Universidad Autónoma de Querétaro

Facultad de Informática

Opción de titulación: Cursos de Actualización

"REDES WLAN."

Profesor Titular: José Luis Gutiérrez

Alumno: Gerardo Rubio Loyola

Generación: 2001-2005

INDICE

INDICE FIGURAS:

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

INDICE DE TABLAS:

CAPITULO 2

INTRODUCCIÓN:

En el terreno de la computación, la historia es diferente, lo inalámbrico ha tenido un gran auge en el mundo de las redes, Las redes inalámbricas conocidas como WLAN se han extendido rápidamente y ampliamente a pesar de la recesión en la economía de las telecomunicaciones en el mundo.

En sus inicios, las aplicaciones de las redes inalámbricas fueron confinadas a industrias y grandes almacenes. Hoy en día, las redes WLAN´s son instaladas en universidades, oficinas y hogares y hasta en espacios públicos. Las WLAN típicamente consisten en equipos portátiles aunque también pueden ser equipos de escritorio que se conectan a dispositivos fijos a los cuales llamamos puntos de acceso (Access Points). Ya que son dispositivos que nos dan la oportunidad de tener una conexión a la red sin necesidad de cables.

Expertos en el campo siguen haciendo énfasis en los problemas inherentes de las tecnologías inalámbricas, tales como las limitaciones del ancho de banda disponible, problemas con interferencia y seguridad de la información transmitida. Sin embargo muchas de estas barreras que han inhibido el crecimiento de la tecnología inalámbrica están siendo resueltas. Se están superando las cuestiones que giraron alrededor de la estandarización y un número creciente de compañías están ofreciendo una gran variedad de soluciones de hardware y software.

CAPITULO 1 ASPECTOS BASICOS:

1.1 Definición de red

Una red es justamente un sistema de comunicación que se da entre distintos equipos para poder realizar una comunicación eficiente, rápida y precisa, para la transmisión de datos de una computadora a otra, realizando entonces un intercambio de Información (recordando que una Información es un conjunto ordenado de Datos) y compartiendo también Recursos disponibles en el equipo.

La red tiene que estar conformada indefectiblemente por una Terminal (el punto de partida de la comunicación) o un nodo que permita la conexión, y esencialmente el Medio de Transmisión, que es definido esencialmente por la conexión que es llevada a cabo entre dichos equipos.

Esta conexión puede ser realizada en forma directa, utilizando cables de todo tipo, o bien mediante Ondas Electromagnéticas, presentes en las tecnologías inalámbricas, que requieren un adaptador específico para esta comunicación, que puede ser incluido en el equipo o conectado al equipo.

1.2 MODELOS DE REDES

Modelo OSI

El modelo OSI (Open System Interconnection) se basa en una propuesta desarrollada por la Organización Internacional de Normas (ISO) como primer paso hacia la estandarización internacional de los protocolos utilizados en las diversas capas.

El modelo OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas se pueden resumir de la siguiente manera:

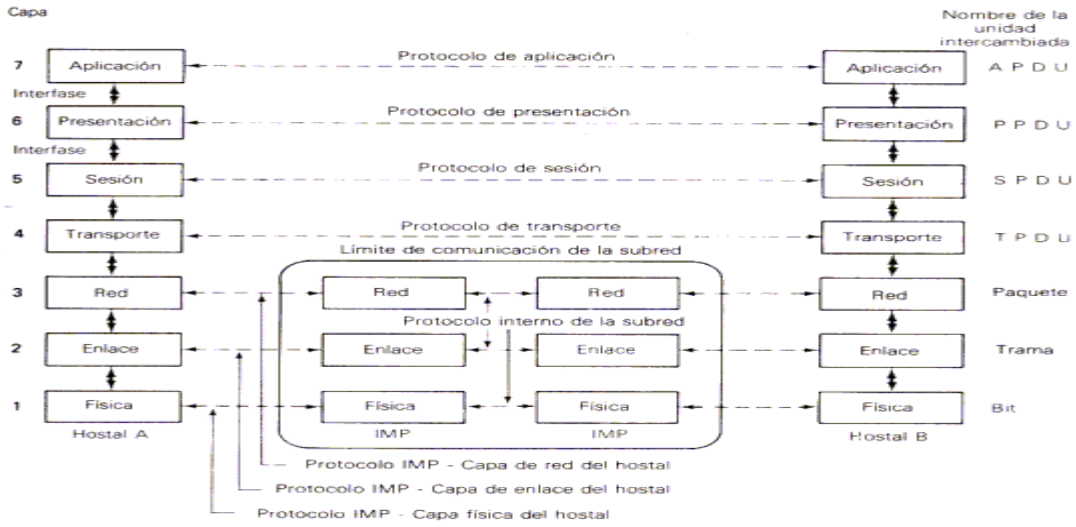

Figura 1.2.1 Capas del modelo OSI

CAPA 1 Capa Física

La capa física abarca los aspectos físicos de la red (cables, **hub's**, y el resto de dispositivos que conforman el entorno físico de la red), se relaciona con la transmisión de **bits** puros a través de un canal de transmisión. Los aspectos de diseño tienen que ver con la acción de asegurarse que cuando uno de los lados envíe un bit 1, el otro lado lo reciba también como un bit 1, Los aspectos de diseño tiene que ver con las interfaces mecánica, eléctrica y de temporización, así como con el medio de transmisión físico que se encuentra bajo la capa física.

CAPA 2 Capa de Enlace de Datos

La principal tarea de la capa de enlace de datos es transformar un medio de transmisión puro en una línea que esté libre de errores de transmisión. Enmascara los errores reales, de manera que la capa de red no los vea. Para lograr esto, el emisor divide los datos de entrada en *tramas de datos* y transmite las tramas en forma secuencial. Si el servicio es confiable, para confirmar la recepción correcta de cada trama, el receptor devuelve una trama de confirmación de recepción.

Las redes de difusión tienen una consideración adicional en la capa de enlace de datos en cómo controlar el acceso al canal compartido, una sub-capa llamada *control de acceso al medio* es la que se encarga de ese problema.

CAPA 3 Capa de Red

La capa de red controla la operación de subred. Su función es determinar cómo se encaminan los paquetes desde el origen hasta el destino, es donde las direcciones físicas (direcciones de hardware de la **NIC**), pasan a convertirse en direcciones lógicas (direcciones IP), Las rutas se pueden basar en tablas estáticas que se "codifican" en la red y rara vez cambian pero es más común que se actualicen de manera automática para evitar las fallas en los componentes. También se pueden determinar el inicio de cada conversación;

por ejemplo, en una sesión de Terminal al iniciar sesión en una maquina remota. Por último, pueden ser muy dinámicas y determinarse de nuevo cada paquete, de manera que se pueda reflejar la carga actual de la red.

Si hay demasiados paquetes en la subred al mismo tiempo se formaran cuellos de botella, El manejo de la congestión de paquetes es también responsabilidad de la capa de red, los "routers" operan precisamente en la capa de red y utilizan los protocolos de encaminamiento de dicha capa para determinar que ruta deben seguir los paquetes de datos.

CAPA 4 Capa de transporte

La función básica de la capa de transporte es aceptar datos de la capa superior, dividirlos en unidades más pequeñas si es necesario, pasar estos datos a la capa de red y asegurar que todas las piezas lleguen correctamente al otro extremo, todo esto se debe realizar con eficiencia y de una manera que aísle las capas superiores de los cambios tecnológicos.

La capa de transporte también determina el tipo de servicio que debe proveer a la capa de sesión y en última instancia a los usuarios de la red. El tipo de conexión más popular en esta capa es la de punto a punto, que es libre de errores y entrega los mensajes en el orden en que se enviaron, también existe el transporte de mensajes aislados, estos no garantizan el orden de entrega.

La capa de transporte es una verdadera capa de extremo a extremo; lleva los datos por toda la ruta desde el origen hasta el destino. En las capas inferiores cada uno de los protocolos está entre una máquina y sus vecinos inmediatos, no entre las verdaderas máquinas de origen y de destino que puedan estar separadas por muchos "routers".

CAPA 5 Capa de Sesión

La capa de sesión es la encargada de establecerle enlace de comunicación o sesión entre dos computadoras, permite a los usuarios en distintas maquinas establecer sesiones entre ellos. Las sesiones nos ofrecen varios servicios, incluyendo el control del diálogo (llevar el control de quien va a transmitir), el manejo de "**tokens**" (evitar que dos partes intenten la misma operación crítica al mismo tiempo) y la sincronización que se refiere a usar a usar puntos de referencia en las transmisiones extensas para reanudar desde el último punto de referencia en caso de una interrupción.

CAPA 6 Capa de Presentación

La capa de presentación se enfoca en la sintaxis y la semántica de la información transmitida. Para hacer posible la comunicación entre computadoras con distintas representaciones internas de datos, podemos definir de una manera abstracta las estructuras de datos que se van a intercambiar, La capa de presentación también se encarga de cifrar

datos (si así lo requiere la aplicación utilizada), así como de comprimirlos para reducir su tamaño. El paquete que crea la capa de presentación contiene los datos prácticamente con el formato con el que viajarán por las restantes capas de la pila OSI. La capa de presentación maneja estas estructuras de datos de mayor nivel (por ejemplo, registros bancarios).

CAPA 7 Capa de Aplicación

La capa de aplicación contiene una variedad de protocolos que los usuarios necesitamos con frecuencia, uno de ellos es el HTTP (HyperText Transfer Protocol), el cual forma la base para la **World Wide Web**. Cuando un navegador desea una página web, envía el nombre de la página que quiere al servidor que la hospeda mediante el uso de http. Después el servidor envía la página de vuelta. Hay otros protocolos de aplicación que se utilizan para transferir archivos, enviar y recibir correo electrónico y noticias.

Modelo de referencia TCP/IP

Es un modelo de descripción de protocolos de res, Este modelo se utilizó en la más vieja de todas las redes de computadoras de área amplia (ARPANET) y su sucesora Internet. ARPANET era una red de investigación patrocinada por el Departamento de defensa de Estados Unidos (DoD), la cual llego a interconectar en un momento dado a universidades e instalaciones gubernamentales mediante el uso de líneas telefónicas arrendadas, poco después se le unieron redes de satélite y de radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitaba una nueva arquitectura de referencia, posteriormente esta arquitectura se dio a conocer como el modelo de referencia TCP/IP.

El modelo TCP/IP, describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos.

TCP/IP tiene cuatro capas de abstracción, Esta arquitectura de capas a menudo es comparada con el Modelo OSI.

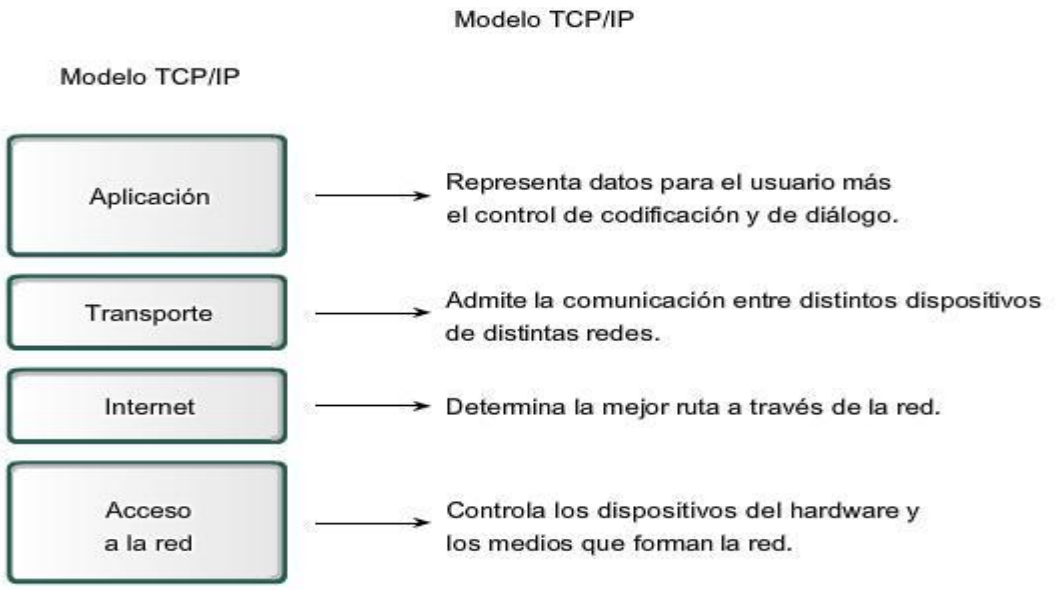

Figura 1.2.2 Modelo TCP/IP

CAPA 1 Capa de acceso de red.

Es la capa más baja de este modelo la cual describe que enlaces (líneas seriales, **Ethernet**) se deben llevar a cabo para cumplir con las necesidades de esta capa de internet sin conexión, más bien se puede considerar como una interfaz entre los hosts y los enlaces de transmisión, esto si lo comparamos con el modelo OSI, vendría siendo como la capa física y la capa de enlace de datos del modelo OSI.

CAPA 2 Capa de internet

Esta capa es el eje que mantiene unidad toda la arquitectura, su trabajo es permitir que los host inyecten paquetes en cualquier red y que viajen de manera independiente hacia el destino, incluso pueden llegar en un orden totalmente diferente al orden en que se enviaron, en cuyo caso es responsabilidad de las capas superiores volver a ordenarlos, la capa de Internet define un formato de paquete y un protocolo oficial llamado IP (Protocolo de Internet), además de un protocolo complementario ICMP (Protocolo de Mensajes de Control de Internet), el cual le ayuda a funcionar, la tarea de la capa de Internet es entregar los paquetes IP a donde se supone que deben ir. Aquí el ruteo de los paquetes es sin duda el principal aspecto, al igual que la congestión.

CAPA 3 Transporte

Esta capa está diseñada para permitir que las entidades pares, en los nodos de origen y de destino, lleven a cabo una conversación, al igual que en la capa de transporte del modelo OSI. Aquí se definieron dos protocolos de transporte de extremo a extremo. El primero es el TCP (Protocolo de control de transmisión), el cual es un protocolo confiable orientado a la conexión que permite que un flujo de bytes originado en una maquina se entregue sin

errores a cualquier otra máquina en Internet, dicho protocolo segmenta el flujo de bytes entrante en mensajes discretos y pasa cada uno a la capa de internet. En la maquina destino el proceso TCP vuelve a ensamblar los mensajes recibidos para formar el flujo de salida que hubo en la maquina transmisora, este protocolo también maneja el control de flujo de paquetes para que un emisor rápido no pueda inundar a un receptor lento con más paquetes de información de los que este pueda manejar.

El segundo protocolo de esta capa es el UDP (Protocolo de Datagrama de Usuario), el cual es un protocolo sin conexión, no confiable para aplicaciones que no desean la asignación de secuencia o el control de flujo de TCP y prefieren proveerlos por su cuenta. También se usa mucho en las consultas de petición-respuesta de una sola ocasión del tipo cliente-servidor, y en las aplicaciones en las que es más importante una entrega oportuna que una entrega precisa, como en la transmisión de voz o video.

En la siguiente figura (1.2.3) se muestra la relación entre IP, TCP y UDP desde que se desarrolló este modelo.

<table>
<tr><td rowspan="2">Aplicación</td><td>FTP</td><td>TFTP</td><td>LDP</td><td>NFS</td></tr>
<tr><td>SNMP</td><td>SMTP</td><td>Telnet</td><td>X Window</td></tr>
<tr><td>Transporte</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td rowspan="2">Internet</td><td>ICMP</td><td>ARP</td><td colspan="2">RARP</td></tr>
<tr><td colspan="4">IP</td></tr>
<tr><td>Acceso a la Red</td><td>Ethernet</td><td>Fast Ethernet</td><td>Token Ring</td><td>FDDI</td></tr>
</table>

Figura 1.2.3 Protocolos da las capas del modelo TCP/IP

CAPA 4 Capa de Aplicación

El modelo TCP/IP no tiene capas de sesión o de presentación, ya que no se consideraron necesarias. Las aplicaciones simplemente incluyen cualquier función de sesión y de presentación que requieran. La experiencia con el modelo OSI ha demostrado que esta visión fue correcta: estas capas se utilizan muy poco en la mayoría de las aplicaciones. La capa de aplicación maneja aspectos de representación, codificación y control de diálogo y a su vez contiene todos los protocolos de alto nivel. Entre los primeros protocolos están el de Terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP), entre otros como el de Sistema de Nombres de Dominio (DNS) el cual se utiliza para la resolución de nombres de host a sus direcciones de red, el HTTP, el cual se utiliza para recuperar páginas de la World Wide Web; y RTP el cual es un protocolo para transmitir medios en tiempo real, como voz o películas.

1.3 TOPOLOGIAS DE REDES :

Una red de área local está formada por varios equipos(a los cuales les llamamos nodos), como computadoras, impresoras, escáneres, etc, unidos entre sí, mediante líneas de comunicación y conectores. Estos elementos se pueden conectar de distintas maneras. A las distintas formas de conectar los componentes de una red local se les llama topologías y esta define la estructura de una red.

1.3.1 TOPOLOGIA DE BUS:

Esta es la topología más sencilla. En las redes que tienen esta tecnología, todos los nodos de la red están conectados a un mismo canal de comunicaciones llamado bus que suele ser un cable coaxial.

En los extremos del cable debe de haber un terminador que elimina las señales de retorno del bus, esto evita que reboten y sean recibidas nuevamente por los nodos conectados al bus.

En esta topología, la información se envía al bus, llega a todos los nodos conectados. Por este motivo cuando un nodo envía información al bus, todos los demás nodos de la red pueden ver dicha información.La información viaja por el cable en ambos sentidos a una velocidad aproximada de 10/100 Mbps. Se pueden conectar una gran cantidad de computadoras al bus, si un computador falla, la comunicación se mantiene, no sucede lo mismo si el bus es el que falla. El tipo de cableado que se usa puede ser coaxial, par trenzado o fibra óptica, el cable puede ir por el piso, las paredes, el techo o por varios lugares, siempre y cuando sea un segmento continuo. Cada nodo tendrá que comparar la dirección de destino de los datos para saber si la información recibida va dirigía a él o no.

VENTAJAS:

- La sencillez de las redes en bus hace que su montaje sea fácil, así como las tareas de añadir o eliminar un nodo de la red.
- Si algo se daña, o si una computadora se desconecta, esa falla es muy barata y fácil de arreglar.
- Es muy barato realizar todas la conexiones de la red, ya que los elementos a emplear no son muy costosos.
- Los cables de internet y electricidad pueden ir juntos en esta topología.

DESVENTAJAS:

- Si un usuario desconecta su computadora de la red, o hay alguna falla de la misma como la rotura del cable, la red deja de funcionar.
- Las computadoras de la red no regeneran la señal sino que se transmite o es generada por el cable y ambas resistencias en los extremos.

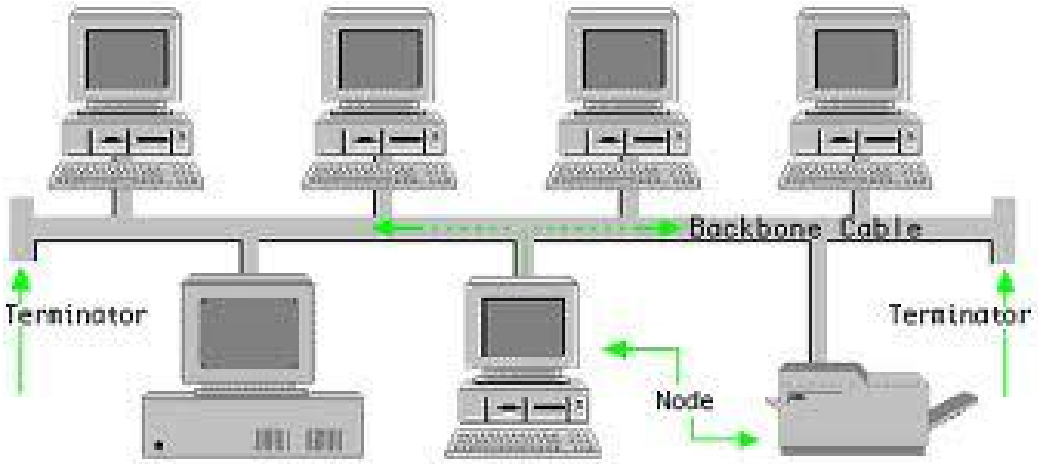

Figura 1.3.1.1 Topología de Bus

1.3.2 TOPOLOGÍA DE ANILLO:

En esta topología cada nodo está conectado a sus dos nodos adyacentes por enlaces punto a punto, formando un anillo cerrado o circulo por el cual viaja la información. Es habitual el uso de fibra óptica como medio físico.

En las redes con topología de anillo, la información circula de un nodo al adyacente, en un único sentido. Para ello, cada nodo del anillo tiene un receptor y un transmisor que hacen la función de repetidor pasando la información al siguiente nodo. En cada momento, solo uno de los nodos que forman el anillo tiene permiso para hablar, este permiso se denomina testigo o *token* y se va pasando de un nodo al siguiente. De esta manera se evitan las colisiones.

En las redes que tienen esta topología, si uno de los nodos deja de funcionar la red también fallará. Sin embargo, actualmente hay conectores especiales que permiten la desconexión del nodo averiado para que el sistema pueda seguir funcionando.

VENTAJAS:

- El sistema provee un acceso equitativo para todas las computadoras.
- El rendimiento no decae cuando muchos usuarios utilizan la red.

DESVENTAJAS:

- La falla de una computadora altera el funcionamiento de toda la red.
- Las distorsiones afectan a la red.

Figura 1.3.2.1 Topología de Anillo

1.3.3 TOPOLOGIA DE ESTRELLA:

En esta topología existe un nodo central, enlazado directamente con todos los demás, que controla el tráfico de datos por la red, reenviando los datos a su destino. Cada nodo tiene un enlace punto a punto con el nodo central. Cuando un nodo quiere mandar datos a otro, los envía a través del nodo central que es quien los reenvía a su destino.

El nodo central puede ser un switch o un hub al que se conectan los otros nodos. Puede ser activo o pasivo. Un concentrador es activo cuando regenera la señal recibida antes de reenviarla, y pasivo cuando simplemente proporciona una conexión entre los dispositivos conectados, sin regeneración de señal.

Si se envían los datos solo al destino o a todas las estaciones, dependerá de si el concentrador es un hub o un switch.

VENTAJAS:

- Es una topología fácil de diseñar, instalar y mantener
- Si un nodo que no sea el central falla, la red sigue funcionando
- La detección y reparación de fallos es sencilla.

DESVENTAJAS:

- Como toda la información que circula por la red debe pasar por el nodo central, este se convierte en el cuello de botella de la red, ya que todos los mensajes deben pasar por él. Si el nodo central falla, la red no funcionará.

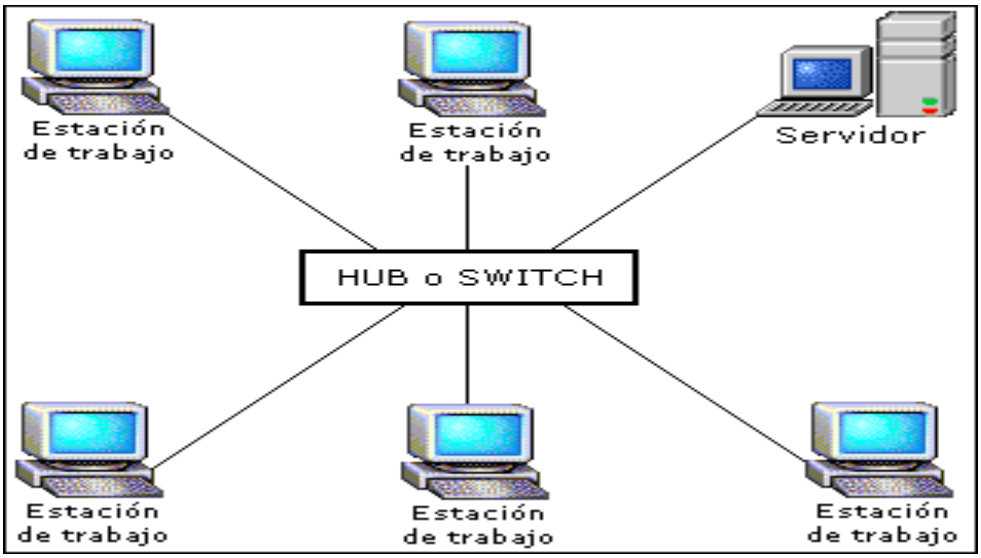

Figura 1.3.3.1 Topología de Estrella

1.3.4 TOPOLOGÍA DE ARBOL:

La red en árbol es una topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto

raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

Los problemas asociados a las topologías anteriores radican en que los datos son recibidos por todas las estaciones sin importar para quien vayan dirigidos. Es entonces necesario dotar a la red de un mecanismo que permita identificar al destinatario de los mensajes, para que estos puedan recogerlos a su arribo. Además, debido a la presencia de un medio de transmisión compartido entre muchas estaciones, pueden producirse interferencia entre las señales cuando dos o más estaciones transmiten al mismo tiempo.

VENTAJAS:

- Facilita la resolución de problemas
- Esta topología facilita el crecimiento de la red

DESVENTAJAS:

- El fallo de un nodo implica la interrupción de las comunicaciones en toda la rama del árbol que cuelga de ese nodo.

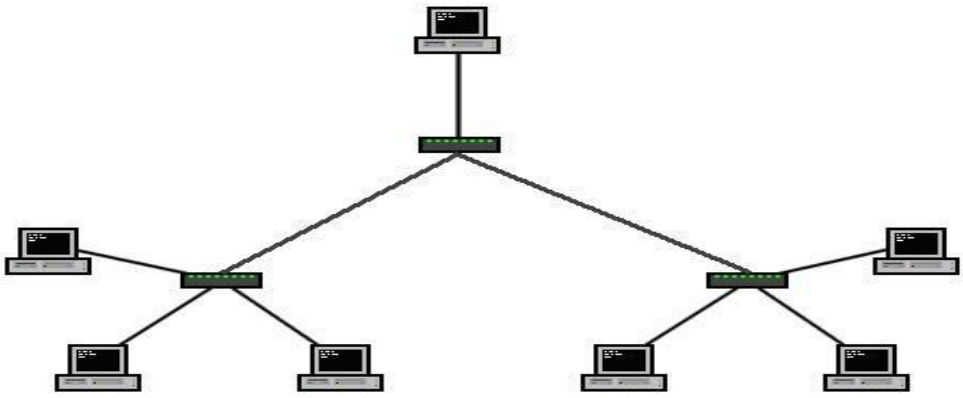

Figura 1.3.4.1 Topología Árbol

1.3.5 TOPOLOGIA EN MALLA:

La topología de red mallada es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

Esta topología, a diferencia de otras (como la topología en árbol y la topología en estrella), no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento (un error en un nodo, sea importante o no, no implica la caída de toda la red).Las redes de malla son

“autoruteables”. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

Es una opción aplicable a las redes sin hilos (wireless), a las redes cableadas (wired) y a la interacción del software de los nodos.

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. Aunque la facilidad de solución de problemas y el aumento de la confiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado. Por ello cobran mayor importancia en el uso de redes inalámbricas (por la no necesidad de cableado) a pesar de los inconvenientes propios de las redes sin hilos.En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida.

Una red de malla extiende con eficacia una red, compartiendo el acceso a una infraestructura de mayor porte.

VENTAJAS:

- Es posible llevar los mensajes de un nodo a otro por diferentes caminos.
- No puede existir absolutamente ninguna interrupción en las comunicaciones.
- Cada servidor tiene sus propias comunicaciones con todos los demás servidores.
- Si falla un cable el otro se hará cargo del tráfico.
- No requiere un nodo o servidor central lo que reduce el mantenimiento.
- Si un nodo desaparece o falla no afecta en absoluto a los demás nodos.
- Si desaparece no afecta tanto a los nodos de redes.

DESVENTAJAS:

- El costo de la red puede aumentar en los casos en los que se implemente de forma alámbrica, la topología de red y las características de la misma implican el uso de más recursos.

Figura 1.3.5.1 Topología Malla

CAPITULO 2 REDES WLAN:

2.1 DEFINICION DE UNA RED WLAN:

Es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Estas redes van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central.

2.2 FUNCIONAMIENTO:

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN 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. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado 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 OperatingSystem) y las ondas, mediante una antena.

2.3 TOPOLOGÍAS DE LAS REDES WLAN:

El conjunto de estandares 802.11 definen 3 modos fundamentales para las redes inalambricas:

1.-BSS
2.-IBSS
3.-EBSS

Es importante comprender que no siempre, los modos se ven reflejados directamente en la topología.Por ejemplo, un enlace punto a punto puede ser implementado en modo *ad hoc* o Infraestructura y nos podríamos imaginar una red en estrella construida por conexiones *ad hoc*. El modo puede ser visto como la configuración individual de la tarjeta inalámbrica de un nodo, más que como una característica de toda una infraestructura.

2.3.1 BSS

Contrario al modo *ad hoc* donde no hay un elemento central, en el modo de infraestructura hay unelemento de "coordinación": un punto de acceso o estación base. Si el punto de acceso se conecta a una red Ethernet cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID. Para asegurar que se maximice la capacidad total de la red, no configure el mismo canal en todos los puntos de acceso que se encuentran en la misma área física. Los clientes descubrirán (a través del escaneo de la red) cuál canal está usando el punto de acceso de manera que no se requiere que ellos conozcan de antemano el número de canal.

A continuación se muestra una imagen de la topología BSS (Figura 2.3.1.1):

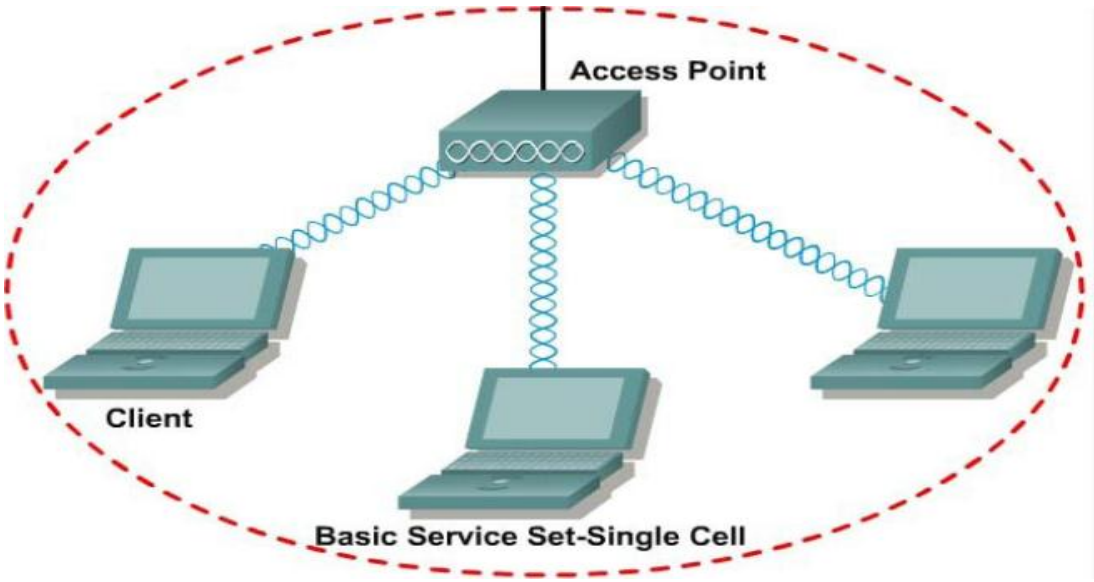

Figura 2.3.1.1 Topología BSS

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

CASO 1: Estrella:

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

Tabla 2.3.1.1 Caso Estrella

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

Caso 2: Punto a Punto

Los enlaces punto a punto son un elemento estándar de la infraestructura inalámbrica. A nivel detopología estos pueden ser parte de una topología de estrella, de una simple línea entre dos puntos u otra topología. Un enlace punto a punto puede establecerse en modo *ad hoc*.

Tabla 2.3.1.2 Caso Punto a Punto

Configuración	Nodo 1	Nodo 2
Modo	Cualquiera	Cualquiera
SSID	MI_SSID	MI_SSID
Canal	Cualquiera	Cualquiera
Dirección IP	Normalmente fija	Normalmente fija
Dirección MAC	Podría referirse a la MAC del otro nodo	Podría referirse a la MAC del otro nodo

La de arriba (Tabla 2.2) se refiere a una configuración típica de un enlace punto a punto. El modo puede ser *ad hoc* o infraestructura, pero los dos nodos deben utilizar el mismo modo y el mismo número de canal. Para enlaces punto a punto de largas distancias se deben configurar opciones inalámbricas avanzadas para lograr un mejor funcionamiento.

CASO 3 Repetidores:

El uso de repetidores se hace necesario generalmente cuando existen obstrucciones en la línea devista directa o hay una distancia muy larga para un solo enlace. En una red cableada, el dispositivoequivalente a un repetidor inalámbrico es un concentrador (hub). La configuración del repetidor depende de factores específicos de hardware y software y es difícil hacer una descripción genérica para este asunto. La unidad repetidora puede consistir en uno o dos dispositivos físicos y tener uno o dos radios. Un repetidor también puede ser visto como un cliente que cumple funciones de receptor y un punto de acceso de retransmisión. Normalmente, el SSID debería ser el mismo para las tres unidades. A menudo, además del SSID, el repetidor está enlazado a una dirección MAC.

CASO 4: Malla

La topología de malla es una opción interesante principalmente en ambientes urbanos, aunque también en áreas remotas en donde es difícil implementar una infraestructura

central. Esta topología se encuentra típicamente en redes municipales, campus universitarios y vecindarios.

Una red en malla es una red que emplea una de las dos distribuciones de conexión: topología de malla completa o de malla parcial. En la topología de malla completa, cada uno de los nodos se conecta directamente con todos los demás. En la topología de malla parcial, los nodos se conectan sólo a algunos de los otros nodos, no a todos. Note que esta definición no menciona dependencias sobre algún parámetro de tiempo de manera que nada es necesariamente dinámico en una malla. Sin embargo, en los años recientes y en relación con redes inalámbricas, el término "malla" se usa a menudo como sinónimo de red "*ad hoc*" o "móvil". Todos los nodos de una malla deben tener el mismo software de enrutamiento de malla (protocolo), pero pueden tener diferentes sistemas operativos y diferentes tipos de hardware.

La configuración de una red de malla depende del protocolo de enrutamiento de malla y de la implementación. La siguiente tabla muestra algunos parámetros típicos.

Tabla 2.3.1.3 Caso Malla

Opción	Nodo x1	Nodo x2
Modo	*ad hoc*	*ad hoc*
SSID	MI_SSID	MI_SSID
Canal	Canal x	Canal x
Dirección IP	Normalmente estática y definida manualmente	Normalmente estática y definida manualmente
Dirección MAC	Podría referirse a la MAC del otro nodo	Podría referirse a la MAC del otro nodo

En una red de malla el uso de DHCP no es trivial, de manera que se recomienda el uso de direcciones IP estáticas. Los gateways requieren la configuración de opciones adicionales para anunciar su presencia.

2.3.2 IBSS

Es también conocido como *ad hoc,* es un método para que los clientesinalámbricos puedan establecer una comunicación directa entre sí. Al permitir que los clientes inalámbricos operen en modo *ad hoc*, no es necesario involucrar un punto de acceso central.

Todos los nodos de una red *ad hoc* se pueden comunicar directamente con otros clientes. Cada cliente inalámbrico en una red *ad hoc* debería configurar su adaptador inalámbrico en modo *ad hoc* y usar los mismos **SSID** y "número de canal" de la red.Una red *ad hoc* normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca unos de otros. En una red *ad hoc* el rendimiento es menor a medida que el número de nodos

crece.Para conectar una red *ad hoc* a una red de área local (LAN) cableada o a Internet, se requiereinstalar una pasarela o **Gateway**especial.

El término latino *ad hoc* significa "para esto" pero se usa comúnmente para describir eventos o situaciones improvisadas y a menudo espontáneas. En redes IEEE 802.11 el modo *ad hoc* se denota como Conjunto de Servicios Básicos Independientes (IBSS – IndependentBasic Service Set), a continuación se muestra una imagen de una topología IBSS:

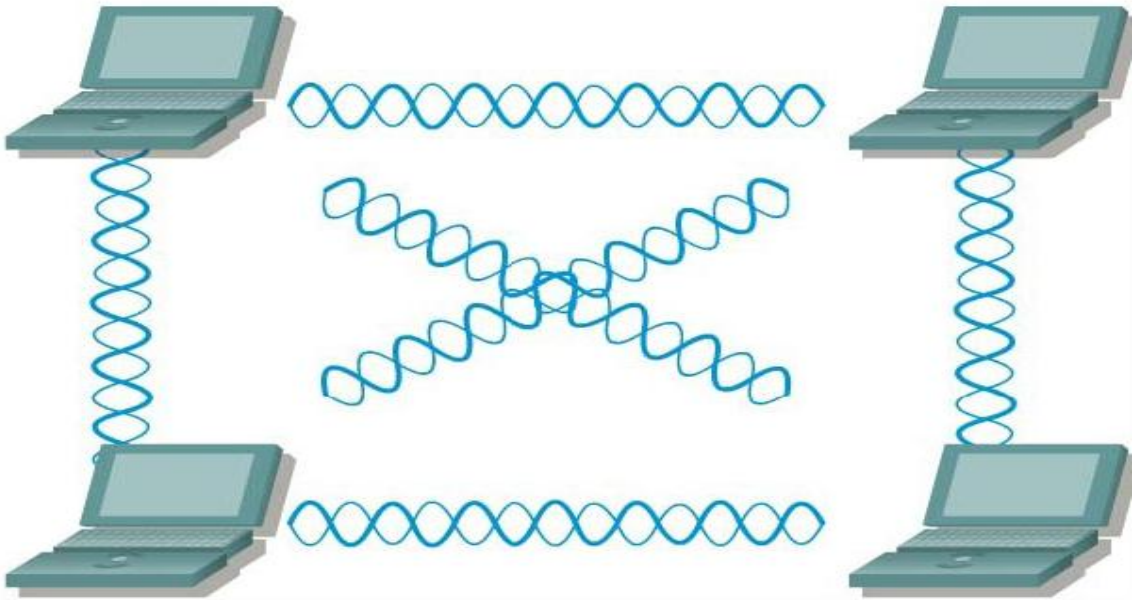

Figura 2.3.2.1 Topología IBSS

Caso 1: Punto a Punto

Puede usar el modo *ad hoc* cuando desea conectar directamente dos estaciones, de edificio aedificio. También lo puede usar dentro de una oficina entre un conjunto de estaciones de trabajo.

Tabla 2.3.2.1 IBSS Punto a Punto

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

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

2.3.3 EBSS

El modo EBSS está formado por un conjunto de BSS asociadas mediante un sistema de distribución formando una subred única. Esto permite una serie de prestaciones opcionales como el **roaming** entre celdas. Teniendo en cuenta que las redes WLAN tendrán la necesidad de conectarse a las redes LAN cableadas, este será el modo de operación generalmente adoptado en las redes WLAN de empresas con más de un **AP**y en las redes públicas.

El sistema de distribución de esta topología puede ser cableado o inalámbrico, así mismo, existen dos tipos de arquitecturas dentro de esta topología:

1.- *La arquitectura de red distribuida:*

Es el mecanismo mediante el cual se comunican los puntos de acceso de las diferentes BSS. En términos generales se clasifican como

- *Sistemas de distribución cableados:* los cuales normalmente se realizan mediante una red LAN Ethernet.
- *Sistemas de distribución inalámbrica:*

    - Enlace inalámbrico WLAN basado en el estándar 802.11 el cual veremos más adelante. En este caso se emplea el mecanismo WDS (WirelessDistributionSystem), Este mecanismo es conocido comoWireless LAN Bringing. Con este sistema, el número máximo de enlaces aconsejados entre puntos de acceso es de 3, a partir de este número, la señal se degrada.

2.- *La arquitectura de red centralizada:*

Esta solución está orientada a entornos empresariales y redes WLAN públicas con determinados requerimientos de calidad de servicio y seguridad.

La figura 2.3.3.1 muestra en ejemplo de la topología EBSS:

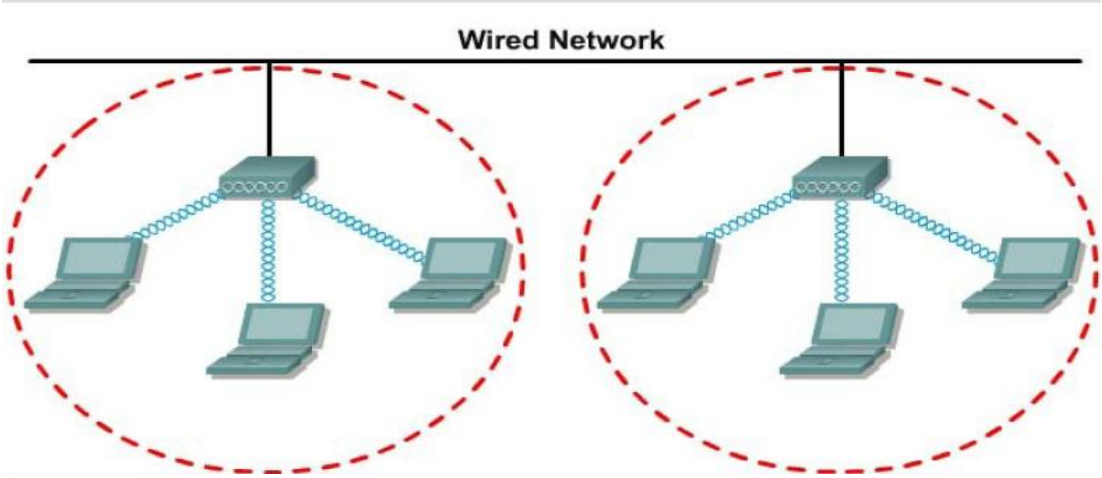

Figura 2.3.3.1 Topología EBSS

2.4 ESTANDAR IEEE 802.11

Define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

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** 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.

2.4.1 ESTANDARES DE CAPA FISICA Y ENLACE:

2.4.1.1802.11a:

Estándar ratificado en 1999, pero los equipos aparecieron hasta el 2001, Una de sus características es que llega a alcanzar velocidades de hasta 54 Mbps gracias a la utilización de OFDM (OrthogonalFrequencyDivisionMultiplexing), con 52 subportadoras, las velocidades que permite son 6, 9, 12, 18, 36, 48 y 54 Mbps.

2.4.1.2802.11b:

Estándar que fue ratificado en septiembre de 1999, y ha sido el estándar más utilizado en las redes WLAN, 802.11b extiende el uso del **DSSS**hasta obtener velocidades máximas de transmisión de datos de 11Mbps, únicamente utiliza modulación DSSS en la capa de enlace y CCK (ComplementaryCodeKeying) en la capa física, las 4 velocidades disponibles de transmisión son 1, 2, 5.5 y 11 Mbps y funciona con una frecuencia de 2.4Ghz

2.4.1.3802.11g:

Estándar ratificado en el año 2003, garantiza la compatibilidad con los dispositivos IEEE 802.11b y ofrece unas velocidades de hasta 54Mbps al igual que el estándar 802.11a, funciona con frecuencias de 2.4GHz con modulaciones DSSS y OFDM. El esquema de modulación es CCK.

2.4.1.4802.11n:

Este estándar es una propuesta de mejorar el estándar 802.11b, su principal objetivo es ofrecer una mayor velocidad de transmisión en redes WLAN, con un objetivo inicial de alcanzar los 100Mbps, pero este en la actualidad puede alcanzar hasta los 600Mbps, este estándar utiliza tecnología MIMO (Multiple-Input Multiple-Output), es una tecnología que usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema, permitiendo manejar más información (cuidando la coherencia) que al utilizar una sola antena. Dos beneficios importantes que provee a 802.11n, son la diversidad de antenas y el multiplexado espacial.

La tecnología MIMO depende de señales "multiruta". Las señales multiruta son señales reflejadas que llegan al receptor un tiempo después de que la señal de línea de visión (line of sight, LOS) ha sido recibida. En una red no basada en MIMO, como son las redes 802.11a/b/g, las señales multiruta son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales "multirutas" para incrementar la habilidad de un receptor de recobrar los mensajes de la señal.

Otra habilidad que provee MIMO es el Multiplexado de División Espacial (SDM). SDM multiplexa espacialmente múltiples flujos de datos independientes, transferidossimultáneamente con un canal espectral de ancho de banda. SDM puede incrementar significativamente el desempeño de la transmisión conforme el número de flujos espaciales es incrementado. Cada flujo espacial requiere una antena discreta tanto en el transmisor como el receptor. Además, la tecnología MIMO requiere una cadena de radio frecuencia separada y un convertidor de analógico a digital para cada antena MIMO lo cual incrementa el costo de implantación comparado con sistemas sin MIMO.

2.4.2 ESTANDARES DE OPTIMIZACIÓN:

2.4.2.1 802.11c:
Este estándar provee la información necesaria para asegurar el correcto funcionamiento de las operaciones en modo **bridge**de los dispositivos inalámbricos.

2.4.2.2 802.11d:
Define los requisitos de nivel físico necesarios para extender las redes 802.11. Permite a los puntos de acceso comunicar información sobre los canales radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios. Sus especificaciones son especialmente importantes en la banda de 5Ghz ya que la utilización de la banda de esta frecuencia varía sustancialmente entre países.

2.4.2.3 802.11e:
Su objetivo es proporcionar QoS(Calidad de servicio) en redes WLAN, es un estándar que realiza modificaciones en el subnivel MAC de la capa de enlace, y es de aplicación a los estándares físicos IEEE 802.11 a, b y g. La finalidad es proporcionar clases de servicio con niveles gestionados de QoS para aplicaciones de datos para aplicaciones de datos, voz y video.

2.4.2.4 802.11f:
Nace con el objetivo de lograr la interoperabilidad de puntos de acceso 802.11b/g dentro de una red WLAN con puntos de acceso de diferentes fabricantes dentro de la misma red. El estándar define un protocolo para la comunicación entre puntos de acceso que permite la trasferencia de usuarios entre puntos de acceso. El protocolo IAPP (Inter Access Point Protocol) es el encargado de transferir la información del contexto para permitir el traspaso de usuarios entre puntos de acceso.

2.4.2.5 802.11h:
El principal objetivo de este estándar es cumplir con los reglamentos europeos para las redes WLAN que emplean la banda de frecuencias de 5 Ghz, y que, por lo tanto es compatible con el estándar 802.11a. Los reglamentos europeos de radiocomunicaciones para la banda de 5Ghz, requiere que los productos tengan control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TCP limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas.

2.4.2.6 802.11i:
Se centra en cubrir aspectos de seguridad en redes WLAN basadas en alguno de los estándares 802.11a, b y g, ofrece nuevos métodos de cifrado y procedimientos de autenticación en el mecanismo WEP

2.4.2.7 802.11j:
Es la mejora del estándar 802.11 para operar en Japón en las bandas de 4.9 y 5 Ghz, permite adaptarse a la regulación de Japón sobre el modo de operación, la velocidad de transmisión, la potencia radiada, la emisión de espúreos y la escucha del medio inalámbrico.

2.4.2.8 802.11k:
Complemento del estándar IEEE802.11 para permitir la gestión de recursos radio en las redes WLAN. La gestión óptima de los recursos radio implica que el punto de acceso descubra de antemano los siguientes parámetros:

- Los puntos de acceso vecinos.
- La distancia a la que se encuentra el usuario que está conectado a los puntos de acceso vecinos.
- La carga de tráfico de los puntos de acceso vecinos.

2.4.2.9 802.11p:
Este estándar opera en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

2.4.2.10802.11r:
También se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función, que una vez enunciada parece obvia e indispensable en un sistema de datos inalámbricos, permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

2.4.2.11802.11v:
IEEE 802.11v servirá para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías: mecanismos de ahorro de energía con dispositivos de mano VoIPWi-Fi en mente; posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación; temporización, para soportar aplicaciones que requieren un calibrado muy preciso; y coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

2.4.2.12802.11w:

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

2.5 ARQUITECTURA (COMPONENTES FÍSICOS)

La arquitectura del IEEE 802.11 está formada por una serie de elementos que interactúan para proveer movilidad a las estaciones en una red local de acceso, que sea transparente a las capas superiores. El elemento básico de las redes de acceso definido en el estándar es la estación (STA en el estándar), definida como cualquier elemento que contenga una capa de Control de Acceso al Medio (MAC) y una capa Física (PHY) acorde con lo definido en el estándar. Las estaciones pueden ser móviles, portátiles o estacionarias. En las LAN´s inalámbricas basadas en el IEEE 802.11 se pueden diferenciar dos tipos de elementos habituales, la estación wireless o tarjeta de red inalámbrica (llamada NIC o simplemente STA) y el punto de acceso (AP en sus siglas en inglés Access Point). Los dos elementos son STA´s en la estricta definición del término, pero el AP es un dispositivo con funcionalidad añadida ya que incluye una interfaz de red adicional normalmente conectada con una red de cable como Ethernet.

CAPITULO 3 SEGURIDAD DE LAS WLAN

Los mecanismos de seguridad de una red WLAN que se pueden aplicar son diversos, estos actúan en diferentes capas del modelo OSI, las cuales son la capa de enlace, capa de red, capa de transporte y la capa de aplicación, a continuación se describen cada una de las capas.

3.1 SEGURIDAD A NIVEL DE ENLACE

La seguridad en las redes WLAN puede ser comprometida en dos aspectos: autenticación y cifrados. Los mecanismos de autenticación se emplean para identificar un usuario inalámbrico ante un punto de acceso y viceversa, mientras que los mecanismos de cifrado aseguran que no sea posible decodificar el número de usuario.

Los protocolos de seguridad para redes WLAN deben proteger estos dos puntos vulnerables ante posibles ataques.

3.1.1 PPTP

Este protocolo es una extensión de PPP desarrollada en modo propietario por Microsoft y normalizado por la IETF como RFC 2637 que puede ser utilizada para la creación de una red privada virtual o una VPN, una VPN permite conectar de forma segura a las empresas con oficinas de su misma organización, empleados a distancia, personas con móviles, proveedores, etc. Empleando recursos de red no dedicados, por lo tanto una VPN es una red que tiene la apariencia y muchas ventajas de un enlace dedicado, pero trabaja sobre una red pública.

Con este propósito se emplea una técnica llamada "tunneling", los paquetes de datos son enrutados por una red pública, internet u otra red comercial en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de una misma infraestructura.

La principal ventaja de PPTP es que es fácil y no muy costoso de implementar, reduce o elimina la necesidad del uso de sofisticados y caros equipos de telecomunicaciones para permitir las conexiones de equipos portátiles y remotos.

3.1.2 L2TP

L2TP (LayerTwoTunnelingProtocol) es una extensión del protocolo PPP que permite la creación de túneles VPN a nivel de enlace de datos (Capa 2 de modelo OSI). L2TP reúne las mejores características de otros dos protocolos de tunelización (PPTP de Microsoft y L2F de Cisco).

Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de internet a un sitio destino. Sin embargo, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de equipamiento tales como X.25, FrameRelay Y ATM.

Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar protocolos aparte de **IP**, tales como **IPX** y **NET BEUI.**

Por otro lado puesto que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación nativos de PPP como **PAP** y **CHAP.**

Los dos principales componentes de L2TP son el LAC (L2TP Access Concentrator), que físicamente termina las llamadas y el LNS (L2TP Network Server) que se encarga de la autenticación. Como en el caso de PPTP, L2TP necesita que los "routers" soporten el protocolo. Al contrario que PPTP, L2TP no depende de las tecnologías de cifrado específicas del fabricante para ofrecer una implementación completamente segura y correcta.

3.1.3 WEP

WEP (Wired Equivalent Privacy) es un protocolo cifrado a nivel de enlace contenido en la especificación original del estándar IEEE 802.11. WEP permite cifrar los datos que se transfieren a través de una red inalámbrica y autenticar los dispositivos móviles que se conectan a sus puntos de acceso.

En una red WLAN en la que se emplea WEP el usuario y el punto de acceso deben de establecer una relación antes de poder intercambiar datos la cual se puede encontrar en 3 estados diferentes:

- Sin autenticación y desasociado.
- Con autenticación y desasociado.
- Con autenticación y asociado.

El punto de acceso transmite tramas con señales de gestión en periodos de tiempo regulares. Las estaciones inalámbricas reciben estas tramas e inician la autenticación mediante el envío de una trama de autenticación. Una vez realizada satisfactoriamente la autenticación, la estación inalámbrica envía la trama asociada y el AP responde con otra trama asociada.

A continuación se presenta este procedimiento en la Figura 3.1.3.1:

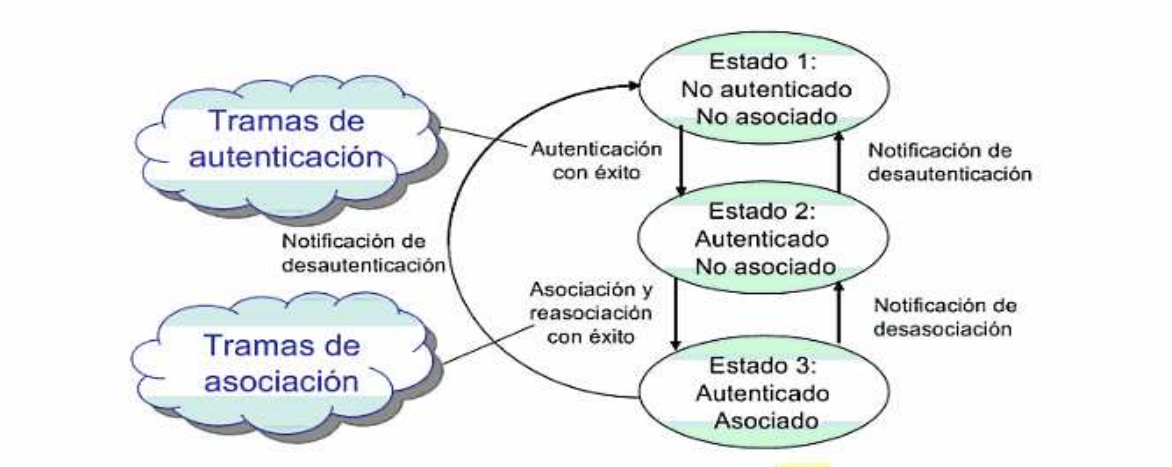

Figura 3.1.3.1 Autenticación WEP

En la autenticación WEP, el punto de acceso queda configurado con una clave, de forma que solo los dispositivos de usuario que intenten asociarse al él usando esta clave, pueda hacerlo.

Existen dos modos de autenticación WEP:

- *Open Key Autentication:* Es el modo de autenticación por defecto. Es un proceso de autenticación nulo en el que se autentica a todo aquel que pide ser autenticado y nunca se comprueba la clave WEP. A pesar de que se pueda completar el proceso de autenticación y asociación entre el usuario y el punto de acceso, no se va a enviar ningún paquete de datos entre ambos si el usuario no conoce la clave WEP correcta, ya que faltará el proceso de descifrado.

- *Shared Key Autentication:*En este caso, el punto de acceso envía al usuario un paquete de texto de invitación que el usuario ah de cifrar con la clave WEP correcta y devolvérsela al punto de acceso.(Figura 3.1.3.2) Si el usuario no dispone de la clave correcta, la clave de autenticación falla.

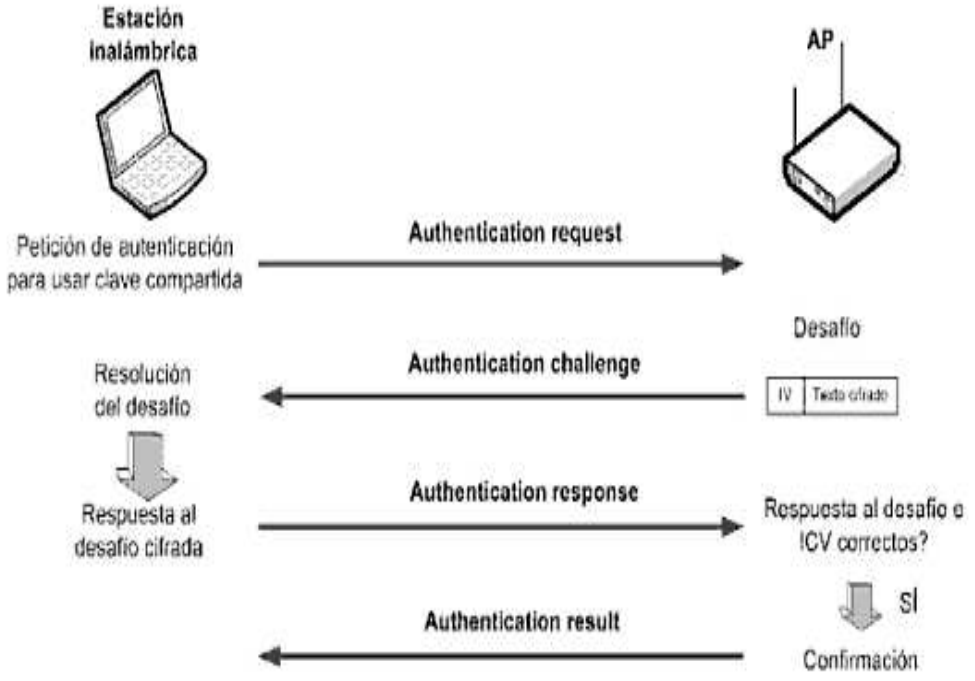

Figura 3.1.3.2 Procedimientos de la Autenticación WEP

La autenticación Shared Key es más insegura que la Open Key, ya que cualquier intruso que consiga detectar el paquete de desafío (AuthenticationChallenge) y el mismo paquete cifrado con la clave compartida (Autentication Response) es capaz de generar la respuesta a cualquier desafío a pesar de desconocer la clave, es decir, puede autenticarse en la red, y descifrar la clave WEP de un modo más sencillo por lo que no es muy recomendable su uso.

El estándar WEP de 64 bits usa una llave de 40 bits (también conocido como WEP-40), Al tiempo que el estándar WEP original estaba siendo diseñado, llegaron de parte del gobierno

de los Estados Unidos una serie de restricciones en torno a la tecnología criptográfica, limitando el tamaño de clave. Una vez que las restricciones fueron levantadas, todos los principales fabricantes poco a poco fueron implementando un protocolo WEP extendido de 128 bits usando un tamaño de clave de 104 bits (WEP-104).

Una clave WEP de 128 bits consiste casi siempre en una cadena de 26 caracteres hexadecimales (0-9, a-f) introducidos por el usuario. Cada carácter representa 4 bits de la clave.

3.1.4 WPA

Es un estándar que opera a nivel MAC y está basado en un borrador del estándar IEEE802.11i. Los principales aspectos que se intentan optimizar mediante el uso de WPA son el proceso de autentificación y cifrado.

Las principales características de WPA son:

- Distribución dinámica de claves.
- Mejora la confidencialidad.
- Nuevas técnicas de integridad y autenticación.
- Actualización de equipamiento radio a WPA mediante software.

En cuanto a la autenticación, en WPA es posible emplear dos modos de autenticación diferentes:

- Entornos personales: Es posible emplear WPA con clave pre compartida o WPA_PSK. En estos casos WPA se ejecuta en un modo especial conocido como "home mode" o PSK (Pre-Shared Key) que permite la utilización de claves configuradas manualmente y facilitar así el proceso de configuración al usuario. El usuario únicamente debe incluir unapalabra de entre 8 y 63 caracteres, conocida como clave maestra en un punto de acceso, así como en cada uno de los dispositivos que se desean conectar a la red WLAN. De esta forma la clave permite, en primer lugar, conectarse a la red únicamente a aquellos dispositivos con la clave adecuada, lo que evita ataques basados en escuchas así como el acceso de usuarios no autorizados y en segundo lugar, la contraseña provee una relación de acuerdo único para generar el cifrado **TKIP**en la red.

- Entornos empresariales: aquí los requerimientos estrictos de cifrado y autenticación hacen que sea más adecuada la utilización de WPA con los mecanismos **IEEE**

802.1x y el protocolo de autenticación extensible (EAP), que disponen de procedimientos de gestión de claves dinámicamente. WPA utiliza el estándar IEEE802.1x y EAP, EAP se emplea como trasporte de extremo a extremo para los métodos de autenticación entre el dispositivo de usuario y los puntos de acceso, mientras que IEEE802.1x define como enviar EAP sobre la red. El conjunto de estos dos mecanismos junto con el esquema de cifrado forman una fuerte estructura de autenticación.

3.1.5 WPA2

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.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (AdvancedEncryption Standard).

WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 les dan a los gerentes de TI la seguridad que la tecnología cumple con estándares de interoperabilidad.

WPA2 Y IEEE802.11i se diferencian principalmente en dos aspectos:

- Se diferencian en su interoperabilidad con WPA. Si la migración no es una preocupación entonces WPA2 funciona según lo definido por IEEE 802.11i.
- WPA y WPA2 están preparados para su utilización en entornos empresariales, pero carecen de ciertos aspectos con los que cuenta IEEE 802.11i para proporcionar servicios de voz inalámbricos, como prevenir la latencia de señal o la perdida de información durante el **roaming.**

3.2 SEGURIDAD A NIVEL DE RED

3.2.1 IPsec VPN

Es conocido como el mecanismo de seguridad más robusto, para este propósito utiliza una técnica llamada "**tunneling**", de tal forma que los paquetes de datos son enrutados por la red pública (Internet u otra red comercial), en un túnel privado se simula una conexión

punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura.

Básicamente se utilizan dos protocolos en IPSec, llamados AuthenticationHeader(AH) y Encapsulating Security Payload(ESP). Ambos se identifican en el campo de protocolo del encabezado IP.AH, provee autenticación del paquete IP completo, (incluido todo lo que es posible de su encabezado), así como a los protocolos de capas superiores. ESP, por su parte solo encripta y autentica el "Payload" del paquete. Se puede opcionalmente encriptar y/o autenticar el paquete, pero al menos una de ambas acciones debe ser ejecutada. Es también posible el uso combinado de AH + ESP, lo que otorga una máxima cobertura en cuanto a Encriptación y Autenticación. Si bien se hace una doble autenticación, (lo cual resulta redundante y genera overhead), resulta un esquema muy utilizado.

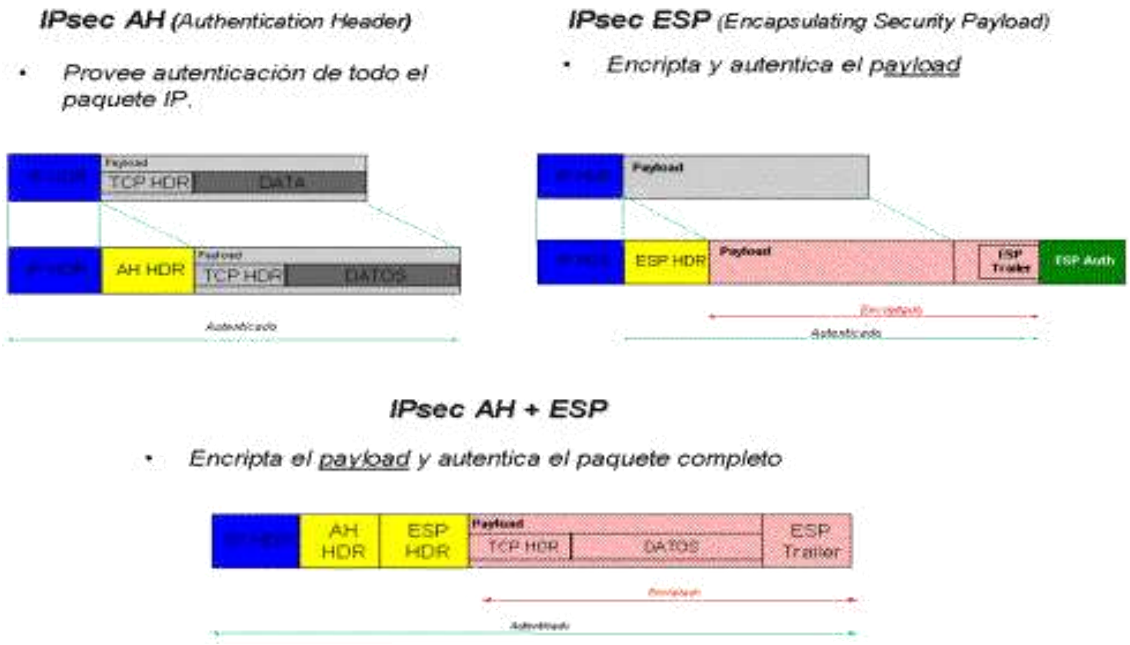

Figura 3.2.1.1 Encabezado IPSec

3.3 SEGURIDAD A NIVEL DE TRANSPORTE

3.3.1 SSL/TLS

SSL (Secure Sockets Layer) traducido al español significa Capa de Conexiones Seguras. Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet. Recientemente ha sido sustituido por TLS (TransportLayer Security) el cual está basado en SSL y son totalmente compatibles.

Nos permite confiar información personal a sitios web, ya que tus datos se ocultan a través de métodos criptográficos mientras se navega en sitios seguros.

Es utilizado ampliamente en bancos, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas. No todos los sitios web usan SSL.

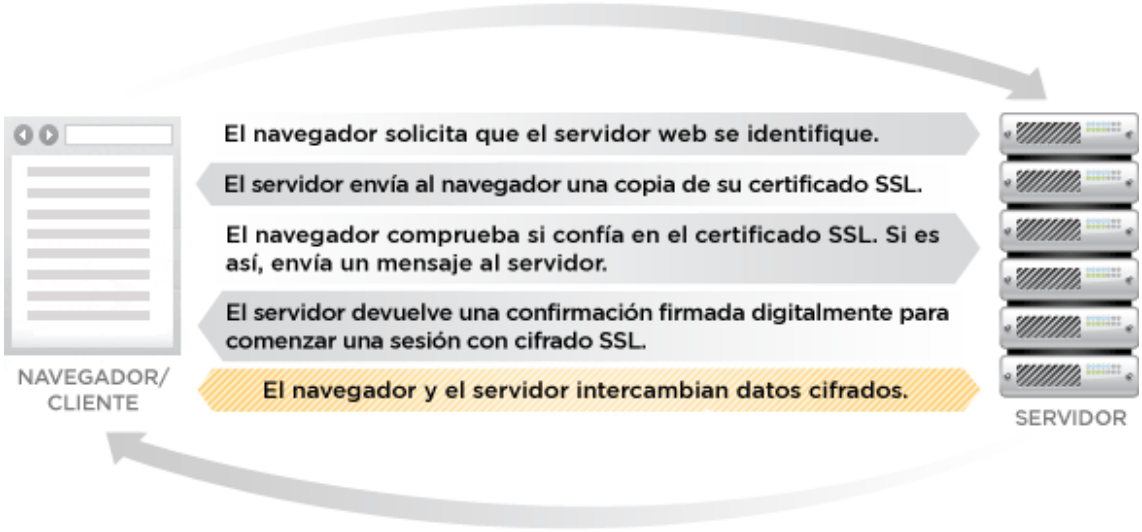

Figura 3.3.1.1 Procedimiento SSL

3.3.2 SSL VPN

En los últimos años se han implementado las VPN´s basadas en el protocolo SSL. Mediante estas soluciones es posible el acceso a aplicaciones Web, aplicaciones usuario / servidor y aplicaciones con ficheros compartidos a través de un **Gateway** SSL VPN que ejerce de **proxy.**

Las SSL VPN aportan ventajas notables respecto a las IPSec VPN, aunque también implican complejidades y consideraciones a tener en cuenta. La ventaja más notable que implementan las SSL VPN es que no es necesario tener instalado ningún usuario en el terminal de usuario, lo único que se necesita es disponer de un navegador web en la terminal del usuario y de una puerta de enlace VPN SSL en la red corporativa, también ofrece otras ventajas:

- Mecanismos para proteger a sus usuarios web en acceso remoto de diversos dispositivos y comunicaciones en Internet entre firewalls y routers.
- Sesiones seguras en computadoras personales y públicas, terminales de mano móviles y dispositivos de negocios.
- Las mismas capacidades y ventajas de un costoso sistema de propiedad de redes a un precio mucho menor para las Organizaciones.

- Acceso seguro a recursos de red, desde el hogar, computadoras públicas en los hoteles, centros de negocioso o cualquier lugar del mundo; eliminando amenazas de fraude y peligros como el software malicioso (malware).

- Facilidad de instalación en los navegadores web estándar y no requiere la instalación de software especializado en los equipos de los usuarios finales.

3.4 SEGURIDAD A NIVEL DE APLICACIÓN

3.4.1 SSH

Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como **telnet** o **rsh**. Un programa relacionado, el **scp**, reemplaza otros programas diseñados para copiar archivos entre hosts como **rcp**. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
- Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

3.4.2 HTTPS

Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.El puerto estándar para este protocolo es el 443.

CAPITULO 4 IMPLANTACION DE UNA WLAN

4.1 FACTORES

Son varios factores los que se deben de considerar al momento de implantar una red wlan, algunos de los aspectos que se deben de tener en cuenta son los siguientes:

- Cobertura.

  La distancia que pueden alcanzar las ondas de radiofrecuencia es función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con los objetos, paredes, metales, o incluso la gente afectan a la propagación de las ondas, la mayor parte de los sistemas de redes inalámbricas utilizan ondas de radiofrecuencia por que pueden penetrar la mayor parte de lugares cerrados y obstáculos. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando varios puntos de acceso que permitan navegar por la red.

- Rendimiento.

  Depende de la puesta a punto de los dispositivos así como el número de usuarios, de los factores de propagación y del tipo de sistema inalámbrico utilizado. Igualmente depende del retardo y de los cuellos de botella de la parte cableada de la red.

- Compatibilidad con redes existentes.

  La mayor parte de las redes inalámbricas proporcionan un estándar de interconexión con redes cableadas como Ethernet. Los nodos de la red inalámbrica son soportados por el sistema de la red de la misma manera que cualquier otro nodo de una red LAN.

- Interoperabilidad de los dispositivos inalámbricos dentro de la red

  Los consumidores deben de estar consientes de que los sistemas inalámbricos de redes LAN de distintas marcas podrían no ser compatibles para operar juntos cuyas razones pueden ser:

  1.- Diferentes tecnologías no interoperan. Un sistema basado en la tecnología de frecuencia esperada (FHSS), no comunicará con otro basado en tecnología de secuencia directa (DSSS).

  2.- Sistemas que utilizan distinta banda de frecuencias no podrán comunicar aunque utilicen la misma tecnología.

  3.- Aun utilizando igual tecnología y banda de frecuencias ambos vendedores, los sistemas de cada uno no comunicarán debido a diferencias de implementación de cada fabricante.

- Interferencia y coexistencia

  La naturaleza en que se basan las redes inalámbricas implica que cualquier otro producto que transmita energía a la misma frecuencia puede potencialmente dar cierto grado de interferencia en un sistema LAN inalámbrico. Por ejemplo los hornos de microondas, otro problema es la colocación de varias redes inalámbricas en lugares próximos.

- Simplicidad y facilidad de uso

  Los usuarios necesitan muy poca información a añadir para utilizar una LAN inalámbrica. Esto es así por que la naturaleza inalámbrica de la red es transparente al usuario, las aplicaciones trabajan de igual manera que lo podrían hacer en una red cableada. Los productos WLAN incorporan herramientas de diagnóstico para dirigir los problemas asociados a los elementos inalámbricos de un sistema. Sin embargo, los productos están diseñados para que los usuarios rara vez tengan que usar estas herramientas.

  Las WLAN simplifican muchos problemas de instalación y configuración que atormentan a los administradores de la red. Ya que únicamente los puntos de acceso WLAN necesitan cable, y ya no es necesario llevar cables hasta el usuario final. La falta de cable hace también que los cambios, extensiones y desplazamientos sean operaciones triviales en una red inalámbrica.

- Seguridad en la comunicación

  Normalmente se suministran elementos de seguridad dentro de la WLAN complejas técnicas de encriptado hacen imposible para todos acceder de forma no

autorizada al tráfico de la red. En general los nodos individuales deben tener habilitada la seguridad antes de poder participar en el tráfico de la red.

4.2 VENTAJAS

Algunas ventajas que ofrecen las redes inalámbricas son:

- Estar basada en estándares y contar con certificación Wi-Fi:

  Wi-Fi es un robusto estándar de redes, comprobado a nivel de la industria de transmisión de datos, que asegura que los productos inalámbricos interoperarán con otros productos certificados de Wi-Fi de otros fabricantes de redes. Con un sistema basado en Wi-Fi, los usuarios gozarán de compatibilidad con el mayor número de productos inalámbricos y evitarán los altos costos y la selección limitada de las soluciones patentados por un sólo fabricante. Además, la selección de una solución inalámbrica basada en estándares, que sea totalmente ínter operable con redes Ethernet y Fast Ethernet, le permitirá al usuario que su red inalámbrica trabaje sin interrupciones con su sistema existente de LAN tradicional.

- Instalación simple:

  La solución inalámbrica debe ser del tipo plug and play; tomando solamente unos minutos para su instalación. Al conectarla, los usuarios empezarán a gozar de inmediato de los servicios en red. Para obtener una instalación aún más fácil, su solución deberá soportar el protocolo denominado Dynamic Host ConfigurationProtocol (DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos. En lugar de instalar un servidor DHCP en algún aparato independiente para obtener esta capacidad de ahorro de tiempo, los usuarios deben seleccionar hubs inalámbricos que ofrezcan servidores DHCP incorporados.

  Si un usuario está agregando un sistema inalámbrico a su red Ethernet, sería una buena opción potenciar un punto de acceso a través de cables estándares de Ethernet; esto le permitirá hacer que el punto de acceso funcione utilizando un voltaje bajo de corriente en el mismo cable que es usado para transmitir datos: eliminando la necesidad de tener una toma de poder local y un cable para cada dispositivo de puntos de acceso.

  Una WLAN es rápida, fácil y elimina la necesidad de tirar cables a través de paredes y techos, permitiendo a la red llegar a puntos de difícil acceso para una LAN cableada.

- Robusta y confiable.

  Considera soluciones inalámbricas robustas que tienen alcances de por lo menos 100 metros. Estos sistemas les ofrecerán a los empleados de una compañía una considerable movilidad dentro sus instalaciones. Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el punto de acceso y las PC cards. Para garantizar una conectividada las velocidades más rápidas posibles incluyendo largo alcance o ambientes ruidosos el usuario debe asegurarse que su nuevo sistema pueda hacer cambios dinámicos de velocidades, basándose en las diferentes intensidades de señal y distancias del punto de acceso. Además, el usuario debe seleccionar PC cards inalámbricas para computadoras portátiles que ofrezcan antenas retractables para prevenir rupturas durante la movilización de los aparatos.

- Escalabilidad.

  Un buen punto de acceso inalámbrico deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red. Las impresoras u otros dispositivos periféricos que no puedan conectarse en red tradicional, se conectan a su red inalámbrica con un adaptador USB inalámbrico o un Ethernet Client Bridge.

- Facilidad de uso.

  Si un usuario planea conectar múltiples puntos de acceso inalámbricos a una red existente de cables, debe considerar una solución que ofrezca conexiones automáticas a la red. Cuando un usuario se desplace fuera de los límites de un Access point al campo de otro, una capacidad automática de conexión a la red transferirá sus comunicaciones sin interrupciones- al siguiente aparato, aún al cruzar límites de routers, sin siquiera tener que reconfigurar la dirección IP manualmente. Esto resulta ser especialmente útil para aquellas compañías con múltiples instalaciones que están conectadas por medio de una red de área amplia (WAN). Como resultado, los usuarios podrán movilizarse libremente dentro de sus instalaciones y más allá- y permanecer conectados a la red.

- Seguridad.

  Si un usuario escoge una solución inalámbrica que ofrezca múltiples niveles de seguridad, incluyendo encriptación y autenticación de usuarios. Una solución segura es utilizar una encriptación de por lo menos 40 bits. Sin embargo, para su facilidad de uso y para una protección más fuerte, se debe seleccionar una solución superior que automáticamente genere una clave nueva de 128 bits para cada sesión de red

inalámbrica, sin tener que ingresar la clave manualmente. Además, el usuario debe considerar un sistema que ofrezca autenticación del usuario, requiriendo que los trabajadores presenten una contraseña antes de acceder la red.

- Costo de propiedad reducido.

  Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida pueden ser significativamente inferiores, ya que en ambientes dinámicos se requieren acciones y movimientos frecuentes, lo cual abarata los costos debido a que no hay instalaciones físicas.

- Fácil configuración para el usuario.

  La persona que se va a conectar a la red sólo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red está abierta no es necesario configurar nada, pues la tarjeta detecta la red automáticamente.

4.3 DESVENTAJAS

Los inconvenientes o desventajas que tienen las redes de este tipo se derivan fundamentalmente de encontrarnos en un periodo transitorio de introducción, donde faltan estándares que permitan trasmisiones más rápidas, por otro lado hay dudas de que algunos sistemas pueden llegar a afectar a la salud de los usuarios, también no está clara la obtención de licencias para las que utilizan el espectro radioeléctrico y son muy pocas las que presentan compatibilidad con los estándares de las redes fijas, sin embargo, se ha estado trabajando en ello, logrando hasta el momento un gran avance que ha permitido la implementación cada vez más de este tipo de comunicación.

Algunas desventajas que se derivan por la implementación de redes inalámbricas son las que se mencionan a continuación:

- Interferencias:

  Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, también puede ser por redes inalámbricas cercanas o incluso por otros equipos conectados inalámbricamente a la misma red.

- Velocidad:

  Las redes cableadas alcanzan la velocidad de 100 Mbps, mientras que las redes inalámbricas alcanzan cuando mucho 54 Mbps.

- Seguridad:

  En una red cableada es necesario tener acceso al medio que transmite la información mientras que en la red inalámbrica el medio de transmisión es el aire.

4.4 COMO INSTALAR UNA WLAN PEQUEÑA

Paso 1.- Instalación deseada.

Lo que se pretende es instalar una WLAN que ahorre tiempo dinero y esfuerzo a los empleados y administrativos de una empresa pequeña, se requiere conectar varios nodos entre si dentro de una empresa.

Paso 2.- Material Necesario.

La mejor configuración es partir de una conexión **ADSL** con router, aunque también podremos montar una red Wi-Fi en nuestra empresa a partir de otras configuraciones (cable, etc.).
Si ya contamos con esto, necesitaremos además:

- Puntos de Acceso Wi-Fi, Es el accesorio adicional que usaremos para incoporar el estándar 802.11 a nuestro equipo (PDA, ordenador portátil o de sobremesa).

Figura 4.4.1 Access Point

El alcance de la señal de nuestra red Wi-Fi dependerá de:

- La potencia del Punto de Acceso.
- La potencia del accesorio o dispositivo Wi-Fi por el que nos conectamos.

- Los obstáculos que la señal tenga que atravesar (muros o metal).

Cuanto más lejos (linealmente) se quiera llegar, más alto se deberá colocar el Punto de Acceso. Muchos de los actuales Puntos de Acceso vienen preparados para poderlos colgar en la pared.

Los rebotes en las esquinas suelen ser negativos para un buen funcionamiento, por esto intenta evitar poner las Antenas ó Puntos de Acceso en esquinas ó a poca altura.

Si se quiere llegar lejos, se debe evitar también interferencias como microondas o teléfonos inalámbricos.

- Si nuestra PC o portátil no incluye Wi-Fi, necesitaremos un accesorio que nos de este tipo de conectividad, a continuación se muestran algunos dispositivos en la figura 4.4.2

Figura 4.4.2 Dispositivos Wi-Fi

Paso 3. Configuración del Access point

Los parámetros básicos que se deben de configurar en un Access point son los siguientes:

- Default Channel (1 a 13): Dejar el de por default, (En la configuración de la red inalámbrica de la PC se explica a detalle), si se tienen instalados más puntos de acceso en la empresa, es importante configurar a cada uno de ellos con distintos canales para evitar problemas de conexión de dispositivos en la red.
- ESSID: Nombre a dar a nuestra red inalámbrica, generalmente debajo del router está el ESSID por defecto de fábrica, es igual al de la pantalla.
- HideSSID: El valor es “true” o “false”, en la primera fase de la instalación ponerlo a false, para poder ver el nombre de la red inalámbrica cuando configuremos nuestros ordenadores en la red LAN.

- Ahora viene lo más importante y es el tipo de política (WEP, WPA), autorización y encriptación de nuestra red inalámbrica para así poder evitar posibles intrusos que quieran entran a nuestro router. Elegimos una de ellas y solamente una, no se

pueden elegir varias a la vez. Una vez conectados todos nuestros Ordenadores al router, cambiar la política a WPA-PSK, si por algún motivo no se conecta una computadora al introducir la clave, el dispositivo no admite dicha política de encriptación, se deberá cambiar a WEP 128bit con clave de muchos dígitos.La política WEP 64bit y WEP 128bit es la más utilizada por ser soportada por todos los dispositivos WIRELESS.

Un ejemplo de ello se muestra en la Figura 4.4.3

Figura 4.4.3 Consola de configuración de un Access point

Paso 4. Configuración de los equipos

En este paso se configuran los parámetros de red que deben de configurarse en cada uno de los equipos para poder tener acceso a internet o a la misma red inalámbrica.

Esto se puede hacer mediante dos formas:

- Asignar conexión a la red inalámbrica mediante servidor DHCP:
  Esta sería la manera más sencilla, ya que no tendríamos que programarle una dirección IP a nuestros dispositivos y se conectarían al Access point de una forma aleatoria, aunque la desventaja seria en que la dirección que asigna este servidor es de manera aleatoria y su administración se hace más complicada.

- Asignar conexión a la red inalámbrica mediante direcciones IP estáticas:
  Esta sería la formamás correcta debido a que nos facilita la administración de nuestra red, y de esta forma ya sabemos qué dirección IP se le asigna a cada uno de

nuestros equipos de computo, y el proceso de conexión es más rápido ya que se omite el proceso de asignación de dirección de forma aleatoria.

4.5 MANTENIMIENTO

Las principales son:

Entorno radio.

Es un área que es exclusiva de entornos inalámbricos y que no existe en redes cableadas. Comprende los problemas que generan las interferencias entre celdas de la propia red o con otras redes, perturbaciones radioeléctricas de otros aparatos(hornos de microondas, radares, celulares) y redes de otras tecnologías (bluetooth, telefonía inalámbrica domestica, repetidores TV en el hogar).

Equipamiento.

Puntos de acceso, antenas, cableado requieren de un cuidado normal. Nuevas actualizaciones de firmware o drivers deberán ser realizadas cuando el experto lo aconseje. En el caso de instalaciones exteriores, se debe tener en cuenta la degradación de los equipos por las inclemencias del tiempo y los casos de robos y vandalismos, lo cual suele afectar sobre todo a antenas, cableado y puntos de acceso.

Seguridad.

Periódicamente es necesario cambiar las claves si son estáticas; las altas, bajas y modificaciones de usuarios, las direcciones **MAC** también tendrán que declararse; las aplicaciones deberán de actualizarse para cerrar posibles agujeros de seguridad; analizar posibles intrusos.

Recomendaciones.

Para que el mantenimiento de una red no sea una tarea compleja y constante fuente de problemas, es aconsejable seguir las siguientes recomendaciones:

- Realizar un buen diseño inicial lo cual implica el estudio exhaustivo previo de posibles fuentes de interferencias externas (otras redes) e internas para minimizar su impacto; análisis de cobertura, potencia de señal y planificación de frecuencias para conseguir una buena recepción interna y reducir su emisión externa; estimaciones adecuadas de uso; etc.
- Acometer mantenimiento interno periódico para detectar degradaciones, saturación, intrusiones.

- Ejecutar la adecuada actualización de drivers y de firmware, reparaciones, análisis de las causas de interferencias o degradaciones detectadas planificación de escalabilidad.

Una red adecuadamente implantada y mantenida puede generar gran satisfacción a los usuarios, implementar la productividad y reducir costos, así como requerir de un mantenimiento bajo.

RESUMEN:

ASPECTOS BASICOS:

Una red es justamente un sistema de comunicación que se da entre distintos equipos para poder realizar una comunicación eficiente, rápida y precisa, para la transmisión de datos de una computadora a otra, existen dos modelos.

Modelo OSI

El modelo OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas se pueden resumir de la siguiente manera:

Capa Física

La capa física abarca los aspectos físicos de la red (cables, hub's, y el resto de dispositivos que conforman el entorno físico de la red).

Capa de Enlace de Datos

La principal tarea de la capa de enlace de datos es transformar un medio de transmisión puro en una línea que esté libre de errores de transmisión. Enmascara los errores reales, de manera que la capa de red no los vea.

Capa de Red

La capa de red controla la operación de subred. Su función es determinar cómo se encaminan los paquetes desde el origen hasta el destino.

Capa de transporte

La función básica de la capa de transporte es aceptar datos de la capa superior, dividirlos en unidades más pequeñas si es necesario.

Capa de Sesión

La capa de sesión es la encargada de establecerle enlace de comunicación o sesión entre dos computadoras.

Capa de Presentación

La capa de presentación se enfoca en la sintaxis y la semántica de la información transmitida.

Capa de Aplicación

La capa de aplicación contiene una variedad de protocolos que los usuarios necesitamos con frecuencia, uno de ellos es el HTTP (HyperText Transfer Protocol).

Modelo TCP/IP

Es un modelo de descripción de protocolos de res, Este modelo se utilizo en la más vieja de todas las redes de computadoras de área amplia (ARPANET) y su sucesora Internet.

TCP/IP tiene cuatro capas de abstracción

Capa 1 Acceso a la red: Controla los dispositivos del hardware y los medios que forman la red.
Capa 2 Internet: Determina la mejor ruta a través de la red
Capa 3 Transporte: Admite la comunicación entre distintos dispositivos de distintas redes.
Capa 4 Aplicación: Representa datos para el usuario más el control de codificación y de dialogo.

TOPOLOGIAS DE REDES:

Una red de área local está formada por varios equipos a los cuales les llamamos nodos y a las distintas formas de conectar los componentes de una red local se les llama topologías y esta define la estructura de una red.

Topología de bus: En las redes que tienen esta tecnología, todos los nodos de la red están conectados a un mismo canal de comunicaciones llamado bus que suele ser un cable coaxial.

Topología de anillo: En esta topología cada nodo está conectado a sus dos nodos adyacentes por enlaces punto a punto, formando un anillo cerrado o círculo por el cual viaja la información.

Topología de estrella: En esta topología existe un nodo central, enlazado directamente con todos los demás, que controla el tráfico de datos por la red, reenviando los datos a su destino.

Topología de árbol: La red en árbol es una topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.

Topología en malla: La topología de red mallada es una topología de red en la que cada nodo está conectado a todos los nodos.

REDES WLAN:

Es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas.

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado.

Topologías WLAN:

1.-BSS: es conocido como Conjunto de Servicios Básicos (BSS – Basic Service Set). También se conoce como Maestro y Cliente.

2.-IBSS: Es también conocido como *ad hoc,* es un método para que los clientes inalámbricos puedan establecer una comunicación directa entre sí. Al permitir que los clientes inalámbricos operen en modo *ad hoc*, no es necesario involucrar un punto de acceso central.

3.-EBSS: El modo EBSS está formado por un conjunto de BSS asociadas mediante un sistema de distribución formando una subred única. Esto permite una serie de prestaciones opcionales como el roaming entre celdas.

Estandar 802.11.

Define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

Estándares de capa física y enlace:

802.11a: Una de sus características es que llega a alcanzar velocidades de hasta 54 Mbps.

802.11b: Ha sido el estándar más utilizado en las redes WLAN, las 4 velocidades disponibles de transmisión son 1, 2, 5.5 y 11 Mbps y funciona con una frecuencia de 2.4Ghz.

802.11g: Ofrece unas velocidades de hasta 54Mbps, funciona con frecuencias de 2.4GHz.

802.11n: Su principal objetivo es ofrecer una mayor velocidad de transmisión en redes WLAN, con un objetivo inicial de alcanzar los 100Mbps, pero este en la actualidad puede alcanzar hasta los 600Mbps.

Estándares de optimización:

802.11c: provee la información necesaria para asegurar el correcto funcionamiento de las operaciones en modo bridgede los dispositivos inalámbricos.

802.11d: Define los requisitos de nivel físico necesarios para extender las redes 802.11.

802.11e: Su objetivo es proporcionar QoS (Calidad de servicio) en redes WLAN.

802.11f: Nace con el objetivo de lograr la interoperabilidad de puntos de acceso 802.11b/g dentro de una red WLAN con puntos de acceso de diferentes fabricantes dentro de la misma red.

802.11h: El principal objetivo de este estándar es cumplir con los reglamentos europeos para las redes WLAN que emplean la banda de frecuencias de 5 Ghz, y que, por lo tanto es compatible con el estándar 802.11a.

802.11i: Se centra en cubrir aspectos de seguridad en redes WLAN basadas en alguno de los estándares 802.11a, b y g.

802.11j: Es la mejora del estándar 802.11 para operar en Japón en las bandas de 4.9 y 5 Ghz.

802.11k: Complemento del estándar IEEE802.11 para permitir la gestión de recursos radio en las redes WLAN.

802.11p: Este estándar opera en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz, especialmente indicado para automóviles.

802.11r: También se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él.

802.11v: Servirá para permitir la configuración remota de los dispositivos cliente.

802.11w: servirá para permitir la configuración remota de los dispositivos cliente.

SEGURIDAD DE LAS WAN

Los mecanismos de seguridad de una red WLAN que se pueden aplicar son diversos, estos actúan en diferentes capas del modelo OSI

Seguridad a nivel de enlace.

PPTP: Este protocolo es una extensión de PPP desarrollada en modo propietario por Microsoft, que puede ser utilizada para la creación de una red privada virtual o una VPN.
L2TP: reúne las mejores características de otros dos protocolos de tunelización (PPTP de Microsoft y L2F de Cisco).

WEP: es un protocolo cifrado a nivel de enlace contenido en la especificación original del estándar IEEE 802.11
WPA: Es un estándar que opera a nivel MAC y está basado en un borrador del estándar IEEE802.11i.
WPA2: Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA.

Seguridad a nivel de red.

IPsec VPN: Es conocido como el mecanismo de seguridad más robusto, para este propósito utiliza una técnica llamada "tunneling", de tal forma que los paquetes de datos son enrutados por la red pública.

Seguridad a nivel de transporte.

*SSL/TLS:*Nos permite confiar información personal a sitios web, ya que tus datos se ocultan a través de métodos criptográficos mientras se navega en sitios seguros.
SSL VPN: La ventaja más notable que implementan las SSL VPN es que no es necesario tener instalado ningún usuario en el terminal de usuario, lo único que se necesita es disponer de un navegador web en la terminal del usuario y de una puerta de enlace.

Seguridad a nivel de aplicación.

SSH: Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.
HTTPS: Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP.

IMPLANTACION DE UNA RED WLAN

Son varios factores los que se deben de considerar al momento de implantar una red WLAN:

Cobertura: La distancia que pueden alcanzar las ondas de radiofrecuencia es función del diseño del producto y del camino de propagación, especialmente en lugares cerrados.

Rendimiento: Depende de la puesta a punto de los dispositivos así como el número de usuarios, de los factores de propagación y del tipo de sistema inalámbrico utilizado.

Compatibilidad con redes existentes: La mayor parte de las redes inalámbricas proporcionan un estándar de interconexión con redes cableadas como Ethernet.

Interoperabilidad de los dispositivos inalámbricos dentro de la red: Los consumidores deben de estar consientes de que los sistemas inalámbricos de redes LAN de distintas marcas podrían no ser compatibles.

Interferencia y coexistencia: La naturaleza en que se basan las redes inalámbricas implica que cualquier otro producto que transmita energía a la misma frecuencia puede potencialmente dar cierto grado de interferencia en un sistema LAN inalámbrico.

Simplicidad y facilidad de uso: Los usuarios necesitan muy poca información a añadir para utilizar una LAN inalámbrica.

Seguridad en la comunicación: Normalmente se suministran elementos de seguridad dentro de la WLAN complejas técnicas de encriptado hacen imposible para todos acceder de forma no autorizada al tráfico de la red.

VENTAJAS

Estar basada en estándares y contar con certificación Wi-Fi: que asegura que los productos inalámbricos ínter operaran con otros productos certificados de Wi-Fi de otros fabricantes de redes.

Instalación simple: Solamente requiere de unos minutos para su instalación. Al conectarla, los usuarios empezarán a gozar de inmediato de los servicios en red.

Robusta y confiable: Considera soluciones inalámbricas robustas que tienen alcances de por lo menos 100 metros. Estos sistemas les ofrecerán a los empleados de una compañía una considerable movilidad dentro sus instalaciones.

Escalabilidad: Un buen punto de acceso inalámbrico deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red.

Facilidad de uso: Si un usuario planea conectar múltiples puntos de acceso inalámbricos a una red existente de cables, debe considerar una solución que ofrezca conexiones automáticas a la red.

DESVENTAJAS

Algunas desventajas que se derivan por la implementación de redes inalámbricas son las que se mencionan a continuación:

Interferencias: Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, también puede ser por redes inalámbricas cercanas o incluso por otros equipos conectados inalámbricamente a la misma red.

Velocidad: Las redes cableadas alcanzan la velocidad de 100 Mbps, mientras que las redes inalámbricas alcanzan cuando mucho 54 Mbps.

Seguridad: En una red cableada es necesario tener acceso al medio que transmite la información mientras que en la red inalámbrica el medio de transmisión es el aire.

COMO INSTALAR UNA WLAN PEQUEÑA:

Paso 1.- Instalación deseada.

Lo que se pretende es instalar una WLAN que ahorre tiempo dinero y esfuerzo a los empleados y administrativos de una empresa pequeña, se requiere conectar varios nodos entre si dentro de una empresa.

Paso 2.- Material Necesario.

La mejor configuración es partir de una conexión ADSL con router, aunque también podremos montar una red Wi-Fi en nuestra empresa.

Cuanto más lejos (linealmente) se quiera llegar, más alto se deberá colocar el Punto de Acceso. Muchos de los actuales Puntos de Acceso vienen preparados para poderlos colgar en la pared.

Si nuestra PC o portátil no incluye Wi-Fi, necesitaremos un accesorio que nos de este tipo de conectividad.

Paso 3. Configuración del Access point

Los parámetros básicos que se deben de configurar en un Access point son los siguientes:

- *Default Channel*: si se tienen instalados más puntos de acceso en la empresa, es importante configurar a cada uno de ellos con distintos canales para evitar problemas de conexión de dispositivos en la red.
- *ESSID:*Nombre a dar a nuestra red inalámbrica.
- Configuración de la WEP o WPA

Paso 4. Configuración de los equipos

En este paso se configuran los parámetros de red que deben de configurarse en cada uno de los equipos para poder tener acceso a internet o a la misma red inalámbrica.

MANTENIMIENTO:

Las principales son:

Entorno radio.

Es un área que es exclusiva de entornos inalámbricos y que no existe en redes cableadas. Comprende los problemas que generan las interferencias entre celdas de la propia red o con otras redes.

Equipamiento.

Puntos de acceso, antenas, cableado requieren de un cuidado normal. Nuevas actualizaciones de firmware o drivers deberán ser realizadas cuando el experto lo aconseje.

Seguridad.

Periódicamente es necesario cambiar las claves si son estáticas; las altas, bajas y modificaciones de usuarios.

Recomendaciones.

Para que el mantenimiento de una red no sea una tarea compleja y constante fuente de problemas, es aconsejable seguir las siguientes recomendaciones:

- Realizar un buen diseño inicial lo cual implica el estudio exhaustivo previo de posibles fuentes de interferencias externas (otras redes) e internas para minimizar su impacto.
- Acometer mantenimiento interno periódico para detectar degradaciones, saturación, intrusiones.
- Ejecutar la adecuada actualización de drivers y de firmware, reparaciones, análisis de las causas de interferencias o degradaciones detectadas planificación de escalabilidad.

GLOSARIO:

- **Hub:** Dispositivo que permite centralizar el cableado de una red.
- **Bits:** Dígito del sistema binario.
- **NIC:** Tarjeta de Interfaz de red.
- **Token:** Cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación.
- **World Wide Web:** Red informática mundial
- **Ethernet:** Estándar de redes de área local para computadoras.
- **SSID:** (**S**ervice**S**et **ID**entifier)Nombre incluido en todos los paquetes de una red. Inalámbrica.
- **Gateway:** Equipo informático configurado para dotar a las máquinas de una red local.
- **Roaming:** Capacidad de un dispositivo para moverse de una zona de cobertura a otra.
- **AP:** dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red.
- **CSMA/CA**:Protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión.
- **DSSS:** Es uno de los métodos de codificación de canal (previa a la modulación) en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan.
- **Bridge:** dispositivo de interconexión de redes de computadoras que opera en la capa 2 del modelo OSI.
- **IP:**Protocolo de Internet.
- **IPX:**Protocolo Intercambio de Paquetes Entre Redes.
- **NET BEUI:** protocolo utilizado por las antiguas redes basadas en Microsoft LAN.
- **PAP: (**PasswordAuthenticationProtocol). protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet.
- **CHAP:** (ChallengeHandshakeAuthenticationProtocol) protocolo de autenticación por desafío mutuo.
- **TKIP:** (**T**emporal **K**ey **I**ntegrity**P**rotocol) mejorar el cifrado de datos inalámbricos.
- **IEEE 802.1x:**Norma del IEEE para el control de acceso a red basada en puertos.
- **Tunneling:** consiste en encapsular un protocolo de red sobre otro.
- **Proxy:**Es un programa o dispositivo que realiza una acción en representación de otro.
- **telnet:**(**TEL**ecommunication **NET**work) es el nombre de un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
- **rsh:**Programa de consola para ejecutar comandos en ordenadores remotos.
- **scp:**Medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos.

- **rcp:**(Remote Procedure Call), técnica para la comunicación entre procesos de una o más computadoras conectadas a la red.
- **ADSL:**(Asymmetric Digital Subscriber Line), Es una tecnología de acceso a Internet de banda ancha.
- **MAC:**(Media Access Control), Identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red.

BIBLIOGRAFIAS:

- Redes de computadoras, Andrew S. Tanenbaum, Edición 2012
- Topologías de redes, http://books.google.com.mx/books?id=duk7k-YoYwEC&pg=PA53&dq=topologias+de+redes&hl=en&sa=X&ei=6aWrUOnvB4my2QXYi4HAAQ&ved=0CEQQ6AEwCQ#v=onepage&q=topologias%20de%20redes&f=false, 2010

- Topología e infraestructura básica de redes inalámbricas, http://www.it46.se/courses/wireless/materials/es/04_Topologia-Infraestructura/04_es_topologia-e-infraestructura_guia_v01.pdf, julio/2007.

- Tutoriales WLAN http://www.tutorial-reports.com/wireless/wlanwifi/index.php?PHPSESSID=f363004d5d4ea4638c805f7f71e3bd6f, año 2007.

- Redes WLAN, http://books.google.com.mx/books?id=k3JuVG2D9lMC&printsec=frontcover&dq=redes+wlan&hl=en&sa=X&ei=jrqvUMCvMumY2wXL5IGYBw&ved=0CDUQ6AEwAQ, año 2006.

- IEEE 208.11, http://es.wikipedia.org/wiki/IEEE_802.11#802.11k, 15/11/2012
- Redes inalámbricas http://www.itcom.com/redesinalambricas.htm