UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"ANÁLISIS COMPARATIVO ENTRE REDES LAN, ALÁMBRICA E INALÁMBRICA BASADA EN EL ESTÁNDAR IEEE 802.11b"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A :

PAOLA PINELO BOLAÑOS

DIRECTOR DE TESIS: ING. RODOLFO ARIAS VILLAVICENCIO

CIUDAD UNIVERSITARIA, AGOSTO 2004

CAPÍTULO 1. Introducción

Una red inalámbrica puede definirse como un conjunto de dispositivos (computadoras, impresoras, puntos de acceso, etcétera) capaces de intercambiar información mediante ondas electromagnéticas, evitando, así, la construcción de un enlace dedicado a un sitio fijo y permitiéndole al usuario obtener mayor movilidad.

La relación entre las redes inalámbricas y los dispositivos de cómputo portátiles es estrecha; sin embargo, no siempre se encuentra presente. Existen computadoras portátiles que requieren de cableado para tener acceso a la red (aquéllas que no cuentan con transmisor inalámbrico). También se pueden observar redes inalámbricas que no son portátiles, por ejemplo, las que se utilizan para la conexión de dos redes en diferentes edificios, por medio de transmisores y receptores inalámbricos colocados en las azoteas de dichos inmuebles.

En los últimos años, la creciente popularidad de las comunicaciones inalámbricas ha llamado la atención de los cuerpos corporativos, de manufactura y académicos. Los servicios de datos en los sistemas inalámbricos se han desarrollado rápidamente y han evolucionado en muchos factores, principalmente económicos, de regulación y hardware. Actualmente es común el uso de dispositivos inalámbricos como son: laptops, teléfonos celulares, PDA's (*Personal Digital Assistant*) radio localizadores, etc.

La evolución de la tecnología basada en el estándar IEEE 802.11b definido para las redes LAN[1] inalámbricas, ha sido relativamente lento, debido a que inicialmente se definieron especificaciones de capa física, especificaciones de control de acceso al medio (MAC) y un esquema de seguridad que pronto se volvió vulnerable. Por otro lado, no se definió un esquema de administración de dispositivos por lo que los fabricantes tomaron sus propias líneas de desarrollo. Debido a esto se presentaron incompatibilidades entre equipos de diferentes fabricantes y actualmente se están creando alianzas entre proveedores para evitar este problema.

1.1. Justificación

La revolución de las telecomunicaciones y el procesamiento de la información están creando una sociedad cuyas actividades y procesos se basan cada día más en la información digital. Los avances e interacciones de estos campos se han incrementado aceleradamente en los últimos años y se prevé que esta tendencia vaya en aumento en un futuro. Por esta razón se puede estimar un incremento considerable en la utilización de las redes de comunicaciones.

[1] LAN: Local Area Network

Las redes cableadas presentan algunos inconvenientes sobre todo de movilidad, por ello se han desarrollado las redes inalámbricas que proporcionan mayor comodidad al usuario brindándole movilidad y facilidad de implementación para el acceso a una red de comunicaciones. Una red inalámbrica puede ser muy útil en lugares donde no existe la infraestructura para la elaboración de cableados dedicados a cada usuario, como techos y pisos falsos; o en lugares donde se requieran redes provisionales. Actualmente no existe una competencia del mercado entre ambas redes, por el contrario una es complemento de la otra; por lo que al implementar una red LAN el usuario debe tener muy bien definidas sus necesidades para elegir la mejor opción de acuerdo con las ventajas y desventajas que ofrece cada una de ellas.

1.2. Objetivo

Realizar un análisis de las ventajas y desventajas de una red LAN alámbrica tradicional y una inalámbrica basada en el estándar IEEE 802.11b.

Los aspectos a analizar son el rendimiento, seguridad, costo, infraestructura, estandarización, movilidad y facilidad de implementación. Inicialmente se dará una breve explicación de cada uno de los dos tipos de redes LAN mencionadas en este trabajo de tesis y con base en ello se realizará la comparación.

Es importante señalar que la comparación entre las redes LAN, será realizada considerando la existencia de una infraestructura de red WAN operando sin problema alguno y con un nivel de seguridad adecuado para las necesidades del usuario.

1.3. Estructura del documento

El presente documento será conformado por ocho capítulos, un glosario, un apéndice y un apartado con referencias bibliográficas y electrónicas. A continuación se describe brevemente el contenido de cada uno de ellos.

El primer capítulo es la introducción, en la que se menciona la justificación, el objetivo y la estructura del documento.

En el segundo capítulo se explica la teoría básica de redes de datos. Se estudian el modelo OSI, medios de transmisión, redes WAN[2], redes LAN y conceptos básicos de redes datos.

En el tercer capítulo se describen las características de una red LAN alámbrica y la tecnología Ethernet. Se mencionan topologías, métodos de acceso al medio y dispositivos empleados.

[2] WAN: Wide Area Netwok

En el cuarto capítulo se explica el estándar IEEE 802.11b, mencionando las especificaciones de capa física, de subcapa MAC y las características de los esquemas de seguridad definidos en el estándar.

En el quinto capítulo se exponen las principales funcionalidades de una red LAN alámbrica, como son las VLAN's[3], esquemas redundantes, enlaces troncales, etc.

En el sexto capítulo se describen algunos esquemas de seguridad aplicables a redes LAN alámbricas e inalámbricas. La seguridad nunca es suficiente para una red de comunicaciones, sobre todo para las privadas, debido a que existen diversas formas de atacar una red, por ello es necesario protegerla lo mejor posible de acuerdo con el nivel de seguridad deseado y al presupuesto del usuario.

Con el respaldo de los capítulos anteriores, en el séptimo se analizan las ventajas y desventajas de las redes de datos alámbricas e inalámbricas, comparando todas las características posibles para obtener conclusiones objetivas.

En el capítulo ocho se mencionan de manera concisa las conclusiones obtenidas del análisis realizado en el capítulo anterior.

En el apéndice uno, se expone una breve explicación de los números de puertos TCP/UDP utilizados para comunicación en una red de datos.

El glosario está formado por los términos más utilizados dentro del ámbito de las redes de comunicaciones alámbricas e inalámbricas, los cuales están acompañados de una breve explicación.

Finalmente se tiene la bibliografía y las referencias electrónicas usadas durante el desarrollo del presente trabajo de tesis.

[3] VLAN: Virtual Local Area Network

CAPÍTULO 2. Teoría básica basada en redes de datos

Las tecnologías de la comunicación de datos están en continua evolución y crecen a una velocidad impresionante. Hoy en día, las redes de información facilitan la comunicación entre individuos ya sea de forma personal, dentro de una organización o entre organizaciones, permitiendo explotar información que nos lleve a mejorar nuestras condiciones de vida e incrementar la productividad empresarial.

Una red de datos se puede definir como una colección de dispositivos interconectados entre sí, con la eficiencia y productividad necesaria para que los usuarios puedan obtener o intercambiar información, independientemente del tiempo o lugar.

2.1 Estructura de red definida por jerarquías

Las redes de datos suelen estar organizadas en forma jerárquica para simplificar el diseño, implementación y administración. El modelo más común se basa en una estructura de red jerárquica que está compuesta de tres niveles: Dorsal, Distribución y acceso.

El nivel de acceso es la región en la cual los usuarios tienen conexión hacia la red, compartiendo recursos (impresoras, servidores, computadoras personales, entre otros.) y ancho de banda. Con esto se logra que el tráfico local entre dispositivos no afecte al de los niveles superiores.

En el nivel de distribución se concentra, distribuye y enruta información dirigida o recibida de los niveles dorsal, distribución y acceso. En este nivel es donde se determina cual es la ruta óptima para la entrega de un paquete, ya sea hacia un enrutador del nivel de acceso que éste concentre, o bien hacia un enrutador del nivel dorsal para su entrega en otro punto de la red.

La función principal del nivel dorsal es conmutar el tráfico tan rápido como sea posible. En la figura 2-1 se muestra el esquema de una red jerárquica.

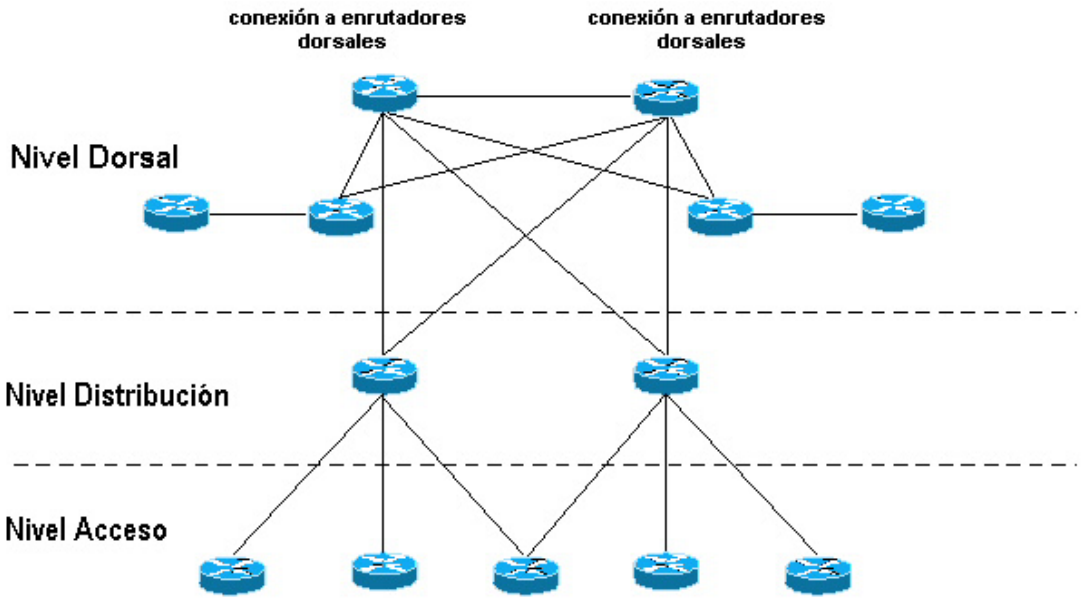


Figura 2-1. Esquema de una red jerárquica

2.2 Modelo de referencia OSI

El modelo de referencia OSI (*Open System Interconnections*) describe cómo se transfiere la información desde una aplicación de software en una computadora a través del medio de transmisión, hasta una aplicación de software en otra computadora. OSI es un modelo conceptual compuesto de siete capas; en cada una de ellas se especifican funciones específicas de red. Fue desarrollado por la ISO (*International Standards Organization*) en 1984 y actualmente se considera el modelo principal de arquitectura para la comunicación entre computadoras. En la siguiente figura se muestran las capas del modelo OSI.

Figura 2-2. Modelo de referencia OSI

2.2.1 Características de las capas del modelo OSI

Las siete capas del modelo OSI se pueden dividir en dos categorías: capas inferiores y capas superiores. Las capas superiores tienen que ver con la aplicación y en general están implementadas sólo en software. Las capas inferiores manejan lo concerniente a la transferencia de datos; las capas física y de enlace de datos se encuentran implementadas en Hardware y Software, mientras las capas de red y transporte están implementadas únicamente en Software. La figura 2-3 muestra la división entre capas superiores e inferiores.

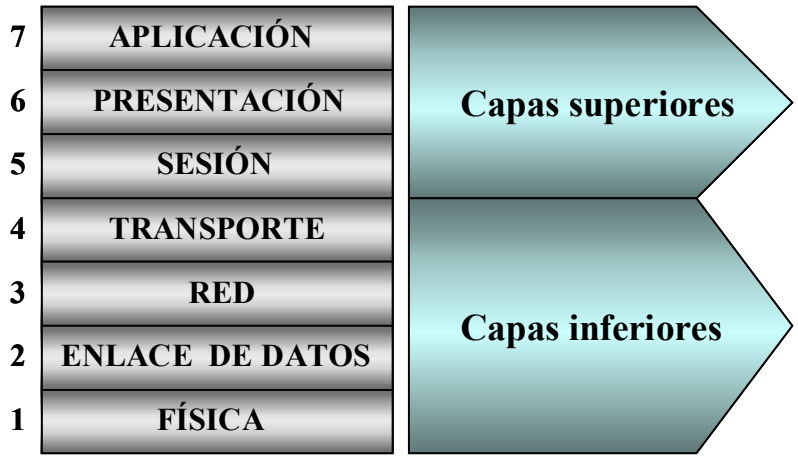


Figura 2-3. Clasificación de capas del modelo OSI

2.2.2 Capa física

Esta capa define las especificaciones eléctricas, mecánicas y funcionales para activar, mantener y desactivar el enlace físico entre sistemas de redes de comunicaciones. Las especificaciones definen características como niveles de voltaje, temporización de cambios de voltaje, velocidades de transferencia de información, distancias máximas de transmisión y conectores físicos. Las implementaciones de la capa física se pueden clasificar como especificaciones LAN o WAN.

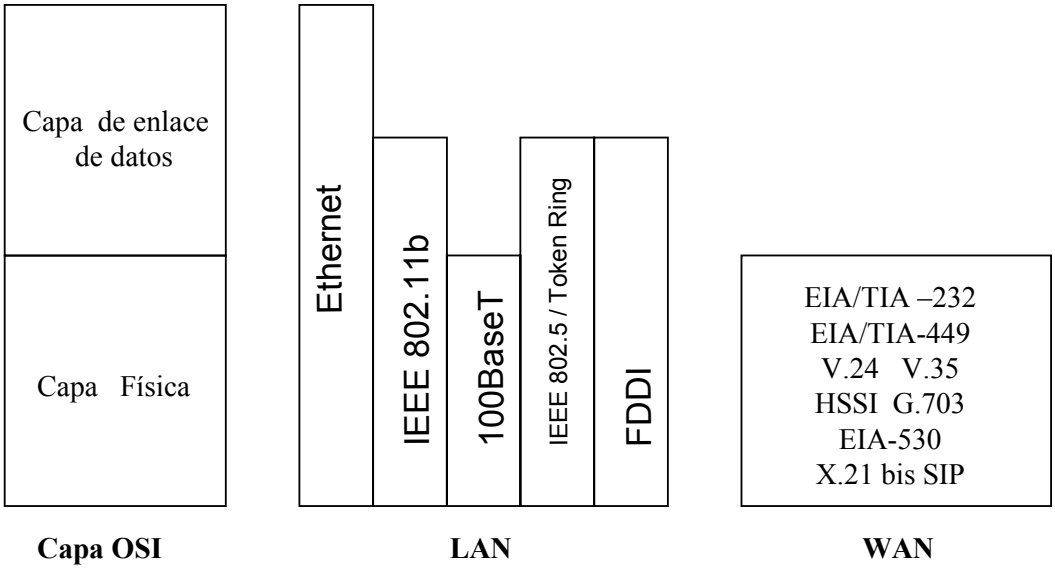


Figura 2-4. Especificaciones de la capa física

2.2.3 Capa de enlace de datos

Proporciona el tránsito confiable de datos a través del enlace físico. Diferentes especificaciones de la capa de enlace de datos definen las características de red y protocolo, incluyendo el direccionamiento físico, la topología de red, notificación de error, secuencia de tramas y el control de flujo. El direccionamiento físico, define cómo se nombran los dispositivos en la capa de enlace de datos. La topología de red consiste en especificaciones, que con frecuencia definen la forma en que se conectarán físicamente los dispositivos, en topología de bus o anillo. La notificación de error alerta a los protocolos de las capas superiores cuando se presenta un error en la transmisión y la secuencia de tramas de datos reordena las que se han transmitido fuera de secuencia. Finalmente, el control de flujo regula la transmisión de datos para que el dispositivo receptor no se sature con más tráfico del que pueda manejar simultáneamente.

El IEEE (*Institute of Electrical and Electronic Engineers*) ha dividido la capa de enlace de datos en dos subcapas: LLC (*Logical Link Control*) y MAC (*Media Access Control*). La subcapa MAC es responsable de las técnicas de acceso al medio de transmisión y del direccionamiento físico de dispositivos; mientras que en la capa superior se ubica el estándar IEEE 802.2, también conocido como LLC que define las funciones lógicas de la capa de enlace, así como la disponibilidad de SAP's[1] para la adecuada transmisión o

[1] SAP (*Service Access Point*). Es un campo definido en el estándar IEEE 802.2 que es parte de una especificación de dirección . Por lo tanto, el SAP destino (DSAP) define el receptor de un paquete, lo mismo se aplica al SAP origen (SSAP).

recepción de información a protocolos que operan en capas superiores del modelo de referecia OSI. En la siguiente figura se ilustran las subcapas de la capa de enlace de datos.

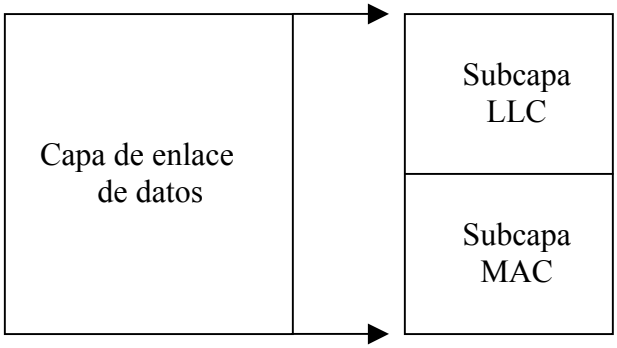


Figura 2-5. Capa de enlace de datos

LLC provee los siguientes servicios de capa de red:

- *Servicio no orientado a conexión*: Definido como el Tipo 1 de operación. En éste las tramas son enviadas con la esperanza de que lleguen correctamente a su destino; es decir, no existe mecanismo alguno de detección de errores y/o retransmisión de información.
- *Servicio orientado a conexión*: Definido como el Tipo 2 de operación. En éste se establecen, usan, reinician y terminan las conexiones a nivel de enlace entre estaciones terminales, con objeto de efectuar la retransmisión de tramas en caso de pérdida o transmisión errónea, así como el control de flujo entre estaciones.

El formato de la trama LLC es el que se muestra a continuación:

1 Byte	1 Byte	1 ó 2 Bytes	N bytes
DSAP	SSAP	Control	Información

Figura 2-6. Formato de la trama LLC

Donde :

DSAP: SAP destino
SSAP: SAP origen
N: Entero mayor o igual a cero

2.2.4 Capa de red

En esta capa se proveen funciones de enrutamiento y otras relacionadas que permiten integrar múltiples enlaces de datos en una red. Se define también, un direccionamiento lógico que permite identificar un dispositivo en cualquier parte de una red. La capa de red soporta servicios orientados y no orientados a conexión de los protocolos de capas superiores. Los protocolos de la capa de red, son de hecho, protocolos de enrutamiento, sin embargo también otro tipo de protocolos están implementados en ésta.

Algunos protocolos de enrutamiento son el BGP (*Border Gateway Protocol*) un protocolo entre dominios de Internet; OSPF (*Open Shortest Path First*) basado en estado de enlaces y desarrollado para utilizarse en redes TCP/IP (*Transfer Control Protocol/ Internet Protocol*) y RIP (*Routing Information Protocol*) el cual es un protocolo en el que utiliza el conteo de saltos como su métrica.

2.2.5 Capa de transporte

Esta capa provee un tránsito confiable de datos a través de la capa de red. Las funciones que otorga esta capa son multiplexaje, control de flujo, administración de circuitos virtuales así como detección y corrección de errores.

El control de flujo administra la transmisión de datos entre dispositivos para que el transmisor no envíe más datos de los que pueda procesar el receptor. El multiplexaje permite que la información de diferentes aplicaciones sea transmitida en una transmisión de capa 3. La verificación de errores implica la creación de varios mecanismos para detectar los errores en la transmisión, en tanto que la corrección implica realizar una acción, como solicitar la retransmisión de los datos.

Algunas implementaciones de la capa de transporte incluyen el protocolo de control de transmisión, el protocolo de enlace de nombres y protocolos de transporte del estándar OSI. TCP es el protocolo en el conjunto TCP/IP que proporciona una transmisión confiable de datos. NBP es el protocolo que asocia nombres *Apple Talk* con direcciones.

2.2.6 Capa de sesión

Establece, administra y finaliza las sesiones de comunicación entre las entidades de la capa de presentación. Las sesiones de comunicación constan de solicitudes y respuestas de servicio que se presentan entre aplicaciones ubicadas en diferentes dispositivos de red, permitiendo a éstas organizar y sincronizar el intercambio de datos. Estas solicitudes y respuestas están coordinadas por protocolos implementados en la capa de sesión. Un

ejemplo de implementación de la capa de sesión es ZIP, el protocolo de *AppleTalk* que coordina el proceso de enlace de nombres.

2.2.7 Capa de presentación

Brinda una gama de funciones de codificación y conversión que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema sea legible por su similar en otro sistema.

Los formatos de presentación de datos comunes o el uso de formatos estándar de vídeo, sonido e imagen, permiten el intercambio de datos de aplicación entre diferentes tipos de sistemas de computadoras. Los esquemas de conversión se utilizan para intercambiar información entre sistemas utilizando diferentes representaciones de texto y datos como, EBCDIC y ASCII. Los esquemas estándar de compresión permiten que los datos que se comprimen en el dispositivo fuente se puedan descomprimir adecuadamente en el destino. Los esquemas estándar de cifrado permiten que los datos originados en el dispositivo fuente, puedan ser descifrados de manera adecuada en el destino.

Las implementaciones en la capa de aplicación no suelen estar asociadas a un grupo particular de protocolos. Algunos estándares bien conocidos son Quick Time, el cual es una especificación de computadoras Apple para vídeo, audio y MPEG que es un estándar de compresión y codificación de vídeo. Entre los formatos conocidos de imagen están GIF (G*raphics Interchange Format*) y JPEG (*Joint Photographic Experts Group*) que son estándares para comprimir y codificar imágenes y TIFF (*Tagged Image File Format*) que es un estándar de codificación para gráficos.

2.2.8 Capa de aplicación

Ésta es la capa más cercana al usuario final, lo cual significa que tanto la capa de aplicación como el usuario interactúan de manera directa. Las funciones de esta capa incluyen la identificación de socios de comunicación, la determinación de la disponibilidad de recursos y la sincronización. Al identificar socios de comunicación, la capa de aplicación determina la identidad y disponibilidad para una aplicación que debe transmitir datos. Cuando se está determinando la disponibilidad de recursos, aquí es donde se decide si hay suficientes recursos en la red para la comunicación que se está solicitando. La sincronización es útil para la coordinación entre aplicaciones.

Dentro de las implementaciones de la capa de aplicación se encuentran las aplicaciones TCP/IP (*Transfer Control Protocol/ Internet Protocol*) y las aplicaciones OSI. Las primeras son protocolos como TELNET, FTP(*File Transfer Protocol*) y SMTP (*Simple Mail Transfer Protocol*) los cuales forman parte del grupo de protocolos de Internet. Las

aplicaciones OSI son protocolos como FTAM (*File Transfer, Access and Management*), VTP (*Virtual Terminal Protocol*) y CMIP (*Common Management Information Protocol*).

2.3 Interacción entre capas del modelo OSI

La información que se transfiere de una aplicación de software en un sistema de computadoras a una aplicación de software de otro, debe pasar a través de cada una de las capas del modelo OSI. Si por ejemplo, una aplicación en el Sistema A tiene que transmitir información a un Sistema B, el programa de aplicación en el Sistema A transferirá su información a la capa de aplicación (Capa 7). Ésta entonces, transferirán los datos junto con información de control a la capa de presentación (Capa 6) la cual hará lo mismo hacia la capa de sesión(capa 5) y así sucesivamente hasta la capa física (Capa 1). En esta última la información se coloca en el medio de transmisión físico y se envía al Sistema B. La capa física (Capa 1) del Sistema B recibe la información del medio físico y posteriormente la transfiere hacia la capa de enlace de datos (Capa 2) que verificará primero la información de control de capa 2 enviada por el sistema A, antes de transferir información a la capa de red (Capa 3) y así sucesivamente hasta que la información llega a la capa de aplicación (Capa 7) del Sistema B. Finalmente, esta última capa transfiere la información al programa de aplicación receptor para completar el proceso de comunicación.

Por lo general una capa determinada del modelo OSI se comunica con otras tres capas: las capas ubicadas directamente arriba y debajo de ésta y su capa equivalente en otro sistema de computadoras. Por ejemplo, la capa de enlace de datos del Sistema A se comunica con la capa de red y con la capa física; además con la capa de enlace de datos del Sistema B. La figura 2-7 ilustra este ejemplo.

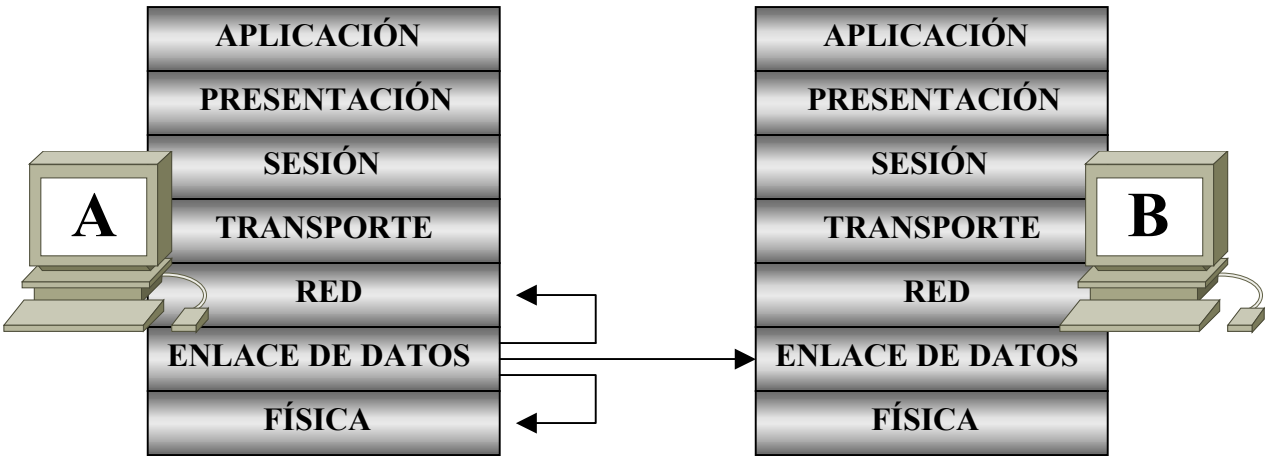


Figura 2-7. interacción de las capas del modelo OSI.

2.3.1 Formatos de información

Los datos y la información de control que se transmiten a través de las redes pueden tomar varios nombres de acuerdo con el nivel del modelo de referencia OSI donde se encuentren. Trama, paquete, datagrama, segmento, mensaje, celda o unidad de datos.

Una trama es la unidad de información cuyo origen y destino son entidades de la capa de enlace de datos. Una trama está compuesta por el encabezado de la capa 2 y los datos de capa superior. El encabezado y la cola contienen información de control para la entidad de la capa de enlace de datos en el sistema destino. Los datos de las entidades de las capas superiores se encapsulan. La figura 2-8 ilustra los componentes básicos de la trama de la capa de enlace de datos.

Encabezado de la capa de enlace de datos	Datos de capa superior	Cola de la capa de enlace de datos

Figura 2-8. Formato de trama

Un paquete o datagrama es una unidad de la información cuyo origen y destino son entidades de la capa de red. Un paquete se compone de un encabezado de la capa de red y datos de capa superior. El encabezado y la cola contienen información de control para la entidad de la capa de red en el sistema destino. Los datos de las entidades de la capa superior se encapsulan. En la figura 2-9 se muestran los componentes básicos de un paquete de la capa de red.

Encabezado de la capa de red	Datos de capa superior	Cola de la capa de red

Figura 2-9. Formato de paquete

Un segmento se refiere a una unidad de información cuyo origen y destino son entidades de la capa de transporte.

Un mensaje es una unidad de información cuyas entidades origen y destino están sobre la capa de sesión.

Una celda es una unidad de información de tamaño fijo cuyo origen y destino son entidades de la capa de enlace de datos. Las celdas se utilizan en entornos conmutados, como son las redes ATM (*Asynchronous Transfer Mode*) y las redes SMDS (*Switched Multi-megabit Data Service)*. Una celda se compone de un encabezado e información útil. El encabezado tiene una longitud de 5 bytes y contiene la información de control para la entidad destino de la capa de enlace de datos. La información útil contiene datos de la capa superior que está

encapsulada en el encabezado de la celda y suele tener la longitud de 48 bytes para el caso de ATM. La longitud de los campos de encabezado e información útil siempre es exactamente la misma para cada celda. La figura 2-10 muestra los componentes de una celda ATM.

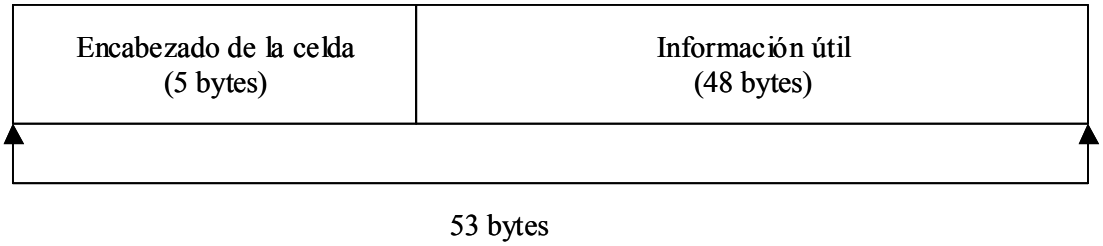


Figura 2-10. Componentes de una celda ATM

2.3.2 Intercambio de información en el modelo OSI

Cada capa del modelo OSI utiliza su propio protocolo para comunicarse con sus capas equivalentes en otros sistemas de computadoras. Para intercambiar información las capas utilizan PDUs (*Protocol Data Unit*) los cuales incluyen información de control de la capa OSI y datos del usuario. La información de control se encuentra en campos llamados encabezados y colas. El encabezado es información añadida al principio de los datos, mientras que las colas consisten en información añadida al final de los mismos datos.

Para relacionar la información de control a un PDU, las capas utilizan un proceso llamado encapsulación. Es decir que cuando una capa recibe un PDU, ésta encapsula el PDU con un encabezado y una cola, transmitiéndose a su vez como un PDU a la capa inferior. La información de control agregada en cada PDU es leída por la capa equivalente en el sistema de computadoras remoto.

Por ejemplo, en una comunicación TCP/IP, si la capa de transporte recibe un PDU de las capas superiores, a éste se le agrega la información de control dependiendo de la aplicación de la cual fue generado. Posteriormente éste pasa como otro PDU a la capa de red y ésta lo encapsula con su propio encabezado de información. El paquete se transfiere a la capa de red y ésta lo encapsula para originar un PDU llamado trama. El encabezado de trama contiene la información requerida realizar las funciones de enlace de datos. Cuando la capa física recibe la trama, ésta la codifica utilizando un sistema binario (unos y ceros) para la transmisión de datos alámbrica o inalámbrica. En la figura 2-11 se muestra este ejemplo.

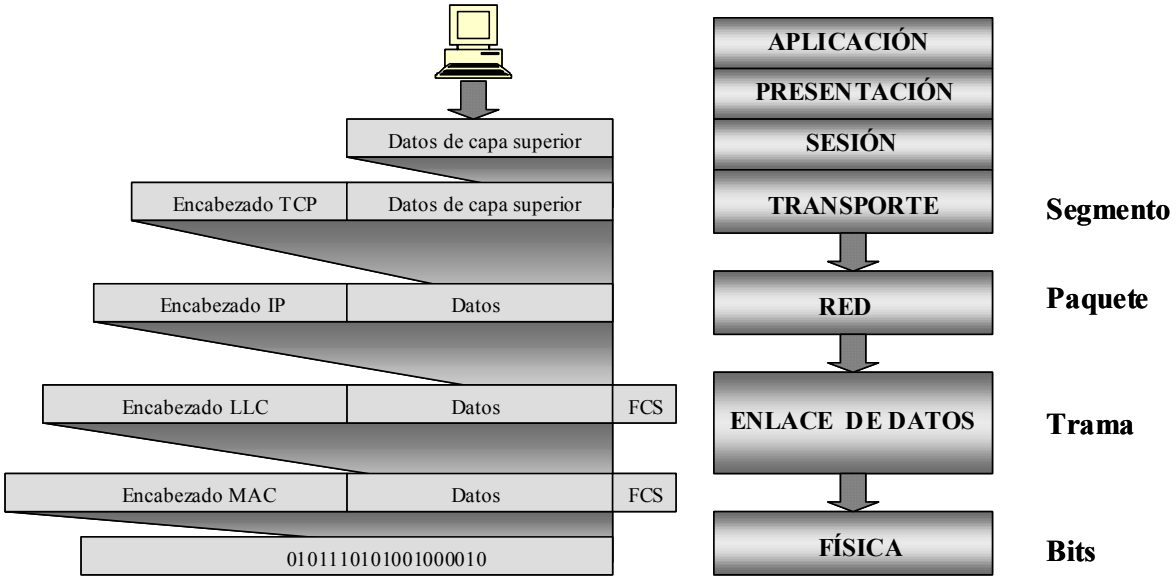


Figura 2-11. Encapsulación de datos

Cuando el sistema remoto recibe la secuencia de bits, éste los transfiere a la capa de enlace de datos y una vez que esta capa recibe la trama se realizan las siguientes funciones:

- Se lee la información de control contenida en el encabezado agregado por la capa de enlace de datos del sistema origen.
- Se desprende la información de control del encabezado de la trama.
- Se transfieren los datos transportados por la trama a la siguiente capa superior, siguiendo las instrucciones que aparecieron en la información de control.

A este proceso se le llama desencapsulación y se realizará en cada una de las capas. En la siguiente figura se ilustra este proceso.

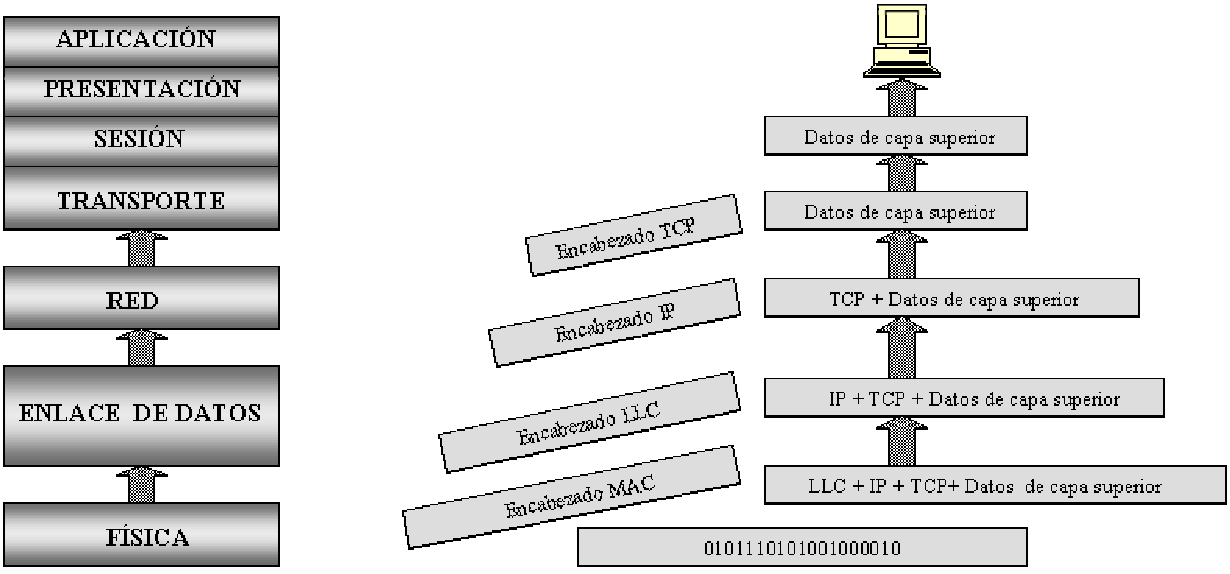


Figura 2-12. Proceso de Desencapsulación

2.4 Medios de transmisión

Los medios de transmisión se refieren al canal de comunicación que se utiliza para conectar la red de computadoras. Los datos son codificados y transmitidos de acuerdo con las características del medio y llegan a su destino ya sea a través de pulsos eléctricos, oscilaciones luminosas, ondas electromagnéticas o cualquier tipo de tecnología disponible. La clasificación de dichos medios se muestra en la siguiente figura.

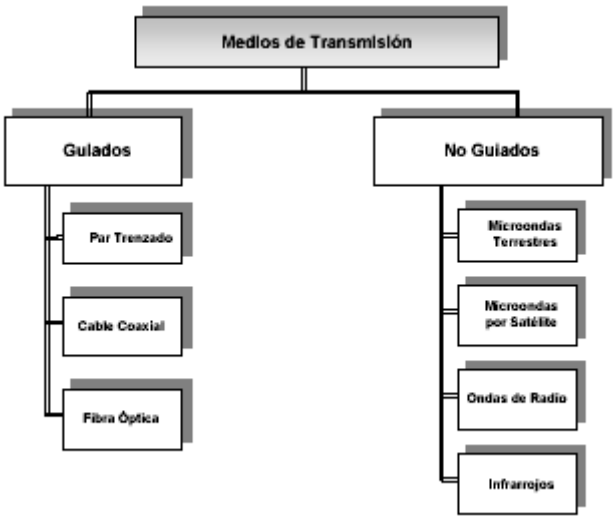


Figura 2-13. Clasificación de los medios de transmisión

2.4.1 Cable coaxial

Durante muchos años, el cable coaxial ha tenido diversas aplicaciones en la interconexión de equipos electrónicos y de cómputo, ya que es un producto maduro, confiable, relativamente económico y fácil de instalar. Este tipo de cable consta de dos conductores coaxiales (tienen un eje común y de ahí el nombre del cable) separados por un dieléctrico. En la siguiente figura se muestra la estructura de un cable coaxial.

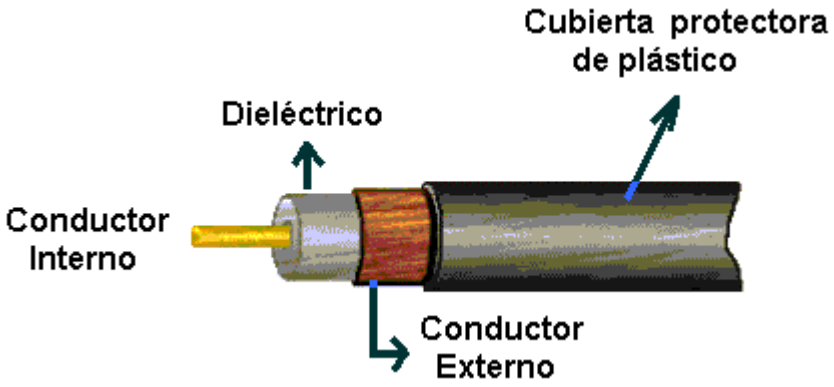


Figura 2-14. Estructura del cable coaxial.

Por lo general, los dos conductores de un cable coaxial son de cobre, aunque puede haber diseños específicos con aluminio recubierto de cobre, acero o inclusive, plata. En cuanto a los dieléctricos empleados, cuando la línea es rígida se prefiere usar simplemente aire; en este caso la distancia entre los conductores se conserva con pequeños separadores plásticos colocados en ciertos puntos a lo largo de la línea. En cambio en los cables semirígidos o flexibles es común encontrar aislantes como el polietileno, polipropileno, teflón y otros compuestos. También existen diseños de líneas con aislante de espuma sólida, hecha de los mismos compuestos anteriores.

La impedancia característica de los cables coaxiales se encuentra aproximadamente en el rango $20\ \Omega \leq Zo \leq 200\ \Omega$, pero para los sistemas de cómputo se utilizan cables con $Zo = 50\ \Omega$.

En el ámbito de las redes de datos, el cable coaxial se usa normalmente en la conexión de redes con topología de bus (mencionada en el capítulo 2). En un inicio se utilizó cable coaxial grueso (*"Thick wire" o "Thick Ethernet"*) para la tecnología 10BASE5, después evolucionó al cable coaxial delgado (*"Thin wire" o "Thin Ethernet"*) para ser utilizado con tecnología 10BASE2, el cual es más fácil de trabajar y de menor costo.

2.4.2 Cable multipar

El rápido crecimiento del tráfico telefónico trajo consigo la invención y la popularidad de los cables multipar. Algunos tienen solamente dos pares en su interior, pero otros pueden tener más. El término *par* equivale a una línea bifilar individual, cuyos conductores de cobre tienen diámetros típicos de entre 0.5 y 2.0 mm, según el fabricante y el uso específico del cable. Por lo general, la separación entre los ejes de los dos conductores es de 1.5 veces el diámetro de cualquiera de ellos. El aislante que ahora se emplea comúnmente entre cada pareja de conductores es polietileno.

En este tipo de cables se presenta el fenómeno de la diafonía, debido a la cercanía entre los pares y al aislamiento o blindaje imperfecto que haya entre ellos. Este acoplamiento entre

líneas se traduce en capacitancias parásitas y se manifiesta como una interferencia que reduce la calidad de la transmisión en cada línea.

El fenómeno de la interferencia por diafonía se puede reducir significativamente trenzando los pares, como se ilustra en la figura 2.15. Esta técnica de trenzado le da el nombre, también, de cable de par trenzado.

Figura 2-15. Estructura del cable multipar

El tipo de cable multipar en las redes de datos es el cable UTP[2] y actualmente existen 5 categorías:

- **Categoría 1**. Especialmente diseñado para redes telefónicas, empleado en teléfonos y dentro de las compañías telefónicas.
- **Categoría 2**. Es también empleado para transmisión de voz y datos hasta 4 Mbps.
- **Categoría 3**. Es empleado en redes de computadoras con velocidades de hasta 16 Mbps.
- **Categoría 4**. Tiene la capacidad de soportar comunicaciones en redes de computadoras a velocidades de 20 Mbps.
- **Categoría 5**. Un verdadero estándar actual dentro de las redes LAN particularmente, con la capacidad de soportar comunicaciones de hasta 100 Mbps. Lo interesante de este último modelo es la capacidad de compatibilidad que tiene contra los tipos anteriores.

Sintéticamente los cables UTP se pueden catalogar en dos clases básicas: los destinados a comunicaciones de voz, y los dedicados a comunicaciones de datos en redes de computadoras.

2.4.3 Fibra óptica

La fibra es un hilo fino de vidrio, cuyo grosor puede asemejarse al de un cabello, capaz de conducir la luz por su interior, generalmente esta luz es de tipo infrarrojo y no es visible al

[2] UTP: *Unshielded Twisted Par* (Par trenzado sin blindaje)

ojo humano. La modulación de esta luz permite transmitir información tal como lo hacen los medios eléctricos.

Desde el punto de vista geométrico, una fibra óptica consiste en una barra dieléctrica cilíndrica muy delgada y larga, rodeada por una capa coaxial de otro material dieléctrico. La barra central se denomina núcleo y la capa es llamada revestimiento o recubrimiento, véase la siguiente figura.

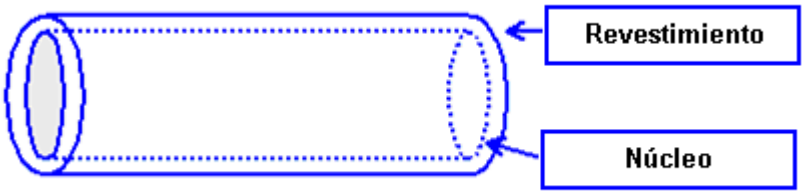


Figura 2-16. Estructura de la fibra óptica

El material que se emplea para fabricar las fibras es un vidrio flexible sumamente puro y transparente, obtenido a través de un proceso de refinamiento muy elaborado, en donde la materia prima es dióxido de silicio (SiO_2) y abunda en la arena de mar. El dióxido de silicio es dopado radialmente con otros materiales, como germanio o pentóxido de fósforo, para aumentar su índice de refracción; o bien si se desea reducir éste, entonces se dopa con boro. La mezcla con mayor índice de refracción se utilizará para el núcleo; y la de menor índice, para el revestimiento.

La fibra óptica es de mayor costo que cualquiera de los cables antes mencionados, pero es insustituible para situaciones donde las distancias son muy grandes y los riesgos ambientales o las emisiones electrónicas son un problema, debido a que éste es el medio de transmisión inmune a las interferencias. También son útiles cuando las distancias son muy grandes.

Las fibras ópticas se clasifican de acuerdo con el modo de propagación que describen los rayos de luz emitidos dentro de ellas. Existen tres tipos en esta clasificación.

Monomodo. En este tipo de fibra, los rayos de luz transmitidos por la fibra viajan linealmente y se puede considerar como el modelo más sencillo de fabricar.

Multimodo índice gradual. Este tipo de fibra es más costosa y tiene una capacidad realmente amplia. Sus costos son elevados ya que el índice de refracción del núcleo varía de más alto a más bajo en el recubrimiento, este hecho produce un efecto espiral en todo rayo introducido en la fibra óptica, describiendo una forma helicoidal a medida que el rayo de luz avanza por la fibra.

Multimodo índice escalonado. Este tipo de fibra se denomina multimodo de índice escalonado. La producción de las mismas resulta adecuada en lo que se refiere a tecnología

y precio. No tiene una capacidad tan grande como la de índice gradual, pero la calidad final es altamente aceptable.

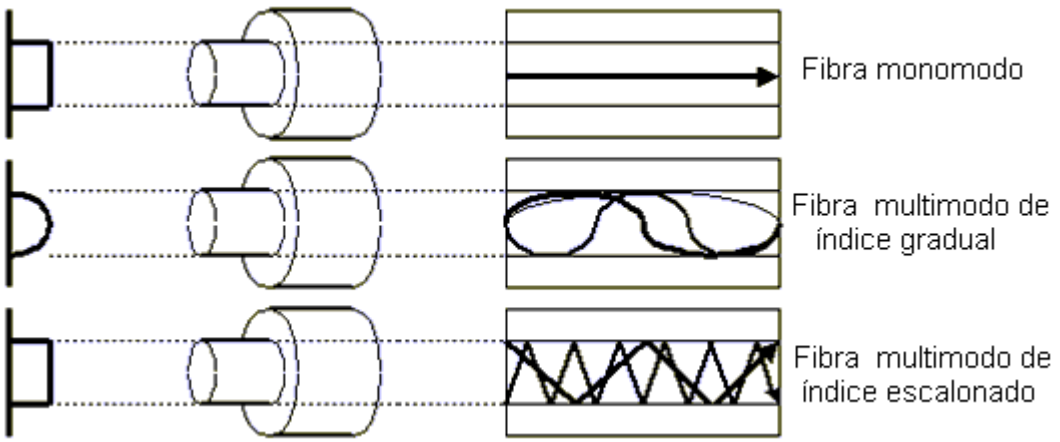


Figura 2-17. Clasificación de la fibra óptica.

2.4.4 Infrarrojos

La transmisión de información mediante infrarrojos está ampliamente extendida en el mercado residencial para manipular equipos de audio y vídeo. La comunicación se realiza entre un diodo emisor de luz, sobre la que se superpone una señal, convenientemente modulada y un fotodiodo receptor cuya misión consiste en reconstruir la información enviada.

Al tratarse de un medio de transmisión óptico, éste es inmune a las radiaciones electromagnéticas producidas por los equipos electrónicos o por los demás medios de transmisión (coaxial, cable multipar, etc.). Sin embargo, dichas interferencias sí afectarán a los dispositivos optoelectrónicos (diodo emisor de luz y fotodiodo receptor) colocados en los extremos del sistema de transmisión.

Los sistemas con tecnología infrarroja pueden utilizar tres modos diferentes de radiación para intercambiar la información entre receptores y transmisores:

- **Punto-a-punto**: los patrones de radiación del emisor y del receptor deben estar lo más cerca posible, para que su alineación sea correcta. Como resultado, el modo punto a punto requiere una línea de vista entre las dos estaciones a comunicarse. Este modo es usado para la implementación de redes inalámbricas infrarrojas *Token-Ring*, el "anillo" físico es construido por el enlace inalámbrico punto-a-punto conectando a cada estación. Por otro lado la transmisión punto a punto es la que menor potencia óptica consume, pero no debe haber obstáculos entre las dos estaciones.

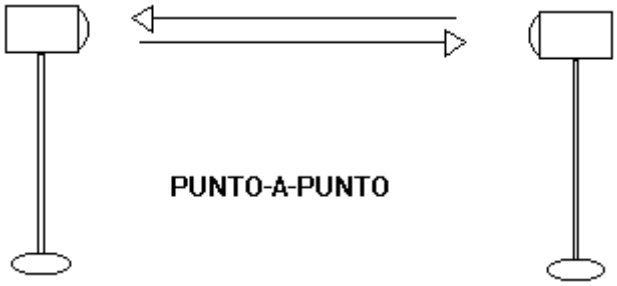


Figura 2-18. Transmisión infrarroja punto a punto

- **Cuasi-difuso**: son de emisión radial, o sea que cuando una estación emite una señal óptica, ésta puede ser recibida por todas las estaciones al mismo tiempo en la célula. En el modo cuasi–difuso las estaciones se comunican entre si, por medio de superficies reflejantes, no es necesario que las dos estaciones estén alineadas, pero sí deben estarlo con la superficie de reflexión. Además es recomendable que las estaciones estén cerca de la superficie de reflexión, ésta puede ser pasiva o activa. En las células basadas en reflexión pasiva, el reflector debe tener altas propiedades reflectivas y dispersivas, mientras que en las basadas en reflexión activa se requiere de un dispositivo de salida reflexivo, conocido como satélite, que amplifique la señal óptica. La reflexión pasiva requiere más energía, por parte de las estaciones, pero es más flexible de usar.

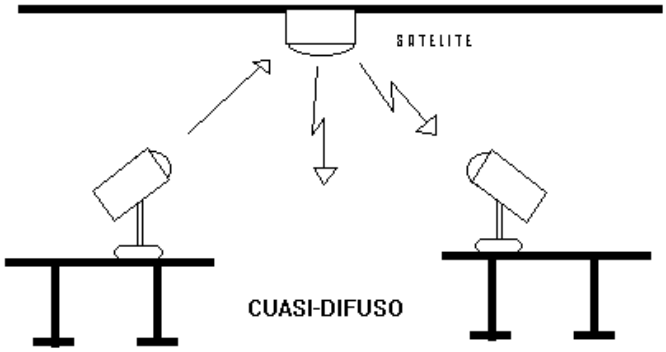
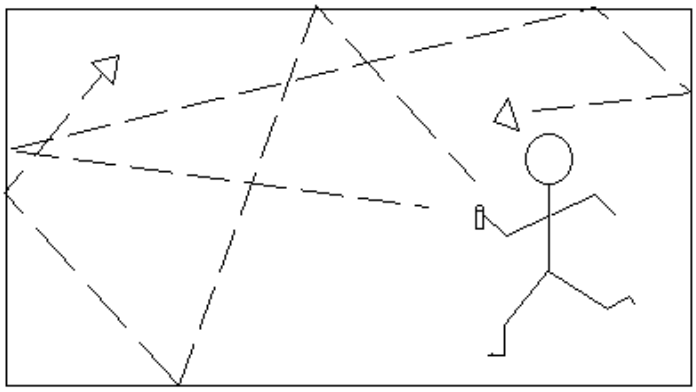


Figura 2-19. Transmisión infrarroja en modo cuasi-difuso

- **Difuso:** la emisión de la señal es radial y la potencia de salida de la señal óptica de una estación debe ser suficiente para llenar completamente el total de una habitación, mediante múltiples reflexiones en paredes y obstáculos; por lo tanto la línea de vista no es necesaria y la estación se puede orientar hacia cualquier lado. El modo difuso es el más flexible, en términos de localización y posición de la estación, sin embargo esta flexibilidad está a costa de excesivas emisiones ópticas.



DIFUSO

Figura 2-20. Transmisión inalámbrica en modo difuso

2.4.5 Microondas Terrestres

Los enlaces de microondas se utilizan mucho como enlaces donde los cables coaxiales o de fibra óptica no son prácticos. Para lograr una comunicación de este tipo frecuentemente es necesario que las estaciones transmisora y receptora tengan línea de vista, de modo que hay que disponer de antenas de microondas en torres elevadas en las cimas de las colinas o en sitios de gran elevación para asegurar un camino directo con la intervención de pocos repetidores; en otras ocasiones no es necesario que los dispositivos transmisor y receptor estén alineados.

Las microondas cubren una parte importante del espectro, de 2 a 300 GHz; el ancho de banda potencial y la velocidad de transmisión aumentan con la frecuencia, por lo que tienen múltiples aplicaciones como la transmisión de vídeo y de voz. El problema fundamental de este tipo de comunicación es la atenuación, que dependerá de la longitud de onda y de las condiciones meteorológicas, por ejemplo, a partir de los 10 MHz aumenta mucho la atenuación a causa de la lluvia.

Los enlaces de microondas tienen múltiples aplicaciones, se pueden utilizar en enlaces de larga distancia, en circuitos cerrados de televisión, interconexión de redes de datos locales y transmisión entre edificios.

2.4.6 Microondas vía satélite

Los satélites artificiales han revolucionado desde los últimos 20 años. Actualmente son muchos los satélites de comunicaciones dando servicio a numerosas empresas, gobiernos o entidades. Un satélite de comunicaciones hace la labor de repetidor electrónico. Una estación terrena A transmite al satélite señales de una frecuencia determinada (frecuencia

de subida). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B mediante una frecuencia distinta (frecuencia de bajada). La señal de bajada puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o imágenes de televisión. De esta manera se impide que las frecuencias de subida y de bajada se interfieran.

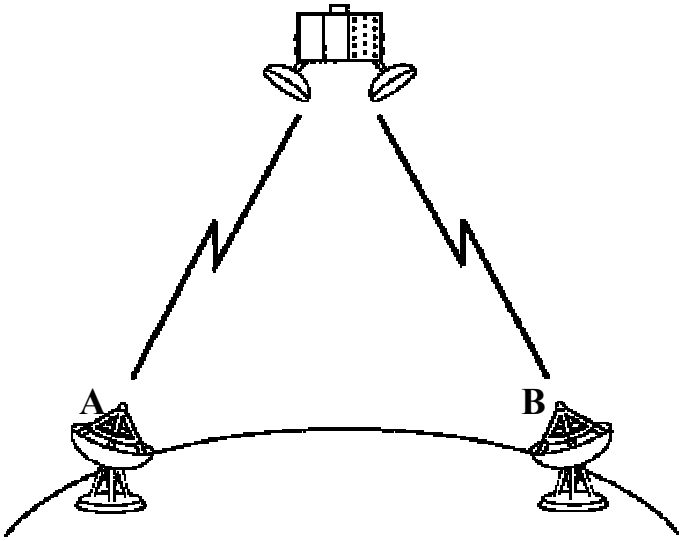


Figura 2-21. Transmisión satelital

La capacidad que posee un satélite de recibir y retransmitir se debe a dispositivos conocidos como transpondedores, los cuales trabajan a frecuencias muy elevadas, generalmente en la banda de los GHz. La mayoría de los satélites de comunicaciones están situados en una órbita denominada geoestacionaria que se encuentra a 36000 km sobre el ecuador . Esto permite que el satélite gire alrededor de la Tierra a la misma velocidad que ésta, de modo que parece casi estacionario. Así, las antenas terrestres pueden permanecer orientadas hacia una posición relativamente estable (lo que se conoce como "sector orbital") ya que el satélite mantiene la misma posición relativa con respecto a la superficie de la Tierra.

Algunas de las características de un sistema de comunicación vía satélite se mencionan a continuación:

- Existe un retardo de aproximadamente 0.5 segundos en las comunicaciones debido a la distancia que han de recorrer las señales. Los cambios en los retrasos de propagación provocados por el movimiento de un satélite geoestacionario necesita transmisiones frecuentes de tramas de sincronización.

- Los satélites tienen una vida útil de siete a diez años, pero pueden sufrir fallos que provoquen que el satélite quede fuera de servicio. Por tanto es necesario disponer de un medio alternativo de servicio en caso de cualquier eventualidad.

- Las comunicaciones vía satélite pueden ser interceptadas por cualquiera que disponga de un receptor en las proximidades de la estación. Es necesario utilizar técnicas de encriptación para garantizar la privacidad de los datos.

- Los satélites geoestacionarios pasan por periodos en los que no pueden funcionar. En el caso de un eclipse de Sol, en el que la Tierra se sitúa entre el Sol y el satélite, se corta el suministro de energía a las células solares que alimentan el satélite, lo que provoca el paso del suministro de energía a las baterías de emergencia, operación que a menudo se traduce en una reducción de las prestaciones o en una pérdida de servicio.

- Actualmente hay un problema de ocupación de la órbita geoestacionaria. Cuando un satélite deja de ser operativo, debe irse a otra órbita, para dejar un puesto libre. La separación angular entre satélites debe ser de 2 grados. Esta medida implicó la necesidad de mejorar la capacidad de resolución de las estaciones terrenas para evitar detectar las señales de satélites próximos en la misma banda de frecuencia.

Dentro de los servicios que prestan las comunicaciones vía satélite se encuentran las siguientes:

- **Difusión de TV**: el carácter multidestino de los satélites los hace especialmente adecuados para la difusión en particular de TV, aplicación para la que están siendo ampliamente utilizados.

- **Telefonía**: los satélites proporcionan enlaces punto-a-punto entre centrales telefónicas en las redes públicas de telefonía. Es el medio óptimo para enlaces internacionales con un alto grado de utilización.

- **Redes privadas**: la capacidad del canal de comunicaciones es dividido en diferentes canales de menor capacidad que se alquilan a empresas privadas que establecen su propia red sin necesidad de colocar un satélite en órbita.

2.4.7 Ondas de radio

Las ondas de radio se caracterizan por ser omnidireccionales para que exista un sistema de comunicación mediante ondas de radio, el emisor y receptor deben sintonizar la misma frecuencia. La señal puede traspasar muros, aunque se produce una atenuación dependiendo del material del que está fabricado dicho obstáculo, y no es necesaria la visión directa de emisor y receptor.

Dentro de las desventajas de este tipo de sistemas de comunicación es la alta sensibilidad a las perturbaciones electromagnéticas producidas, tanto por los medios de transmisión, como por los equipos domésticos. La frecuencia de transmisión suele ser baja, aproximadamente de los 30 Hz a los 300 MHz.

2.5 Direccionamiento en redes de datos

Las direcciones de red identifican a los dispositivos por separado o como miembros de un grupo. Los esquemas de direccionamiento varían dependiendo de la familia de protocolos y de la capa OSI. Los dos tipos de direccionamiento de red que se utilizan comúnmente son: direcciones MAC (*Media Access Control*) y direcciones de la capa de red.

2.5.1 Direcciones MAC

Las direcciones MAC sirven para identificar a un dispositivo a nivel físico dentro de un grupo de dispositivos que comparten un medio de transmisión y son únicas.

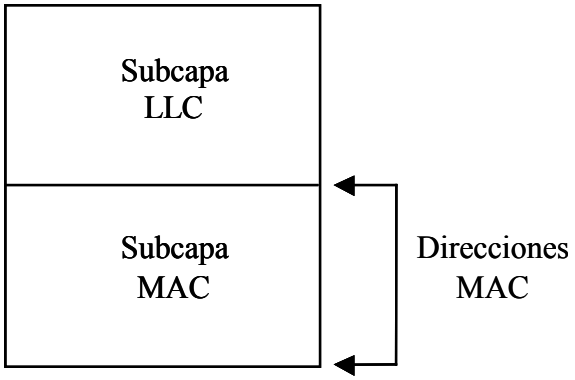
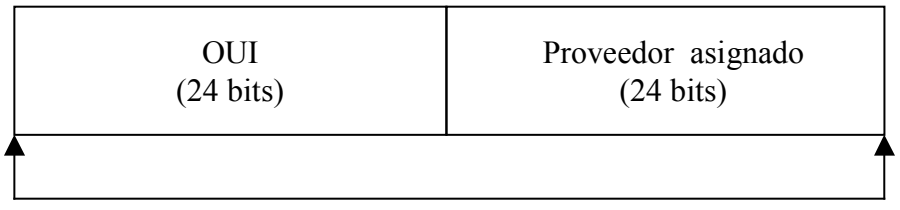


Figura 2-22. Esquema de las direcciones MAC

Las direcciones MAC tienen 48 bits de longitud y se expresan con 12 dígitos hexadecimales. Los 6 primeros son administrados por el IEEE e identifican al fabricante y, por lo tanto comprenden al OUI (*Organizational Unique Identifier*). Los últimos 6 dígitos comprenden el número de serie de la interfase u otro valor administrado por un proveedor específico. Las direcciones MAC están grabadas en un ROM (*Read Only Memory*) y son copiadas en RAM (*Random Access Memory*) al reiniciarse la tarjeta de interface. La siguiente figura muestra el formato de la dirección MAC.



DIRECCIÓN MAC

Figura 2-23. Formato de la dirección MAC

2.5.2 Direcciones de la capa de red

Una dirección de la capa de red identifica a un dispositivo en toda la red, haciendo posible la comunicación entre dispositivos que no comparten el mismo medio de transmisión. A menudo se les llama direcciones lógicas.

La relación entre una dirección de red y un dispositivo es lógica y no fija; se basa tanto en las características físicas de la red (dispositivo que está en un segmento de red particular) como en agrupaciones no físicas (dispositivo que es parte de la zona de AppleTalk). Los enrutadores y otros dispositivos requieren una dirección de la capa de red por cada conexión física a la red y por cada protocolo soportado; por ejemplo un enrutador con tres interfaces que corran AppleTalk, TCP/IP y X25, deben tener tres direcciones de la capa de red por cada interface.

2.6 Clasificaciones de una red

2.6.1 Red LAN

Una LAN (*Local Area Network*) es una red de datos de alta velocidad que cubre un área geográfica relativamente pequeña. Por lo general conecta estaciones de trabajo, computadoras personales, impresoras, y otros dispositivos. Las LANs tienen muchas ventajas para los usuarios de computadoras, entre otras el acceso compartido a dispositivos y aplicaciones , el intercambio de archivos entre los usuarios conectados y la comunicación entre usuarios vía correo electrónico.

Dentro de las tecnologías LAN más importantes se encuentran las siguientes:

- **Ethernet**: Especificación LAN de banda base, inventado por *Xerox Corporation* y desarrollado por *Xerox, Intel y Digital Equipment Corporation.* Posteriormente fue estandarizado por la IEEE con la norma 802.3. Las redes LAN Ethernet utilizan el método de acceso CSMA/CD[3].

- **FDDI**(*Fiber Distributed Data Interface*): Especificación LAN definido por la ANSI X3T9.5, que especifica una red *Token Ring* a 100 Mbps que utiliza cables de fibra óptica, con distancias de transmisión de hasta dos kilómetros. Esta especificación utiliza una arquitectura de anillo doble para proporcionar redundancia.

[3] CSMA/CD. *Carrier Sense Multiple Access Collision Detect, explicado en el capítulo 3.*

- **Token Ring**: En una LAN con protocolo de acceso de estafeta circundante, desarrollada y soportada por IBM. Su velocidad de transmisión es de 4 a 16 Mbps, sobre una topología física de estrella, pero funciona lógicamente como anillo.

2.6.2 Red WAN

Una WAN (*Wide Area Network*) es una red de comunicación de datos que tienen una cobertura geográfica relativamente grande y suele utilizar las instalaciones de transmisión que ofrecen compañías portadoras de servicios como las telefónicas

Las tecnologías y protocolos más comunes de las redes WAN se pueden clasificar en tres grupos :

- Tecnologías para la implementación de enlaces WAN.
- Protocolos WAN.
- Tecnologías de redes WAN públicas.

El primer grupo abarca sólo funciones de la capa 1 del modelo de referencia OSI:

- **ADSL** (*Asymmetric Digital Subscriber Line*). Tecnología para transmitir información digital a elevados anchos de banda. A diferencia del servicio *Dial up*, ADSL provee una conexión permanente y de gran velocidad. Esta tecnología utiliza la mayor parte del canal para enviar información al usuario, y sólo una pequeña parte para recibir información de usuario.

- **ISDN**(*Integrated Services Digital Network*). Protocolo de conmutación que ofrecen las compañías telefónicas, el cual permite transportar datos y voz.

- **SDH** (*Synchronous Digital Hierarchy*). Norma europea que define un conjunto de estándares de velocidad y de formato de transmisión, utilizando señales ópticas a través de fibras. SDH tiene una tasa básica de 155.52 Mbps, conocida como STM-1.

- **PDH** (*Plesiochronous Digital Hierarchy*). Define un conjunto de sistemas de transmisión para el transporte de voz digitalizada entre centrales teléfonicas, usando un método de multicanalización por división de tiempo (TDM) para interpolar múltiples canales de voz digital. Existen tres diferentes estándares PDH utilizados en las telecomunicaciones mundiales: T1 (estadounidense) E1 (europeo) y J1 (japonés). Para el caso de México, el estándar usado es el E1, cuya tasa de transmisión es de 2048 Kbps.

Dentro del segundo grupo se encuentran los siguientes protocolos, los cuales se encuentran definidos dentro de la capa 2 del modelo del referencia OSI:

- **PPP** (*Point to Point Protocol*). Provee un método estándar para transportar paquetes de múltiples protocolos sobre un enlace punto a punto. PPP consta de tres componentes principales: un método para encapsular paquetes de múltiples protocolos, un LCP (*Link Control Protocol*) para establecer, configurar y verificar la conexión, una familia de NCPs (*Network Contro Protocols*) para establecer y configurar diferentes protocolos de la capa de red. Este protocolo también posee mecanismos de seguridad como PAP[4] y CHAP[5].

- **HDLC** (*High Level Data Link Control*). Es un protocolo orientado a bit que especifica un método de encapsulamiento sobre enlaces seriales síncronos, utilizando caracteres de tramas y sumas de verificación, empleando la estrategia de inserción de bit. Posee tres etapas de comunicación que son: establecimiento del enlace , transmisión de información y liberación del enlace.

- **SDLC** (*Synchronous Data Link Control*). Protocolo de comunicaciones de la capa de enlace de datos orientado a bit, cuyo modo es *full duplex*.

Las siguientes tecnologías proveen servicios públicos tanto de capa 1 como de capa 2 del modelo de referencia OSI, pertenecen al tercer grupo:

- **X.25**. Estándar de la ITU-T[6] que define cómo se mantienen las conexiones entre DTE[7] y DCE[8] para el acceso a terminales remotas y comunicaciones de computadoras. Dentro de la perspectiva de X.25, una red opera en gran parte como un sistema telefónico. Una red X.25 se asume como si estuviera formada por complejos conmutadores de paquetes que tienen la capacidad necesaria para el ruteo de paquetes.

- **Frame Relay**. Protocolo conmutado de la capa de enlace de datos que maneja circuitos virtuales múltiples utilizando encapsulamiento HDLC entre los dispositivos conectados. La conmutación de tramas es más eficiente que X.25.

- **ATM** (*Asynchronous Transfer Mode*). Estándar internacional para conmutación de celdas, en el que se transportan varios tipos de servicios (voz, vídeo y datos) por medio de las celdas de longitud fija (53 bytes). Éstas permiten que el procesamiento de información se realice en hardware, reduciéndose así los retardos de transmisión.

- **SMDS** (*Switched Multimegabit Data Services*). Es una tecnología de red WAN de conmutación de paquetes a alta velocidad.

[4] PAP. *Password Authentication Protocol*
[5] CHAP. *Challenge Handshake Authentication Protocol*
Ambos explicados en el capítulo 5.

[6] ITU-T. *Internacional Telecomunication Union-Telecommunication*
[7] DTE. *Data Terminal Equipment*
[8] DCE. Data Communications Equipment

CAPÍTULO 3. Ethernet y Redes LAN alámbricas

3.1 Red LAN

Una red de datos es el conjunto de dispositivos que pueden compartir información digital , aplicaciones y recursos (por ejemplo impresoras, servidores, PC's,etc.). Las computadoras de una red de área local (LAN, *Local Area Network*) están separadas por distancias de pocos metros, y suelen usarse en oficinas o campus universitarios. Una red de este tipo permite la transferencia rápida y eficaz de información de un grupo de usuarios.

La conexión física entre los dispositivos de una LAN puede ser un cable coaxial, cable de par trenzado (UTP) o una fibra óptica. También pueden efectuarse conexiones inalámbricas empleando transmisores de infrarrojos, microondas o radiofrecuencia. Un dispositivo LAN puede transmitir y recibir señales de todos los demás dispositivos de la red LAN a la que se halla conectado.

3.1.1 Métodos de acceso al medio

Los protocolos LAN emplean métodos para intercambiar información a través de un único medio de transmisión compartido. Estos métodos impiden colisiones de datos provocadas por la transmisión simultánea entre dos o más computadoras. Los métodos de acceso al medio físico más comumente usados en una red LAN son: CSMA/CD (*Carrier Sense Multiple Access / Collision Detection*) y estafeta circundante (*Token Ring*).

En el esquema de acceso a medios CSMA/CD, los dispositivos de la red compiten por el uso del medio de transmisión físico de la red. Por esta razón, a este método a veces se le llama acceso por contención. Éste permite que cualquier estación de la red transmita información en cualquier momento siempre y cuando el medio de transmisión se encuentre libre. Antes de transmitir datos, las estaciones verifican si en ese momento se está efectuando una transferencia de datos y si la hay, la estación debe esperar a no detectar tráfico para poder transmitir. Una colisión se presenta cuando dos estaciones detectan que el medio de transmisión está libre y después transmiten de manera simultánea. En esta situación ambos envíos serán afectados y en consecuencia, las estaciones involucradas deberán retransmitir sus mensajes después de que haya pasado cierto tiempo. Los algoritmos de retransmisión determinan el momento en que las estaciones deben transmitir nuevamente.

En el esquema de acceso al medio llamado estafeta circundante, los dispositivos de la red tienen acceso al medio de transmisión con base en la posesión de una estafeta (*Token*). Cuando una estación desea mandar información debe esperar a que le llegue la estafeta vacía y cuando le llega, la utiliza para mandar la información a la estación destino; al llegar a esta última, la estafeta es enviada a la estación que originalmente envío la

información, con el mensaje de que fue recibida la información. De esta forma se libera la estafeta para volver a ser usada por cualquier otra estación. Debido a que se requiere la estafeta para enviar información, no se generan colisiones. Aquí el problema reside en el tiempo que debe esperar una estación para disponer de una estafeta vacía.

3.1.2 Métodos de transmisión en las redes LAN

La transmisión de datos en las redes LAN se clasifican en tres tipos: unidifusión (*unicast*) multidifusión (*multicast*) y difusión (*broadcast*).

En las transmisiones de unidifusión, se envía un solo paquete de un origen a un destino de la red. Primero, el nodo origen direcciona el paquete utilizando la dirección del nodo destino, luego el paquete es enviado a la red y finalmente, la red transfiere el paquete a su destino.

Las transmisiones de multidifusión constan de un solo paquete de datos que se copia y envía a un conjunto específico de nodos en la red. Primero el nodo origen dirige el paquete utilizado hacia la dirección de multidifusión. Después el paquete es enviado a través de la red, la cual genera copias del paquete de tal forma que cada uno de los nodos que se indican en la dirección de multidifusión reciba una copia del paquete original.

Las transmisiones de difusión constan de un sólo paquete de datos que se copia y se envía a todos los nodos de la red. En este tipo de transmisiones, el nodo origen dirige el paquete utilizando la dirección de difusión. Posteriormente el paquete es enviado a través de la red, la cual hace copias del paquete y las envía a cada uno de los nodos de la red.

3.1.3 Topologías LAN

Éstas definen la forma de organización entre los dispositivos de la red. Existen tres topologías comunes usadas en LAN: bus, anillo y estrella. Estas topologías son arquitecturas lógicas, por lo tanto, los dispositivos no necesitan estar ubicados físicamente de acuerdo con estas configuraciones. Por ejemplo, las topologías lógicas en bus y anillo, por lo común están dispuestas físicamente como una estrella.

Una topología de bus es una arquitectura lineal en la que los envíos de las diferentes estaciones de red se propagan a todo lo largo del medio de transmisión y son recibidas por todas las estaciones. En la tecnología Ethernet/ IEEE 802.3 se utiliza este tipo de tecnología. En la siguiente figura se muestra esta topología.

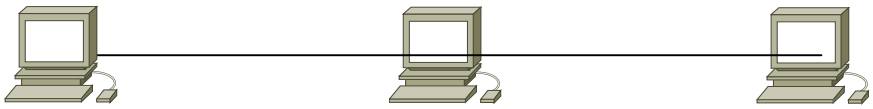


Figura 3-1 Topología de bus

Una topología de anillo es una arquitectura que consta de una serie de dispositivos conectados el uno con el otro por medio de enlaces de transmisión unidireccionales para formar un lazo cerrado. Tanto *Token Ring* como FDDI implementan una topología de anillo, la figura 3.2 muestra la topología de anillo.

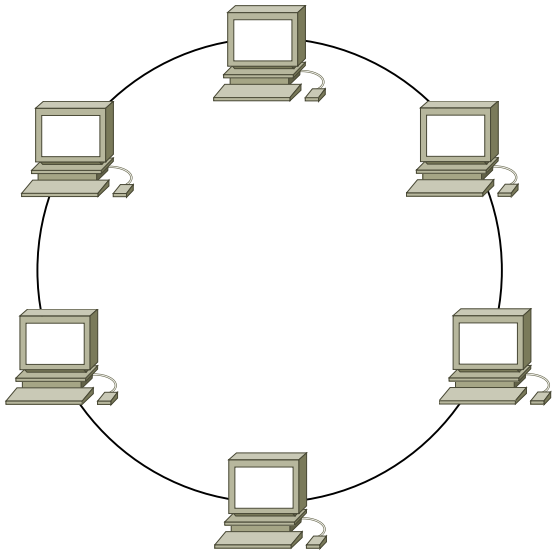


Figura 3-2. Topología de anillo

En una red LAN, una topología de estrella es una arquitectura en la que los puntos extremos de la red se conectan hacia un concentrador (*hub*) central común o *switch* por medio de enlaces dedicados. Las topologías lógicas en bus o anillo a menudo se implementan físicamente como una topología de estrella, la cual se ilustra en la siguiente figura.

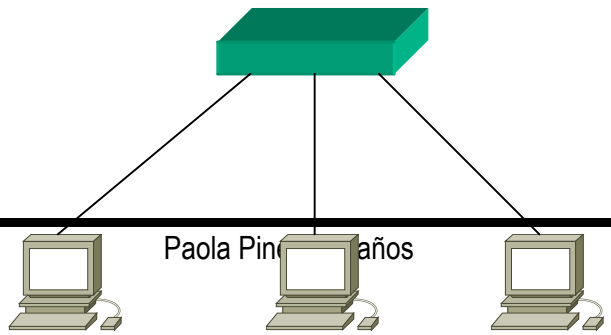


Figura 3-3.Topología de estrella

3.2 Ethernet e IEEE 802.3

Ethernet fue inventada en *Xerox Palo Alto Research Center* en los 70's por el Dr. Robert M. Metcalfe. El primer sistema Ethernet funcionaba aproximadamente a una tasa de transmisión de 3 Mbps y era conocido como "ethernet experimental".

Las especificaciones formales para Ethernet fueron publicadas en 1980 por un conjunto de compañías: *Digital Equipment Corp., Intel Corp., y Xerox Corporation*. Este impulso convirtió el "ethernet experimental" en un sistema abierto y de calidad que operaba a 10 Mbps y utilizaba CSMA/CD. La tecnología Ethernet fue tomada como base por el comité de estándares LAN del Instituto de Ingenieros Eléctricos y Electrónicos *(IEEE*) y emitieron la norma 802.3.

El estándar IEEE fue publicado por primera vez en 1985, bajo el título *"IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications."* (IEEE 802.3 Acceso Múltiple por Detección de Portadora con Detección de Colisiones, CSMA/CD, Método de Acceso y Especificaciones Físicas). Éste ha sido adoptado desde entonces por la Organización Internacional para la Estandarización (ISO[1]) lo que lo convierte en un estándar a nivel mundial. Además el estándar 802.3 es periódicamente actualizado para incluir nuevas tecnologías. Así, desde 1985 el estándar ha crecido para incluir nuevas velocidades y medios de transmisión para el sistema Ethernet de 10 Mbps (p.e. par trenzado) así como las últimas especificaciones para 100 Mbps (Fast Ethernet) y Gigabit Ethernet a 1 Gbps.

El estándar 802.3 difiere de la especificación Ethernet original en cuanto a que describe una familia completa de sistemas CSMA/CD, operando a diferentes velocidades de transmisión en distintos medios. También difieren en el uso de uno de los campos del encabezado de la trama, que contiene un número de tipo de protocolo para Ethernet y la longitud de los datos de trama en IEEE 802.3.

Todos los equipos denominados Ethernet desde 1985 se construyen de acuerdo con el estándar IEEE 802.3, es decir que, actualmente, deberíamos referirnos a Ethernet como "IEEE 802.3 CSMA/CD". De cualquier modo la mayor parte del mundo todavía lo conoce por su nombre original.

[1] ISO: *International Organization for Standardization*

3.2.1 Formatos de la trama Ethernet e IEEE 802.3

La siguiente figura muestra los campos de las tramas Ethernet e IEEE 802.3.

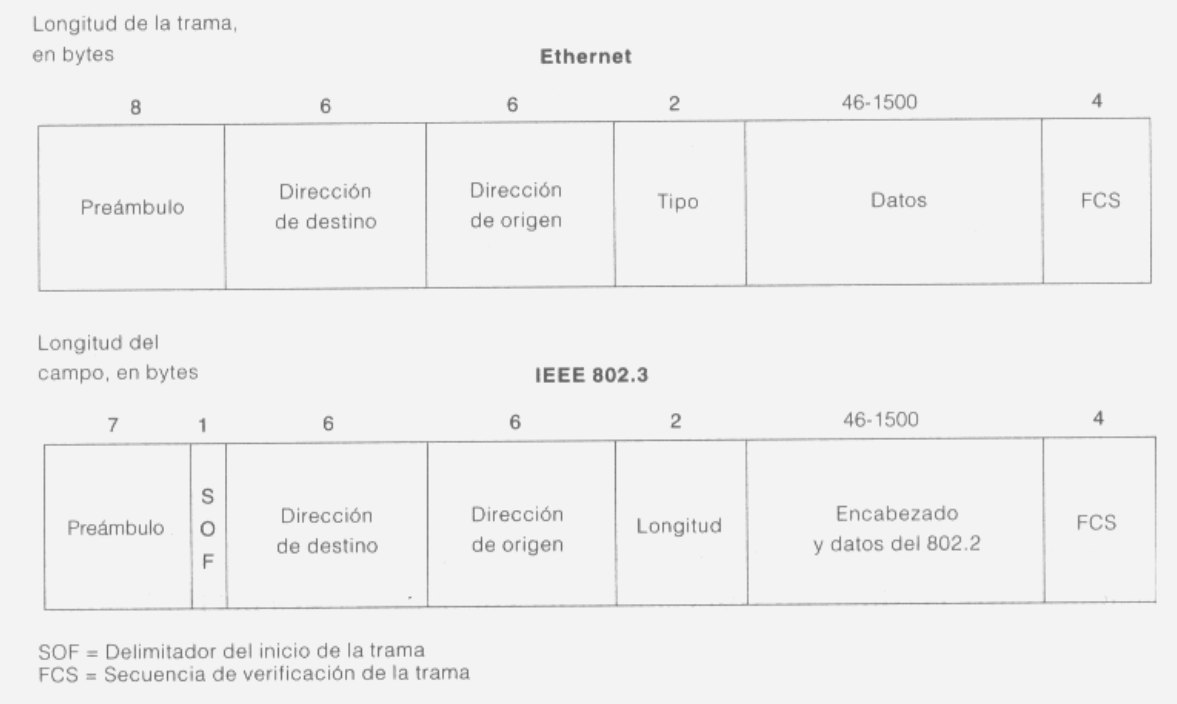


Figura 3-4. Formatos de las tramas IEEE 802.3 y Ethernet

La descripción de cada uno de los campos se mencionan a continuación:

- **Preámbulo**. Es un patrón alternado de unos y ceros que informa a las estaciones de recepción que una trama está por llegar (Ethernet o IEEE 802.3). La trama de Ethernet incluye un byte adicional que es equivalente al campo de inicio de la trama (SOF) que se especifica en la trama IEEE 802.3.

- **SOF (Inicio de la trama)**. El byte delimitador en IEEE 802.3 termina con dos bits consecutivos con valor 1, que sirven para sincronizar las porciones de recepción de tramas de todas las estaciones de la LAN. El SOF se especifica explícitamente en la trama Ethernet.

- **Direcciones de origen y destino**. Se trata de las direcciones MAC de las estaciones fuente y destino de la transmisión. Los primeros tres bytes de las direcciones MAC están especificados por el IEEE con base en el fabricante. Los tres últimos bytes son especificados por el fabricante Ethernet o IEEE 802.3. La dirección de origen es siempre una dirección de unidifusión. La dirección destino puede ser unidifusión, multidifusión o difusión.

- **Tipo (Ethernet)**. El parámetro especifica el protocolo de la capa superior que recibe los datos una vez terminado el procesamiento de Ethernet.

- **Longitud (IEEE 802.3)**.La longitud indica el número de bytes de datos, que se transfieren en la trama. El valor máximo es de 1500.

- **Datos (Ethernet)**. Terminando el procesamiento de la capa física y de la capa de enlace de datos, los datos contenidos en la trama se envían hacia un protocolo de capas superiores, que se identifica en el campo tipo. A diferencia de IEEE 802.3 Ethernet no especifica relleno alguno de datos y espera al menos 46 bytes de datos, para poder considerarlo como un paquete de transmisión.

- **Datos (IEEE 802.3)**. Una vez terminado el procesamiento de la capa física y de la capa de enlace de datos, la información se envía a un protocolo de las capas superiores, que deben definirse dentro de la porción de datos de la trama, si es que existe. Si los datos que contiene la trama no son suficientes para llenarla a su tamaño mínimo de 64 bytes, se insertan bytes de relleno para asegurar que la longitud de la trama sea de por lo menos 64 bytes.

- **FCS (*Frame Check Secuence*)**. Esta secuencia tiene un valor de 4 bytes para CRC (*Cyclic Redundancy Check*) creado por el dispositivo emisor y recalculada por el dispositivo receptor para verificar si existen tramas dañadas.

3.2.2 Implementaciones físicas de Ethernet

Existen diversas implementaciones físicas que se encuentran especificadas en el estándar IEEE 802.3, las cuales definen el tipo de cable de red, las especificaciones de longitud y la topología física que debe utilizarse para conectar nodos en la red. Dichas especificaciones se dividen en tres grandes grupos:

- **Especificación para velocidades de 10 Mbps**: 10Base2, 10Base5 , 10BaseT y 10BaseFL.

- **Especificación para velocidades de 100Mbps**: 100BaseT, 100BaseTX, 100BaseFX, 100BaseT4 y 100VG-AnyLAN.

- **Especificación para velocidades de 1000Mbps**: Gigabit Ethernet.

La notación con la que comúnmente se designan a las especificaciones anteriores se asignó con base en la forma XBaseY, cuya interpretación es la siguiente:

X	Este valor denota la velocidad de transmisión de datos.

Base	Indica que los datos se transmiten en banda base. Esto significa que transmite la información tal y como se recibe
Y	Este número denota el tipo o longitud máxima en cientos de metros del medio de transmisión correspondiente

Tabla 3-1. Notación XbaseY.

Ethernet 10Base2. También es denominado como *Thin wire, Thin coax, Thin Ethernet o Cheapernet*. Es parte del estándar IEEE 802.3, los datos son transmitidos en banda base a 10 Mbps, utiliza cable coaxial delgado de 50 ohms, la longitud máxima del segmento de cable es de casi 200 metros empleando una topología de bus. Esta tecnología fue muy popular en negocios e instalaciones pequeñas, debido a que era el método menos caro para poner en servicio una red Ethernet y es menos susceptible a la inferencia eléctrica que el par trenzado. Una desventaja de 10Base2 es que, si llegase a darse una ruptura en cualquier parte del cable, dejaría de funcionar toda la red.

Ethernet 10Base5. También es llamado Thick Ethernet o Thick wire. Es parte de la especificación de la capa física banda base IEEE 802.3, la velocidad de transmisión de datos es de 10 Mbps, utiliza cable coaxial grueso de 50 ohms, la longitud máxima de un segmento de cable es de 500 metros y se emplea en topologías de bus. Fue el primer tipo de Ethernet que se diseño y utilizó. Es relativamente difícil trabajar con esta tecnología debido a la rígidez del cable coaxial, en comparación con Ethernet 10Base2 y 10BaseT; sin embargo, fue el único Ethernet disponible durante un tiempo.

Ethernet 10BaseT. Forma parte del estándar IEEE 802.3 La transmisión de datos se efectúa en banda base a 10 Mbps, el medio de transmisión es cable UTP[2] (par trenzado sin blindaje) categoría 3, 4 ó 5. El cable consta de cuatro pares trenzados, siendo sólo dos pares utilizados, uno para transmitir y el otro para recibir. La longitud máxima de cada segmento de cable es de 100 metros y se emplea en topologías físicas tipo estrella.

Ethernet 10BaseFL. Es parte del estándar IEEE 802.3 10BaseF. Los datos se transmiten a velocidad de 10 Mpbs en banda base, el medio de transmisión es fibra óptica y la longitud máxima de cada segmento es de 2 kilómetros. La topología empleada es punto a punto.

Ethernet 100BaseTX. Especificación Fast Ethernet. La transmisión de datos es en banda base a 100 Mbps , utiliza dos tipos de cable UTP o STP[3], los cuales cuentan con dos pares de hilos trenzados, uno para recibir y el otro para transmitir. Para garantizar una adecuada temporización de la señal, la longitud de un segmento de cable no puede exceder los 100 metros. Esta tecnología es parte del estándar IEEE 802.3.

Ethernet 100BaseFX. Especificación Fast Ethernet banda base a 100 Mbps que utiliza como medio de transmisión fibra óptica multimodo. Para garantizar una temporización

[2] UTP: *Unshielded Twisted Pair*
[3] STP: *Shielded Twisted Pair*

adecuada de la señal, un enlace 100BaseFX, no puede exceder de 400 metros. Esta tecnología forma parte del estándar 802.3.

Ethernet 100BaseT4. Especificación Fast Ethernet que utiliza cuatro pares de hilos trenzados de cable UTP categorías 3,4 ó 5, uno de los pares se utiliza para la detección de colisiones y los otros tres para transmisión y recepción de datos. Para garantizar una señal de temporización adecuada un segmento 100BaseT4 no puede exceder una longitud de 100 metros. Esta tecnología está incluida en el estándar 802.3.

Ethernet Gigabit. La IEEE ha emitido extensiones del estándar 802.3 para gigabit ethernet: 802.3z y 802.3ab. El primero se aprobó en junio de 1998, el cual especifica Ethernet Gigabit sobre cable de fibra óptica y cable de cobre (no UTP). No obstante, la creación de una red de cable de fibra óptica presenta sus problemas, debido a que se tendría que cambiar el cableado de toda la infraestructura. Con la aprobación de 802.3ab (1000BaseT) en junio de 1999, las empresas pueden hacer uso de una tecnología probada y estandarizada para mejorar el flujo de tráfico en áreas de red congestionadas usando cable UTP categoría 5 como medio de transmisión. El estándar 802.3z permite la operación *half-duplex y full duplex* a 100 Mbps, el método de acceso al medio es CSMA/CD y la longitud máxima por segmento es, para fibra óptica multimodo, de 500 metros, para fibra óptica monomodo de 2 kilómetros y para cable de cobre 25 metros.

3.3 Dispositivos LAN

Dentro de los dispositivos de comunicaciones para implementar una red LAN podemos encontrar a *hubs* y *switches*. Dentro de las características principales de estos dispositivos se encuentran el dominio de colisión y de difusión (*broadcast*). El primero se refiere a que un conjunto de dispositivos comparten un mismo ancho de banda y por lo tanto existen colisiones, en caso de que dos estaciones retransmitan información al mismo tiempo. El dominio de difusión se refiere a que todos los paquetes etiquetados como difusión serán recibidos por todas las estaciones que comparten el ancho de banda.

Un *hub* o concentrador es un dispositivo que opera en la capa física y que permite extender el medio de transmisión para que más estaciones de un mismo segmento se puedan integrar a la red. Las interconexiones eléctricas se establecen dentro del concentrador. Este tipo de dispositivos no manipulan el tráfico que circula a través de ellos, por lo que las estaciones conectadas comparten el mismo dominio de colisión y difusión, además de compartir también el ancho de banda. Un inconveniente de los concentradores es que entre más estaciones se conecten a él más colisiones habrá. Todas compiten por el mismo ancho de banda, por lo que la probabilidad de colisiones aumenta.

Un *switch* es un dispositivo que opera hasta la capa 2 del modelo OSI, y permite incrementar el ancho de banda sin agregar complejidad a la red, permitiendo que cada una de las estaciones conectadas a este dispositivo tengan su propio ancho de banda sin tener que compartirlo con el resto, teniendo por puerto, su propio dominio de colisión. Todos los dispositivos conectados al mismo *switch* son parte del mismo dominio de difusión, es

decir que cuando llegue a éste una dirección difusión, ésta será repetida por todos los puertos para asegurarse de que llegue a todas las estaciones del mismo segmento.

CAPÍTULO 4. Funcionalidades de una red LAN alámbrica

De acuerdo con la red jerárquica descrita en el capítulo 2, la red LAN corresponde a la región marcada como Nivel de acceso y se explicarán las funcionalidades avanzadas, correspondientes a esta región que permiten un funcionamiento eficaz de la red LAN alámbrica.

4.1 VLAN

Inicialmente para el nivel de acceso se utilizaban enrutadores en los que se contaba con puertos independientes asignados a cada usuario, lo cual originaba insuficiencia de recursos cuando el número de usuarios aumentaba, pero se tenía la ventaja de que los enrutadores aparte de ser multiprotocolo podían detener las tormentas de difusión (*broadcast*). Posteriormente se integraron los concentradores o *hub's* que se conectaban a un puerto del enrutador y se podían conectar varios usuarios, pero la desventaja es que se compartía el mismo dominio de difusión y de colisión. Después surgió un nuevo modelo en donde se involucraba un *switch*. Aquí ya no se compartía el dominio de colisión, pero ahora el problema consistía en la expansión del dominio de difusión por la red.

Como solución a estos problemas se creó una red con agrupamientos lógicos independientes, las VLAN (*Virtual Local Area Network*) los cuales forman grupos lógicos para definir los dominios de difusión; así la red es segmentada de tal forma que los paquetes de difusión sólo afectarán al segmento lógico que los genera y no a toda la red. Aunque físicamente las estaciones estén conectadas al mismo dispositivo (*switch*) lógicamente pertenecerán a una VLAN distinta dependiendo de la configuración efectuada. Las VLAN's son implementadas en los *switches* y enrutadores para que las funcionalidades de cada uno en conjunto disminuyan la cantidad de elementos dentro de los dominios de difusión y colisión.

Para que se establezca la comunicación entre un enrutador y un *switch* con dos o más VLAN's configuradas sobre una misma interface física, es necesario un protocolo para establecer enlaces troncales.

4.2 Troncales

Un enlace troncal se da entre dos *switches* o un *switch* y un enrutador. Este tipo de enlace tiene la capacidad de transportar tráfico de múltiples VLAN's y permite la extensión de VLAN's a otros *switches*. Véase la siguiente figura.

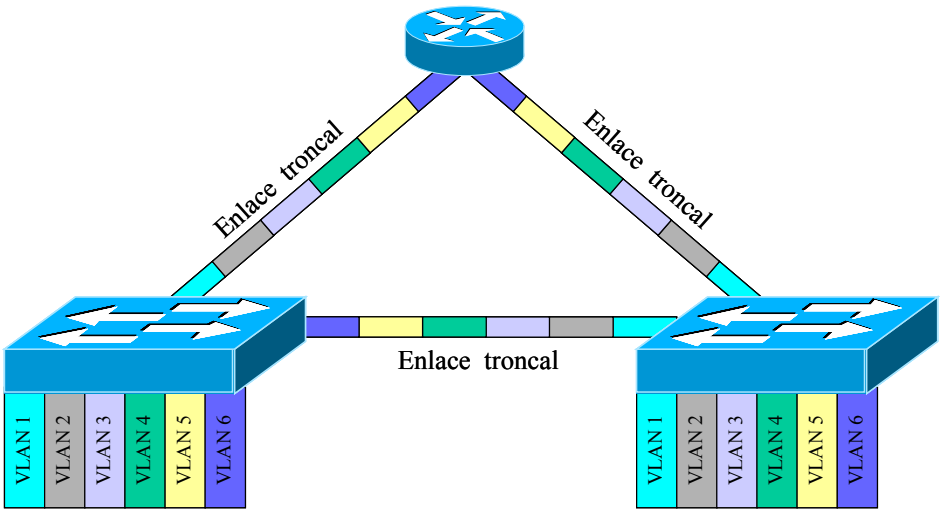


Figura 4-1. Enlaces troncales

Un enlace troncal no pertenece a ninguna VLAN y es configurado para transportar el tráfico de todas las VLAN's. Los dispositivos terminales de este tipo de enlace deben ser capaces de determinar a que VLAN pertenecen las tramas y para poder realizar esto se emplea el estándar IEEE 802.1Q o su cuasi-equivalente diseñado por cada fabricante; como ISL (*Inter- Switch Link Protocol*) diseñado por Cisco. Existen dispositivos de diferentes marcas y con el fin de que tengan interoperabilidad se estableció el estándar antes mencionado, pero es muy común que los proveedores implementen funcionalidades adicionales a las que establece la IEEE.

Para que los dispositivos determinen que información pertenece a cada VLAN es necesario que se etiquete cada una de las tramas con un identificador de VLAN, la identificación de las tramas ha sido específicamente diseñada para los *switches*. El proceso consiste en colocar un identificador en cada trama enviada por el *switch* sobre un enlace troncal, permitiendo que el swich o enrutador receptor pueda conocer a que VLAN pertenece la información y retransmitirla de manera adecuada.

4.2.1 ISL

Es un método por el cual es posible multiplexar VLAN's sobre un enlace troncal, encapsulando la trama Ethernet con un encabezado que contiene el identificador de VLAN, transportándola así entre *switches* y enrutadores. El encabezado ISL tiene una longitud de 26 bytes, además es agregada una cola de 4 bytes con CRC (*Cyclic Redundancy Check*) el cual permite detectar errores de transmisión en la recepción.

El identificador de VLAN sólo es colocado si la trama se dirige a un puerto configurado como troncal. Cuando la trama se dirige a un puerto configurado como parte de un enlace

de acceso (no configurado como troncal) el identificador no es colocado, o bien, la encapsulación ISL es eliminada si la trama provino de un enlace troncal.

En la figura de abajo los puertos A y B de la VLAN 200, han sido configurados como enlaces de acceso, es decir que no pueden recibir tramas con identificador de VLAN. Si el *switch* Y recibe trafico del puerto A con destino al puerto B, el *switch* no encapsula la trama con ISL. Ahora, si el puerto C es también parte de un enlace de acceso, configurado en la VLAN 200 y a éste se le envía información, sucede lo siguiente:

1. El *switch* Y recibe la trama e identifica a que VLAN va dirigida y el puerto hacia donde puede llegar a su destino.
2. El *switch* Y encapsula la trama con ISL, identificándola como la VLAN 200, posteriormente la envía a través del enlace troncal, y al pasar por *switches* intermedios es reenviada, tal cual, sobre enlaces troncales.
3. El *switch* Z recibe la trama, elimina la encapsulación y envía la trama al puerto C.

Debido a que ISL es una tecnología desarrollada por Cisco, sólo es posible implementarlo en dispositivos de la misma marca y no puede interactuar con otros fabricantes. Además a mediados del año 2002 Cisco anunció que su tendencia era eliminar el uso de ISL e implementar IEEE 802.1q en sus nuevos dispositivos.

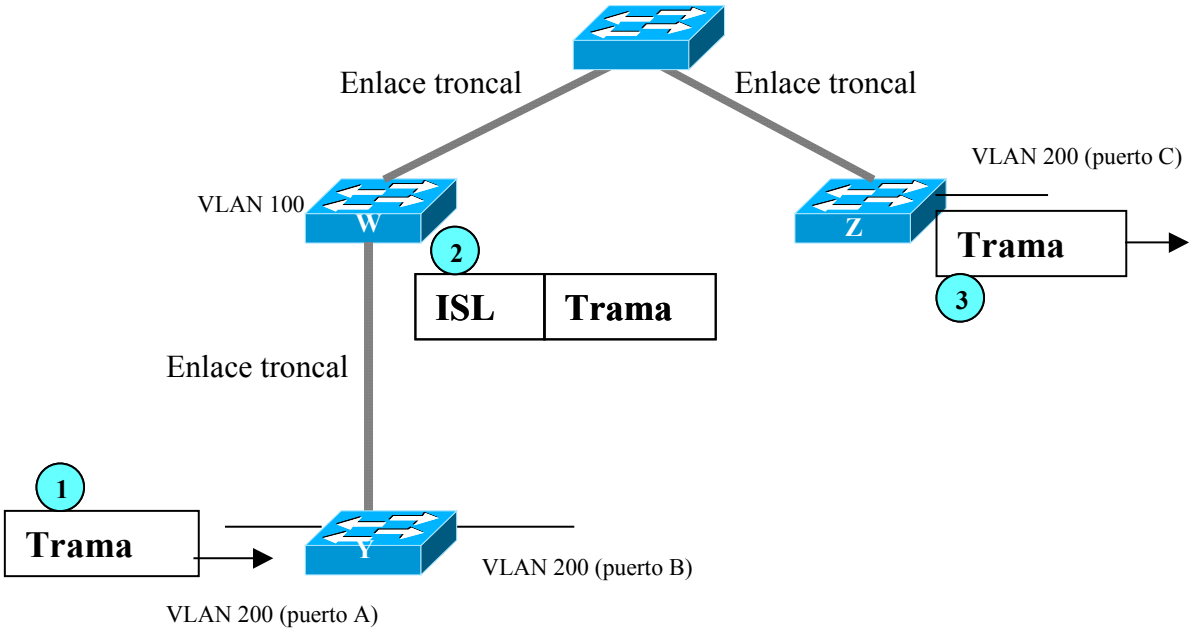


Figura 4-2. Encapsulación ISL

4.2.2 IEEE 802.1Q

El nombre oficial para este estándar es "*Standard for Virtual Bridged Local Area Networks"* y define los siguientes aspectos:

- Una arquitectura para VLAN's
- Servicios ofrecidos por VLAN's
- Protocolos y algoritmos involucrados para la provisión de dichos servicios.

Este estándar define la adición de un nuevo campo a la trama de información, cuya longitud es de 4 bytes , con los siguientes elementos:

- 2 bytes para el TPID (*Tag Protocol Identifier*) con un valor fijo de 0x8100, el cual indica que la trama es del tipo 802.1Q.
- 2 bytes para el TCI (*Tag control Information*)

  - ✓ 3-bits para prioridad de usuario
  - ✓ 1-bit de formato canónico (*CFI Indicator*)
  - ✓ 12 bits para el identificador de VLAN (VID) que únicamente identifica la VLAN a la cual pertenece la trama.

Tanto ISL como IEEE 802.1Q agregan campos a la trama, pero la diferencia es que el primero únicamente agrega a la trama un encabezado y una cola, sin modificar la trama de Ethernet; mientras que el segundo incrusta el nuevo campo en el interior de la misma, modificándola. Con la utilización de este último método es posible enviar una trama con identificador de VLAN tanto en el enlace troncal como en el enlace de acceso.

4.3 Redundancia

El principal propósito de las redes es proveer a los usuarios conectividad en cualquier momento. Comúnmente se utilizan enlaces que no garantizan la conectividad de los usuarios, por ejemplo en la siguiente figura se muestra una topología en la que el usuario conectado al enrutador 1 (operando como *default gateway* o puerta de enlace) mediante un *switch*, intenta obtener información del servidor A, pero si se produjera una falla en el enlace hacia el enrutador 1, la comunicación deseada sería imposible.

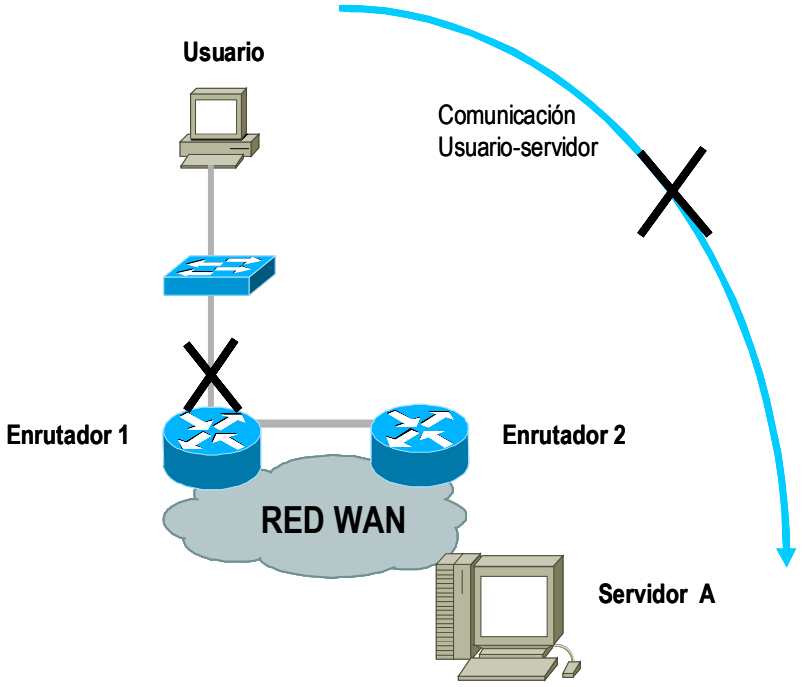


Figura 4-3. Enlace no redundante

Para evitar lo anterior y asegurar la conectividad, se utilizan enlaces redundantes, con protocolos como HSRP y *Spanning Tree*, a continuación explicados.

HSRP (*Hot Standby Router Protocol*) es un protocolo desarrollado por Cisco que impide que la ruta que siguen los paquetes IP se rompa debido a la falla del enrutador que opera como *default gateway,* y consiste en un conjunto de enrutadores que poseen sus propias direcciones IP y MAC pero que a su vez comparten otra direccion IP y otra MAC virtuales, por lo que lógicamente representan un sólo enrutador (enrutador virtual) el cual será visto por los usuarios como *default gateway*. El funcionamiento consta de que un enrutador del grupo es elegido responsable (enrutador activo) para enrutar los paquetes enviados por los usuarios al enrutador virtual, mientras que el otro permanecerá en *standby*. En caso de que el enrutador activo por alguna razón deje de funcionar, el que permanece en *standby*, asumirá las responsabilidades del activo.

La comunicación de enrutadores con HSRP es a través de paquetes llamados *Hello's*. Estos paquetes son enviados a la dirección IP *multicast* 224.0.0.2 (dirección reservada para comunicar a todos los enrutadores) sobre UDP (*User Datagram Protocol*) por el puerto 1985. El enrutador activo origina los *Hello's* con la IP propia y con la MAC compartida, mientras que el enrutador en *standby* envía los mismos paquetes con su IP y MAC propias, esto permite que ambos enrutadores puedan identificarse mutuamente. Cuando el enrutador en *standby* deja de recibir los *Hello's* del enrutador activo, entonces el primero asume las direcciones IP y MAC virtuales, convirtiéndose en el activo.

4.3.1 Implementación de HSRP

Una implementación típica de este protocolo es la que se muestra en la siguiente figura.

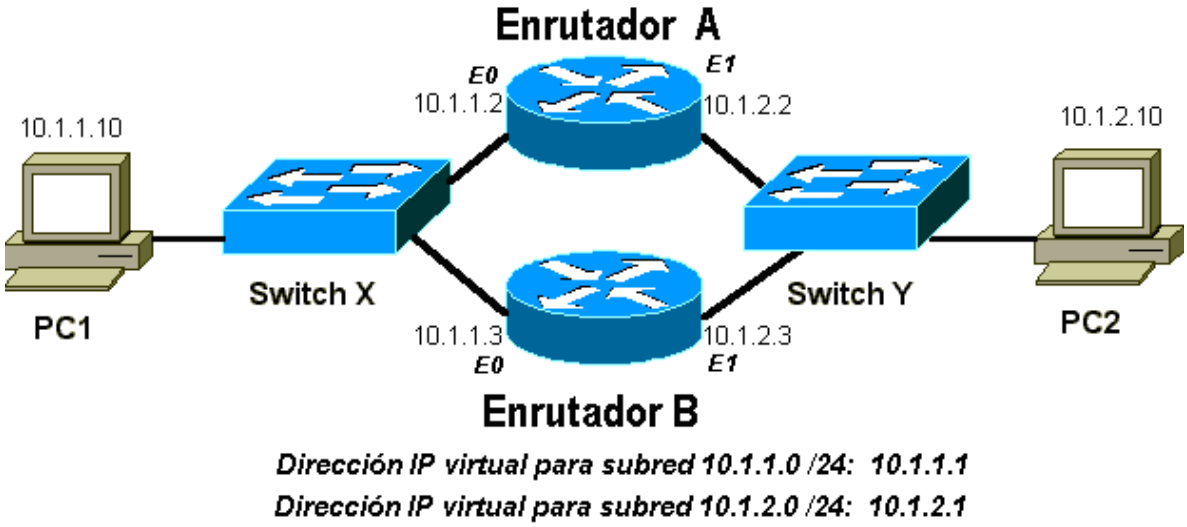


Figura 4-4. Topología redundante

Las direcciones correspondientes a cada PC se muestran en la siguiente tabla:

Dispositivo	MAC Address	IP Address	Máscara de subred	Default Gateway (IP virtual)
PC1	0000.0c00.0001	10.1.1.10	255.255.255.0	10.1.1.1
PC2	0000.0c00.1110	10.1.2.10	255.255.255.0	10.1.2.1

Tabla 4-1. Direccionamiento de dispositivos

La configuración de los enrutadores se muestra a continuación:

Configuración para el enrutador A (Enrutador Activo):

```
interface ethernet 0
  ip address 10.1.1.2 255.255.255.0      (comando que define la dirección IP de la interface)
    mac-address 4000.0000.0010           (comando no requerido, utilizado solo para fines ilustrativos)
    standby 1 ip 10.1.1.1                (comando que define cuál será la dirección IP vitual para la interface)
    standby 1 priority 200               (comando que establece que este enrutador será el activo para la interface ethernet 0, debido a que la prioridad es mayor a la definida en el otro enrutador)
interface ethernet 1
    ip address 10.1.2.2 255.255.255.0
```

```
   mac-address 4000.0000.0011
   standby 1 ip 10.1.2.1
   standby 1 priority 200
```

Configuración para el enrutador B (Enrutador en *standby*):

```
interface ethernet 0
   ip address 10.1.1.3 255.255.225.0
   mac-address 4000.0000.0020
   standby 1 ip 10.1.1.1
  standby 1 priority 100

interface ethernet 1
    ip address 10.1.2.3 255.255.255.0
    mac-address 4000.0000.0021
    standby 1 ip 10.1.2.1
    standby 1 priority 100
```

Es importante recordar que las configuraciones anteriores son únicamente para dispositivos Cisco.

4.4 Spanning tree

STP (*Spanning Tree Protocol*) es un protocolo de capa dos diseñado para *switches*, cuyo propósito principal es evitar *loops* en redes con topología redundante. La norma referente a este protocolo es la IEEE 802.1d.

Para entender el funcionamiento de STP es necesario entender el funcionamiento de un *switch* sin este protocolo habilitado. Por definición un *switch* tiene las siguientes características:

- No modifica las tramas que recibe y son reenviadas por él.
- Debe reenviar los paquetes difisión (*broadcast)* por todos sus puertos excepto por el que los recibió.
- Si la dirección destino es desconocida, el *switch* reenvía la trama por todos los puertos, excepto por el que la recibió.
- El *switch* aprende las direcciones MAC de los dispositivos conectados a él y hace una tabla donde se asocian dichas direcciones con el puerto correspondiente. Con esto se logra que cuando llegue una trama con dirección MAC destino conocida por el *switch*, éste la reenviará por el puerto correspondiente.

En la figura de abajo se muestra un esquema en el que la estación A intenta mandar un paquete a la estación B, y el proceso a efectuarse es el siguiente:

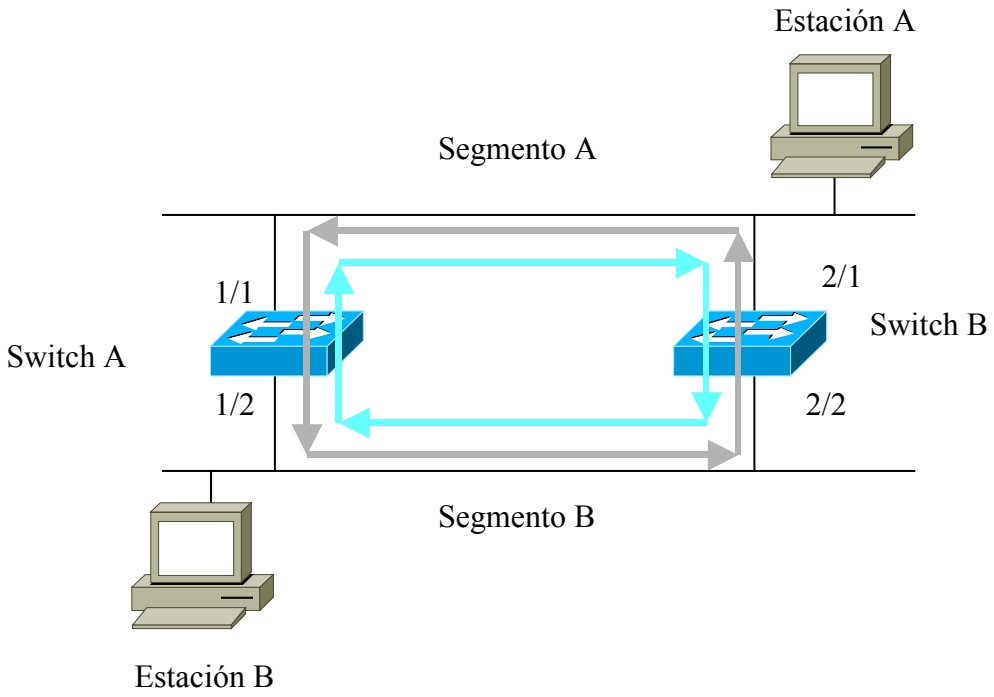


Figura 4-5. Generación de *loops* en la topología

- La estación A transmite la trama al segmento B y ambos *switches* la reciben uno por el puerto 1/1 y el otro por el 2/1. Los *switches* A y B registran la dirección MAC de la estación A y la registran asociándola a los puertos antes mencionados.

- Ambos *switches* reenvían la trama al segmento B y además, también la reciben los *switches* A y B, registrando nuevamente la dirección MAC por los puertos 1/2 y 2/2 respectivamente.

- Lo anterior ocasiona que cuando la estación A envié una trama a B, ésta la reciba pero además será devuelta al segmento A y viceversa. De esta manera es como se genera el *loop.*

- Si lo que se enviara fuera un paquete de difusión (*broadcast*) el problema originado sería de gravedad, ya que la red se inundaría de paquetes y provocaría una falla por sobrecarga en los *switches*.

El STP ha sido creado para solucionar los problemas antes mencionados. Este protocolo determina dónde existen *loops* de este tipo y apaga los enlaces redundantes, asegurándose que sólo exista una ruta para cada destino. Esto lo hace ejecutando un algoritmo llamado STA (*Spanning Tree Algorithm*). Véase la siguiente figura.

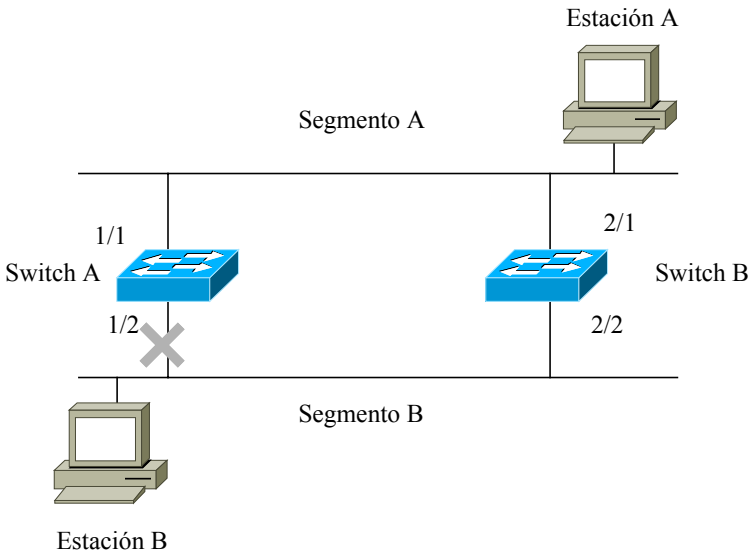


Figura 4-6. Eliminación de enlaces redundantes

En caso de que el enlace que quedó activo falle, el *switch* automáticamente dará de alta el enlace que se había eliminado previamente.

Todos los *switches* contenidos en una red LAN participan en el proceso de STP, intercambiando información por medio de paquetes llamados BPDU (*Bridge Protocol Data Unit*) lo cual trae como resultado lo siguiente:

- La elección de un *switch* raíz que establece la topología STP.
- La elección de un *switch* para cada segmento.
- La eliminación de *loops*, dando de baja los enlaces redundantes.

Los BPDU's son enviados cada dos segundos.

STP utiliza dos conceptos básicos para elaborar la topología redundante libre de loops:

- Costo de la ruta
- Identificador (ID)

El costo de la ruta es un valor establecido por el protocolo para determinar la ruta óptima. Este costo es calculado con base en la velocidad de transmisión del enlace, ancho de banda y en el número de enlaces que el paquete BPDU tiene que atravesar. El puerto que tiene el costo más bajo es el que permanece activo y todos los demás son dados de baja.

El primer paso para la liberación de *loops* es elegir a un *switch* raíz, el cual es el punto de referencia para que todos los demás *switches* determinen si existen *loops* en la red. En principio todos los *switches* asumen que son el raíz y generan su respectivo ID, el cual está compuesto por los siguientes componentes:

- 2 bytes de prioridad. El switch coloca un número que por omisión, es el mismo para todos los *switches*, cuyo valor es : 32,768, para equipos Cisco. Pero también puede ser modificado por el administrador de red.

- 6 bytes. Corresponden a la dirección MAC del *switch*.

La combinación de estos dos números determinan cual *switch* será el raíz. El primer criterio a tomar en cuenta en la comparación es la prioridad, pero si ésta es igual en todos los dispositivos, el *switch* raíz será el de menor dirección MAC. Después de que el *switch* raíz ha sido elegido, todos los demás deben buscar la asociación con él.

Para cada segmento de red se define un *switch* designado, con base en el costo de la ruta, es decir que el *switch* designado será el que tenga el costo de ruta menor. En la siguiente figura se muestra que el *switch* A y B forman parte del segmento 1, el puerto A-1/1 tiene un costo de ruta igual a 0, porque pertenece al *switch* raíz, mientras que el puerto B-1/1 tiene un costo de 19, por lo que el *switch* A se convierte en el *switch* designado. Análogamente se determina el *switch* designado para el segmento 2. El enlace entre los *switches* B y C, forman el segmento 3 y ambos tienen puertos con un costo de ruta de 19; por lo que el siguiente criterio a tomar en cuenta es el ID; el cual para B es 32,768.BB-BB-BB-BB-BB-BB y para C es 32,768.CC-CC-CC-CC-CC-CC, por lo tanto el *switch* designado para el segmento 3 sería el B, por tener el menor ID.

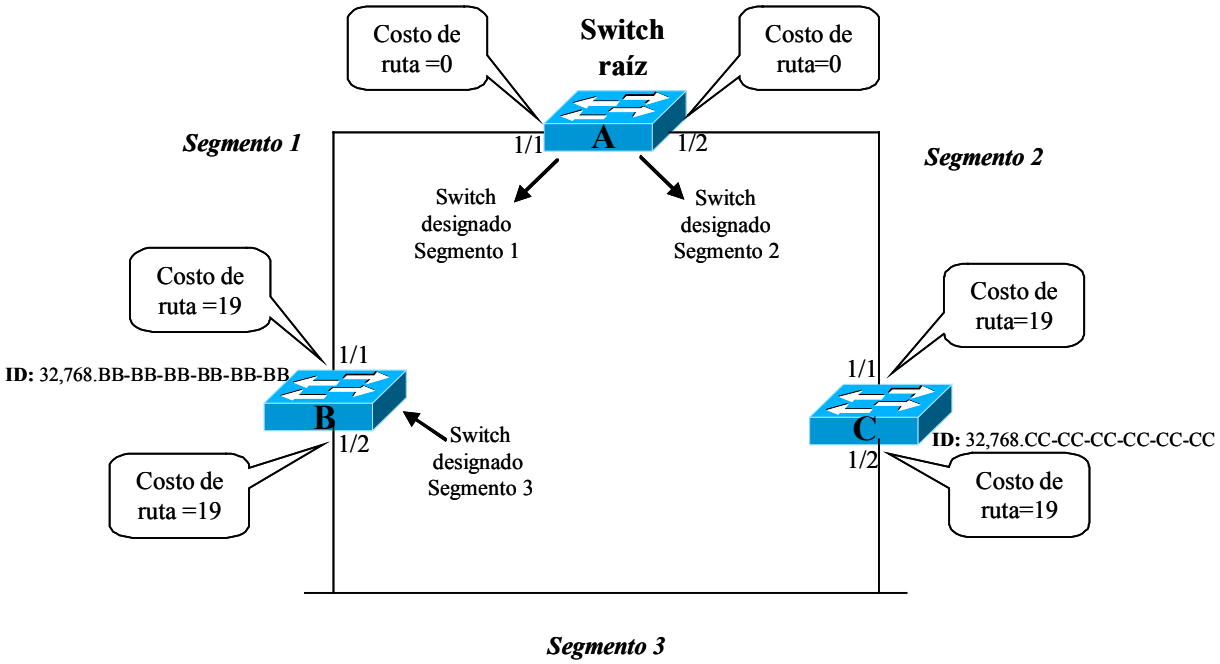


Figura 4-7. Elección del *switch* designado por segmento

Una vez que los *switches* de cada segmento determinaron cual de ellos será el *switch* designado , establecen una relación mediante la cual, cada *switch* verifica si existe alguna ruta redundante entre éste y el *switch* raíz; si recibe BPDU's en múltiples puertos indica que existe redundancia y entonces ésta debe ser eliminada.

Con STP los puertos del *switch* pueden tener diferentes estados:

- *Bloking*. Todos los puertos empiezan a operar en este modo, mediante el cual previenen al *switch* de la probable creación de un *loop*. El puerto permanece en este estado, hasta que el proceso de STP determina que hay otra ruta más eficiente hacia el *switch* raíz.

- *Listening*. En este estado el puerto determina si existen otras rutas hacia el *switch* raíz. Durante este estado el *switch* puede visualizar las tramas sin enviar o recibir datos; tampoco está permitido agregar información a la tabla de direcciones MAC.

- *Learning*. Este estado es similar al anterior, debido a que no puede enviar ni recibir datos, pero sí puede agregar información a la tabla de direcciones MAC.

- *Forwarding*. Significa que el puerto está capacitado para enviar y recibir datos.

CAPÍTULO 5. Estandarización de las redes LAN inalámbricas

Las redes WLAN (*Wireless Local Area Network*) son compatibles con los estándares genéricos aplicables al mundo de las LAN alámbricas (IEEE 802.3 ó equivalentes) pero necesitan una normativa específica adicional que defina el uso de los recursos radioeléctricos. Estas normativas definen de forma detallada los protocolos de la subcapa física y de la capa de Control de Acceso al Medio (MAC).

En 1990, se asigna un comité para el estándar IEEE 802.11 que empieza a trabajar para generar una norma de redes LAN inalámbricas. Desde entonces varios organismos internacionales han desarrollado una amplia actividad en la estandarización.

En 1992 se crea *Winforum*, consorcio encabezado por *Apple* y formado por empresas del sector de las telecomunicaciones y de la informática, para conseguir bandas de frecuencia para los sistemas PCS (*Personal Communications Systems*). En ese mismo año, la ETSI (*European Telecommunications Standards Institute*) a través del comité ETSI-RES 10, crea una norma, para redes LAN, denominada HiperLAN (*High Performance LAN*). En 1993 también se constituye la IRDA (*Infrared Data Association*) para promover el desarrollo de las redes inalámbricas basadas en enlaces por infrarrojos.

En 1996, finalmente, un grupo de empresas del sector de informática móvil (*Mobile Computing*) y de servicios forman el WLI Forum (*Wireless LAN Interoperability Forum*) para potencializar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Entre los miembros fundadores de WLI Forum se encuentran empresas como ALPS Electronic, AMP, Data General, Contron, Seiko, Epson y Zenith Data Systems.

La función principal de las redes inalámbricas es proporcionar conectividad y acceso a las tradicionales redes cableadas, como si se tratara de una extensión de estas últimas, pero con la flexibilidad y movilidad que ofrecen las primeras. El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE 802.11 a mediados de 1997, en éste se encuentran las especificaciones técnicas que se deben cumplir tanto en los dispositivos como en el diseño de una red de área local inalámbrica. Otro de los estándares definidos para este tipo de redes son: *WLIF, Home RF, Home RF2, HyperLAN y Bluetooth.*

La norma 802.11 ha sufrido diferentes extensiones para especificar con más detalle cada una de las tecnologías, a continuación se mencionan dichas extensiones:

- **802.11**. Define dos tecnologías FHHS (*Frecuency Hopped Spread Spectrum*) y DSSS (*Direct Sequence Spread Spectrum*) para velocidades de 2Mbps y 1Mbps.
- **802.11b.** Es el estándar que encabeza los desarrollos actuales de WLAN, opera en la banda de 2.4 GHz y emplea DSSS y alcanza velocidades de 1,2.2,5.5 y 11 Mbps.
- **802.11a.** Es una evolución del 802.11b, opera en la banda de 5GHz y ofrece una velocidad de transmisión de hasta 54 Mbps. Utiliza OFDM (*Orthogonal Frecuency*

División Multiplexing). Este estándar compite directamente con *HiperLAN 2*, estándar de ETSI (*European telecommunications Standars Institute*).

- **802.11g**. Fue aprobada en Junio del 2003, el cual opera con OFDM y alcanza velocidades de transmisión de 54 Mbps en la banda de 2.4GHz. Permite interoperabilidad con el estándar 802.11b.

En este capítulo se explicará el contenido del estándar IEEE 802.11b , ya que el objetivo de esta tesis es la comparación de una red alámbrica con una inalámbrica basada en dicho estándar.

5.1 Estándar IEEE 802.11b

En la actualidad, se está extendiendo la implantación del estándar en ámbitos empresariales, docentes e incluso domésticos, llevando consigo una gran libertad de movimiento en las comunicaciones.

El estándar define dos elementos fundamentales para una red: un cliente o una estación inalámbrica, la cual usualmente es una PC, laptop o PDA (*Personal Digital Assistant*) con una tarjeta de red inalámbrica también llamada WNIC (*Wireless Network Interface Card*) y un punto de acceso, el cual actúa como un puente entre la red alámbrica e inalámbrica. Estos elementos pueden formar dos tipos de topologías:

- **Ad-Hoc**. Cada estación se puede comunicar con todas los demás, sin necesidad de utilizar un punto de acceso como medio de enlace; siempre y cuando se encuentren dentro de la misma área de cobertura. A este tipo de topología se le denomina también IBSS (*Independent Basic Service Set*) Véase la siguiente figura.

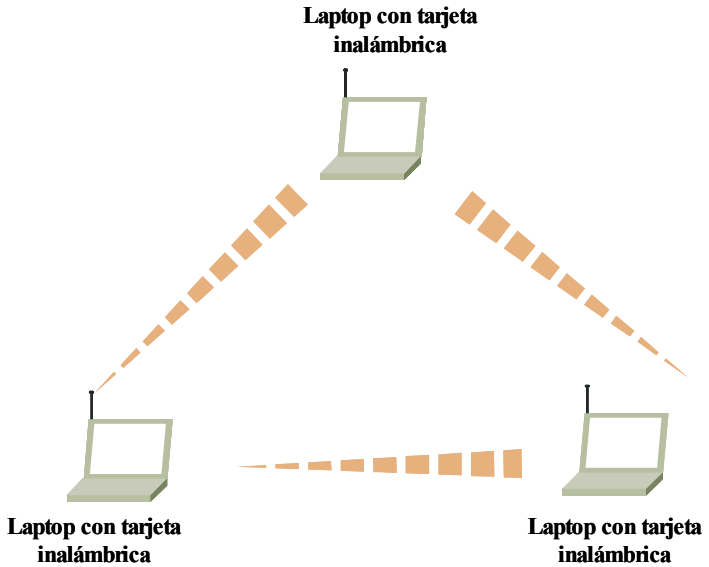


Figura 5-1. Topología Ad hoc

- **Infraestructura**. Topología que consiste de al menos un punto de acceso, mediante el cual se comunican varias estaciones. A la infraestructura con un solo punto de acceso y varias estaciones inalámbricas le llama BSS (*Basis Service Set*) y el ESS (*Extended Service Set*) es un conjunto de BSS's donde los puntos de acceso se comunican entre sí, para intercambiar información. En la siguiente figura se ilustra un BSS.

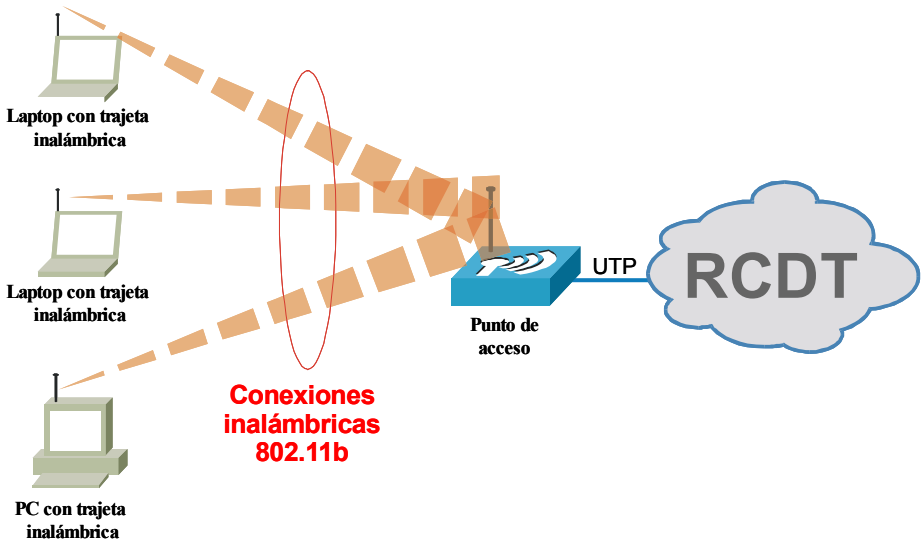


Figura 5-2. Topología Infraestructura

El estándar IEEE 802.11b opera en la banda de 2.4 Ghz (2.400 –2.4835 GHz) y está diseñado para transmitir a velocidades de 1, 2, 5.5 y 11 Mbps. Dicho estándar está definido en las dos primeras capas del modelo OSI, como se muestra en la siguiente figura.

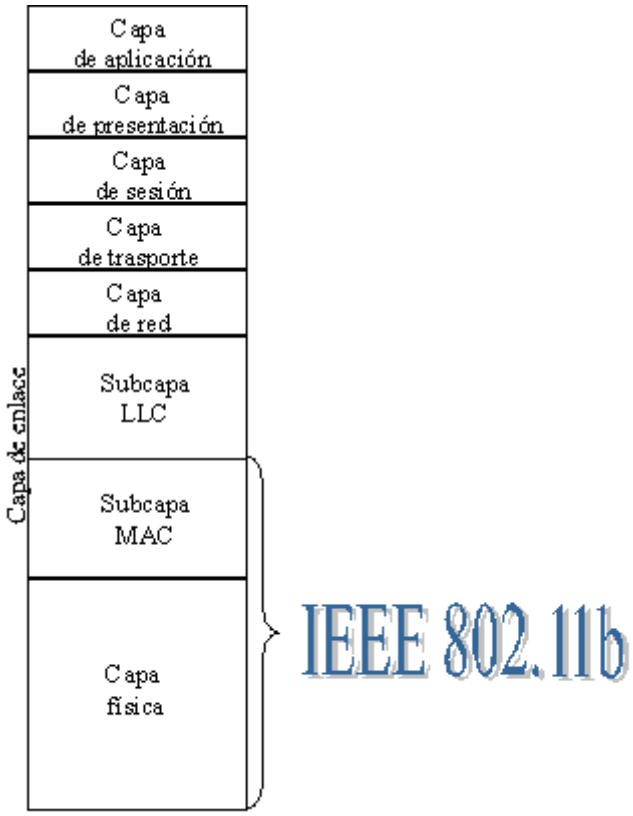


Figura 5-3. Ubicación del estándar IEEE 802.11b en el modelo OSI

5.1.1 Capa física

Las especificaciones de capa física del estándar 802.11b determinan las características de la transmisión de datos. La técnica de transmisión definida es: DSSS (*Direct Sequence Spread Spectrum*) la cual está basada en el espectro expandido que consiste en expandir la información de la señal sobre un ancho de banda mayor al de la señal original. Los datos fuente por transmitir se someten primero a una operación OR exclusiva (XOR) con una secuencia binaria pseudoaleatoria, es decir, cada bit de información se combina con la secuencia pseudoaleatoria, para lograr una secuencia mayor a la original. La secuencia pseudoaleatoria utilizada para el procesamiento de cada uno de los bits de información pueden ser la secuencia de Barker o CCK, dependiendo de la velocidad de transmisión. En la siguiente figura se muestra como se efectúa el procesamiento de la señal, con la secuencia de Barker, la cual tiene la siguiente forma: 10110111000.

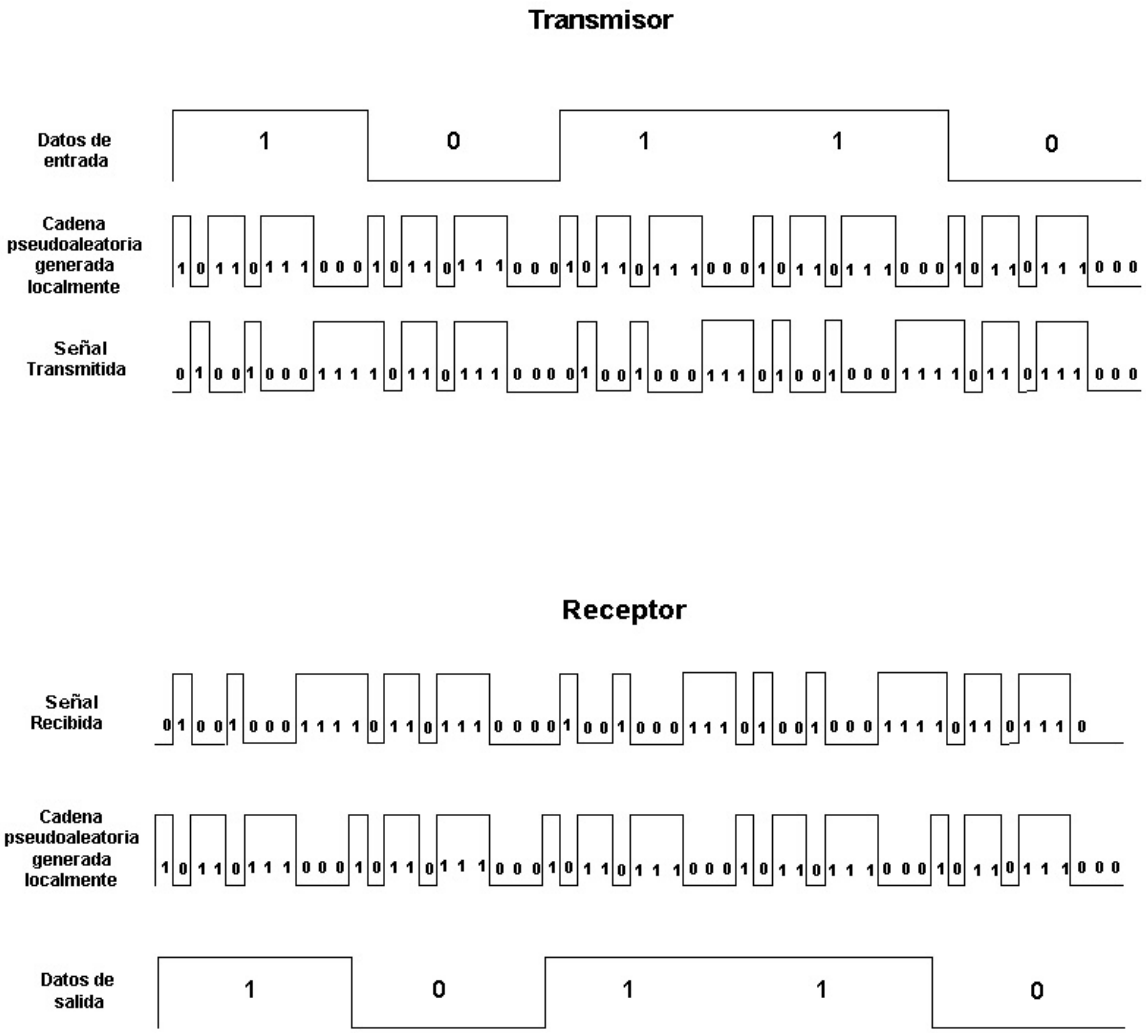


Figura 5-4. Procesamiento de la señal con DSSS

Cada secuencia de 11 bits representa un solo bit de datos (1 ó 0) y se convierte en una forma de onda llamada símbolo. Estos símbolos son transmitidos con una tasa de 1MSps (Mega símbolos por segundo) usando la técnica de modulación BPSK (*Binary Phase Shift Keying*). En el caso de 2 Mbps, se usa una modulación más sofisticada llamada QPSK (*Quadrature Phase Shift Keying*) que dobla la tasa de datos que soporta BPSK mejorando la eficiencia en el uso del ancho de banda.

Para incrementar la tasa de transmisión de datos en el estándar, se desarrollaron técnicas de codificación avanzadas, mejor que la secuencia de Barker. El IEEE 802.11b especifica la técnica de codificación CCK (*Complementary Code Keying*) que consiste en un conjunto de 64 palabras código de 8 bits, estas palabras código tienen propiedades matemáticas únicas que les permiten distinguirse correctamente una de otra, incluso en presencia de un ruido importante. La tasa de 5.5 Mbps usa el CCK para codificar 4 bits por portadora, mientras que la tasa de 11 Mbps codifica 8 bits por portadora. Ambas velocidades usan la técnica de modulación QPSK y señal a 1.375 MSps (véase la tabla 5-1). El estándar también define un

DRS (*Dynamic Rate Shifting*) el cual permite ajustar automáticamente la velocidad de transmisión, de acuerdo con la cantidad de ruido, es decir que los dispositivos transmitirán en las velocidades bajas, 5.5, 2 y 1 Mbps en condiciones de ruido y cuando el nivel de éste baje la velocidad aumentará automáticamente.

Especificaciones de transmisión de datos IEEE 802.11b				
Tasa de transmisión de datos	**Longitud de código [bits]**	**Modulación**	**Tasa de transmisión de símbolo**	**Bits/Símbolo**
1 Mbps	11 (Secuencia de Barker)	BPSK	1 MSps	1
2 Mbps	11 (Secuencia de Barker)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Tabla 5-1. Especificaciones de transmisión de datos

La técnica DSSS o Técnica de Espectro Expandido divide la banda en 14 canales, los cuales tienen diferente disponibilidad según la regulación de cada país. Véase la siguiente tabla.

Identificador de canal	**Frecuencia central**	**Normas por región**				
		Américas	**EMEA**[1]	**Israel**	**China**	**Japón**
1	2412	X	X	-	X	X
2	2417	X	X	-	X	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X

[1] EMEA. *Europe, Middle East and Africa*

8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	-	X	X
11	2462	X	X	-	X	X
12	2467	-	X	-	-	X
13	2472	-	-	-	-	X
14	2484	-	-	-	-	X

Tabla 5-2. Disponibilidad de canales según la región geográfica

México está incluido en la región de Américas, por lo que sólo es permitido el uso de 11 canales de transmisión.

El ancho de banda total disponible es de 83.5 MHz (2.400-2.4835 GHz) dividido en 14 canales de 22 MHz cada uno; la separación entre frecuencias centrales es de 5MHz, con excepción del último canal, cuyo espaciamiento es de 6 MHz. De lo anterior se deduce que sólo tres de los 14 canales (1, 6 y 11) no se interfieren entre sí. Véase la siguiente figura.

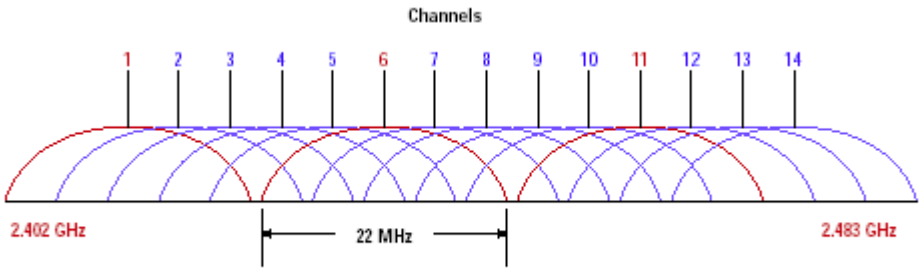


Figura 5-5. Distribución de canales

Lo anterior debe ser considerado para lograr un buen diseño en las redes LAN inalámbricas, las antenas utilizadas deben radiar únicamente en los canales 1, 6 y 11; evitando que exista traslape entre zonas de cobertura utilizando el mismo canal de transmisión. En la siguiente figura se muestran varias regiones transmitiendo en diferente canal, sin adyacencia con regiones de canales iguales.

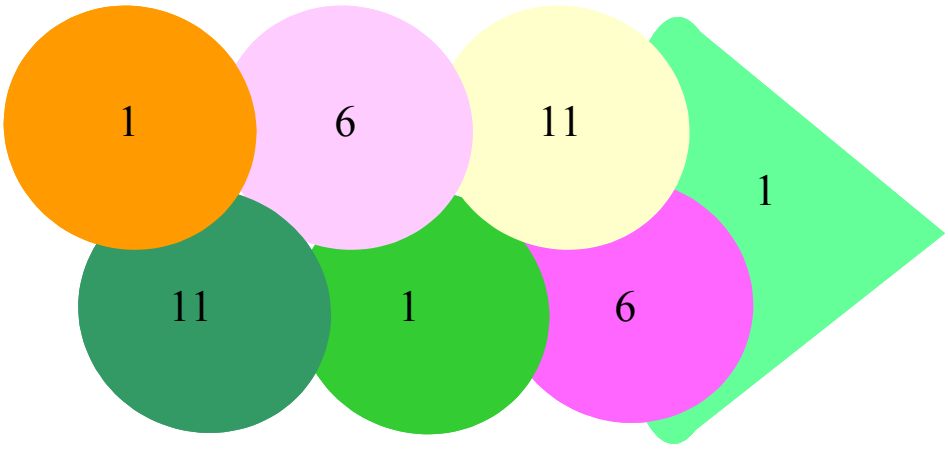


Figura 6-6. Distribución de canales independientes

5.1.1.1 PLCP y PMD

La capa física se encuentra dividida en dos subcapas PDM (*Physical Medium Dependent*) y PLCP (*Physical Layer Convergence Protocol*); la primera tiene la función de definir las características de transmisión y recepción en el medio inalámbrico; la capa PLCP, es llamada así por utilizar dicho protocolo, el cual se encarga de establecer una comunicación entre las subcapas PDM y MAC. Esta subcapa puede emplear dos formatos de trama una con preámbulo largo y otra con preámbulo corto, desarrollado posteriormente para mejorar el rendimiento de la red. Véase las siguientes figuras.

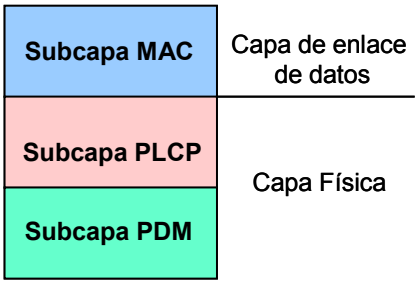


Figura 5-7. Subdivisión de capa física

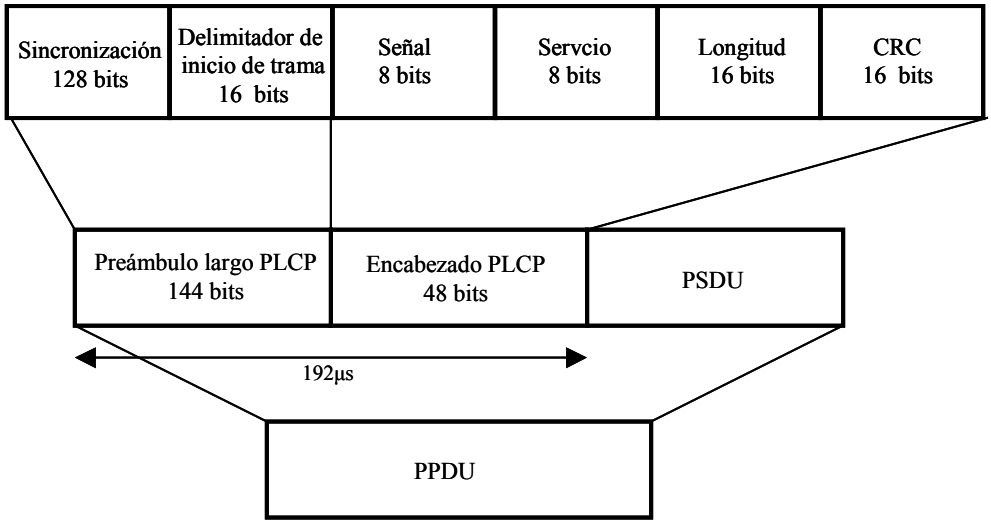


Figura 5-8. Formato de trama con preámbulos largos

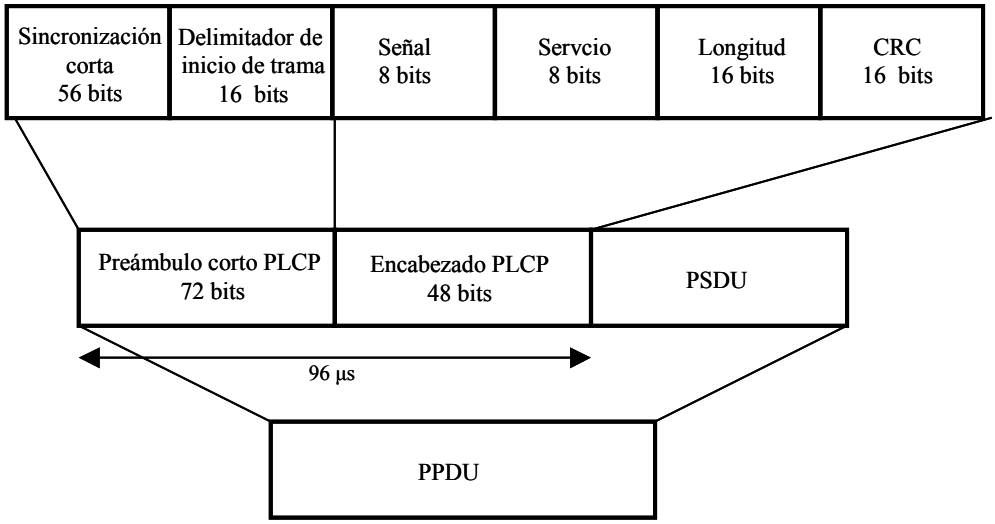


Figura 5-9. Formato de trama con preámbulos cortos

El preámbulo PLCP consiste de dos campos; uno de sincronización de la señal, de 128 bits para preámbulo largo y 56 bits para preámbulo corto; y el Delimitador de inicio de trama, como su nombre lo indica, delimita el inicio de trama. Ambos son transmitidos a 1 Mbps con DBPSK.

El encabezado PLCP, contiene 48 bits de información y consta de 4 campos; Señal, que indica qué tan rápido serán transmitidos los datos contenidos en el PSDU (*PLCP Service Data Unit*); Servicio, indica la modulación empleada para el PSDU; Longitud, indica la longitud del campo PSDU y el CRC (*Cyclic Redundancy Check*) valor calculado, de

acuerdo con la información de los cuatro campos del encabezado para la detección de errores. El contenido del encabezado es el mismo para preámbulo largo y corto, sin embargo para el primero la información es transmitida a 1 Mbps con DBPSK y para el segundo a 2 Mbps con DQPSK.

Los datos contenidos en el PSDU pueden ser transmitidos con velocidades de 2, 5.5 y 11 Mbps para preámbulo corto y a 1, 2,5.5 y 11 Mbps para preámbulo largo.

La trama completa compuesta del preámbulo PLCP, encabezado y PSDU, es denominada PPDU (*PLCP Protocol Data Unit*).

5.1.2 Subcapa MAC

5.1.2.1 Formato de tramas MAC

La trama de la subcapa MAC es llamada MPDU (*MAC Protocol Data Unit*) y el formato general de la misma se muestra en la siguiente figura.

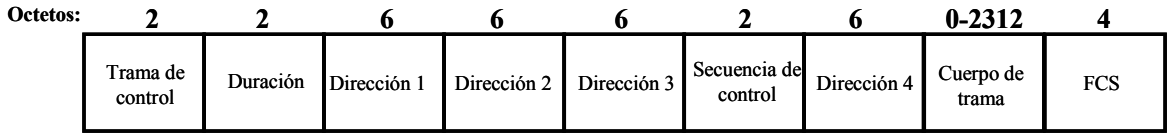


Figura 5-10. Formato general de la trama MAC

Cada uno de los campos definidos en la trama anterior serán explicados brevemente a continuación.

El campo denominado Trama de control, tiene una longitud de dos bytes y su formato se muestra en la siguiente figura.

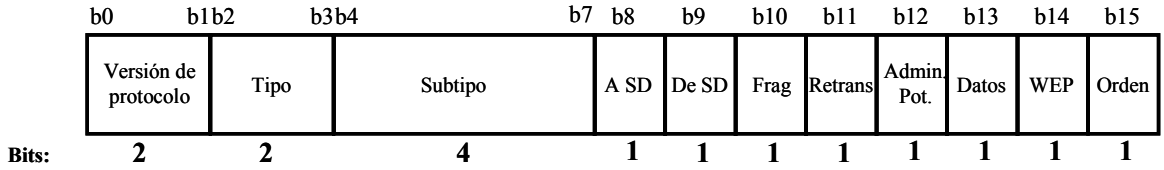


Figura 5-11. Formato de la trama de control

La descripción de los subcampos que componen la trama de control se mencionan enseguida:

- **Versión de protocolo**. Es un campo que indica la versión de protocolo y su valor binario es 0.

- **Tipo /subtipo**. Campos que identifican si la trama es de datos, de control o de administración (*Frames of Data, Control or Management*). Las tramas de administración únicamente contienen información de gestión como por ejemplo, servicios de asociación o información pendiente por transmitir en el punto de acceso; las tramas de control se utilizan para controlar el acceso al medio (ACK, RTS, CTS[2]) y las tramas de datos, como su nombre lo indica, son datos que regularmente provienen de capas superiores. En la siguiente tabla se indican los valores que puede tomar cada uno de estos campos.

Tipo b2 b3	Descripción	Subtipo b4 b5 b6 b7	Descripción
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message(ATIM)

[2] ACK. Acknowledge; RTS: Request To Send
CTS. Clear to Send.

00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	Power save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data +CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF- Ack (no data)
10	Data	0110	CF- Poll (no data)
10	Data	0111	CF- Ack + CF- Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Tabla 5-3. Tipos de tramas

- **A SD / De SD**. Indica si la trama envía o recibe información del sistema de distribución o red alámbrica.
- **Fragmentación**. Su valor es 1 si la trama MAC está fragmentada.
- **Retransmisión**. Su valor es 1 si la trama es una retransmisión.
- **Administración de potencia**. Se activa si la estación utiliza el modo de ahorro de energía
- **Datos**. Se activa si la estación tiene tramas pendientes por transmitir.
- **WEP**. Su valor es 1 si la clave de cifrado WEP[3] ha sido aplicada a los bits de información.
- **Orden**. Se activa cuando se utiliza el servicio de reordenamiento estricto para la transmisión.

[3] WEP. *Wired Equivalent Privacy*

De acuerdo con la figura 5-10 el segundo campo de la trama MAC es el denominado Duración, el cual indica la duración de la transmisión de la trama. Este valor es utilizado para informar a todas las estaciones durante cuanto tiempo estará reservado el medio.

Los valores de los cuatro campos referentes a las direcciones 1, 2, 3 y 4 de la trama MAC, dependen de los valores dados en los campos A SD y De SD de la trama de control.

A SD	De SD	Dirección 1	Dirección 2	Dirección 3	Dirección 4
0	0	DD	DO	SSID	N/A
0	1	DD	SSID	DO	N/A
1	0	SSID	DO	DD	N/A
1	1	DR	DT	DD	DO

Tabla 5-4. Valores para los campos de direcciones de la trama MAC

Donde:

DD. Dirección Destino
DO. Dirección Origen
DT. Dirección Transmisora
DR. Dirección Receptora
SSID. *Service Set Identifier*

El campo de Secuencia de control de la trama MAC, contiene tanto el Número de secuencia como el número de fragmento en la trama que se está enviando. El Número de secuencia empieza en 0 e identifica cada MSDU[4] con un valor único, si los paquetes son fragmentados cada fragmento permanece con el mismo número de secuencia. En el campo de Número de fragmento se contabilizan los fragmentos empezando desde 0. Cuando no hay fragmentación de paquetes el número de fragmento permanecerá en 0. Véase la siguiente figura.

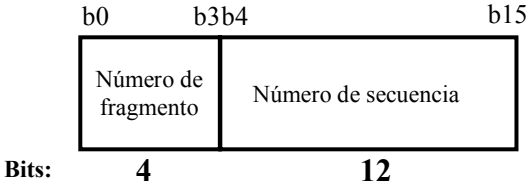


Figura 5-12. Campo de secuencia de control de la capa MAC.

El Cuerpo de la trama contiene los datos provenientes de la capa LLC (*Logical Link Control*) y la longitud de la trama varía de 0 a 2312 bytes.

[4] MSDU. *Mac Service Data Unit*

El FCS (*Frame Check Sequence*) contiene un CRC[5] (*Cyclic Redundancy Check*) de 32 bits.

7.6.1.1 Arquitectura de la subcapa MAC

La arquitectura MAC del estándar IEEE 802.11 se compone de dos funciones de coordinación: la función de coordinación puntual (PCF[6]) y la función de coordinación distribuida (DCF[7]) cada una de éstas definen el modo de operación para las estaciones que desean tener acceso a la WLAN. La ubicación de dichas funciones en el modelo de referencia OSI se ilustra en la siguiente figura.

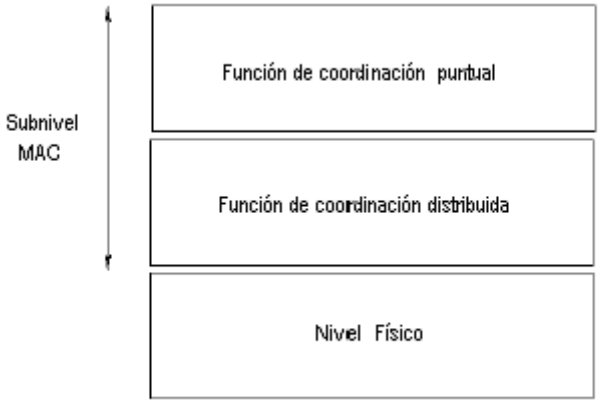


Figura 5-13. Funciones de coordinación de la subcapa MAC

La función de coordinación está definida como la función que determina, dentro de un BSS o celda, cuando una estación está habilitada para transmitir o recibir MPDU's (*Mac Protocol Data Unit*) a través de un canal inalámbrico.

7.6.1.1.1 DFC Función de Coordinación Distribuida

La función de coordinación distribuida se encuentra ubicada en la parte baja de la subcapa MAC y es un modo de operación básico para todas las estaciones, su funcionalidad está basada en técnicas de contienda que introducen retardos aleatorios no predecibles, por lo que el tráfico que se transmite bajo esta función es asíncrono.

[5] CRC. Técnica de verificación de errores en la que el receptor de la trama calcula un residuo dividiendo el contenido de la trama entre un número binario, y compara el residuo calculado con un valor almacenado en la trama del emisor.
[6] PCF. *Punctual Coordination Function*
[7] DCF. *Distributed Coordination Function*

Las características de la Función de coordinación distribuida, las podemos resumir en los siguientes puntos:

- Utiliza MACA[8] (CSMA/CA[9] con RTS[10]/CTS[11]) como protocolo de acceso al medio.
- Son necesarios los paquetes de reconocimientos ACK's[12], provocando retransmisiones si éste no es recibido.
- Definición de un campo Duration/ID que contiene el tiempo de reserva para transmisión y el ACK. Esto quiere decir que todos los nodos sabrán en que momento el medio de transmisión quedará libre.
- Implementa fragmentación de datos.
- Concede prioridad a tramas mediante el espaciado entre tramas (DIFS13).
- Soporta Broadcast y Multicast sin ACK's.

7.6.1.1.2 Protocolo de Acceso al medio CSMA/CA y MACA

El mecanismo básico de acceso al medio es muy similar al implementado en el estándar IEEE 802.3 (CSMA/CD) y es el llamado CSMA/CA (*Carrier Sense Multiple Access / Collision Advoidance*). Este mecanismo funciona tal y como se describe a continuación:

1.- Antes de transmitir información una estación debe verificar si el medio inalámbrico está libre.

2.- Si el medio no está ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (DIFS).

3.- Si durante este intervalo, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transmisión actual antes de realizar cualquier acción.

4.- Una vez finalizada la espera necesaria del DIFS, la estación ejecuta el algoritmo de Backoff, según el cual se determina un intervalo de espera adicional y aleatorio llamado ventana de contienda o temporizador (CW). El algoritmo de Backoff nos da

[8] MACA. *Multi Access Collision Advoidance*
[9] CSMA/CA. *Carrier Sence Multiple Access/Collision Advoidance*
[10] RTS. *Request to Send*
[11] CTS. *Clear to Send*
[12] ACK. *ACKnowledge*
[13] DIFS: Distributed Inter Frame Space

un número aleatorio y entero de ranuras temporales (*slot time*) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5.- El intervalo de tiempo obtenido mediante el algoritmo de Backoff es utilizado para activar el temporizador, llamado *Timer of Backoff,* el cual decrece durante el tiempo en que el canal está libre y se detiene cuando se detecta una transmisión de datos. Posteriormente se reactiva cuando el canal se libera nuevamente por un tiempo mayor al DIFS. Una estación transmite cuando el *Timer* llega a cero.

En la siguiente figura se puede observar el funcionamiento de CSMA/CA.

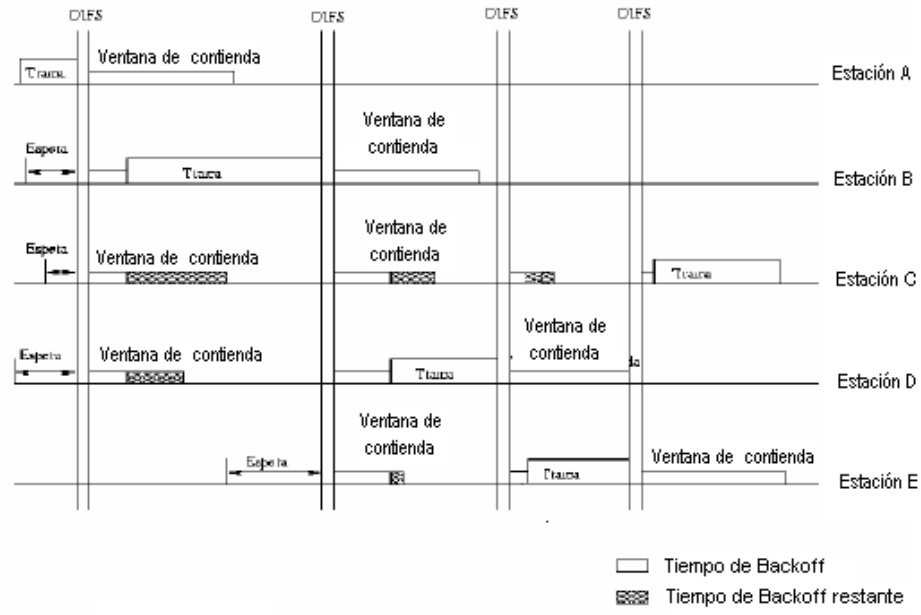


Figura 5-14. Funcionamiento del CSMA/CA.

Sin embargo, CSMA/CA en un entorno inalámbrico presenta dos principales problemas que son los siguientes:

- **Nodos ocultos**. Un cliente A cree que el canal está libre, pero en realidad está ocupado por otro cliente B que no es detectado por A.

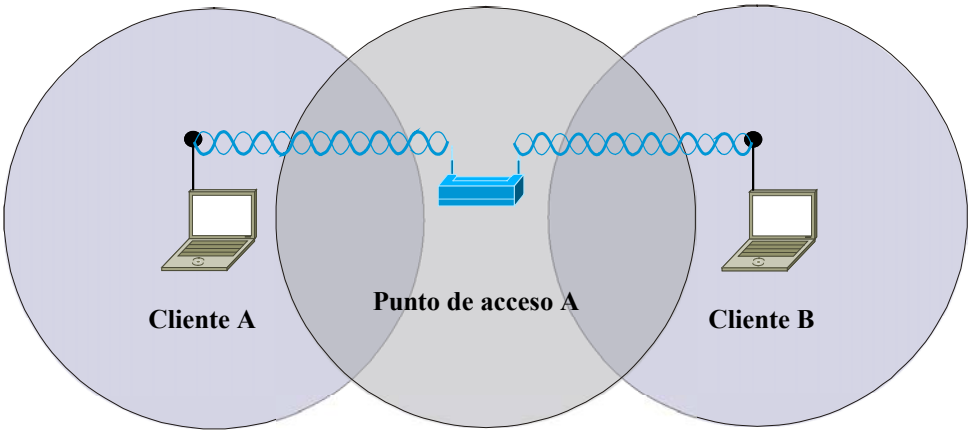


Figura 5-15 .Diagrama de nodo oculto

- **Nodos expuestos**. Un cliente A cree que el canal está ocupado, pero en realidad está libre, pues el cliente B al que detectó no le interferiría para transmitir a otro destino (punto de acceso A).

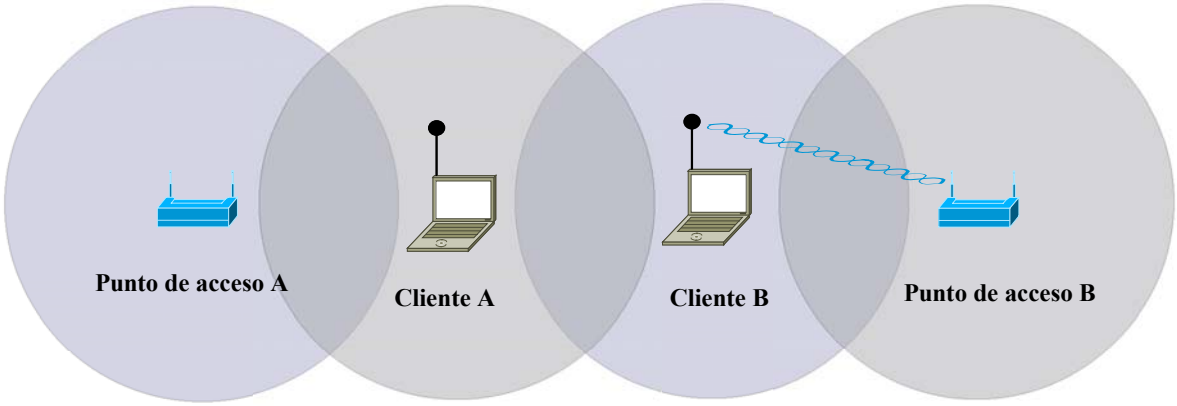


Figura 5-16. Diagrama de nodo expuesto

La solución que propone es estándar IEEE 802.11 es la utilización MACA o *MultiAccess Collision Avoidance*, en donde antes de transmitir el emisor envía una trama RTS (*Request to Send*) indicando la longitud de los datos a transmitir, en el campo Duración. El receptor le contesta con una trama CTS (*Clear to Send*) repitiendo la información del campo Duración. Al recibir el CTS, el emisor inicia la transmisión. Este mecanismo permite reservar el medio para evitar las colisiones por nodos ocultos o expuestos.

Para evitar esta problemática, las estaciones esperarán a que se ejecute la siguiente secuencia:

- Al escuchar un RTS, es necesario esperar un tiempo hasta recibir el CTS.

- Al escuchar un CTS, se requiere esperar hasta que transcurra el tiempo necesario según la longitud de datos.

5.1.2.4 Función de coordinación puntual

La Función de coordinación puntual está localizada por encima de la Función de coordinación distribuida y está asociada a las transmisiones libres de contienda que permiten la transmisión de tráfico síncrono que no tolera retardos aleatorios en el acceso al medio. El algoritmo de acceso a este nivel está basado en un poleo efectuado por el punto de acceso, mediante técnicas de acceso deterministas, para que los clientes con datos síncronos puedan transmitir su información (MPDU's) es decir que el punto de acceso controla al medio y emite peticiones de transmisión a cada uno de los clientes inalámbricos, en ciertos intervalos de tiempo, para la transmisión de datos. Ningún cliente puede transmitir o recibir información hasta que no sea elegido. Por lo que la Función de coordinación puntual otorga a cada cliente un turno para transmitir en un momento determinado. El hecho de que un punto de acceso tenga el control de acceso al medio hace que no sea eficaz para un gran número de usuarios.

Las dos funciones de coordinación pueden operar dentro de una misma celda o BSS dentro de un mecanismo llamado supertrama. Durante la primera parte de la supertrama la red opera bajo el modo de Función de coordinación distribuida, asignando un periodo de contienda, permitiendo que el subconjunto de estaciones puedan transmitir mediante mecanismos aleatorios; una vez finalizado este periodo el punto de acceso, llamado coordinador central, toma el medio y se inicia un periodo libre de contienda para la transmisión de datos síncronos.

5.1 Mecanismos de seguridad

El proceso de conexión del cliente a la red inalámbrica, comienza cuando éste hace un barrido en el rango de frecuencia usada por el estándar IEEE 802.11b enviando su dirección MAC y el SSID. Todos los puntos de acceso en el rango de frecuencia responderán con su propio SSID, canal de transmisión y dirección MAC. Con esta información el cliente define con qué punto de acceso se asociará e iniciará el proceso de autenticación.

Debido a que las WLAN están limitadas en seguridad, el estándar define un servicio de autenticación para controlar el acceso a la red, tanto el cliente como el punto de acceso deben estar debidamente identificados para tener acceso a la red. Si los componentes de una red inalámbrica forman parte de un IBSS, BSS o ESS, éstos tienen como prioridad efectuar la autenticación para lograr la comunicación con otra estación.

Uno de los elementos principales de algunos tipos de autenticación es la clave WEP (*Wired Equivalent Privacy*). La cual ha sido diseñada para proveer un nivel de seguridad para datos equivalente al de las redes alámbricas con acceso físico restringido.

WEP aplica un conjunto de instrucciones, las cuales combinan *texto plano* con una secuencia de números hexadecimales llamados *clave de cifrado WEP*. Las redes inalámbricas compatibles con el estándar IEEE 802.11b pueden utilizar dos diferentes longitudes en la clave de cifrado WEP:

- 40 bits: Clave que consiste de 10 números haxadecimales .
- 128 bits. Clave que consiste de 26 números hexadecimales.

5.1.2 Autenticación abierta

Es la autenticación que se implementa por omisión en los dispositivos del estándar IEEE 802.11b. Este tipo de autenticación es simple, primeramente el cliente envía una petición de autenticación, mediante una trama de administración, la cual contiene información de la identidad del cliente. La estación receptora regresa la trama indicando si la autenticación es exitosa o no. El único requisito para que la autenticación sea exitosa es que todos los elementos de la red inalámbrica sean configurados con el mismo SSID. En la siguiente figura se muestra el flujo de datos.

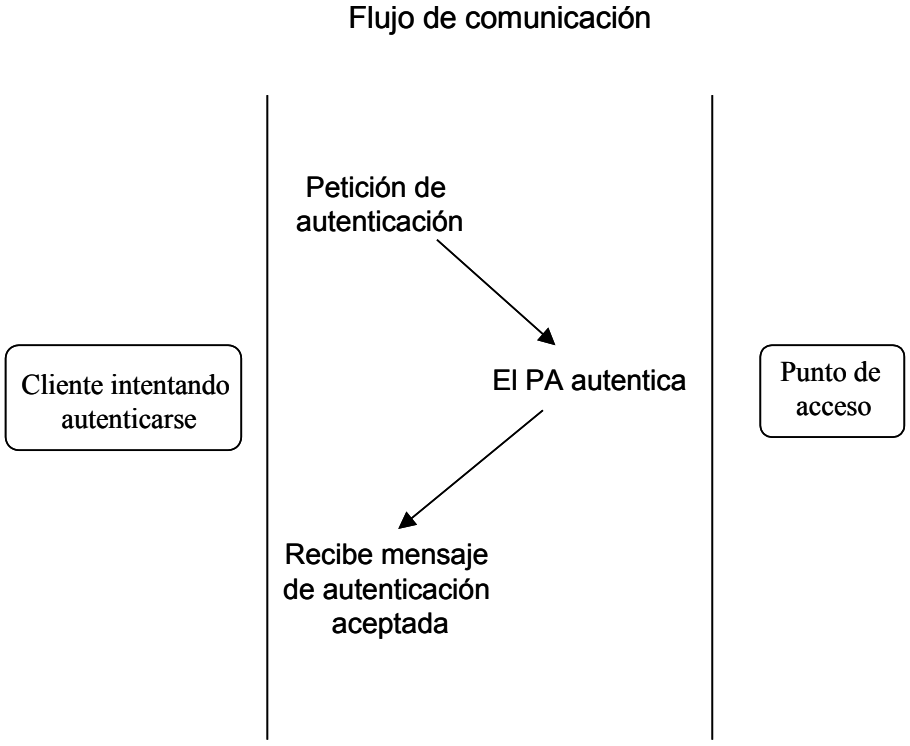


Figura 5-18. Diagrama de autenticación abierta

5.2.2 Autenticación *Shared Key*

Este método permitirá la autenticación del cliente únicamente después de demostrar que conoce la clave de cifrado WEP. A continuación se enlistan los pasos a seguir en este tipo de autenticación.

1. La estación envía una petición de autenticación.

2. El punto de acceso envía un texto desafío al cliente.

3. La estación cifra el texto desafío usando la clave WEP.

4. La estación envía el texto cifrado al punto de acceso.

5. El punto de acceso descifra el texto con la clave WEP y lo compara con el texto que envió originalmente. Si éste coincide, indica que tanto el cliente como el punto de acceso conocen la clave WEP, por lo tanto la autenticación es aceptada. Si no existe coincidencia la autenticación se rechaza.

En la siguiente figura se muestra el flujo de datos para la autenticación "*Shared Key*".

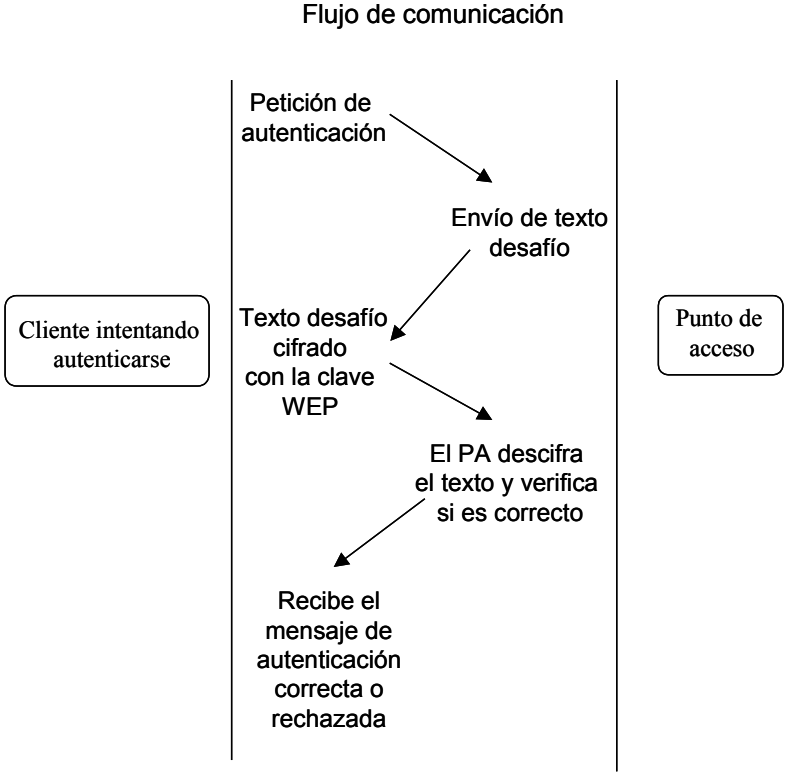


Figura 5-19. Diagrama de autenticación *Shared Key*

5.1.3 Autenticación por MAC

Este tipo de autenticación se basa en direcciones MAC autorizadas por cada punto de acceso o por sistema centralizado de autenticación, mediante listas previamente configuradas. La vulnerabilidad de este tipo de autenticación es que las direcciones físicas viajan en texto plano y con un analizador de protocolos, es posible capturar las direcciones permitidas y modificar la MAC de la WNIC (*Wireless Netwok Interface Card*) para que sea permitida.

CAPÍTULO 6. Seguridad en redes LAN

La seguridad es un aspecto muy importante en el ámbito de las redes de datos, debido a que es indispensable proteger la información para que no pueda ser leída, copiada o modificada por usuarios no autorizados. Para lograr esto es necesario implementar diversas funcionalidades que dependen de las necesidades del usuario; no obstante siempre deben utilizarse todas las estrategias posibles para obtener una red mejor protegida.

Debido a que las redes WLAN utilizan la infraestructura de la red alámbrica (WAN) para su funcionamiento, gran parte de los esquemas de seguridad son aplicables a ambas redes. En las siguientes figuras se muestra la topología utilizada por cada una de dichas redes.

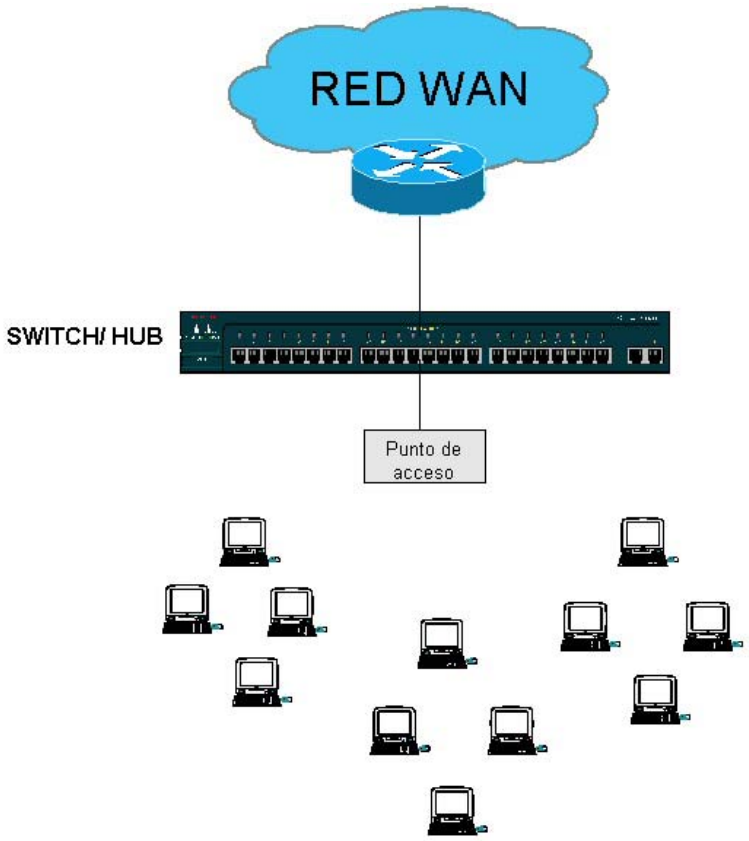


Figura 6.1. Topología de la red inalámbrica

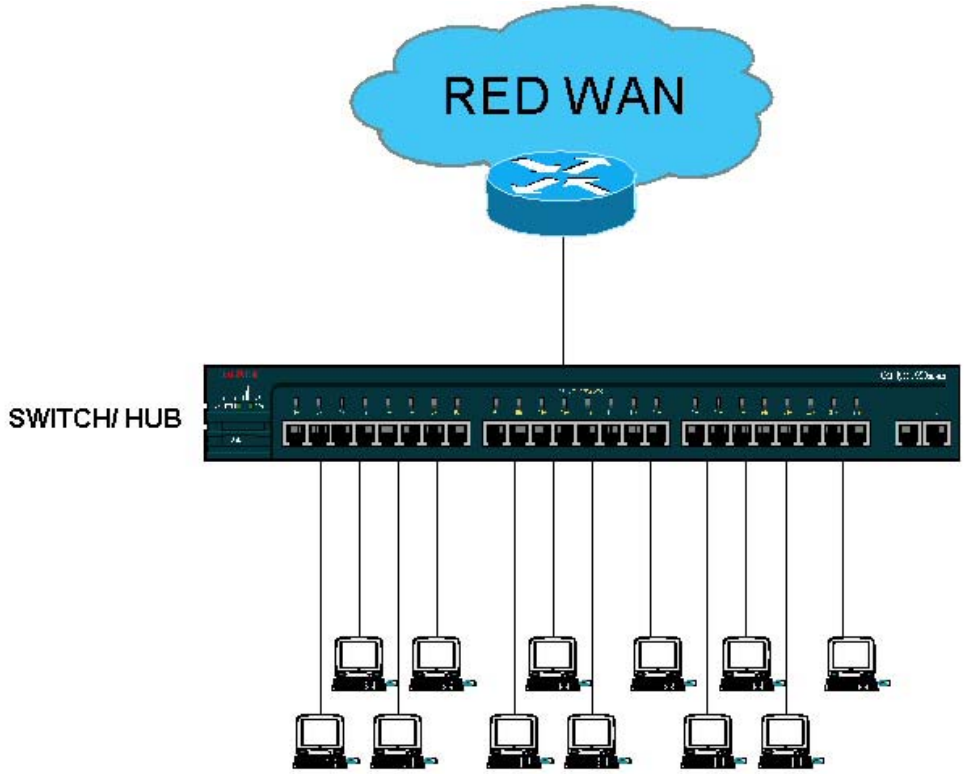


Figura 6.2. Topología de la red alámbrica

De las figuras se observa que la diferencia entre redes está en el último tramo del medio de transmisión, uno es alámbrico y otro inalámbrico. Los esquemas de seguridad que son implementados en la red alámbrica, son compatibles para infraestructuras inalámbricas.

Los esquemas de seguridad de la red pueden ser clasificados en cinco grupos que son los siguientes:

- **Identidad**. Identificación exacta de usuarios de la red, aplicaciones, servicios y recursos mediante servidores de autenticación que permitan determinar niveles de acceso y archivar los datos necesarios para la utilización de servicios.

- **Seguridad Perimetral**. Esto se refiere a delimitar con claridad las necesidades de cada uno de los usuarios y controlar el acceso a aplicaciones, datos y servicios críticos en la red, de forma tal que solo los usuarios permitidos puedan obtener información de la red. Una de las herramientas más utilizadas con las listas de acceso.

- **Conectividad segura**. Es fundamental disponer de un medio de comunicación autenticado y confidencial, para protegerla de intentos de captura, alteración y procesos que permitan conocer la información. Para esto existen diversos métodos de autenticación.

- **Monitoreo de seguridad**. Para confirmar que la red sigue siendo segura luego de la implementación de una política de seguridad, es fundamental tener en observación continua la red para detectar ataques o cualquier tipo de irregularidad. El software de búsqueda de vulnerabilidades de manera proactiva identifica áreas de debilidad dentro del esquema general, y los sistemas de detección de intrusos pueden monitorear y responder en forma activa ante intentos de vulnerar la seguridad a medida que ocurran.

A continuación se describen algunos de los esquemas de seguridad más utilizados en el mercado para la protección de la información.

6.1 Servidor de autenticación

Dentro de los esquemas de identidad y conectividad segura se encuentran los servidores AAA (*Authentication, Autorización and Accounting*) los cuales permiten realizar las siguientes funciones.

- **Autenticación.** Determina la identidad del usuario mediante un nombre y contraseña.
- **Autorización.** Permite a los administradores de la red limitar los servicios por cada usuario, según sus necesidades.
- **Contabilidad.** Permite tener un registro de la utilización de los recursos de la red.

Para realizar la autenticación, los servidores comúnmente utilizan los siguientes protocolos:

- **PAP** ***(****Password Authentication Protocol)*. Este protocolo emplea un método de autenticación muy inseguro, debido a que envía constantemente en forma de texto plano, el nombre de usuario y contraseña, hasta que el servidor acepta o rechaza la petición.

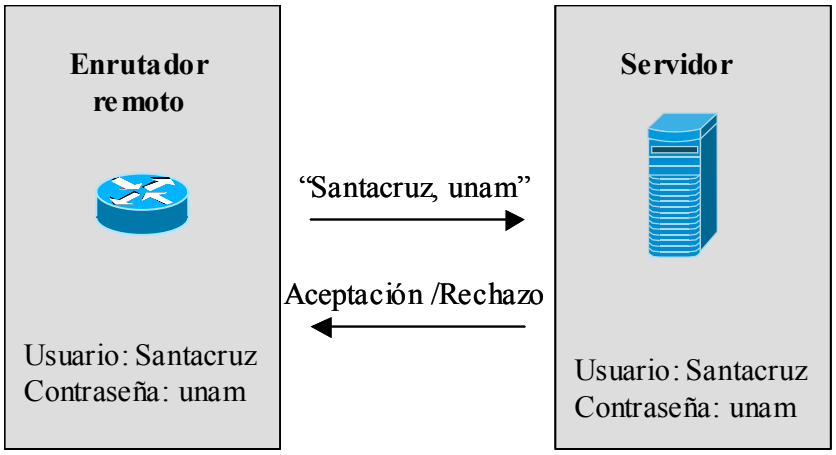


Figura 6.3 Autenticación PAP

- **CHAP** (*Challenge Handshake Authentication Protocol*). En este protocolo se emplea un mecanismo en el que los nombres de usuario viajan por la red como texto plano, mientras que las contraseñas son cifradas, aplicando el algoritmo MD5[1]. Una vez establecida la conexión, el servidor envía un mensaje de invitación a la autenticación (llamado también *challenge message* o mensaje desafío) el cual contiene parte de la información para que el nodo remoto aplique el algoritmo en su respuesta al servidor y éste al recibirlo recalcule el algoritmo para comparar si ambos valores son iguales. Si los valores obtenidos coinciden, el servidor manda un mensaje de aceptación, de lo contrario rechaza la autenticación.

  CHAP proporciona protección contra atacantes que con ayuda de un analizador de protocolos pretendan obtener información confidencial del usuario

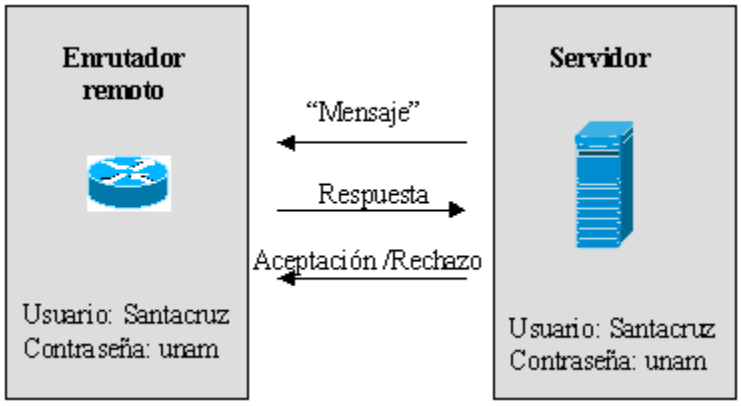


Figura 6.4. Autenticación CHAP

- **EAP (***Extensible Authentication Protocol***).** Este protocolo está definido en el estándar IEEE 802.1x, para poder ofrecer un mecanismo de autenticación estándar. EAP es un protocolo que se utiliza para encapsular los mensajes que permiten la autenticación y pueden ser enviados a través de redes LAN alámbricas e inalámbricas, aunque es mucho más común en las últimas. En una red inalámbrica EAP ofrece un esquema de autenticación mutua, el cual elimina la posibilidad de que el cliente entregue la información confidencial a un punto de acceso ilegítimo; también permite una administración centralizada de los recursos de la red y generación dinámica de claves WEP[2] cada determinado tiempo.

  El proceso EAP, consiste de los siguientes puntos:

  1. El cliente detecta al punto de acceso y se asocia con él.

  2. El punto de acceso bloquea cualquier petición de autenticación, de otro cliente que requiera tener acceso a la red LAN.

[1] Message Digest 5
[2] WEP. *Wired Equivalent Privacy*

3. Posteriormente el cliente proporciona su contraseña y nombre para ser enviados encapsulados en paquetes EAP.

4. Se realiza la autenticación mutua entre el servidor y el cliente, en el punto de acceso, la autenticación consta de dos fases; la primera se lleva a cabo cuando el servidor RADIUS verifica las credenciales del cliente o viceversa; y la segunda es efectuada por el cliente verificando las credenciales del servidor RADIUS o viceversa. En los puntos de acceso es configurada una palabra clave compartida, la cual es utilizada para obtener las credenciales del servidor, es decir que cuando el paquete EAP llega al punto de acceso, éste debe demostrar que es un dispositivo válido, enviando otro paquete EAP al servidor que contiene la información necesaria para identificarse como un punto de acceso registrado; es hasta entonces cuando el paquete EAP emitido, inicialmente por el cliente es desencapsulado para que el nombre de usuario y contraseña sean validados por el servidor. Es importante mencionar que si el punto de acceso no es validado por el servidor la autenticación mutua fallará y el paquete EAP no es descifrado.

5. Una vez que la autenticación mutua se ha completado satisfactoriamente el servidor RADIUS y el cliente determinan la clave WEP que utilizarán para comunicarse entre ambos (Clave WEP *unicast*).

6. El servidor entrega la clave WEP *unicast* al punto de acceso, por el medio alámbrico.
7. El punto de acceso cifra su clave WEP (Clave WEP *broadcast*) con la clave WEP *unicast* y la envía al cliente.

8. El cliente y el punto de acceso activan las claves WEP *unicast y broadcast* para utilizarlas, entre sí, durante el tiempo restante de la comunicación o hasta que se generen nuevas claves WEP, en caso que se utilice la asignación de claves WEP dinámicas. Véase la siguiente figura.

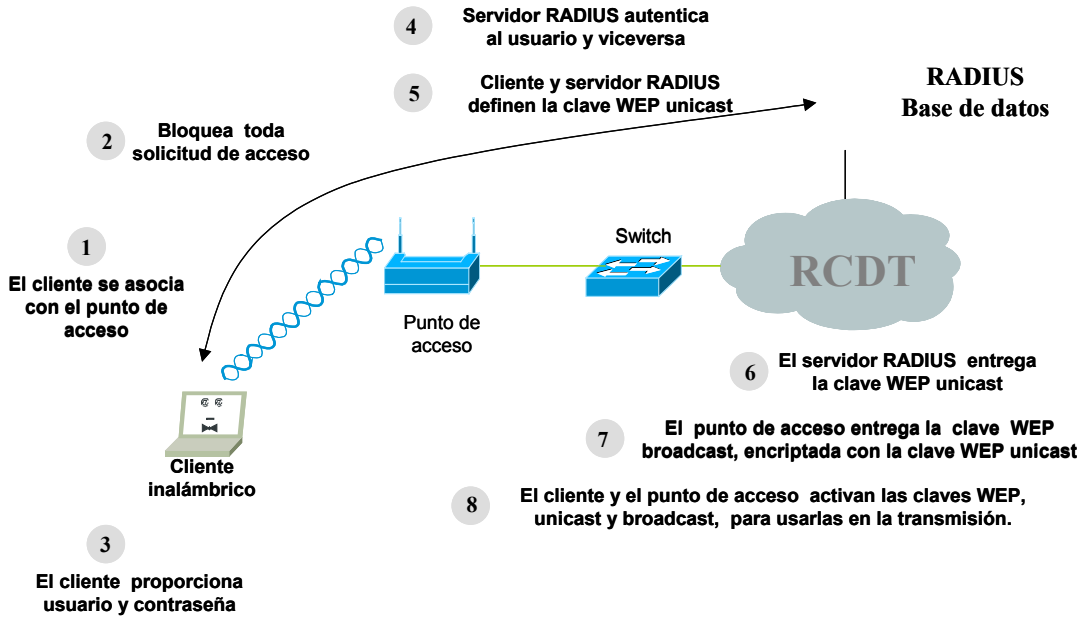


Figura 6.5. Autenticación LEAP

6.2 Listas de acceso

Las listas de acceso pueden ser aplicadas tanto en redes alámbricas como inalámbricas, debido a que son configuradas principalmente en los enrutadores. Su principal función es controlar el flujo de paquetes mediante filtros que determinan si la información es enviada a su destino o no.

Cuando el enrutador es configurado con varias listas de acceso, éste analiza a los paquetes de acuerdo con cada una de las condiciones de la lista. Para el caso de enrutadores Cisco , la primera coincidencia determina si el enrutador acepta o rechaza el paquete. Si no hay condiciones que coincidan con alguna lista, el paquete es rechazado o ceptado dependiendo de la lógica de la lista.

Cisco clasifica a las listas de acceso en dos tipos:

- **Listas de acceso estándar**. Verifican la dirección origen de los paquetes para determinar si se permite o se niega la entrada o salida del paquete.

- **Listas de acceso extendidas**. Verifica las direcciones origen y destino de cada uno de los paquetes. También con este tipo de listas se puede realizar un filtrado por protocolo y número de puerto TCP/UDP.

Las listas de acceso pueden ser de lógica positiva o negativa, en la primera se permite todo el tráfico excepto el que cumple con las condiciones especificadas por la palabra *deny* en las listas de acceso y en la segunda sucede todo lo contrario; por omisión ningún paquete es

permitido a menos que cumpla con las condiciones especificadas con la palabra *permit* en las listas de acceso.

En los enrutadores Cisco la sintaxis para una lista de acceso estándar es la siguiente:

access-list ***lista*** **{permit ¦ deny}** ***dirección origen*** ***wildcard***

Donde:

Parámetro	Descripción
access-list	Comando de lista de acceso
lista	Identificador de lista, el cual es un número entero del 1 al 99.
permit | deny	Indica si la lista es de lógica positiva o negativa.
Dirección origen	Dirección origen de los paquetes
Wildcard	Identifica que bits serán verificados. El valor por omisión es 0.0.0.0.

Tabla 6-1. Sintaxis de una lista de acceso estándar

La dirección IP origen en el paquete se compara con el valor de dirección especificado en el comando *access – list*. Si se utiliza la palabra clave *permit*, se logra que el paquete sea aceptado, por el contrario si se utiliza la palabra clave *deny*, el paquete es rechazado.

La *wildcard* es un valor de 32 bits que no debe confundirse con las máscaras de subred que se utilizan para subdividir bloques de direcciones IP. Para obtener la *wildcard* es necesario realizar una comparación de la mascara de subred con valores de ceros y unos que determinarán que bits serán ignorados y cuales tomados en cuenta al analizar el segmento IP. Para comprensión de lo anterior, a continuación se presenta un ejemplo.

Ejemplo:

Si se requiere permitir el acceso al bloque de direcciones 10.1.2.0 con máscara 255.255.255.0., y se representa dicho segmento IP en sistema binario, se obtiene lo siguiente.

00001010.00000001.00000010.00000000	Representación del segmento: 10.1.2.0 (valores a verificar)
11111111.11111111.11111111.0.0.0.0.0.0	Máscara de subred, que verifica el valor de los primeros 24 bits (1) e ignora los últimos 8 (0).
00000000.00000000.00000000.11111111	*Wilcard* que verifica el valor de los primeros 24 bits del segmento (0) y los restantes se ignoran (1).

Como se puede observar en el ejemplo anterior la *wildcard* y la máscara de subred ejecutan una función equivalente usando lógicas inversas.

Finalmente si se representa la *wildcard* en forma decimal se obtiene: **0.0.0.255**, y el comando completo para este ejemplo se escribiría de la siguiente manera:

access – list 1 permit 10.1.2.0 0.0.0.255

Es posible utilizar el comando "***no access – list*** *..."* para eliminar toda la lista de acceso, pero debe ser utilizado con precaución, porque si se especifica una lista de acceso incorrecta, podría eliminarse algo que se desee conservar.

Las listas de acceso extendidas permiten filtrar el tráfico según se requiera con base en la dirección IP origen y destino; además de permitir y negar el acceso a protocolos IP específicos.

La sintaxis para la lista de acceso extendida para los equipos Cisco, es la siguiente:

access-list ***lista*** **{permit ¦ deny}** ***protocolo dirección origen wildcard origen*** **[*puerto operador*] *dirección destino wildcard destino*** **[*puerto operador*] [*established*] [*log*]**

En la siguiente tabla se especifican cada uno de los parámetros.

Parámetro	Descripción
access-list	Comando de lista de acceso
lista	Identificador de lista, el cual es un número entero del 100 al 199.
permit | deny	Indica si la lista es de lógica positiva o negativa.
protocolo	IP,TCP,UDP,ICMP[3],GRE [4]o IGRP[5]
dirección origen	dirección origen de los paquetes
Wildcard origen	Identifica que bits serán verificados. El valor por omisión es 0.0.0.0.
Dirección destino	Dirección destino de los paquetes
Wildcard destino	Identifica que bits serán verificados. El valor por omisión es 0.0.0.0.
Puerto operador	lt,gt,eq,neq (less than, greater than,equal, no

[3] ICMP. *Intenet Control Message Protocol*
[4] GRE. *Generic Routing Encapsulation*
[5] IGRP. *Interior Gateway Routing Protocol*

	equal) y un número de puerto TCP/UDP
Established	Únicamente se utiliza para paquetes TCP en la entrada, si los paquetes utilizan una conexión establecida.
log	Se almacena el registro en un archivo.

Tabla 6-2. Sintaxis de una lista de acceso extendida

Los números de 100 a 199 están reservados para listas de acceso extendidas y se encuentran fuera del rango de los números de 1 a 99 utilizados para las listas de acceso estándar.

De manera análoga a las listas de acceso estándar, si se utiliza la palabra *permit*, los paquetes que cumplan con la condición dada serán permitidos. Si se utiliza la palabra *deny*, los paquetes serán rechazados.

El puerto operador indica que tipo de tráfico será permitido y negado con base en el número de puerto TCP/UDP (véase Apéndice1) es decir que es posible filtrar el tráfico de manera específica o por grupos. Para ejemplificar lo anterior podemos decir que si tomamos como referencia el puerto 25 correspondiente a SMTP, podemos seleccionar el tráfico mayores que, menores a, iguales a o no iguales a este puerto.

En listas de acceso aplicadas a la información que ingresa al enrutador, es posible utilizar el parámetro *established,* el cual permite establecer una conexión TCP y permitir el tráfico de ésta sólo en paquetes de entrada.

Ejemplo:

Supóngase que la política de la red exige que se rechacen los paquetes entrantes de SMTP provenientes de la dirección 132.124.23.55 y dirigidos al semento de red 199.245.180.0.

access – list 101 deny tcp 132.124.23.55 0.0.0.0 199.245.180.0 0.0.0.255 eq 25

El comando anterior rechaza los paquetes tcp que provienen de la dirección 132.124.23.55 a la red 199.245.180.0/24 que pertenezcan a aplicaciones SMTP (puerto 25).

6.3 Detectores de intrusos

Un sistema de detector de intrusos o IDS (*Intrusion Detection System*) es una herramienta de seguridad encargada de monitorear los eventos que ocurren en un sistema informático en busca de intentos de intrusión, los cuales son cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o seguridad de una red. Las intrusiones se pueden producir de varias formas: atacantes que acceden a los sistemas desde Internet,

usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados y usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado.

La detección de intrusiones permite a las organizaciones proteger la red de las amenazas que aparecen al incrementar la conectividad en red y la dependencia que tenemos hacia los sistemas de información. Cuando un individuo ataca un sistema, lo hace típicamente en fases predecibles. En la primera fase el atacante hace pruebas y examina la red en busca de un punto débil. En redes que no disponen de un IDS, el atacante es libre de examinar el sistema con un riesgo mínimo de ser detectado, lo cual facilita la búsqueda de un punto débil en nuestra red.

En la misma red con un IDS implementado, las operaciones para examinar la red presentan mayor dificultad al atacante, debido a que el IDS observará las pruebas, las identificará como sospechosas, podrá bloquear el acceso del atacante y avisará al personal encargado de la seguridad de la red de lo ocurrido para que tome las acciones pertinentes.

Cuando se hace un plan para la administración de seguridad de la red o se desea redactar políticas de seguridad de la organización, es necesario conocer cual es el riesgo de la organización a posibles amenazas, la probabilidad de ser atacada o incluso si ya está siendo atacada. Un IDS nos puede ayudar a conocer la amenaza existente fuera y dentro de la organización, ayudándonos a tomar decisiones acerca de los recursos y seguridad que debemos emplear en nuestra red y del grado de cautela que debemos considerar al redactar las políticas de seguridad.

La detección de intrusos se centra en identificar comportamientos inusuales en una red. Funciona asumiendo que los ataques son diferentes a la actividad normal. Lo detectores de intrusos construyen perfiles representando el comportamiento normal de los usuarios, mediante datos históricos recolectados durante un periodo normal de operación. Las técnicas usadas en la detección de intrusos incluyen las siguientes:

- Detección de un umbral sobre ciertos atributos del comportamiento del usuario que pueden incluir el número de archivos accedidos por un usuario en un periodo de tiempo dado, el número de intentos fallidos para entrar en el sistema, la cantidad de CPU utilizada por un proceso, etc.

- Medidas estadísticas, que pueden ser paramétricas, donde se asume que la distribución de usuarios y atributos coinciden con un determinado patrón, donde dicha distribución es aprendida de un conjunto de valores históricos, observados a lo largo del tiempo.

Una de las desventajas del IDS es que produce un gran número de falsas alarmas debido a los comportamientos no predecibles de los usuarios en la red.

Una vez que se ha producido un análisis de los eventos y se ha detectado un ataque, el IDS reacciona con respuestas pasivas y activas. Las primeras notifican al responsable de seguridad de la red que el sistema ha sido atacado y las activas son acciones automáticas

que se ejecutan cuando ciertos tipos de intrusiones son detectados, una de estas acciones puede ser bloquear la dirección IP del atacante en el enrutador.

Los detectores de intrusos son implementados dentro de la infraestructura alámbrica, por lo que pueden ser utilizados para detectar intrusos alámbricos o inalámbricos.

CAPÍTULO 7. Comparativo entre una red LAN alámbrica y una inalámbrica

De acuerdo con lo analizado anteriormente, en este capítulo se analizarán varios puntos de comparación entre ambos tipos de redes, como son los siguientes:

- Estandarización
- Infraestructura
- Rendimiento
- Movilidad y facilidad de implementación
- Seguridad
- Costo

7.1 Estandarización

La estandarización de las tecnologías es muy importante para el desarrollo de las mismas, ya que permite la homologación de todos lo productos del mercado y evita las incompatibilidades entre fabricantes. Para ello existen organizaciones como la IEEE y la ITU-T[1] que realizan esta importante labor.

La madurez en cualquier tipo de tecnología es alcanzada a través del proceso natural de su evolución; corrigiendo errores, impulsando el desarrollo de herramientas de diagnóstico y administración, agregando nuevas funcionalidades y logrando la compatibilidad total entre la gran diversidad de fabricantes.

Los estándares utilizados en las redes alámbricas, ya han alcanzado la madurez; mientras que los estándares utilizados para las inalámbricas se encuentran en proceso de evolución y ante esto, han surgido algunas otras organizaciones como la WECA (*Wireless Ethernet Compatibility Alliance*) la cual sin fines de lucro fue fundada en 1999. Su lanzamiento público y oficial se realizó el 23 de agosto de 1999 en Santa Clara, California y su misión consiste en certificar la capacidad de interoperabilidad de los productos WLAN, aplicándoles estrictas pruebas y sólo aquéllos que cumplen con la norma de interoperabilidad pueden llevar el logotipo de Wi-Fi (*Wireless Fidelity*).

Actualmente el estándar utilizado en México es el IEEE 802.11b, pero en un futuro próximo se evolucionará a otros estándares como IEEE 802.11g o IEEE 802.11a. Y también es probable que surjan nuevos estándares para las redes cableadas.

7.2 Infraestructura

[1] ITU-T: *Internacional Telecomunication Union-Telecommunication*

La infraestructura básica de una red LAN alámbrica tradicional, consta de un *switch* o concentrador, encargado de la interconexión de los usuarios a la red; de un servidor que permite la autenticación de los usuarios, ya sea para tarificación o para la adquisición de privilegios. Véase la siguiente figura.

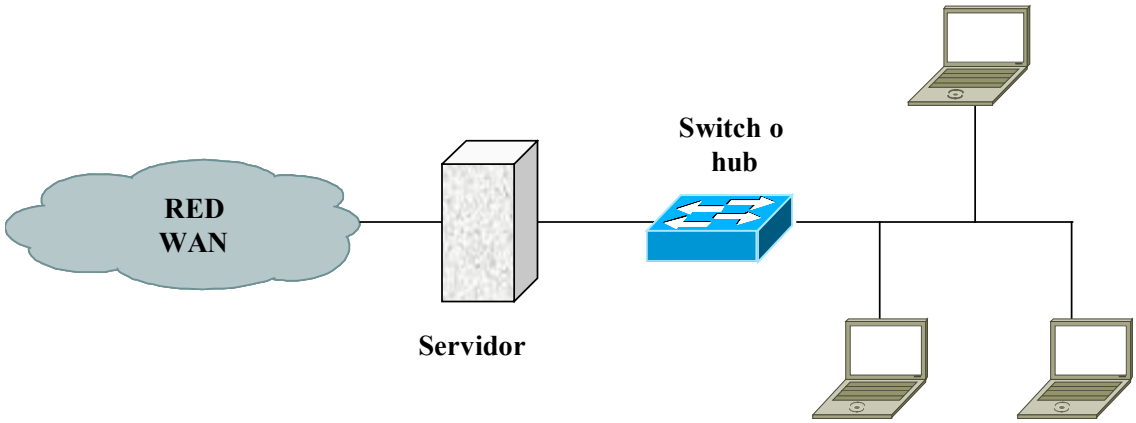


Figura 7-1. Infraestructura básica de una red LAN alámbrica

En cambio en la red inalámbrica, se inserta un nuevo dispositivo llamado punto de acceso, entre el *switch* o concentrador y los usuarios. En este tipo de red el servidor realiza las mismas funciones que una red alámbrica. En este caso, es el punto de acceso el que interconecta a los usuarios a la red alámbrica, mediante ondas electromagnéticas, evitando de esta manera, la construcción del cableado. Véase la siguiente figura.

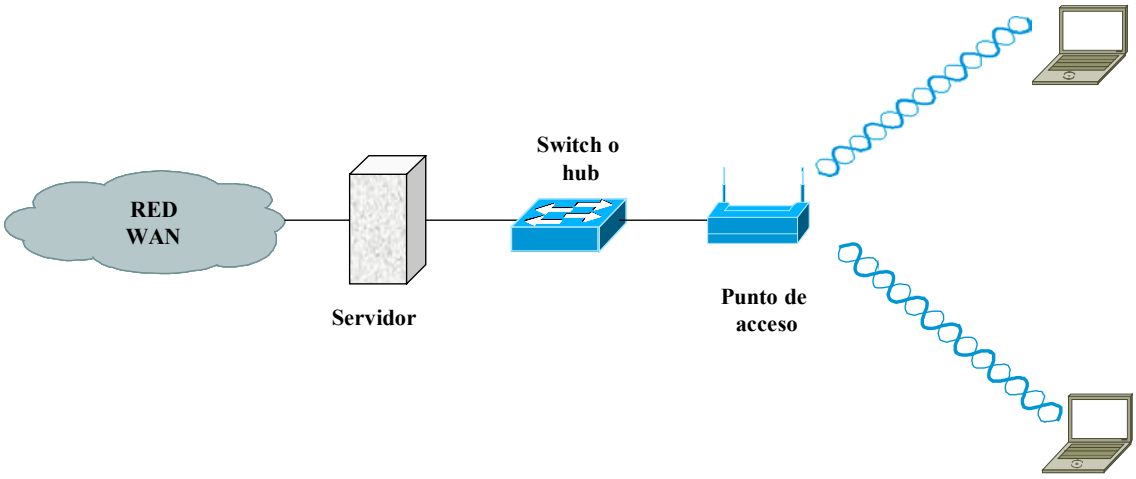


Figura 7-2. Infraestructura básica de una red LAN inalámbrica.

7.3 Rendimiento

Indiscutiblemente, el rendimiento es una de las desventajas de las redes inalámbricas, porque mientras los estándares de las redes alámbricas definen velocidades hasta de 1Gbps, en las inalámbricas, regidas por el estándar IEEE 802.11b, se define una velocidad máxima de 11Mps.

Algo muy importante a destacar es que para el caso de las redes LAN alámbricas la velocidad de transmisión y el ancho de banda son dedicados para cada uno de los usuarios; por otro lado para una red LAN 802.11b dichos parámetros son compartidos por todos los usuarios. Es decir que si tenemos una red alámbrica cuya velocidad está definida a 10 Mbps, cada usuario tendrá disponible esta velocidad (considerando que cada puerto del *switch* tiene conectado un solo host) mientras que en una red inalámbrica la velocidad definida en 11 Mbps es compartida para cada uno de los usuarios, por lo que en este caso el ancho de banda es inversamente proporcional al número de usuarios.

Se han realizado diversos estudios de rendimiento real en las redes de datos transportadoras de tráfico IP y de acuerdo con éstos se ha determinado que el pico máximo de rendimiento en una red alámbrica con velocidad definida en 10 Mbps, es de 6.5 a 7 Mbps, logrando una eficiencia aproximada del 70%; por otra parte para una red inalámbrica se encontraron valores del máximo rendimiento para cada una de las velocidades definidas en el estándar. Véase la siguiente tabla.

Velocidad definida por el estándar [Mbps]	Pico máximo de rendimiento real [Mbps]	Eficiencia [%]
11	6.2	56
5.5	3.9	71
2	1.7	85
1	0.9	90

Tabla 7-1. Rendimiento de una red inalámbrica

Tomando en cuenta las velocidades máximas de transmisión, se obtuvieron las siguientes tablas, en donde se obtiene el rendimiento real por usuario en los dos tipos de redes LAN.

Red LAN inalámbrica	
Número de usuarios	**Velocidad de trasmisión [Kbps] promedio por usuario**
1	6,200
2	3,100
3	2,067
4	1,550
5	1,240
6	1,033
7	886
8	775
9	689
10	620
11	564
12	517
13	477
14	443
15	413
16	388
17	365
18	344
19	326
20	310

Red LAN alámbrica	
Número de usuarios	**Velocidad de trasmisión [Kbps] promedio por usuario**
1	7,000
2	7,000
3	7,000
4	7,000
5	7,000
6	7,000
7	7,000
8	7,000
9	7,000
10	7,000
11	7,000
12	7,000
13	7,000
14	7,000
15	7,000
16	7,000
17	7,000
18	7,000
19	7,000
20	7,000

Tabla 7-2. Comparativo de rendimiento por usuario

Con la información de las tablas anteriores se confirma que una red LAN alámbrica tiene mejor rendimiento, por ello no es recomendable la instalación de una red inalámbrica en sitios donde operen aplicaciones de gran consumo de recursos.

La cantidad de usuarios en una red cableada depende de la capacidad de puertos del *switch* o concentrador; en cambio en una red inalámbrica el número de usuarios es, en teoría, ilimitado pero está directamente relacionado con el rendimiento que se desee para cada usuario. Usualmente en el diseño de una WLAN se consideran 25 usuarios por punto de acceso.

Existe la posibilidad de aumentar el ancho de banda en una red inalámbrica instalando varios puntos de acceso, pero eso se verá reflejado en el costo de la red.

7.4 Movilidad y Facilidad de instalación

La gran ventaja de las redes inalámbricas es la movilidad, porque el usuario no está obligado a trabajar en sitios predeterminados y tiene mayor flexibilidad para utilizar los servicios de red.

Las redes locales inalámbricas se instalan más fácilmente que las redes locales alámbricas, principalmente porque se evita el gran desplegado de cables, lo cual puede ser muy útil en lugares donde se requieran redes provisionales, e inclusive, pueden ser instaladas sin problema alguno en el hogar.

La movilidad también permite que el usuario sea más productivo, porque a diferencia de las soluciones de redes que utilizan cables, las redes WLAN permiten al usuario trasladarse libremente con su computadora portátil y utilizarla para pagar cuentas, leer y enviar mensajes de correo electrónico o tener acceso a la Internet desde cualquier lugar, sin usar cables. Actualmente existen redes inalámbricas públicas en hoteles, restaurantes, centros de convenciones y aeropuertos, por lo que el usuario puede realizar sus actividades sin requerir presencia física en su oficina o lugar de trabajo. Además mediante las redes públicas los usuarios pueden acceder a sus redes corporativas.

7.5 Seguridad

La seguridad en una red cableada es más robusta, principalmente porque el acceso físico está más controlado, es decir es necesario disponer de un puerto de red para poder elaborar un ataque; por el contrario una red inalámbrica tiene más facilidad de acceso, por que la radiación de las ondas electromagnéticas no puede tener una limitación física e inclusive los ataques pueden llevarse a cabo desde la vía pública.

Los ataques a cualquiera de los dos tipos de redes son muy similares; se pueden presentar ataques de virus, alteraciones o robo de información confidencial realizado por personal no autorizado, instalación de equipo no permitido, etc. La diferencia radica en el último tramo de la red, que puede ser alámbrico o inalámbrico.

Actualmente existen diversos y homologados esquemas de seguridad para las redes alámbricas, como detectores de intrusos, sistemas de autenticación, protección para los puertos de acceso a la red, etc. Desgraciadamente los esquemas de seguridad para la tecnología inalámbrica no han madurado lo suficiente para que puedan ser implementados en cualquier red, independientemente del fabricante.

Las redes inalámbricas tienen una gran debilidad en la seguridad definida en el estándar. Durante el desarrollo del IEEE 802.11b se consideró que la transmisión de datos por ondas electromagnéticas era más vulnerable a conexiones no autorizadas que las redes alámbricas, por tanto se desarrolló el sistema WEP (*Wireless Equivalent Protocol*) que cifra todos los paquetes antes de transmitirlos, de forma tal que se posea una seguridad equivalente a la que brindan las redes alámbricas.

Para cifrar y descifrar un paquete se requiere que los dos dispositivos que se comunican inalámbricamente conozcan una clave digital de cifrado (clave WEP) un dispositivo que no conoce la clave no puede descifrar los paquetes que recibe y por tanto los datos para él son ininteligibles.

WEP se basa en el algoritmo de cifrado estándar conocido como RC-4 desarrollado para teléfonos celulares digitales; a la fecha se ha publicado que existe información en la Internet para lograr descifrar el algoritmo y obtener la clave WEP, de esta forma tener acceso total a la red. La manera de descifrar este algoritmo se describe en los siguientes puntos:

- Para descifrar la clave se requiere de programas especializados capaces de realizar análisis en múltiples iteraciones sobre una gran cantidad de información recopilada con un analizador de protocolos; a esto se le conoce como un "ataque estadístico". La cantidad de información requerida para el análisis debe ser de 100 Mbytes a 1Gbyte, para lo cual se requiere de un tiempo de ocho horas aproximadamente.

- Hasta la fecha los programas de descifrado de clave WEP trabajan en plataformas LINUX y requieren ser compilados para que sean compatibles con el hardware de la tarjeta de red inalámbrica (WNIC[2]) instalada en la computadora utilizada para el ataque.

En las siguientes figuras se ilustra la técnica empleada para realizar los ataques a una red inalámbrica descifrando la clave WEP.

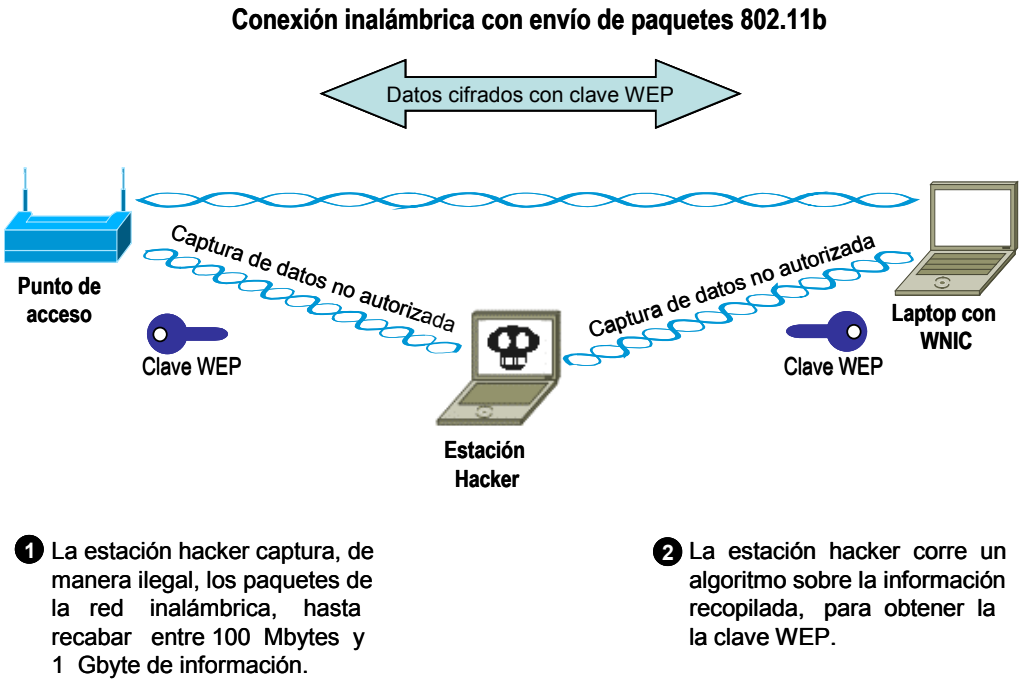
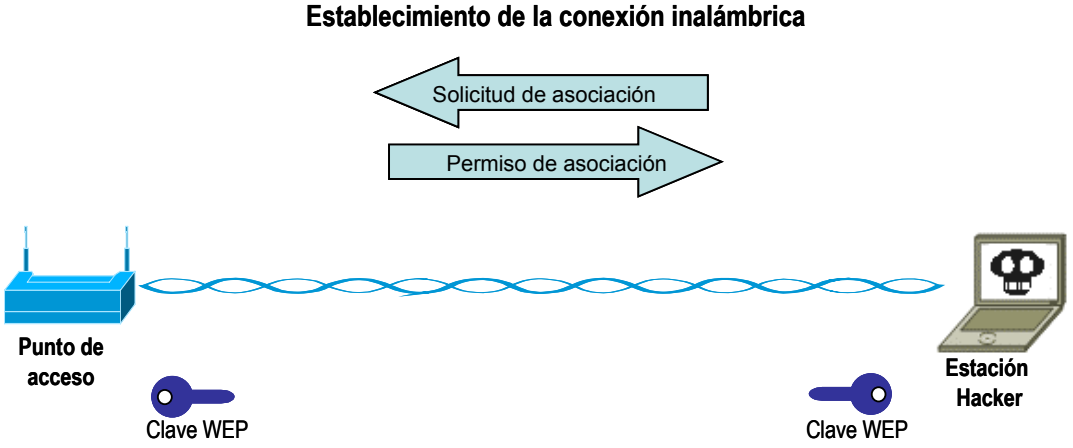


Figura 7-3. Ataque a una red LAN inalámbrica

[2] WNIC. *Wireless Network Interface Card*

❸ Ahora, la estación hacker posee la clave WEP, con la cual puede descifrar todos los paquetes que son transmitidos por la red inalámbrica.

Figura 7-4. Obtención ilegal de la clave WEP de una red LAN inalámbrica



❹ Conociendo la clave WEP la estación hacker puede asociarse al punto de acceso para tener una comunicación completa con la red LAN inalámbrica.

Figura 7-5. Intromisión de un usuario no autorizado a una red LAN inalámbrica

Por las vulnerabilidades del estándar en el aspecto de seguridad, los fabricantes han optado por implementar sus propios sistemas de seguridad, logrando una gran diversidad pero al mismo tiempo incompatibilidades.

Los esquemas de seguridad agregados por los fabricantes están directamente relacionados con el costo de los dispositivos, inclusive, el precio puede elevarse al doble. Por esta razón es necesario que el usuario tenga bien definidos los niveles de seguridad requeridos para su red y tome la mejor decisión con base en su presupuesto.

La seguridad es un aspecto muy importante a cuidar, sobretodo en las redes privadas, donde es necesario implementar mecanismos de seguridad extrema, tanto en la parte alámbrica como inalámbrica.

7.6 Análisis de Costo

Como anteriormente se ha mencionado las redes cableadas han madurado lo suficiente en cuanto a estandarización e interoperabilidad de distintos fabricantes, lo cual ha repercutido directamente en la estabilización de su precio y homologación de infraestructuras. Por otra parte para las redes inalámbricas, todavía existe gran diversidad de implementaciones, tanto en infraestructura como en funcionalidades y precio.

Debido a lo anterior para el análisis de costo se tomará como base el precio de una red alámbrica y mediante porcentajes comparativos se establecerá la diferencia entre el precio de tres infraestructuras de red inalámbricas. Para dicho comparativo se considerarán infraestructuras para veinte usuarios, según los diagramas mostrados para cada caso.

7.6.1 Red alámbrica

Una red LAN alámbrica básicamente, consta de un *switch* o *hub*, de cableados dedicados a cada usuario y de tarjetas de red. Sus funcionalidades son, usualmente las que se mencionan a continuación:

- Puertos a velocidades de 10/100 Mbps y modos Full o Half duplex
- Soporte de VLAN's
- Utilización de enlaces troncales
- Seguridad a nivel MAC en cada uno de sus puertos (en caso de tratarse de un *Switch*)
- Administración remota vía telnet y vía browser
- Ancho de banda dedicado para cada usuario

La infraestructura para este tipo de red es la que se muestra en la siguiente figura.

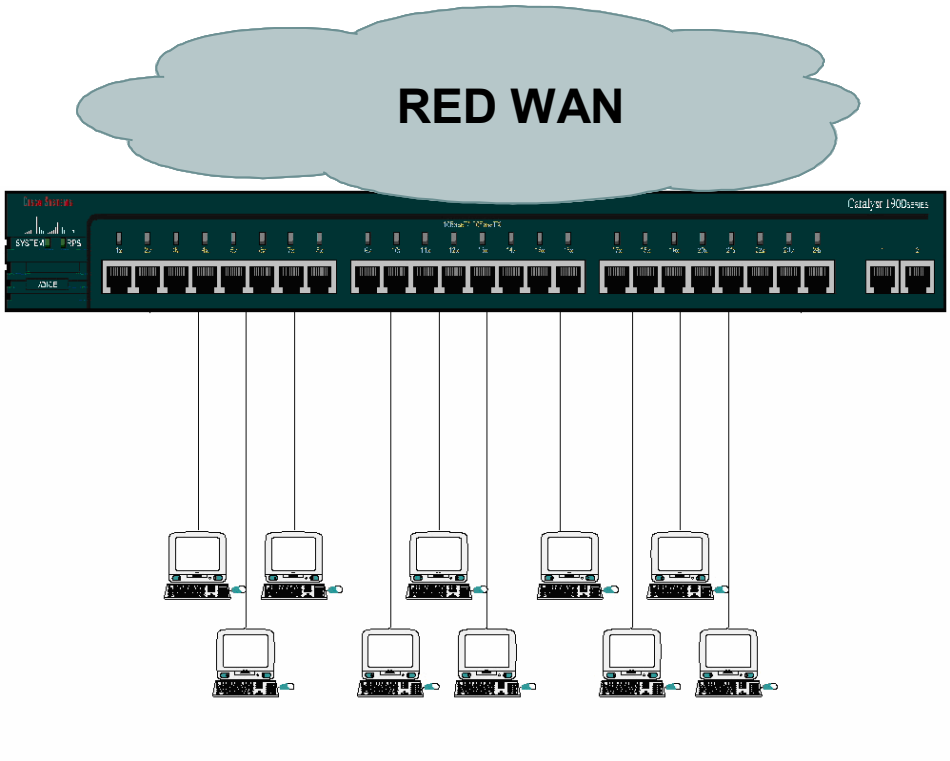


Figura 7-6. Diagrama de una red LAN alámbrica

El costo de esta infraestructura LAN considerando únicamente los cableados, el *switch* y las tarjetas de red alámbricas, se describe en la siguiente tabla.

Dispositivo	Descripción	Costo unitario(USD)
Switch (CA[3])	24 puertos 10/100 Mbps	2495.00
Cableado UTP	Nodo de red sencillo	107.00
Tarjeta de red	Velocidad 10/100 Mbps	12.00

Tabla 7-3. Distribución de costos para la red LAN alámbrica

Con base en la información anterior, el costo total de la red alámbrica para viente usuarios es de aproximadamente 4875 USD.

7.6.2 Redes inalámbricas

El costo de una red inalámbrica puede variar dependiendo del nivel de seguridad y de las funcionalidades de los dispositivos como las que se indican a continuación:

- Soporte de un esquema de seguridad adicional al especificado en el estándar.
- Soporte de algunas funcionalidades adicionales como VLAN's, balanceo de carga, redundancia, administración remota vía browser y telnet, troncales, etc.

[3] CA: Especifica que la alimentación del swtich es de corriente alterna.

A continuación se describen las características y el precio de las implementaciones de tres proveedores de dispositivos WLAN.

7.6.2.1 Proveedor 1

El primer proveedor a analizar es uno de los más básicos en cuanto a funcionalidades e infraestructura, la cual se muestra en la siguiente figura.

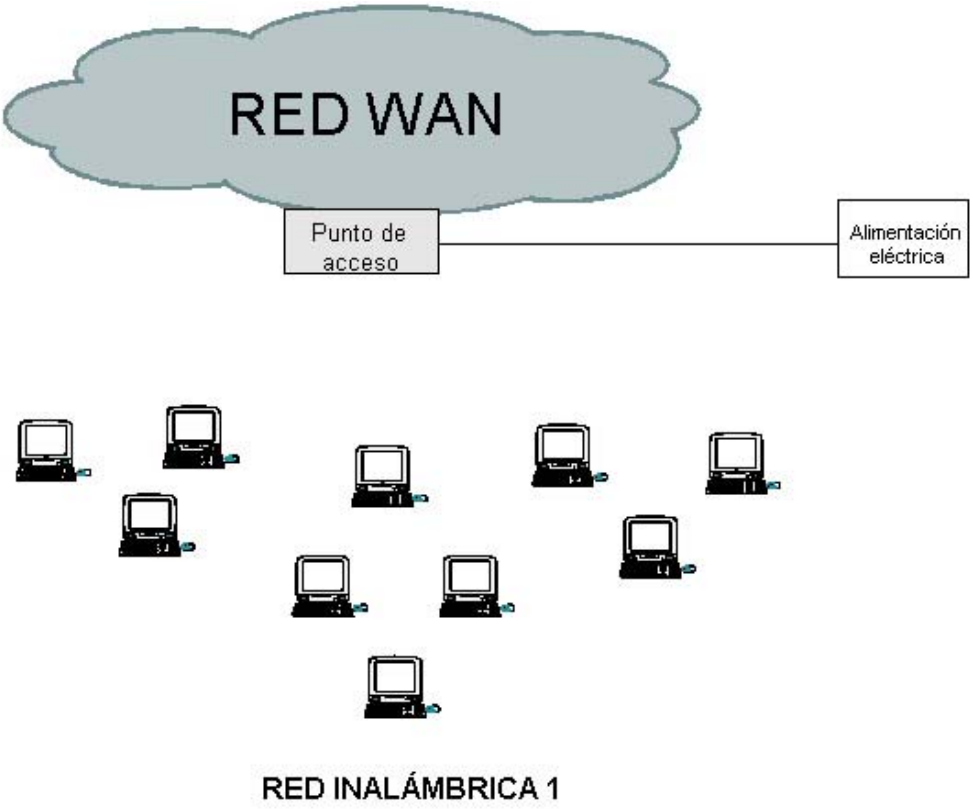


Figura 7-7. Infraestructura de una red LAN inalámbrica del proveedor 1

La infraestructura del proveedor 1 consta de un punto de acceso que no tiene la opción de incluir la alimentación eléctrica en el mismo medio físico (cable ethernet) de transporte de datos. La implementación ofrece las siguientes funcionalidades:

- SSID (Service Set Identifier) con opción a que éste no se propague por medio de *broadcast*, evitando así que analizadores de protocolos lo detecten.
- Autenticación por dirección MAC.
- Autenticación abierta
- Autenticación con clave WEP de 128 bits
- Administración remota vía Web
- Roaming

El costo por dispositivo es el que se menciona en la siguiente tabla:

Dispositivo	Descripción	Costo Unitario(USD)
Punto de acceso	1 puerto 10/100 Mbps, 1 antena dipolo.	69.90
Tarjetas de red	Tarjeta inalámbrica	59.99

Tabla 7-4. Distribución de costos para la red inalámbrica 1

Con base en la información anterior el costo de esta infraestructura para veinte usuarios es de 1269.7 USD, por lo tanto es 73.95 % más barata que el modelo de la red alámbrica.

7.6.2.2 Proveedor 2

El proveedor 2 ofrece el servicio WLAN con una infraestructura más compleja en cuanto a componentes, ya que cuenta con veinte tarjetas inalámbricas, un punto de acceso y un dispositivo denominado Sistema de potencia que permite que en el mismo cable se transporte la alimentación eléctrica y los datos; además también se requiere de un Controlador de puntos de acceso, el cual es el encargado de ejecutar todas las funcionalidades ofrecidas por el proveedor. Es muy importante considerar que tanto el Controlador de puntos de acceso como el Sistema de potencia, soportan hasta diez puntos de acceso. Lo anterior se ilustra en la siguiente figura.

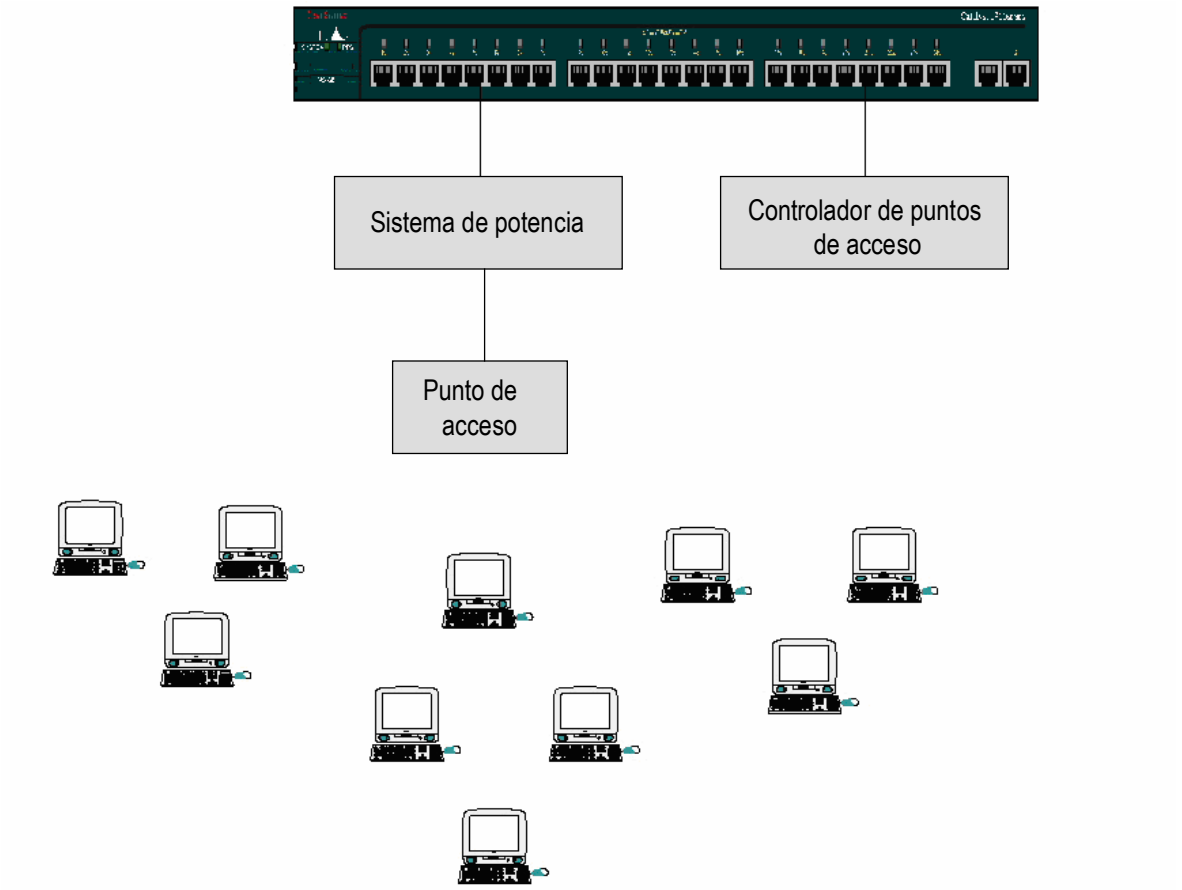


Figura 7-8. Infraestructura de una red LAN inalámbrica del proveedor 2

Por el tipo de infraestructura, para este caso es necesario un *switch*, ya que no es como en el caso anterior, en el que se considera que la conexión del punto de acceso puede ser a un a un *switch* o a un enrutador directamente.

Las funcionalidades ofrecidas por este proveedor son las que se describen a continuación:

- SSID (Service Set Identifier).
- Autenticación abierta
- Autenticación con clave WEP de 40 y128 bits
- Redundancia
- Balanceo de carga
- Autenticación por dirección MAC
- Roaming
- Administración remota vía Web
- Protocolo de autenticación propietario, para reforzar la seguridad.
- Estadísticas de paquetes transmitidos y recibidos

Para la estimación total del costo se consideraron los precios unitarios mencionados en la siguiente tabla:

Dispositivo	Descripción	Costo unitario(USD)
Switch (CA)	24 puertos 10/100 Mbps	2495.00
Punto de acceso	1 puerto 10/100, 1 antena dipolo.	645.00
Controlador de puntos de acceso	Capacidad de controlar a 10 puntos de acceso	1495.00
Sistema de potencia, con capacidad para 10 puntos de acceso	Permite que la alimentación eléctrica sea proveída por el cable UTP.	695.00
Tarjetas de red	Tarjeta inalámbrica	149.00

Tabla 7-5. Distribución de costos para la red inalámbrica 2

Con base en la información anterior el costo total de la infraestructura del proveedor 2 para veinte usuarios es 8310 USD, por lo tanto es 70.46 % mayor que el costo de la red cableada. Con esta cifra es claro que existe gran diversidad en precio de los diferentes proveedores, puede haber implementaciones muy baratas como la del proveedor 1, pero sacrificando seguridad y rendimiento.

7.6.2.3 Proveedor 3

El proveedor 3 ofrece una infraestructura que cuenta con veinte tarjetas inalámbricas PCMCIA, un punto de acceso y un dispositivo Inyector de potencia que permite transportar la energía eléctrica en el cable UTP categoría 5. En la siguiente figura se muestra el diagrama de la infraestructura.

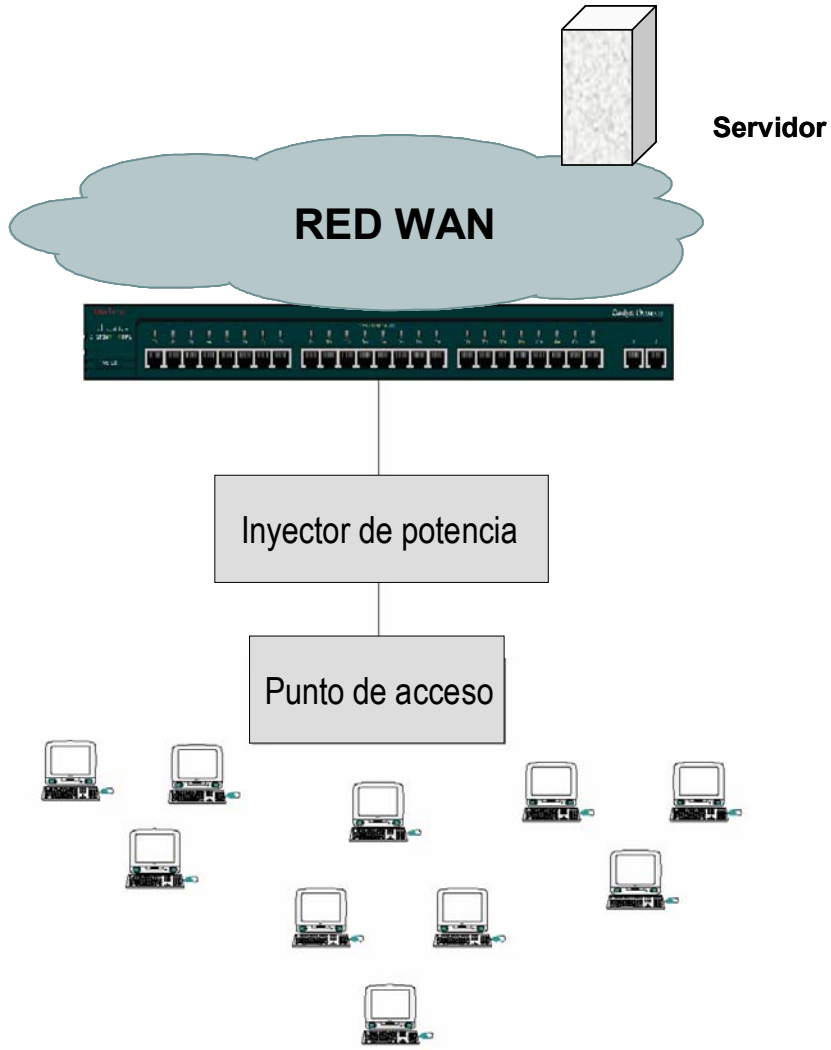


Figura 7-9. Infraestructura de una red LAN inalámbrica del proveedor 3

La infraestructura anterior ofrece las siguientes funcionalidades:

- SSID (Service Set Identifier)
- Autenticación abierta
- Autenticación con clave WEP de 40 y 128 bits
- Redundancia
- Enlaces troncales y VLAN's
- Balanceo de carga a partir de 10 usuarios
- Autenticación por dirección MAC
- Roaming
- Administración remota vía Web y telnet.

- Administración vía puerto de consola
- Protocolo de autenticación propietario, para reforzar la seguridad.
- Estadísticas de paquetes transmitidos y recibidos
- TKIP
- MIC
- Autenticación EAP

TKIP es una nueva especificación de seguridad para las WLAN que incluye dos funcionalidades PPK (*Per-Packet Keying*) y MIC (*Message Integrity Check*). El primero permite que los paquetes sean transmitidos con diferente clave WEP, de acuerdo con un tiempo configurable en el punto de acceso; el segundo protege las tramas WEP, realizando una función equivalente al CRC en las tramas ethernet; se calcula un valor MIC antes de la transmisión, dependiendo del contenido de la trama, y al ser recibida este valor se recalcula, permitiendo saber si la trama ha sido alterada.

Es importante mencionar que para la implementación de la infraestructura del Proveedor 3, es necesaria la adquisición de la licencia de un software adicional que evidentemente aumenta el costo. Las principales funciones de dicho software están relacionadas con la seguridad (LEAP, TKIP, MIC, autenticación por MAC, registro de puntos de acceso, asignación de claves de usuario y contraseñas).

El costo de la infraestructura de este proveedor para una red WLAN de veinte usuarios es mayor que la red cableada, véase la siguiente tabla:

Dispositivo	Descripción	Costo unitario (USD)
Punto de acceso	1 puerto 10/100, 1 antena dipolo con ganancia de	899.00
Licencia para servidor	Sofware que realiza las funciones de un servidor RADIUS[4], para un número infinito de usuarios.	5995.00
Servidor	Los servidores varían de 4000 a 30000 USD según la marca y equipamiento,para este ejemplo consideraremos un precio de 5000.	5000.00
Inyector de potencia	Permite que la alimentación eléctrica sea proveída por el cable UTP.	59.00
Tarjetas de red	Tarjeta inalámbrica	169.00

Tabla 7-6. Distribución de costos para la red inalámbrica 3

[4] RADIUS. *Remote Access Dial In User Service*

De acuerdo con la información anterior, se deduce que el costo total para este tipo de infraestructura con veinte usuarios es 15,333 USD por lo que el precio es 214.52% mayor que el de la red cableada.

7.6.3 Gráfica comparativa

Como una manera de visualizar mejor la diferencia de precios en las infraestructuras antes mencionadas, en la siguiente gráfica se muestra el costo de cada una de las implementaciones, considerando ahora, redes alámbrica e inalámbrica de 100 usuarios.

Para la realización de la siguiente gráfica se tomaron en cuenta 25 usuarios por punto de acceso y 22 por *switch* para el caso de la red alámbrica.

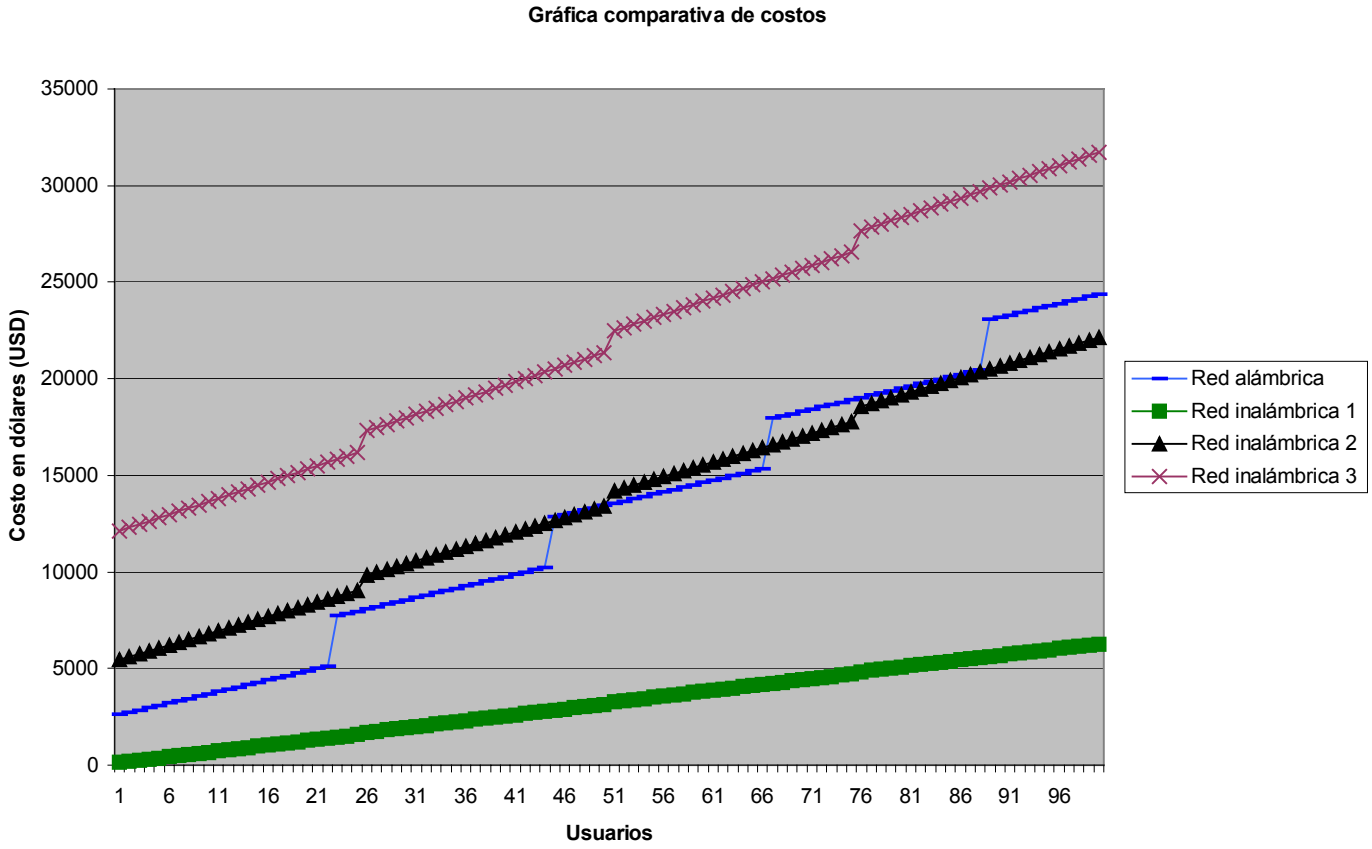


Figura 7-10. Tabla comparativa de costos entre ambos tipos de redes

De la gráfica anterior se puede concluir que la implementación de una red inalámbrica con la seguridad básica, es de mucho menor costo que la red alámbrica y al considerar un nivel de seguridad mayor con funcionalidades adicionales a las definidas por el estándar, el costo

se eleva de manera considerable. Otro punto a destacar es que la relación entre costo y número de usuarios es directamente proporcional.

7.7 Síntesis

Con el fin de resumir todas las características mencionadas anteriormente, se presenta la siguiente tabla comparativa entre la red alámbrica y los tres proveedores de dispositivos de red inalámbrica.

Característica	Red alámbrica	Red inalámbrica Proveedor 1	Red inalámbrica Proveedor 2	Red inalámbrica Proveedor 3
Apego a las especificaciones de los estándares correspondientes	Total	Total	Total	Total
Madurez del estándar que las rige.	Alta	Mediana	Mediana	Mediana
Interoperabilidad con dispositivos LAN de diferentes fabricantes.	Total	Total	Total	Total
Interoperabilidad con dispositivos WLAN de diferentes fabricantes.	Total	Parcial	Parcial	Parcial
Rendimiento real	7 Mbps por usuario	6.2 Mbps compartido	6.2 Mbps compartido	6.2 Mbps compartido
Movilidad	Baja	Alta	Alta	Alta
Facilidad de implementación	Baja	Alta	Mediana	Mediana
Seguridad	Alta	Baja	Mediana	Alta
Costo	Mediano	Bajo	Mediano	Alto
Funcionalidades adiciones a las especificadas por el estándar IEEE 802.11b		• SSID (Service Set Identifier) • Autenticación por dirección MAC. • Autenticación abierta • Autenticación con clave WEP de 128 bits • Administración remota vía	• SSID (Service Set Identifier). • Autenticación abierta • Autenticación con clave WEP de 40 y128 bits • Redundancia • Balanceo de carga • Autenticación por dirección	• SSID (Service Set Identifier). • Autenticación abierta • Autenticación con clave WEP de 40 y 128 bits • Redundancia • Enlaces troncales y VLAN's. • Balanceo de

		Web • Roaming	MAC • Roaming • Administración remota vía Web • Protocolo de autenticación propietario, para reforzar la seguridad. • Estadísticas de paquetes transmitidos y recibidos	carga a partir de 10 usuarios • Autenticación por dirección MAC • Roaming • Administración remota vía Web y telnet. • Administración vía puerto de consola • Protocolo de autenticación propietario, para reforzar la seguridad. • Estadísticas de paquetes transmitidos y recibidos • TKIP • MIC • Autenticación EAP

Tabla 7-7. Síntesis de las características de las redes LAN alámbrica e inalámbrica

CAPÍTULO 8. Conclusiones

De acuerdo con el análisis realizado en el capítulo anterior, se concluye que los aspectos más importantes a considerar en la elección de una red LAN alámbrica o inalámbrica, dependerán de las necesidades específicas de cada empresa, las cuales pueden ser el rendimiento, costo, movilidad y seguridad. La selección final estará comprometida a obtener la mejor relación costo-beneficio para la empresa o usuario.

El rendimiento debe ser considerado cuando el usuario pretenda la implementación de aplicaciones que requieran gran procesamiento de datos como interfaces gráficas, voz sobre IP, video conferencia, etc. En este caso es de suma importancia elegir el mayor ancho de banda posible para evitar saturaciones en la red. Por otro lado las aplicaciones de menor procesamiento, pueden ser implementadas en redes de rendimiento limitado.

Indudablemente el costo de una red está directamente relacionada con el equipamiento y cableado, por lo regular la infraestructura alámbrica es más costosa que la inalámbrica principalmente por los cableados desplegados a cada uno de los usuarios, por lo que cuando se pretenda crear una red permanente que dará servicio por un largo periodo de tiempo es conveniente la implementación de una red alámbrica; de lo contrario para redes provisionales o que requieran de una rápida implementación es conveniente optar por la red inalámbrica. Otro factor que influye en el costo de la infraestructura es la seguridad; recordemos que una red LAN inalámbrica está respaldada por infraestructura alámbrica y en ambas infraestructuras deben estar implementados esquemas de seguridad que protejan la información sobre todo si se trata de una red privada. El no tener asegurada una red implica un gran riesgo para la información confidencial de una empresa corporativa, el hecho de dejar desprotegida este tipo de información puede propiciar el mal uso de la misma ocasionando graves problemas dentro de la empresa, incluso la quiebra. Algunos ejemplos de información confidencial son los siguientes: listas de precios, evolución estratégica de la empresa, información sobre la nómina del personal, información sobre diseños tecnológicos, entre otros. Por lo anterior se deduce que la seguridad es el punto más importante a tomar en cuenta por el usuario que necesita tomar la decisión correcta. Si la red a implementar no requiere de seguridad, por ejemplo las utilizadas para Internet en los restaurantes, hoteles, en el hogar o en cualquier otro lugar, es posible prescindir de dispositivos más sofisticados que elevan el nivel de seguridad. Sin embargo es necesario hacer énfasis en que ningún tipo de red es 100 % segura, por lo que nunca está de más un esquema seguridad, ya sea en la red LAN o en la WAN.

La movilidad es una comodidad para el usuario, ya que en las redes alámbricas es problemático cambiar de ubicación constantemente, debido a que se requiere de modificaciones en el cableado. Además en las redes inalámbricas públicas, los usuarios pueden tener acceso a Internet, desde lugares como aeropuertos, restaurantes, hoteles, etc. Con la movilidad, la productividad de las personas de trabajo se incrementa, ya que mediante el uso de redes públicas se puede tener acceso a las redes privadas y desde cualquier lugar estar completamente informado para tomar las mejores decisiones.

En cuestión de escalabilidad, podemos decir que una red alámbrica no hay limites de crecimiento, siempre y cuando la red WAN tenga la suficiente capacidad de procesamiento. Sin embargo en una red inalámbrica sí existe un número finito de dispositivos (puntos de acceso) a instalar, para garantizar el buen funcionamiento de la misma.

En general la elección de una red LAN alámbrica o inalámbrica depende de las necesidades del usuario, si se requiere rapidez de instalación, movilidad, bajo costo y las aplicaciones no demandan gran ancho de banda, es conveniente la red inalámbrica, aunque se tenga que sacrificar el rendimiento y la seguridad. Por otro lado si desea implementar una red que dará servicio durante un largo periodo de tiempo, con excelente rendimiento y estricta seguridad, la mejor opción es una red alámbrica. Obviamente se si cuenta con un amplio presupuesto, es posible que ambos tipos de redes LAN puedan convivir, complementándose mutuamente.

Las redes inalámbricas son muy útiles en restaurantes, aeropuertos, centros de convenciones, en lugares donde se requieren redes provisionales, en oficinas pequeñas y en el hogar. Mientras que las redes alámbricas son convenientes en lugares, donde se manejan grandes flujos de información y el rendimiento, en conjunto con la seguridad, sean factores fundamentales.

En México, el estándar IEEE 802.11b está perfectamente regulado ante la COFETEL[1] y actualmente, redes LAN inalámbricas, regidas por este estándar, se encuentran operando en los aeropuertos, universidades, hoteles, centros de convenciones y en algunos restaurantes; además de empresas del sector privado.

En nuestro país se vislumbra que las redes inalámbricas basadas en el estándar IEEE 802.11b aumentarán, y paulatinamente irán evolucionando al estándar IEEE 802.11g que opera a la misma frecuencia (2.4 GHZ) pero con mayor ancho de banda (54 MHz). Los dispositivos diseñados para el estándar IEEE 802.11g serán totalmente compatibles con el estándar IEEE 802.11b. En general, las redes alámbricas continuarán su evolución, sobre todo para aumentar la velocidad de transmisión.

El estándar IEEE 802.11a, que opera a 54MHz, en la banda de los 5MHz, también está regulado ante la COFETEL, y probablemente se implemente a mediano plazo, el problema es que este estándar, aunque puede coexistir con el IEEE 802.11b sin causar interferencia, no es compatible con él, por lo que los usuarios que actualmente lo utilizan, tendrían que implementar una nueva infraestructura inalámbrica para el estándar IEEE 802.11a. Por lo anterior sería más complicada la instalación de redes basada en este estándar porque la banda de la frecuencia de operación no es una banda libre de licencias como lo es en otros países, por ejemplo, Estados Unidos y Europa.

[1] COFETEL. Comisión Federal de Telecomunicaciones.

GLOSARIO

A

- **ACK** (*ACKnowledge*). Bit usado en los paquetes para indicar que el paquete anterior ha sido recibido correctamente.
- **Autenticación**. Procedimiento de seguridad durante el cual, dos dispositivos verifican que ambos poseen la misma clave secreta.

B

- **BPDU** (*Bridge Protocol Data Units*). Existen dos tipos de BPDU´s, los de configuración y los de notificación de cambio de topología; los primeros son originados por el *switch* raíz y se transmiten a través de las rutas activas difundidas desde dicho *switch*; mientras que los otros son flujos recibidos por el *switch* raíz, que contienen información de cambios de topología, estos últimos son originados por el *switch* que tuvo cambio en sus puertos.
- **Broadcast**. mensajes que son recibidos por todas las demás estaciones.
- **BSS** (*Basis Service Set*). Se define en el estándar IEEE 802.1b, como la infraestructura básica de una red LAN, que consta de un punto de acceso y varios clientes asociados a él.

C

- **CRC (***Cyclic Redundancy Check***).** Es una técnica de verificación de errores en la que el receptor de la trama calcula un residuo, dividiendo el contenido de la trama entre un binario primo, y lo compara con un valor almacenado en la trama del emisor.
- **CSMA/CA** (*Carrier Sense Multiple Access / Collision Advoidance*). Técnica de acceso al medio para las transmisiones inalámbricas.
- **CSMA/CD** (*Carrier Sense Multiple Access / Collision Detect*). Técnica de acceso al medio utilizada en las redes Ethernet e IEEE 802.3.

D

- **DIFS (***Distributed Inter Frame Space*). Intervalo de tiempo que puede debe esperar la estación antes de transmitir en el medio inalámbrico

E

- **ESS** (*Extended Service Set*)**.** Conjunto de BSS's, donde los puntos de acceso se comunican entre sí.

H

- **Hello.** Paquete utilizado por los enrutadores para descubir y recuperar vecinos. Estos paquetes también indican que un cliente aún está funcionando.

I

- **IBSS** (*Independent Basic Service Set*). En el estándar IEEE 802.11b, define esta topología para dispositivos cliente que se comunican entre sí, sin necesidad de utilizar un punto de acceso.
- **IEEE** (*Institute of Electronic and Electrical Engineers*). El Instituto de ingenieros eléctricos y electrónicos es una organización profesional cuyas actividades incluyen, el desarrollo de los estándares de comunicaciones.
- **ICMP** (*Intenet Control Message Protocol*). Protocolo de Internet de la capa de red que reporta errores y proporciona otra información relevante al procesamiento de paquetes IP.
- **IGP** (*Interior Gateway Protocol*)**.** Protocolo de Internet que se utiliza para el intercambio de información dentro de un sistema autónomo.
- **IGRP** (*Interior Gateway Routing Protocol*)**.** IGP desarrollado por Cisco para resolver los problemas asociados con el enrutamiento en redes heterogéneas de gran tamaño.
- **IP** (*Internet Protocol*). Protocolo de Internet que provee de direccionamiento, transporte y segmentación.
- **ISM** (*Industrial, Scientific and Medical*). Bandas de frecuencias disponibles sin licencia, ubicadas en los rangos: 902-908 Mhz, 2.4-2.5 GHz y 5.8-5.9 GHz.
- **ISO** (*International Organization for Standardization*). La Organización Internacional para la Normalización es una federación mundial de entidades nacionales de normalización que comprende alrededor de cien países, integrando una entidad por cada país. La misión de ISO es la de promover en todo el mundo el desarrollo de la normalización y otras actividades relacionadas con ella con vista a facilitar el intercambio internacional de bienes y servicios, asimismo desarrollar la cooperación en el ámbito de las actividades intelectuales, científicas, tecnológicas y económicas.
- **ITU-T** (*Internacional Telecomunication Union-Telecommunication*). Organización internacional que desarrolla estándares para las diferentes tecnologías de las telecomunicaciones a nivel mundial. La ITU-T realiza las funciones que desempeñaba CCITT.

- **L**

- **LAN** (*Local Area Network*). Red de datos de alta velocidad y baja tasa de errores que cubre un área geográfica relativamente pequeña. Los estándares de las LAN especifican el cableado y la señalización en las capas física y de enlace de datos del modelo OSI.
- **LLC** (*Logical Link Control*). Es la subcapa más alta de las dos incluidas dentro de la capa de enlace de datos. LLC maneja el control de errores, el control de flujo y el direccionamiento de la subcapa MAC.

M

- **MAC** (*Media Access Control*)**.** Es la subcapa inferior de las dos incluidas en la capa de enlace de datos. MAC maneja el acceso a medios compartidos.
- **MD5** (*Message Digest*)**.** Algoritmo utilizado para la autenticación que verifica la integridad de la comunicación.
- **Microonda.** Onda electromagnética cuya longitud de onda es muy pequeña, del orden de centímetros.
- **Multicast.** Es una tecnología que reduce el tráfico al mismo tiempo que entrega un flujo de información único a múltiples oficinas corporativas y hogares. Entre las aplicaciones que toman mayor ventaja de Multicast se incluyen la videoconferencia las comunicaciones corporativas, aprendizaje a distancia así como distribución de software, noticias y hasta el valor de las acciones de la empresa en la bolsa de valores.

O

- **Onda electromagnética.** Perturbación de carácter ondulatorio asociada con un campo eléctrico y otro magnético, perpendiculares entre sí, variables con el tiempo, que se producen por cargas eléctricas aceleradas.
- **OSI** (*Open System Interconnect*). Modelo de referencia cuya finalidad es garantizar la interoperabilidad entre sistemas abiertos; creado por la ISO y la ITU-T para desarrollar estándares para las redes de datos que faciliten la interoperabilidad de diferentes equipos.

P

- **PDA** (*Personal Digital Assistant*). Asistente digital personal, el cual es un dispositivo pequeño y portátil. Incluye las características de agenda, almacenamiento de datos, correo electrónico, etc.
- **PDU** (*Protocol Data Unit*). Agrupación lógica de información que incluye un encabezado que contiene información de control y ,generalmente, datos de usuario.

R

- **Ranura de tiempo** (*Slot Time*). Lapso utilizado para transmitir o recibir datos. El uso de ranuras es necesario en el multiplexaje por división de tiempo para compartir el canal de comunicaciones entre varios dispositivos.

S

- **SAP** (*Service Access Point*)**.** Son puntos lógicos localizados entre las capas del modelo de referencia OSI que permiten la comunicación entre ellas.

- **STA** (*Spanning Tree Algorithm*)**.** Algoritmo utilizado en los *switches* para asegurar que sólo exista una ruta para cada destino en una red LAN.
- **STP** (*Spanning Tree Protocol*). Es un protocolo de capa dos diseñado para *switches*, cuyo propósito principal es evitar *loops* en redes con topología redundante. La norma referente a este protocolo es la IEEE 802.1d.

T

- **TCP** (*Transmission Control Protocol*). Protocolo orientado a conexión que pertenece a la capa de transporte y que ofrece una transmisión confiable de datos en modo *Full Duplex.*
- **Temporizador** (*Timer*). Reloj de cuenta regresiva que indica que debe producirse una determinada acción al finalizar dicha cuenta.

U

- **UDP** (*User Datagram Protocol*). Es un protocolo de capa de transporte no orientado a conexión es decir, que intercambia datagramas sin reconocimientos (*acknowledges*) y por lo tanto el procesamiento de errores y la retransmisión son manejados por protocolos de capas superiores.
- **Unicast**. Esquema de transmisión de información donde un paquete se envía a un solo destino específico en la red.

V

- **VLAN** (*Virtual Local Area Network*). LAN basada en conexiones lógicas, lo cual permite que en una misma conexión física existan varios segmentos de red.

W

- **WAN** (*Wide Area Network*). Red de datos que da servicio a usuarios localizados en un área geográfica amplia.
- **WECA** (*Wireless Ethernet Compatibility Alliance*). Organización que tiene como misión certificar la capacidad de interoperabilidad de los productos WLAN, identificándolos con la etiqueta *WiFi*.
- **WEP** (*Wired Equivalent Privacy*). Es una característica especificada por la norma IEEE 802.11b, que permite la integridad de datos en un enlace inalámbrico, utilizando el algoritmo RC4 mediante una clave de 40 bits o de 128 bits.
- **WIFI** (*Wireless Fidelity*). Es un logotipo que indica la interoperabilidad de un equipo y es avalado por la WECA.
- **WLAN (***Wireless Local Area Network***)**. Red LAN inalámbrica.

Apéndice 1. Número de puertos

La tabla de número de puertos está dividida en tres grandes rangos:

- Los puertos bien conocidos, del puerto 0al 1023
- Los puertos registrados, del puerto 1024 al 49151
- Los dinámicos y/o puertos privados, del puerto 49152 al 65535

Cada proceso que se comunica con otro proceso se identifica a sí mismo con un puerto específico de la familia de protocolos TCP/IP. Un puerto es un número de 16 bits, que especifica la dirección a la cual se dirige una conexión TCP o UDP. En un mismo *host*, un número de puerto puede ser utilizado simultáneamente por una aplicación para UDP y por otra para TCP, lo que es posible sin ocasionar conflicto alguno.

Los "bien-conocidos" los controla y asigna la IANA (Internet Assignet Names Authority) y en la mayoría de los sistemas sólo pueden usarlo los procesos del sistema o programas ejecutados con privilegios de usuario. Los puertos "bien-conocidos" asignados ocupan números de puerto en el rango de 0 a 1023. Los puertos con números dentro del rango 1024-65535 no los controla la IANA y la mayor parte de los sistemas únicamente usan programas desarrollados por usuarios.

Los puertos dinámicos son asignados aleatoriamente o utilizados en procesos privados. A continuación se mencionan puertos de las aplicaciones más comunes.

Puerto	Aplicación	Descripción
9	Discard	Descarta todos los datos recibidos (para pruebas)
19	Chargen	Intercambio de strings (para pruebas)
20	FTP-Data	Transferencia de datos en FTP
21	FTP	Intercambio de información de control en FTP
22	SSH	Sesión remota segura en una máquina
23	Telnet	Sesión remota en una máquina
25	SMTP	Envío de correos electrónicos a través de servidor de correos
53	DNS	Consultas y transferencia de datos de servicio de nombres
80	HTTP	Protocolo HTTP para intercambio de páginas web
110	POP3	Lectura de correo electrónico
139	NetBIOS	Intercambio de datos usando NetBIOS en redes locales con Windows
143	IMAP	Lectura de correo electrónico
179	BGP	Sesión de intercambio de información del protocolo BGP
443	HTTPS	Protocolo HTTP para intercambio de páginas web seguras
443	HTTPS	Protocolo HTTP para intercambio de páginas web seguras

Para la lista de todas las aplicaciones por puerto refiérase a la siguiente página web:

h**ttp://www.iana.org/assignments/port-numbers**

REFERENCIAS

Libros

1. Merilee Ford, "Tecnologías de interconectividad de redes", Prentice Hall, México, 1998.
2. Catherine Paquet, "Building Cisco Remote Access Network", Cisco Press, Indianapolis, 1999
3. Hecht Zajac, "Optica",Addison-Wesley Iberoamérica, México, 1986.

Cursos

1. "Interconecting Cisco Network Devices", Mexico D.F, 2001.
2. "Building Cisco Multilayer Swiching Network", Mexico, D.F., 2002.
3. "Despliegue de la tecnología Wireless 802.11b, México, D.F., 2003
4. "Soluciones inalámbricas para redes de área local", México, D.F., 2003

Artículos

1. Luis Muñoz, Johnny Choque, "Optimizing Internet Flows over IEEE 802.11b Wireless Local Area Networks: A performance-enhancing Proxy based on forward error correction", IEEE Communications Magazine, diciembre 2001.
2. Roger O. Crocket, "All net, all the time", BusinessWeek Magazine, abril, 2002.
3. John Edwards, "Wireless Networking", BusinessWeek Magazine, agosto,2002.
4. Joanie Wexler, "A guide to wireless LAN", NetworkWorld, mayo. 2003.

Referencias eléctronicas

Cisco System:
www.cisco.com

Introducción a las redes inalámbricas:
http://mailweb.udlap.mx/~lgojeda/telecomsis/wireless_lan/indice.html

Redes locales inalámbricas:
http://www.unincca.edu.co/boletin/indice.htm

Artículo sobre el estándar IEEE 802.11b:
http://www.coit.es/publicac/publbit/bit138/wifi.pdf

Intel:
http://www.intel.com/es/home/trends/wireless/nw/transition.htm

Preguntas frecuentes sobre redes WLAN:
http://landatel.com/html/wireless2.html#FAQ7-WRL

Guía para redes WLAN:
http://www.sindominio.net/suburbia/article.php3?id_article=12

Síntesis de estándar IEEE 802.11b:
http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf

Redes WLAN:
http://www.kernelpanik.org/docs/kernelpanik/Wireless.pdf

Tutorial sobre WLAN:
http://www.sss-mag.com/pdf/802_11tut.pdf

Convivencia entre los estándares IEEE 802.11 b y Bluetoth:
http://dinki.mine.nu/coexist/Articles/TechnicalSpecificationsof-2.html