



FACULTAD DE: INFORMÁTICA Y CIENCIAS APLICADAS.

CARRERA: TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES.



TEMA:

Diseño de la infraestructura de red que permita mejorar la conectividad inalámbrica para la comunidad estudiantil, cuerpo docente y usuarios en general que acceden a Internet dentro y fuera de las instalaciones del edificio Benito Juárez de la Universidad Tecnológica de El Salvador.

PRESENTADO POR:

David Alexander Arriaga Herrera

Carlos José Reyes Juárez

Geovanny Alexander Romero Mejía.

PARA OPTAR AL GRADO DE:

Técnico en Ingeniería de Redes.

Marzo 2012

SAN SALVADOR, EL SALVADOR, CENTRO AMÉRICA.

INDICE

INTRODUCCION.....	i
CAPITULO I SITUACION ACTUAL.....	1
1.1. SITUACION PROBLEMÁTICA.....	1
1.2. JUSTIFICACION DEL PROYECTO.....	3
1.3. OBJETIVOS.....	3
1.4. ALCANCES.....	4
1.5. ESTUDIOS DE LAS FACTIBILIDADES.....	4
1.5.1. TECNICA.....	4
1.5.2. OPERACIONAL.....	6
1.5.3. ECONOMICA.....	6
CAPITULO II	
DOCUMENTACION TECNICA Y DISEÑO DE LA SOLUCION.....	8
2.1. MARCO TEORICO DE LA SOLUCION.....	8
2.2. DOCUMENTACION TECNICA DE LA SOLUCION.....	10
2.2.1 ¿QUE SON LAS REDES?.....	10
2.2.2 CLASIFICACION DE LAS REDES.....	11
2.2.3 TIPO DE CONEXIÓN.....	15
2.2.4 TOPOLOGIAS DE RED.....	17
2.2.5 ¿QUE ES UNA RED INALAMBRICA ?.....	22

2.2.6 TIPOS DE REDES INALAMBRICAS.....	23
2.2.7 VENTAJAS DE LAS REDES INALAMBRICAS.....	25
2.2.8 DESVENTAJAS DE LAS REDES INALAMBRICAS.....	27
2.2.9 MEDIOS DE TRANSMISION INALAMBRICOS.....	29
2.2.10 TECNOLOGIA DE REDES INALAMBRICAS.....	31
2.2.11 CLASES DE TECNOLOGIAS MÁS UTILIZADAS.....	33
2.2.12 PROTOCOLOS DE RED INALAMBRICA.....	37
2.2.13 VELOCIDADES DE RED.....	46
2.2.14 SEGURIDAD DE REDES INALAMBRICAS.....	47
2.2.15 COMPONENTES DE UNA RED INALAMBRICA.....	58
 CAPITULO III PROPUESTA DE LA SOLUCION.....	 72
3.1. PROPUESTA DE SOLUCION.....	72
3.1.1 PLANTEAMIENTO DEL PROYECTO TEMATICO.....	73
3.1.2 CRONOGRAMA DE ACTIVIDADES.....	76
3.1.3 TECNOLOGIAS Y RECURSOS SELECCIONADOS.....	77
3.1.4 DISEÑO DE LA PROPUESTA.....	83
3.1.5 DISEÑO DE LA RED.....	87
3.1.6 TOPOLOGIA DE LA RED.....	88
3.1.7 IMPLEMENTACION DE LA PROPUESTA.....	89
3.1.8 PRESENTACION DE LA PROPUESTA.....	90
3.1.8.1 OFERTA TECNICA.....	90
3.1.8.2 OFERTA ECONOMICA.....	91
3.1.9 EVIDENCIAS DEL PROYECTO.....	92

CONCLUSIONES.....	94
RECOMENDACIONES.....	95
BIBLIOGRAFIA.....	96
ANEXO.....	97
GLOSARIO.....	104

INTRODUCCIÓN.

El presente trabajo se realizó en las instalaciones de la universidad tecnológica de El Salvador, por estudiantes de la carrera de Técnico en Ingeniería de Redes Computacionales, sobre el tema de Diseño de la infraestructura de red que permita mejorar la conectividad inalámbrica para la comunidad estudiantil, cuerpo docente y usuarios en general que acceden a Internet dentro y fuera de las instalaciones del edificio Benito Juárez de la Universidad Tecnológica de El Salvador.

En este documento se especifica la investigación de la problemática de la red actual del edificio Benito Juárez, se presenta una solución basada en especificaciones técnicas de los dispositivos de red y estándares de las redes inalámbricas, se presenta la solución a la topología de red así como también el rediseño de la red inalámbrica con sus respectivas mejoras.

Cabe mencionar que el presente trabajo contiene un amplio contenido acerca de las redes computacionales su clasificación y características y factores de importancia para dar mayor comprensión al lector al igual que la comprensión del desarrollo del trabajo de investigación y la propuesta del mejoramiento de red del edificio Benito Juárez de la Universidad Tecnológica de El Salvador.

CAPITULO I

SITUACIÓN ACTUAL

1.1 SITUACIÓN PROBLEMÁTICA.

La situación del problema de la red inalámbrica del Edificio Benito Juárez de la Universidad Tecnológica de El Salvador, es evidente que para los estudiantes, cuerpo docente y usuarios en general. Que la conectividad a la red inalámbrica es limitada y en algunas zonas del edificio no hay señal, el edificio está compuesto por cinco niveles y un sótano. La investigación descubrió que en el sótano del edificio no hay conectividad y los dispositivos no detectan ninguna red de la Universidad Tecnológica de El Salvador, en el primer piso esta la biblioteca hay un punto de acceso cerca de la puerta en el segundo piso existe una barra point instalada que esta fuera de uso, también en el segundo piso del edificio hay un punto de acceso cerca de las gradas de acceso principal pero a pesar de eso la conectividad es mínima en la mayoría del piso, en el tercer piso no existe punto de acceso y no hay conectividad, en el cuarto piso existe un punto de acceso justo en medio del pasillo pero está fuera de servicio y no hay conectividad, en el quinto piso hay punto de acceso y la conectividad a la red también es nula.

Lo que genera atrasos, complicaciones e inconformidad en las operaciones relacionas con el aprendizaje de los estudiantes, impide el acceso inmediato a los docentes a las herramientas de red, por ejemplo corregir notas, subir archivos para las actividades de la materia entre otras situaciones en las que la red inalámbrica sería de gran utilidad su cobertura total como su rápido acceso. Por lo que es urgente resolver el problema de conectividad inalámbrica de la red en todo el edificio y sus alrededores cercanos, lo antes posible para facilitar las operaciones internas de aprendizaje dentro y a la redonda del edificio Benito Juárez, para los usuarios antes mencionados. Veremos un cuadro de la situación actual Cuadro 1.1 del edificio por nivel para entrar en detalles.

Nivel	Situación actual
Sótano	Ausencia total de la Señal, existen pruebas que hubieron puntos de acceso pero fueron removidos
Nivel 1	Existe señal solo dentro de la biblioteca. Y a siete metro máximo fuera de esta.
Nivel 2	Existe un punto de acceso pero no hay señal de red
Nivel 3	No hay señal ni punto de acceso
Nivel 4	Hay un punto de acceso justo en medio del pasillo pero no hay conexión, el punto de acceso está apagado
Nivel 5	Hay un punto de acceso pero no hay señal

Cuadro 1.1 situación actual de la red

1.2 JUSTIFICACIÓN DEL PROYECTO

Este proyecto plantea la solución a los problemas de conectividad de la red del edificio Benito Juárez de la Universidad Tecnológica de El Salvador, el beneficio en general de la mejora de red será el acceso rápido y en cualquier lugar del edificio, aulas, pasillos y sus alrededores cercanos a la red interna de la universidad. Un aspecto específico del diseño de esta mejora de red, será la correcta distribución de los puntos de acceso en todo el edificio logrando así conectividad en toda la estructura, para toda aquella persona que se desee conectar teniendo el dispositivo adecuado, por ejemplo estudiantes, docentes y particulares.

1.3 OBJETIVOS

GENERAL.

Diseñar una infraestructura de red que permita mejorar la conectividad inalámbrica actual del edificio Benito Juárez de la universidad tecnológica de el salvador beneficiando a la comunidad estudiantil, cuerpo docente y usuarios en general que acceden a Internet dentro y fuera de las instalaciones

ESPECÍFICOS

- Identificar el problema de conectividad inalámbrica del edificio Benito Juárez de la Universidad Tecnológica de El Salvador cuales son los puntos donde existe conectividad.

- Examinar los dispositivos en uso actualmente para lograr conectividad inalámbrica en el edificio Benito Juárez de la Universidad Tecnológica de El Salvador
- Elaborar una propuesta de mejoramiento de red inalámbrica para el mejorar la red inalámbrica del edificio Benito Juárez de la Universidad Tecnológica de El Salvador

1.4 ALCANCES

- Puntos de acceso de mayor rango de conectividad, empleando dispositivos de red de mayor rango de alcance se lograra una cobertura total en el edificio Benito Juárez de la Universidad Tecnológica de El Salvador
- Propuesta a escala de la distribución de los puntos de acceso a la red, con la buena distribución de los puntos de acceso se lograra mayor conectividad en aulas, pasillos y los alrededores del edificio Benito Juárez de la Universidad Tecnológica de El Salvador beneficiando a la comunidad estudiantil, cuerpo docente y usuarios en general.

1.5 ESTUDIOS DE LAS FACTIBILIDADES.

1.5.1 TÉCNICA:

Con lo investigado haciendo énfasis en la situación que se presenta y recurriendo causas y beneficios que se obtendrán al hacer uso de una nueva

tecnología y distribución de una red inalámbrica en el edificio Benito Juárez de la Universidad Tecnológica de El Salvador teniendo en cuenta que es un ámbito de frecuencia de mayor cobertura en comparación con la red actual, en la red actual hay tres puntos de acceso uno situado en la biblioteca otro en el segundo piso y el tercero en el cuarto piso, pero solamente está habilitado el punto de acceso que se ubica en la biblioteca del edificio, la propuesta de diseño contemplará la distribución y cantidad de puntos de acceso por piso dentro del edificio como también afuera

El equipo existente en el edificio es el siguiente cuadro 1.2 todos los puntos de acceso cuya marca es 3com, están instalados en la parte interior del edificio en mención.

nivel	Cantidad de puntos de acceso
Sótano	0 punto de acceso
Primer piso	2 punto de acceso
Segundo piso	1 punto de acceso 1 barra point en la parte externa del edificio Benito Juárez
Tercer piso	0 punto de acceso
Cuarto piso	1 punto de acceso
Quinto piso	1 punto de acceso

Cuadro: 1.2 cantidad de puntos de acceso actuales

1.5.2 OPERACIONAL.

Durante la elaboración de la propuesta del mejoramiento de red del edificio Benito Juárez de la Universidad Tecnológica de El Salvador, se considera tiempo a utilizar de tres meses, cuyos pasos se desglosan de la siguiente manera:

- 1- Pruebas de campo dentro del edificio en cuestión para probar el rango de la conectividad, e identificar los dispositivos en uso.
- 2- Investigación de dispositivos adecuados para la funcionabilidad de la red y su cobertura total en el edificio
- 3- Elaboración de presupuesto incluyendo todos los dispositivos y materiales de red a utilizar en la propuesta.
- 4- Prueba de la cobertura con la nueva distribución de los dispositivos de red en el edificio para evidenciar su cubierta uniforme.
- 5- Planificación y elaboración de una maqueta a escala del edificio, para demostrar la distribución adecuada de los puntos de acceso dentro y fuera del edificio en cuestión.

1.5.3 ECONÓMICO.

Considerando el trabajo que se desarrollara la función principal es el diseño de una infraestructura de red, a lo cual el costo será de cero inversión por parte de los encargados del proyecto: Diseño de una infraestructura de red que permita

mejorar la conectividad inalámbrica para la comunidad estudiantil, cuerpo de docentes y usuarios en general que acceden a Internet dentro y fuera de las instalaciones del edificio Benito Juárez de la Universidad Tecnológica de El Salvador, además el beneficio será del 100% para las personas que deseen conectarse a esa infraestructura.

CAPITULO II

DOCUMENTACIÓN TÉCNICA Y DISEÑO DE LA SOLUCIÓN.

2.1 MARCO TEÓRICO DE LA SOLUCIÓN.

En el presente trabajo se tomara en cuenta los problemas de conectividad de red del edificio Benito Juárez de la Universidad Tecnológica de El Salvador, la importancia de una red inalámbrica de mayor cobertura que la actual, lo importante de esta solución es el diseño de la distribución correcta de los puntos de acceso dentro del edificio para la mayor cobertura de la señal, en el desarrollo del tema se dan a conocer de forma indispensable ¿que son las redes inalámbricas? ¿Cuáles son los dispositivos de red que se utilizan para implementar las redes inalámbricas? ¿Cuáles son los dispositivos que se usaran en la propuesta del mejoramiento de red?

La tecnología de red inalámbrica es una herramienta de productividad esencial para los profesionales de hoy cada día más móviles. Con una red inalámbrica, los usuarios pueden permanecer conectados a las aplicaciones de productividad y a los recursos informativos prácticamente en todo momento y lugar. La red inalámbrica la transmisión de datos de manera flexible y segura sin la necesidad de ceñirse al cableado instalado. Envía todos los datos necesarios a través de ondas de radio. Gracias a esta tecnología se puede

llegar hasta donde no el cable no llega, o este es demasiado costoso o complicado de instalar.

La red inalámbrica es un perfecto sustituto del cableado tradicional para montar una red local. En lugar de transmitir la información por medio de cable, se transmiten a través de ondas de radio cifradas, con lo que se elimina una costosa y problemática instalación. Esto permite la perfecta movilidad de los equipos en red dentro del radio de cobertura de la red inalámbrica. El término red inalámbrica o Wireless Network en inglés es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física. Una de sus principales ventajas es notable en los costos, ya que se elimina todo el cable Ethernet¹ y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

En la actualidad las redes inalámbricas son una de las tecnologías más prometedoras y con diferentes ventajas tomando en cuenta las siguientes:

- Comodidad. Acceda a sus recursos de red desde cualquier ubicación dentro del área de cobertura de su red inalámbrica o desde cualquier punto de acceso
- Movilidad. Estar atado a un escritorio, como ocurría con una conexión por cable.

¹estándar de redes de área local

- Productividad. El acceso inalámbrico a Internet , a las aplicaciones y recursos.
- Instalación sencilla. No se instalan cables, por tanto, la instalación puede ser rápida y económica.
- Capacidad de ampliación. Puede ampliar fácilmente las redes inalámbricas con el equipo existente, mientras que una red por cable requiere cableado adicional.
- Coste. Puesto que las redes inalámbricas eliminan o reducen los costes de cableado, su funcionamiento puede resultar más económico que el de las redes por cable.

2.2 DOCUMENTACIÓN TÉCNICA DE LA SOLUCIÓN.

2.2.1¿QUÉ SON LAS REDES?

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos y ofrecer servicios. Este término también engloba aquellos medios técnicos que permiten compartir la información.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la

disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones.

2.2.2 CLASIFICACIÓN DE LAS REDES

RED DE ÁREA PERSONAL o PAN (personal area network) Es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona.

REDES DE ÁREA LOCAL o LAN (local area network) Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña. Estas redes son usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión por lo general broadcast², alta velocidad y topología.

Son redes con velocidades entre 10 y 100 Mbps, tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos.

Dentro de este tipo de red podemos nombrar a intranet, una red privada que utiliza herramientas tipo internet, pero disponible solamente dentro de la organización.

² transmisión de un paquete

REDES DE ÁREA METROPOLITANA o MAN (metropolitan area network) Es una versión de mayor tamaño de la red local. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos. La razón principal para distinguirla de otro tipo de redes, es que para las MAN's se ha adoptado un estándar llamado DQDB (Distributed-Queue Dual Bus) o IEEE 802.6. Utiliza medios de difusión al igual que las Redes de Área Local.

RED DE ÁREA DE CAMPUS o CAN (campus area network) es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar.

REDES DE AMPLIA COBERTURA o WAN (wide area network) Son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales (endsystem). Los sistemas finales están conectados a una subred de comunicaciones. La función de la subred es transportar los mensajes de un host a otro.

En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio o Conmutación³. Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.

³ es el envío de datos en una red

Las redes de área local son diseñadas de tal forma que tienen topologías simétricas, mientras que las redes de amplia cobertura tienen topología irregular. Otra forma de lograr una red de amplia cobertura es a través de satélite o sistemas de radio.

RED DE ÁREA DE ALMACENAMIENTO o SAN (storage area network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte.

RED DE ÁREA LOCAL VIRTUAL (Virtual LAN, VLAN) es un grupo de computadoras con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast (dominio de broadcast) en la capa de enlace de datos, a pesar de su diversa localización física.

RED IRREGULAR es un sistema de cables y buses que se conectan a través de un módem, y que da como resultado la conexión de una o más computadoras. Esta red es parecida a la mixta, solo que no sigue los parámetros presentados en ella. Muchos de estos casos son muy usados en la mayoría de las redes.

RED COLUMNA VERTEBRAL (Backbone Network) También llamada Red de Transporte (Carrier Network). Este tipo de red cubre, por lo general, un país o un continente. Sirve como apoyo a las empresas que poseen redes locales y no

pueden costear la inversión en la infraestructura y mantenimiento de una red de área extendida propia.

RED INTERNACIONAL (INTERNETworking) También llamada Telaraña de área Mundial (World Wide Web). Es una enorme red de redes que se enlaza a muchas de las redes científicas, de investigación y educacionales alrededor del mundo así como a un número creciente de redes comerciales.

DIFERENCIAS ENTRE UNA LAN Y UNA WAN

LAN:

- 1) Canales de difusión
- 2) Pocos kilómetros
- 3) Velocidad de varios mbps⁴
- 4) Una sola organización
- 5) Libertad de elegir el medio físico de comunicación
- 6) Canal confiable (tasa de error 1000 menor que en Wan)
- 7) Estructura simple para el manejo de errores
- 8) Protocolos más sencillos, sin importar mucho el rendimiento.

⁴ Mega Bits por Segundo

WAN:

- 1) Canales punto a punto (excepto satélites)
- 2) Incluye países enteros
- 3) Velocidad menor a 1 Mbps
- 4) Varias organizaciones
- 5) Obligación de utilizar servicios públicos (ej. Red telefónica)
- 6) Canal poco confiable
- 7) Estructura compleja para el manejo de errores
- 8) Búsqueda para un gran rendimiento.

2.2.3 TIPO DE CONEXIÓN

MEDIOS GUIADOS

- El cable coaxial se utiliza para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes.

- El cable de par trenzado es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes.
- La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

MEDIOS NO GUIADOS

- Red por radio es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red. Es un tipo de red muy actual, usada en distintas empresas dedicadas al soporte de redes en situaciones difíciles para el establecimiento de cableado, como es el caso de edificios antiguos no pensados para la ubicación de los diversos equipos componentes de una Red de ordenadores.
- Red por infrarrojos. Las redes por infrarrojos no permiten la comunicación entre dos nodos, usando una serie de leds⁵ infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala.
- Esa es su principal desventaja, a diferencia de otros medios de transmisión inalámbricos (Bluetooth, Wireless, etc.).

⁵Es un diodo semiconductor que emite luz

- Red por microondas es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. El protocolo más frecuente es el IEEE 802.11b y transmite a 2.4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo). Otras redes utilizan el rango de 5,4 a 5,7 GHz para el protocolo IEEE⁶ 802.11a

2.2.4 TOPOLOGÍAS DE RED:

La topología de una red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (en computadoras, impresoras, servidores, hubs, switches, enrutadores, etc.) se interconectan entre sí sobre un medio de comunicación.

a) **Topología física:** Se refiere al diseño actual del medio de transmisión de la red

b) **Topología lógica:** Se refiere a la trayectoria lógica que una señal a su paso por los nodos de la red.

Existen varias topologías de red básicas (ducto, estrella, anillo y malla), pero también existen redes híbridas que combinan una o más de las topologías anteriores en una misma red.

⁶*Institute of Electrical and Electronic Engineers*

TOPOLOGÍA DE BUS

Una topología de ducto o bus figura 2.1 está caracterizada por una dorsal principal con dispositivos de red interconectados a lo largo de la dorsal. Las redes de ductos son consideradas como topologías pasivas. Las computadoras "escuchan" al ducto. Cuando éstas están listas para transmitir, ellas se aseguran que no haya nadie más transmitiendo en el ducto, y entonces ellas envían sus paquetes de información. Las redes de ducto basadas en contención (ya que cada computadora debe contender por un tiempo de transmisión) típicamente emplean la arquitectura de red ETHERNET.

Las redes de bus comúnmente utilizan cable coaxial como medio de comunicación, las computadoras se conectaban al ducto mediante un conector BNC en forma de T. En el extremo de la red se ponía un terminador (si se utilizaba un cable de 50 ohm, se ponía un terminador de 50 ohm también).

Las redes de ducto son fáciles de instalar y de extender. Son muy susceptibles a quebraduras de cable, conectores y cortos en el cable que son muy difíciles de encontrar. Un problema físico en la red, tal como un conector T, puede precipitar toda la red.

Figura 2.1 topología bus



TOPOLOGÍA DE ESTRELLA

En una topología de estrella, figura 2.2 las computadoras en la red se conectan a un dispositivo central conocido como concentrador o a un conmutador de paquetes. En un ambiente LAN cada computadora se conecta con su propio cable típicamente par trenzado a un puerto del hub o switch.

Debido a que la topología estrella utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el hub o switch aunque se pueden conectar hubs o switches en cadena para así incrementar el número de puertos. La desventaja de esta topología es la centralización de la comunicación, ya que si el switch falla, toda la red se cae.

Hay que aclarar que aunque la topología física de una red Ethernet basada en switch es estrella, la topología lógica sigue siendo basada en ducto.

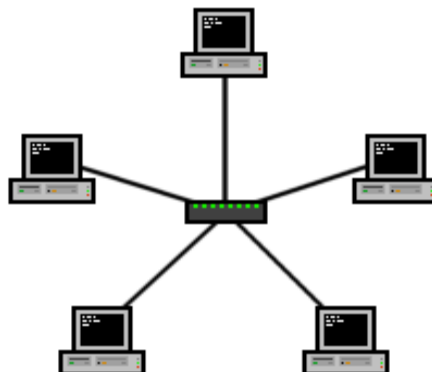


Figura 2.2 topología estrella.

TOPOLOGÍA DE ANILLO.

Una topología de anillo figura 2.3 conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. La topología de anillo mueve información sobre el cable en una dirección y es considerada como una topología activa. Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora en la red.

El acceso al medio de la red es otorgado a una computadora en particular en la red por un "token". El token⁷ circula alrededor del anillo y cuando una computadora desea enviar datos, espera al token y posiciona de él. La computadora entonces envía los datos sobre el cable. La computadora destino envía un mensaje a la computadora que envió los datos que fueron recibidos correctamente. La computadora que transmitió los datos, crea un nuevo token y los envía a la siguiente computadora, empezando el ritual de paso de token o estafeta (tokenpassing) nuevamente.

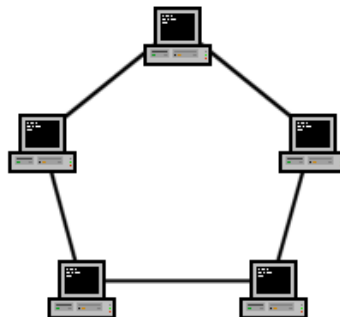


Figura 2.3 topología de anillo.

⁷ es un dispositivo electrónico que se le da a un usuario autorizado de un servicio

TOPOLOGÍA DE MALLA.

La topología de malla figura 2.4 utiliza conexiones redundantes entre los dispositivos de la red ahí como una estrategia de tolerancia a fallas. Cada dispositivo en la red está conectado a todos los demás todos conectados con todos. Este tipo de tecnología requiere mucho cable cuando se utiliza el cable como medio, pero puede ser inalámbrico también. Pero debido a la redundancia, la red puede seguir operando si una conexión se rompe.

Las redes de malla, obviamente, son más difíciles y caras para instalar que las otras topologías de red debido al gran número de conexiones requeridas.

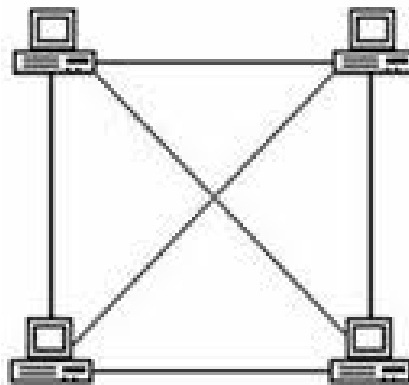


Figura 2.4 topología de malla

2.2.5 ¿QUÉ ES UNA RED INALÁMBRICA?

Una red inalámbrica es, como su nombre lo indica, una red en la que dos o más terminales por ejemplo, ordenadores portátiles, agendas electrónicas, etc. se pueden comunicar sin la necesidad de una conexión por cable.

Una red inalámbrica (Wireless network en inglés) ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.

Una de sus principales ventajas es notable en los costos, ya que se elimina casi todo el cable ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

Pero el término suele utilizarse más para referirse a aquellas redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin cables.

Las redes inalámbricas de telecomunicaciones son generalmente implementadas con algún tipo de sistema de transmisión de información que usa ondas electromagnéticas, como las ondas de radio.

Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema.

Categorías Existen dos categorías de las redes inalámbricas.

Larga distancia: estas son utilizadas para distancias grandes como puede ser otra ciudad u otro país.

Corta distancia: son utilizadas para un mismo edificio o en varios edificios cercanos no muy retirados.

2.2.6 TIPOS DE REDES INALÁMBRICAS

WPAN: Wireless Personal Area Network

En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central, en Bluetooth se requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo, RFID sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

WLAN: Wireless Local Area Network

En las redes de área local podemos encontrar tecnologías inalámbricas basadas en HIPERLAN (del inglés, High Performance Radio LAN), un estándar

del grupo ETSI, o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.

WirelessMetropolitanArea Network

Para redes de área metropolitana se encuentran tecnologías basadas en WiMAX (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service).

Wireless Wide Area Network

Una WWAN difiere de una WLAN (wireless local área network) en que usa tecnologías de red celular de comunicaciones móviles como WiMAX (aunque se aplica mejor a Redes WMAN), UMTS (Universal Mobile telecommunications System) GPRS, EDGE, CDMA2000, GSM, CDPD, Nobitex, HSPA y 3G para transferir los datos . También incluye LMDS y Wi-Fi autónoma para conectar a internet.

2.2.7 VENTAJAS DE LAS REDES INALÁMBRICAS

Las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son las siguientes:

Movilidad. La libertad de movimientos es uno de los beneficios más evidentes las redes inalámbricas. Un ordenador o cualquier otro dispositivo por ejemplo, una PDA⁸ o una webcam pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de que si es posible o no hacer llegar un cable hasta este sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos.

Compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

Desplazamiento. Con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

⁸ también denominado ordenador de bolsillo u organizador personal

Flexibilidad. Las redes inalámbricas no solo nos permiten estar conectados mientras nos desplazamos por una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red. A veces extender una red cableada no es una tarea fácil ni barata. En muchas ocasiones acabamos colocando peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten en la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

Ahorro de costes. Diseñar o instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costos al permitir compartir recursos: acceso a Internet, impresoras, etc.

Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado quede instalado.

2.2.8 DESVENTAJAS DE LAS REDES INALÁMBRICAS

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tiene unos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

Menor ancho de banda. Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.

Mayor inversión inicial. Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

Seguridad. Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella.

Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

Interferencias. Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 Ghz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi ⁹ funcionan en la misma banda de frecuencias incluida la de los vecinos.

Este hecho hace que no se tenga la garantía de nuestro entorno radioelectrónico este completamente limpio para que nuestra red inalámbrica

⁹ mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

Incertidumbre tecnológica. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11B). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual.

Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.

2.2.9 MEDIOS DE TRANSMISIÓN INALÁMBRICOS.

Según el rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser las ondas de radio, las microondas terrestres o por satélite, y los

infrarrojos, por ejemplo. Dependiendo del medio, la red inalámbrica tendrá unas características u otras:

ONDAS DE RADIO: las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30 Hz¹⁰, hasta la banda UHF que va de los 300 a los 3000 MHz,

MICROONDAS TERRESTRES: se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar en enlaces punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.

MICROONDAS POR SATÉLITE: se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal (denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuencia les de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta

¹⁰hertzio o hertz

frecuencia se mezclan bastante, así que pueden haber interferencias con las comunicaciones en determinadas frecuencias.

INFRARROJOS: se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz.

2.2.10 TECNOLOGÍA DE REDES INALÁMBRICAS.

¿QUÉ ES LA TECNOLOGÍA INALÁMBRICA?

El término "inalámbrico" hace referencia a la tecnología sin cables que permite conectar varias máquinas entre sí. Las conexiones inalámbricas que se establecen entre los empleados remotos y una red confieren a las empresas flexibilidad y prestaciones muy avanzadas.

Se mide en Mbps. Un Mbps es un millón de bits por segundo, o la octava parte de un MegaByte por segundo - MBps. (Recordemos que un byte son 8 bits.)

Existen principalmente dos tecnologías inalámbricas certificadas. Una es la tecnología 802.11b y la otra 802.11g (ésta última tecnología es más reciente -ha sido aprobada a finales de 2003- y más rápida).

EN QUE SE BASA LA TECNOLOGÍA INALÁMBRICA

Actualmente el término se refiere a comunicación sin cables, usando frecuencias de radio u ondas infrarrojas. Entre los usos más comunes se incluyen a IrDA (Infrared Data Association, estándar físico en la forma de transmisión y recepción de datos por rayos) y las redes inalámbricas de computadoras.

Ondas de radio de bajo poder, como los que se emplea para transmitir información entre dispositivos, normalmente no tienen regulación, en cambio transmisiones de alto poder requieren normalmente un permiso del estado para poder transmitir en una frecuencia específica. Las plataformas inalámbricas en la historia han transmitido voz y han crecido y hoy por hoy son una gran industria, llevando miles de transmisiones alrededor del mundo.

DIFERENCIAS ENTRE TECNOLOGÍA MÓVIL E INALÁMBRICA

La tecnología móvil hace referencia a la posibilidad de trasladar el trabajo de un sitio a otro, es decir, de llevar a cabo unas tareas determinadas fuera del campo de trabajo; en cambio, la tecnología inalámbrica hace referencia a la posibilidad de conectar varios dispositivos entre sí o a una red sin necesidad de cables, se puede emplear estas conexiones inalámbricas para transferir la información entre un sistema de empresa, donde un grupo de personas necesitan estar comunicados entre sí.

2.2.11 CLASES DE TECNOLOGÍA MÁS UTILIZADAS.

BLUETOOTH

Bluetooth es una frecuencia de radio de disponibilidad universal que conecta entre sí los dispositivos habilitados para Bluetooth situados a una distancia de hasta 10 metros. Permite conectar un ordenador portátil o un dispositivo de bolsillo con otros ordenadores portátiles, teléfonos móviles, cámaras, impresoras, teclados, altavoces e incluso un ratón de ordenador.

VENTAJAS

Permite conectar de forma rápida y sencilla los dispositivos habilitados para Bluetooth entre sí y de este modo crear una red de área personal (PAN) en la que es posible combinar todas las herramientas de trabajo principales con todas las prestaciones de la oficina. El uso de una red de igual a igual Bluetooth permite intercambiar archivos en reuniones improvisadas con suma facilidad y ahorrar tiempo imprimiendo documentos sin necesidad de conectarse a una red fija o inalámbrica. Con Bluetooth, se puede hacer actividades de inmediato como imprimir un informe desde el escritorio mediante cualquier impresora habilitada para Bluetooth dentro del radio, sin cables, sin problemas y sin moverse siquiera.

WI-FI

Wi-Fi o red de área local inalámbrica (WLAN) es una red de TI de tamaño medio que utiliza la frecuencia de radio 802.11a, 802.11b o 802.11g en lugar de cables y permite realizar diversas conexiones inalámbricas a Internet. Si sabe dónde se encuentra una red Wi-Fi o WLAN, puede navegar por Internet, utilizar el correo electrónico y acceder a la red privada de una empresa. Esta es una buena opción para un empleado móvil que pasa fuera de su compañía.

VENTAJAS

Donde haya una red Wi-Fi, existe un portal de información y comunicación. La incorporación de una red WLAN a la oficina proporciona una mayor libertad y favorece la versatilidad del entorno de trabajo tradicional. Ahora bien, estas posibilidades no se limitan a la oficina, y cada vez aparecen más redes WLAN en lugares como cybers, restaurantes, hoteles y aeropuertos, lo que permite a los usuarios acceder a la información que necesitan. Acceda a la red de la empresa y obtenga las respuestas que necesite, en el momento preciso. Wi-Fi pone a su disposición un acceso a Internet sin igual.

WI-MAX

“Específicamente, la tecnología 802.16, a menudo denominada WiMAX, complementa la WLAN conectando hotspots con tecnología 802.11 a Internet y

ofrece una alternativa inalámbrica para la conectividad de banda ancha de última generación a empresas y hogares.”

Esta es una red muy costosa que aplica Microsoft verdaderamente podremos tener una banda ancha y no solo un ancho de banda, donde la velocidad de transmisión será mayor.

¿CUÁL ES LA DIFERENCIA ENTRE UNA RED WI-FI Y WI-MAX?

Una red Wi-Fi, red ad hoc puede ser establecida por cualquiera para conectar la casa con la oficina, mientras que Wimax está diseñado para cubrir una ciudad entera a través de estaciones base dispersas alrededor del área metropolitana.

TECNOLOGÍA GPRS

GPRS es la sigla de General Packet Radio Services (servicios generales de paquetes por radio). A menudo se describe como "2,5 G", es decir, una tecnología entre la segunda (2G) y la tercera (3G) generación de tecnología móvil digital. Se transmite a través de redes de telefonía móvil y envía datos a una velocidad de hasta 114 Kbps. El usuario puede utilizar el teléfono móvil y el ordenador de bolsillo para navegar por Internet, enviar y recibir correo, y descargar datos y soportes. Permite realizar videoconferencias con sus colegas y utilizar mensajes instantáneos para charlar con sus familiares y amigos, esté

donde esté. Además, puede emplearse como conexión para el ordenador portátil u otros dispositivos móviles.

TECNOLOGÍA 3G

Al igual que GPRS, la tecnología 3G (tecnología inalámbrica de tercera generación) es un servicio de comunicaciones inalámbricas que le permite estar conectado permanentemente a Internet a través del teléfono móvil, el ordenador de bolsillo, el Tablet PC o el ordenador portátil. La tecnología 3G promete una mejor calidad y fiabilidad, una mayor velocidad de transmisión de datos y un ancho de banda superior (que incluye la posibilidad de ejecutar aplicaciones multimedia). Con velocidades de datos de hasta 384 Kbps, es casi siete veces más rápida que una conexión telefónica estándar.

VENTAJAS

Se dice que los usuarios de GPRS y 3G están "siempre conectados", dado que con estos métodos de conexión tienen acceso permanente a Internet. Mediante los mensajes de texto cortos, los empleados de campo pueden comunicar su progreso y solicitar asistencia. Los ejecutivos que se encuentran de viaje pueden acceder al correo electrónico de la empresa, de igual modo que puede hacerlo un empleado de ventas, que también puede consultar el inventario. Puede automatizar su casa o su oficina con dispositivos GPRS y 3G supervisar sus inversiones.

2.2.12 PROTOCOLOS DE RED INALAMBRICA.

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI capas físicas y de enlace de datos, especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar.

El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como “802.11 legacy.” La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizó una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g.

ESTÁNDAR 802.11 legacy

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

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

ESTÁNDAR 802.11a

La revisión 802.11a fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz 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 sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con 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 (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), 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 a 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 son más fácilmente absorbidas.

ESTÁNDAR 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con

este estándar es de aproximadamente 5,9 Mbits sobre TCP y 7,1 Mbit/s sobre UDP.

ESTÁNDAR 802.11c

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

ESTÁNDAR 802.11d

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

ESTÁNDAR 802.11e

IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad

añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, ésta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad con ellos. Estas prestaciones resultan fundamentales para las redes domésticas y para que los operadores y proveedores de servicios conformen ofertas avanzadas.

ESTÁNDAR 802.11f

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

ESTÁNDAR 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Que es la evolución del estándar 802.11b, Este utiliza la banda de 2,4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a

la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

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

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

ESTÁNDAR 802.11h

Se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones estimó convenientes para minimizar el

impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM.

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

Selección Dinámica de Frecuencias y Control de Potencia del Transmisor

DFS (DynamicFrequencySelection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (Transmitter Power Control) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

ESTÁNDAR 802.11i

Está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP

(Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

ESTÁNDAR 802.11j

Es equivalente al 802.11h, en la regulación Japonesa

ESTÁNDAR 802.11k

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

ESTÁNDAR 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. Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

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

ESTÁNDAR 802.11p

Este estándar opera en el espectro de frecuencias de 5,9 GHz y de 6,2 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

2.2.13 VELOCIDADES DE RED.

LA VELOCIDAD DE LAS REDES INALÁMBRICAS

La velocidad máxima de transmisión inalámbrica de la tecnología 802.11b es de 11 Mbps. Pero la velocidad típica es solo la mitad: entre 1,5 y 5 Mbps dependiendo de si se transmiten muchos archivos pequeños o unos pocos archivos grandes. La velocidad máxima de la tecnología 802.11g es de 54 Mbps. Pero la velocidad típica de esta última tecnología es solo unas 3 veces más rápida que la de 802.11b: entre 5 y 15 Mbps.

Resumiendo, las velocidades típicas de los diferentes tipos de red son:

Con Cables:

Ethernet 10: transmitía a un máximo de 10 Mbps.

Ethernet 10/100: (sucesora de ethernet 10) que transmite un máximo de 100 Mbps y tiene una velocidad típica de entre 20 y 50 Mbps. Compatible Con Ethernet 10.

Ethernet 10/100/1000: Es la más usada ahora en tecnología con cables y 10 veces más rápida que la anterior. Como se ha empezado a instalar a la par que las redes inalámbricas tiene que luchar con la versatilidad y facilidad de implantación de éstas. Compatible con las dos anteriores.

Sin Cables:

802.11b: aproximadamente entre 1.5 y 5 Mbps

802.11g: aproximadamente entre 5 y 15 Mbps. Compatible con la anterior.

802.11n: próximo estándar. Compatible con las anteriores.

2.2.14 SEGURIDAD DE REDES INALAMBRICAS

Introducción a WEP, WPA y WPA2

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas

precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.

WEP

Características y funcionamiento WEP (Wired Equivalen Privacy, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autenticación y control de acceso en redes WLAN.

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

El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización, en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes. Se concatena la clave secreta a continuación del IV formando el seed.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la

clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

Otras debilidades de WEP

WEP también adolece de otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (Integrity Check Value) un algoritmo diseñado para tal fin como SHA1-HMAC

El estándar IEEE 802.11 incluye un mecanismo de autenticación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autenticación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de autenticación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como si no, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas más arriba [8].

WEP no incluye autenticación de usuarios. Lo más que incluye es la autenticación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autenticación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso tendríamos una autenticación de sistema abierto, es decir, sin autenticación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (replay). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica.

Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autenticación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autenticación (RADIUS normalmente) funcionando en

la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperabilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA [5] y WPA2 (IEEE 802.11i) [3]. El primero es de 2003 y el segundo se espera para 2004. Se estudian a continuación.

WPA

WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para remplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de

seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente maduro y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autenticación.

WPA incluye las siguientes tecnologías:

IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique.

Con este fin se utiliza el protocolo EAP y un servidor AAA (AuthenticationAuthorizationAccounting) como puede ser RADIUS (RemoteAuthentication Dial-In UserService). Si la autorización es positiva, entonces el punto de acceso abre el puerto

Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2^{48} combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autenticación, se sustituye el mecanismo de autenticación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la

red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

Modos de funcionamiento de wpa

WPA puede funcionar en dos modos:

Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad.

Con clave inicial compartida. Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autenticación, pero no para el cifrado de los datos.

WPA2

WPA2 (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas Wi-Fi; creado para corregir las vulnerabilidades detectadas en WPA

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las

características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). "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 que la tecnología cumple con estándares de inter operatividad" 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 802.11i.

Conclusiones

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

El sistema WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, tiene distintas debilidades que lo hacen no seguro, por lo que deben buscarse alternativas.

Tanto la especificación WPA como IEEE 802.11i solucionan todos los fallos conocidos de WEP y, en estos momentos, se consideran soluciones fiables.

La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente en los dispositivos para los próximos meses.

La apuesta de seguridad del IEEE para sustituir al desafortunado WEP, 802.11i, todavía está pendiente de ser estudiada en profundidad por investigadores debido a que sus especificaciones no son públicas.

2.2.15 COMPONENTES DE UNA RED INALÁMBRICA

PUNTO DE ACCESO INALÁMBRICO

Un punto de acceso inalámbrico figura 2.5 (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente 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. Muchos 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- se convierten en una red ad-hoc. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. 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. Este o su antena normalmente se colocan en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

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.

Los puntos de acceso, también llamados APs o wireless access point, son equipos hardware configurados en redes Wifi y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El *access point* o punto de

acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.

Los puntos de acceso utilizados en casa o en oficinas, son generalmente de tamaño pequeño, componiéndose de un adaptador de red, una antena y un transmisor de radio.



Figura 2.5 punto de acceso.

Existen redes Wireless pequeñas que pueden funcionar sin puntos de acceso, llamadas redes “*ad-hoc*” o modo *peer-to-peer*, las cuales solo utilizan las tarjetas de red para comunicarse. Las redes más usuales que veremos son en modo estructurado, es decir, los puntos de acceso harán de intermediario o puente entre los equipos wifi y una red Ethernet cableada. También harán la función de escalar a mas usuarios según se necesite y podrá dotar de algunos elementos de seguridad.

Los puntos de acceso normalmente van conectados físicamente por medio de un cable de pares a otro elemento de red, en caso de una oficina o

directamente a la línea telefónica si es una conexión doméstica. En este último caso, el AP estará haciendo también el papel de Router. Son los llamados Wireless Routers los cuales soportan los estándares 802.11a, 802.11b y 802.11g.

Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a él se llama “celda”. Usualmente se hace un estudio para que dichas celdas estén lo mas cerca posible, incluso solapándose un poco. De este modo, un usuario con un portátil, podría moverse de un AP a otro sin perder su conexión de red.

Los puntos de acceso antiguos, solían soportar solo a 15 a 20 usuarios. Hoy en día los modernos APs pueden tener hasta 255 usuarios con sus respectivos ordenadores conectándose a ellos.

Si conectamos muchos Access Point juntos, podemos llegar a crear una enorme red con miles de usuarios conectados, sin apenas cableado y moviéndose libremente de un lugar a otro con total comodidad.

A nivel casero y como se ha dicho, los puntos de acceso inalámbricos nos permitirán conectar varias conexiones Ethernet o Fast Ethernet, y a su vez conectar varios clientes sin cable. Sin embargo debemos ser cautos. Cualquier persona con una tarjeta de red inalámbrica y un portátil puede conectarse a nuestra red Wifi y aprovecharse gratuitamente de nuestro ancho de banda. Para evitar esto, el AP puede hacer filtrados por MAC o dirección física no

permitiendo la conexión de clientes desconocidos. Muchos de estos dispositivos llevan ya instalado su propio Firewall con el que proteger la red. Para que la integridad de nuestros datos no se vea vulnerada, tenemos la opción de utilizar métodos de encriptación como WEP o la más moderna WPA.

EL SWITCH

Los switches figura 2.6 son otra pieza fundamental de muchas redes porque hacen que la transferencia de datos vaya mucho más deprisa. Un switch permite a diferentes nodos (un punto de conexión de la red, normalmente un ordenador o servidor), comunicar directamente con otro elemento en la red de una manera eficiente, rápida y transparente para los usuarios. Hay muchos tipos de switches y redes. Los switches que proveen una conexión separada para cada nodo en una red interna de una empresa, se llaman switches *LAN*. En este curso, nos centraremos en las típicas redes ethernet que usan este tipo de switches. Sabremos que es lo que hace, y como utiliza las vlans, los troncales (trunks) y el protocolo de STP (*SpanningTreeProtocol*).

Figura 2.6 switch



Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

EL ROUTER

Router figura 2.7 que literalmente quiere decir “encaminador”, en el mundo de las computadoras es un dispositivo que selecciona caminos (o "rutas") en redes informáticas para enviar por ellos información. En términos técnicos se traspasan "paquetes" de información desde su fuente hacia un destino a través de "nodos" intermediarios, que en este caso corresponde al router como aparato físico en cuestión.



figura 2.7router.

En términos sencillos, el router que vemos en casas y oficinas cumple la función de crear redes inalámbricas, lo que en términos prácticos se utiliza normalmente para conectarnos a la Internet sin la necesidad de conectar un cable físicamente a nuestras computadoras.

- El router se asegura de que la información no va a donde no es necesario
- El router se asegura que la información si llegue al destinatario

El router se encargará de analizar paquete por paquete el origen y el destino y buscará el camino más corto de uno a otro. Esta forma de transmitir información tiene grandes ventajas:

- El router es capaz de ver si una ruta no funciona y buscar una alternativa.
- El router es capaz incluso de buscar la ruta más rápida (por ejemplo la que tenga menos tráfico) en caso de poder escoger entre varias posibilidades.

TIPOS DE ROUTERS

Los routers pueden proporcionar conectividad dentro de las empresas, entre las empresas e Internet, y en el interior de proveedores de servicios de Internet (ISP). Los routers más grandes interconectan ISPs, se suelen llamar metro router, o pueden ser utilizados en grandes redes de empresas.

CONECTIVIDAD SMALL OFFICE, HOME OFFICE (SOHO)

Los routers se utilizan con frecuencia en los hogares para conectar a un servicio de banda ancha, tales como IP sobre cable o ADSL. Un router usado en una casa puede permitir la conectividad a una empresa a través de una red privada virtual segura.

Si bien funcionalmente similares a los routers, los routers residenciales usan traducción de dirección de red en lugar de enrutamiento. En lugar de conectar ordenadores locales a la red directamente, un router residencial debe hacer que los ordenadores locales parezcan ser un solo equipo.

ROUTER DE EMPRESA

En las empresas se pueden encontrar routers de todos los tamaños. Si bien los más poderosos tienden a ser encontrados en ISPs, instalaciones académicas y de investigación, pero también en grandes empresas.

El modelo de tres capas es de uso común, no todos de ellos necesitan estar presentes en otras redes más pequeñas.

ROUTER DE ACCESOS

Los routers de acceso, incluyendo SOHO, se encuentran en sitios de clientes como sucursales que no necesitan de enrutamiento jerárquico de los propios. Normalmente, son optimizados para un bajo costo.

ROUTER DE DISTRIBUCIÓN

Los routers de distribución agregan tráfico desde routers de acceso múltiple, ya sea en el mismo lugar, o de la obtención de los flujos de datos procedentes de múltiples sitios a la ubicación de una importante empresa. Los routers de distribución son a menudo responsables de la aplicación de la calidad del servicio a través de una WAN, por lo que deben tener una memoria considerable, múltiples interfaces WAN, y transformación sustancial de inteligencia.

También pueden proporcionar conectividad a los grupos de servidores o redes externas. En la última solicitud, el sistema de funcionamiento del router debe ser cuidadoso como parte de la seguridad de la arquitectura global. Separado del router puede estar un cortafuegos o VPN concentrador, o el router puede incluir estas y otras funciones de seguridad. Cuando una empresa se basa

principalmente en un campus, podría no haber una clara distribución de nivel, que no sea tal vez el acceso fuera del campus.

En tales casos, los routers de acceso, conectados a una red de área local (LAN), se interconectan a través del Corerouters.

ROUTER DE NÚCLEO

En las empresas, el corerouter puede proporcionar una "columna vertebral" interconectando la distribución de los niveles de los routers de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto.

Cuando una empresa está ampliamente distribuida sin ubicación central, la función del corerouter puede ser asumido por el servicio de WAN al que se suscribe la empresa, y la distribución de routers se convierte en el nivel más alto.

ROUTER DE BORDE

Los routers de borde enlazan sistemas autónomos con las redes troncales de Internet u otros sistemas autónomos, tienen que estar preparados para manejar el protocolo BGP y si quieren recibir las rutas BGP, deben poseer una gran cantidad de memoria.

ROUTERS INALÁMBRICOS

A pesar de que tradicionalmente los routers solían tratar con redes fijas (Ethernet, ADSL, RDSI...), en los últimos tiempos han comenzado a aparecer routers que permiten realizar una interfaz entre redes fijas y móviles (Wi-Fi, GPRS, Edge, UMTS, Fritz!Box, WiMAX...) Un router inalámbrico comparte el mismo principio que un router tradicional. La diferencia es que éste permite la conexión de dispositivos inalámbricos a las redes a las que el router está conectado mediante conexiones por cable. La diferencia existente entre este tipo de routers viene dada por la potencia que alcanzan, las frecuencias y los protocolos en los que trabajan. En Wi-Fi estas distintas diferencias se dan en las denominaciones como clase a/b/g/ y n.

CABLE ETHERNET

Un cable Ethernet figura 2.8 es un tipo de cable usado normalmente para conectar dispositivos informáticos y red, como pueden ser ordenadores, Routers, Switches, etc. Puede utilizarse entre ordenadores o para conectar estos a otros equipos, con la finalidad de crear una red de datos. Se puede decir que el cable Ethernet más común y popular es el cable cruzado. Un cable Ethernet corriente, tipo UTP¹¹ de categoría 5, dispone de 4 pares de hilos y suele venir con una malla metálica que protege los datos contra interferencias.

¹¹*Cable de red*

Normalmente la categoría 5 es para velocidades de 10/100 Mb, y categoría 5e o 6 para 1000 Mb (gigabyte). Este tipo de cables puede venir en dos clases, aunque hay dos categorías básicas, sólidos y trenzados.

Dentro del cable hay 8 cables coloreados y trenzados de unos colores determinados. Están trenzados por parejas, y cada una de las parejas tiene un color común. Cada uno de los colores tiene una pareja de color blanco. Estos cuatro pares de cables acaban en un conector especial llamado RJ45 que tiene la misma forma que un conector de teléfono normal, y de hecho son de la misma clase siendo los de teléfono del tipo RJ11.

La forma de hacer el conector viene en dos formas: un cable cruzado y un cable plano, donde la diferencia es simplemente como hagamos coincidir los hilos en cada punta. Un cable plano normalmente se utiliza para conectarse a un hub o a un switch, y un cable cruzado se utiliza para conectar dos dispositivos del mismo tipo. Algunos equipos de red pueden cruzar y descruzar un cable según se necesite.

Figura 2.8 cable UTP.



Antena WIFI

En varias ocasiones he tenido que personalizar la antena figura 2.9 del router que da acceso a internet o a la intranet, para ampliar la distancia de cobertura. Existen 3 tipos de antenas según como se quiera amplificar esa distancia:



Figura 2.9 Antena Wifi

ANTENAS DIRECCIONALES: Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance, actúa de forma parecida a un foco de luz que emite un haz concreto y estrecho pero de forma intensa (más alcance). El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

ANTENA OMNIDIRECCIONALES: Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un

foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones con menor alcance. Las antenas Omnidireccionales “envían” la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

ANTENAS SECTORIALES: Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. Para tener una cobertura de 360° (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120° ó 4 antenas sectoriales de 80°. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

CAPITULO III

PROPUESTA DE LA SOLUCIÓN

3.1 PROPUESTA DE SOLUCIÓN.

El siguiente trabajo se desarrollara dentro de la Universidad Tecnológica de El Salvador la propuesta de solución es para el mejoramiento de conectividad de la red del edificio Benito Juárez, y así contribuir al mejorar la cobertura de la red inalámbrica beneficiando a estudiantes cuerpo docente y usuarios en general esto es porque actualmente la red inalámbrica del edificio en cuestión no posee una cobertura adecuada porque solo hay conexión o cobertura en el primer piso en lugares específicos.

Por lo mismo se estudia la forma de mejorar la conectividad y se proponen nuevos dispositivos de red inalámbrica con una distribución especifica en todos los pisos del edificio en cuestión incluyendo el sótano y sus alrededores cercanos la propuesta del nuevo diseño de red inalámbrica se hace con el objetivo y la necesidad de una mayor conectividad y cobertura por eso mismo que se presenta la opción de suplantar los dispositivos actuales y en mas cantidad distribuidos cuidadosamente en toda la estructura con tecnología WIFI y compatibles con estándares 802.11.

Al tener todo esto en claro se procederá a crear una topología de red donde se explique claramente la distribución y las tecnologías a proponer al mismo

tiempo que una maqueta a escala del edificio Benito Juárez para mayor compresión de la propuesta.

3.1.1 PLANTEAMIENTO DEL PROYECTO TEMÁTICO.

Primera Fase: investigación del estado de la red inalámbrica del edificio Benito Juárez de la Universidad Tecnológica de El Salvador.

En esta fase se determina que la cobertura de la red es muy escasa en su mayoría que solamente están habilitados dos puntos de acceso dentro de la biblioteca del primer piso y una barra point, Actualmente en el edificio Benito Juárez de la Universidad Tecnológica de El Salvador, están implementado en su red inalámbrica los puntos de acceso de la marca 3COM el modelo 7160 con soporte POE¹² figura 3.1.



Figura 3.1 punto de acceso 3COM el modelo 7160

¹² *alimentación a través de Ethernet*

Los dispositivos están distribuidos de la siguiente forma: en el primer piso esta la biblioteca hay un punto de acceso cerca de la puerta en el segundo piso existe una barra point instalada que esta fuera de uso también en el segundo piso del edificio hay un punto de acceso cerca de las gradas de acceso principal, en el tercer piso no existe punto de acceso, en el cuarto piso existe un punto de acceso justo en medio del pasillo, en el quinto piso hay punto de acceso. Cuadro 3.1

Distribución actual de los puntos de acceso inalámbricos	
Sótano	0 punto de acceso
Primer piso	2 punto de acceso
Segundo piso	1 punto de acceso 1 barra point en la parte externa del edificio Benito Juárez
Tercer piso	0 punto de acceso
Cuarto piso	1 punto de acceso
Quinto piso	1 punto de acceso

Cuadro 3.1 Distribución actual de los puntos de acceso inalámbricos

Con esta información se llega a la conclusión inmediata que la red necesita una reforma en su distribución y la sustitución de los dispositivos de red para mejorar su cobertura y ser de más eficiencia a los usuarios finales.

Segunda fase: Investigación del equipo adecuado para la red inalámbrica del edificio Benito Juárez de la Universidad Tecnológica de El Salvador.

En esta fase se investigó cual equipo le convenía a la estructura para logra el objetivo de dar cobertura a todo el campo y sus alrededores cercanos, que cumplan con los requisitos que exige dicha red que beneficie a los usuarios finales y se empezaron a plantear las formas de la distribución de los puntos de acceso

Tercera fase: Diseño de la red

Esta es la parte más importante del proyecto ya que se distribuirán los dispositivos de red en el ámbito teórico basado en las especificaciones técnicas de cada dispositivo para lograr la cobertura deseada basándose en la investigación anterior del estado actual de la red y teniendo el equipo de red seleccionado.

Cuarta fase: Diseño de seguridad

La medida de seguridad lógica de la propuesta es la configuración de encriptación WPA2 y las características de control parental impiden a usuarios

ver el contenido inadecuado, soportada por el dispositivo WIFI seleccionado, esto es para seguridad de la red e impedir tráfico innecesario.

Quinta fase: Desarrollo de la maqueta.

Debido a que este proyecto es una propuesta de mejoramiento de la red inalámbrica del edificio Benito Juárez de la Universidad Tecnológica de El Salvador, su implementación no tendrá lugar en cambio se realiza una maqueta de todo el edificio del tipo descriptiva donde se desplegara cada piso del edificio con el objetivo de explicar con mayor facilidad la distribución de los puntos de acceso dentro de cada nivel y su rango de cobertura.

3.1.2 CRONOGRAMA DE ACTIVIDADES.

Se realizaron diferentes actividades en el desarrollo del proyecto a partir del mes de agosto hasta el mes de noviembre entre las cuales se destacan a continuación: Cuadro 3.2

# de actividad	Actividad	Duración	Calendario
1	Investigación de la red actual	1 día 4 horas	Sábado 13 de agosto
2	Investigación de los dispositivos de red a recomendar	7 días	Del 16 al 23 de agosto
3	Contacto con el personal de GBM	1 día 1 hora	05 de septiembre

4	Diseño de la red	24 días	06 de sep. Al 29 de septiembre
5	Diseño de la propuesta	20 días	1 de octubre al 20 de octubre
6	Elaboración de la maqueta	15 días	22 de octubre
7	Entrega de la propuesta	1 día una hora	21 de noviembre

Cuadro 3.2 cronograma de actividades.

3.1.3 TECNOLOGÍAS Y RECURSOS SELECCIONADOS.

En el presente trabajo y de acuerdo con la investigación, de campo realizada en el edificio Benito Juárez de la Universidad Tecnológica de El Salvador, se propone como solución del mejoramiento de la red inalámbrica y cobertura total en el edificio y sus alrededores cercanos la instalación del siguiente dispositivo Cisco aironet 1100 series Access point y una correcta distribución del dispositivo o puntos de acceso a la red dará como resultado una mejor cobertura de la señal de red en todo el edificio Benito Juárez de la Universidad Tecnológica de El Salvador. Beneficiando así a estudiantes, cuerpo docente y público en general.

Los dispositivos y las siguientes tecnologías se explican en el cuadro 3.3:

Tecnologías y dispositivos seleccionados	
Cable UTP	Cable UTP categoría 5e
9 Acces point	Cisco aironet 1100 series access point
1 switch	Switch Catalyst 2960G 24 puertos, Cisco
Estandares	802.11g ,compatible con 802.11b
Seguridad	128-bit WEP,WPA,WPA2,
Frecuencia	2.4 GHz
Protocolos	CSMA/CA , QoS, DHCP
Tecnologia de cableado	10/100/BASE-T

Cuadro 3.3 Tecnología y dispositivos seleccionados.

Cisco aironet 1100 series Access point, figura 3.2 es el dispositivo más utilizado en la propuesta y está compuesto por las siguientes tecnologías:



Figura 3.2 Cisco aironet 1100 series access point

Las principales características y ventajas del Cisco aironet 1100 series Access point son las siguientes cuadro 3.4

Principales características y ventajas	
Punto de Acceso de la Serie Cisco Aironet 1100	
Características	Ventajas
Radio a 2,4 GHz, configurable hasta los 100 mW	• La gran calidad del diseño del transmisor y del receptor proporciona una cobertura grande y fiable
Software Cisco IOS	• Proporciona soporte para soluciones de extremo a extremo para servicios de red inteligentes

	• Logra un comportamiento de la red predecible y consistente • Ofrece aplicaciones y servicios uniformes
Compatibilidad con LAN virtual (VLAN)	• Permite la segmentación de un máximo de 16 grupos de usuarios • Aumenta la flexibilidad del sistema, ya que se pueden alojar clientes con distintos requisitos de seguridad y capacidades
Calidad de servicio (QoS)	• Asigna prioridad al tráfico en función de los requisitos de las diferentes aplicaciones • Mejora la voz y el vídeo
IP móvil de proxy en el software Cisco IOS	• Proporciona una itinerancia transparente entre subredes • Mejora la movilidad de la voz a través de dispositivos inalámbricos 802.11
Capacidad de gestión	
Compatibilidad con el protocolo Cisco Discovery Protocol y con los estándares MIB I y MIB II de SNMP	• Interoperable con sistemas de administración de redes compatibles con SNMP, como HP OpenView y CA Unicenter • Gestionable a través de muchas aplicaciones de CiscoWorks en Resource Manager Essentials (Inventory Manager, Software Image Manager, Availability Manager),
Principales características y ventajas	
Punto de Acceso de la Serie Cisco Aironet 1100	
La CLI de Cisco admite Telnet, FTP y TFTP	• La interfaz no resulta extraña a la gran comunidad de administradores de redes • Permite la administración centralizada de

	puntos de acceso remoto • Facilita la estandarización de la configuración de la red
Seguridad	
WEP de 40 bits y 128 bits	• Admite métodos de seguridad basados en los estándares, con lo que se garantiza la interoperatividad.
Utiliza la suite Cisco Wireless Security Suite	• Proporciona las galardonadas características de seguridad de WLAN • Defiende contra ataques a la seguridad pasivos y activos • La autenticación basada en 802.1X y en el apoyo EAP de las listas de acceso de los usuarios • Permite utilizar servidores RADIUS para realizar el registro de las conexiones de los usuarios.
Capacidad de ampliación	• Las funciones de gestión y seguridad autónomas se amplían junto con la cambiante arquitectura • Requiere una inversión de capital mínima
Rango de opciones de gestión y seguridad	
Potencia de transmisión configurable	• Facilita la gestión del tamaño de las celdas • Es posible reducir la cobertura al mismo tiempo que los requisitos de densidad de la instalación con el fin de optimizar el aumento del ancho de banda
Disponibilidad	
Espera en funcionamiento	• Protección transparente en caso de error para dejar en espera el punto de acceso

Balanceo de cargas	• Distribuye las conexiones de los usuarios por los puntos de acceso disponibles • Optimiza la transferencia agregada
Escalado de velocidad automático	Mantiene la conectividad a larga distancia
Principales características y ventajas Punto de Acceso de la Serie Cisco Aironet 1100	
Protección de la inversión	
Compatibilidad con 802.11b	Admite una base instalada de clientes 802.11b • La madura tecnología incorpora las generaciones de mejoras
Diseño que permite actualizar la radio	• Proporciona una ruta de migración a las futuras tecnologías, como 802.11g y Advanced Encryption Standard (AES) asistido por hardware • Es posible apoyarse en el diseño de la instalación existente para actualizaciones progresivas
El tamaño del almacenamiento duplica el de la carga inicial del firmware	• Proporciona más capacidad para las versiones de características de seguimiento
Ranura de seguridad antirrobo y cierre de seguridad	• Admite cables de seguridad o candados estándar (no se incluyen) • Los candados pueden tener una sola llave o llaves maestras, lo que simplifica la gestión del inventario
Instalación simplificada	
Orientación de montaje flexible	• Admite la instalación en varias ubicaciones, entre las que se incluyen paredes, techos,

	mesas y despachos
Antenas dipolares con diversidad integradas	• Perfil compacto de antena • El patrón de cobertura esférico está optimizado para poder utilizar cualquier orientación • Las antenas con diversidad aumentan la fiabilidad en entornos con varias rutas, como las oficinas
Selección automática de canales	• Determina cuál es el canal menos congestionado y lo selecciona
Admite alimentación en línea a través de Ethernet (figuras 6, 7 y 8)	• Elimina la necesidad de tener alimentación CA local • Reduce el número de cables • Posibilita que se instale en lugares remotos
Servidor HTTP con GUI rediseñada y basada en navegador Web	• Diseño orientado a gráficos y por el que es posible desplazarse, el más habitual en los productos Cisco • La configuración express consolida las tareas principales de configuración en una sola vista
Dynamic Host Configuration Protocol (DHCP)	• Obtiene automáticamente las direcciones IP del servidor DHCP

Cuadro 3.4

Características y ventajas del Cisco aironet 1100 series Access point

3.1.4 DISEÑO DE LA PROPUESTA.

Anteriormente se ha mencionado los dispositivos a utilizar en la propuesta en esta sección de documento se conocerá y analizará los planos de la distribución

física de los dispositivos de red de la propuesta de mejoramiento de red del edificio Benito Juárez de la Universidad Tecnológica de El Salvador. El diseño está basado en una estructura muy básica de cableado horizontal y vertical con la distribución de un Punto de Acceso de la Serie Cisco Aironet 1100 en cada piso como el Punto de Acceso de la Serie Cisco Aironet 1100 trabaja con el estándar 802.11g quiere decir que puede llegar las siguientes velocidades y coberturas cuadro 3.5:

Velocidad hipotética	Rango en ambiente cerrado	Rango en ambiente abierto
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

Cuadro 3.5 velocidades y coberturas.

Cisco Catalyst 2960 24 10/100/1000figura 3.3, 4 T/SFP LAN Base Image/WS-C2960G-24TC-L Detalle de Producto ElSwitch Cisco Catalyst 2960 (WS-C2960G-24TC-L) es una completísima línea de switches de alto rendimiento diseñados para ayudar a los usuarios a que pasen de forma sencilla de las redes LAN compartidas tradicionales a redes completamente conmutadas.



Figura 3.3 Cisco Catalyst 2960 24 puertos.

Los switches Catalyst de Cisco ofrecen un amplio espectro para aplicaciones de usuarios, desde switches para pequeños grupos de trabajo hasta switches multicapa para aplicaciones empresariales escalables en el centro de datos o en el backbone.

Los switches Catalyst ofrecen rendimiento, administración y escalabilidad, se puede encontrar equipos Ethernet, Fast Ethernet y con opciones modulares las cuales permiten adaptarlos a las necesidades del negocio.

Características

Cisco Catalyst 2960G-24TC - conmutador - 20 puertos

Tipo de dispositivo Conmutador

Factor de forma Externo - 1U

Dimensiones (Ancho x Profundidad x Altura) 44.5 cm x 32.8 cm x 4.4 cm

Peso 4.5 kg

Memoria RAM 64 MB

Memoria Flash 32 MB

Cantidad de puertos 20 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T

Velocidad de transferencia de datos 1 Gbps

Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet

Puertos auxiliares de red 4x10/100/1000Base-T/SFP (mini-GBIC)(señal ascendente)

Protocolo de gestión remota SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c

Modo comunicación Semidúplex, dúplex pleno

Auto-sensor por dispositivo, soporte de DHCP, negociación automática, soporte VLAN, snooping IGMP

Alimentación CA 120/230 V (50/60 Hz)

Apoyados en la tabla anterior y las pruebas de campo en cada piso del edificio la distribución para lograr una mayor cobertura del ancho de banda la veremos desplegada por cada piso a continuación figura 3.4:

3.1.5 DISEÑO DE LA RED.

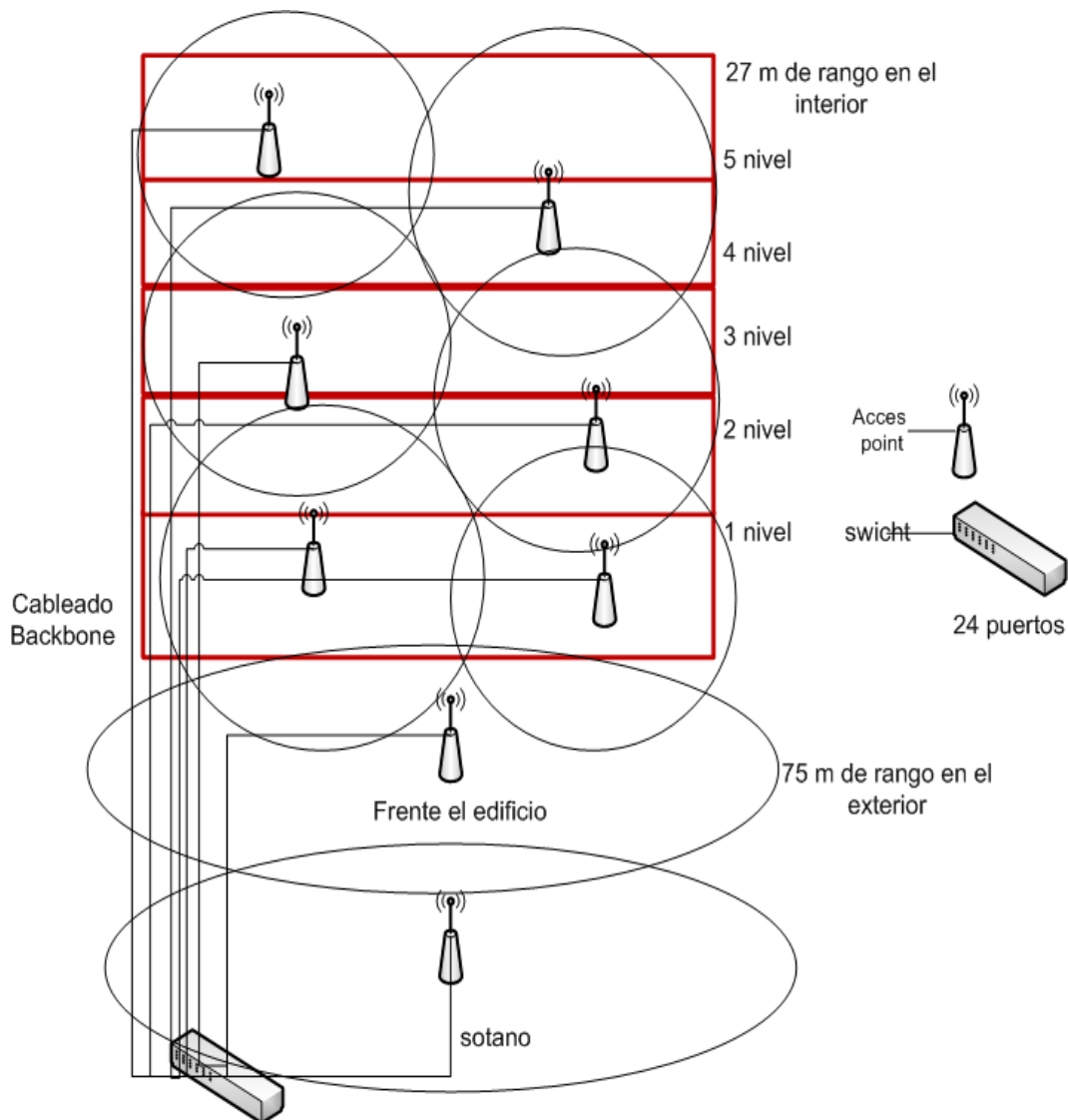


Figura 3.4 diseño de red

3.1.6 TOPOLOGÍA DE LA RED.

En la propuesta del diseño de red se utilizara la topología estrella figura 3.5 que es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste. Los dispositivos no están directamente conectados entre sí

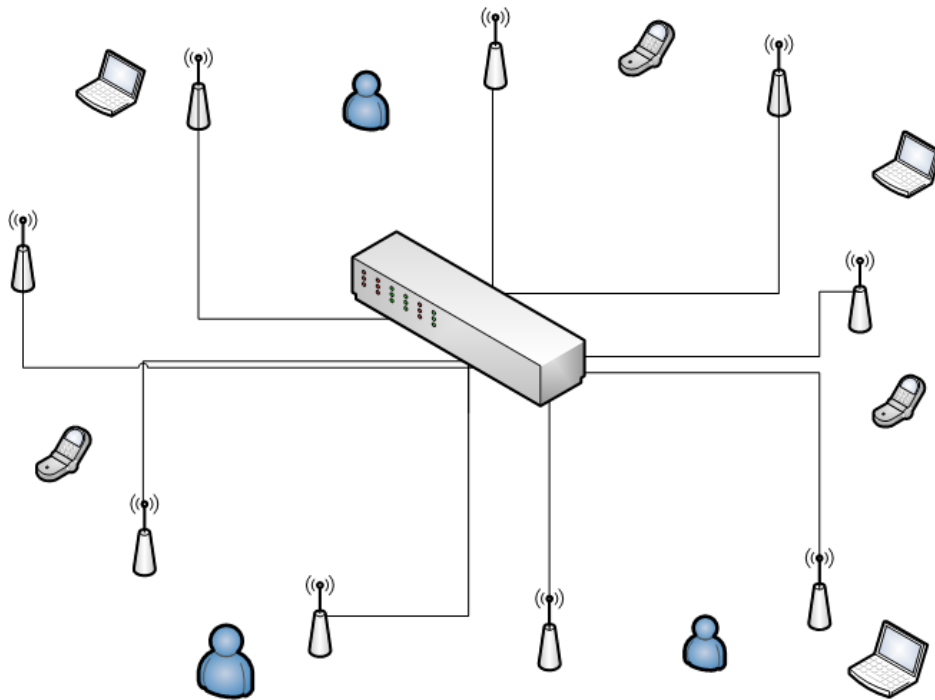


Figura 3.5 topología de la red.

3.1.7 IMPLEMENTACIÓN DE LA PROPUESTA.

Considerando la localización de los AP, se ha tomado en cuenta, los lugares posibles para la mejor recepción de la señal, basándose en Normativa 802.11 wireless En total son tres puntos de acceso los que se proponen para el primer piso todos con la frecuencia de 54 Mbit/s que tendrán un rango de cobertura en ambiente cerrado de 27 metros y en aire libre de 75 metros. En los pisos del dos a cinco habrá un acces point de la Serie Cisco Aironet 1100 por nivel en el segundo al final del pasillo en el tercero al inicio del pasillo en el cuarto al final y en quinto al inicio como lo muestra el diseño de red anterior, Figura 3.4 diseño de red, esta distribución intercalada promete la cobertura en todos sus niveles frecuencia de 54 Mbit/s para un mayor ancho de banda con un alcance de 27 metros lo que es suficiente en cada pasillo y sus aulas. La red tendrá una topología estrella, es una red en la cual las estaciones están conectadas directamente a un punto central que es un switch en el sótano de donde saldrán el cableado backbone hacia los puntos de red en cada piso.

3.1.8 PRESENTACIÓN DE LA PROPUESTA.

3.1.8.1 OFERTA TÉCNICA

Universidad Tecnológica de El Salvador,

Debido al presente problema de conexión inalámbrica la red interna e internet presente actualmente en el edificio Benito Juárez de la Universidad Tecnológica de El Salvador, se presenta la siguiente propuesta técnica de mejoramiento de la red inalámbrica del edificio en cuestión.

La propuesta consiste en: la sustitución de los acces point actuales marca 3COM modelo 7160 por el Cisco Aironet 1100 en total serán nueve distribuidos según su capacidad y estándares dentro del edificio con el objetivo de dar cobertura a todo el campo y sus alrededores, con una topología tipo estrella con un cableado estructurado backbone donde el punto central será el Cisco Catalyst 2960 24 puertos ubicado en el sótano.

La distribución de los puntos de acceso en los niveles será intercalada como lo explica el diseño de red para dar cobertura en cada nivel basado en el estándar 802.11 g que es con el que trabaja el Cisco Aironet 1100 en el primer nivel habrán tres puntos de acceso y en la parte trasera del edificio donde existe una zona de estudio habrá un punto de acceso el cual dará cobertura a 75 m de rango.

Atentamente:

David Alexander Arriaga Herrera.

Carlos José Reyes Juárez

Geovanny Alexander Romero Mejía.

3.1.8.2 OFERTA ECONÓMICA

Universidad Tecnológica de El Salvador,

Debido al presente problema de conexión inalámbrica la red interna e internet presente actualmente en el edificio Benito Juárez de la Universidad Tecnológica de El Salvador, se presenta la siguiente propuesta técnica de mejoramiento de la red inalámbrica del edificio en cuestión. Se proponen los siguientes dispositivos e instalaciones:

Costo de los dispositivos y mano de obra.	Cantidad	TOTAL
9 accespointCiscoAironet 1100 \$ 280.00 cada uno.	9 acces point	\$2,520.00
1 Cisco Catalyst 2960 24 puertos \$490.00	1 switch	\$490.00
260 metros de cable utp cat. 5e \$80.00 los 100 metros	3 bobinas	\$240.00

18 conectores macho RJ-45	\$0.20 cada uno	18 conectores	\$3.60
Costo por instalación de cada punto de red	\$150.00	9 puntos de red	\$1,350.00
<u>SUB TOTAL:</u>			<u>\$4,960.00</u>
<u>IMPREVISTOS:</u>			<u>\$500.00</u>
<u>TOTAL</u>			<u>\$5,460.00</u>

Atentamente:

David Alexander Arriaga Herrera.

Carlo José Reyes Juárez

Geovanny Alexander Romero Mejía.

3.1.9 EVIDENCIAS DEL PROYECTO.



Figura 3.6 Ubicación de las Barras point



Figura 3.7 altura entrada nivel promedio 3 mts.



Figura 3.8 ausencia de puntos de acceso.

CONCLUSIONES.

Para que la red del edificio Benito Juárez de la Universidad Tecnológica de El Salvador. Tenga una mejor cobertura que la actual habría que sustituir los dispositivos de red inalámbrica actuales por unos de mayor rango de cobertura y distribuirlos de una mejor forma basados en los estándares y normas que los rigen con esto logramos una amplia cobertura en el edificio y sus alrededores cercanos logrando así el objetivo principal de la investigación y propuesta. También debemos mencionar la cantidad mas elevada que la actual de los dispositivos colocando así uno por nivel del edificio en cuestión.

Basados en la oferta técnica el dispositivo cumple con los requisitos de los objetivos tanto general como los específicos para lograr la propuesta y la oferta económica resulto un total de \$4,960.00 mas los imprevistos con un rango de \$500.00 hace un total general de \$5,460.00 los imprevistos tanto como para un inconveniente electrónico o humano.

La red o topología de red es la de estrella por cuestiones del cableado estructurado de la propuesta y tratando de economizar aún más los gastos para la Universidad Tecnológica de El Salvador ya que esta topología utilizara menos cable de red.

RECOMENDACIONES.

- Una recomendación importante que acompaña la propuesta del mejoramiento de red es la de una instalación de toma corrientes hembra para exteriores en los alrededores del edificio especialmente en la parte trasera donde hay unas mesas que funciona como área de estudio, ya que se ve la necesidad que los alumnos conecten sus computadoras portátiles para obtener carga en sus baterías.
- Se recomienda también en un futuro cercano y con el objetivo de mayor seguridad en la red interna de la universidad, crear políticas de autenticación por medio de la MAC de cada dispositivo de red que se estará conectando continuamente a la red inalámbrica del edificio Benito Juárez de la Universidad Tecnológica de El Salvador.

BIBLIOGRAFIA

ALEGSA (2011) Diccionario de informática. Recuperado de

<http://alegsa.com.ar/dic/red%20inalambrica.php>

Creative Commons (2007) Topologías de red. Recuperada de

<http://www.eveliux.com/mx/topologias-de-red.php>

Jeff (2012) Redes Inalámbricas. Recuperado de

<http://es.kioskea.net/contents/wireless/wlintro.php3>

Wikipedia (2008) Router. Recuperado de <http://es.wikipedia.org/wiki/router>

Wikipedia (2010) Wi-fi. Recuperado de <http://es.wikipedia.org/wiki/wi-fi>

Wikipedia (2011) Bluetooth. Recuperado de <http://es.wikipedia.org/wiki/Bluetooth>

Wikipedia (2011) Comunicación inalámbrica. Recuperado de

http://es.wikipedia.org/wiki/Tecnolog%C3%AD_a_inal%C3%A1mbrica

Wikipedia (2011) Red inalámbrica. Recuperado de

http://es.wikipedia.org/wiki/red_inal%C3%A1mbrica.

Wikipedia (2012) Punto de acceso inalámbrico. Recuperado de

http://es.wikipedia.org/wiki/punto_de_acceso_inal%C3%A1mbrico

ANEXOS

Introducción a Wi-Fi (802.11)

El estándar 802.11 establece los niveles inferiores del modelo OSI para las conexiones inalámbricas que utilizan ondas electromagnéticas, por ejemplo:

- La capa física (a veces abreviada capa "PHY") ofrece tres tipos de codificación de información.
- La capa de enlace de datos compuesta por dos subcapas: **control de enlace lógico (LLC)** y **control de acceso al medio (MAC)**.

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red. En realidad, el estándar 802.11 tiene tres capas físicas que establecen modos de transmisión alternativos:

Capa de enlace de datos		802.2
(MAC)		802.11
Capa	física	DSSS FHSS Infrarrojo
(PHY)		

Cualquier protocolo de nivel superior puede utilizarse en una red inalámbrica Wi-Fi de la misma manera que puede utilizarse en una red Ethernet.

Los distintos estándares Wi-Fi

El estándar 802.11 en realidad es el primer estándar y permite un ancho de banda de 1 a 2 Mbps. El estándar original se ha modificado para optimizar el ancho de banda (incluidos los estándares 802.11a, 802.11b y 802.11g, denominados estándares físicos 802.11) o para especificar componentes de mejor manera con el fin de garantizar mayor seguridad o compatibilidad. La tabla a continuación muestra las distintas modificaciones del estándar 802.11 y sus significados:

Nombre del estándar	Nombre	Descripción
802.11a	Wifi5	El estándar 802.11 (llamado WiFi 5) admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mbps). El estándar 802.11a provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	Wifi	El estándar 802.11 es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mbps (6 Mbps en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de

		frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	Combinación del 802.11 y el 802.1d	El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Internacionalización	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Mejora de la calidad del servicio	El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la <i>capa de enlace de datos</i> . El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	Itinerancia	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el <i>protocolo IAPP</i> que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la

red. También se conoce a esta propiedad simplemente como *itinerancia*.

802.11g El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mbps en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.

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

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

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

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

También es importante mencionar la existencia de un estándar llamado "*802.11b+*". Éste es un estándar patentado que contiene mejoras con respecto

al flujo de datos. Por otro lado, este estándar tiene algunas carencias de interoperabilidad debido a que no es un estándar IEEE.

Rango y flujo de datos

Los estándares 802.11a, 802.11b y 802.11g, llamados "estándares físicos", son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos.

Estándar	Frecuencia	Velocidad	Rango
WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2,4 GHz	11 Mbit/s	100 m
WiFi G (802.11g)	2,4 GHz	54 Mbit/s	100 m

802.11a

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

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

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

802.11b

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

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

802.11g

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

Velocidad hipotética	Rango	Rango
	(en ambientes cerrados)	(al aire libre)
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

GLOSARIO

WIRELESS

Wireless Application Protocol o **WAP** protocolo de aplicaciones inalámbricas es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, p.ej. acceso a servicios de Internet desde un teléfono móvil.

Se trata de la especificación de un entorno de aplicación y de un conjunto de protocolos de comunicaciones para normalizar el modo en que los dispositivos inalámbricos, se pueden utilizar para acceder a correo electrónico, grupo de noticias y otros.

BROADCAST

Un **dominio de difusión** es un área lógica en una red de ordenadores en la que cualquier ordenador conectado a la red puede transmitir directamente a cualquier otro en el dominio sin precisar ningún dispositivo de encaminamiento, dado que comparten la misma subred, dirección de puerta de enlace y están en la misma VLAN (VLAN por defecto o instalada).

INTRANET

Una **intranet** es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de

información y sistemas operacionales. El término intranet se utiliza en oposición a Internet, una red entre organizaciones, haciendo referencia por contra a una red comprendida en el ámbito de una organización.

IEEE

Corresponde a las siglas de (Institute of Electrical and Electronics Engineers) en español **Instituto de Ingenieros Eléctricos y Electrónicos**, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Con cerca de 400.000 miembros y voluntarios en 180 países, es la mayor asociación internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación e ingenieros en Mecatrónica.

HOMERF

El grupo que desarrollaba el estándar HomeRF se disolvió en Enero de 2003.

Existen el HomeRF y el HomeRF2.

La idea de este estándar se basa en el Teléfono inalámbrico digital mejorado (Digital Enhanced Cordless Telephone, DECT) que es un equivalente al estándar de los teléfonos celulares GSM. Transporta voz y datos por separado, al

contrario que protocolos como el WiFi que transporta la voz como una forma de datos. Los creadores de este estándar pretendían diseñar un aparato central en cada casa que conectara los teléfonos y además proporcionar un ancho de banda de datos entre las computadoras.

Las prestaciones de este sistema son:

- Modulación FSK (Frequency Shift Keying).
- Velocidad de datos variables de entre 800 Kbps y 1.6Mbps.
- Utiliza la banda de 2.4 Ghz.
- 75 canales de 1 Mhz para voz.

El HomeRF2:

- Velocidad de entre 5 y 10 Mbps.
- 15 canales de 5 MHz para voz

Cabe resaltar que el estándar HomeRF posee multitud de capacidades de voz (identificador de llamadas, llamadas en espera, regreso de llamadas e intercomunicación dentro del hogar).

RFID

(siglas de Radio Frequency IDentification, en español identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos

remoto que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (automatic identification, o identificación automática).

GPRS

General Packet Radio Service (GPRS) o servicio general de paquetes vía radio es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes). Existe un servicio similar para los teléfonos móviles que del sistema IS-136. Permite velocidades de transferencia de 56 a 144 kbps.

GSM CDMA2000

es una familia de estándares de telecomunicaciones móviles de tercera generación (3G) que utilizan CDMA, un esquema de acceso múltiple para redes digitales, para enviar voz, datos, y señalización (como un número telefónico marcado) entre teléfonos celulares y estaciones base. Ésta es la segunda generación de la telefonía celular digital IS-95.

CDMA

(code division multiple access ó acceso múltiple por división de código) es una estrategia de multiplexado digital que transmite flujos de bits. Básicamente, CDMA permite que múltiples terminales compartan el mismo canal de frecuencia, identificándose el "canal" de cada usuario mediante (secuencias PN). CDMA2000 ha tenido relativamente un largo historial técnico, y aún sigue siendo compatible con los antiguos estándares en telefonía CDMA (como cdmaOne) primero desarrollado por Qualcomm, una compañía comercial, y propietario de varias patentes internacionales sobre la tecnología.

Los estándares CDMA2000 **CDMA2000 1x**, **CDMA2000 1xEV-DO**, y **CDMA2000 1xEV-DV** son interfaces aprobadas por el estándar ITU IMT-2000 y un sucesor directo de la 2G CDMA, IS-95 (cdmaOne). CDMA2000 es estandarizado por 3GPP2.

CDMA2000 es una marca registrada de la Telecommunications Industry Association (TIA-USA) en los Estados Unidos, no del término genérico CDMA. (Similarmente Qualcomm bautizó y registró el estándar 2G basado en CDMA, IS-95, como cdmaOne).

CDMA2000 es un competidor incompatible con otros estándares 3G como W-CDMA (UMTS).

Debajo están las diferencias entre los diferentes tipos de CDMA2000, en orden de complejidad ascendente:

- 1_CDMA2000 1x
- 2_CDMA2000 3x
- 3_CDMA2000 1xEV-DO
- 4_CDMA2000 1xEV-DV

CDPD

Es el acrónimo de "Cellular Digital Packet Data" es una tecnología de transmisión de datos en terminales TDMA, El sistema está basado en la tecnología IBM CelluPlan II, pero desarrollada por Ericsson y descontinuada a finales de los 90, que pretendía mejorar las prestaciones de la existente tecnología celular analógica.

CDPD usa canales libres en terminales AMPS/TDMA para transmitir datos. Requiere un canal libre de 30 KHz, con una velocidad de **19200 bps** y una tasa de transferencia neta de 9600 bps, si todos los canales de voz de la red están copados, los datos son almacenados hasta que alguno de ellos quede libre. Poseía para la época un excelente rendimiento inalámbrico, compresión de paquetes y corrección de errores; además poseía la función "Always On", lo

cual facilitaba el desempeño en sus aplicaciones. Igualmente era compatible con servicios de Roaming internacional.

Se distinguen tres tipos de host:

- el móvil.
- la estación base.
- la estación base de la interfaz.

Y tres tipos de interfaz:

- E: externa al proveedor CDPD, para conexión con otras redes.
- I: interna al proveedor CDPD, para conectar zonas del mismo CDPD.
- A: interfaz entre las estaciones bases y las móviles.

MOBITEX

Es un OSI basado en estándar abierto, el acceso público nacional inalámbrica de conmutación de paquetes de red de datos. Mobitex pone gran énfasis en la seguridad y la fiabilidad de su uso por militares, policías, bomberos y servicios de ambulancia. Mobitex se desarrolló a principios de la década de 1980 por el sueco Televerket Radio. Desde 1988, el desarrollo tuvo lugar en Eritel, una joint-venture entre la Ericsson y Televerket, más tarde como un Ericsson subsidiarios. Mobitex entró en funcionamiento en Suecia en 1986.

HSPA

La tecnología HSDPA (High Speed Downlink Packet Access), también denominada 3.5G, 3G+ o turbo 3G, es la optimización de la tecnología espectral UMTS/WCDMA, incluida en las especificaciones de 3GPP release 5 y consiste en un nuevo canal compartido en el enlace descendente que mejora significativamente la capacidad máxima de transferencia de información pudiéndose alcanzar tasas de bajada de hasta 14 Mbps (1.8, 3.6, 7.2 y 14.4 Mbps). Soporta tasas de throughput promedio cercanas a 1 Mbps. Es la evolución de la tercera generación (3G) de tecnología móvil, llamada 3.5G, y se considera el paso previo antes de la cuarta generación (4G), la futura integración de redes. Actualmente se está desarrollando la especificación 3.9G antes del lanzamiento de 4G.

3G

Es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (Universal Mobile Telecommunications System o servicio universal de telecomunicaciones móviles).

Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz y datos (una llamada telefónica o una video llamada) y datos no-voz (como la descarga de programas, intercambio de email, y mensajería instantánea). Aunque esta tecnología estaba orientada a la telefonía

móvil, desde hace unos años las operadoras de telefonía móvil ofrecen servicios exclusivos de conexión a Internet mediante módem usb, sin necesidad de adquirir un teléfono móvil, por lo que cualquier computadora puede disponer de acceso a Internet. Existen otros dispositivos como algunos ultra portátiles (netbooks) que incorporan el módem integrado en el propio equipo, pero requieren de una tarjeta SIM (la que llevan los teléfonos móviles) para su uso, por lo que en este caso sí es necesario estar dado de alta con un número de teléfono.

LMDS

El Sistema de Distribución Local Multipunto o LMDS (del inglés Local Multipoint Distribution Service) es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda. LMDS usa señales en la banda de las microondas, en concreto la banda Ka (en torno a los 28 GHz, dependiente de las licencias de uso de espectro radioeléctrico del país), por lo que las distancias de transmisión son cortas (a esto se debe la palabra "Local" en el nombre de la tecnología), a tan altas frecuencias la reflexión de las señales es considerable (nótese que la banda Ka, es la banda del espectro usado para las comunicaciones satelitales). Pero también en muchos países europeos, se trabaja en 3,4 - 3,5GHz

WI-FI

Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros (65 pies) en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso. **Wi-Fi** es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

QOS

La calidad del servicio (QoS) se refiere a varios aspectos relacionados con la telefonía y las redes de computadoras que permiten el transporte de tráfico con requerimientos especiales. En particular, mucha de la tecnología ha sido desarrollada para permitir a las redes de computadoras para ser tan útil como la red telefónica para las conversaciones de audio, así como el apoyo a nuevas aplicaciones con más demanda de servicios estrictas.

IAPP

El acceso a Inter-Point Protocol (IAPP) es un estándar publicado por redes Wi-Fi. Fue diseñado para facilitar la itinerancia, donde el dueño de un dispositivo inalámbrico se mueve de una zona a otra, cambiar el dispositivo de la huella de un punto de acceso inalámbrico a otro.

ITINERANCIA

La itinerancia (popularmente se usa el vocablo inglés roaming, pr. róming, que significa vagar, rondar) es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra.

El concepto de roaming o itinerancia utilizado en las redes Wi-Fi significa que el dispositivo Wi-Fi del cliente puede desplazarse e ir registrándose en diferentes bases o puntos de acceso.

En telefonía móvil, la itinerancia (roaming en inglés) es la capacidad de enviar y recibir llamadas en redes móviles fuera del área de servicio local de la propia compañía, es decir, dentro de la zona de servicio de otra empresa del mismo país, o bien durante una estancia en otro país diferente, con la red de una empresa extranjera.

MIMISM (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (e.g. Wi-Fi) o WPAN (e.g. Bluetooth). Las bandas **ISM** fueron definidas por la ITU en el artículo 5 de las Regulaciones Radio (RR),¹ concretamente puntos 5.138 y 5.150. El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia, respetando las regulaciones que limitan los niveles de potencia transmitida. Este hecho fuerza a que este tipo de comunicaciones tengan cierta tolerancia frente a errores y que utilicen mecanismos de protección contra interferencias, como técnicas de ensanchado de espectro

RC4

Dentro de la criptografía **RC4** o **ARC4** es el sistema de cifrado de flujo Stream cipher más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

CRC

El CRC se utiliza como una detección de errores de código, el cual tiene una serie de aplicaciones usadas cuando se implementa mediante normas, convirtiéndolo así en un sistema práctico.

Estas son algunas de las aplicaciones:

- Se usa un patrón de prefijos de bit para comprobar su autenticidad. Esto es útil cuando la trama podría tener errores en los bits de delante de un mensaje, una alteración que, de otro modo dejaría sin cambios al CRC. A veces un envío agrega n bits (n es el tamaño de la CRC) al mensaje que se debe controlar ya que se cogería un polinomio que no sería el correcto para la división. Esto tiene la conveniencia de que el CRC del mensaje original con el CRC adjunto es exactamente cero, por lo que el CRC se puede comprobar simplemente por la división polinómica y comparando con el resto cero. A veces se realiza una implementación del CRC con OR exclusivos en el resto de la división polinómica.

- **Orden de los bits:** en ocasiones, el orden en el que se envían las tramas de datos no corresponden exactamente con la posición que tendrán los bits en la división polinómica; es decir, que puede que el primer bit enviado sea el de más peso o viceversa. Este convenio tiene sentido cuando las tramas a enviar se envían por puertos series ya que el CRC es comprobado por el hardware de

cada máquina, y cada uno tendrá un convenio conjunto de lectura y posicionamiento de paquetes para el envío a la capa siguiente.

- **Omisión del orden del bit de más peso del polinomio divisor:** algunos escritores proponen omitir esto, puesto que el bit mayor peso es siempre 1, y ya que el bit CRC debe ser definido por un $(n + 1)$ bits del divisor, es innecesario mencionar el divisor mayor peso en el mensaje y en el CRC.

AES

Advanced Encryption Standard (AES), también conocido como **Rijndael** (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

El cifrador fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, ambos estudiantes de la Katholieke Universiteit Leuven, y enviado al proceso de selección AES bajo el nombre "Rijndael"