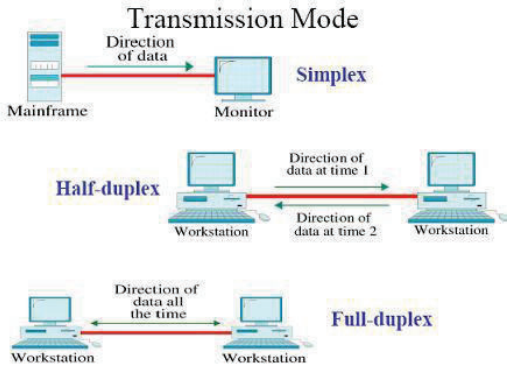


Gráfico 17.- Modo de transmisión[15]

[14] (Johan, 2010)
[15] (Henriquez, 2011)

2.4.5. REDES SEGÚN GRADO DE AUTENTIFICACIÓN

Redes Privadas y Redes de Acceso Público, son 2 tipos de redes clasificadas según el grado de autentificación necesario para conectarse a ella. De este modo una red privada requiere el ingreso de claves u otro medio de validación de usuarios, una red de acceso público en cambio, permite que dichos usuarios accedan a ella libremente.

2.4.5.1. Según grado de difusión

Otra clasificación similar a la red por grado de autentificación, corresponde a la red por Grado de Difusión, pudiendo ser Intranet o Internet. Una intranet, es un conjunto de equipos que comparte información entre usuarios validados previamente, Internet en cambio, es una red de alcance mundial gracias a que la interconexión de equipos funcionan como una red lógica única, con lenguajes y protocolos de dominio abierto y heterogéneo.

2.4.5.2. Redes según servicio o función

Por último, según Servicio o Función de las Redes, se pueden clasificar como Redes Comerciales, Educativas o Redes para el Proceso de Datos.

2.5. MODELOS DE REFERENCIA[16]

Constituyen un modo de informar a los diseñadores sobre la estructura general de esta clase de sistemas. Los modelos de referencia normalmente se obtienen a partir de un estudio del dominio de la aplicación. Representan una arquitectura ideal que incluye todas las características que los sistemas podrían incorporar.

2.5.1. EL MODELO DE REFERENCIA OSI[17]

El modelo OSI (Open Systems Interconnection) fue creado por la ISO y se encarga de la conexión entre sistemas abiertos, esto es, sistemas abiertos a la comunicación con otros sistemas. Los principios en los que basó su

[16] (WETHERALL, 2012)
[17] (UNICEN, 2015)

creación eran: una mayor definición de las funciones de cada capa, evitar agrupar funciones diferentes en la misma capa y una mayor simplificación en el funcionamiento del modelo en general.

Este modelo divide las funciones de red en siete capas diferenciadas:

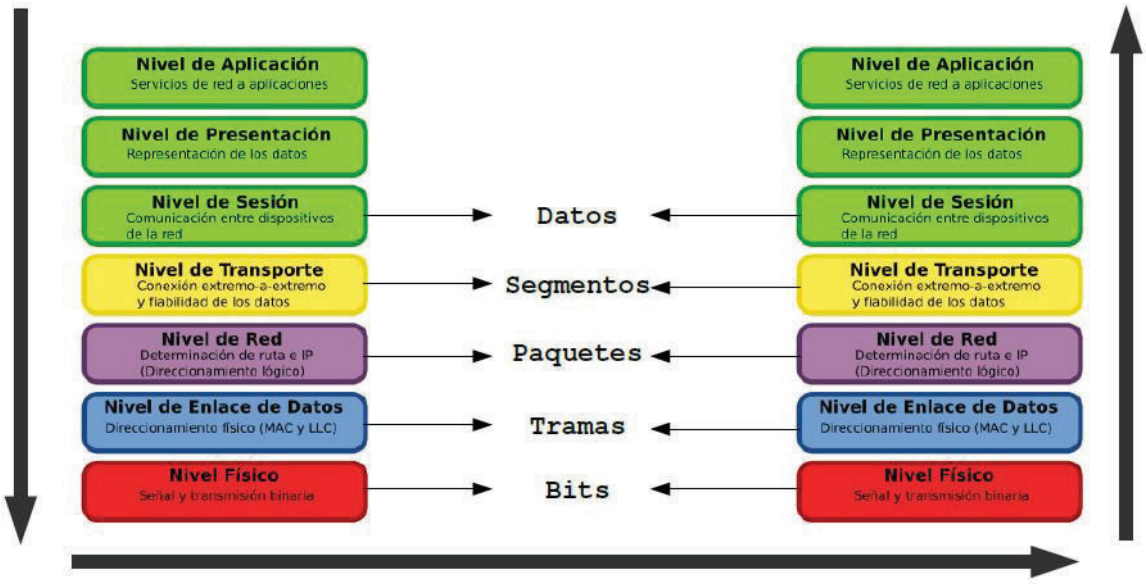


Gráfico 18.- Modelo OSI[18]

2.5.2. MODELO TCP/IP[19]

Este modelo fue manipulado en ARPANET y es utilizado actualmente a nivel global en Internet y redes locales. Su nombre deriva de la unión de los nombres de los dos principales protocolos que lo conforman: TCP en la capa de transporte e IP en la capa de red y se compone de cuatro capas descritas en la siguiente imagen:

[18] (Rodríguez, 2013)
[19] (Microsoft, 2005)

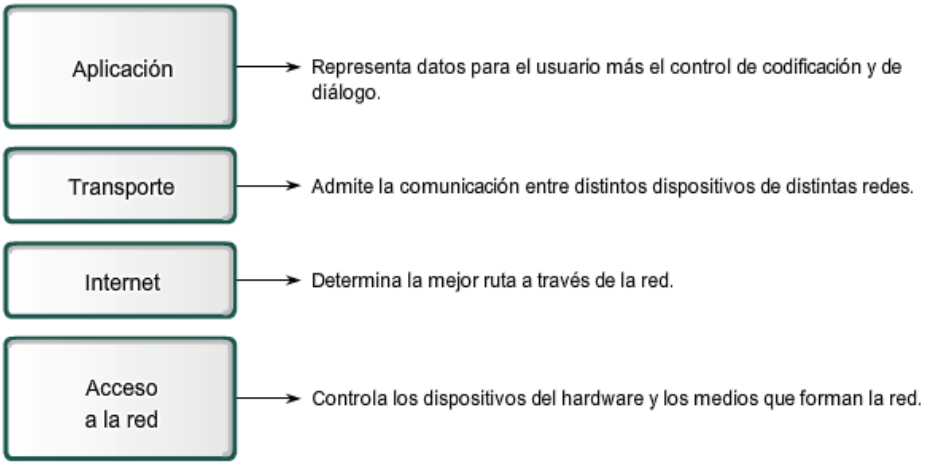


Gráfico 19.- Modelo TCP/IP[20]

2.5.3. MEDIOS DE TRANSMISIÓN

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos. Distinguimos dos tipos de medios: guiados y no guiados. En ambos casos la transmisión se realiza por medio de ondas electromagnéticas.

Los medios guiados conducen (guían) las ondas a través de un camino físico, ejemplos de estos medios son el cable coaxial, la fibra óptica y el par trenzado. Los medios no guiados proporcionan un soporte para que las ondas se transmitan, pero no las dirigen; como ejemplo de ellos tenemos el aire y el vacío.

La naturaleza del medio junto con la de la señal que se transmite a través de él constituye los factores determinantes de las características y la calidad de la transmisión. En el caso de medios guiados es el propio medio el que determina las limitaciones de la transmisión: velocidad de transmisión de los datos, ancho de banda que puede soportar y espaciado entre repetidores. Sin embargo, al utilizar medios no guiados resulta más determinante en la transmisión el espectro de frecuencia de la señal producida por la antena que el propio medio de transmisión.

[20] (Jomix, 2011)

Algunos medios de transmisión guiados son:

2.5.3.1. Pares trenzados

Este consiste en dos alambres de cobre aislados, en general de 1mm de espesor. Los alambres se entrelazan en forma helicoidal, como en una molécula de DNA. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor. Los pares trenzados se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende del calibre del alambre y de la distancia que recorre; en muchos casos pueden obtenerse transmisiones de varios megabits, en distancias de pocos kilómetros. Debido a su adecuado comportamiento y bajo costo, los pares trenzados se utilizan ampliamente y es probable que se presencia permanezca por muchos años.

2.5.3.2. Cable coaxial

El cable coaxial consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante. Este material aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector.

La construcción del cable coaxial produce una buena combinación y un gran ancho de banda y una excelente inmunidad al ruido. El ancho de banda que se puede obtener depende de la longitud del cable; para cables de 1km, por ejemplo, es factible obtener velocidades de datos de hasta 10Mbps, y en cables de longitudes menores, es posible obtener velocidades superiores. Se pueden utilizar cables con mayor longitud, pero se obtienen velocidades muy bajas. Los cables coaxiales se emplean ampliamente en redes de área local y para transmisiones de largas distancia del sistema telefónico.

2.5.3.3. Fibra óptica

Un cable de fibra óptica consta de tres secciones concéntricas. La más interna, el núcleo, consiste en una o más hebras o fibras hechas de cristal o plástico. Cada una de ellas lleva un revestimiento de cristal o plástico con propiedades ópticas distintas a las del núcleo. La capa más exterior, que recubre una o más fibras, debe ser de un material opaco y resistente.

Un sistema de transmisión por fibra óptica está formado por una fuente luminosa muy monocromática (generalmente un láser), la fibra encargada de transmitir la señal luminosa y un fotodiodo que reconstruye la señal eléctrica.

Algunos medios no guiados:

2.5.3.4. Radio enlaces de VHF y UHF

Estas bandas cubren aproximadamente desde 55 a 550 Mhz. Son también omnidireccionales, pero a diferencia de las anteriores la ionosfera es transparente a ellas. Su alcance máximo es de un centenar de kilómetros, y las velocidades que permite del orden de los 9600 bps. Su aplicación suele estar relacionada con los radioaficionados y con equipos de comunicación militares, también la televisión y los aviones.

2.5.3.5. Microondas

Además de su aplicación en hornos, las microondas nos permiten transmisiones tanto terrestres como con satélites. Dada sus frecuencias, del orden de 1 a 10 Ghz, las microondas son muy direccionales y sólo se pueden emplear en situaciones en que existe una línea visual que une emisor y receptor. Los enlaces de microondas permiten grandes velocidades de transmisión, del orden de 10 Mbps.

2.6. ESTANDARIZACIÓN DE REDES INALÁMBRICAS[21]

La diferencia principal entre la mayoría de los estándares inalámbricos es su definición.

- Definición de las especificaciones técnicas.
- Definición de los productos actuales.
- Definición de las aplicaciones.

Wi-Fi, Bluetooth y Zig-Bee representan diferentes etapas de desarrollo y ofrecen varios niveles de funcionalidad. El truco es ajustar sus expectativas de acuerdo al nivel de definición y entonces determinar cómo es que cada uno se ajusta al mundo multilenguaje de una infraestructura inalámbrica.

2.6.1. CATEGORIAS IEEE 802[22]

Es un proyecto que empezó en febrero de 1980 (802) se desarrolló paralelamente con el modelo OSI pero es específicamente para el hardware. El proyecto 802 define aspectos relacionados al cableado físico y transmisión de datos correspondiente a las capas físicas y enlace de datos. Los estándares OSI y IEEE 802 fueron desarrollados simultáneamente y en cooperación debido a que comparten características e interactúan muy bien. Se dividen en 12 categorías:

802.1	Supervisión y arquitectura de LAN's
802.2	Control lógico de enlace
802.3	Ethernet
802.4	Token bus (se utilizó por un corto tiempo en plantas manufactureras)
802.5	Token ring (entrada de IBM al mundo de las LANs)
802.6	Cola dual , bus (primera red de área metropolitana)
802.7	Grupo de consultoría técnico de tecnologías de banda anche
802.8	Grupo de consultoría de tecnologías de fibra óptica

[21] (Andreu, Redes inalámbricas (Servicios en red), 2011)
[22] (José Manuel Huidobro, 2005)

802.9	LAN's síncrona (para aplicaciones de tiempo real)
802.10	LAN's virtuales y seguridad
802.11	LAN's inalámbricas
802.12	Demanda de prioridad (AnyLAN de Hewlett-Packard)

Tabla 1.- Categorías IEEE 802

2.6.2. PROTOCOLOS[23]

2.6.2.1. Estándar IEEE 802.11 Legacy

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

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas.

Una de las mayores debilidades de este estándar fue que dejaba mucha libertad de implementación a los proveedores de equipos, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

2.6.2.2. Estándar IEEE 802.11b

La revisión 802.11b del estándar original fue ratificada en junio del 1999, su velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar

[23] (Bernhard H. Walke, 2007)

es de aproximadamente 5.9 Mbits/s sobre TCP y 7.1 Mbit/s sobre UDP. El problema es que al ser esta un frecuencia sin regulación se podría causar interferencias con hornos microondas, teléfonos móviles y otros aparatos que funcione con la misma frecuencia, sin embargo si las instalaciones 802.11b están a una distancia razonable de otros elementos, estas interferencias son fácilmente evitables, aunque esto suponga utilizar una frecuencia sin regulación.

2.6.2.3. Estándar IEEE 802.11a

La revisión 802.11a al estándar original fue ratificada en 1999, utiliza en mismo protocolo de base que es estándar original, opera en la banda 5GHz con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. la velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede utilizar equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 GHz tiene gran uso, el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a únicamente puntos en línea de vista con lo que se hace necesario la instalación de un mayor número de puntos de acceso. Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas se catalogan como débiles bajo estas condiciones.

2.6.2.4. Estándar IEEE 802.11g

En Junio de 2003 se ratificó un estándar de modulación: 802.11g. Este nuevo estándar intenta aprovechar lo bueno de cada uno de los anteriores 802.11a y 802.11b. La 802.11g permite velocidades de hasta 54 Mbits/s y utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o

cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a.

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

2.6.2.5. Estándar IEEE 802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a esto, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

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

En la actualidad la mayoría de productos son de la especificación b o g, sin embargo ya se ha ratificado el estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen el estándar N con un máximo de 600 Mbps (80-100 estables). Hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz y las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la

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

Sin duda esta es la principal ventaja que diferencia wifi de otras tecnologías propietarias, como LTE, UMTS y Wimax, las tres tecnologías mencionadas, únicamente están accesibles a los usuarios mediante la suscripción a los servicios de un operador que está autorizado para uso de espectro radioeléctrico, mediante concesión de ámbito nacional. Se conoce que el futuro estándar sustituto de 802.11n será 802.11ac con tasas de transferencia superiores a 1 Gb/s.

2.7. SEGURIDAD EN REDES INALÁMBRICAS[24]

La seguridad para WLAN se basa en el control de acceso y en la privacidad. La utilización de medidas estrictas de control de acceso a la WLAN ayuda a garantizar que los puntos de acceso de cada estación sean confiables y que no tengan acceso personas no autorizadas. Es necesario dar una clave para que pueda ser utilizado solo el destinatario deseado.

Para proteger una red inalámbrica, hay tres acciones que pueden ayudar:

- Proteger los datos durante su transmisión mediante el cifrado. Traduce los datos a un lenguaje indescifrable que sólo el destinatario indicado comprende. El cifrado requiere que tanto el remitente como el destinatario tengan una clave para decodificar los datos transmitidos.
- Desalentar a los usuarios no autorizados mediante autenticación. Los nombres de usuario y las contraseñas son la base de la autenticación, pero otras herramientas pueden hacer que la autenticación sea más segura y confiable. La mejor autenticación es la que se realiza por usuario, por autenticación mutua entre el usuario y la fuente de autenticación.

[24] (Alan Holt, 2010)

- Impedir conexiones no oficiales mediante la eliminación de puntos de acceso dudosos.

Un empleado bienintencionado que goza de conexión inalámbrica en su hogar podría comprar un Access Point barato y conectarlo al zócalo de red sin pedir permiso. A este Access Point se le denomina dudoso, y la mayoría de estos puntos de acceso los instalan empleados, no intrusos maliciosos.

2.7.1. FIREWALL[25]

Es un sistema que permite proteger a una computadora o una red de computadoras de los intrusos que provienen de una tercera red (expresamente de Internet). Permite filtrar los paquetes de datos que andan por la red. Se trata de un "puente angosto" que filtra, al menos, el tráfico entre la red interna y externa.

Un firewall puede ser un programa (software) o un equipo (hardware) que actúa como intermediario entre la red local (o la computadora local) y una o varias redes externas.

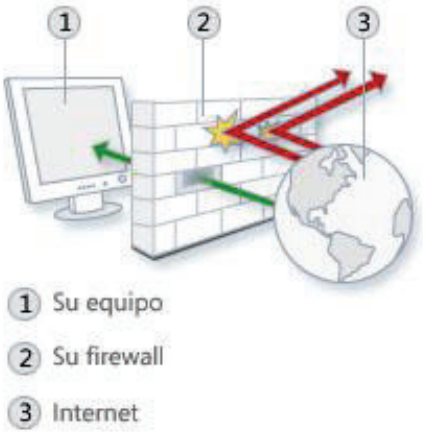


Gráfico 20.- Firewall[26]

[25] (Liu, 2011)
[26] (Microsoft, 2015)

Un sistema firewall contiene un conjunto de reglas predefinidas que permiten:

- Autorizar una conexión (allow);
- Bloquear una conexión (deny);
- Redireccionar un pedido de conexión sin avisar al emisor (drop).

El conjunto de estas reglas permite instalar un método de filtración dependiente de la política de seguridad adoptada por la organización. Se distinguen habitualmente dos tipos de políticas de seguridad que permiten:

- Permitir únicamente las comunicaciones autorizadas explícitamente: "Todo lo que no es autorizado explícitamente está prohibido".
- Impedir cualquier comunicación que fue explícitamente prohibida.

El primer método es el más seguro, pero requiere de una definición precisa de las necesidades de comunicación de toda la red.
Los Firewall pueden ser implementados en hardware o software, o una combinación de ambos. Los Firewall se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. También es frecuente conectar al Firewall a una tercera red, llamada (Zona Desmilitarizada) o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

2.7.2. Pre-RSNA - RSNA

Con la adición de la enmienda IEEE 802.11i en 2004, IEEE 802.11 ofrece dos clases generales de las capacidades de seguridad de IEEE 802.11 WLAN.

- La primera clase, seguridad pre-RSN, incluye las capacidades de seguridad que es un legado de los desarrollados. Como se define en la especificación IEEE 802.11 original el sistema abierto o de autenticación de clave compartida para la validación de la identidad

de una estación inalámbrica, y WEP para la protección de la confidencialidad de tráfico.

- La segunda clase de capacidades de seguridad incluye una serie de mecanismos de seguridad para crear RSN. Un RSN incluye mejoras de seguridad para hacer frente a todos los defectos conocidos de WEP y proporcionar una sólida protección para el enlace inalámbrico, incluidas la integridad y confidencialidad de datos.

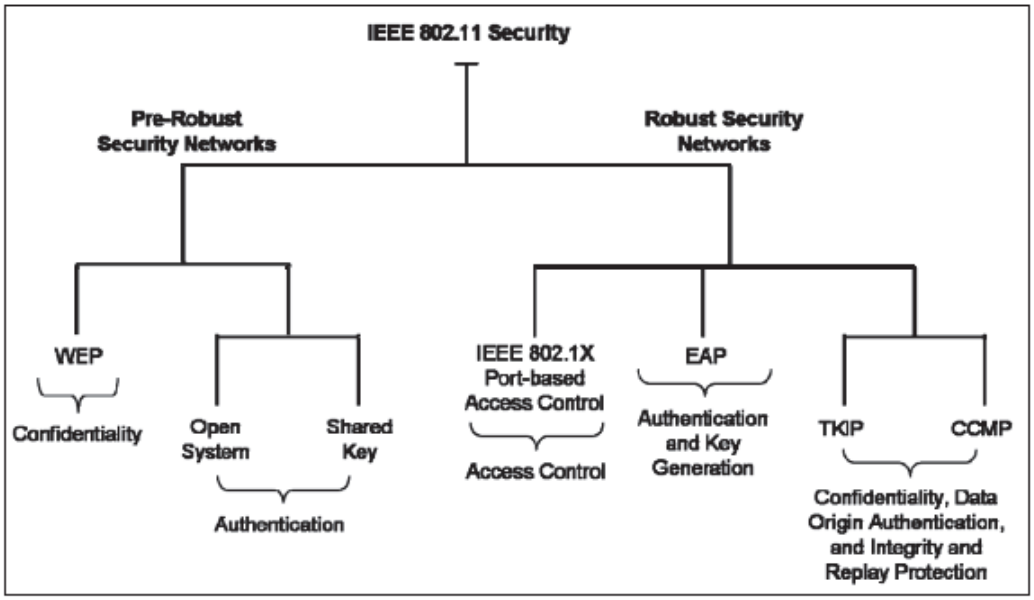


Gráfico 21.- Taxonomía para Pre-RSN y RSN[27]

2.7.3. FASES DE LA OPERACIÓN DEL IEEE 802.11 RSN

El funcionamiento RSN puede ser pensado como ocurre en cinco fases distintas, algunas de las cuales también se producen en pre-RSN IEEE 802.11 durante el proceso de las implementaciones. En el Gráfico 32 se muestra las fases en una configuración de modo de infraestructura y los asigna a los componentes de la red WLAN que intervienen en cada fase, así como las estaciones finales fuera de la RSN WLAN en el sistema de distribución (por ejemplo, otros equipos de la red por cable). Los rectángulos representan la secuencia de fotogramas entre los componentes de red.

[27] (National Institute of Standards and Technology, 2007)

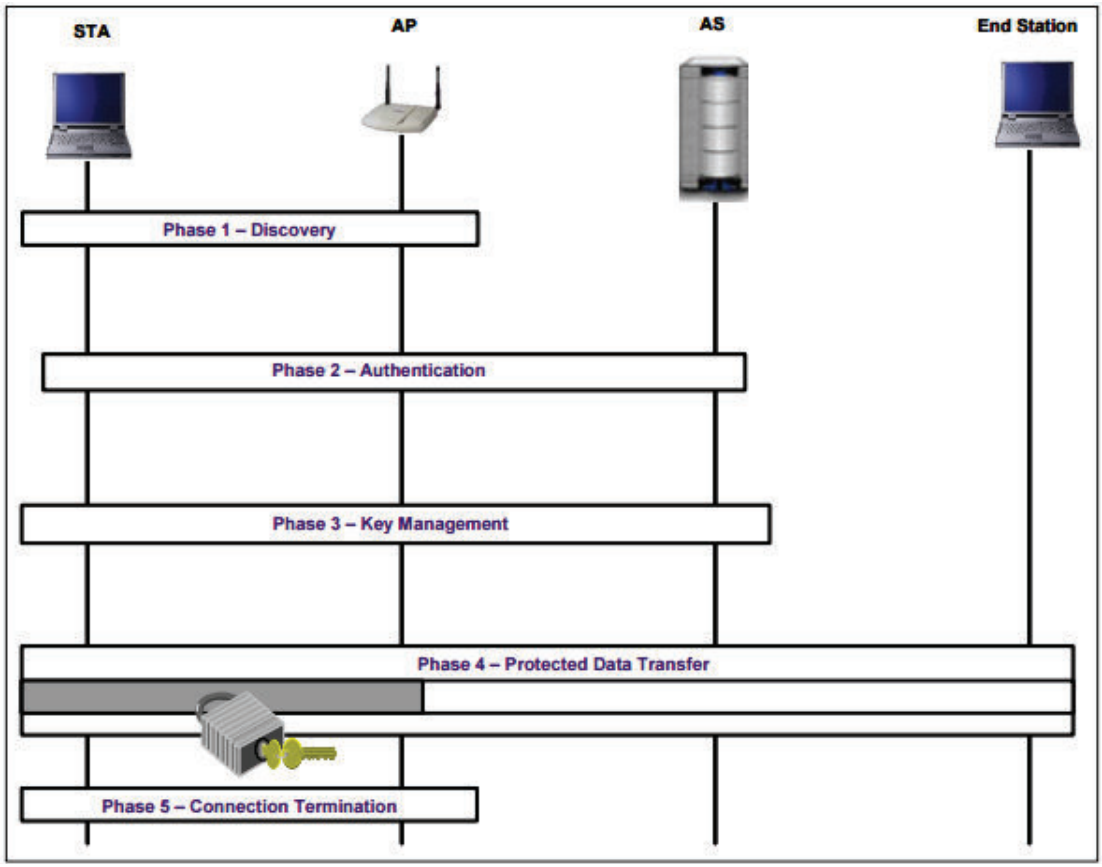


Gráfico 22.- Cinco fases de la Operación[28]

2.7.4. SOLUCIONES PARA ACCESOS

Soluciones disponibles para proteger el cifrado y la autenticación de LAN inalámbrica: Acceso protegido Wi-Fi (WPA), Acceso protegido Wi-Fi 2 (WPA2) y Privacidad Equivalente a Cableado (WEP). La solución que elija es específica del tipo de LAN inalámbrica a la que está accediendo y del nivel de cifrado de datos necesario.

2.7.4.1. WEP (Wired Equivalent Privacy)[29]

La seguridad de la red es extremadamente importante, especialmente para las aplicaciones o programas que almacenan información valiosa.

[28] (National Institute of Standards and Technology, 2007)
[29] (Lehembre, 2006)

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. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire.

Cuanto más larga sea la clave, más fuerte será el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales y 5 o 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 o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo. Por lo tanto, se recomienda cambiar la clave WEP frecuentemente. A pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo.

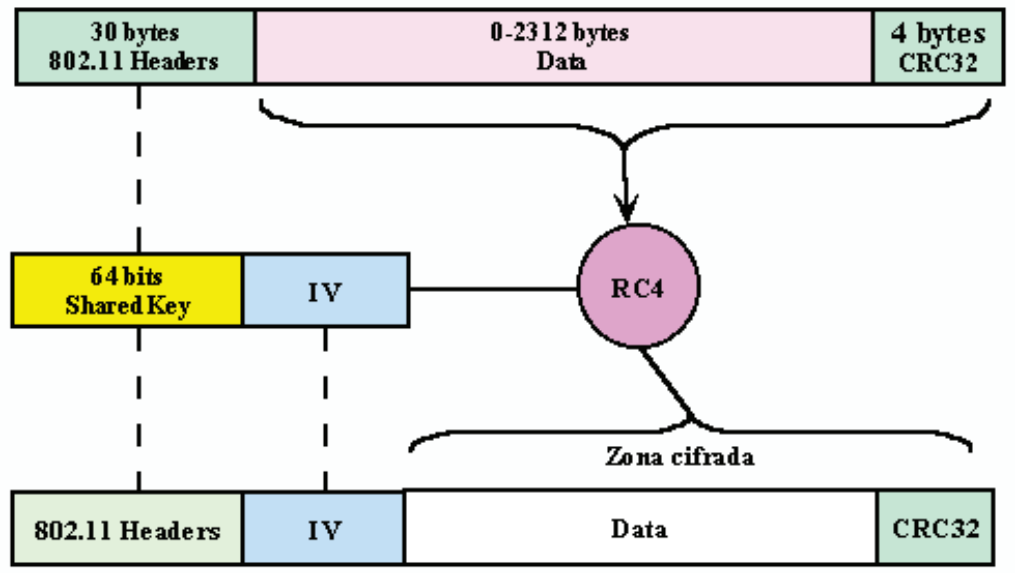


Gráfico 23.- Algoritmo de Encriptación WEP[30]

[30] (Lehembre, 2006)

2.7.4.2. WPA/WPA2[31]

Estas certificaciones de seguridad basadas en normas de la Wi-Fi Alliance para LAN de grandes empresas, empresas en crecimiento y para la pequeña oficina u oficinas instaladas en el hogar proporcionan autenticación mutua para verificar a usuarios individuales y cifrados avanzados.

WPA proporciona cifrado de clase empresarial y WPA2, la siguiente generación de seguridad Wi-Fi, admite el cifrado de clase gubernamental. "Recomendamos WPA o WPA2 para las implementaciones de LAN inalámbrica en grandes empresas y empresas en crecimiento".

Los fabricantes comenzaron a producir la nueva generación de puntos de acceso apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad de que la tecnología cumple con estándares de interoperabilidad" declaró Frank Hazlik Managing Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11.

[31] (Kdocs, 2007)

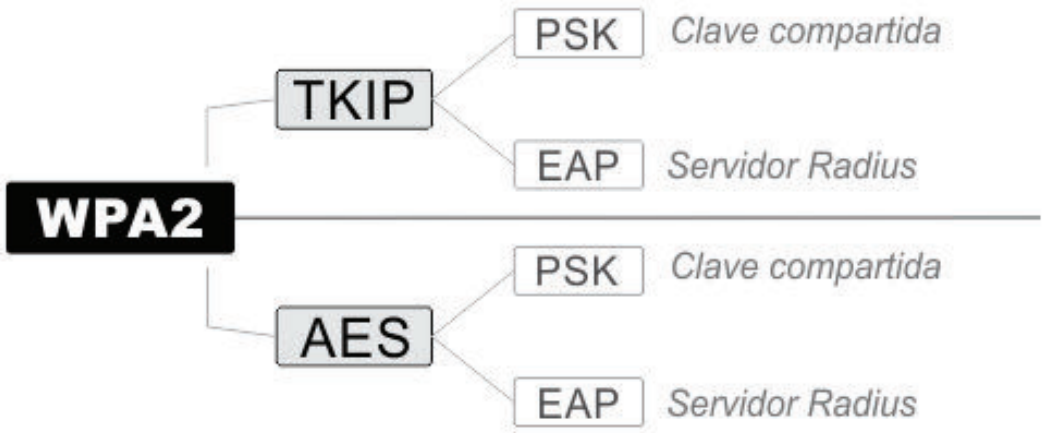


Gráfico 24.- Método de encriptación inalámbrica WPA2[32]

[32] (Kdocs, 2007)

CAPÍTULO 3

ANÁLISIS DE ALTERNATIVAS

De acuerdo lo planteado en el Capítulo 1, para solventar la necesidad en la institución se requiere hacer uso de un punto para acceso inalámbrico y la instalación de tarjetas inalámbricas para cada estación, desarrollaremos dentro de este capítulo un análisis de las tecnologías y equipos existentes en el mercado, dispositivos que proporcionarán la solución adecuada a esta implementación, tomando en cuenta parámetros indispensables como velocidades, distancias de transmisión, costos y tráfico de transferencia, para finalizar, dentro las tecnologías modernas se verificará la compatibilidad de hardware y software existente en las instalaciones de la institución, con el objetivo de aplicar las mejores prácticas en la tecnología inalámbrica y con esto dar funcionalidad en su totalidad.
También en el desarrollo de este capítulo se requiere escribir especificaciones de ciertos puntos ya definidos en el Capítulo 2 para conocer más a fondo como se desarrollara a nivel tecnológico este tipo de conexiones.

3.1. WIRELESS FIDELITY (WIFI)[33]

WiFi, o "Wireless Fidelity", es una asociación internacional sin ánimo de lucro formada en 1999 para asegurar la compatibilidad de los distintos productos de redes de área local inalámbrica basadas en la especificación IEEE 802.11.

A nivel de capa física, WiFi utiliza diferentes esquemas de transmisión, uno de ellos SS y otro mutliplexación por división ortogonal de frecuencia (por sus siglas en inglés Orthogonal Frequency Division Multiplexing, OFDM). Sin embargo, la robustez de OFDM para enlaces multicamino, en los que el desvanecimiento del canal toma un rol importante, lo ha llevado el ser el más utilizado para poder alcanzar mayores tasa de datos. A nivel de capa de enlace (MAC), WiFi presenta muchas desventajas.

[33] (Carballar, 2010)

Es una tecnología que no fue preparada para implementar calidad de servicio (QoS). Esto lleva a inseguridades en la red de información, lo cual hoy en día, constituye un factor importante dentro del mercado. Revisando el estándar WiFi, podemos encontrar que el mismo fue diseñado para redes LAN, de ahí su nombre WLAN. Sin embargo, debido a los bajos costos de estos productos, se ha tratado de extender este servicio a redes MAN, lo que implica ser más eficiente en la seguridad de la red y otros factores que se clarificaran en el estudio de WiMAX. Sin embargo, precisamente WiMAX es el estándar aprobado por la IEEE para garantizar una alta calidad de servicio en regiones MAN y WAN.

3.2. TARJETAS DE RED PCI INALAMBRICA[34]

También llamadas tarjetas WiFi, son tarjetas para expansión de capacidades que sirven para enviar y recibir datos sin la necesidad de cables en las redes inalámbricas de área local ("WLAN "Wireless Local Area Network"), esto es entre redes inalámbricas de computadoras. Esta tarjeta de red se inserta dentro de las ranuras de expansión o "Slots" integradas en la tarjeta principal ("Motherboard") y se atornilla al gabinete para evitar fallas y por ende movimientos. En su mayoría las tarjetas de red inalámbricas integran una antena externa de recepción para las señales. Estos dispositivos recibirán y enviarán la información hacía su destino desde el ordenador en el que esté trabajando y de la mano se mide la velocidad de transmisión/recepción que dependiendo del fabricante varían los estándares que cumpla.

Compiten actualmente en el mercado contra los adaptadores USB-WiFi, tarjetas para red LAN y Adaptadores USB-RJ45.

3.2.1. CARACTERÍSTICAS GENERALES DE LA TARJETA DE RED INALÁMBRICA

- Están diseñadas para ciertos tipos de estándares de redes inalámbricas, por lo que tienen una velocidad máxima de transmisión de datos en bits por segundo acorde al estándar.

[34] (Julio Barbancho Concejero, 2014)

- Poseen una antena interna/externa que permite la buena recepción de datos de la red, así como para su envío.
- Tienen un slot PCI en su parte inferior que permite insertarlas en las ranuras de expansión de la tarjeta principal.
- Con la idea de compactar el hardware para optimizar espacio físico en ocasiones las tarjetas de red ya vienen integradas en la tarjeta principal.
- Se puede obtener acceso a redes de manera independiente considerando que no hay límite de tarjetas de red conectadas en una computadora, solo la tarjeta principal dependiendo de su tecnología puede definir este parámetro.
- Contienden actualmente frente a los adaptadores USB para redes inalámbricas, las cuales ofrecen muchas ventajas con respecto a la portabilidad, la facilidad de uso y el tamaño.

3.2.2. ESTÁNDARES BÁSICOS PARA REDES DE DATOS INALÁMBRICAS

Se describen las convenciones y protocolos que se pactó utilizar para el correcto funcionamiento entre redes de datos inalámbricas ("*Wireless*").

Estándar	Norma	Velocidad (Megabits por segundo)	Características
Wireless N	IEEE 802.11n	300 Mbps	Utiliza tecnología MIMO ("*Multiple Input - Múltiple Output*"), que por medio de múltiples antenas trabaja en 2 canales (frecuencia 2.4 GHz y 5 GHz simultáneamente).
Wireless G	IEEE 802.11g	11 / 22 / 54/125 Mbps	Trabaja en la banda de frecuencia de 2.4 GHz solamente.

Tabla 2.- Estándares tarjetas PCI inalámbricas

3.2.3. INTERFASE PARA LAS RANURAS PCI

Al ser una tecnología reciente, han determinado que la ranura para uso extendido de estas es el PCI.

PCI ("Peripheral Components Interconect") compone una capacidad de datos de 32 bits y 64 bits para el microprocesador, tiene una velocidad de transferencia de hasta 125.88 Megabytes/s (MB/s) a 503.54 MB/s respectivamente, cuentan con una velocidad interna de trabajo de 33 MHz para 32 bits y 66 MHz para 64 bits.

3.2.4. LOW PROFILE EN TARJETAS DE RED INALÁMBRICA

El término "Low Profile" se traduce textualmente como bajo perfil, pero en las tarjetas de red no quiere decir que tenga un bajo rendimiento como se podría suponer o que sea una tarjeta económica debido a mala calidad del producto, sino que el bosquejo que tiene es para trabajar de manera dedicada incluso cuándo se utilizan varias tarjetas PCI sin incomunicar negativamente con los otros componentes.

3.3. ACCESS POINT (AP)[35]

Se define como un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Habitualmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Diversos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos sin la necesidad de un punto de acceso convirtiéndose en una red ad-hoc). Los puntos de acceso inalámbricos tienen direcciones IP determinadas, para poder ser configurados.

El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

[35] (Ehrlich, 2011)

Este dispositivo con su antena normalmente son colocados en lugares alto y se facilite su instalación, pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio anhelada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica.

3.3.1. FUNCIÓN BRIDGE O PUENTE DEL ACCESS POINT (AP)

Una red inalámbrica posee una doble función: interconectar computadoras y dispositivos cercanos entre sí y la segunda es la de proveer de servicios de Internet a los dispositivos.

Un servidor o un Módem inalámbrico de un proveedor de Internet es el encargado de recibir la señal y distribuirla a la red local. Sin embargo, el servidor cuenta con un sistema operativo específico (Novell®, Microsoft Windows NT®, Linux Apache, etc.) y cada dispositivo que se conecta a la red cuenta con el propio.

Los sistemas operativos básicamente son incompatibles entre sí y los usuarios que acceden a la red local generalmente tendrán en sus dispositivos sistemas operativos muy diferentes a los del servidor como: MacOS® Leopard, Linux Ubuntu, GoogleOS® Chrome, Microsoft® Windows Vista, etc.; es en este momento en el que un dispositivo como el Access Point puede funcionar como puente entre todos ellos y evitar que se interrumpa la comunicación, lo que hace es permitir la comunicación entre dispositivos a pesar de las diferentes plataformas, siendo cada una la encargada de interpretar los datos recibidos. También permite evaluar la información, realizando actividades de limpieza, seguridad y filtro con la información, así como descongestionar las redes dividiendo en subredes y enviando la información de manera paralela y por lo tanto más ágilmente.

3.3.2. ESTÁNDARES DEL ACCESS POINT (AP)

Los Access Point (AP) están diseñados para funcionar con ciertos estándares o protocolos (reglas de comunicación establecidas), se pueden encontrar para redes Wi-Fi (Wireless Fidelity), e incluso para redes BlueTooth.

Estándar	Características	Velocidad (Mbps)
IEEE 802.11b (Wireless B)	Es uno de los primeros estándares populares que aún se utiliza.	1 / 2 /5.5 / 11 Mbps
IEEE 802.11g (Wireless G) / Super G	Trabaja en la banda de frecuencia de 2.4 GHz solamente.	11 / 22 / 54 / 108 Mbps
IEEE 802.11n (Wireless N)	Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.	Hasta 300 Mbps
Bluetooth	Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio de corto alcance (1, 20 y 100 m a la redonda dependiendo la versión). Las ondas pueden incluso ser capaces de cruzar cierto tipo de materiales, incluyendo muros.	Hasta 1 Mbps

Tabla 3.- Estándares del Access Point

3.4. FUNCIONAMIENTO DE LOS DISPOSITIVOS[36]

Cuando una tarjeta de red inalámbrica se conecta a un Access Point (AP) se ve afectado principalmente por los siguientes parámetros:

- Velocidad máxima del AP (normalmente en 802.11 b/g/n será de 150Mbps).
- Distancia al AP (a mayor distancia menor velocidad).
- Elementos intermedios entre la tarjeta de red inalámbrica y el Access Point (las paredes, campos magnéticos o eléctricos) elementos interpuestos entre el Access Point y la tarjeta de red inalámbrica modificando la velocidad de transmisión a la baja.
- Saturación del espectro e interferencias (cuantos más usuarios inalámbricos existan en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá, esto también es aplicable para las interferencias.)

[36] (Staff, 2010)

Normalmente los fabricantes de Access Point (AP) presentan un enlace teórico de los mismos que suele andar alrededor de los 400 metros. Esto obviamente considerado por la tecnología del dispositivo, realmente todo dispositivo es sometido a una prueba de laboratorio en donde se determina su alcance estimado.

En términos generales, un dispositivo puede alcanzar el 60% de la capacidad especificada. Por lo tanto, es más probable que un adaptador inalámbrico que puede alcanzar una capacidad máxima de 300 Mbps, llegue a una capacidad real de 130 Mbps (o menos).

Un AP puede afectar el ancho de banda y la velocidad de conexión de su cliente de la siguiente manera:

3.4.1. EL CLIENTE Y EL AP UTILIZAN EL MISMO ESTÁNDAR INALÁMBRICO

Si el cliente y el AP utilizan el mismo estándar inalámbrico, la capacidad máxima que el cliente puede lograr en la red es igual a la capacidad máxima del AP. Por ejemplo, si el AP utiliza 802.11n, su capacidad máxima es de 300 Mbps. Si un cliente desea conectarse a esa velocidad, debe contar con un adaptador WLAN que también admita 802.11n.

3.4.2. EL CLIENTE USA UN ESTÁNDAR INALÁMBRICO MÁS ANTIGUO QUE EL AP

Si un cliente usa un estándar más lento o más antiguo que el AP, la capacidad máxima del cliente se verá limitada por la capacidad máxima de su adaptador inalámbrico. Por ejemplo, si el adaptador WLAN de un cliente utiliza 802.11g (capacidad máxima de 54 Mbps) y se conecta a un AP que utiliza 802.11n (capacidad máxima de 300 Mbps), el cliente sólo puede conectarse a una capacidad máxima de 54 Mbps.

3.4.3. EL CLIENTE USA UN ESTÁNDAR INALÁMBRICO MÁS NUEVO QUE EL AP

Si un cliente usa un estándar más nuevo o más rápido que el AP, la capacidad máxima se verá limitada por el AP. Por ejemplo, si el adaptador

WLAN del cliente usa 802.11n (capacidad máxima posible de 300 Mbps) y se conecta a un AP que utiliza 802.11g (capacidad máxima de 54 Mbps), el cliente sólo puede conectarse a una capacidad máxima de 54 Mbps.

3.4.4. EL AP TIENE UNA CAPACIDAD CABLEADA SUPERIOR A LA CAPACIDAD INALÁMBRICA

Muchas veces, un AP tiene un enrutador conectado a él, que a su vez está conectado a Internet o a una red de área local mediante un cable. Si dicho enrutador tiene una capacidad cableada superior a la capacidad inalámbrica, la capacidad máxima del cliente es igual a su capacidad inalámbrica. Por ejemplo, si el cliente y el AP tienen una capacidad inalámbrica de 300 Mbps (802.11n) y la capacidad cableada es de 1000 Mbps (Gigabit Ethernet), el cliente puede lograr una capacidad máxima de 300 Mbps con la red del AP.

3.4.5. EL AP TIENE UNA CAPACIDAD CABLEADA INFERIOR A LA CAPACIDAD INALÁMBRICA

Por otro lado, si el enrutador conectado al AP tiene una capacidad cableada inferior a la capacidad inalámbrica del AP, la capacidad máxima del cliente será igual a la capacidad cableada. Por ejemplo, si el cliente y el AP tienen ambos una capacidad inalámbrica de 300 Mbps (802.11n), pero la capacidad cableada es de 20 Mbps (DSL), el cliente puede alcanzar una capacidad máxima de 20 Mbps con la red del AP.

Si hay varios clientes inalámbricos, la mayoría de los AP detectarán el dispositivo con el estándar más antiguo y disminuirán la velocidad de todas las conexiones hasta llegar a la más lenta. Los AP más nuevos pueden detectar las conexiones 802.11g y 802.11n, y comunicarse con cada dispositivo a la mejor velocidad. Consulte la documentación que vino con su AP para ver instrucciones sobre cómo determinar su capacidad y sus opciones de configuración.

3.4.6. SEGURIDAD INALÁMBRICA Y RENDIMIENTO DE LA RED

Cada vez que se conecta a una red inalámbrica, debe usar un protocolo de seguridad para proteger sus datos. El estándar 802.11n requiere que utilice

autenticación WPA2 con encriptación AES o ninguna seguridad, a fin de poder utilizar las velocidades de 802.11n por completo. Seleccionar otros algoritmos de seguridad inalámbrica, como WEP o WPA, que eran populares con 802.11g, o métodos de encriptación TKIP, puede reducir significativamente el rendimiento a los niveles de 802.11g.

3.4.7. ANCHOS DE BANDA Y FRECUENCIAS INALÁMBRICAS[37]

Todos los dispositivos inalámbricos funcionan con un ancho de banda de 20 MHz (802.11a, 802.11b, 802.11g y 802.11n) o con un ancho de banda de 40 MHz (802.11n). Estos dos anchos de banda, a su vez, se dividen en tres bandas de frecuencia: 2,4 GHz, 3,6 GHz y 5,0 GHz. Además, cada banda permite una cantidad específica de canales. Cuando un cliente inalámbrico se conecta a un punto de acceso, se conecta a un canal específico en una frecuencia y ancho de banda específicos.

Existen distintos problemas relacionados con la frecuencia y el ancho de banda que pueden afectar la capacidad de un cliente en una red inalámbrica. Los problemas más comunes son:

- **Espacio aéreo saturado._** En un área donde muchos AP transmiten en el mismo ancho de banda y en la misma frecuencia habrá un alto nivel de interferencias. Esto sucede principalmente si los AP también transmiten en el mismo canal. Esto puede reducir el rango efectivo de cada canal, presentar una tasa de daño de datos más alta y, por lo general, disminuir las velocidades de la red.
- **Estándares inalámbricos mixtos._** Si un AP es de doble banda, pero no tiene dos antenas, y si está configurado para permitir dispositivos que usan un rango de estándares inalámbricos en la misma red (como 802.11b/g/n), las conexiones probablemente utilizarán el denominador común más bajo. Si un cliente 802.11n se conecta a un AP 802.11b/g/n, sólo puede ver velocidades de 802.11b o de 802.11g si no hay clientes 802.11b conectados al mismo tiempo.

[37] (Andreu, Redes inalámbricas (Servicios en red), 2011)

- **Restricciones regionales._** Cada país tiene sus propias leyes con respecto a qué canales de radio los dispositivos inalámbricos pueden y no pueden usar. Así, un AP podría automáticamente limitar su ancho de banda y frecuencia según su ubicación física. Aunque su cliente esté correctamente configurado para alcanzar su capacidad máxima, el AP local está lentificando la conexión intencionalmente.
- **Selección de ancho de banda**
  - Si un dispositivo 802.11n puede funcionar en el ancho de banda de 40 MHz, alcanzará su capacidad más alta posible. Esto permite que cada antena (consulte Entrada múltiple - Salida múltiple para obtener más información) transmita y reciba hasta 150 Mbps.
  - Si se impulsa a un dispositivo 802.11n a funcionar en el ancho de banda de 20 MHz, su capacidad se reduce a la mitad, lo que permite que cada antena transmita y reciba solamente hasta 75 Mbps.
  - De ser posible, un cliente 802.11n también debería operar en el rango de frecuencia de 5,0 GHz, aunque usando un rango de 2,4 GHz no necesariamente tiene como resultado problemas de rendimiento.
- **Controladores de dispositivos antiguos._** Para lograr un rendimiento óptimo, asegúrese de que el controlador de su adaptador inalámbrico esté actualizado. Un controlador desactualizado, genérico o ausente puede afectar la capacidad si, sin querer, aplica la configuración equivocada al adaptador inalámbrico.

La capacidad real del AP suele ser más baja, ya que la sobrecarga de las redes, como la gestión de enlaces, la calidad del servicio, la detección y corrección de errores, siempre reducirá la capacidad máxima.

Con las redes inalámbricas, también se debe tomar en cuenta la degradación de la señal si el dispositivo del cliente está demasiado lejos del punto de acceso y si hay interferencias de otros dispositivos en el área, como teléfonos inalámbricos, que suelen funcionar en las mismas bandas de radio que los clientes.

3.4.8. COMPARTIR ANCHO DE BANDA CON VARIOS CLIENTES

Cuando varios equipos y clientes inalámbricos comparten una única conexión a través del mismo punto de acceso, la cantidad total de ancho de banda disponible se divide entre los dispositivos. Por ejemplo, en una red inalámbrica, cuando una persona accede una consulta en línea, al mismo tiempo que otra reproduce un video y otra trata de navegar por Internet, la cantidad total de ancho de banda disponible se divide entre todos los usuarios. Esto puede tener un impacto significativo en la capacidad de su cliente.

Asimismo, cuando su equipo se conecta en forma inalámbrica a un punto de acceso público o a una red corporativa, la capacidad del equipo se reduce, ya que está compartiendo ancho de banda con todas las demás personas que se encuentran conectadas a la red.

3.4.9. PÉRDIDAS DE SEÑAL / ATENUACIÓN[38]

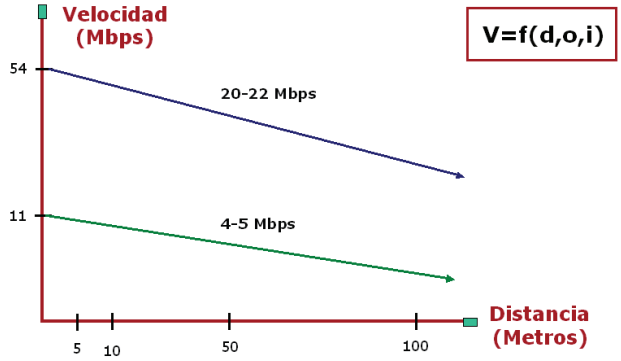
Toda señal inalámbrica va perdiendo potencia a medida que se propaga y va traspasando obstáculos. Lo que se transmite es energía y esta es atraída por los objetos (paredes, muebles metálicos, etc.) que encuentra a su paso. Los instaladores de redes WIFI deben comprender muy bien este fenómeno para tomarlo en cuenta en sus cálculos.

Cuando la señal es muy débil, la estación receptora encontrará errores y no acusará recibo del paquete y, por lo tanto, el paquete será retransmitido. Si la señal se vuelve muy débil se perderá la conectividad.

Existen 2 tipos de interferencias: Las que provienen del "mundo WIFI" (otras redes WLAN y la implementada) y las que surgen de otras fuentes como Bluetooth, hornos microondas, teléfonos fijos sin cable, etc. Muchas de estas fuentes (o todas) pueden ser desconocidas, lo que hace muy compleja su localización.

Así pues, se podría decir que en condiciones "de laboratorio" y a modo de ejemplo teórico, la transmisión entre dispositivos podría ser como se muestra en el gráfico:

[38] (Mailxmail, 2014)



- **Obstáculos (o):** paredes/columnas, muebles...
- **Interferencias (i):** Bluetooth, Microondas
- **Distancia (d):** entre usuario y Access Point

Gráfico 25.- Funcionamiento del dispositivo[39]

3.5. MODOS DE FUNCIONAMIENTO WI-FI[40]

El modo de funcionamiento es el modo atenuación de cada dispositivo dentro de la topología escogida.

Existen varias posibilidades que ofrecen los AP es el uso de diferentes modos de configuración. A continuación hacemos un repaso a los modos de funcionamiento más habituales que un AP puede soportar:

3.5.1. MODO AP O INFRAESTRUCTURA

Este es el más habitual y el que está implementado en los Routers Wi-Fi. Permite establecer una red Wi-Fi en la zona de cobertura del dispositivo. En ciertas ocasiones este modo también se utiliza para ampliar la capacidad de una red Wi-Fi, ampliando el número de APs.

3.5.2. MODO WDS (WIRELESS DISTRIBUTION SYSTEM)

Este modo de funcionamiento permite establecer una conexión directa inalámbrica entre dos APs. Es un modo utilizado para establecer puentes inalámbricos que permitirán conectar dos redes separadas. El problema de este modo es que no está incluido en el estándar Wi-Fi por lo que puede dar problemas si se utiliza con APs de distinto fabricante.

[39] (ADRFormacion, 2014)
[40] (Voinea, 2011)

3.5.3. MODO WDS CON AP

Este modo es una mezcla de los dos anteriores. Permite a un AP establecer un puente inalámbrico con otro AP y al mismo tiempo establecer una red Wi-Fi. No es un modo muy utilizado por cuestiones de rendimiento.

3.5.4. MODO REPEATER (TAMBIÉN DENOMINADO MODO RANGE EXTENDER)

Este modo de funcionamiento se ha popularizado en los entornos residenciales ya que permite ampliar la cobertura de la red Wi-Fi proporcionada por el router Wi-Fi del ISP de forma fácil. De hecho, se han comercializado dispositivos Wi-Fi específicos que funcionan en este modo, conocidos como Repetidores Wi-Fi.

3.5.5. MODO WIRELESS CLIENT

Este modo permite que un AP se comporte como un cliente Wi-Fi. Se utiliza en ciertos casos para establecer un puente inalámbrico con APs de diferente fabricante.

Tanto los modos WDS como Wireless Client, técnicamente no constituyen redes Wi-Fi, ya que no permiten la conexión de dispositivos Wi-Fi. Su función es la de establecer puentes inalámbricos.

3.6. PARÁMETROS PARA LA SELECCIÓN DE DISPOSITIVOS

3.6.1. MODO DE FUNCIONAMIENTO PARA LA RED

Para resolver el requerimiento de conexión para todos los usuarios debemos analizar su cobertura y limitaciones, basándonos en la experiencia se analizará el modo Infraestructura.

3.6.1.1. Modo infraestructura con AP[41]

Esta es una configuración muy común en entornos profesionales donde es necesario proporcionar acceso Wi-Fi en áreas extensas o donde exista un número alto de dispositivos. La clave de este modo es tener la infraestructura de cableado necesaria ya que todos los APs deben ir

[41] (Voinea, 2011)

conectados a la red cableada donde se encuentre el router que proporcione salida a Internet.

Este modo de funcionamiento es totalmente interoperable, es decir, funciona utilizando APs de diferentes fabricantes. Lo importante es que todos los dispositivos de red inalámbrica y AP utilicen el mismo estándar Wi-Fi o a su vez que el AP posea un estándar compatible con los dispositivos inalámbricos y los mismos parámetros (SSID, tipo de seguridad y clave).

Cuando el número de APs que conforman la red inalámbrica es alto, algunos fabricantes proporcionan soluciones tanto software como hardware para gestionar de forma eficiente y unificada todos los dispositivos. El inconveniente en este caso es que todos los APs deben ser del mismo fabricante que aporta la solución de gestión.

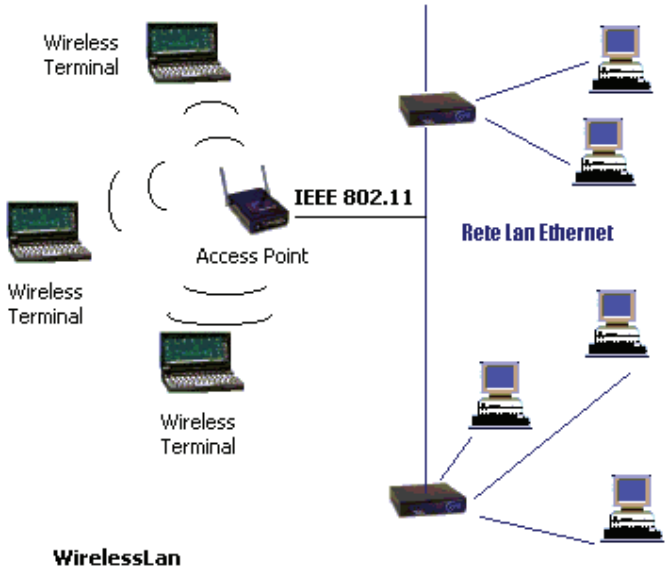


Gráfico 26.- Wireless AP[42]

3.6.2. VELOCIDAD DE TRANSMISIÓN DE DATOS

En las transmisiones inalámbricas en general, incluyendo Wi-Fi, la velocidad de transmisión de los datos, que en última instancia es una medida de las prestaciones de la propia tecnología de transmisión, depende de numerosos factores. Al fin y al cabo los datos viajan por el aire en forma de ondas electromagnéticas y sufren los efectos de atenuación y degradación típicos

[42] (Dany, 2011)

de este tipo de transmisiones. Con todo ello, el estándar IEEE 802.11 proporciona una velocidad teórica máxima de 54 Mbps, cifra que aparecerá como principal argumento en todos los catálogos publicitarios de los productos Wi-Fi que cumplan dicho estándar.

3.6.2.1. Factores que influyen en la velocidad de las conexiones Wi-Fi

El estándar Wi-Fi utiliza un modo de transmisión llamado half-dúplex, que básicamente significa que una comunicación mediante Wi-Fi no puede enviar y recibir datos simultáneamente. En la práctica significa que esos teóricos 54 Mbps se reparten entre la transmisión y la recepción de datos. En determinados momentos se transmiten datos y en otros momentos se reciben, pero no puede hacerse a la vez. Por comparar, las tecnologías cableadas de acceso como ADSL, HFC (utilizado por los operadores de cable) o de redes locales como Ethernet, tienen canales separados e independientes para transmitir y recibir datos.

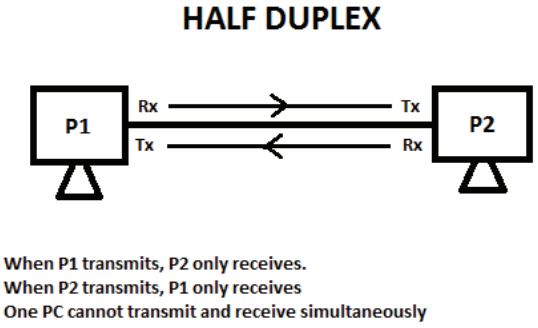


Gráfico 27.- half-dúplex[43]

La distancia entre el dispositivo inalámbrico y el punto de acceso (o router con capacidades inalámbricas) es un factor muy importante de atenuación de la señal Wi-Fi. Y esto tiene un efecto inmediato en la velocidad.

[43] (ccnachamp.com, 2012)

Lo mismo ocurre con los obstáculos (principalmente paredes y techos). La frecuencia utilizada por las ondas electromagnéticas en Wi-Fi son capaces de atravesar obstáculos, pero la señal queda atenuada y por tanto la velocidad se ve afectada.

3.6.2.2. Velocidad por protocolo[44]

Protocolo	Frecuencia	Señal	Máxima velocidad de datos de
Legacy 802.11	2.4 GHz	FHSS o DSSS	2 Mbps
802.11A	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	HR-DSSS	11 Mbps
802.11g	2.4 GHz	OFDM	54 Mbps
802.11N	2.4 o 5 GHz	OFDM	600 Mbps (teóricas)

Tabla 4.- Velocidad por Protocolo

- Legacy 802.11
  - ✓ Tres canales no superpuestos en industrial, científica, médica (ISM) banda de frecuencia de 2,4 GHz.
  - ✓ Definida en un principio carrier sense (acceso múltiple con prevención de colisiones CSMA -CA).
- 802.11A
  - ✓ Las velocidades de datos con modulación diversos tipos: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.
  - ✓ Multiplexación por división de frecuencia (OFDM) sub-carrier de forma ortogonal con 52 canales.

[44] (INTEL, 2014)

- ✓ 12 Infraestructura (UNII) canales que no se solapan sin licencia nacional de información en banda de frecuencia de 5 GHz.

- 802.11b
  - ✓ Las velocidades de datos con diversos tipos modulación: 1, 2, 5.5 y 11 Mbps.
  - ✓ Secuencia directa de distribución de espectro de alta velocidad (HR-DSSS).
  - ✓ Tres canales no superpuestos en industrial, científica, médica (ISM) banda de frecuencia de 2,4 GHz.
- 802.11g
  - ✓ Las velocidades de datos con modulación diversos tipos: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps; puede volver a 1, 2, 5.5 y 11 Mbps utilizando DSSS y cck.
  - ✓ Multiplexación por división de frecuencia (OFDM) de forma ortogonal con 52 sub-carrier canales; al revés compatible con 802.11b mediante DSSS y cck.
  - ✓ Tres canales no superpuestos en industrial, científica, médica (ISM) banda de frecuencia de 2,4 GHz.
- 802.11N
  - ✓ Las velocidades de datos con diversos tipos modulación: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps; consulte la siguiente tabla.
  - ✓ Multiplexación por división de frecuencia (OFDM) de forma ortogonal con multiple-input multiple-output (MIMO/) y unión de canales (CB).
  - ✓ Tres canales no superpuestos en industrial, científica, médica (ISM) banda de frecuencia de 2,4 GHz.
  - ✓ 12 Infraestructura (UNII) canales que no se solapan sin licencia nacional de información en banda de frecuencia de 5 GHz con y sin CB.

3.7. ESPECIFICACIONES DE DISPOSITIVOS INALÁMBRICOS

3.7.1. ACCES POINT (AP)

Existen en la actualidad centenares de fabricantes de Access Points, muchos de los cuáles no están debidamente certificados o no son adecuados a las necesidades de nuestros requerimientos.

Los especialistas recurren a normas y estándares para dar valides a cada equipo fabricado y verifican de acuerdo a sus especificaciones las acciones de estos equipos en un laboratorio de pruebas, por lo cual la tarea de selección de un Access Point es muy compleja y delicada.

Vamos a revisar las características de 3 dispositivos inalámbricos seleccionados para solventar el requerimiento de la institución.

El resumen muestra las características requeridas, todos los parámetros revisados nos da a conocer una mejor visión a la hora de tomar una decisión de uso a un dispositivo, tomando en cuenta las exigencias planteadas.

Marca	D-Link	Linksys	Ubiquiti
Imagen			
Nombre del producto	DAP	N300	NanoStation
Transmisión	100 Mbps	100 Mbps	150 Mbps
Cable UTP	Cat 5e o superior	Cat 5e o superior	Cat 5e o superior
Modelo	2360	WAP300N	M2

Características principales	Access Point (AP) WDS with AP WDS/Bridge (No AP Broadcast) Wireless Client	Modo Punto de acceso Modo Cliente de punto de acceso Modo Base inalámbrica Modo Amplificador de señal	Access Point (AP) WDS with AP WDS/Bridge (No AP Broadcast) Wireless Client
Estándares Certificaciones	IEEE 802.11n IEEE 802.11g IEEE 802.3ab IEEE 802.3af IEEE 802.3u IEEE 802.3	IEEE 802.3u IEEE 802.11g IEEE 802.11b IEEE 802.11a IEEE 802.11n	FCC Part 15.247 IC RS210 CE RoHS Compliance
Administración	Telnet - Secure (SSH) Telnet Web Browser Interface HTTP - Secure HTTP (HTTPS) SNMP Support D-View Module - Private MIB AP Manager II AP Array	Telnet - Secure (SSH) Telnet Web Browser Interface HTTP - Secure HTTP (HTTPS) SNMP Support D-View Module - Private MIB AP Manager II AP Array	Telnet - Secure (SSH) Telnet Web Browser Interface HTTP - Secure HTTP (HTTPS) SNMP Support D-View Module - Private MIB AP Manager II AP Array
Frecuencias	2.4 GHz to 2.4835 GHz	2.4 GHz and 5 GHz	2.4 GHz and 5 GHz
Interface de red	1 x 10/100	1 x 10/100	(2) 10/100 Ethernet Ports
Antena	5 dBi @ 2.4 GHz	5 dBi @ 2.4 GHz	14dBi x2
Dimensiones	166 x 188 x 37 mm	150 x 178 x 35 mm	26.4 cm x 8 cm x 3cm
Seguridad	WPA™ - Personal WPA2™ - Enterprise WPA2™ - Personal WPA2™ - Enterprise 64/128-bit WEP SSID Broadcast Disable MAC Address Access Control Rogue AP Detection	WPA™ - Personal WPA2™ - Enterprise WPA2™ - Personal WPA2™ - Enterprise	WPA™ - Personal WPA2™ - Enterprise WPA2™ - Personal WPA2™ - Enterprise 64/128-bit WEP SSID Broadcast Disable MAC Address Access Control Rogue AP Detection

Temperatura	Operating: 0 to 40 °C Storage: -20 to 65 °C	Operating: -05 to 35 °C	Temperatura de funcionamiento -30C to +80C
Precios	$ 110	$ 97	$ 125
Fuente de poder	Externo, 5V DC 2,5A	Externo, 5V DC 2,4A	12V, 1A POE

Tabla 5.- Comparación de APs

3.7.2. TARJETAS INALAMBRICAS PCI

Para definir la más adecuada se realizó pruebas con un AP como emisor de señal y un computador base para montar las tarjetas PCI a ser probadas.

De igual forma vamos a revisar las características de 3 tarjetas PCI inalámbricas para las estaciones de trabajo destinados a solventar el requerimiento de la institución.

Marca	D-Link	LinkSys	TrendNet
Imagen			
Nombre Producto	DWA	WMP	TEW
Modelo	525	54G	423PI
Transmisión	54 Mbps	54 Mbps	54 Mbps
Estándares	•IEEE 802.11n •IEEE 802.11g	IEEE 802.11g IEEE 802.11b	IEEE 802.11b IEEE 802.11g
Rango de frecuencia inalámbrica	2.4GHz to 2.4835GHz	2.4GHz to 2.4835GHz	2.412 a 2.484 GHz

Administración Dispositivo	•Internet Explorer® v7 or later •Mozilla® Firefox® v3.0 or later •Other Java-enabled Browsers	Todos los navegadores con JAVA	Todos los navegadores con JAVA
Interface	PCI 2.0	PCI 2.2 PCI 2.3	PCI 2.0
Certificaciones	•FCC Class B •IC •Wi-Fi®	Wi-Fi CERTIFIED FCC RoHS	CE, FCC
Seguridad	•Wi-Fi Protected Access (WPA, WPA2)® •Wi-Fi Protected Setup™ (WPS) •Push Button	WEP WPA CCX 2.0	WPA/WPA2(TKIP), WPA-PSK/WPA2-PSK(AES/TKIP), 64/128-Bit WEP (Hex o ASCII)
LED´s	Link/Activity	Enlace	Link (Enlace)
Temperatura de operación	32ºF to 104ºF (0°C to 40°C)	0° ~ 35° C	0° ~ 40° C (32° ~ 104° F)
Dimensiones	Item (WxDxH): 4.7” x 4.8” x 0.9” (120mm x 122mm x 22mm)	16 X 2,1 X 21 cm	121 x 44 mm (4,8 x 1,7 pulgadas)
Sistema operativo compatible	Compatible con Windows 7 (32/64-bit), Vista (32/64-bit), XP (32/64-bit), 2000, ME, 98SE	Windows 98SE, Me, 2000 o XP con Service Pack 1 (o superior)	Compatible con Windows 7 (32/64-bit), Vista (32/64-bit), XP (32/64-bit), 2000, ME, 98SE
Precios	$ 15	$ 35	$ 45

Tabla 6.- Comparación de Tarjetas PCI

El resumen muestra las características requeridas de las tarjetas inalámbricas PCI, todos los parámetros revisados nos dan a conocer una mejor visión a la hora de tomar una decisión.

3.8. ANALISIS TECNICO DEL REQUERIMIENTO

Según las características expuestas anteriormente sobre los dispositivos “Access Point” y tarjetas inalámbricas, actualmente disponibles en el mercado se ha elegido, tomando en cuenta varios aspectos técnicos que cumplen de acuerdo a las normas aplicadas, mencionaremos las características y el beneficio técnico

que nos llevó a la elección.

- Un tema de mucha importancia en el ámbito general de las telecomunicaciones, es la velocidad de transmisión. Actualmente existen muchos dispositivos Access Point los cuales cumplen estándares que definen parámetros importantes a la hora de su operación. En este caso es de mucha importancia que la velocidad de transmisión sea alta para que los usuarios tengan la facilidad de acceder a los servicios con rapidez. Hoy en día servicios como el de internet, correo electrónico, base de datos, etc. Son de vital importancia para las actividades cotidianas y los usuarios desean acceder a ellos con facilidad y rapidez, por lo que el dispositivo a elegir debe cumplir con este requerimiento.
- Los equipos inalámbricos APs en la actualidad requieren ser instalados en una ubicación donde pueda ofrecer la cobertura en su totalidad, en este caso se requiere que esté instalado en los altos del centro de cómputo por lo que el flujo eléctrico hasta ese punto es imposible instalarlo y adicional debe soportar condiciones de alta/baja temperatura y condiciones húmedas ya que estará ubicado casi a la intemperie, por lo que se requiere que posea adaptador POE.
- Las tarjetas inalámbricas deben ser compatibles con el sistema operativo Windows XP, ya que el 100% de equipos funcionan bajo este sistema y adicional debe llevar una antena externa para lograr una mejor recepción por que la ubicación de cada equipo es irregular.

3.9. SELECCIÓN DE LOS EQUIPOS PARA LA CONEXIÓN

De acuerdo al análisis realizado a los dispositivos y en comparación a los requerimientos planteados por la institución se ha determinado que para este proyecto es necesario instalar el Access Point UBIQUITI NanoStation M2, bajo los siguientes criterios:

- Este dispositivo está en la capacidad de soportar condiciones ambientales dinámicas.
- Su alimentación eléctrica se basa en la tecnología POE.

- Su velocidad de transmisión es de 150 Mbps y haciendo uso de característica (2 - 10/100 Ethernet Ports) la velocidad de transmisión será de 300 Mbps.
- Aprovechando esta característica se conseguirá una cobertura de 360°.
- Los algoritmos de seguridad que posee son plenamente compatibles con todas las tarjetas inalámbricas, que funcionaran como clientes del AP.
- En este caso no se ha puesto atención al costo ya que para cumplir con la exigencia del requerimiento, se demanda un equipo robusto.

De acuerdo a la decisión tomada con respecto al dispositivo AP se alinea el dispositivo D-Link DWA-525 debido a los siguientes criterios:

- Cada estación de trabajo con tecnología PCI 2.0.
- Compatibilidad con sistema operativo Windows XP.
- Posee una antena externa para mejorar la recepción de señal.

CAPÍTULO 4

INSTALACIÓN Y CONFIGURACIÓN DEL ACCESS POINT Y ESTACIONES DE TRABAJO

El grado de complejidad de una red de área local inalámbrica es variable, dependiendo del costo, las necesidades y en función de los requerimientos de la red que se desea implementar se puede utilizar diversas configuraciones de red, en este capítulo se hablará acerca de la implementación, configuración y pruebas en modo de infraestructura.

Se conoce el área donde se distribuirán los dispositivos de acuerdo a lo descrito en el plano (ver Anexo 1) y en base a esto implementar una red inalámbrica con frente a posibles intrusos, algo que aunque no resulta complicado, es de vital importancia ya que sin la protección adecuada, el producto se afectaría con accesos no autorizados y caídas en la red, los cuales podrían ingresar a la los computadores ejecutando cualquier modificación en él o mucho peor accedería a utilizar nuestra conexión a Internet para delinquir en la red.

4.1. ASPECTOS FÍSICOS DEL ACCESS POINT

4.1.2. LED's

- Power
- LAN1 / WAN Main Ether
- LAN2 / Secondary Ethernet
- Signal

4.1.3. CONECTORES

- Main Ethernet Port
- Secondary Ethernet Port

4.1.4. BOTONES

- Reset

4.2. INSTALACION INICIAL DEL ACCES POINT[45]

4.2.1. CONTENIDO DEL PAQUETE

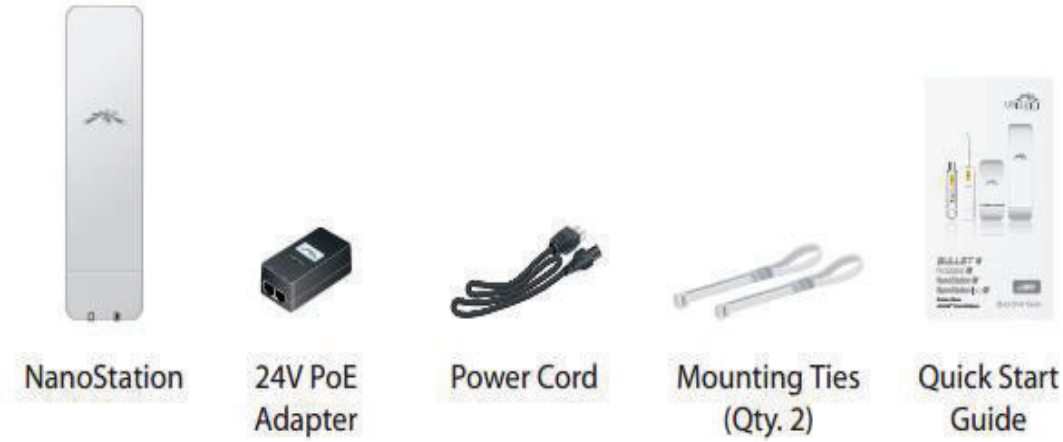


Gráfico 28.- Paquete AP

4.2.2. CONEXIÓN HARDWARE PARA CONFIGURACIÓN INICIAL

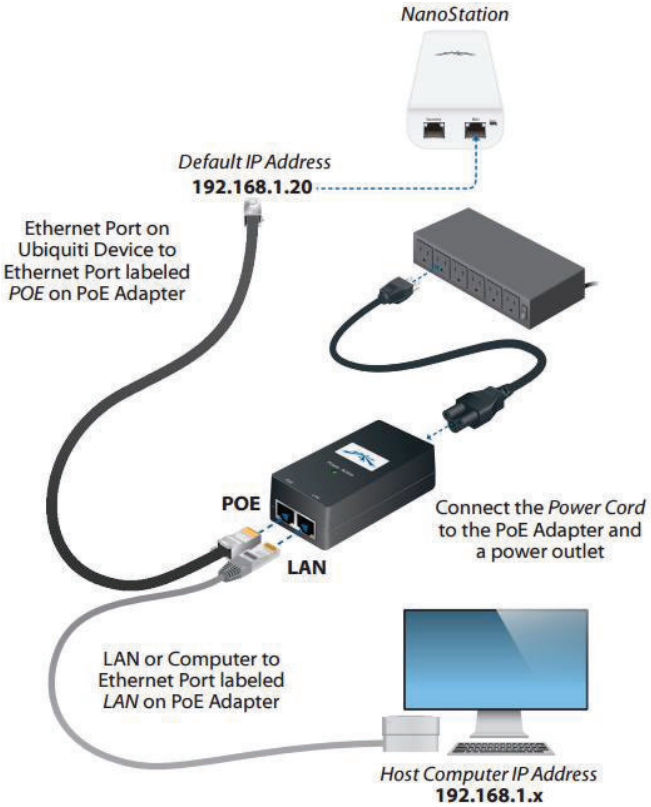


Gráfico 29.- Conexión Física AP

[45] (Ubiquiti Networks™, 2013)

4.2.3. CONFIGURACIÓN RED INICIAL

Una vez realizada la conexión el siguiente paso es configurar el PC. Debido a que la NanoStation no trae habilitado por defecto el protocolo DHCP, esta no proveerá, ninguna dirección IP al PC, por lo que será necesario configurar la tarjeta de red del PC de forma manual con una dirección IP dentro del rango de red de la dirección IP de la NanoStation.

Esto lo configuramos en el apartado de conexiones de red, buscamos la conexión de área local a la que tenemos conectada la NanoStation y abrimos las propiedades.

Una vez dentro de las propiedades de la conexión de área local, seleccionamos el protocolo TCP/ IP (versión 4 en Windows 7) y pulsamos propiedades.

La NanoStation por defecto tiene la dirección IP: 192.168.1.20, por lo que nosotros podemos ponerle a nuestro ordenador, por ejemplo la 192.168.1.35.

Como puerta de enlace utilizamos la NanoStation, por lo que ponemos su dirección IP.

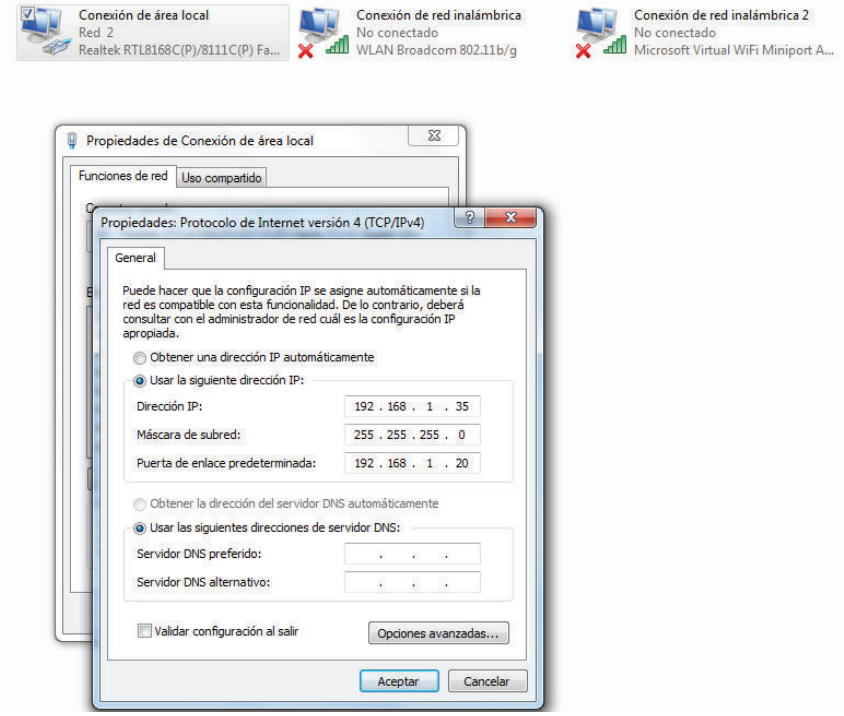


Gráfico 30.- Configuración de la red del equipo

4.2.4. INGRESO AL DISPOSITIVO

Abrimos un navegador y en la barra de dirección colocamos lo siguiente:

https://192.168.1.20/login.cgi?uri=/

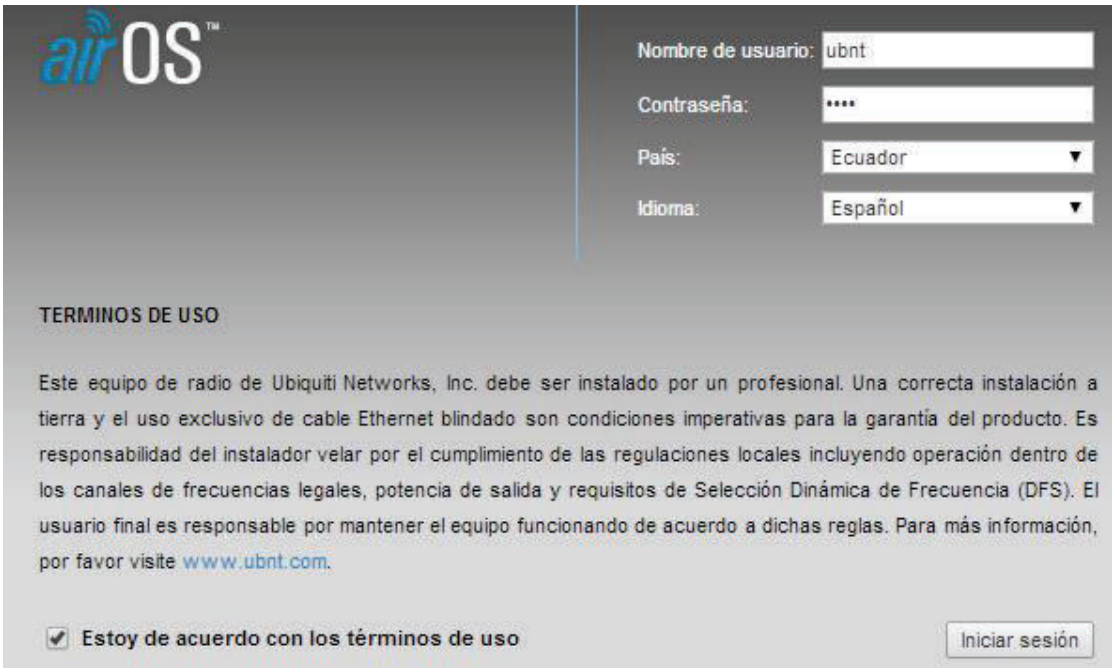


Gráfico 31.- Inicio Ubiquiti NanoStation

Llenamos los campos indicados con los valores de fábrica.

Nombre de usuario: ubnt

Contraseña: ubnt

4.2.5. CONFIGURACIÓN WIRELESS

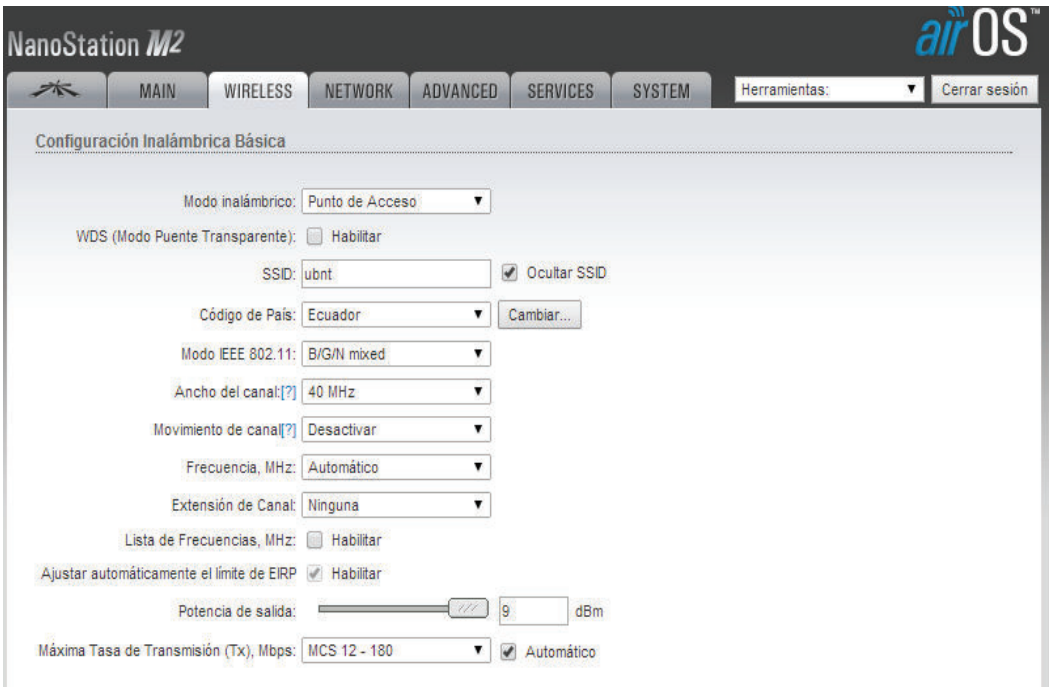


Gráfico 32.- Pantalla Wireless

- Definimos como Access Point.
- País a United States por efecto de ancho de canal para distribución de señal.
- Potencia de salida la ajustamos ya que de esto depende el alcance de la señal.

En este caso lo configuramos como oculto.

Gráfico 33.- Ocultar SSID

4.2.6. SEGURIDADES PARA EL DISPOSITIVO

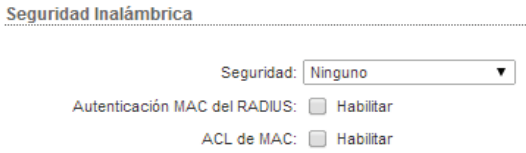


Gráfico 34.- Plantilla de seguridad AP

Escogemos el tipo de seguridad

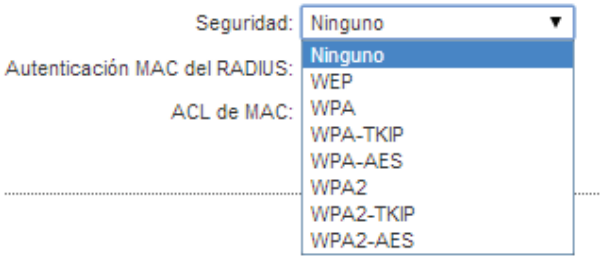


Gráfico 35.- Tipo Seguridad AP

Definido el tipo de seguridad tenemos los siguientes lineamientos.

Gráfico 36.- Definir seguridad AP

- Definimos su clave de acceso
  - 64 bits que son 5 Caracteres o 10 dígitos hexadecimales ("0 a 9" "A a F", precedidos por la cadena "0x").
  - 128 bits.-, 13 Caracteres o 26 dígitos hexadecimales ("0 a 9" "A a F", precedidos por la cadena "0x").
  - 256 bits.-, 29 Caracteres o 58 dígitos hexadecimales ("0 a 9" "A a F",...).

4.2.7. CONFIGURACIÓN NETWORK

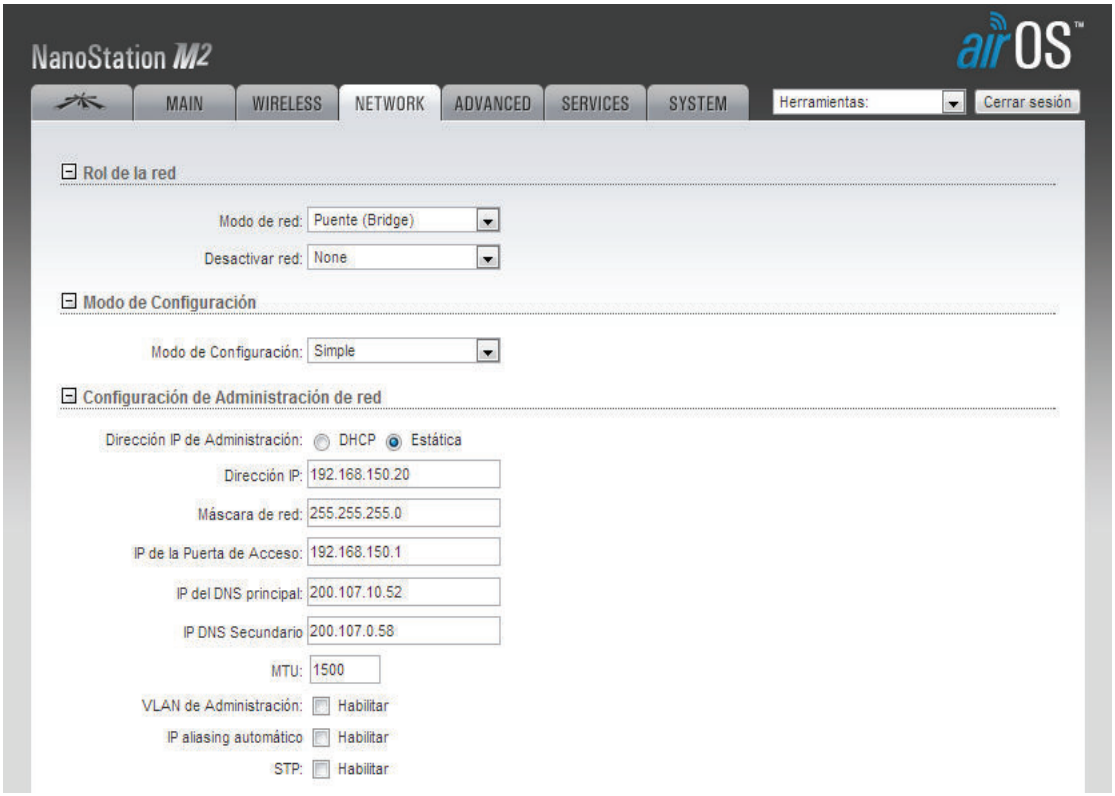


Gráfico 37.- Pantalla Network

Definimos la especificación de los servidores si deseamos que tenga una IP estática, caso contrario usamos DHCP.

4.2.8. CONFIGURACIÓN ESTÁNDAR

Gráfico 38.- Configuraciones de AIRMAX

Esta tecnología permite a los dispositivos conectarse entre sí con una frecuencia de 5.8 GHz. Permitiendo armarlos con repetidores y con la ventaja de un excelente alcance.

Para nuestro efecto se desactiva ya que no usaremos esta función.

4.2.9. RESUMEN DE LA CONFIGURACIÓN

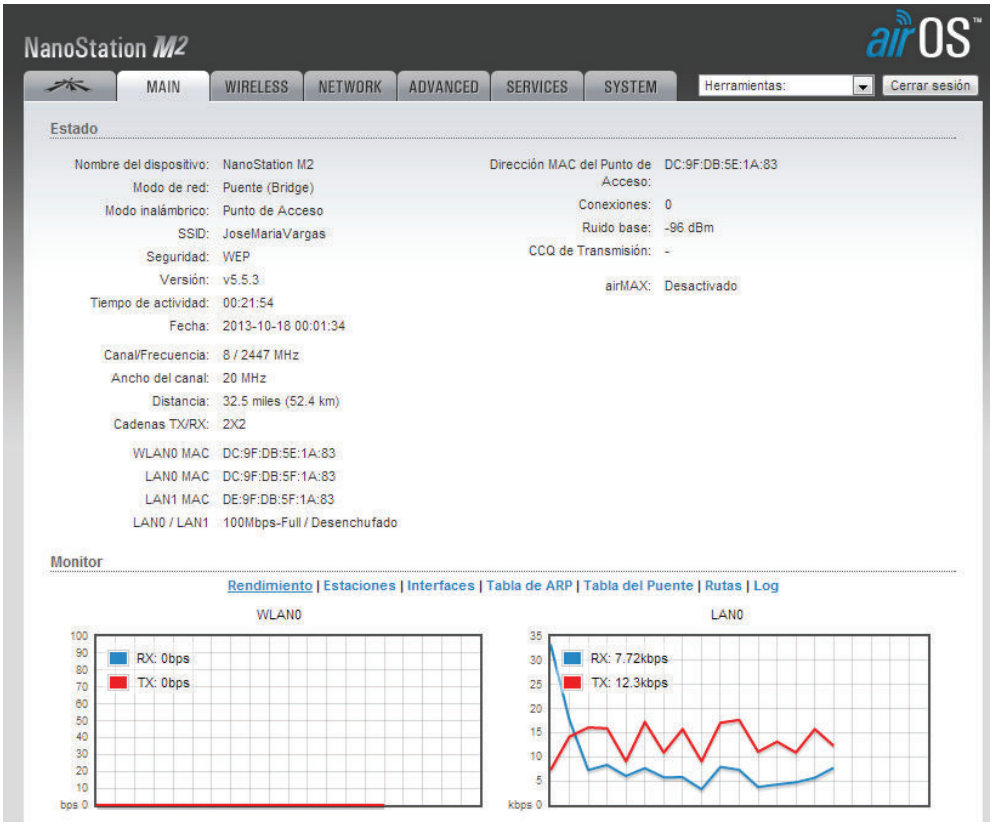


Gráfico 39.- Revisión MAIN

4.3. INSTALACIÓN FISICA DEL DISPOSITIVO

Al verificar la infraestructura se procedió a instalar sobre en el centro de cómputo ya que ahí es donde se puede cubrir a todo la escuela con la señal y se lanzó un cable Cat. 6 desde el switch que distribuye LAN.

De igual forma junto al switch se aseguró el adaptador POE. (Ver Anexo 3)

Para dar constancia a que los equipos fueron instalados se generó un Acta Entrega-Recepción de esta forma se evidencia la implantación de los dispositivos. (Ver Anexo 4)

4.4. CONFIGURACIÓN PARA EL CLIENTE

Ocultar el nombre de la red (SSID) es un método efectivo para asegurar su red, el cual evita que los usuarios no deseados accedan a su red, ya que el nombre de esta no aparece en la lista de las redes disponibles a las que pueden conectarse. Esta parte se mostrará cómo conectarse a una red inalámbrica con un SSID oculto. Antes de iniciar el procedimiento, asegúrese de saber cuáles son el nombre de red inalámbrica (SSID), el tipo de seguridad inalámbrica y la contraseña de red inalámbrica de la red oculta.

4.4.1. Configurar SSID

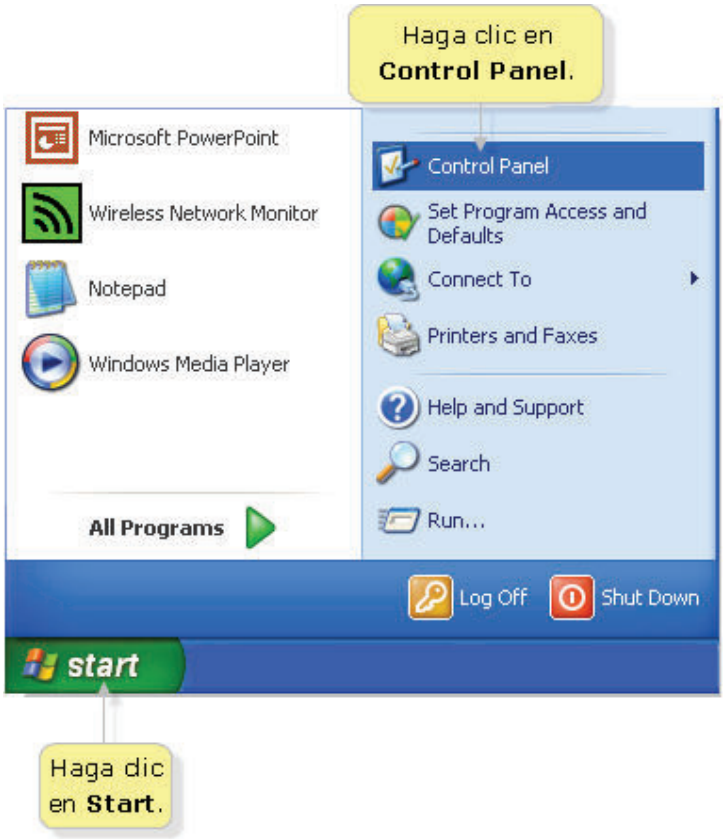


Gráfico 40.- Windows XP inicio

Seleccionamos el icono Network Connections (Conexiones de Red). Haga clic con el botón derecho del mouse en Wireless Network Connection (Conexión de Red Inalámbrica), luego seleccione Properties (Propiedades).

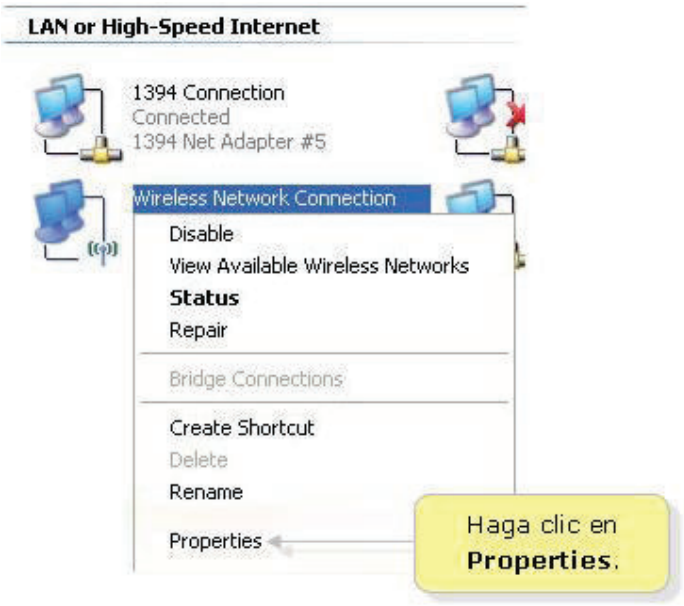


Gráfico 41.- Propiedades red

Seleccione la pestaña Wireless Networks (Redes Inalámbricas). Haga clic en la casilla "Use Windows to configure my wireless network settings" (Utilizar Windows para configurar los ajustes de mi red inalámbrica), luego haga clic en Add (Añadir).

Gráfico 42.- Wireless Network

- Realice las siguientes acciones en esta ventana:
  - Introduzca el nombre de su red inalámbrica en el campo Network name (SSID) (Nombre de red SSID).
  - Seleccione los ajustes específicos en Network Authentication (Autenticación de la Red) y Data Encryption (Criptografía de Datos) (consulte el tipo de seguridad inalámbrica).
  - Desactive la casilla The Key is provided for me automatically (La Clave la proporciono yo automáticamente), luego introduzca la contraseña inalámbrica en el campo Network key (Clave de la red).
  - Vuelva a introducir la contraseña en el campo Confirm network key (Confirmar la clave de red).
  - Una vez realizados todos los cambios, haga clic en OK.

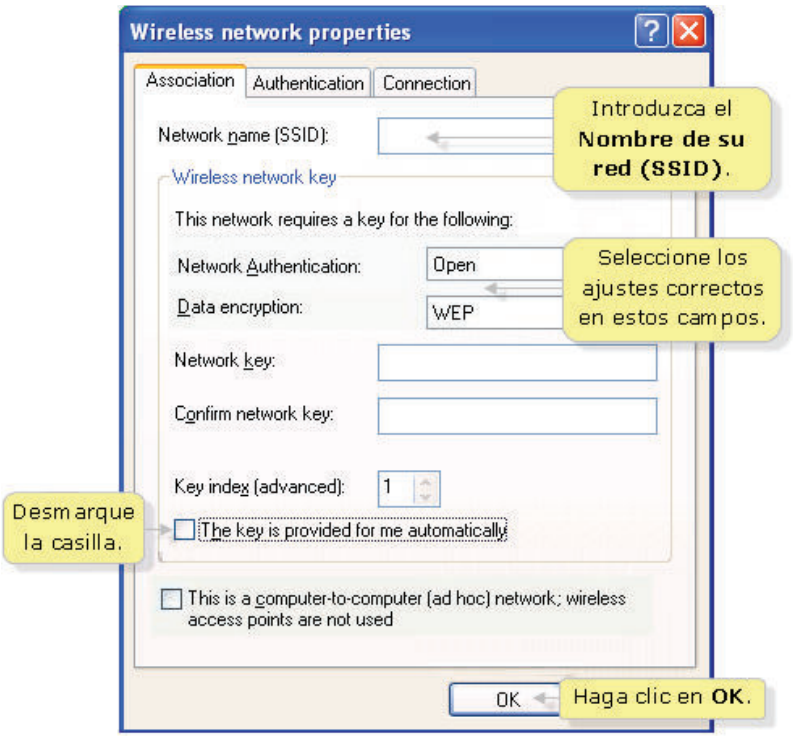


Gráfico 43.- Propiedades Wireless

Asegúrese de que la red aparezca en la lista Preferred networks (Redes preferidas), luego haga clic en OK.

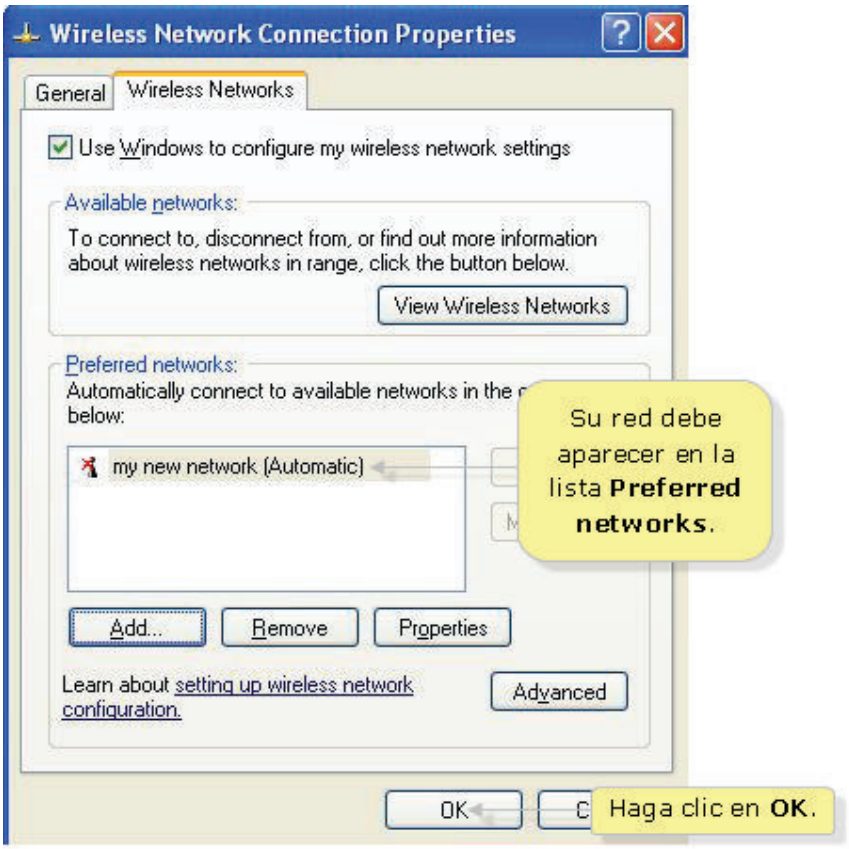


Gráfico 44.- Red Wireless Configurada

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Cada aula tiene una estación de trabajo, integrada con una tarjeta inalámbrica para hacer uso del servicio de Internet.
- La conexión permanente a Internet permite mejorar continuamente la enseñanza de los docentes.
- El acceso efectivo al servicio de Internet contribuye con el aumento de la eficiencia de un Docente ayudándole a cumplir sus tareas diarias.
- Al implementar una red inalámbrica el costo se lo puede considerar como un poco alto ya que los dispositivos de acceso inalámbrico, al llevar esta tecnología su valor se lo considera como un poco más elevado, pero en este caso el montar una red de cableado estructurado doblaría la inversión planteada.
- Las redes WLAN no son sustitutas de las redes LAN, al contrario cumple con el objetivo de complementarlas y lograr una eficiencia absoluta en el manejo de recursos de comunicación y transmisión.
- La óptima propagación de la red inalámbrica a través del Access Point está ligada a los obstáculos e interferencias que se presenten al momento de establecer comunicación con el receptor.
- Las redes WLAN son de gran ayuda para cubrir lugares de infraestructura irregular.
- El alcance del Access Point asegura el correcto funcionamiento de las estaciones conectadas dentro de la red.

RECOMENDACIONES

- Considerando la gran demanda de uso de redes inalámbricas en la actualidad es de suma importancia establecer políticas adecuadas para evitar accesos no autorizados e intrusos.
- Se recomienda que las estaciones de trabajo permanezcan en un lugar abierto dentro del aula u oficina.
- Se recomienda agregar bancos de memoria RAM en las estaciones de trabajo para otorgar un mejor rendimiento al momento de usar la red.
- Dentro del espacio que cubre las frecuencias 2.4 GHz, se la considera como bandas no licenciadas.
- Se recomienda que las próximas aulas que se creen, tengan establecido un espacio para la ubicación y aseguramiento de las estaciones de trabajo.
- Se recomienda no instalar varios Access Point sin previo análisis para su implementación y ubicación.
- Se recomienda crear un plan de control, para que cada periodicidad se obtenga una lista de MAC conectadas al dispositivo y verificar si no existen accesos no autorizados.
- Como administradores deberán cambiar la clave de acceso al Access Point cada cierto periodo determinado dentro de la institución, con esto se evitaría tener intrusos.
- Se recomienda que dentro del Access Point se plantee un plan de segmentación para distribuir adecuadamente el servicio de internet, ya que no es un servicio con la mayor velocidad requerida.
- Se recomienda siempre llevar un histórico de equipos y dispositivos conectados para solventar cualquier auditoria que pueda plantear el Ministerio de Educación.
- Se recomienda llevar estadísticas de tráfico de red para respaldar el uso del servicio ante las autoridades.

Bibliografía

ADRFormacion. (01 de Febrero de 2014). *Curso de Iniciación al Diseño de Redes WIFI Seguras*. Obtenido de http://www.adrformacion.com/cursos/wifi/leccion3/tutorial2.html

Alan Holt, C.-Y. H. (2010). *802.11 Wireless Networks: Security and Analysis.* New York: Springer.

ALOMIA. (14 de Mayo de 2013). *Tinyhippos-Injected*. Obtenido de http://mdm.unicundi.edu.co/repositorio/libres/servicios_red/DHCP/REDES/1/runtime.xml

Andreu, J. (2011). *Redes inalámbricas (Servicios en red).* Madrid: Editex.

Andreu, J. (2011). *Servicios DHCP (Servicios en red).* Madrid: Editex.

Bernhard H. Walke, S. M. (2007). *IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence.* England: John Wiley & Sons.

Carballar, J. A. (2010). *Wi-Fi : lo que se necesita conocer.* España: RC Libros.

Carmen de Pablos, J. J. (2004). *Informática y comunicaciones en la empresa.* Madrid: ESIC EDITORIAL.

ccnachamp.com. (11 de Diciembre de 2012). *Physical Layer*. Obtenido de http://ccna-routingswitching-ciscochamp.netai.net/1_25_Lecture-15-Physical-Layer.html

Colin, M. (12 de Junio de 2010). *Redes2*. Obtenido de http://red2marisolcolin.blogspot.com/2010/06/definicion-de-topologias-de-red.html

Dany. (11 de Junio de 2011). *IDENTIFICACIÓN DE LA INFRAESTRUCTURA DE REDES LAN INALÁMBRICAS.* Obtenido de http://configuracion-redes.blogspot.com/2011/06/blog-post_11.html

Ehrlich, S. D. (2011). *Access Points: An Institutional Theory of Policy Bias and Policy Complexity.* New York: Oxford.

Fernández, G. (06 de Enero de 2012). *TOPOLOGÍAS FÍSICAS DE RED*. Obtenido de https://gustavo2792.wordpress.com/tag/topologias/

Groth, D., & Skandier, T. (2005). *Guía del estudio de redes, (4ª edición).* Sybex: Inc. ISBN 0-7821-4406-3.

Henriquez, S. (04 de Octubre de 2011). *TIPOS DE REDES INFORMATICAS*. Obtenido de https://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/

HOME-NETWORK. (16 de Septiembre de 2014). *HOME-NETWORK-HELP.COM*. Obtenido de http://www.home-network-help.com/computer-networking-about.html

Infoepo11. (24 de Mayo de 2012). *Informática y Computación II*. Obtenido de https://infoepo11.wordpress.com/2012/05/24/3-3-3-de-acuerdo-a-su-topologia-estrella-anillo-arbol-bus-malla-hibrida/

INTEL. (27 de Octubre de 2014). *Redes Inalámbricas*. Obtenido de http://www.intel.com/support/sp/wireless/wlan/sb/cs-025321.htm

Jaime Gutierrez, J. T. (2003). *Protocolos Criptográficos y seguridad en redes (Primera Edición).* Santander: Graficas Calima.

Johan. (1 de Agosto de 2010). *EL BLOG DE LAS REDES*. Obtenido de http://elblogdelasredes.blogspot.com/p/red-por-relacion-funcional.html

Jomix. (05 de Febrero de 2011). *Modelo TCP/IP*. Obtenido de http://www.soycisco.com/2011/02/modelo-tcpip.html

José Manuel Huidobro, J. M. (2005). *Sistemas telemáticos.* Madrid: Editorial Paraninfo.

Julio Barbancho Concejero, J. B. (2014). *Redes locales.* España: Ediciones Paraninfo.

Kdocs. (12 de Febrero de 2007). *Diferencia entre WEP y WPA*. Obtenido de http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa/

Lehembre, G. (01 de Enero de 2006). *Seguridad Wi-Fi – WEP, WPA y WPA2.* Obtenido de http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Liu, A. X. (2011). *Firewall Design and Analysis.* Singapore: World Scientific Publishing.

Mailxmail. (05 de Octubre de 2014). *Redes Inalámbricas, el futuro de la Comunicación*. Obtenido de http://www.mailxmail.com/curso-redes-inalambricas-wi-fi-futuro-comunicacion/dispositivos-wireless

Microsoft. (01 de Enero de 2005). *El modelo TCP/IP*. Obtenido de https://msdn.microsoft.com/es-es/library/cc786900(v=ws.10).aspx

Microsoft. (01 de Enero de 2015). *¿Qué es un firewall?* Obtenido de http://windows.microsoft.com/es-xl/windows/what-is-firewall#1TC=windows-7

National Institute of Standards and Technology. (01 de Febrero de 2007). *Establishing Wireless Robust Security Networks.* Obtenido de http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

Orellana, M. (25 de Agosto de 2011). *Redes informáticas*. Obtenido de http://redesinformaticasmario.blogspot.com/

Pablo Gil Vázquez, J. P. (2010). *Redes y transmisión de datos.* Alicante: Compobell.

RengerTH. (13 de Noviembre de 2013). *Componentes, Protocolos y Topologias de Red*. Obtenido de

http://componentesprotocolosytopologiasdered.bligoo.com.ve/content/view/7218532/Topologias.html

Rodríguez, L. S. (07 de Septiembre de 2013). *Modelo OSI (Open System Interconnection)*. Obtenido de http://leonardosanchezrodriguez96.blogspot.com/2013_09_01_archive.html

Staff, U. (2010). Instalación y configuración de una red. *Técnico en Redes*, 11 - 115.

Ubiquiti Networks™. (01 de Enero de 2013). *Quick Start Guide.* Obtenido de http://dl.ubnt.com/guides/NanoStation_M/NanoStation_M_Loco_M_QSG.pdf

UNICEN. (01 de Enero de 2015). *El modelo OSI.* Obtenido de http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

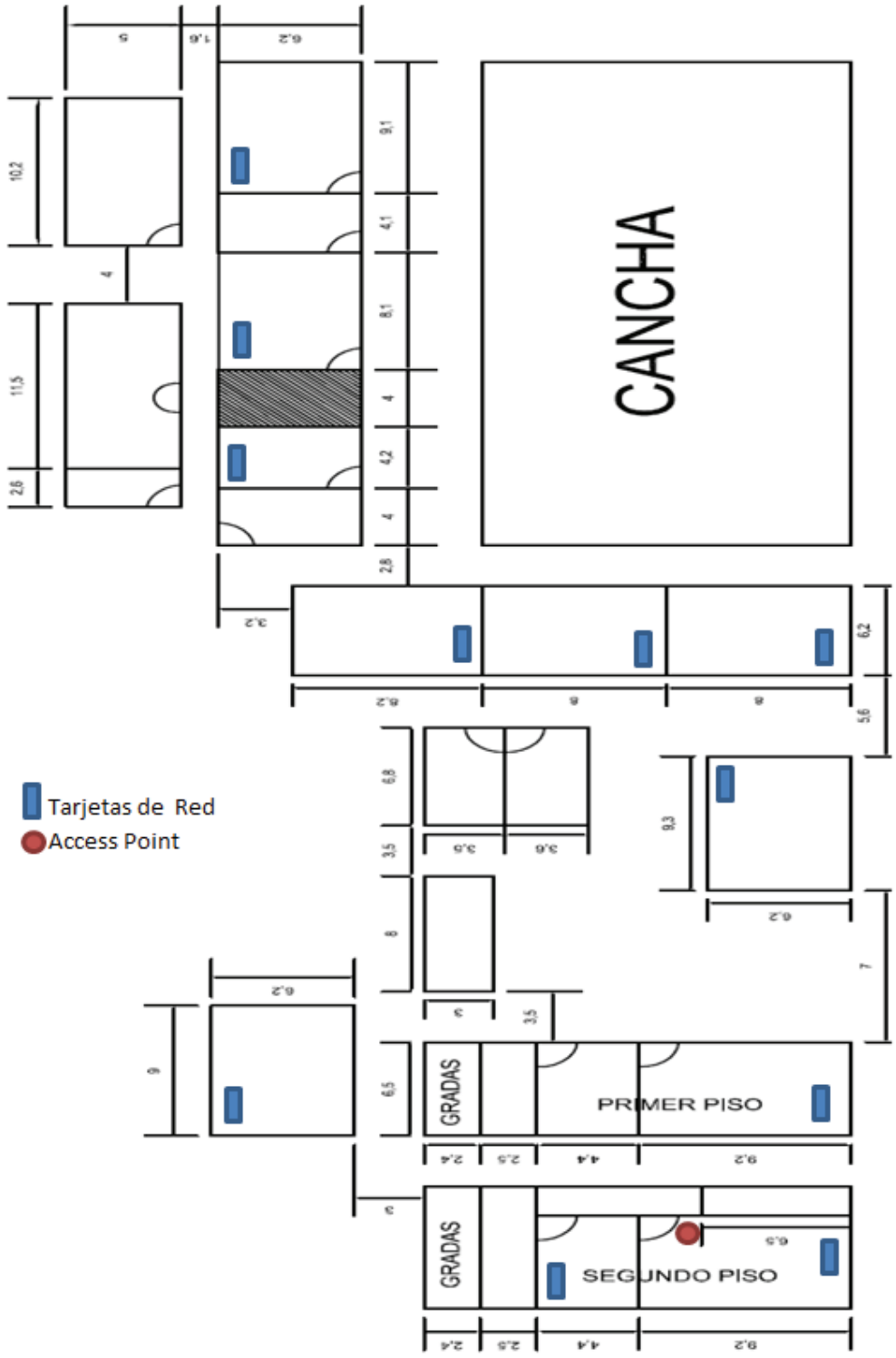
Voinea, J. G. (2011). *Redes de Comunicaciones. Administración y gestión.* Almeria: El Parador.

WETHERALL, A. S. (2012). *Redes de Computadores (Quinta edición).* Mexico: Pearson Education México.

Xavier Hesselbach Serra, J. A. (2002). *Análisis de redes y sistemas de comunicaciones.* Catalunya: Editions UPC.

ANEXOS

(Anexo1) Plano Institución



(Anexo2) Glosario de Términos

- **Access Point:** puente entre la red inalámbrica y la red cableada, actúa como un concentrador para los usuarios de dispositivos inalámbricos.
- **Ancho de Banda:** Determina la cantidad de megas que pueden "viajar" en una conexión. Se mide por lo general en bites o bits por segundo. Al contratar un proveedor de Internet, debemos tener claro cuál será su ancho de banda, y puede estar comprendida entre 64 Kbps (Kilo bits por segundo), 128 Kbps, 256, Kbps, 1 Mbps (Mega bit por segundo) o 2 Mbps.
- **Antena:** Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacía que punto emitan la señal, podemos encontrarlas direccionales u omnidireccional.
- **Bluetooth:** Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, etc.)que implementan esta tecnología ya que su FHSS/Hopping Pattern es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras. En cuanto a su implementación Bluetooth utiliza el termino piconet.
- **Un piconet** es un grupo de 2 u 8 aparatos que utilizan "Bluetooth" que comparten el mismo rango que es utilizado por un "Hopping Sequence", a su vez cada piconet contienen un aparato principal ("master") que es el encargado de coordinar el "Hopping Pattern" del piconet para que los demás aparatos "slaves" sean capaces de recibir información.
- **Bridge Puente:** Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.
- **Cliente Inalámbrico (Wireless Client):** Todo dispositivo susceptible de integrarse en una red wireless como PDAs, portátil, cámaras inalámbricas, impresoras, etc.

- **Broadcast:** Posibilidad de difundir programación, como lo hace la televisión, pero a través de la PC. Por ejemplo: una empresa con una Intranet puede capacitar a su personal facilitando un video de entretenimiento que aparecerá en cada una de las terminales de intranet.
- **Browser:** termino aplicado normalmente a los programas que permiten acceder al servicio WWW o también llamados navegadores (Netscape, Internet Explorer, etc.).
- **Certificado Digital (Certificate):** Es la certificación electrónica que emiten las Autoridades Certificadoras donde constan unos datos de verificación de firma a un signatario y confirma su identidad. Entre los datos figuran la fecha de emisión y la fecha de caducidad, la clave pública y la firma del emisor. Los certificados Digitales siguen las estipulaciones del estándar X.509. Este documento sirve para vincular una clave pública a una entidad o persona.
- **Clave Encriptación (Encryption Key):** Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente), en datos ciphertext (encriptados o cifrados) y viceversa.
- **Clave de Registro (Registry Key):** el registro (Registry) de Windows es un elemento en el que se guardan las especificaciones de configuración del PC mediante claves. Estas claves cambiaran de valor y/o se crearán cuando se instalen nuevos programas o se altere la configuración del sistema. Los virus pueden modificar estas claves para producir efectos dañinos.
- **Cliente / Servidor:** El servidor es una simple computadora que ha sido configurada con la aplicación de software adecuada para ofrecer los archivos que sean solicitados. El programa cliente es un browser que muestra los documentos que se seleccionan del WEB.
- **Cortafuegos (Firewall):** Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca ente una red e internet para asegurar que todas las comunicaciones se realicen

conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc.

- **CSMA/CD:** significa que la computadora escucha el cable de la red y espera hasta un periodo de silencio para poder mandar su mensaje. El CSMA/CD funciona de la siguiente manera: cuando una computadora desea mandar información primero escucha el cable de la red para revisar que no se esté usando en ese preciso momento (Carrier-Sense), cuando se produce una colisión las computadoras detectan la colisión y deciden reenviar su información a un intervalo al azar, es importante que sea al azar ya que si ambas computadoras tuvieran el mismo intervalo fijo se produciría un ciclo vicioso de colisiones y reenvíos (Colisión Detection).
- **Ethernet:** Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. En cooperación con DEC e Intelque. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Basse-T (o Fast Etthernet) soporta velocidades de 100 Mbps. Gigabit Ethernet soporta 1 Gb por segundo.
- **Estaciones de Trabajo:** Son máquinas que no son servidores pero que forman parte de la red de cómputo y en las cuales se centraliza todo el trabajo a realizar y las cuales están e intercomunicación permanente.
- **Fast (Flexible Authentication Secure Tunneling):** Protocolo de seguridad WLAN del tipo EAP. Desarrollado por Cisco y presentado a la IETF como borrado a principios de 2004. Impide los denominados ataques de diccionario por fuerza bruta enviado una autenticación de contraseña entre el cliente WLAN y el Access Point inalámbrico a través de un túnel cifrado. Elimina la necesidad de instalar servidores separados para tratar los certificados digitales empleados en otro sistema de seguridad WLAN (como el PEAP).

- **FTP (Protocolo de Transferencia de Archivos):** Permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombres de usuarios y contraseñas. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.
- **Gateway:** Puerta de acceso, dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red En las distintas normas o estándares se definen también los gateways o conversores que permiten por ejemplo, que una persona se pueda comunicar mediante un enlace ISDN bajo norma H.320 con alguien en internet utilizando H.323
- **Hacker:** Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.
- **Hacking:** Técnica de como descubrir los secretos y debilidades de los sistemas informáticos.
- **Hardware:** Todo lo físico que compone el equipamiento de una PC: la misma PC y sus componentes internos y todos sus periféricos, o sea lo que va conectado a ella, como por ejemplo la impresora, scanner, cámara video, parlantes, mouse, teclado, etc.
- **Host:** Ordenador conectado a Internet. También, cada uno de los ordenadores de una red que comparten recursos con otros conectados a la misma.
- **IAPP (Inter Access Point Protocol):** Protocolo de conexión entre puntos de acceso (AP), 802.11f
- **IEEE:** Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos. Asociación Norteamericana.
- **Interconexión:** es el medio por el cual se “unen” las maquinas con el fin de intercambiar información, haciendo así lo que se le llama red digital de computo.

- **Intranet:** Se llama así a las redes tipo internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW.
- **IP:** Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de Internet. También se refiere a las direcciones de red internet. Estas se componen de cuatro bytes (es decir, de dos números menores de 255) separados por puntos, de la siguiente forma. Por ejemplo: 128.114.6.100
- **ISO:** Internacional Standard Organization. Organización Internacional de Estándar. Patrocinada por la CCITT. Organización con sede en Genova, encargada de establecer (normas) internacionales.
- **ISP:** Internet Service Provider. Proveedor de Servicios Internet. Divididos en dos grandes grupos: los grandes proveedores (Impsat, Startel, Satlink), que son a su vez los dueños de sus propias redes, y los demás.
- **Navegador:** Visualizador especial que permite ver hipertexto y conectarse a los servidores Web para pedirles los documentos a los que apuntan los hiperenlaces.
- **Network Computer:** Ordenador de Red. Ordenador concebido para funcionar conectado a internet. Se trata de equipos de hardware muy reducido (algunos no tienen ni disco duro).
- **NET:** Red
- **OSI:** Open System Interconnection. Interconexión d Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuestos por la ISO. Divide las tareas de la red en siete niveles. También: modelo de capas de la ISO para organización de hardware y software genéricos para manejar integralmente las necesidades de procesamiento de datos y comunicaciones.
- **PAP:** Password Authentication Protocol. Protocolo de Autenticación por password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante password.

- **Paquete:** Cantidad mínima de datos que se transmite en una red o entre dispositivos. Tiene una estructura y longitud distinta según el protocolo al que pertenezca. También llamado trama.
- **PDA:** Persona Digital Assistant Personal Digital. Programa que se encarga de atender a un usuario concreto en tareas como búsquedas de información o selecciones atendiendo a criterios personales del mismo. Suele tener tecnología de IA (Inteligencia Artificial).
- **Ping:** Packet Internet Gropher. Rastreador de paquetes Internet. Programa utilizado para comprobar si un Host está disponible. Envía paquetes de control para comprobar si el host está activo y los devuelve.
- **Protocolo:** Serie de normas o especificaciones técnicas para las comunicaciones vía puerto serial (serie). Los protocolos soportados en los módems pueden variar de uno a otro.
- **Protocolo de Control de Transmision (TCP):** Protocolo orientado a la conexión de redes, establece una línea de dialogo entre el emisor y el receptor antes de que se transfieran los datos.
- **Protocolo Internet (IP):** Es el estándar que define la manera como se transmiten los mensajes a la maquinas que forman la red.
- **Proveedor de conexión:** Entidad que proporciona y gestiona enlace físico a Internet.
- **Proxy:** servidor Cache. El proxy es un servidor de que conectado normalmente al servidor de acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.
- **Access Point (Access Point AP):** Dispositivo Inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

- **PVC:** Permanent Virtual Circuit. Circuito Virtual Permanente. Línea punto a punto virtual establecida normalmente mediante conmutaciones de carácter permanente, es decir, a través de un circuito establecido.
- **Recursos:** Son todos y cada uno de los componentes de la red desde las piezas físicas hasta todos y cada uno de los programas usados para su operación.
- **Red:** Conjunto de computadores conectados con la finalidad de compartir recursos de software y hardware.
- **Router:** Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.
- **Roaming:** En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Access Point a otra sin interrumpir el servicio o perdida de conectividad.
- **Sniffer:** Herramienta que lee el tráfico de las redes Wireless que se encuentran en su alcance y permiten almacenarlo en ficheros para su posterior procesamiento. Además, en muchos casos, permiten relacionar los diferentes paquetes leídos y clasificados por conversaciones, protocolos, paso de claves, etc.
- **TCP/IP:** Transmision Control Protocol / Internet Protocol. Es un protocolo mediante el cual se comunican unas PC's con otras en Internet y es independiente de la plataforma. Es decir, puede funcionar en cualquier computadora, de manera que un PC puede comunicarse (cambiar datos) con una compatible PC. También se puede utilizar en redes locales.
- **Tarjeta de red Inalámbrica:** Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos.

- **Topologia:** es el tipo de forma que se le dará a la red, una vez que esté en construcción tales como: Anillo, Bus y Estrella.
- **VPN (Virtual Private Network):** Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autenticación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de Área Local (LAN).
- **WAN (Wide Área Network):** Red de Área Amplia es un tipo de red compuesta por dos o más redes de área local (LANs) conectas entre si vía telefónica (generalmente digital).
- **WIFI:** abreviaturas de Wireless Fidelity. Es el nombre comercial con que se conoce a todos los dispositivos que funcionan sobre la base de estándar 802.11 de transmisión inalámbrica. En el lenguaje popular: Red wi-fi
- **WLAN (Wireless Local Área Network):** Red de Área local Inalámbrica también conocido como red wireless. Permite a los usuarios comunicarse con una red local o a internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.
- **802.11:** En países que tienen restricciones sobre el uso de las frecuencias que este es capaz de utilizar. De esta forma se puede usar en cualquier parte del mundo.
- **802.11a:** Estándar de comunicaciones en la banda de los 5 Ghz.
- **802.11b:** Estándar de comunicaciones en la banda de los 2.4 Ghz.
- **802.11g:** Estándar que permite la comunicación en la banda de los 2.4 Ghz.
- **802.11n:** Estándar que define la encriptación y la autentificación para complementar, completar y mejorar el WEP. Es un estándar que mejorara la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).

(Anexo3) Instalación física del AP

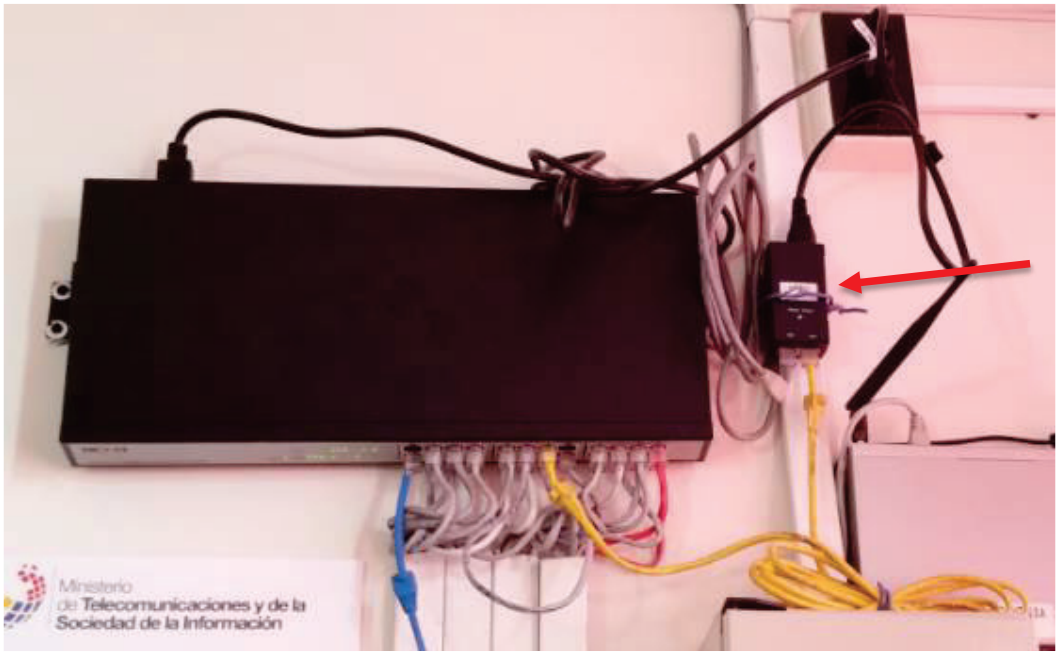


Gráfico 45.- Adaptador POE

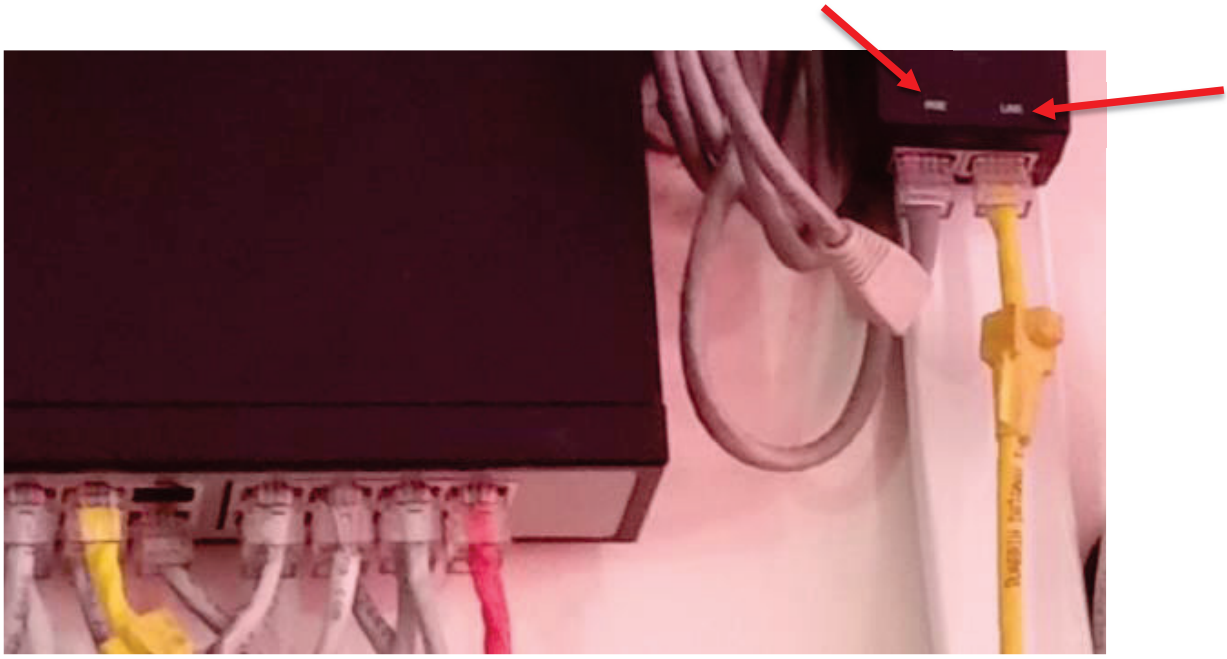


Gráfico 46.- Conexión LAN / POE

Gráfico 47.- Camino del UTP al AP

Gráfico 48.- Ubicación del AP

Gráfico 49.- Aseguramiento del AP

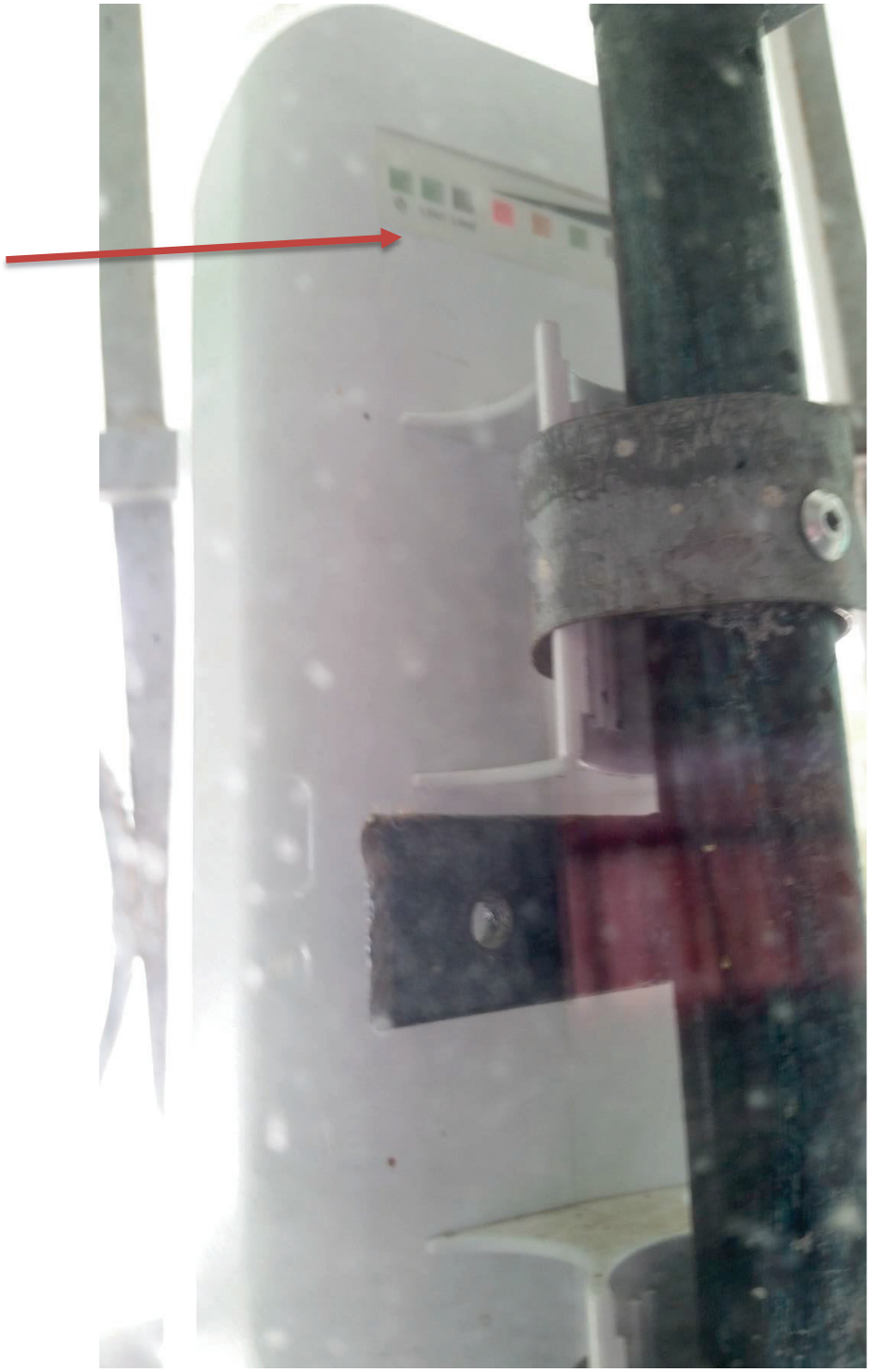


Gráfico 50.- Verificación de funcionalidad

(Anexo4) Acta Entrega-Recepción

ACTA DE ENTREGA-RECEPCIÓN

Proyecto: Implementación de una red WLAN que permita el acceso a la internet, a las PC´s de todas las aulas de la escuela fiscal mixta "José María Vargas" ubicada en el barrio de Santo Domingo de Conocoto.

Fecha: 23 de Febrero 2015

Por medio de este documento la Escuela "José María Vargas" da constancia que los dispositivos y accesorios implementados en la institución, no presentan ninguna falla y actualmente están operando sin novedades.

Los dispositivos y accesorios son los siguientes:

Cantidad	Detalle
1	Access Point Wireless Airmax Ubiquiti NanoStation M2 630mw 2.4Ghz Con Antena Panel 11 Dbi.
12	Tarjetas de red inalámbricas
1	Patch Cord 3t Panduit Cat 6
40	Metros de Cable UTP CAT. 6
1	Caja para soporte de AP
30	Canaletas Plásticas sin división Adhesiva PVC 20 X 12 Mm

Atentamente:

Lic. Azucena Delgado

DIRECTORA

Escuela "José María Vargas"

Cel. 0983476362

Telf. 2607-351