



UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISION DE INGENIERÍA ELÉCTRICA

“ARQUITECTURA Y FUNCIONAMIENTO DEL
ACCESO A INTERNET INALÁMBRICO Y LOS
ASPECTOS TÉCNICOS PARA SU IMPLEMENTACION”

INGENIERÍA EN TELECOMUNICACIONES

T E S I S

Que para obtener el titulo de

INGENIERO EN TELECOMUNICACIONES

PRESENTAN:

PÈREZ ROA CARLOS RICARDO
RONQUILLO VALDÉS SAÚL CERVANDO



DIRECTOR DE TESIS: DR. MIGUEL MOCTEZUMA

CIUDAD UNIVERSITARIA

2009

En agradecimiento a:

*La Universidad Nacional Autónoma de México,
que me brindó desinteresadamente su apoyo a lo
largo de mi formación profesional.*

*A mis profesores que dan su tiempo en las aulas
impartiendo enseñanzas académicas y de vida,
y a aquellos profesores que ya no están con nosotros
pero siguen en mi corazón.*

*A mis padres y mi hermano, que nunca me han dejado caer
y siempre han estado conmigo brindándome un gran apoyo
en el transcurso de mi vida.*

*Le agradezco a DIOS por permitirme concluir
ésta etapa de mi vida y continuar con nuevos proyectos
en compañía de mis seres queridos.*

En especial dedicatoria a:

A todos mis profesores y compañeros de toda la vida..

*A mis padres Saúl y Gloria, a mi hermano Mauricio, sé
que siempre cuento son ustedes, gracias por su apoyo y sus
consejos que han sido fundamentales en este camino .*

*A mi esposa Yolanda, que siempre esta conmigo y me da
aliento para continuar, quien me ha enseñado que siempre
hay una mano para levantarte cuando hay un tropiezo.*

*Ya mis dos luceros que iluminan mi camino día a día, mis
angelitos que me recuerdan siempre tener una sonrisa,
regalar un abrazo y a quienes puedo sobornar por un beso,
mis hijas:*

Natalia y Montserrat

*Se cierra un capítulo de este libro y se comienza con una nueva etapa, teniendo frente a mí a
nuevas generaciones, con quienes tengo el deber y la obligación de la enseñanza, abriendo el camino
para que éste sea menos áspero y se vislumbre claro el objetivo a donde queremos llegar.*

*Sin embargo va a ser necesario que yo también aprenda, comparta experiencias y en ocasiones
guarde silencio para escuchar, ya que para saber guiar es necesario haber aprendido a escuchar.*

Saúl Cervando Ronquillo Valdés

Durante estos escasos seis años de espera para culminar mi trabajo de tesis he tenido gratas vivencias, momentos de éxitos y angustias. Todo para poder cumplir mis objetivos, puedo decir que con éste trabajo alcanzo uno de mis más grandes anhelos, culminar mi carrera.

Es por ello que debo dedicar y agradecer este triunfo a quienes, en todo momento, me llenaron de amor y apoyo.

En agradecimiento a:

A Dios Todopoderoso por iluminarme el camino para seguir y que siempre está conmigo en los buenos y, sobre todo, en los malos momentos. Por llenar mi vida de dicha y bendiciones.

A La Universidad Nacional Autónoma de México y a mis profesores por su disposición y ayuda brindada.

A todos mis profesores no sólo de la carrera sino de toda la vida, mil gracias porque de alguna manera forman parte de lo que ahora soy.

Son muchas las personas especiales a las que me gustaría agradecer su amistad, apoyo, ánimo y compañía en las diferentes etapas de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en el corazón.

En especial dedicatoria a:

A mis Padres Onésimo y Martha. Pilares fundamentales en mi vida, dignos de ejemplo, trabajo y constancia. Quienes han brindado todo el apoyo necesario para alcanzar mis metas y sueños, han estado allí cada día de mi vida compartiendo los buenos y los malos ratos desde el día en que nací. . . . Los amo mucho y gracias, muchas gracias.

A mi esposa Alejandra porque siempre hay un Te Amo para seguir adelante. A mi pequeñita Sofía Ximena, por alegrarme con tus susurros y tu eterna mirada. A mis dos amores por brindarme esa paz y tranquilidad para levantarme cada día a dar lo mejor de mí para ustedes, los amo.

A mi hermano Oscar y hermanas Olga e Irene, a ti hermano porque me has enseñado a no dejarnos caer en cualquier circunstancia y a través de tu ejemplo me has sabido guiar y tomar las mejores decisiones. Te quiero Hermano, gracias.

Irene, cuñada. Te agradezco por estar al lado de mi hermano y quererlo como hasta hoy y se que directa o indirectamente siempre cuento con tu apoyo.

A ti hermanita. Eres la mejor hermana que pude haber tenido y no puedo dejar de decir gracias. Gracias por todos tus minutos donde me escuchaste y donde logramos comunicarnos para darnos ánimos y siempre seguir adelante, te quiero.

Y nuevamente al más especial de todos, a ti Señor porque hiciste realidad este sueño, por todo el amor con el que me rodeas y porque me tienes en tus manos. Esta tesis es para ti.

Carlos Ricardo Pérez Roa

“Por mi raza hablará el espíritu”

ÍNDICE DE CAPÍTULOS

	PAG.
INTRODUCCIÓN	6
OBJETIVOS	7
METODOLOGÍA	8
CAPITULO 1	
SERVICIOS Y CARACTERÍSTICAS DE LOS ISP	
1.1 INTRODUCCIÓN	9
1.2 CONEXIÓN A INTERNET Y SERVICIOS DE LOS ISP	10
1.2.1 FORMAS DE ACCESO A INTERNET	10
1.2.1.1 INTERNET DEDICADO	10
1.2.1.2 INTERNET MEDIANTE FRAME RELAY Y ATM	10
1.2.1.3 ACCESO TELEFONICO	10
1.2.1.4 LINEA DE ABONADO DIGITAL (DSL)	11
1.2.1.5 MODEMS POR CABLE	11
1.2.1.6 ACCESO INALAMBRICO	12
1.2.2 SERVICIOS	12
1.2.2.1 ALOJAMIENTO DEDICADO (WEB-HOSTING)	12
1.2.2.2 CORREO ELECTRONICO	13
1.2.2.3 MOTOR DE BUSQUEDA	13
1.2.2.4 OTROS SERVICIOS	13
CAPITULO 2	
FUNCIONAMIENTO GENERAL DE LAS REDES DE DATOS	
2.1 INTRODUCCION	14
2.2 REDES DE DATOS	15
2.3 MODELO DE REFERENCIA OSI (OPEN SYSTEM INTERCONNECTION)	16
2.3.1 PROCESO DE INTERCAMBIO DE INFORMACIÓN	16
2.3.2 CAPA FÍSICA	17
2.3.2.1 MEDIOS DE TRANSMISIÓN	17
2.3.2.2 TÉCNICAS DE CODIFICACIÓN	20
2.3.3 CAPA DE ENLACE	20
2.3.3.1 TOPOLOGÍAS	20
2.3.3.2 LLC	22



2.3.3.3 MAC	23
2.3.3.4 ETHERNET	24
2.3.3.4.1 MÉTODO DE ACCESO AL MEDIO CSMA/CD	26
2.3.3.5 TOKEN-RING	27
2.3.3.6 FDDI	28
2.3.4 CAPA DE RED	30
2.3.5 CAPA DE TRANSPORTE	31
2.3.6 CAPA DE SESIÓN	32
2.3.7 CAPA DE PRESENTACIÓN	32
2.3.8 CAPA DE APLICACIÓN	32
2.4 TCP/IP	33
2.4.1 IPv4	34
2.4.2 IPv6	36
2.4.2.1 DIRECCIONAMIENTO IPv6	37
2.4.2.2 NOTACION PARA LAS DIRECCIONES IPv6	38
2.4.2.3 IDENTIFICACION DE LOS TIPOS DE DIRECCIONES	39
2.4.2.4 PAQUETES IPv6	40
2.4.2.5 IPv6 Y EL SISTEMA DE NOMBRES DE DOMINIO	41
2.4.2.6 VENTAJAS Y DESVENTAJAS DEL USO DE IPv6	41
2.4.2.7 MECANISMOS DE TRANSICION A IPv6	42
2.4.3 TCP (TRANSMISSION CONTROL PROTOCOL)	43
2.4.4 IP (INTERNET PROTOCOL)	43
2.4.5 PROTOCOLOS DE TCP/IP	43
2.5 DHCP	44
2.5.1 RARP	44
2.5.2 BOOTP	45
2.5.3 OBJETIVOS DE DHCP	45
2.5.4 ESTRUCTURA DEL PAQUETE DE DHCP	47
2.5.5 ASIGNACION DE DIRECCIONES IP	49
2.5.6 DURACION DE LA CONCESIÓN DE DHCP	50
2.6 DIPOSITIVOS DE INTERCONEXION DE REDES	53
2.6.1 REPETIDORES	54
2.6.2 PUENTES (BRIDGES)	54
2.6.3 ENRUTADORES (ROUTERS)	54
2.6.4 GATEWAY	54

CAPITULO 3 INTERNET INALAMBRICO

3.1 INTRODUCCION	56
3.2 REDES LOCALES INALAMBRICAS, WLAN (WIRELESS LOCAL AREA NETWORK)	57
3.2.1 VENTAJAS Y DESVENTAJAS DE LAS REDES WLAN	57
3.2.2 FUNCIONAMIENTO DE UNA RED WLAN	58
3.2.3 TOPOLOGÍA DE LAS REDES WLAN	58
3.2.4 NORMALIZACIÓN	60
3.2.5 REGULACION DEL USO DE FRECUENCIAS EN MEXICO	61



3.3 ACCESO INALAMBRICO DE BANDA ANCHA (BROADBAND WIRELESS ACCESS, BWA)	64
3.3.1 ESPECTRO ENSANCHADO POR SALTO DE FRECUENCIA, FHSS	65
3.3.2 ESPECTRO ENSANCHADO POR SECUENCIA DIRECTA, DSSS	66
3.3.3 MULTIPLEXACIÓN POR DIVISIÓN DE FRECUENCIAS ORTOGONALES (OFDM)	68
3.4 ESTÁNDAR 802.11	70
3.4.1 INTRODUCCIÓN	70
3.4.2 CONFIGURACIONES DE RED	70
3.4.3 MODELO DE CAPAS	71
3.4.4 COMO SE AGREGA UNA ESTACION DE TRABAJO A UNA CELDA EXISTENTE	73
3.4.4.1 AUTENTICACION Y PRIVACIDAD	74
3.4.4.1.1 AUTENTICACION DE SISTEMA ABIERTO (OPEN SYSTEM)	74
3.4.4.1.2 AUTENTICACION DE LLAVE COMPARTIDA (SHARED KEY)	74
3.4.4.1.3 WEP (WIRED EQUIVALENT PRIVACY)	75
3.4.5 ROAMING O MOVILIDAD DE USUARIOS	76
3.4.6 SOPORTE DE VOZ Y VIDEO	77
3.4.7 CONSUMO	77
3.4.8 OTROS ASPECTOS	77
3.5. COMPARATIVA DE ESTÁNDARES	77
3.5.1 802.11b (2.4 GHz)	77
3.5.2 802.11g (2.4 GHz)	78
3.5.3 802.11a (5 GHz)	78
3.5.4 802.11n (2.4 y 5 GHz)	78
3.5.4.1 TECNOLOGÍA DE MÚLTIPLE ENTRADA MÚLTIPLE SALIDA, MIMO	79
3.5.4.2 UNIÓN DE CANALES (CHANNEL BONDING)	79
3.5.4.3 AGREGACIÓN DE PAQUETES	79

CAPITULO 4

EQUIPOS DE ACCESO INALAMBRICO A LA RED

4.1 INTRODUCCION	81
4.2 EQUIPOS DE ACCESO INALAMBRICO (INFRAESTRUCTURA DE LA RED)	82
4.2.1 PUNTO DE ACCESO, AP (ACCESS POINT)	82
4.2.2 ROUTER INALAMBRICO	83
4.2.3 MODEM/ROUTER INALAMBRICO, SERVICIO DE ADSL	85
4.3 DISPOSITIVO DE ACCESO INALAMBRICO A LA RED (CLIENTES)	86
4.3.1 TARJETAS INALAMBRICAS PCMCIA	86
4.3.2 TARJETAS INALAMBRICAS PCI	86
4.3.3 ADAPTADORES USB	87
4.3.4 TARJETAS PARA ORGANIZADORES PERSONALES	87

CAPITULO 5

ARQUITECTURA FUNCIONAL

5.1 SOLUCIÓN DE TECNOLOGÍA Y PRODUCTOS	88
5.1.1 TECNOLOGÍA APLICADA	88
5.1.2 ELECCIÓN DE PRODUCTOS	89



5.2 CÁLCULOS DEL DISEÑO DE LA RED	92
5.2.1 BASES DEL DISEÑO	92
5.2.2 CARACTERÍSTICAS DEL SITIO	92
5.2.3 NÚMERO DE USUARIOS CON ACCESO INALÁMBRICO	93
5.2.4 PRESTACIONES NECESARIAS DE LA RED	94
5.2.5 INTEGRACIÓN E INTEROPERABILIDAD CON OTRAS REDES	94

CAPITULO 6 EL FUTURO DE LAS REDES INALAMBRICAS

6.1 INTRODUCCION	96
6.2 CARACTERISTICAS DE WIMAX	97
6.3 WIMAX FIJO Y WIMAX MOVIL	97
6.4 COMPARACION DE WIMAX FIJO Y WIMAX MOVIL	99
6.5 EL MERCADO DE WIMAX	100

CAPITULO 7 CONCLUSIONES

ANEXO GLOSARIO	103
---------------------------	-----

REFERENCIAS BIBLIOGRAFICAS	109
-----------------------------------	-----

INDICE DE TABLAS	110
-------------------------	-----

INDICE DE IMAGENES	111
---------------------------	-----

INTRODUCCIÓN

Después del impacto y la ayuda que trajo Ethernet con las redes tradicionales cableadas, hoy en día se ha expandido y evolucionado la tecnología abriendo paso a las comunicaciones inalámbricas. La necesidad de una constante comunicación, han propiciado el crecimiento de las redes locales de tipo inalámbrico. En México, este servicio está creciendo constantemente, instalándose puntos de acceso a Internet en restaurantes, aeropuertos, hospitales, plazas comerciales, etc., permitiendo la conexión a Internet mediante el servicio que el ISP brinda, el cliente puede acceder usando dispositivos que van desde una computadora portátil hasta un organizador personal (PDA) o un teléfono celular con tecnología WiFi. Es común que el empresario de estos tiempos necesite revisar su correo electrónico y estar en contacto con los trabajadores de su oficina prácticamente en cualquier lugar a donde vaya.

Trasladando este esquema a una red de carácter privado, podemos pensar en los meseros que toman la orden e inmediatamente les aparece en el servidor de la cocina y en la caja de cobro; en el hospital donde los enfermeros tienen que actualizar las bases de datos de los enfermos en tiempo real, o en el edificio donde se encuentran nuestras oficinas, así estando en una junta con los jefes podemos conectarnos al punto de acceso inalámbrico más cercano a nosotros, teniendo a nuestro alcance los recursos de la red local o tener salida a Internet si nuestro administrador de red lo permite. O simplemente se puede implementar una red local inalámbrica en el hogar u oficina para permitir la movilidad al usuario, y complementado con un servicio de ADSL podemos dar salida a Internet a todos los usuarios de nuestra red. Analizando estos dos esquemas, tanto el acceso directo a Internet mediante el servicio de un ISP, como el acceso a los recursos de la red local del lugar de trabajo o del hogar, podemos entender que la tecnología inalámbrica está situada inmediatamente después del cliente.

Partiendo de la importancia del tema y del auge que están teniendo en estos días las redes inalámbricas en México, principalmente el acceso inalámbrico a Internet, esta tesis tiene como objetivo la descripción y exponer al usuario de una red la forma en que puede acceder a Internet, principalmente, y para la implementación de una red local de tipo inalámbrico.

La siguiente tesis comprende 7 capítulos, los primeros 2 capítulos tratan de conceptos básicos exponiendo un panorama completo acerca de las redes de datos. El capítulo 1 habla acerca de los servicios que un Proveedor de



Internet puede brindar, así como los diferentes tipos de conexión que se han tenido para el acceso a Internet. En el capítulo 2 se tocan temas referentes a los conceptos de las redes de datos, topologías, medios de transmisión, protocolos, direccionamiento IP y el Modelo de Referencia OSI, entre otros. A partir del capítulo 3 al 5 se habla de las redes inalámbricas, en el capítulo 3 se tienen temas como redes inalámbricas locales (WLAN), topologías, se habla acerca del estándar de la IEEE 802.11 y en el transcurso del capítulo se habla de porque no se usan otras tecnologías como IRDA, Bluetooth, Home RF. El capítulo 4 expone equipos para el acceso a redes inalámbricas, se hace una clasificación de dos tipos, por un lado se tienen equipos propios de la infraestructura de la red que tienen funciones de Puntos de Acceso, y por otro lado se tienen equipos que el cliente usa para tener el acceso, como accesorios periféricos de su estación de trabajo. En el capítulo 5 se plantea un pequeño sitio para el acceso inalámbrico, proponiendo marcas y analizando costos. Es capítulo 6 es un agregado que nos da un panorama de las futuras redes inalámbricas en México, cabe mencionar estas mismas ya se emplean en otros países en Latinoamérica y Europa, habla acerca del surgimiento de las redes inalámbricas de carácter metropolitano. Finalmente el capítulo 7 son las conclusiones a las cuales llegamos haciendo la presente tesis.

El contenido de la tesis está estructurado de tal forma que, teniendo las bases teóricas y los antecedentes de una red local tradicional, se haga una vinculación y al mismo tiempo una comparativa entre redes cableadas e inalámbricas y así anteponer la simplicidad y ventajas que una red inalámbrica brinda sobre la red local tradicional.

OBJETIVOS.

Describir la arquitectura y el funcionamiento del acceso inalámbrico a Internet así como anteponer las ventajas de una red de tipo inalámbrico a las de una red cableada.

Disponer de una referencia para la implementación de un sitio pequeño para el hogar o la oficina de acceso inalámbrico, mediante un documento que explique los conceptos básicos de las redes locales, y que exponga la transición de las redes cableadas a las redes inalámbricas.

Dar a conocer marcas y modelos de los dispositivos de acceso inalámbrico tanto de la infraestructura de la red como los periféricos de las estaciones de trabajo del usuario.



METODOLOGÍA.

Para el desarrollo de la presente tesis partimos de la experiencia laboral en la configuración e implementación de sitios para el servicio de Internet.

La investigación documental se basó en libros especializados en el tema, artículos de sociedades científicas, y especificaciones de equipos comerciales en México.

CAPITULO 1

SERVICIOS Y CARACTERÍSTICAS DE LOS ISP

1.1 INTRODUCCIÓN

Antes que nada podemos definir al INTERNET como un conjunto integrado por las distintas redes de cada país en todo el mundo, donde el usuario, dependiendo de los permisos apropiados que otorga un “Proveedor de servicios de Internet” (ISP, Internet Service Provider), puede incluso tener conexión directa con otra computadora en cualquier otro sitio del planeta. La mayoría de la gente usa el acceso a Internet para revisar su correo electrónico, buscar publicidad, hacer compras electrónicas, incluso para conectarse remotamente a la red de trabajo de su empresa.

Es importante que se familiarice con los servicios básicos de un proveedor y las características que afectan la calidad de las conexiones a Internet. Cualquiera que pueda ofrecer conectividad a Internet puede reivindicar ser un proveedor de servicios; el término “Proveedor de Servicios” incluye todo, desde un proveedor con un backbone y una infraestructura de varios millones de dólares, hasta un proveedor con un único router y el servidor de acceso en su garaje.

El precio no debería ser el principal factor para basar la decisión al elegir un ISP. Lo que realmente debería preocupar son factores tales como los servicios que ofrece, el diseño del backbone, la tolerancia a las fallas, la redundancia, la estabilidad, los cuellos de botella, los acuerdos de equipamiento proveedor-cliente.

Los comportamientos del enrutamiento en Internet se ven afectados por el comportamiento de los protocolos de enrutamiento y el tráfico de datos sobre una infraestructura física y establecida. El buen diseño de la infraestructura y su mantenimiento son factores primordiales para un enrutamiento eficiente en Internet.

El presente capítulo pretende exponer las diferentes formas de conexión a Internet, así como los principales productos que ofrece un Proveedor de Servicios de Internet.

1.2 CONEXIÓN A INTERNET Y SERVICIOS DE LOS ISP

Los servicios que ofrece un Proveedor de conexión a Internet son muy diversos, esto va a depender de su infraestructura. Principalmente, los proveedores pueden clasificarse por su método de acceso físico a Internet, las aplicaciones que proporcionan a los clientes, y los servicios de seguridad que ofrecen.

1.2.1 FORMAS DE ACCESO A INTERNET

1.2.1.1 INTERNET DEDICADO

Se ofrece habitualmente a velocidades desde 56 Kbps o 64 Kbps hasta líneas T1/E1 (1,5 y 2 Mbps, respectivamente) en el extremo inferior, y T3/E3 (45 y 34 Mbps, respectivamente) y OC3 (155 Mbps) en el extremo superior.

Las conexiones de acceso dedicado se utilizan cuando el ancho de banda que se va a usar es previsible y la frecuencia del acceso a la red es lo suficientemente alta para justificar una línea de estas características 24 horas al día, sin embargo, el mayor inconveniente del acceso dedicado es el costo, que normalmente es más alto que el de otros métodos de acceso.

Normalmente el acceso dedicado a Internet implica la terminación del circuito físico en el Equipo Terminal de Abonado (CPE Customer Premises Equipment), así como una terminación de circuito directa en un router IP en el lado del proveedor de servicio. Los protocolos de la capa de enlace, como PPP o HDLC de Cisco (un derivado de PPP), son utilizados para señalar y transferir tramas a través de la conexión

1.2.1.2 INTERNET MEDIANTE FRAME RELAY Y ATM

Están entre las formas más económicas que las empresas pueden elegir para conectarse a Internet ya que los proveedores de servicio a menudo proporcionan puerta de enlace (gateways de acceso) desde el Internet hasta sus redes IP, por lo que no se requiere de una infraestructura adicional para acomodarse a la nueva conexión.

Los servicios ATM y Frame Relay, en comparación con el acceso dedicado, ejecutan una multiplexación estadística, y esto mismo es lo que permite a los proveedores de servicios ejecutar una capa adicional de agregación de servicio, reduciendo así el costo del servicio.

1.2.1.3 ACCESO TELEFÓNICO

Los servicios de acceso telefónico incluyen el tradicional acceso a través de un MODEM, con velocidades de hasta de 56 Kbps. También incluyen ISDN-RDSI (Red digital de servicios integrados), BRI (Interfaz de acceso básico) de hasta 128 Kbps y PRI (Interfaz de acceso primario) de hasta 1,5 Mbps. Estos

servicios han experimentado un crecimiento debido a que su naturaleza es bajo demanda (se utiliza solo cuando se necesita).

1.2.1.4 LÍNEA DE ABONADO DIGITAL (DSL, Digital Subscriber Line)

Los servicios de DSL proporcionan acceso a Internet de alta velocidad y bajo costo. Los tipos de servicio DSL varían en función de la tecnología xDSL que se utilice siendo x la representación de las diferentes técnicas de codificación utilizadas a través de la línea física de la Capa 1. La siguiente tabla muestra los tipos más comunes de tecnología DSL y sus características

Tecnología DSL	Tasa de flujo ascendente	Tasa de flujo descendente	Simétrica / Asimétrica	POTS coexistentes	Estandarización
ADSL (Línea asimétrica de abonado digital)	16 Kbps a 640 Kbps	1,5 a 8 Mbps	Asimétrico	Si	Si
HDSL (Línea de abonado digital de alta tasa de transferencia)	Fijo 1544, 2048 Kbps	Fijo 1544, 2048 Kbps	Simétrico	No	Si
SDSL (Línea simétrica de abonado digital)	1,5 ó 2048 Mbps	1,5 ó 2048 Mbps	Simétrico	Si	No
VDSL (Línea de abonado digital de muy alta tasa de transferencia)	1,6 a 19,2 Mbps, depende de la distancia	12,96 Mbps a 4.500 pies 55,2 Mbps a 1.000 pies	Ambos	Si	En desarrollo

Tabla 1.1 Tecnología DSL

Este servicio también se ofrece al cliente a través de su línea telefónica, la clave de la tecnología DSL es que se puede utilizar los bucles de cable de par trenzado de cobre, convirtiéndola en una tecnología de acceso popular para el hogar y el pequeño negocio, por otro lado su rendimiento y tasa de transferencia esta en función de la calidad de los cables tendidos y la distancia a la Oficina Central. El más usado es el ADSL, la característica principal de este servicio es que tanto los datos como la voz viajan en el mismo medio de transmisión pero a frecuencias diferentes.

1.2.1.5 MODEMS POR CABLE

Este servicio de módems por cable utiliza el alto ancho de banda de las líneas de televisión por cable para proporcionar servicios de acceso a Internet. Fue diseñado para utilizar la infraestructura existente de fibra y cable coaxial de televisión, los servicios típicos proporcionados están cercanos a los 2 Mbps en flujo descendente (hacia la ubicación del suscriptor) y 64 Kbps de flujo ascendente (hacia la red del proveedor del servicio).

Su más notoria diferencia radica en que el ancho de banda descendente es compartido por múltiples usuarios del servicio, creándose de este modo

problemas de seguridad para los fabricantes, proveedores de servicio y los propios consumidores.

1.2.1.6 ACCESO INALÁMBRICO.

El servicio de acceso inalámbrico a Internet se brinda a través de Puntos de Acceso (AP) ubicados en sitios como restaurantes, aeropuertos, hospitales, cafeterías, etc. La diferencia con los servicios convencionales es la parte inalámbrica que se encuentra inmediatamente después del cliente, y la facilidad de movimiento, así como la opción de tener un punto de acceso a Internet en casi cualquier parte de la ciudad, obviamente no es gratis porque se debe de contar con un contrato con el ISP.

1.2.2 SERVICIOS

1.2.2.1 ALOJAMIENTO DEDICADO (WEB-HOSTING)

El servicio de alojamiento dedicado se conoce comúnmente como Proveedores de Contenido, los cuales son los centros de datos con alta tolerancia a fallas que alojan armarios o *racks* en los cuales tanto empresas como clientes pueden alquilar espacio y colocar servidores u otro equipamiento informático.

Por ejemplo:

- a) **Hospedaje de Páginas Web.** Consiste en el almacenamiento de páginas previamente diseñadas por el cliente en los servidores del ISP, para poder ser visitados vía Internet.
- b) **Actualización vía remota.** El cliente puede realizar sus propias actualizaciones a través de las herramientas de software tales como: Front Page, Posting Aceptor y Web Publishing Wizard.
- c) **Registro del Dominio ante el NIC (trámite).** Consiste en dar de alta el dominio del cliente ante el NIC (Network Information Center).
- d) **Administración del dominio.** Consiste en el alta y administración del dominio de los clientes en los servidores Web y DNS del ISP.
- e) **Correo Electrónico.** Se proveerá de servicios de mensajería a los clientes del servicio de hospedaje.
- f) **Correo Electrónico Personalizado.** Consiste en personalizar las cuentas de correo electrónico utilizando el dominio propio del cliente.

g) Reportes de Estadísticas.

- Se le proporciona información al cliente sobre las siguientes estadísticas:
- Número de hits.
- Número de visitas
- Páginas más visitadas.

h) Soporte para Inserción de Contador de Visitas. Se asesora al cliente para colocar un contador en la página principal del cliente para que éste conozca las veces que han visitado esa página.

i) Soporte Front Page. Front Page es una herramienta de Microsoft que permite al cliente administrar y editar sitios.

1.2.2.2 CORREO ELECTRÓNICO

El correo electrónico es el intercambio de información tales como documentos, imágenes, pequeños videos y música, entre otros, los cuales son enviados como archivos anexos al mensaje original. El correo electrónico hoy en día ha sustituido casi por completo al correo tradicional debido a su rapidez, seguridad de arribo al destinatario, y versatilidad. El proveedor designa un espacio en memoria para alojar la información del cliente, remotamente éste accede con una computadora personal mediante un nombre de usuario y contraseña, ya estando en el sitio web del correo electrónico puede “descargar” a su PC los archivos y / o mensajes que tiene en su buzón. Este es un servicio que ofrecen los ISP, en muchas ocasiones de forma gratuita cuando se trata de poco almacenaje, sin embargo hay algunos ISP que cobran cuando se trata de una memoria mayor. Aunado al correo electrónico, también los ISP brindan el servicio de antivirus, que protegen a los mensajes del usuario.

1.2.2.3 MOTOR DE BÚSQUEDA

El motor de búsqueda no se trata de un servicio propio de un ISP, más bien podemos hablar de un sitio web o una sección de éste donde el usuario puede encontrar, mediante una palabra clave, otros sitios web que tengan un vínculo al mismo motor de búsqueda.

1.2.2.4 OTRO SERVICIOS

Otros servicios de capa superior incluyen servicios de noticias, Redes privadas Virtuales (VPN, Virtual Private Networks) y multidifusión IP. Muchos ISP también ofrecen consultorías, servicios de valor añadido como la seguridad los cuales incluyen filtros de paquetes en el dispositivo de acceso al igual que encriptación de datos y detección de virus.

CAPITULO 2

FUNCIONAMIENTO GENERAL DE LAS REDES DE DATOS

2.1 INTRODUCCIÓN

Antes de 1980 las computadoras se consideraban como elementos aislados, cada una tenía sus propios recursos tanto de hardware como de software. Esto era un problema para las empresas que contaban con un gran número de equipos, por ejemplo si querían compartir datos o imprimir un documento en una computadora que no contaba con impresora se tenía que pasar la información a una disco flexible para llevarla al equipo donde se tenía la impresora instalada, esto generaba aún un problema mayor: el alto costo para la administración, la implementación de periféricos para todas las computadoras y el mantenimiento preventivo y correctivo. Entonces se pensó en un sistema que permitiera la transferencia de datos y el uso de hardware entre las computadoras, surgiendo así el concepto de Redes de Datos.

A mediados de la década de 1970 a 1980 varios fabricantes desarrollaron sus propias redes, sin embargo, fue hasta 1980 cuando las empresas Xeros, Digital Equipment Corporation e Intel desarrollaron las especificaciones del sistema de red Ethernet. Cabe mencionar que esta idea de establecer una comunicación entre computadoras comienza a trabajar a principios de 1960, siendo un proyecto de origen militar, estableciéndose así la primera red llamada ARPANET. Pero no fue hasta mediado de 1970 cuando se empezaron a hacer más comerciales las computadoras personales. Conforme pasaba el tiempo varios fabricantes implementaban sus redes pero éstas no eran compatibles unas con otras. Fue evidente que era necesario el establecimiento de organismos que dirigieran el proceso de estandarización a nivel mundial para interfaces y protocolos de comunicación. Algunos organismos más reconocidos son: Internacional Organization for Standarization (ISO), American National Standar Institute (ANSI), Institute of Electrical and Electronic Engineers (IEEE), entre otros.

En el siguiente capítulo se expone la teoría general de redes de datos, sus topologías, medios de transmisión, el Modelo de Referencia OSI y su relación con TCP/IP, métodos de acceso al medio, la definición y el uso del direccionamiento IP, diversos protocolos de enrutamiento y enrutables, entre otros conceptos.

2.2 REDES DE DATOS

Una red de datos está formada por computadoras, el hardware que entre ellas comparten, tales como impresoras, scanners, unidades de disco, etc., y elementos propios de la red que permiten el intercambio de información, así como switches, routers, hubs, etc.. Todos estos elementos se conectan directamente por un medio de transmisión: cable coaxial, cable STP (Shielded Twisted Pair), UTP (Unshield Twisted Pair), fibra óptica o por medio de microondas, ondas de radio frecuencia o comunicación infrarroja, de acuerdo a una topología específica. Para que sea posible el intercambio de información entre las estaciones de trabajo se requiere que ellas tengan los mismos protocolos, es decir, normas y convenciones que definen el formato y la transmisión de los datos.

De acuerdo al alcance físico que tienen las redes, se les da una clasificación, estas son:

- a) **Redes de Área Personal, PAN (Personal Area Network).** Las redes PAN son las más cercanas al usuario, son redes de muy corto alcance que interconectan dispositivos como organizadores personales (PDA), celulares, impresoras inalámbricas, cámaras digitales, computadoras portátiles, etc., no tiene una cobertura mayor a los 10 metros y pueden ser extensiones de una red LAN. Las tecnologías mas empleadas son Bluetooth, 802.11 (algunos casos), Home RF e IRDA.
- b) **Redes de Área Local, LAN (Local Area Network).** Las redes LAN son redes de pequeño alcance, empleadas en oficinas, hogares, incluso en campus. Esto implica que pueden tener dimensiones desde unos cuantos metros, hasta unos cuantos kilómetros, la finalidad principal es compartir directamente datos y dispositivos periféricos. Los estándares que han tenido más auge son Ethernet y Token Ring. Las velocidades de transmisión van desde los 10 Mbps hasta 1Gbps en Ethernet, y entre 4 y 16 Mbps en Token Ring.
- c) **Redes de Área Metropolitana, MAN (Metropolitan Area Network).** En éste caso, las rede MAN son el conjunto de las LAN, corresponde a una versión mas grande en cuanto a topología, protocolos, y medios de transmisión. Son muy variadas las opiniones de acuerdo al alcance físico de este tipo de redes, sin embargo podemos hablar que van desde unas decenas de kilómetros hasta unos cuantos cientos de kilómetros.
- d) **Redes de Área Amplia, WAN (Wide Area Network).** Son redes que cubren una gran zona geográfica, por ejemplo, un país o continente. Los beneficios de estas redes son para los usuarios que se encuentran en las pequeñas redes LAN. Las redes WAN utilizan una gran variedad de medios de transmisión, anchos de banda, e involucran diversas tecnologías, estándares y protocolos. En sí una red WAN es el conjunto de más redes LAN y MAN.

2.3 MODELO DE REFERENCIA OSI (OPEN SYSTEM INTERCONNECTION)

La Organización Internacional de Estandarización (ISO) desarrolló el Modelo de Referencia OSI para describir la transferencia de datos entre las computadoras desde una aplicación de software a través del medio de transmisión hasta una aplicación en otro elemento de la red. El Modelo de Referencia OSI es un concepto que se divide en 7 capas, estas son: la capa Física, Enlace, Red, Transporte, Sesión, Presentación y Aplicación. De esta manera se construye una arquitectura de comunicaciones.

7 Aplicacion
6 Presentacion
5 Sesion
4 Transporte
3 Red
2 Enlace
1 Fisica

Fig. 2.1 Capas del Modelo de Referencia OSI

El Modelo de Referencia OSI es sólo un concepto que da una idea acerca del intercambio de información, para hacer posible la comunicación entre computadoras se necesitan los protocolos, que no son otra cosa que reglas y convenciones que indican cómo es el intercambio de la información a través del medio de transmisión.

2.3.1 PROCESO DE INTERCAMBIO DE INFORMACIÓN

Si se va a transmitir información desde una aplicación de software de una computadora a otra, es evidente que ésta pasará a través de las 7 capas de la computadora origen y de las 7 capas de la computadora destino. De esta manera las 7 capas usan información de control que consiste en instrucciones específicas para la comunicación con otras capas, esta información toma la forma de encabezado y de datos. Por ejemplo si en la capa 4 se tiene encabezado y datos, y se pasa la información hacia la capa 3, en ella estos serán únicamente datos y se tendrá un nuevo encabezado, así finalmente en la capa Física se estará dispuesto a transmitir a través del medio únicamente datos, que en sí contienen encabezados y datos de las capas superiores.

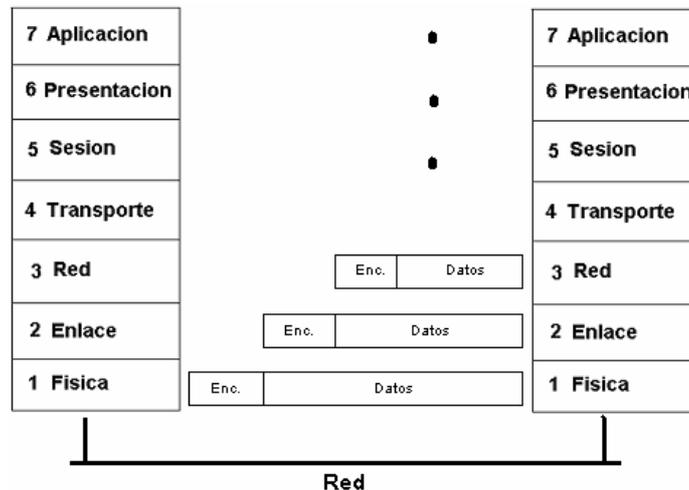


Fig. 2.2 Información de control.

Cada una de las dos columnas de capas, en ambos sistemas, se denomina Peer. La comunicación, como se mencionó, pasa a través de las 7 capas, pero también se hace entre capas análogas de los Peer's. Cada capa en la máquina origen agrega información de control (encabezado) a los datos, y la capa respectiva del Peer de la máquina destino analiza y remueve la información de control de los datos, es por eso que una capa lee como dato el encabezado de la capa anterior, siendo que únicamente la capa análoga pueda tener la capacidad de leer la información que se le esta transmitiendo.

2.3.2 CAPA FÍSICA

Esta capa tiene como objetivo principal el de transportar la información por un medio de transmisión. Define las características físicas del medio de transmisión, de tipo mecánico, eléctrico y óptico, el tipo de cable a usar, los conectores, los niveles de voltaje y la codificación de la información.

2.3.2.1 MEDIOS DE TRANSMISIÓN

Los medios de transmisión que se emplean en las redes son diversos y la implementación de ellos depende del tipo de red y las distancias a cubrir, por ejemplo si se requiere de un enlace de varios kilómetros no conviene el uso de cable coaxial debido a las atenuaciones, es mejor el uso de microondas o fibra óptica. Los cables se describen a continuación.

- a) **Cable coaxial:** está formado por un alambre central rodeado por una malla metálica, separados por un aislante, y cubiertos por una funda de material aislante. La malla se usa como la Tierra y el conductor central es el positivo. Es usado en dos versiones de Ethernet, 10base2 o thin y 10base 5 o thick. En la televisión por cable se emplea la infraestructura para la transmisión de Internet convencional.

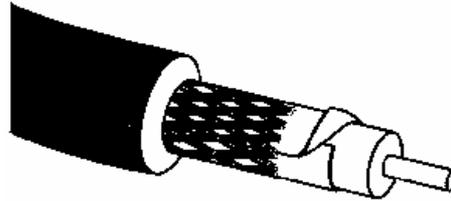


Fig. 2.3 Cable coaxial

(Imagen obtenida de la página de Internet www.techfest.com/networking)

b) **Cable par trenzado:** el par trenzado es un cable formado por un par de hilos aislados independientemente y trenzados para reducir la inducción electromagnética, en esta categoría existen dos tipos, el cable UTP (Unshield Twited Pair), con una impedancia de 100 Ohms, y el STP (Shield Twited Pair), con una impedancia de 150 Ohms, este último tiene una protección que impide la interferencia electromagnética. Estos cables están formados por 4 pares de hilos, se usan en transmisión tanto analógica como digital, usan un conector RJ-45, parecido al usado por los aparatos telefónicos pero con 8 filamentos para la conexión. De acuerdo a las velocidades que soportan se divide en varias categorías:

- **Categoría 1 y 2:** son cables usados en la transmisión de voz, principalmente a velocidades bajas de 1 a 4 Mbps.
- **Categoría 3:** se implementa en redes que usan frecuencias de hasta 16 MHz, y en redes de datos de Ethernet con velocidades de 10 Mbps, tiene 4 pares de conductores, un ejemplo del uso de éste es la implementación de Ethernet 10Base-T.
- **Categoría 4:** soporta señales de hasta 20 MHz, trabaja a velocidades de hasta 16 Mbps, también tiene 4 pares de conductores.
- **Categoría 5:** este tipo de cable soporta señales de hasta 100 MHz, y se puede implementar en redes Ethernet con velocidades de operación de 100 Mbps, tiene 4 pares de conductores, se usa principalmente para redes 10Base-T, 100Base-TX.
- **Categoría 5e:** también opera con señales de hasta 100 MHz, y es frecuentemente usado en redes Ethernet tanto de 100 Mbps como de 1000 Mbps (Gigabit).
- **Categoría 6:** es adecuado para trabajar a 250 MHz, y se usa principalmente en Gigabit Ethernet.
- **Categoría 6a:** es una especificación futura que se pretende usar en redes de 10 Gbps.
- **Categoría 7:** este estándar especifica 4 pares blindados individualmente dentro de otro blindaje, opera con señales de hasta 600 MHz.

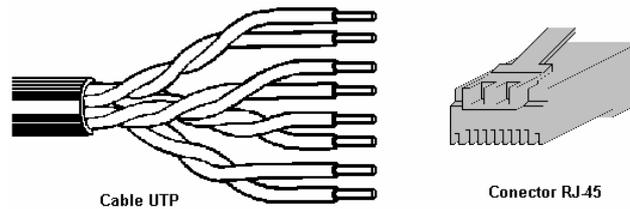


Fig. 2.4 Cable par trenzado
(Imagen obtenida de la página de Internet www.techfest.com/networking)

- c) **Fibra óptica:** La fibra óptica es un medio que transporta información luminosa, es un hilo muy delgado hecho principalmente de silicio, tiene un recubrimiento gelatinoso que le sirve como cojín, y tiene otro finalmente que es la cubierta. La fibra óptica brinda ventajas como menor peso, menor espacio de instalación, propagación de la información a altas velocidades, ya que se trata de la banda óptica, ancho de banda muy grande, aislamiento electromagnético y se puede tener una distancia mayor entre repetidores. Existen dos tipos de fibras ópticas: la Mono modal, esta permite solo el paso de un haz luminoso en forma axial; y la fibra Multimodal: permite el paso de haces luminosos en varios ángulos de propagación. El manejo de las fibras es muy delicado, se usan conectores de varios tipos, ya sea LC, FC, SC. En este caso los transmisores que se usa es un Láser o Led.

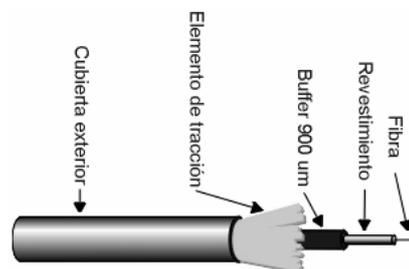


Fig. 2.5 Cable de fibra óptica
(Imagen obtenida de la página de Internet <http://platea.pntic.mec.es/~lmarti2/optral/imagenes/fibra-6b.jpg>)

- d) **Microondas terrestres:** Son enlaces que se hacen a través del espacio en frecuencias de 5 GHz a los 20 GHz aproximadamente, éstos abarcan las bandas designadas como C, Ka y Ku, se transmite mediante antenas parabólicas con una línea de vista y en ocasiones se emplean repetidores cuando las condiciones topográficas son muy accidentadas. Al hablar de levantamientos topográficos nos referimos a que los enlaces de microondas pueden cubrir distancias muy largas formando redes de gran extensión. Un punto muy importante a considerar es que todas las frecuencias de transmisión están reguladas por el gobierno y se debe de asignar una frecuencia cuando se desee hacer uso de un enlace de este tipo.

2.3.2.2 TÉCNICAS DE CODIFICACIÓN

La transmisión de información a nivel físico se hace a través de cadenas de bits representadas por niveles de voltaje o mediante señales ópticas que viajan a lo largo del medio de transmisión. Las técnicas de codificación digital definen la representación de los bits como señales a través de los conocidos códigos de línea. Existen numerosos métodos para codificar datos digitales, desde el más simple NRZ hasta el más complicado HDB3. A manera de mención, las técnicas de codificación se clasifican:

- a) **Unipolar:** los datos binarios se representan con un solo nivel de voltaje, positivo cuando es “1” y con el nivel de voltaje cero cuando es “0”, existe un problema cuando se tiene una cadena muy grande de “1” o “0”, se pierde la sincronía, no es tan fácil detectar el número de bits.
- b) **Polar:** este método usa dos niveles de voltaje, negativo para la representación de los “0” y positivo para los “1”. Podemos encontrar el NRZ polar, éste tiene el nivel de voltaje para los “0” y “1” tal y como se mencionó; el RZ polar, éste código tiene la siguiente regla: los “1” tienen voltaje positivo durante medio periodo y voltaje cero en la segunda mitad del periodo, para los “0” es similar, tienen voltaje negativo medio periodo y voltaje cero en la segunda mitad.
- c) **Bipolar:** en este caso se tienen tres niveles de voltaje, los “1” se van alternando primero uno es positivo, y el siguiente “1” será negativo, mientras que el “0” se representa como voltaje cero.

2.3.3 CAPA DE ENLACE

Esta capa provee un tránsito confiable de datos a través del medio físico, se definen el direccionamiento físico, topología de la red, notificaciones de error, además organiza los datos y define como son las tramas de datos, e incluye en cada uno información de control para detectar errores y mantener la integridad de los datos.

2.3.3.1 TOPOLOGÍAS

Las topologías son arquitecturas lógicas, es decir que los dispositivos no están ubicados físicamente de acuerdo a las configuraciones, en algunos casos éstas dependen del tipo de medio de transmisión. Las topologías más comunes en redes de datos son las que se muestran en la Fig. 2.6 y en la Tabla 2.1

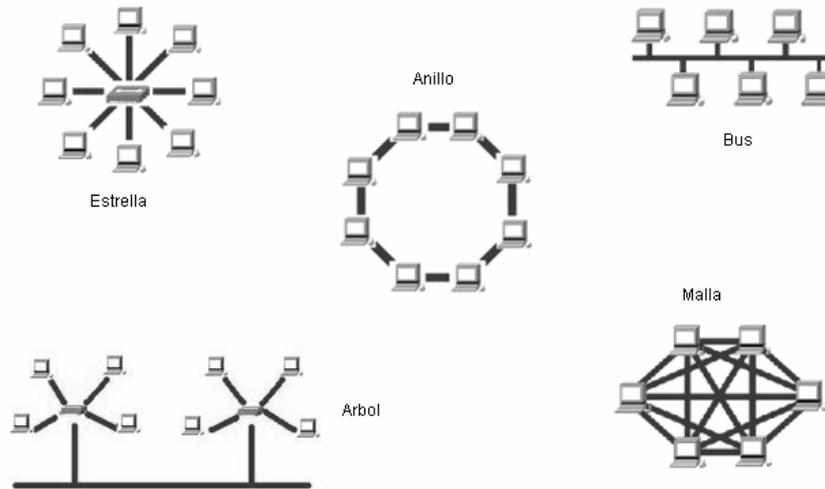


Fig. 2.6 Topologías de red.

Topología	Características	Ventajas	Desventajas
Estrella	<ul style="list-style-type: none"> -Nodo central. -Conexión de equipos al nodo en forma radial. -La información de nodo a nodo pasa por el equipo central. 	<ul style="list-style-type: none"> -Comunicación rápida entre el nodo y el eq. Central. -Si un equipo pierde conexión no perjudica a otros. -Fácil de detectar fallas. -Crecimiento de la red sin perjudicar a los equipos operando. 	<ul style="list-style-type: none"> -Comunicación lenta entre equipos. -Si falla el equipo central se pierde la red por completo.
Bus	<ul style="list-style-type: none"> -Es un medio de transmisión en forma dorsal donde los nodos se conectan uno tras otro. -En los extremos se conectan unas resistencias de 50 Ohm para evitar la reflexión de la señal. 	<ul style="list-style-type: none"> -Fácil de instalar. -Evita cantidad grande de cableado. -No existe un elemento central del cual dependan los nodos. 	<ul style="list-style-type: none"> -Si se pierde la comunicación en un punto del cable dorsal, se pierde toda la red.
Anillo	<ul style="list-style-type: none"> -Es un medio de transmisión en forma dorsal donde los nodos se conectan uno tras otro cerrando un bucle. -La información circula en un solo sentido del anillo, regenerándose en cada nodo del anillo. 	<ul style="list-style-type: none"> -Fácil de instalar. -Evita cantidad grande de cableado. -No existe un elemento central del cual dependan los nodos. 	<ul style="list-style-type: none"> -Si se pierde la comunicación en un punto del cable dorsal, se pierde toda la red.
Malla	<ul style="list-style-type: none"> -Es una topología donde cada nodo se conecta con los demás nodos. 	<ul style="list-style-type: none"> -Permite que existan varios caminos para establecer una comunicación. -Hay redundancia en los enlaces. 	<ul style="list-style-type: none"> -Existe gran cantidad de cableado.
Árbol	<ul style="list-style-type: none"> -Es una generalización de la topología de bus y 	<ul style="list-style-type: none"> -Permite establecer una jerarquía de 	



estrella, donde se acuerdo a grupos o
conectan varios buses niveles.
secundarios.
-También puede
combinarse con la
topología de estrella
donde las
ramificaciones se
originan en switch's o
hub's.

Tabla 2.1 Comparativa de topologías.

La IEEE ha definido que dentro de la capa de Enlace se consideran dos subcapas, en la parte inferior está la subcapa MAC (Media Access Control) responsable de las técnicas de acceso al medio de transmisión y el direccionamiento físico de dispositivos. En la parte superior se encuentra la subcapa LLC (Logical Link Control), descrita por el estándar IEEE 802.2, la cual define las funciones lógicas de la capa de Enlace y la forma en que los datos son transmitidos sobre el medio físico proporcionando servicios a las capas superiores.

2.3.3.2 LLC (LOGICAL LINK CONTROL)

LLC es responsable de iniciar el intercambio de información, organizar el flujo de datos, además provee una interfaz para los protocolos de la capa de Red del Modelo de Referencia OSI, a través de una serie de servicios que permite que ésta capa intercambie paquetes con su capa análoga de otro Peer.

El primer servicio se denomina Modo sin conexión y sin reconocimiento, conocido como Tipo 1 de operación, en este modo las tramas son enviados sin garantizar que lleguen en buen estado, no existen mecanismos de detección y corrección de errores y/o retransmisión de información.

El Tipo 2 de operación es el servicio en Modo de conexión, aquí se establecen, usan, reinician y terminan conexiones en la capa de Enlace, éstas se establecen punto a punto entre los Puntos de Acceso de Servicios de la capa de Enlace (LSAP, Link Service Access Point,). En si el Tipo 2 de operación es un grupo de servicios:

- a) **Servicios de establecimiento de conexión:** provee los medios por los cuales una entidad de la red hace la petición para establecer la conexión a nivel de enlace, la *petición de conexión* es pasada a la subcapa LLC para indicar que una conexión a nivel de Enlace se establece entre el LSAP local y uno remoto. La *indicación de conexión* es pasada de la subcapa LLC para indicar la petición de una entidad remota a establecer una conexión con el LSAP local. La *respuesta de conexión* es pasada a la subcapa LLC para indicar la aceptación de la conexión. La *confirmación de conexión* pasa de la subcapa LLC para llevar los resultados de la *petición de conexión* previa asociada.



- b) Servicio de transferencia de datos orientada a conexión:** provee los medios por los cuales una entidad de red puede enviar y recibir información a través de la conexión establecida en la capa de Enlace, este servicio también provee control de flujo, detección y corrección de errores. Una *petición de transferencia de datos* pasa a la subcapa LLC pidiendo qué unidades de datos deben ser enviadas usando el procedimiento orientado a conexión. La indicación de transferencia de datos pasa de la subcapa análoga para indicar la llegada de unidades de datos.
- c) Servicio de reinicio de conexión:** provee los medios por cuales conexiones establecidas pueden regresar al estado inicial, la *petición de reinicio* pasa a la capa LLC para indicar que la conexión debe regresar de inmediato a su estado inicial, la *indicación de reinicio* pasa de la capa LLC para indicar que una conexión debe regresar a su estado inicial solicitada por una entidad de la red o por la misma capa LLC. La *respuesta de reinicio* pasa a la capa LLC para aceptar la condición de reinicio.
- d) Servicio de terminación de conexión:** la *petición de desconexión* pasa a la capa LLC para indicar la terminación de la conexión existente, la indicación de conexión, pasa de la capa LLC para indicar a la red que la conexión ha sido terminada.
- e) Servicio de control de flujo en la conexión:** provee los medios para el control de flujo de los datos asociados a la conexión específica a través de la interfaz de la capa de Red y de la capa de Enlace.

El Tipo 3 de operación es el servicio con reconocimiento pero sin conexión, este servicio provee los medios por los cuales las entidades del nivel de Red intercambian unidades de datos que son reconocidas por la subcapa LLC pero sin establecer una conexión a nivel de la capa de Enlace.

2.3.3.3 MAC (MEDIA ACCESS CONTROL)

En la capa MAC se considera el direccionamiento físico del dispositivo para acceder al medio de transmisión, este direccionamiento consta de 48 bits de largo y se expresa por 12 dígitos hexadecimales. Los 6 primeros identifican al fabricante o proveedor, y los 6 siguientes definen el número de serie de la interfaz u otro valor que el proveedor especifique. Aquí también se tienen las diferentes técnicas de acceso al medio, en términos generales son las siguientes, obviamente dentro de cada categoría existen los métodos específicos:

- a) Por contención:** el dispositivo que va a transmitir verifica que el medio este libre, si lo está, entonces transmite, si no, espera un determinado tiempo. No existe un control de qué dispositivo será el siguiente en transmitir. Se usa principalmente en Ethernet.

b) Round-robin: todos los dispositivos que comparten el mismo medio de transmisión tienen asignada una secuencia en tiempo y en turnos, si el dispositivo en turno no tiene nada que transmitir cede su lugar al siguiente. Lo emplea Token-Ring y FDDI.

c) Por reservación: es la misma técnica que el Round-robin pero con la posibilidad de que un dispositivo reserve el siguiente turno de transmisión para sí mismo. Lo emplea Token-Ring y FDDI.

2.3.3.4 ETHERNET

Es una familia de implementaciones LAN que opera en las capas Física y de Enlace del Modelo de Referencia OSI, se divide en tres categorías de acuerdo a su velocidad de transmisión y al tipo de cable usado:

- a) 10 Mbps – 10Base-T Ethernet
- b) 100 Mbps – Fast Ethernet
- c) 1000 Mbps ó 1 Gbps – Gigabit Ethernet

Ethernet ha prevalecido desde que se consideró como un proyecto en la Universidad de Hawai entre los años 1960 y 1970, posteriormente fue desarrollado por Xerox a mitad de los años 1970's, lanzándose al mercado en 1980 a través del Consorcio DIX (DEC-Intel-Xerox). Cabe mencionar que Ethernet es la red más usada en todo el mundo, como dato significativo, el 80% de las redes son de este tipo.

La topología que se emplea en este caso es variada, puede usarse una tipo bus, usando cable coaxial como medio de transmisión, pero para facilitar la implementación se ha optado por usar hubs para formar una red tipo estrella o árbol físicamente, sin embargo debe recalcar que la topología lógica siempre debe ser del tipo bus. Otro aspecto importante se tiene en las variantes de los medios de transmisión, los cuales provocan que existan varias versiones, dentro de una misma velocidad de transmisión. Hablando de 10 Base-T, se muestra una tabla comparativa de algunas características que se presentan.

Características	10-Base5	10-Base2	10-BaseT	10-BaseFL
Medio de TX.	Coaxial (thick) 50 Ohms.	Coaxial (thin) 50 Ohms	UTP cat: 3/5	Fibra óptica 62.5/125 um.
Max. long. cable de un segmento (m).	500	185	100	2,000
Tasa de TX. (Mbps).	10	10	10	10
Topología física.	Bus	Bus	Estrella	Estrella/punto a punto
Conector.	BNC	BNC	RJ45	ST
Nodos /distancia máx.	100	30	1024	1024

Tabla 2.2 Características de Ethernet 10 Base-T

Para el caso de 100 Base-T se tiene:

Características	100-BaseTX	100-BaseT4	100-BaseT2	100-BaseFX
Medio de TX.	UTP cat. 5 STP cat. 1 y 2.	UTP cat. 3,4 o 5	UTP cat. 3 ó superior.	Fibra óptica 62.5/125 um.
Max. long. cable de un segmento (m).	100	100	-----	400
Tasa de TX. (Mbps).	100	100	100	100
Topología física.	Estrella	Estrella	Estrella	Estrella
Conector.	RJ-45	RJ-45	RJ-45	SC

Tabla 2.3 Características de Ethernet 100 Base-T

Para el caso de 1000-BaseT se tiene:

Características	1000-BaseT	1000-BaseCX	1000-BaseSX	1000-BaseLX
Medio de TX.	UTP cat. 5	STP	Fibra óptica multimodo.	Fibra óptica multimodo y monomodo
Max. long. cable de un segmento (m).	100	25	500	5000
Tasa de TX. (Mbps).	1000	1000	1000	1000
Topología física.	Estrella	Estrella	Estrella	Estrella
Conector.	RJ-45	9 pin D sub	SC	SC

Tabla 2.4 Características de Ethernet 1000 Base-T

En Ethernet se emplea una trama definida por la IEEE en el estándar 802.3, el formato básico consta de 8 campos:

- a) **Preámbulo (PRE):** este campo consta de 7 bytes, es una cadena alternada de 1 y 0 que indica cuando una trama esta llegando y esto indica una especie de sincronía de recepción de las tramas de información.
- b) **Delimitador de comienzo de trama, Start of Frame Delimiter (SFD):** este campo es de un solo byte, consta de una serie de 1 y 0 con terminación de dos 1 consecutivos indicado que el siguiente bit es el primer bit del direccionamiento de la maquina destino.
- c) **Dirección de destino, Destination Address (DA):** consiste de 6 bytes (48 bits) estos campos identifican la estación que debe de recibir la información.
- d) **Dirección de origen, Source Address (SA):** identifica a la máquina origen de los datos.
- e) **Largo/Tipo, Length/Type:** esta formado por 4 bytes, este campo indica el numero de bytes contenidos en el campo de Datos de la trama, o el ID del tipo de trama si éste es ensamblado usando algún formato.

- f) **Datos:** es una secuencia de “n” bytes de cualquier longitud, donde “n” es menor o igual a 1500, pero si “n” es aun menor a 46 entonces este campo se debe extender agregando bytes para completar los 46 bytes.
- g) **Frame check sequence (FCS):** esta formado por 4 bytes, dentro de este campo se encuentra el CRC de 32 bits. El CRC (Cyclic Redundancy Check) es generado por la MAC que envía la información, y a su vez es recalculado por la MAC receptora, ambos se comparan para determinar las tramas dañados en el camino. FCS es generado cubriendo las partes de DA, SA, Largo/Tipo y el campo de Datos.

PRE	SFD	DA	SA	LARGO/TIPO	DATOS	FCS
7	1	6	6	4	46-1500	4

Fig. 2.7 Trama de Ethernet

2.3.3.4.1 MÉTODO DE ACCESO AL MEDIO CSMA/CD

Una característica muy distintiva de Ethernet es su mecanismo de control de acceso al medio llamado Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD, Carrier Sense Multiple Access with Collision Detection). CSMA/CD es un método de acceso al medio diseñado con el objetivo para que dos o más computadoras puedan compartir un medio de transmisión sin ningún tipo de conmutación y sin un intermediario central, token de acceso o cuando no se tiene una división de tiempo indicando cuando una computadora va a transmitir. En este caso cada MAC determina por si misma cuando le será posible la transmisión de datos. Las reglas principales que caracterizan a CSMA/CD son:

- a) Cada computadora esta censando continuamente el medio para determinar cuando existe una interrupción de la transmisión existente.
- b) Las estaciones pueden empezar a transmitir en cualquier momento que detecten que la red esta quieta, es decir cuando no hay tráfico.
- c) Si dos computadoras o más empiezan a transmitir casi al mismo tiempo ocurre una colisión de las cadenas de bits de las computadoras involucradas. Si esto ocurre, cada una de las estaciones transmisoras son capaces de detectar la colisión antes de que termine el envío, y deben detenerse tan pronto como se haya detectado la colisión y esperar un tiempo determinado antes de retransmitir la información.

Existe un caso crítico que es cuando las dos maquinas más alejadas de la red van a transmitir, sin embargo una de ellas no lo hace sino justo antes de que a ella lleguen las tramas transmitidas por la primera. Aquí, la colisión es detectada casi inmediatamente por la segunda máquina, pero para que la primera maquina se entere, tiene que propagarse de regreso por toda la red la

señal corrompida. De aquí se obtiene que el tiempo máximo para detectar la colisión sea aproximadamente igual al doble del tiempo de propagación de la señal entre las dos computadoras más lejanas en la red. Cada uno de los nodos de la red esta escuchando el medio y tomado las tramas que van pasando, pero si uno es un fragmento de una colisión éste es ignorado y siguen en espera del próximo.

2.3.3.5 TOKEN-RING

Token-Ring es originalmente creado por IBM en la década de 1970. Por otro lado la IEEE desarrolló el estándar 802.5 que es muy semejante a las implementaciones de IBM, es por eso que el termino Token-Ring se generaliza para ambas. Token-Ring, aunque originalmente trabaja a 4 Mbps, la mayor parte de las redes actuales operan a 16 Mbps, sin embargo éste no ha penetrado en el mercado tanto como Ethernet. Los nodos en este tipo de redes se conectan en una topología lógica de anillo, y una configuración física de estrella, la unidad central que incorpora a las estaciones de trabajo a la red se denomina Unidad de Acceso Multi-Estación (MAU o MSAU, Multistation Access Unit), a su vez estas unidades se pueden conectar para formar un gran anillo. Los cables que unen las computadoras con las unidades MSAU se denominan cables Lobe, y los que unen las MSAU se llaman cables Patch.

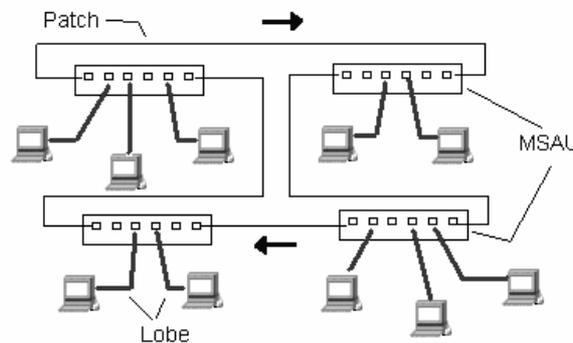


Fig. 2.8 Topología de una red Token-Ring

Token-Ring usa un método de acceso al medio distinto del empleado por Ethernet, llamado Token Passing clasificado como el tipo Round-robin. Este se basa en un paquete de 3 bytes llamado Testigo (Token) que arbitra la comunicación en toda la red y la posesión de éste garantiza el derecho a transmitir. El Testigo circula en toda la red de nodo en nodo hasta que llega a aquel que desea transmitir, éste modifica el Bit Monitor en la trama del Testigo para indicar que la red se ha ocupado y lo envía a la siguiente computadora, seguido de su paquete de datos. El paquete de datos circula en todo el anillo, cada una de las estaciones de trabajo lo toma y lee la dirección destino que contiene, de esta forma el paquete viaja hasta llegar a su destino y ser procesado, la maquina destino modifica los bits de Address (indicando que la trama llego a sus destino final) y el Bit Copied (indicando que la información fue copiada por el dispositivo destino). Una vez que el Testigo llega de nuevo al



nodo emisor compara los datos que llegan con los que transmitió para verificar si ha ocurrido algún error, si es así se transmite de nuevo la información. En caso de que la comunicación sea exitosa se eliminan los datos de la red y modifica el Bit Monitor para que esté libre el Testigo otra vez. Debido a que la computadora que transmite tiene en su poder el Testigo, en las redes Token-Ring no existen colisiones a menos que ocurra un mal funcionamiento de la red. En las redes Token-Ring existe un equipo designado como Monitor Activo, cuya función es garantizar el buen funcionamiento de la red, este no posee ningún software especial o programa específico, mientras que las demás máquinas se denominan Monitores de Reserva en caso de que el activo falle.

Mediante el proceso de Contienda de Monitor se elige a la estación que será el Monitor Activo. Los monitores de respaldo inician la Contienda de Monitor cuando detectan que el Monitor Activo no está trabajando apropiadamente o a fallado. La estación que se desempeñaba como Monitor Activo no entra en el proceso de elección. La forma en que se procede es la siguiente:

- a) Una o varias estaciones detectan un evento que inicia la Contienda de Monitor, entrando en estado de Claim Token Transmit Mode. Mientras se está en este estado, la estación manda una trama tipo Claim Token conteniendo su dirección MAC.
- b) Si la dirección MAC de la trama que acaba de recibir es mayor a la propia, sólo repetirá la trama, entrando en modo Claim Token Repeat.
- c) En caso contrario, entra en modo Claim Token Transmit, transmitiendo una trama tipo Claim Token con su dirección MAC.
- d) Eventualmente, todas las estaciones entraran en modo Claim Token Repeat, excepto una que estará en modo Claim Token Transmit. Cuando esta última reciba tres tramas con su propia dirección MAC, habrá ganado el proceso de selección y se convertirá inmediatamente en el Monitor Activo.

Al activarse como Monitor Activo, ejecuta las siguientes funciones: activa en sí las funciones de Monitor Activo, comienza el sondeo del anillo, transmite un primer testigo.

2.3.3.6 FDDI

FDDI (Fiber Distributed Data Interface) o Interfaz de Datos Distribuidos por Fibra se desarrolló a mediados de la década de 1980, fue creada por el ANSI en el comité X3T9.5, y se convirtió en el primer protocolo a nivel de enlace de datos de 100 Mbps. En el momento en que FDDI apareció en el mercado se vislumbraba mucho éxito debido a la velocidad de transmisión, en ese entonces las tecnologías dominantes implementadas en las redes LAN eran Ethernet gruesa y delgada con su velocidad de hasta 10 Mbps. El empleo

de fibra óptica prometía un aumento espectacular en la velocidad de transmisión, en el tamaño de los paquetes, la longitud de los segmentos de red y el número de estaciones de trabajo empleadas. Otra ventaja que destaca sobre las implementaciones de Ethernet es que las fibras ópticas son inmunes a la contaminación electromagnética es por eso que FDDI paso a ser una red de soporte muy buena.

La topología que usa FDDI es en forma de anillo doble o en estrella, a comparación de Token-Ring que su topología en forma de anillo es lógica y no física. El anillo doble de FDDI se compone de dos anillos independientes, uno es el Primario y otro es el Secundario, la circunferencia de anillo doble puede medir hasta 100 Km. y las estaciones de trabajo pueden estar separadas hasta 2 km. Las estaciones de trabajo conectadas a los dos anillos se denominan Estaciones de Acoplamiento Doble (DAS, Dual Attachment Station). Si se presenta una falla en una estación de trabajo, o un corte en un cable, el tráfico se desvía al anillo secundario, cuando una red entra en operación en estas condiciones se denomina anillo plegado.

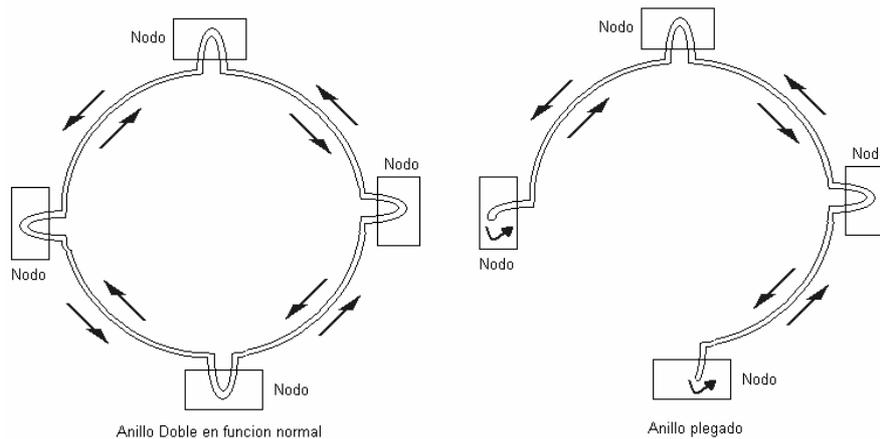


Fig. 2.9 Topología de una red FDDI, anillo doble (izquierda), anillo plegado (derecha)

FDDI utiliza un método de acceso al medio similar al de Token Ring, utilizando un testigo como intermediario, aunque difiere en los mecanismos de manejo del testigo, asignación de accesos y gestión de fallos. Un paquete de datos con un formato específico (el Testigo) pasa de una estación a la siguiente alrededor del anillo. Cuando una estación recibe el Testigo, se permite la transmisión. La estación puede enviar tantos paquetes de datos como desee hasta que se consume un tiempo predeterminado. Cuando las estaciones no tienen más datos que transmitir o se ha alcanzado el límite de tiempo transmite el Testigo. Cada estación de la red vuelve a transmitir los paquetes de datos y recibe y copia aquellos que van dirigidos a ella. Cuando un paquete de datos vuelve a la estación que lo ha enviado, dicha estación es responsable de eliminarla del anillo para que no quede circulando indefinidamente. Cuando las estaciones copian los paquetes de datos, pueden establecer bits de estado en ellos en el campo FS para indicar si se han detectado errores, en base a estos bits de estado, la estación transmisora puede determinar si un paquete de



datos se ha recibido con éxito. Dado que el Testigo pasa a otra estación tan pronto como ha terminado de transmitir los paquetes de datos, una estación puede transmitir nuevos datos mientras que los otros están circulando por el anillo. Por tanto, múltiples paquetes de datos de múltiples estaciones podrían estar en la red al mismo tiempo.

FDDI no utiliza el mecanismo de prioridad como en Token Ring. En lugar de ello, utiliza un esquema de asignación de capacidad basada en el tiempo que tarda el testigo en volver. Este esquema está diseñado para soportar una mezcla de transmisiones de flujos y ráfagas y transmisiones que implican diálogo entre una pareja de estaciones. Para ello se definen dos tipos de paquetes de datos: síncronos y asíncronos.

2.3.4 CAPA DE RED

Esta capa se encarga de la transmisión de los datos al establecer funciones de enrutamiento, y se asigna una dirección lógica a los equipos para su identificación en la red. Es decir, se define la estructura de direcciones y rutas que van a seguir las tramas de datos creando tablas de direcciones en los routers que se involucran en la red. Pueden establecerse rutas fijas a seguir de acuerdo a la dirección lógica de las computadoras o dispositivos determinados por un enrutamiento estático. En otros casos, se plantea un enrutamiento dinámico donde intervienen los protocolos de enrutamiento, tales como BGP (Border Gateway Protocol), EIGRP (Enhanced Inter-Gateway Routing Protocol) OSPF (Open Shortest Path First), los protocolos de TCP/IP y RIP (Routing Information Protocol), entre otros. En términos generales estos protocolos funcionan buscando las trayectorias más cortas o buscando la ruta que no ponga obstáculos. Los protocolos del nivel de Red aceptan datos del nivel de Transporte y los encapsulan en un datagrama, añadiendo su propio encabezado. Al igual que los encabezados de la capa de Enlace, los encabezados del nivel de Red contiene la dirección del sistema de destino, sin embargo, en el caso del nivel de Red se trata de una dirección que identifica al sistema destino mientras que en la capa de Enlace solo se identifica al siguiente dispositivo en la red.

En este nivel se definen dos tipos de dispositivos, los ES (End Systems), tales como computadoras personales, servidores, etc., en sí son dispositivos terminales que están en contacto directo con el usuario; y los IS (Intermediate Systems), estos son equipos intermedios en las rutas de los paquetes, pertenecen a la arquitectura de la red, ejemplos de éstos son routers, switches, etc. De acuerdo a esta clasificación se tienen a la vez dos tipos de protocolos: los Enrutables, (IP, IPX, Apple Talk, Decnet) éstos tienen información útil para el usuario, principalmente los usan equipos ES. Los protocolos de Enrutamiento los usan los equipos IS para definir las trayectorias de los paquetes de datos. El hablar de los protocolos de red se involucra también al grupo de TCP/IP es por eso que se hace un apartado al final de este capítulo mencionando algunos de los protocolos y sus características generales.

2.3.5 CAPA DE TRANSPORTE

La capa de Transporte implementa servicios confiables para el transporte de los datos que son transparentes para las capas superiores. Las funciones de ésta capa son el control de flujo, que sirve para identificar y diferenciar las múltiples conexiones existentes, y para determinar en que momento se inicia y termina una conversación. Otra función es la de multiplexar varias conexiones que tienen diferentes capacidades de transmisión para ofrecer una velocidad adecuada a la capa de Sesión. Además en esta capa se tiene la detección y corrección de errores en los paquetes que se transmiten. En el nivel de transporte existen dos tipos de servicios: Orientados a la Conexión y los No Orientados a la Conexión. Lo más usual es trabajar con servicios Orientados a la Conexión, donde se tienen tres fases: establecimiento, transferencia de datos y desconexión. Algunas implementaciones en la capa de Transporte incluyen los protocolos del grupo de TCP/IP y protocolos propios del Modelo de Referencia OSI.

De acuerdo a los servicios orientados o no orientados a conexión se definen tres tipos:

- a) **Tipo A:** muy confiable, servicio Orientado a Conexión.
- b) **Tipo B:** no confiable, servicio Orientado a Conexión.
- c) **Tipo C:** no confiable, servicio No Orientado a Conexión.

La selección de un protocolo de transporte depende de las necesidades de la aplicación que genera los mensajes y de los servicios ya proporcionados por los protocolos de nivel inferior, de acuerdo a esto tienen cinco clases teóricas de protocolos de transporte.

- a) **TP0 (Transfer Protocol Class 0):** es el protocolo más simple, asume un servicio tipo A, se supone que los protocolos de inferior nivel ya proporcionan todos los servicios que necesita la aplicación.
- b) **TP1 (Transfer Protocol Class 1):** asume un servicio tipo B, corrección de errores señalados, proporciona la capacidad de corregir errores detectados por los protocolos de nivel inferior.
- c) **TP2 (Transfer Protocol Class 2):** multiplexación, incluye códigos que identifican el proceso que generó el paquete y el que lo procesará en su destino, permitiendo que un único medio de transmisión transporte el tráfico de múltiples aplicaciones.
- d) **TP3 (Transfer Protocol Class 3):** corrección de errores señalados y multiplexación, combina los servicios proporcionados por las clases TP1 y TP2.



- e) **TP4 (Transfer Protocol Class 4):** servicio completo con conexión, incluye detección y corrección de errores, control de flujo y otros servicios.

2.3.6 CAPA DE SESIÓN

Esta capa 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. Estas solicitudes y respuestas están coordinadas por protocolos implementados en esta capa. Otro servicio de este nivel es la sincronización y el establecimiento de puntos de chequeo. Por ejemplo, si es necesario transferir un archivo muy grande entre dos nodos que tienen una alta probabilidad de sufrir una caída, es lógico pensar que una transmisión ordinaria nunca terminaría porque algún interlocutor se caerá y se perderá la conexión. La solución es que se establezcan cada pocos minutos un punto de chequeo de manera que si la conexión se rompe más tarde se pueda reiniciar a partir del punto de chequeo, lo cual ahorrará tiempo y permitirá tarde o temprano la terminación de la transferencia.

2.3.7 CAPA DE PRESENTACIÓN

La capa de Presentación provee servicios que permiten transmitir datos con alguna sintaxis propia para las aplicaciones o para el nodo en que se está trabajando, provee una variedad de codificación y funciones que se aseguran de que una información enviada desde la capa a aplicación de una computadora sea legible por la capa análoga de otra computadora. La conversión es usada para el intercambio de información entre sistemas que usan diferentes formas de representación de datos, ejemplos de esto es EBCDIC y ASCII. Las implementaciones en la capa de presentación no están asociadas con un protocolo específico, sin embargo existen diferentes estándares de codificación y compresión de la información tales como MPEG para video, Graphics Interchange Formart (GIF), Joint Photographic Experts Group (JPEG) y Tagged Image File Format (TIFF).

2.3.8 CAPA DE APLICACIÓN

Esta capa esta en contacto directo con el usuario, describe como hacen su trabajo los programas de aplicación, por un lado es la interfaz y por otro lado interactúa con la capa de presentación. Existen aplicaciones bajo el esquema de TCP/IP como, File Transfer Protocol (FTP), TELNET, Simple Mail Transfer Protocol (SMTP). Y por otro lado existen aplicaciones propias de OSI, como File, Transfer, Access and Management (FTAM), Virtual Terminal Protocol (VTP) y Common Management Information Protocol (CMIP).

2.4 TCP/IP

El departamento de la defensa de E.U.A. definió un conjunto de reglas que establecieron cómo conectar computadoras entre sí para el intercambio de información, fue así como surgió el conjunto de protocolos de TCP/IP (Transmission Control Protocol / Internet Protocol) y en algunos casos adopta protocolos ya existentes. La pila de TCP/IP recibe ese nombre debido a sus dos más importantes protocolos, TCP (Transmission Control Protocol) e IP (Internet Protocol). El objetivo principal que tiene TCP/IP es la interconexión de redes para tener una comunicación universal y para que al usuario final le parezca como una única y gran red, independientemente de la implementación física o las políticas que tenga cada red independientemente.

Este conjunto de protocolos se ubican en un modelo que podemos ubicar dentro del Modelo de referencia OSI, pero no podemos comparar su funcionalidad; constan de 4 capas: Interfaz de Red, corresponde a las capas Física y de Enlace del Modelo de Referencia OSI; Internet, corresponde a la capa de Red; Transporte, corresponde a la capa de Transporte y la de Aplicación corresponde a las capas de Sesión, Presentación y Aplicación.

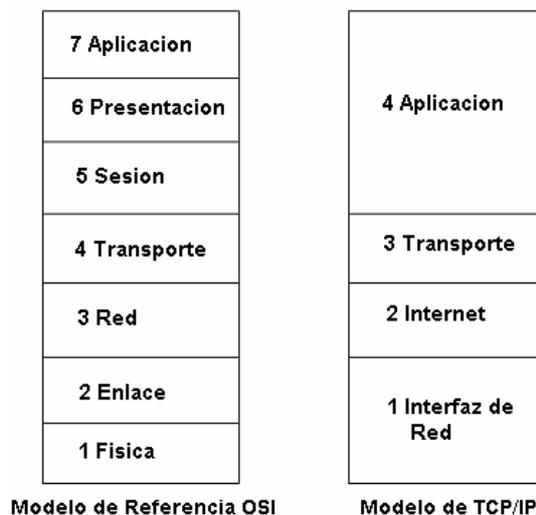


Fig. 2.10 Modelo de Referencia de TCP/IP

- a) **Capa de Interfaz de Red:** es responsable de la comunicación directa con la red, es capaz de entender la arquitectura usada como Token-Ring o Ethernet, y proveer una interfaz para que la capa de Internet se comunique con la red.

- b) **Capa de Internet:** en esta capa se definió el protocolo IP (Internet Protocol) cuya responsabilidad es entregar paquetes en los destinos indicados a través del enrutamiento. El protocolo IP incluye reglas de cómo agregar direccionamiento y como dirigir los paquetes a la máquina destino, de la fragmentación y ensamblaje de paquetes. Otros protocolos



que se incluyen en esta capa son, por ejemplo, Internet Control Messaging Protocol (ICMP), Internet Group Management Protocol, (IGMP) y el Address Resolution Protocol (ARP)

c) Capa de Transporte: esta capa esta al mismo nivel que la capa de Transporte del modelo de referencia OSI. Es responsable de proveer una Comunicación Orientada o No Orientada a Conexión, para el caso de una Comunicación Orientada a Conexión se usa el protocolo TCP, y para la comunicación no orientada a conexión se usa el UDP (User Datagram Protocol).

d) Capa de Aplicación: es responsable de todas las actividades que se llevan a cabo en las capas de Sesión, Presentación, y Aplicación del Modelo de Referencia OSI. En ésta capa existen numeroso protocolos que interactúan con el usuario, tales como Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), Telnet, Simple Mail Transfer Protocol (SMTP), HTTP, DNS, entre otros.

2.4.1 IPv4

La dirección IPv4 es el identificador de la máquina individualmente y de la red en la que reside. Estas direcciones de IP tienen una longitud de 32 bits, su notación se expresa con 4 números decimales de 8 bits separados por puntos, por ejemplo 192.168.2.45, ya que cada número es equivalente de un número binario de 8 bits, el intervalo completo de direcciones IP posibles va de 0.0.0.0 hasta 255.255.255.255. Estas direcciones no identifican una computadora sino una interfaz de red, es decir, una computadora tiene tantas direcciones IP como tarjetas de red o MODEM.

Toda dirección IP se divide en dos partes, la parte izquierda representa la red o el segmento de red donde se ubica la estación de trabajo, y la parte derecha es el número identificador único dentro de la red de la computadora (Host), pero la cantidad de bits utilizados para cada propósito no siempre es el mismo. Para determinar los bits que se usaran para identificar la red y para identificar el host, todo sistema TCP/IP dispone de una máscara de subred además de su dirección IP. Esta máscara es también un número binario de 32 bits divididos en 4 octetos, donde cada uno de los bits tienen una relación con los bits de la dirección IP, en este caso los números "1" de la máscara significa que esos bits de la dirección IP identifican la parte de red, mientras que los "0" de la máscara determinan los bits de la dirección IP que representan al host. Por ejemplo si tenemos la siguiente configuración en un sistema:

Dirección IP: 192.168.2.45

Máscara de subred: 255.255.255.255.0

La parte que identifica de la subred es 192.168.2, mientras que el 45 identifica al host, por otro lado observamos que el último octeto de la máscara es cero, es este caso este octeto varía de 0 a 255, sin embargo el número de

posibles host que pueden existir en la red son del 1 al 254 ya que el 0 se usa como identificador de red (NET ID) y el 255 como Broadcast. Si vemos las direcciones IP y la máscara en forma binaria tenemos:

Dirección IP: 11000000.10101000.00000010.00101101
Máscara de subred: 11111111.11111111.11111111.00000000

Esta máscara se denomina de 24 bits ya que los primeros 24 son usados para la parte de la red. No necesariamente la división entre la red y el host debe estar entre los octetos, por ejemplo una mascara de 28 bits es como sigue:

Máscara de 28 bits: 255.255.255.240
En su forma binaria: 11111111.11111111.11111111.11110000

Existe una organización a cargo de registrar direcciones de red para Internet llamada Autoridad de Asignación de Números de Internet (IANA, Internet Assigned Numbers Authority), la cual registra varias clases de direcciones de red que se diferencian en las máscaras de subred, estas son:

- a) **Clase A:** Esta clase es usada para redes muy grandes usa los 8 bits del primer octeto de lado izquierdo para las subredes ya que el más significativo siempre es 0, los siguientes 24 los usa para los equipos, se dice que tiene una máscara de 8 bits. El primer octeto en su forma decimal varía de 0 a 127.

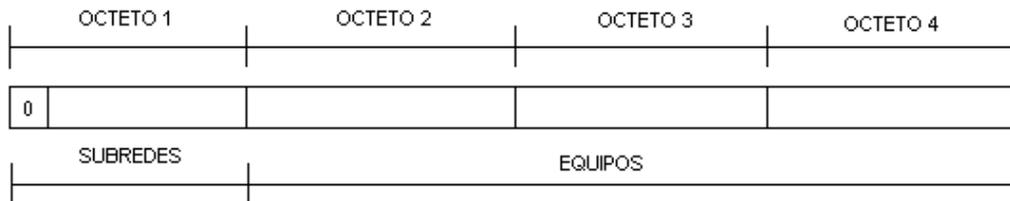


Fig. 2.11 Octetos del direccionamiento en una clase A.

- b) **Clase B:** Esta clase está destinada a redes de tamaño mediano, usa 14 bits de los dos primeros octetos para las subredes ya que los dos primeros siempre son 10, y los siguientes 16 son para asignar a equipos, tiene una máscara de 16 bits. Su primer octeto varía de 128 a 191.

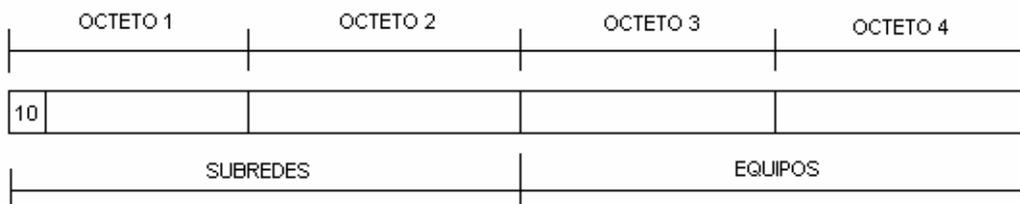


Fig. 2.12 Octetos del direccionamiento en una clase B



- c) **Clase C:** Esta clase se usa para redes de menor tamaño, para aquellas que no tienen más de 255 equipos. Usas 21 bits para las subredes, ya que los tres primero siempre son 110, y solo 8 bits para los equipos. Su primer octeto varía de 192 a 223.

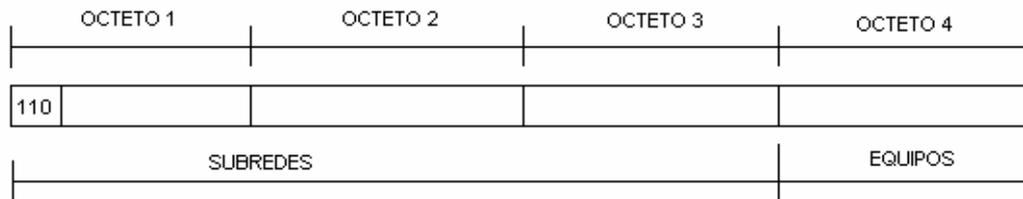


Fig. 2.13 Octetos del direccionamiento en una clase C

- d) **Clase D:** Se emplea para el Multicast IP, los primeros 4 bits siempre son 1110, con lo que el primer byte varía de 224 a 239. Junto con los siguientes 28 bits forman el identificador de un grupo Multicast.
- e) **Clase E:** por el momento es de uso experimental, los primeros 4 bits siempre son 1111, con lo que el primer byte al menos tiene el valor de 240.

2.4.2 IPv6

El protocolo IPv6 es una nueva versión de IP (Internet Protocol), diseñada para reemplazar a la versión 4 (IPv4) RFC 791, actualmente en uso.

IPv4 posibilita 4,294,967,296 (2^{32}) direcciones de red diferentes, en cambio, IPv6 admite 340,282,366,920,938,463,463,374,607,431,768,211,456 (2^{128} o 340 sextillones de) direcciones

Propuesto por el Internet Engineering Task Force en 1994 (cuando era llamado "IP Next Generation" o IPng), la adopción de IPv6 por parte de Internet es menor, la red todavía está dominada por IPv4. La necesidad de adoptar el nuevo protocolo debido a la falta de direcciones ha sido parcialmente aliviada por el uso de la técnica NAT. Pero NAT rompe con la idea originaria de Internet donde todos pueden conectarse con todos y hace difícil o imposible el uso de algunas aplicaciones P2P, de voz sobre IP y de juegos multiusuario. Un posible factor que influya a favor de la adopción del nuevo protocolo podría ser la capacidad de ofrecer nuevos servicios, tales como la movilidad, Calidad de Servicio (QoS), privacidad, etc.

Los cambios de IPv4 a IPv6 se clasifican en las siguientes categorías:



- a) **Capacidad extendida de direccionamiento:** IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multicast se mejora agregando un campo "ámbito" a estas direcciones. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.
- b) **Simplificación del formato de cabecera:** Algunos campos de la cabecera IPv4 se han suprimido o se han hecho opcionales, para reducir el costo del procesamiento de los paquetes y para ahorrar ancho de banda.
- c) **Soporte mejorado para las extensiones y opciones:** Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.
- d) **Capacidad de etiquetado de flujos:** Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".
- e) **Capacidades de Autenticación y Privacidad:** IPv6 incluye la especificación de extensiones que proveen autenticación, integridad, y (opcionalmente) confidencialidad de los datos.

2.4.2.1 DIRECCIONAMIENTO IPV6

El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

El número de direcciones IPv6 posibles es de $2^{128} \approx 3.4 \times 10^{38}$. Este número puede también representarse como 16^{32} , con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores (véase combinatoria).

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

2.4.2.2 NOTACIÓN PARA LAS DIRECCIONES IPV6

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales. Por ejemplo,

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

es una dirección IPv6 válida.

Se puede comprimir un grupo de cuatro dígitos si éste es nulo (es decir, toma el valor "0000"). Por ejemplo,

2001:0db8:85a3:0000:1319:8a2e:0370:7344

2001:0db8:85a3::1319:8a2e:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

son todas válidas y significan lo mismo, pero

2001::25de::cade

-- --

no es válida porque no queda claro cuántos grupos nulos hay en cada lado.

Los ceros iniciales en un grupo también se pueden omitir:

2001:0DB8:02de::0e13

2001:DB8:2de::e13

Si la dirección es una dirección IPv4 empotrada, los últimos 32 bits pueden escribirse en base decimal, así:

::ffff:192.168.89.9

::ffff:c0a8:5909

No se debe confundir con:

::192.168.89.9

::c0a8:5909

El formato ::ffff:1.2.3.4 se denomina dirección IPv4 mapeada, y el formato ::1.2.3.4 dirección IPv4 compatible.

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a 0000:0000:0000:0000:0000:0000:874B:2B34 o ::874B:2B34. Entonces, uno puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser ::135.75.43.52. Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

2.4.2.3 IDENTIFICACIÓN DE LOS TIPOS DE DIRECCIONES

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

::

La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1

La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.

::1.2.3.4

La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.

::ffff:0:0

La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.

fe80::

El prefijo de enlace local (en inglés link local) especifica que la dirección sólo es válida en el enlace físico local.

fec0::

El prefijo de emplazamiento local (en inglés site-local prefix) especifica que la dirección sólo es válida dentro de una organización local. La RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial. Se deben sustituir por direcciones Local IPv6 Unicast.

ff00::

El prefijo de multicast. Se usa para las direcciones multicast.

Hay que resaltar que no existen las direcciones de difusión (en inglés broadcast) en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast FF01::1, denominada todos los nodos.

2.4.2.4 PAQUETES IPV6

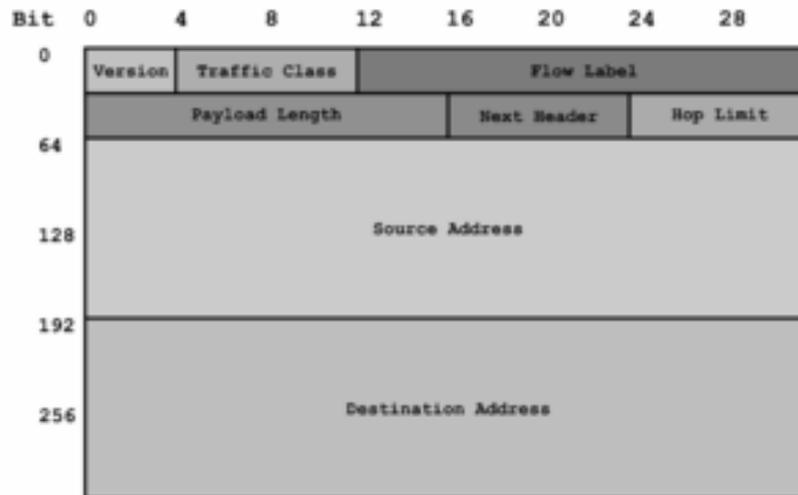


Fig. 2.14 Trama de IPv6

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera y los datos.

Los primeros 40 bytes (320 bits) son la cabecera del paquete y contiene las direcciones de origen y destino (128 bits cada una), la versión del protocolo IP (4 bits), la clase de tráfico (8 bits, Prioridad del Paquete), la etiqueta de flujo (20 bits, manejo de la Calidad de Servicio), la longitud del campo de datos (16 bits), la cabecera siguiente (8 bits), y el límite de saltos (8 bits, Tiempo de Vida). Después viene el campo de datos, con los datos que transporta el paquete, que puede llegar hasta 64k de tamaño en el modo normal, o más con la opción "jumbo payload".

Hay dos versiones de IPv6 levemente diferentes. La ahora obsoleta versión inicial, descrita en el RFC 1883, difiere de la actual versión propuesta de estándar, descrita en el RFC 2460, en dos campos: hay 4 bits que han sido reasignados desde "etiqueta de flujo" (flow label) a "clase de tráfico" (traffic class). El resto de diferencias son menores.

En IPv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en IPv4 en donde los routers pueden fragmentar un paquete. En IPv6, las opciones también desaparecen de la cabecera estándar y son especificadas por el campo "Cabecera Siguiente" (Next Header), similar en funcionalidad en IPv4 al campo Protocolo. Un ejemplo: en IPv4 uno añadiría la opción "ruta fijada desde origen" (Strict Source and Record Routing) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo "Cabecera Siguiente" indicando que viene una cabecera de encaminamiento. La cabecera de encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete, e

indicar que, por ejemplo, la cabecera TCP será la siguiente. Este procedimiento es análogo al de AH y ESP en IPsec para IPv4 (que aplica a IPv6 de igual modo, por supuesto).

2.4.2.5 IPV6 Y EL SISTEMA DE NOMBRES DE DOMINIO

Las direcciones IPv6 se representan en el Sistema de Nombres de Dominio (DNS) mediante registros AAAA (también llamados registros de quad-A, por tener una longitud cuatro veces la de los registros A para IPv4)

El concepto de AAAA fue una de las dos propuestas al tiempo que se estaba diseñando la arquitectura IPv6. La otra propuesta utilizaba registros A6 y otras innovaciones como las etiquetas de cadena de bits (bit-string labels) y los registros DNAME.

Mientras que la idea de AAAA es una simple generalización del DNS IPv4, la idea de A6 fue una revisión y puesta a punto del DNS para ser más genérico, y de ahí su complejidad.

2.4.2.6 VENTAJAS Y DESVENTAJAS DEL USO DE IPV6

a) Desventajas:

- La necesidad de extender un soporte permanente para IPv6 a través de todo Internet y de los dispositivos conectados a ella.
- Para estar enlazada al universo IPv6 durante la fase de transición, todavía se necesita una dirección IPv4 o algún tipo de NAT (compartición de direcciones IP) en los routers pasarela (IPv6<-->IPv4) que añaden complejidad y que significa que el gran espacio de direcciones prometido por la especificación no podrá ser inmediatamente usado.
- Problemas restantes de arquitectura, como la falta de acuerdo para un soporte adecuado de IPv6 multihoming.
- Las direcciones IPv6 son mucho más largas que las direcciones IPv4 y, por lo tanto, más difíciles de memorizar.

B) Ventajas

- Convivencia con IPv4, que hará posible una migración suave.
- Gran cantidad de direcciones, que hará virtualmente imposible que queden agotadas. Se estima que si se repartiesen en toda la superficie de la Tierra habría $6,67 \times 10^{23}$ IPs por m².
- Direcciones unicast, multicast y anycast.
- Formato de cabecera más flexible que en IPv4 para agilizar el encaminamiento.
- Nueva etiqueta de flujo para identificar paquetes de un mismo flujo.
- No se usa ninguna comprobación de integridad (checksum).



- La fragmentación se realiza en el nodo origen y el reensamblado se realiza en los nodos finales, y no en los routers como en IPv4.
- Nuevas características de seguridad. IPSEC formará parte del estándar.
- Nueva versión de ICMP, que incluye a MLD, el equivalente del IGMP de IPv4.
- Auto-configuración de los nodos finales, que permite a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.
- Movilidad incluida en el estándar, que permitirá cambiar de red sin perder la conectividad.

2.4.2.7 MECANISMOS DE TRANSICIÓN A IPV6

Ante el agotamiento de las direcciones IPv4, el cambio a IPv6 ya ha comenzado. Se espera que convivan ambos protocolos durante 20 años y que la implantación de IPv6 sea paulatina. Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario. En general, los mecanismos de transición pueden clasificarse en tres grupos:

- Pila dual
- Túneles
- Traducción

La pila dual hace referencia a una solución de nivel IP con pila dual (RFC 2893), que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo de pila dual en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

- A favor: Fácil de desplegar y extensamente soportado.
- En contra: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

Los túneles permiten conectarse a redes IPv6 "saltando" sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como siguiente capa IP el protocolo número 41, y de ahí el nombre proto-41. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

La traducción es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicar con un nodo que sólo soporta IPv6. Los mecanismos de traducción se pueden dividir en dos grupos basados en si la información de estado está guardada:

- Con estado: NAT-PT RFC 2766, TCP-UDP Relay RFC 3142, Socks-based Gateway RFC 3089.

- Sin estado: Bump-in-the-Stack, Bump-in-the-API RFC 276

Actualmente el protocolo IPv6 está soportado en la mayoría de los sistemas operativos modernos, en algunos casos como una opción de instalación. Linux, Solaris, Mac OS, NetBSD, OpenBSD, FreeBSD, Windows (2000, XP y Vista de forma nativa) y Symbian (dispositivos móviles) son sólo algunos de los sistemas operativos que pueden funcionar con IPv6.

2.4.3 TCP (TRANSMISSION CONTROL PROTOCOL)

TCP es un protocolo que trabaja en la capa 3 del modelo de TCP/IP y esta orientado a conexión, provee confiabilidad para el intercambio de datos entre diferentes nodos de la red. TCP es usado a la vez por protocolos de capas superiores suministrando los siguientes servicios:

- a) Transferencia de datos:** TCP transfiere un flujo continuo de bytes a través de la red, se encarga de agruparlos en segmentos que pasan a IP para ser enviados a su destino.
- b) Fiabilidad:** TCP asigna un número de secuencia a cada byte enviado y espera una respuesta (ACK) por parte del equipo destino, si esta no se recibe en un determinado tiempo, se envía de nuevo la información.
- c) Control de flujo:** el equipo destino al regresar el ACK, para validar que la información llego correctamente, también incluye el número de bytes que puede seguir recibiendo sin provocar un desbordamiento en su buffer. Estas son las principales características de TCP.

2.4.4 IP (INTERNET PROTOCOL)

IP es un protocolo no orientado a la conexión que trabaja en la capa 2 del modelo de TCP/IP, no garantiza que los paquetes lleguen a su destino. IP se ayuda de protocolos de la capa de Transporte o de Aplicación para proveer un servicio orientado a la conexión si éste es necesario. Es responsable del direccionamiento de los paquetes de información, fragmentación y reensamble de éstos, así como el movimiento de los datos entre la capa de Transporte y la de Interfaz de Red.

2.4.5 PROTOCOLOS DE TCP/IP

Los protocolos que componen la familia de TCP/IP están clasificados de acuerdo a su función, sin embargo existen docenas de protocolos que intervienen pero solo unos pocos son los que se usan de forma habitual en una red.

- a) **Transporte:** Transmission Control Protocol (TCP), User Datagram Protocol (UDP).
- b) **Internet:** Internet Protocol (IP), Internet Protocol V6 (IPv6), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Domain Name System (DNS), Reverse Address Resolution Protocol (RARP).
- c) **Enrutamiento:** Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Inter-Gateway Routing Protocol (EIGRP).
- d) **Servicios de usuarios:** Boot Protocol (BOOTP), File Transfer Protocol (FTP), Telnet.
- e) **Protocolos de pasarela:** Exterior Gateway Protocol (EGP), Gateway-to-Gateway Protocol (GGP), Interior Gateway Protocol (IGP), Border Gateway Protocol (BGP).
- f) **Otros:** Network File System (NFS), Network Information Service (NIS), Remote Procedure Call (RPC), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), Point to Point Protocol (PPP), Serial Line Internet Protocol (SLIP).

2.5 DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

El Protocolo de Configuración Dinámica de Host (DHCP) se desarrolló para resolver el problema de asignar una dirección IP única a cada nodo y configurar los demás parámetros con los valores adecuados en una red de grandes magnitudes. DHCP toma la forma de un servicio que los administradores configuran con intervalos de direcciones IP y otros parámetros. Las estaciones de trabajo son configuradas como clientes, y al iniciar su sistema contactan con el servicio y se les asigna un conjunto de parámetros TCP/IP adecuados, incluida una dirección IP única en la red, sin necesidad de configuraciones manuales.

DHCP es un servicio independiente que puede operar en cualquier sistema operativo. Existe software de servidor DHCP para muchas plataformas, incluidas Windows de Microsoft, NetWare de Novell y varias versiones de Unix.

Sin embargo, el concepto de asignación de direcciones IP con base en el servidor no es propio de DHCP, se basa en dos protocolos llamados RARP y BOOTP.

2.5.1 RARP (REVERSE ADDRESS RESOLUTION PROTOCOL)

El Protocolo de Resolución Inversa de Direcciones (RARP) hace lo contrario que el Protocolo de Resolución de Direcciones (ARP) que se utiliza en todos los sistemas TCP/IP. ARP convierte las direcciones IP del nivel de red en



direcciones hardware del nivel de enlace de datos, y RARP trabaja difundiendo las direcciones hardware de un sistema y recibiendo como respuesta de un servidor RARP las direcciones IP.

Diseñado para su uso en estaciones de trabajo sin disco que no tienen medio de almacenar la información de su propia configuración TCP/IP, un servidor RARP puede suministrar direcciones IP a todos los sistemas de un segmento de red. RARP se basa en mensajes de difusión generados por el cliente porque no hay medio de que las estaciones de trabajo sin disco almacenen la dirección del servidor RARP. Por consiguiente, como las difusiones se limitan a la red local, había que tener un servidor RARP en cada segmento de red para el servicio de las estaciones de trabajo de dicho segmento. RARP sólo es capaz de proporcionar a los sistemas cliente una dirección IP. Para que sea útil en las redes actuales, un protocolo debe proporcionar también los valores de otros parámetros de configuración, como DNS y puertos de enlaces predeterminadas. RARP sólo es un mecanismo para el almacenamiento y la entrega de direcciones IP. Los administradores todavía tienen que asignar manualmente direcciones a los clientes creando una tabla de búsqueda en el servidor RARP.

2.5.2 BOOTP (BOOTSTRAP PROTOCOL)

El protocolo Bootstrap (BOOTP) supone una mejora con respecto a RARP. Diseñado también para estaciones de trabajo sin disco, BOOTP es capaz de dar más que una dirección IP, usa datagramas estándar UDP/IP. Los servidores BOOTP pueden usar el Protocolo Trivial de Transferencia de Archivos (TFTP) para enviar un archivo de arranque a un sistema cliente sin disco, además de una dirección IP y otros parámetros de configuración de TCP/IP. Al igual que RARP, los clientes BOOTP usan transmisiones de difusión para contactar con el servidor, pero el estándar propone el uso de agentes relé (relay agents) de BOOTP para que un servidor BOOTP pueda proporcionar servicio a clientes de varios segmentos de red.

Un agente relé de BOOTP detecta las difusiones BOOTP en un segmento de la red y las transmite al servidor de otro segmento de red. Muchos routers del mercado admiten el retransmisor de BOOTP. El principal inconveniente de BOOTP es que los administradores tienen que crear manualmente, como con RARP, en el servidor una tabla de búsqueda que contenga las direcciones IP y otros parámetros de configuración para su asignación a los clientes.

2.5.3 OBJETIVOS DE DHCP

BOOTP elimina la necesidad de que los administradores configuren en cada cliente parámetros de TCP/IP, pero existe la posibilidad de que se asigne a los sistemas direcciones IP duplicadas por errores de mecanografía en la tabla de búsqueda. Lo que se necesitaba era un servicio que asignará automáticamente direcciones a los sistemas cuando se le pidiera, y que llevara una



cuenta de las direcciones ya asignadas y de cuales estaban disponibles. DHCP mejora el concepto de BOOTP permitiendo a los administradores crear un conjunto de direcciones IP. Cuando un sistema cliente arranca, pide una dirección al servidor DHCP, que le asigna una del conjunto de direcciones, junto con otros parámetros que el cliente necesita.

Si a un cliente se le asigna una dirección en una subred particular, y éste se traslada a otro departamento con otra subred, DHCP asignará al sistema otra dirección en la nueva subred, y debe recuperar la dirección antigua. Para solucionar éste problema, DHCP tiene un mecanismo para la concesión de direcciones IP a los clientes. Cada vez que un servidor asigna una dirección, inicia un temporizador que al final expirará si el sistema no renueva la concesión. Cada vez que se inicia el cliente, se renueva la concesión. Si expira la concesión, el servidor libera la dirección IP asignada y la devuelve al conjunto de direcciones IP para una posible asignación nueva.

Otro problema que surge es la posibilidad de que la dirección IP de un cliente cambie periódicamente. Si la concesión expira por alguna razón, es probable que el servidor asigne al sistema una dirección diferente la próxima vez que se conecte a la red. A los clientes de Windows se les asigna con frecuencia nombres permanentes en el servicio de nombres DNS o NetBIOS, o en ambos. En cualquier caso, un cambio de dirección IP puede hacer que la información de resolución de nombres no sea válida. Sin embargo, la mejor solución es WINS, que registra el nombre NetBIOS de cada sistema cliente y su nueva dirección IP cada vez que éste se conecta a la red.

Para los nombres DNS el problema es más complejo, ya que la mayoría de los servidores DNS tradicionalmente no han actualizado dinámicamente los registros de recursos que contienen los nombres de host y sus direcciones IP equivalentes. En un sistema de red que funciona como servidor de Internet (como un servidor Web o FTP), su dirección IP se debe asignar de modo permanente.

Cuando se configura una estación de trabajo para ser cliente DHCP, el sistema inicia un intercambio de mensajes con el servidor DHCP. El primer intercambio de mensajes, cuyo resultado es la asignación de una dirección IP al cliente, es el mismo independientemente de que la asignación de direcciones sea dinámica, automática o manual.

Los objetivos de DHCP son los siguientes:

- a) El servidor DHCP debe ser capaz de proporcionar a la estación de trabajo todos los parámetros necesarios para configurar el cliente TCP/IP de modo que no fuera necesaria la configuración manual.
- b) El servidor DHCP debe ser capaz de funcionar como un almacén de parámetros de configuración TCP/IP para todos los clientes de la red.



- c) El servidor DHCP debe asignar la dirección IP de tal modo que no fuera posible duplicar las direcciones de red.
- d) El servidor DHCP debe ser capaz de configurar los clientes de otras redes por medio de la utilización de agentes retransmisores.
- e) Los servidores DHCP deben admitir la asignación de direcciones IP específicas a sistemas cliente específicos.
- f) Los clientes DHCP deben conservar sus parámetros de configuración TCP/IP a pesar de una recarga de los sistemas cliente o servidor.

2.5.4 ESTRUCTURA DEL PAQUETE DE DHCP

Las comunicaciones DHCP usan ocho tipos de mensajes diferentes, todos ellos con el mismo formato básico de paquete. DHCP se transporta en datagramas UDP/IP estándar, que usan el puerto 67 del servidor y el puerto 68 del cliente, los mismos puertos que BOOTP. El paquete de DHCP contiene los siguientes campos:

- a) **Código OP (Op, 1 byte):** especifica si el mensaje es una petición o una respuesta, usando los siguientes códigos:1 BOOTREQUEST, 2 BOOTREPLY
- b) **Tipo de hardware (Htype, 1 byte):** especifica el tipo de dirección hardware usado en el campo chaddr, los cuales son los siguientes:1 Ethernet, 4 Token Ring, 6 Redes IEEE 802, 7 ARCnet, 11 LocalTalk, 14 SMDS, 15 Frame Relay, 16 A TM, HDLC, 18 Fibre Channel, 19 ATM, Serial Line,21 ATM
- c) **Longitud de dirección hardware (hlen, 1 byte):** especifica la longitud (en bytes) de la dirección hardware que se encuentra en el campo chaddr, de acuerdo con el valor del campo htype, si htype es igual a 1, lo que indica una dirección hardware Ethernet, el valor de hlen será 6 bytes.
- d) **Hops (1 byte):** Especifica el número de segmentos de red entre el cliente y el servidor. El cliente pone el valor a 0 y cada sistema retransmisor DHCP lo incrementa en uno durante su viaje hasta el servidor.
- e) **Identificador de Transacción (xid, 4 bytes):** contiene un identificador de transacción que el sistema usa para asociar los mensajes de petición y de respuesta de una transacción.
- f) **Segundos (secs, 2 bytes):** Especifica el número de segundos transcurridos desde que se asignó la dirección IP o se renovó la



concesión. Esto permite al sistema distinguir entre mensajes del mismo tipo generados durante una única transacción DHCP.

- g) **Indicadores (flags, 2 bytes):** contiene los indicadores de difusión, como el bit primero, que, cuando se pone a 1, especifica que el servidor DHCP y los agentes retransmisores deben usar difusión para transmitir a los clientes, y no unidifusión. Los restantes bits del campo no se usan y deben tener valor 0.
- h) **Dirección IP del cliente (ciaddr, 4 bytes):** especifica la dirección IP del cliente en los mensajes DHCPREQUEST transmitidos durante los estados asociado, renovación o asociando. En todos los demás casos el valor debe ser 0.
- i) **Dirección IP propia (yiaddr, 4 bytes):** especifica la dirección IP que el servidor ofrece o asigna mediante los paquetes DHCPOFFER o DHCPACK. En otros casos su valor debe ser 0.
- j) **Dirección IP del servidor (siaddr, 4 bytes):** especifica la dirección IP del siguiente servidor en la secuencia de arranque. Los servidores incluyen esta información en los mensajes DHCPOFFER o DHCPACK solamente cuando DHCP está configurado para enviar un archivo ejecutable de arranque a los clientes y los archivos de arranque de varias plataformas de cliente están almacenados en diferentes servidores.
- k) **Dirección IP del enlace predeterminado (giaddr, 4 bytes):** especifica la dirección IP del agente retransmisor DHCP al cual debe enviar el servidor sus respuestas cuando el servidor y el cliente están situados en diferentes subredes. Cuando el cliente y el servidor están situados en el mismo segmento, el valor debe ser 0.
- l) **Dirección hardware del cliente (chaddr, 16 bytes):** especifica la dirección hardware del sistema cliente en los mensajes DHCPDISCOVER y DHCPREQUEST, que usa el servidor para dirigir sus respuestas unidifusión al cliente. El formato de la dirección hardware se especifica por los valores de los campos htype y hlen.
- m) **Nombre de host del servidor (sname, 64 bytes):** especifica el nombre (opcional) de host del servidor DHCP. El campo se usa más comúnmente para contener datos sobrantes del campo opciones.
- n) **Nombre del archivo de arranque (file, 128 bytes):** especifica el nombre del archivo ejecutable de arranque para estaciones de trabajo sin disco en los mensajes DHCPDISCOVER, en cuyo caso se envía un nombre de archivo genérico, o DHCPOFFER, en el que el campo contiene un nombre y una ruta completos. El campo se usa más comúnmente para contener datos sobrantes del campo opciones.



- o) Tamaño variable (options, mínimo 312 bytes):** especifica la cookie mágica que indica cómo se deben interpretar el resto de los campos y la opción Tipo de mensaje DHCP que define la función del mensaje, así como otras opciones, que contienen datos de configuración de otros parámetros TCP/IP.

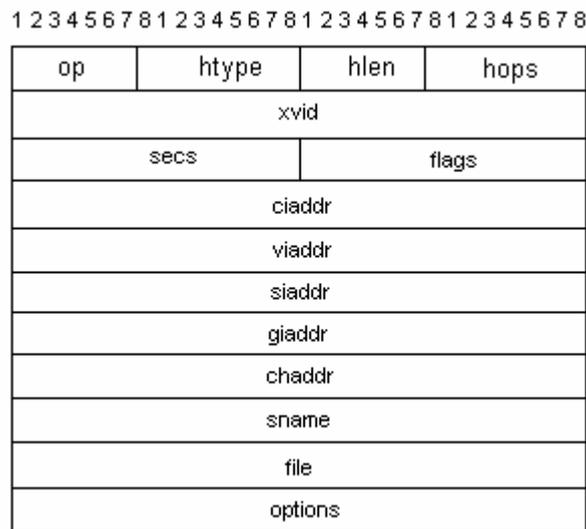


Fig. 2.15 Paquete básico de DHCP.

2.5.5 ASIGNACIÓN DE DIRECCIONES IP

La función principal de DHCP es asignar direcciones IP y configurar las necesidades de todos los tipos de clientes. El estándar define tres tipos de asignación de direcciones, que son los siguientes:

- a) Asignación manual:** el administrador configura el servidor DHCP para asignar direcciones IP específicas a un sistema dado, que no cambian nunca a menos que se modifiquen manualmente. Esta funcionalidad es equivalente a RARP y BOOTP. La asignación manual es adecuada para los servidores de Internet y otras máquinas que requieren direcciones IP estáticas, porque se basan en resolución de nombres DNS para el acceso de los usuarios. Si se guardan todas las asignaciones de dirección en una base de datos, resulta más fácil controlar las asignaciones y se reduce la probabilidad de duplicaciones. Puede haber direcciones IP duplicadas accidentalmente si se configura el cliente TCP/IP a mano con una dirección que está incluida en el ámbito DHCP.
- b) Asignación automática:** el servidor DHCP asigna direcciones IP permanentes de un conjunto, que no cambian a menos que las modifique el usuario o el administrador. La asignación automática es útil en redes estables de un solo segmento, o en redes multisegmento en las que las máquinas no se mueven con frecuencia a otros segmentos. Este método reduce el tráfico de la red eliminando los procedimientos de renovación de concesiones de direcciones. En la mayoría de los casos,



los ahorros son mínimos. Tampoco se recomienda la asignación automática si la organización trabaja con muchas direcciones IP registradas.

- c) Asignación dinámica:** el servidor DHCP asigna direcciones IP de un conjunto usando una concesión limitada en el tiempo, de modo que las direcciones pueden ser reasignadas si el cliente no las renueva periódicamente. La asignación dinámica proporciona la mayor flexibilidad con la menor intervención administrativa. El servidor DHCP asigna direcciones IP a los sistemas de una subred y recupera automáticamente las direcciones que ya no se usan para su reasignación. Tampoco hay posibilidad de que existan direcciones duplicadas en la red, siempre que DHCP administre todas las direcciones de la red.

Antes de que pueda comenzar el intercambio cliente/servidor, se presenta la pregunta de cómo puede el cliente encontrar el servidor y comunicarse con él cuando su pila TCP/IP aún no se ha configurado. Se dice que un cliente DHCP que todavía no tiene una dirección IP está en el estado de inicialización. En este estado, aunque la estación de trabajo no tiene información acerca de los servidores de la red y tampoco dirección IP propia, es capaz de enviar mensajes de difusión. El cliente inicia el intercambio difundiendo una serie de mensajes DHCPDISCOVER. En este paquete la opción tipo de mensaje DHCP tiene un valor 1 en el campo data y lleva la dirección hardware del cliente en el campo chaddr (o dirección hardware del cliente). En la mayoría de los casos ésta será la dirección MAC grabada en la tarjeta adaptadora de red, identificada por el valor de los campos htype y hlen. Como el cliente no tiene aún una dirección IP propia, el campo dirección origen de la cabecera IP contiene el valor 0.0.0.0. El mensaje puede contener también otras opciones para pedir información específica del servidor, como la opción Dirección IP pedida.

2.5.6 DURACIÓN DE LA CONCESIÓN DHCP

Una vez configurados los servidores DHCP, requieren poca o ninguna supervisión. Dependiendo de la red y de la disponibilidad de direcciones IP, los administradores pueden modificar la duración de la concesión para minimizar el tráfico generado en la red por las comunicaciones DHCP. En una red TCP/IP no registrada no va a haber escasez de direcciones IP, de modo que se puede incrementar la duración de las concesiones de modo seguro para hacer menos frecuentes las renovaciones.

Por ejemplo, al incrementar la concesión de 3 a 30 días un sistema puede estar funcionando continuamente durante 15 días sin intentar renovar su dirección. Si hay que mantener asignadas algunas direcciones durante unas semanas después de que una máquina se traslade a otra subred no hay ningún problema.



Sin embargo, en las redes que usan direcciones IP registradas, y que tienen una cantidad limitada de éstas, se puede disminuir la duración de la concesión para prevenir que las direcciones queden huérfanas durante un periodo largo, sin embargo, en una red estable en la que los equipos raramente se trasladan, puede no ser necesario que las concesiones expiren en absoluto.

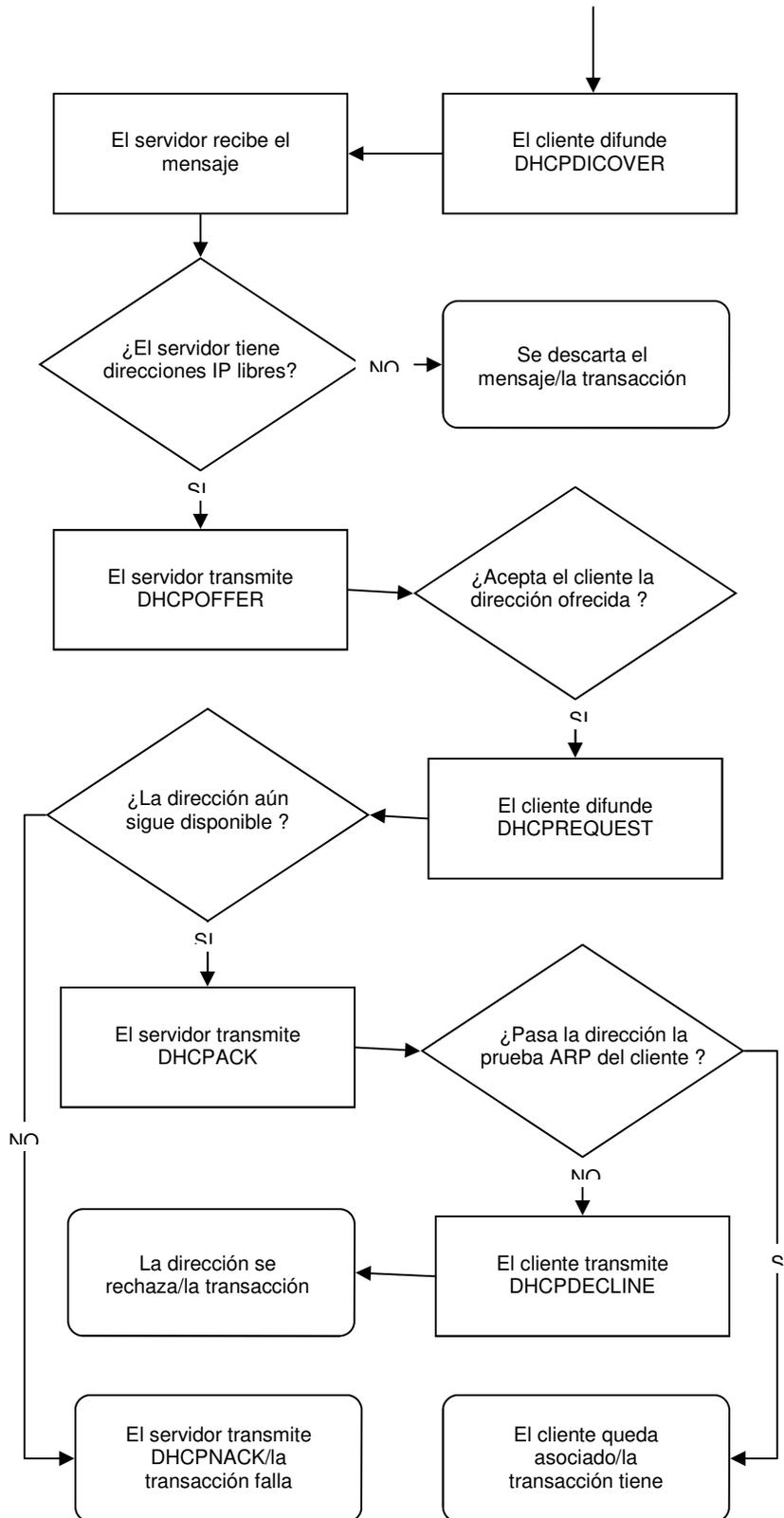


Fig. 2.16 Negociación de dirección IP en DHCP.

2.6 DIPOSITIVOS DE INTERCONEXIÓN DE REDES

Una interconexión de redes es una colección de varias redes individuales que se conectan mediante dispositivos para formar una gran red con el objetivo de dar una comunicación transparente al usuario independientemente de que tecnologías se utilizan en cada una. Las interconexiones de Redes de Área Local (LAN) han crecido en número debido a que día a día se requiere estar comunicados con la oficina y compartir archivos y todo tipo de información. Cabe mencionar que se pueden considerar dos tipos de interconexiones de acuerdo a la extensión geográfica que se alcanza, por ejemplo:

- a) **Interconexión de Área Local (LAN con LAN):** conecta redes que están relativamente cerca, así como redes LAN dentro de un mismo edificio, o redes que están en diferentes edificios, como consecuencia se tiene una Red de Área Metropolitana (MAN).
- b) **Interconexión de Área Extensa (LAN con MAN ó LAN con WAN):** este concepto se refiere a la incorporación de red LAN a una red metropolitana (MAN) o a una red extensa (WAN).

Existen varios dispositivos que nos permiten hacer conexiones entre redes, estos caen en las categorías de repetidores, puentes (bridges), enrutadores (routers) y gateways, cada uno de estos tiene una aplicación específica de acuerdo al nivel del Modelo de Referencia OSI que alcanza, es decir, mientras que algunos de estos solo hacen una conexión física, otros pueden alcanzar un nivel superior donde regulen el tráfico, o garanticen la transmisión de información del usuario.

Aplicación		Gateways
Presentación		
Sesión		
Transporte		
Red		Enrutadores (Routers)
Enlace		Puentes (Bridges)
Física		Repetidores

Fig. 2.17 Alcance de los equipos sobre el Modelo de Referencia OSI

2.6.1 REPETIDORES

Este es el dispositivo más simple que opera en la capa Física. Su función principal es la de conectar dos segmentos de red, regenerando eléctricamente la señal para tener un alcance mayor. Los repetidores no tiene la capacidad de regular tráfico o tener información acerca de las rutas, otro uso de los repetidores es la conexión de segmentos que usan medios de transmisión diferentes, por ejemplo conectar fibra con cable coaxial.

2.6.2 PUENTES (BRIDGES)

Los puentes operan en la capa de Enlace, se consideran como dispositivos inteligentes y nodos de la red, se usan para conectar dos redes totalmente independientes una de le otra, por lo general del mismo tipo o tecnología, sin embargo existen algunos de ellos que pueden conectar por ejemplo Ethernet con Token-Ring. Tienen la capacidad de distinguir entre el tráfico local y el no local permitiendo así solo el paso de la información inter-LAN. Pueden conocer las direcciones MAC (Media Access Control) de los dispositivos en la red, por lo tanto cuentan con una tabla de direccionamiento de 48 bits para cada estación y teniendo, por consecuencia, la capacidad de conocer las rutas de las redes.

2.6.3 ENRUTADORES (ROUTERS)

Los enrutadores trabajan en la capa de Red, son dispositivos que direccionan información de una red a otra de un protocolo común y dependen del protocolo de enrutamiento propio de cada red, son capaces de convertir los paquetes de información de una red de área local en paquetes capaces de ser enviados mediante redes de área extensa. Además pueden seleccionar la ruta por la cual van a enviar la información, cuando llega un paquete de información a un enrutador, éste examina la dirección destino y busca en su tabla de rutas la mejor. Esta tabla de rutas contiene las direcciones de los nodos así como las trayectorias para llegar a ellos y un factor que determina la mejor trayectoria, digamos un costo. En primer lugar para poder establecer una tabla de rutas se tiene que considerar dos tipos de enrutamiento, la estática y la dinámica, la primera es cuando el administrador de la red fija las rutas a seguir, y la dinámica es cuando los enrutadores están actualizando constantemente sus tablas y recalculan la trayectoria óptima. Hablando particularmente de los enrutadores que operan bajo TCP/IP, estos utilizan protocolos de enrutamiento dinámico como RIP, OSPF, ES-IS, BGP, IGRP, que determinan las mejores rutas de acuerdo al numero de saltos (entre enrutadores) o un costo asignado a la ruta.

2.6.4 GATEWAY

Son dispositivos que operan en las capas de Transporte, Sesión, Presentación y Aplicación, soportan diversos protocolos y hacen la conversión de estos para establecer la conexión, además pueden usarse como



dispositivos generales en una red compuesta por redes de diversos tipos, aseguran que la información transportada de una red sea compatible con otra. Estos dispositivos hacen totalmente transparente una red.

CAPITULO 3. INTERNET INALÁMBRICO.

3.1 INTRODUCCIÓN

En los últimos años las Redes Locales Inalámbricas (WLAN, Wireless Local Area Network) han cobrado gran interés y ha crecido su demanda conforme a sus prestaciones y las nuevas aplicaciones que se descubren para las mismas. Las WLAN permiten la movilidad del usuario eliminando los cables. Al igual que las LAN, son implementadas en edificios, entre edificios y en campus de algunos kilómetros, pero no solamente se encuentran aplicaciones en empresas o lugares privados, sino también en lugares públicos como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios (hot spots), tales como aeropuertos, restaurantes, plazas comerciales, hospitales, etc.

Las WLAN ofrecen ventajas, sobre las LAN convencionales, se pueden utilizar como ampliación o sustitución directa de las redes cableadas cuando el costo es muy alto o cuando esta prohibido el tendido de cables, o bien cuando solo se requiere una red local temporal, la implementación de una WLAN es rápida, sencilla, y se evita dañar instalaciones.

A pesar de que este capítulo se llama Internet Inalámbrico, se hace énfasis más que nada en redes locales de tipo inalámbricas, sus topologías, las tecnologías que se utilizan para la implementación de las mismas, los diferentes organismos que rigen y normalizan la tecnología inalámbrica, las técnicas de modulación y el estándar 802.11, entre otros conceptos.

Se ha definido al Internet como un conjunto de redes de todo tipo a nivel mundial, donde el usuario tiene acceso a ciertos recursos dependiendo de los privilegios que le brinda su ISP. La tecnología inalámbrica es un recurso que emplea el usuario para conectarse a Internet, se tienen restricciones de cobertura que sirve al proveedor para restringir el número de usuarios y para controlar la calidad de su servicio, es por eso que se estudian en este capítulo las redes locales de tipo inalámbricas (WLAN).



3.2 REDES LOCALES INALÁMBRICAS, WLAN (WIRELESS LOCAL AREA NETWORK)

Las WLAN son sistemas de comunicación de datos muy utilizadas como una alternativa a las redes LAN, o como una extensión de éstas. La aparición en el mercado de las computadoras portátiles y los organizadores personales (PDA, Personal Digital Assistant), y en general de sistemas y equipos de informática portátiles es lo que ha generado realmente la necesidad de una red que los pueda acoger, o sea, de las WLAN. De esta manera, las WLAN hace posible que los usuarios de equipos portátiles puedan estar en continuo movimiento, al mismo tiempo que están en contacto con los servidores y con los otros equipos de la red, es decir, las WLAN permiten movilidad y acceso simultáneo a la red. Con la implementación de las WLAN se tienen ventajas como movilidad del usuario, facilidad de instalación, reducción de costos e implementación de varias topologías. Cabe mencionar que las WLAN, actualmente basadas en estándares, funcionan a altas velocidades y anchos de banda extensos. El uso de este tipo de redes ha crecido considerablemente en varios sectores, por ejemplo se han instalado redes en campus universitarios donde los alumnos tiene acceso a las lecciones del profesor o archivos y tareas; en Reino Unido se han implementado redes en los hospitales que permiten a los doctores y enfermeras tener acceso al historial clínico del paciente; un ejemplo muy preciso es el uso de WLAN en oficinas donde se intenta sustituir las redes cableadas para una mayor movilidad del ejecutivo dentro del edificio, en estos días en México se han implementado redes WLAN como puntos de acceso hacia Internet en lugares públicos, en determinadas zonas, comúnmente llamados "Hotspot", localizados en restaurantes, bares, hospitales, aeropuertos, zonas comerciales, etc.; este tipo de redes también se han incorporado a tiendas de autoservicio, donde se usan para llevar el inventario, la actualización de los precios de los productos y también como forma de preregistro de los productos que se compran sin llegar a la caja de pago, entre otros muchos ejemplos.

3.2.1 VENTAJAS Y DESVENTAJAS DE LAS REDES WLAN

Las redes WLAN tienen ciertas ventajas sobre las redes LAN:

- a) Es fácil de agregar o remover un equipo de la red.
- b) Es fácil y rápido de proveer conectividad en áreas donde es difícil el tendido de cableado o la perforación de muros.
- c) El acceso a la red se puede hacer desde cualquier parte dentro de la cobertura del AP.
- d) El costo puede ser menor.

También se tienen ciertas desventajas al usar una red WLAN:

- a) El crecimiento de estaciones de trabajo en una red disminuye la tasa de transferencia destinada a cada equipo, esto mismo sucede con las LAN, pero como las WLAN trabajan a velocidades menores es más notable este comportamiento.
- b) La rápida evolución de estas redes implica la actualización de dispositivos, AP's, tarjetas de red, etc.
- c) En estos días, debido a la tasa de transferencia relativamente baja respecto a las redes LAN, es más eficiente la transmisión de video en redes cableadas.
- d) Los dispositivos operan a una determinada distancia, sin embargo a pesar de estar muy cerca del AP pero con un obstáculo como muros reforzados, árboles, agua estos puedes determinar la calidad de recepción, por lo que será necesario el aumento de AP's para tener mas cobertura, implicando mayor costo.

3.2.2 FUNCIONAMIENTO DE UNA RED WLAN

Las WLAN utilizan ondas de radio frecuencia para enlazar los equipos conectados a la red, mediante infrarrojos, láser, o mediante comunicaciones basadas en microonda. La IEEE ha desarrollado el estándar 802.11x, que ha ido evolucionando constantemente y es el que ofrece una red más robusta a comparación con tecnologías como Home RF, Bluetooth, HyperLan o IRDA. Las WLAN operan hoy en día a una velocidad de transmisión cercana a los 54 Mbps en la frecuencia de 5 GHz (para IEEE 802.11a), cercana a los 11 Mbps alrededor de 2.4 GHz (para IEEE 802.11b) y 54 Mbps en la frecuencia de 2.4 GHz (para IEEE 802.11g). En una red inalámbrica local existe un dispositivo receptor/transmisor llamado punto de acceso (Access Point, AP) cuya función es análoga a un hub y/o como punto de interconexión entre una red cableada y la WLAN.

3.2.3 TOPOLOGÍA DE LAS REDES WLAN

- a) **Peer–Peer (igual a igual):** es una configuración muy sencilla donde dos computadoras están equipadas con tarjetas de red inalámbrica y se comunican directamente.



Fig. 3.1 WLAN Peer - Peer

- b) **Red con un solo punto de acceso:** es una configuración donde existe un equipo que sirve como punto de acceso (Access Point, AP) que se conecta a una red cableada o a una red con mayor extensión, esta

configuración es la usada por los proveedores de Internet inalámbrico para que los usuarios tengan acceso él. Los equipos AP actúan como mediadores en el tráfico, cada uno sirve a varios clientes, tienen una capacidad determinada de usuarios. El punto de Acceso (AP) es normalmente colocado en una parte alta o donde se pueda tener una cobertura amplia.

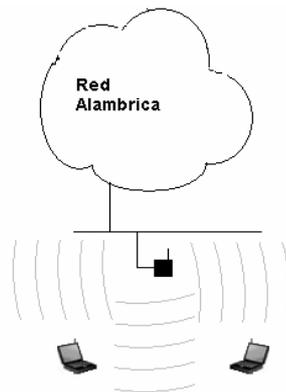


Fig. 3.2 WLAN con un AP

c) **Red con varios puntos de acceso:** este tipo de redes son utilizadas en campus o en edificios extensos, donde el usuario al moverse requiere no perder la comunicación, cada punto de acceso crea una célula de cierta extensión, 100 m. para lugares cerrados y 300 m. para lugares en el exterior.

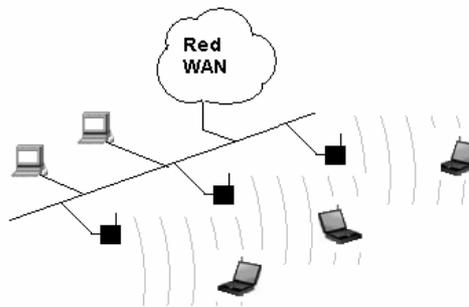


Fig. 3.3 WLAN con varios AP's

d) **Red con puntos de extensión:** es una variante de las redes con puntos de acceso, la diferencia es que se usa un dispositivo para extender el área de cobertura, no está físicamente ligada con la red cableada.

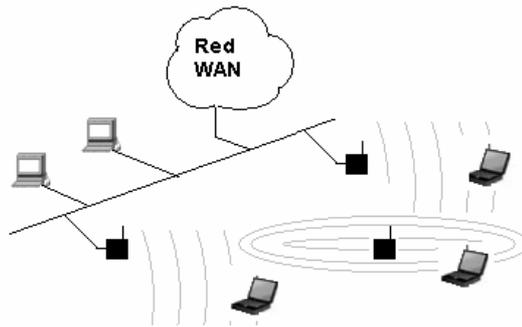


Fig. 3.4 WLAN con puntos de extensión

- e) **Red con antena direccional:** esta puede considerarse como un enlace de microondas interconectando dos redes LAN convencionales o dos redes WLAN. Posiblemente es una de las configuraciones más usadas desde años atrás, además puede ser el origen de las redes inalámbricas WAN, ya que frecuentemente se usa para la conexión de redes LAN ubicadas a distancias mayores, ya sea de unos cuantos kilómetros.

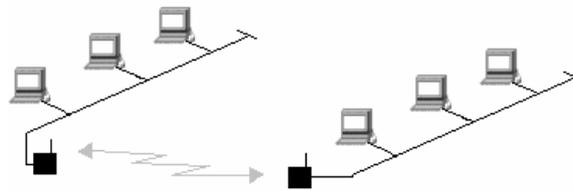


Fig. 3.5 WLAN con antena direccional

3.2.4 NORMALIZACIÓN

El origen de la LAN inalámbrica se da en el año 1979 siendo un experimento de IBM en Suiza que consistía en una red de infrarrojos para un área industrial. La parte experimental duro varios años estudiando infrarrojos y microondas. En 1985 la FCC (Federal Communications Commission) asignó las bandas IMS (Industrial, Scientific and Medical) que son las de 902 - 929 MHz, 2.400 - 2.4835 GHz y 5.725 - 5.850 GHz. A partir de entonces, desde 1985 a 1990, se comenzó a trabajar en la etapa de desarrollo, en 1990 se crea el comité IEEE 802.11 y fue en 1991 cuando se publicaron varios trabajos referentes a las WLAN que superaban la velocidad de transmisión de 1Mbps.

Debido a la demanda de las redes inalámbricas se han creado organizaciones que se encargan de establecer estándares y desarrollar nueva tecnología. Estos organismos pueden dividirse en tres tipos:

1. **Alianzas de tecnología:** las alianzas están formadas para introducir en el mercado una tecnología o protocolo específico y proveer interoperabilidad y certificación de las compañías que utilicen esa tecnología. Como ejemplos están:



- a) **Bluetooth SIG:** trabaja la especificación Bluetooth que utiliza ondas radioeléctricas para permitir la conexión a Internet a equipos portátiles.
 - b) **La HiperLAN1, HiperLAN Alliance e HiperLAN2 Global Forum:** son dos organizaciones Europeas que utilizan enlaces en las frecuencias de 5 GHz.
 - c) **Home RF:** trabaja una tecnología inalámbrica que se implementa más en hogares utilizando el protocolo SWAP (Shared Wireless Access Protocol). El nombre completo que se le da a ésta alianza es HRFWG (Home RF Working Group).
 - d) **OFDM:** se basa en una tecnología llamada WOFDM (Wideband Orthogonal Frequency Division Multiplexing)
 - e) **WLI Forum:** en 1996 estableció un estándar conocido como OpenAir, es una tecnología que opera en la frecuencia de 2.4 GHz usando espectro disperso con salto de frecuencia.
 - f) **WECA (Wireless Ethernet Compatibility Alliance):** se encarga de la interoperabilidad del estándar de la Wi-Fi que es la versión de la IEEE 802.11 que opera a 11 Mbps.
2. **Organizaciones de estándares:** proponen, definen y establecen estándares a nivel internacional abiertos a la industria, algunos ejemplos de estos organismos son: el IEEE (Institute of Electrical and Electronics Engineers) y el ETSI (European Telecommunications Standards Institute).
3. **Asociaciones de la industria:** estas organizaciones se crean para proveer el crecimiento de la industria proveyendo información educativa, tecnológica y de promoción. Como ejemplo de asociaciones de la industria esta la WLANA (Wireless LAN Association), esta es una organización que fomenta el crecimiento de la industria de las redes inalámbricas mediante la difusión educativa, promueve la competencia y avances tecnológicos.

3.2.5 REGULACIÓN DEL USO DE FRECUENCIAS EN MEXICO.

A partir del 9 de agosto de 1996 se creó un organismo descentralizado de la Secretaría de Comunicaciones y Transportes (SCT), denominado Comisión Federal de Telecomunicaciones (COFETEL), el cual tiene como principal objetivo regular y promover el desarrollo eficiente de las telecomunicaciones en el territorio mexicano.

En México se empezó a comercializar el acceso a Internet inalámbrico en el segundo semestre del 2004, de aquí en adelante la COFETEL ha estado



trabajando, en conjunto con la SCT y la Comisión Federal de Mejora Regulatoria, respecto a la regulación del uso de las frecuencias que se disponen para tal objetivo, sin embargo, durante el 2005 y el 2006 se tuvo un panorama un tanto confuso sobre éste tema, debido a que en México se tenían ciertas frecuencia destinadas para un propósito específico, mientras que la tecnología iba de la mano con la regulación de otros países, principalmente europeos, donde estas mismas frecuencias eran de uso libre. Desde el inicio, la COFETEL libero varias bandas de frecuencias para el uso del Internet libre, siendo estas: 902 a 928 MHz, de 2.4 a 2.4835 GHz, 5.150 a 5.250 GHz y 5.250 a 5.350 GHz, derivado de esta resolución que se tomó, varias entidades de la misma SCT estaban en desacuerdo, argumentando que sería caótico abrir sin restricciones estas bandas de frecuencias. No fue, sino hasta febrero del 2006 cuando finalmente la SCT y la COFETEL llegan a un acuerdo y se establece cuales con las bandas de frecuencia de uso restringido y cual las de uso libre, publicando en el Diario Oficial de la Federación, con fecha del 13 de marzo de 2006, su "Acuerdo por el que se establece la política para servicios de banda ancha y otras aplicaciones en las bandas de frecuencias des espectro radioeléctrico 902 a 928 MHz, 2400 a 2483.5 MHz, 3600 a 3700 MHz, 5150 a 5250 MHz, 5250 a 5350 MHz, 5470 a 5725 Mhz, y 5725 a 5850 MHz" . En éste acuerdo se establece:

- Como espectro de uso libre nacional las siguientes bandas de frecuencias para servicios de banda ancha y otras aplicaciones:
 - 902 a 928 MHz
 - 2,400 a 2,483.5 MHz
 - 5,150 a 5,250 MHz
 - 5,250 a 5,350 MHz
 - 5,725 a 5,850 MHz.

- Como espectro de uso determinado, las siguientes bandas de frecuencias del espectro radioeléctrico:
 - 3,600 a 3,700 MHz
 - 5,470 a 5,725 MHz

Las características de operación de los equipos que trabajen en estas bandas de frecuencias deben de cumplir con lo señalado a continuación:

- Banda 902-928 MHz, la potencia máxima de transmisión entregada a las antenas de los sistemas no deberá exceder de 1 W, pudiéndose utilizar antenas de transmisión con ganancia direccional máxima de 6 dBi de manera que se obtenga una Potencia Isotrópica Radiada Equivalente (PIRE) máxima de 4 W. Si se utilizan antenas de ganancia direccional mayor a 6 dBi, la potencia total de entrada a las mismas deberá ser reducida en la misma cantidad que la ganancia direccional exceda de 6 dBi.



- Banda 2,400-2,483.5 MHz, la potencia máxima de transmisión entregada a las antenas de los sistemas de radiocomunicación fijos punto a punto no deberá exceder de 500 mW, pudiéndose utilizar antenas de transmisión con ganancia direccional máxima de 6 dBi de manera que se obtenga una Potencia Isotrópica Radiada Equivalente (PIRE) máxima de 2 W. Asimismo, la potencia máxima de transmisión entregada a las antenas de los sistemas de radiocomunicación punto a multipunto no deberá exceder de 250 mW, pudiéndose utilizar cualquier tipo de antena de transmisión con ganancia direccional máxima de 6 dBi de manera que se obtenga una Potencia Isotrópica Radiada Equivalente (PIRE) máxima de 1 W. En ambos casos, si se utilizan antenas de ganancia direccional mayor a 6 dBi, la potencia total de entrada a las mismas deberá ser reducida en la misma cantidad que la ganancia direccional exceda de 6 dBi.
- Banda 5,150-5,250 MHz, la potencia máxima de transmisión entregada a las antenas de los sistemas de radiocomunicación no deberá exceder de 50 mW, pudiéndose utilizar antenas de transmisión con ganancia direccional máxima de 6 dBi, de manera que se obtenga una Potencia Isotrópica Radiada Equivalente (PIRE) máxima de 200 mW. La densidad de PIRE no deberá exceder de 10 mW/MHz en cualquier banda de 1 MHz o su valor equivalente de 0.25 mW/25 kHz en cualquier banda de 25 kHz. Si se utilizan antenas de ganancia direccional mayor a 6 dBi, la potencia total de entrada a las mismas y la correspondiente densidad de PIRE deberán ser reducidas en la misma cantidad que la ganancia direccional exceda de 6 dBi. Todas las emisiones fuera de banda de los sistemas operando en esta banda de frecuencias, no deberán exceder una densidad de PIRE de -27dBm/MHz.
- Banda 5,250-5,350 MHz, la potencia máxima de transmisión entregada a las antenas de los sistemas de radiocomunicación no deberá exceder de 250 mW, pudiéndose utilizar antenas de transmisión con ganancia direccional máxima de 6 dBi, de manera que se obtenga una Potencia Isotrópica Radiada Equivalente (PIRE) máxima de 1 W. La densidad de PIRE no deberá exceder de 50 mW/MHz en cualquier banda de 1 MHz. Si se utilizan antenas de ganancia direccional mayor a 6 dBi, la potencia total de entrada a las mismas y la correspondiente densidad de PIRE deberán ser reducidas en la misma cantidad que la ganancia direccional exceda de 6 dBi. Todas las emisiones fuera de banda de los sistemas operando en esta banda de frecuencias, no deberán exceder una densidad de PIRE de -27dBm/MHz.
- Bandas 3,600-3,700 MHz y 5,470-5,725 MHz, las condiciones de operación para los sistemas de radiocomunicación que operen en esta banda, serán dadas a conocer durante el proceso de licitación correspondiente



3.3 ACCESO INALÁMBRICO DE BANDA ANCHA (BROADBAND WIRELESS ACCESS)

Los equipos inalámbricos emplean ondas de radio en sus comunicaciones, de esta manera, se puede llevar la información de un punto a otro sin necesidad de disponer de una instalación para ello, evitando posibles obstáculos entre emisor y receptor. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora (modulación) de radio y el receptor debe extraerlos de ésta (desmodulación).

Las tecnologías empleadas en la transmisión en banda ancha se basan en la “Modulación por Esparcimiento en el Espectro” (Spread Spectrum Modulation). El “esparcimiento de espectro” consiste en diseminar la potencia de la señal en una banda ancha de frecuencias, consiguiendo ganar rendimiento en la relación señal/ruido, a costa de sacrificar ancho de banda. Con esta técnica se consiguen señales menos susceptibles al ruido eléctrico que con las modulaciones tradicionales de radio. Dado que las señales de radio comunes tienen un espectro estrecho solo interferirán en una pequeña porción de la señal “esparcida en el espectro”, obteniendo como resultado una menor interferencia y menores errores en la transmisión.

En 1985 la FCC, en un intento de fomentar los productos inalámbricos, modificó la regulación del radio-espectro. Esta modificación autorizaba a los productos de redes inalámbricas a operar en las bandas de Industria, Científicas y Médicas (ISM – Industry, Scientific and Medical) mediante modulación de “esparcimiento del espectro” y con una potencia de salida de hasta 1 watt. Las bandas ISM son:

- 902-928 MHz
- 2.4-2.4835 GHz
- 5.725-5.850 GHz

Para poder vender productos de sistemas LAN inalámbricos en un país particular, el fabricante debe asegurar la certificación por la Agencia Reguladora de radio-transmisión correspondiente.

Existen dos tecnologías de radio-transmisión con “esparcimiento de espectro” empleadas en las transmisiones en banda ancha: FHSS (Frequency Hopping Spread Spectrum) y DSSS (Direct Sequence Spread Spectrum). Ambas se basan en distintos fundamentos por lo que una no puede ínter operar con la otra.



3.3.1 ESPECTRO ENSANCHADO POR SALTO DE FRECUENCIA, FHSS (FREQUENCY HOPPING SPREAD SPECTRUM)

Esta técnica consiste en tomar la señal de transmisión y modularla con una señal portadora que “salta” (hops) de frecuencia en frecuencia, dentro del ancho de la banda asignada, en función del tiempo. El cambio periódico de frecuencia de la portadora, reduce la interferencia producida por otra señal originada por un sistema de banda estrecha, afectando solo si ambas señales se transmiten en la misma frecuencia y en el mismo momento.

Un patrón de salto (hopping code), determina las frecuencias por las que se transmitirá y el orden de uso de estas. Para recibir correctamente la señal, el receptor debe disponer del mismo patrón de salto que el emisor y escuchar la señal en la frecuencia y momento correcto. La regulación impone a los fabricantes el uso de al menos 75 frecuencias distintas para la transmisión de un canal con un tiempo máximo de 400ms de uso por frecuencia. La imposición de al menos 75 frecuencias distintas en una banda, permite tener varios canales que no se interfieran.

Es posible por tanto, disponer de varios equipos empleando la misma banda de frecuencia sin que se interfieran, asumiendo que cada uno de ellos emplea un patrón de salto diferente. Dos patrones de saltos que nunca emplean la misma frecuencia se dice que son ortogonales.

La secuencia de pseudo-ruido pn_t generada en el modulador es usada en conjunto con una modulación M-FSK para desplazar la frecuencia de la portadora de la señal FSK pseudo-aleatoriamente a una velocidad de saltos R_h . La señal transmitida ocupa un determinado número de frecuencias en el tiempo, cada una por un periodo de tiempo $T_h = 1/R_h$, llamado (dwell time). FHSS divide el ancho de banda disponible en N canales y saltos entre esos canales de acuerdo a la secuencia PN. Para cada tiempo de salto de frecuencia, el generador PN inyecta al sintetizador de frecuencias una señal FW el cual indica una de las 2^n posiciones en las frecuencias f_{hi} . El transmisor y el receptor deben de seguir el mismo patrón de saltos en las frecuencias.

El ancho de banda de transmisión esta determinada por la frecuencia más baja y la frecuencia más alta que limita los saltos y por el ancho de banda por salto en cada posición Δf_{ch} . Para un salto cualquiera, el ancho de banda ocupado instantáneamente es idéntico al ancho de banda de M-FSK, el cual por lo general es mucho menor que W_{ss} . En FHSS la potencia transmitida se concentra en un solo canal dependiendo de la frecuencia donde se ubica instantáneamente.

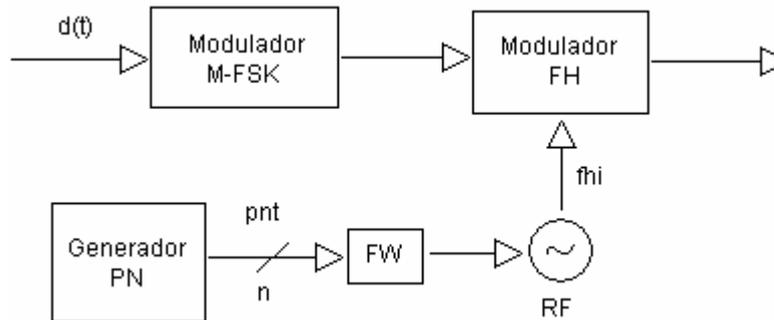


Fig. 3.6 Transmisor FHSS.

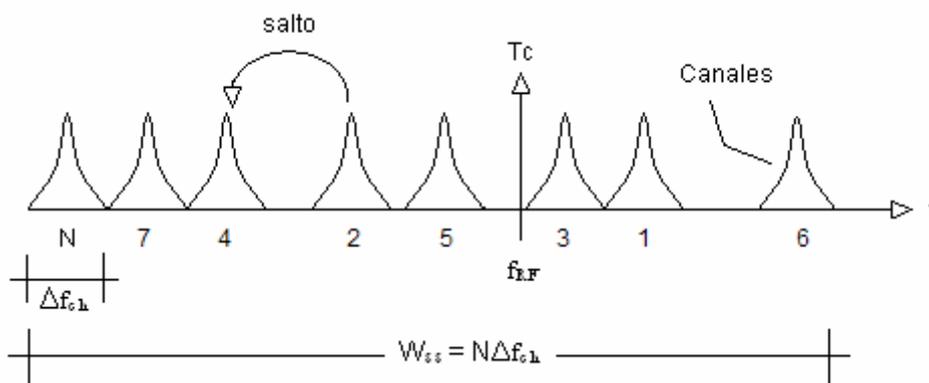


Fig. 3.7 Señal transmitida con FHSS.

A continuación se detallan algunas características de ésta técnica de modulación con respecto a DSSS:

- Menor costo.
- Consumo menor.
- Menor cobertura.
- Tolerante a interferencias de señales.

3.3.2 ESPECTRO ENSANCHADO POR SECUENCIA DIRECTA, DSSS (DIRECT SEQUENCE SPREAD SPECTRUM)

Esta técnica consiste en utilizar un código de pseudo ruido para modular directamente una portadora, así se aumentará el ancho de banda de la transmisión y reducir la densidad de potencia espectral. La señal que resulta, y la cual se va a transmitir, tiene un espectro muy parecido al ruido, de tal forma que a cualquier receptor le parecerá ruido menos al que va dirigida la señal. La combinación de la señal a transmitir con el código de pseudo ruido produce que se envíe una secuencia de bits mayor a la original. A esta secuencia se la conoce como chipping code o “código de troceado”, y no es más que un patrón redundante de bits asignado a cada bit a enviar. Cuando se desea enviar la información, realmente se transmiten los códigos correspondientes.

Si tenemos un pulso cuadrado de duración T_b que representan a la señal binaria que se va a transmitir, su representación en el dominio de la frecuencia es una función seno que cruza por cero para valores $1/T_b$, Esta señal se multiplica por una secuencia de pseudo ruido con pulsos de corta duración T_c y que en el dominio de la frecuencia cruza por cero en valores de $1/T_c$, formando así la señal dispersa en el espectro. El incremento de tiempo más pequeño en la señal de pseudo ruido, T_c , se le conoce como “tiempo chip”.

Mediante un diagrama de bloques de un transmisor y receptor DSSS se tiene lo siguiente: la señal binaria que será transmitida $m(t)$ entra a un modulo dispersor donde se va a extender en el espectro utilizando el código de pseudo ruido originado en éste modulo $c(t)$, posteriormente entra a un modulador donde se multiplicara con la portadora $A_c \cos(\omega_c t)$, resultando una señal $s(t)$ modulada y dispersa en el ancho de banda empleado. Para el caso del equipo receptor se tiene el mismo modelo pero con el proceso inverso.

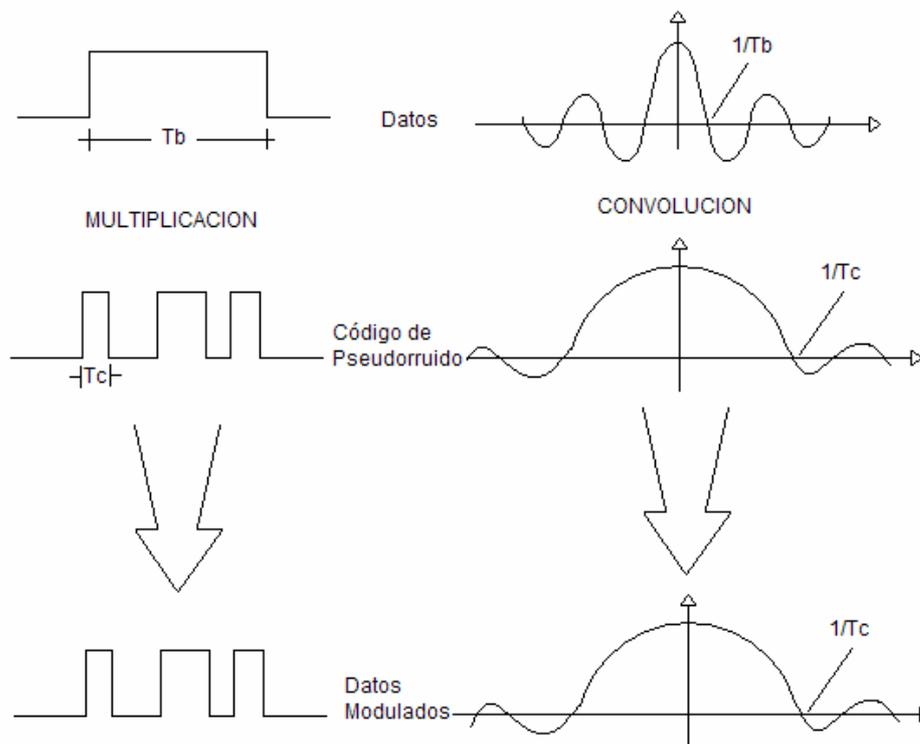


Fig. 3.8 Dispersión en el espectro de una modulación DSSS.
(imagen editada y obtenida de la pagina <http://es.wikipedia.org/wiki/DSSS>)

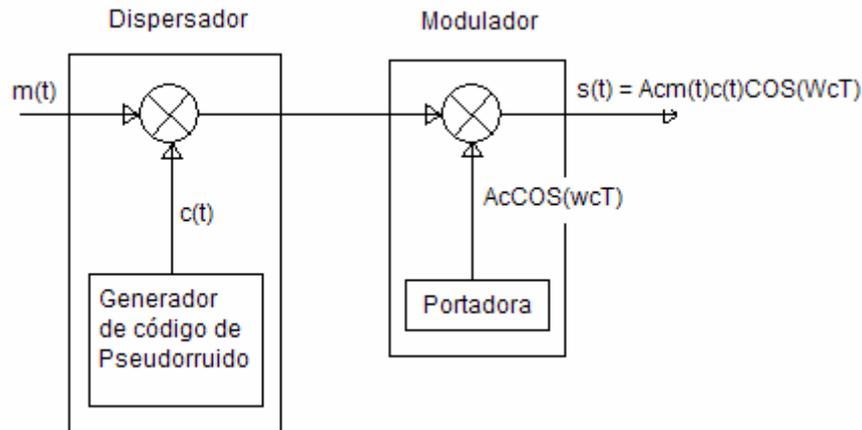


Fig. 3.9 Transmisor DSSS.

A continuación se detallan algunas características de ésta técnica de modulación con respecto a FHSS:

- Costo superior.
- Consumo superior.
- Mayor velocidad de transmisión.
- Mayor cobertura.
- Menor número de canales.

3.3.3 MULTIPLEXACIÓN POR DIVISIÓN DE FRECUENCIAS ORTOGONALES (OFDM)

La Multiplexación por División de Frecuencias Ortogonales, en inglés Orthogonal Frequency Division Multiplexing (OFDM), también llamada modulación por multitono discreto, en inglés Discrete Multitone Modulation (DMT), es una modulación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK.

Normalmente se realiza la multiplexación OFDM tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta modulación se denomina COFDM, del inglés Coded OFDM.

Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles, de portadoras equiespaciadas que forman una modulación OFDM, los procesos de modulación y demodulación se realizan en tiempo discreto mediante la IDFT y la DFT respectivamente.

La modulación OFDM es muy robusta frente al multitrayecto (multi-path), que es muy habitual en los canales de radiodifusión, frente a las atenuaciones selectivas en frecuencia y frente a las interferencias de RF.

Debido a las características de esta modulación, es capaz de recuperar la información de entre las distintas señales con distintos retardos y amplitudes (fading) que llegan al receptor, por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia.

Si se compara a las técnicas de banda ancha como CDMA, la modulación OFDM genera una alta tasa de transmisión al dividir el flujo de datos en muchos canales paralelos que se transmiten en igual número de carriers de banda angosta y con tiempos de símbolo (uno o varios bits) mayores al caso de usar banda ancha donde para lograr la misma tasa de transmisión los tiempos de símbolo son más cortos.

Los canales de banda angosta de OFDM son ortogonales entre sí, lo que evita el uso de bandas de guardas y así un eficiente uso del espectro. Ya que los desvanecimientos (fading) afectan selectivamente a uno o un grupo de canales, es relativamente simple ecualizarlos en forma individual lo que también se contrapone a la ecualización de un sistema de banda ancha.

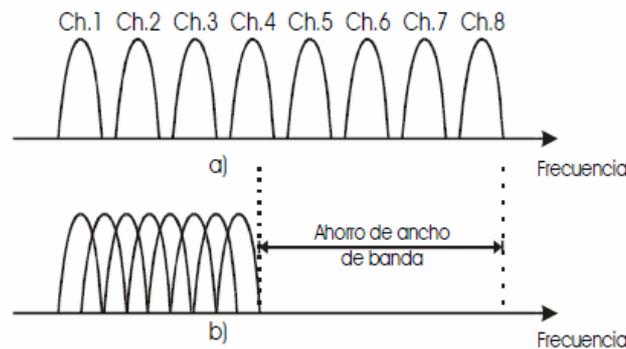


Fig. 1. a) Técnica Multiporadora convencional, b) Modulación con portadoras ortogonales

Fig. 3.10 OFDM

Entre los sistemas que usan la modulación OFDM destacan:

- La televisión digital terrestre DVB-T, que es un estándar de TDT
- La radio digital DAB
- La radio digital de baja frecuencia DRM
- El protocolo de enlace ADSL
- El protocolo de red de área local IEEE 802.11a/g/n, también conocido como Wireless LAN
- El sistema de transmisión inalámbrica de datos WiMAX

El sistema de transmisión de datos basados en PLC HomePlug AV

3.4 ESTÁNDAR 802.11

3.4.1 INTRODUCCIÓN

802.11 es un estándar de redes inalámbricas (WLAN), desarrollado por el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE) cuya especificación apareció en el año 1997. En su primera versión del estándar, 802.11, proporcionaba unas velocidades de transmisión de 1 o 2 Mbps trabajando en la frecuencia de 2.4 GHz, y una serie fundamental de métodos de señalización y otros servicios. El primero escollo que se encontró este estándar, fue el de su baja tasa de transferencia de datos, incapaz de soportar los requerimientos de las empresas en la actualidad. En consecuencia se trabajó en un nuevo estándar, el 802.11b (también conocido como 802.11 High Rate), que apareció en 1999 y proporcionaba unas tasas de transferencia de hasta 11 Mbps. Gracias a las prestaciones ofrecidas por 802.11b, similares a las de las redes cableadas, ha logrado tener una buena acogida en el mundo empresarial, siendo una de las tecnología más expandidas y que posee un amplio abanico de productos y compañías que la soportan.

Muchas de las empresas dedicadas al desarrollo de equipamiento informático se han unido en una alianza denominada WECA (Wireless Ethernet Compatibility Alliance), cuya misión es la de velar por la interoperabilidad entre productos 802.11b de distintos fabricantes y promocionar dicha tecnología en el ámbito empresarial, PYMES y hogar. Cuando un producto es comprobado que funciona correctamente con otros dispositivos 802.11b, recibe el certificado de Wi-Fi (Wireless Fidelity) como garantía de interoperabilidad y buen funcionamiento.

3.4.2 CONFIGURACIONES DE RED

802.11 define dos modos de red denominados: modo Infraestructura y modo Ad hoc. En el modo Infraestructura, la red consiste en al menos un punto de acceso (AP) y varios clientes inalámbricos, a esta configuración se la conoce como conjunto básico de servicio (BSS – Basic Service Set). Otra posible configuración es la de conjunto extendido de servicio (ESS – Extended Service Set) y consiste en una agrupación de dos o más BSS. El modo Adhoc, también conocido como peer to peer (de igual a igual), consiste en que cada cliente se comunique uno a uno con el resto de los clientes inalámbricos, sin emplear por tanto un punto de acceso.

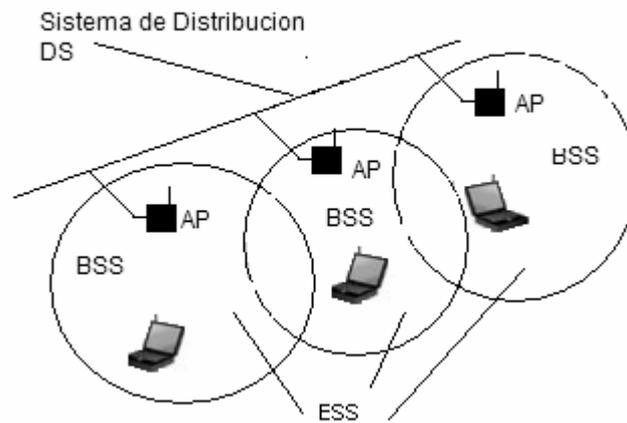


Fig. 3.11 Modo infraestructura



Fig. 3.12 Modo Adhoc o peer to peer

3.4.3 MODELO DE CAPAS

El estándar 802.11b abarca las capas Física y de Enlace del Modelo de Referencia OSI. A nivel físico, el estándar 802.11b trabaja en la banda ISM de los 2.4 GHz, reconocida por las Agencias Reguladores americana (FCC), europea (ETSI) y japonesa (MKK) para transmisiones de radio sin licencia. En el primer estándar que trabajaba a 1 o 2 Mbps se podía emplear FHSS o DSSS en la capa física, pero debido a las limitaciones de FHSS, para el estándar a 11 Mbps solo se emplea DSSS.

Empleando FHSS, la banda de los 2.4 GHz se divide en 75 subcanales de 1 MHz. El emisor y el receptor se ponen de acuerdo en un patrón de salto o "hopping pattern" para enviar los datos sobre una secuencia establecida de subcanales. En cada conversación en 802.11 se emplea un patrón de salto, en cuyo diseño se ha buscado minimizar la posibilidad de que dos emisores empleen el mismo subcanal a la vez. Las limitaciones de velocidad de FHSS provienen de las restricciones de los anchos de banda de los subcanales a 1 MHz.

Por el contrario, DSSS divide la banda de los 2.4 GHz en 14 canales de 22MHz. Los canales adyacentes se superponen parcialmente con un total de 3 canales de los 14 que no se superponen en ningún momento. Los datos son enviados en cualquiera de estos 22 canales, sin saltar de un canal a otro. Para compensar el ruido producido en cada canal se emplea la técnica del "chipping" o troceamiento.

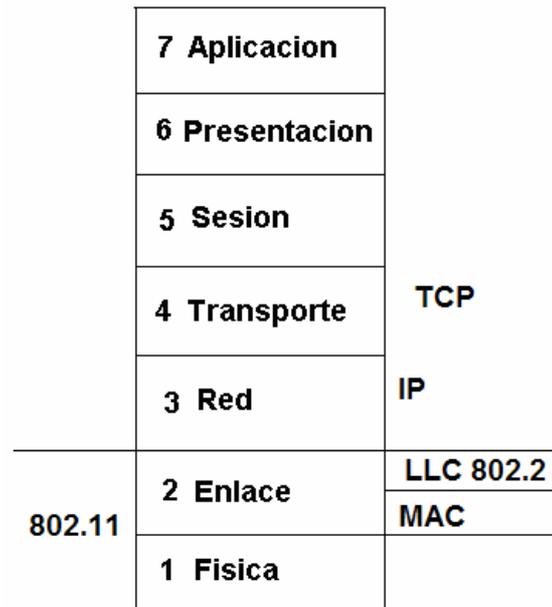


Fig. 3.13 802.11 y el modelo de capas OSI.

Para adaptarse a entornos con mucho ruido, esta tecnología dispone de desplazamiento dinámico de velocidad (dynamic shift ratio), que permite adaptar de manera automática la velocidad de transmisión para compensar el ruido del canal. Dependiendo de la cantidad de interferencia presente en el medio, el estándar es capaz de trabajar a: 11, 5.5, 2 o 1 Mbps. En la siguiente tabla podemos apreciar las especificaciones sobre las tasas de transferencia.

Data rate	Code length	Modulation	Symbol rate	Bits/Symbol
1 Mbps	11 (barker seq)	BPSK	1 MSps	1
2 Mbps	11 (barker seq)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Tabla 3.1 Tasas de transferencia.

La capa de enlace de 802.11 consiste en dos subcapas: LLC (Logical Link Control) y MAC (Media Access Control). La primera de ellas emplea la misma subcapa LLC de 802.2 con una dirección de 48 bits empleada también en las redes LAN 802. Esto permite la facilidad de transportar datos entre un sistema cableado y no uno cableado. La capa MAC es propia de 802.11, aunque en concepto es muy similar a la de 802.3, debido a que se basa en el principio de que muchos usuarios acceden al mismo y único medio. Debido a la imposibilidad de emplear la misma tecnología CSMA/CD (Carrier Sense Multiple Access with Collision Detect) de 802.3, dada la dificultad de “escuchar” una colisión, 802.11 emplea una modificación del protocolo denominada CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Este protocolo evita las colisiones, enviando un paquete de reconocimiento (ACK) para confirmar la llegada al receptor del paquete enviado.



CSMA/CA trabaja de la siguiente manera:

1. La estación transmisora comprueba el medio (aire), si no detecta ninguna transmisión en curso se pone a esperar una cantidad aleatoria de tiempo, si pasado este tiempo, el medio sigue "libre" comienza la transmisión.
2. Si el paquete se recibe intacto, la estación receptora envía un paquete ACK a la estación emisora. Si este paquete de reconocimiento llega al emisor, el ciclo es completado.
3. Si el emisor no recibe un ACK, bien porque el paquete de datos no llegó o porque se perdió el ACK, se asume que se produjo una colisión, y se esperará de nuevo un tiempo aleatorio para volver a intentarlo.

Debido a la sobrecarga u "overhead" del sistema de reconocimiento con ACK de 802.11, este presenta un peor rendimiento que su homólogo cableado 802.3.

Otro problema que presenta la capa MAC de 802.11 es debido a que dos estaciones en la misma cobertura de un punto de acceso pueden no poderse comunicar entre ellas debido a la distancia o los obstáculos. Dados que ambas pueden comunicarse con el punto de acceso, se habilita un protocolo denominado Request to Send/Clear to Send (RTS/CTS), en el que se reserva el medio para que ambas estaciones puedan comunicarse, haciendo esperar a las demás estaciones en la cobertura. La sobrecarga producida por RTS/CTS solo la hace factible en el envío de paquetes de gran tamaño.

Finalmente, la capa MAC ofrece dos características que mejoran la robustez del estándar: comprobación de suma CRC y fragmentación de paquetes. Cada paquete lleva asociado un CRC para asegurar que este no se ha corrompido en la transmisión. Esta es una diferencia con respecto a Ethernet, ya que esta dejaba tales comprobaciones a los protocolos de niveles superiores. La fragmentación de paquetes permite enviar pequeños fragmentos de paquete que permiten optimizar las comunicaciones en entornos congestionados o donde la interferencia es un factor a tener en cuenta.

3.4.4 COMO SE AGREGA UNA ESTACIÓN A UNA CELDA EXISTENTE

Para que una estación de trabajo se agregue a una celda en operación, necesita obtener información de sincronización del Punto de Acceso (AP). Esto se puede hacer de dos formas distintas:

- a) **Escaneo Pasivo:** En este caso la estación de trabajo espera para recibir una señal de sincronía que el Punto de Acceso está enviando constantemente.
- b) **Escaneo Activo:** Aquí la estación de trabajo trata de encontrar un Punto de Acceso enviando señales en forma de peticiones de aprobación, y esperando las respuestas de aprobación por parte del AP.

Una vez que la estación de trabajo haya encontrado el AP se lleva un proceso de autenticación donde se intercambia información ente el AP y la estación y en cuyo caso se tiene que validar una contraseña (password). Cuando la estación de trabajo se valida mediante esa contraseña, se inicia el proceso de asociación a la celda (BSS), mediante el intercambio de información acerca de las capacidades tanto de la estación de trabajo como del BSS. Ya concluido el proceso de asociación, entonces la estación de trabajo es capaz de transmitir y recibir información.

3.4.4.1 AUTENTICACIÓN Y PRIVACIDAD

En IEEE 802.11 se definen dos tipos de servicios para la autenticación, el primero se llama “Sistema Abierto” y el segundo “Llave compartida”. Cualquiera de estos dos tipos de autenticación se debe de indicar cuando se lleva a cabo el intercambio de información para que una estación de trabajo se anexe a la red, y ambos dispositivos deben de tener el mismo tipo de servicio para llevar a cabo una autenticación exitosa.

3.4.4.1.1 AUTENTICACIÓN DE SISTEMA ABIERTO (OPEN SYSTEM)

Prácticamente en este tipo de autenticación no se restringe a ningún dispositivo que se encuentre dentro de la cobertura del AP y que esté registrando señal de esa red. Aparentemente no tiene sentido éste método, sin embargo fue diseñado originalmente para tener un acceso rápido y para ser implementado en dispositivos portátiles como lectores de códigos de barras u organizadores personales. La autenticación de sistema abierto involucra dos pasos básicos:

- El cliente del AP envía un pedido de autenticación.
- El AP responde al pedido de la autenticación, si este es satisfactorio, entonces las dos estaciones están mutuamente autenticadas.

3.4.4.1.2 AUTENTICACIÓN DE LLAVE COMPARTIDA (SHARED KEY)

En este método se utiliza un código secreto que cada una de las estaciones de la red deben conocer, así como tenerlo configurado correctamente y tener activado el mecanismo de privacidad WEP (Wired Equivalent Privacy). Para llevarse a cabo la autenticación en el método de Llave compartida se tiene cuatro pasos:

- El cliente envía un pedido de autenticación.
- El AP responde al pedido de autenticación con un mensaje de texto.
- El cliente cifra el mensaje con la clave WEP que tiene configurada.
- Si el AP puede descifrar el mensaje con su clave WEP y coincide con el que envió originalmente, entonces responde dando acceso al cliente.



3.4.4.1.3 WEP (WIRED EQUIVALENT PRIVACY)

WEP (Wired Equivalent Privacy) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP son proporcionar confidencialidad, autenticación y control de acceso en redes WLAN. WEP utiliza una misma clave que tanto las estaciones de trabajo como el punto de acceso deben conocer. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Originalmente el algoritmo de encriptación utilizado es RC4 con claves (seed) de 64 bits, donde 24 bits corresponden al vector de inicialización más 40 bits de la clave secreta, posteriormente se paso a 128 bits, siendo los mismo 24 bits del vector de inicialización y siendo 104 bits para el código WEP.

El código WEP se debe distribuir manualmente y, por otro lado, el vector de inicialización (IV) es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave WEP. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. El código WEP, de primera instancia, ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value).
2. Se concatena la clave secreta a continuación del IV formado el "seed".
3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el seed y con ello podrá generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendrá el mensaje sin cifrar (datos y CRC-32) y finalmente se comprobará que el CRC-32 es correcto.

3.4.5 ROAMING O MOVILIDAD DE USUARIOS

La capa MAC es la encargada de asociar un cliente inalámbrico con un punto de acceso (AP). Cuando un cliente entra en la cobertura de uno o más puntos de acceso, se elige uno de ellos al cual se vincula, basándose en criterios sobre la potencia de la señal recibida. Una vez vinculado un punto de acceso, el cliente sintoniza un canal de radio en el que el punto de acceso está configurado.

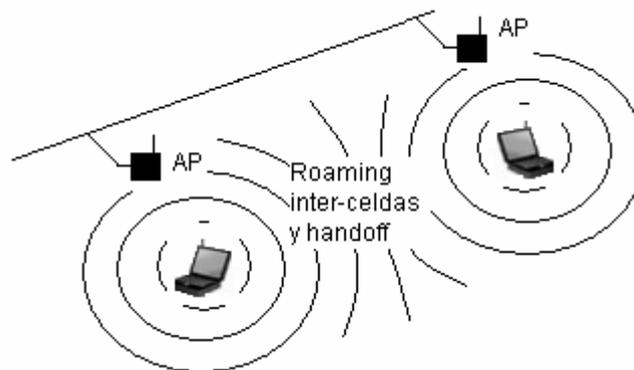


Fig. 3.14 Roaming y Handoff.

Aunque en principio la re-vinculación a un punto de acceso viene producida por la movilidad del usuario, también puede darse el caso de una re-vinculación derivada de una sobrecarga de la red, permitiendo el balanceo del tráfico de datos. Esta vinculación dinámica de los puntos de acceso, permite habilitar amplias zonas de cobertura empleando para ello una serie de células superpuestas.

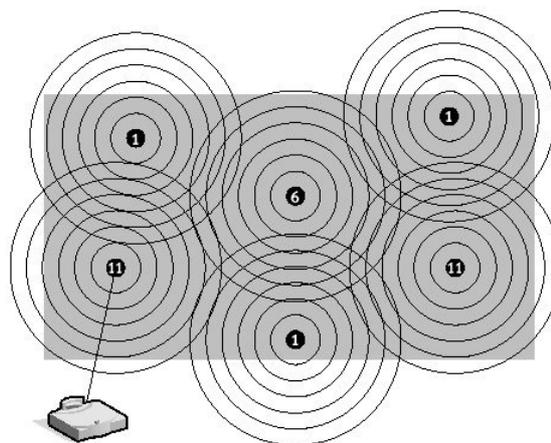


Fig. 3.15 Mapa de cobertura

Como se ve en la imagen, dado que la modulación DSSS empleada en la capa física del estándar provee de 3 canales sin superposición, se emplean dichos canales de manera adecuada en la confección de las células de

cobertura, evitando las posibles interferencias. La relación del número total de canales disponibles por países es: Estados Unidos/Canadá 11 canales, Europa 13 canales y Japón 14 canales.

3.4.6 SOPORTE DE VOZ Y VIDEO

Los datos limitados en tiempo para su transmisión, como la voz y el vídeo, son soportados por PCF (Point Coordination Function) a nivel de la capa MAC. A diferencia de CSMA/CA, donde el control era distribuido a cada estación, en PCF, el punto de acceso es el que controla el acceso al medio. Si un punto de acceso está configurado para emplear PCF, el tiempo es dividido entre el modo PCF y el modo CSMA/CA. En el modo PCF, el punto de acceso preguntará a cada estación si tiene datos a transmitir, no pudiendo enviar ésta antes de que se le haya preguntado. Pasado un periodo de tiempo el punto de acceso preguntará a la siguiente estación. Dado que el modo PCF asegura a cada estación un turno para enviar sus datos, es posible determinar la máxima latencia.

3.4.7 CONSUMO

802.11 provee de mecanismos para el ahorro de energía en dispositivos móviles alimentados con baterías. El estándar proporciona dos modos de energía: Modo de Alerta Continua y Modo de Ahorro de Energía y Sondeo. En la primera el equipo está consumiendo continuamente energía, mientras que en la segunda el equipo entra en estado de bajo consumo, mientras el punto de acceso se encarga de almacenar en un buffer los datos enviados a dicha estación. La estación se despertará periódicamente para recibir señales de notificación en las que el punto de acceso indica que estaciones tienen datos pendientes por recibir.

3.4.8 OTROS ASPECTOS

Los productos 802.11b suelen tener un radio de cobertura de unos 100 metros en interiores y 300 metros en exteriores. Las potencias que manejan estos dispositivos deben ser inferiores a los 100mw según la regulación, la cual es menor que la de los teléfonos móviles convencionales, con lo que los efectos para la salud son mínimos.

3.5 COMPARATIVA DE ESTÁNDARES

3.5.1 802.11b (2.4 GHz)

802.11b, trabaja en la frecuencia de los 2.4 GHz brindando una tasa de transferencia de 2 Mbps, 5.5 Mbps y hasta los 11 Mbps, utiliza Espectro ensanchado por secuencia directa (DSSS, Direct Sequence Spread Spectrum) para la modulación de la señal.

3.5.2 802.11g (2.4 GHz)

La evolución de 802.11 llega en 2003 al 802.11g, utilizando la misma frecuencia de 2.4 GHz pero alcanzando mayor tasa de transferencia hasta los 54 Mbps, también cuenta con la diferencia de que usa modulación OFDM (Orthogonal Frequency Division Multiplexing) para la emisión de la señal, lo cual permite un mejor desempeño en la transmisión de datos. A pesar de las diferencias percibidas entre los estándares b y g, estos dos pueden convivir en la misma red, a diferencia de que en una red cableada no se puede mezclar Ethernet y Fast Ethernet. En 802.11 g se tiene una particularidad, cuando se tienen clientes usando tecnología g y b en un mismo punto de acceso, los clientes g se ven afectados ya que deben de bajar su tasa transferencia al nivel de los clientes b; cuando esto sucede, la señal g ya no es transmitida en OFDM sino en DSSS.

802.11g define 14 diferentes canales de 22 Mhz de ancho cada uno, pero en Estados Unidos se establecen únicamente 11, donde el 1, 6 y 11 no se traslapan, esto permite tener 3 puntos de acceso cercanos operando en cada uno de estos tres canales y así se evita tener interferencia entre ellos.

3.5.3 802.11a (5 GHz)

802.11a nace en 1999, la tasa de transferencia máxima es de 54Mbps, utilizando la frecuencia de 5.4 GHz, en este caso se tienen 12 canales que no se traslapan, una ventaja de que trabaja en frecuencias altas es que no hay equipo que le haga interferencia como hornos de microondas, teléfonos inalámbricos, y Bluetooth. Sin embargo, equipos de 802.11b, g y a no son compatibles debido a las diferentes frecuencias en las que operan.

3.5.4 802.11n (2.4 y 5 GHz)

En el 2003 surge un Grupo de Trabajo de la IEEE enfocado a mejorar las redes inalámbricas creando el estándar 802.11n. Este nuevo estándar de operación aun no se encuentra en el mercado para uso común, se contempla la venta de dispositivos "n" en el 2010.

Se espera que 802.11n opere con tasas de transferencia superiores a los 300 Mbps, usando ya sea la frecuencia de 2.4 GHz, la de 5 GHz o ambas, lo cual permitirá que sea compatible con dispositivos actuales de 802.11a/b/g, sin embargo la tendencia de la tecnología es implementar redes que operen en la banda de los 5 GHz, dada la mayor capacidad disponible y por tener una frecuencia mas limpia.

802.11n tiene características muy particulares diferentes a los demás estándares empleando técnicas para garantizar un mejor desempeño de la red, las 3 características primordiales son:

- Múltiple Entrada Múltiple Salida (MIMO, Multiple Input Multiple Output)

- Agregación de paquetes
- Channel Bonding (canales de 40 MHz)

3.5.4.1 TECNOLOGÍA DE MÚLTIPLE ENTRADA MÚLTIPLE SALIDA, MIMO

Los equipos que operan con tecnología 802.11a/b/g se comunican a través de una sola secuencia de datos usando una sola antena, en cambio los equipos que operan con 802.11n transmiten 2 o mas señales cuando se tienen equipos operando con 802.11n y emplean varias antenas para la recepción y avanzados procesos para recuperar la información de las múltiples señales transmitidas. MIMO permite usar el Multiplexaje espacial para transmitir diferentes bits de un mensaje a través de diferentes antenas, permitiendo un mejor rendimiento y una red mas robusta, es decir se tienen múltiples transmisiones por parte de punto de acceso y se tienen múltiples recepciones por parte del equipo del usuario, considerando que las tecnologías inalámbricas anteriores tenían problemas relativos a las reflexiones de señal, MIMO utiliza estas reflexiones para aumentar el alcance y reducir los "puntos muertos" en el área de cobertura inalámbrica

3.5.4.2 UNIÓN DE CANALES (CHANNEL BONDING)

Los estándares 802.11a/b/g usan canales de 20 MHz de ancho, pero 802.11n usa una técnica que denomina Unión de canales (Channel Bonding) con la cual une dos canales adyacentes de 20 Mhz para formar un solo canal de 40 Mhz y así ampliar el ancho de banda que utiliza para la transmisión. Esta técnica es más efectiva si se emplea en las frecuencias de 5 GHz, donde se tienen mas canales disponibles sin traslaparse, ya que el 2.4 GHZ solo se tienen 3 canales adyacentes que no se traslapan. Pero cuando 802.11n convive con 802.11a/b/g transmite en canales de 20 MHz.

3.5.4.3 AGREGACIÓN DE PAQUETES

802.11n incrementa la eficiencia agregando múltiples paquetes de datos en una sola trama transmitida, de esta forma pueden enviar múltiples paquetes de datos con un encabezado fijo. La agregación de paquetes es beneficiosa para ciertas aplicaciones pero cuando se trata de aplicaciones en tiempo real como la voz no es conveniente la agregación de paquetes debido a que sus paquetes se intercalan a intervalos regulares y si combinamos paquetes en una carga de datos muy larga se puede producir un retardo.



En la siguiente tabla se resumen las características de cada tecnología.

	802.11b	802.11g	802.11a
Características técnicas			
Espectro	2.4 GHz	2.4 GHz	5 GHz
Velocidad máx.	11 Mbps	54 Mbps	54 Mbps
Técnica de modulación	DSSS	DSSS/OFDM	OFDM
Canales disponibles (no traslapados)	3	3	23
Usuarios por celda, aprox.	25	20 (se reduce el rendimiento cuando se tienen cliente 802.11b)	15

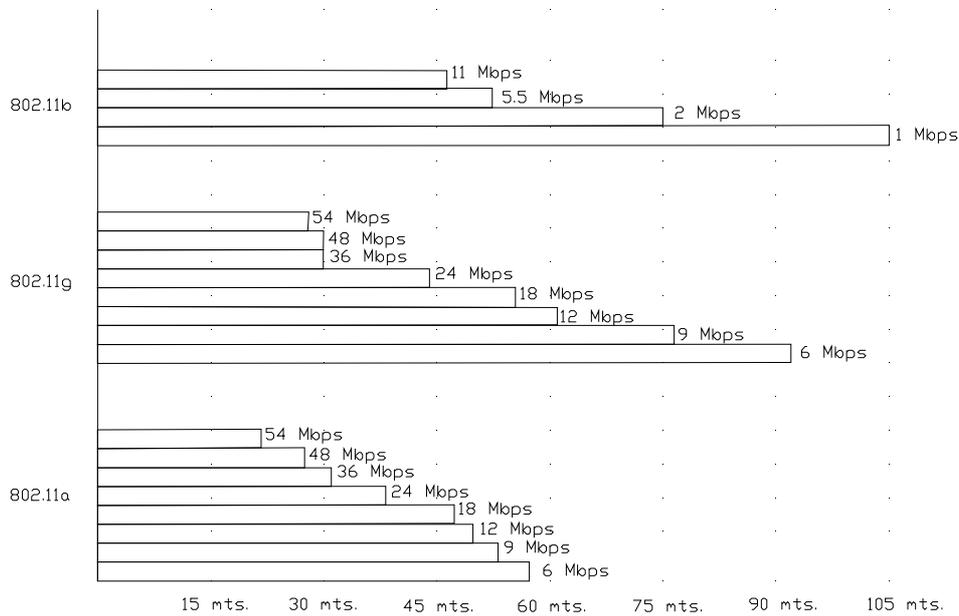


Tabla 3.2 Características de tecnología Inalámbrica.

CAPITULO 4. EQUIPOS DE ACCESO INALÁMBRICO A LA RED

4.1 INTRODUCCIÓN

Para la implementación de una red local inalámbrica se debe de contar con dos tipos de dispositivos, los primeros son propios de la infraestructura de la red, tales como Access Point, routers inalámbricos, Modems, etc.. Estos proveen el acceso inalámbrico a la red al cliente y la propagación de sus datos hacia otros usuarios. En el mercado hay una gran variedad de marcas, modelos y costos que satisfacen las necesidades de acuerdo al diseño de la red que el cliente propone. Por otro lado, el usuario debe de contar en su estación de trabajo con un dispositivo que permita la conexión de su computadora u organizador personal hacia el punto de acceso a la red, estas pueden ser tarjetas de tipo PCMCIA, tarjetas internas, dispositivos con conexiones USB, etc., de igual manera, existen varias marcas y modelos de acuerdo a las necesidades del cliente.

El presente capítulo pretende exponer los diferentes tipos de equipos de acceso inalámbrico tanto de infraestructura para la implementación de la red, como personales que se emplean en las estaciones de trabajo, no se profundiza en detalles ni características de los dispositivos, ya que son muy variadas y depende del fabricante, cabe hacer mención que estos dispositivos cumplen con los estándares de comunicaciones tales como las frecuencias de operación y las tasas de transferencia, entre otras, establecidas por la FCC, Wi-Fi y 802.11.

4.2 EQUIPOS DE ACCESO INALÁMBRICO (INFRAESTRUCTURA DE LA RED)

4.2.1 PUNTO DE ACCESO, AP (ACCESS POINT)

Un Punto de Acceso (AP, Access Point) es un dispositivo que recibe y transmite datos entre los usuarios, siendo el punto central, es decir que un cliente tiene que pasar sus datos por el AP para dirigirse a otro cliente; o bien, funciona como un punto de conexión entre una red cableada y una red inalámbrica, siendo el equivalente inalámbrico de un Hub o un Switch de Ethernet, no es capaz de otorgar enrutamiento a los clientes, es por eso que se debe de conectar a un router. En sí, como su nombre lo indica, es un Punto de Acceso a la red. La cobertura de un AP va desde unos cuantos metros hasta los 250 metros en promedio, esto depende de la tasa de transferencia a la que se configure.

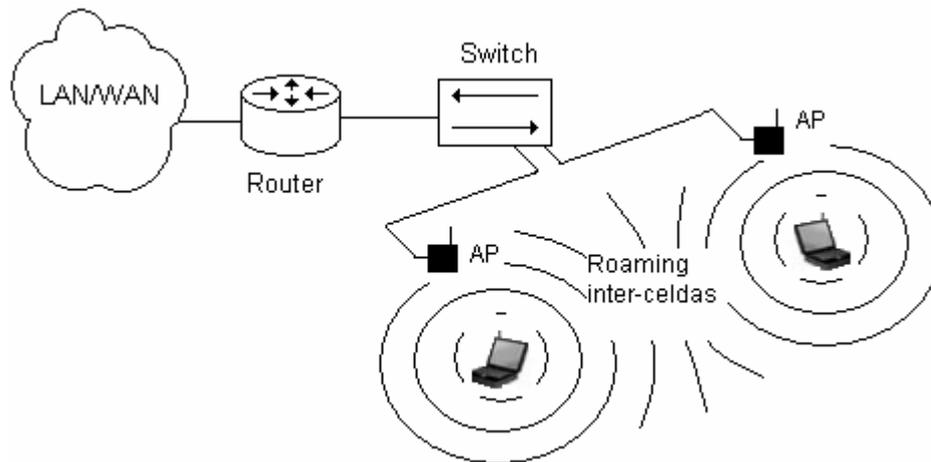


Fig. 4.1 Arquitectura de Access Point.

Existe una gran variedad de modelos y marcas, cada una con características y funciones propias, a continuación se ilustran algunos modelos:



Fig. 4.2 Access Point Cisco Aironet 1230
(Imagen obtenida de la página de Internet www.cisco.com)



Fig. 4.3 Access Point Cisco Aironet 1100
(Imagen obtenida de la página de Internet www.cisco.com)

4.2.2 ROUTER INALÁMBRICO

Un router inalámbrico es un dispositivo dentro de una red local inalámbrica que determina el siguiente punto de la red hacia el cual los datos deben ser enviados. Este trabaja de la misma manera que un router convencional usado en redes cableada, pero con la ventaja de que provee movilidad a los usuarios, y con la ventaja de que cuenta ya con un Access Point integrado. Tiene la capacidad de crear tablas de enrutamiento, manejar diferentes protocolos de enrutamiento, asignar direccionamiento dinámico o fijo, en su mayoría cuentan con puertos Ethernet para conectarlos a la red local. Hoy en día los routers inalámbricos brindan un ancho de banda mayor permitiendo la conexión de más clientes a la red. Los más actuales operan bajo el estándar 802.11g, ofreciendo tasa de transferencia de 54 Mbps. Debido a su versatilidad de contar con puertos Ethernet y un acceso inalámbrico, se puede usar para tener dos tipos de redes con un mismo dispositivo, una cableada y una inalámbrica, también se puede tener una conexión hacia una red LAN/WAN o proveer enrutamiento a los clientes a través del servicio Telefónico/DSL o Internet por Cable, sin embargo para este último caso se debe de contar con un MODEM DSL o un Cable MODEM.

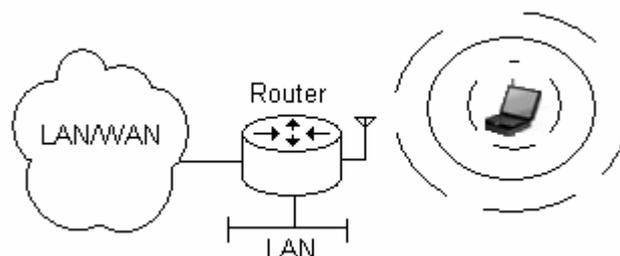


Fig. 4.4 Arquitectura básica de un router inalámbrico.

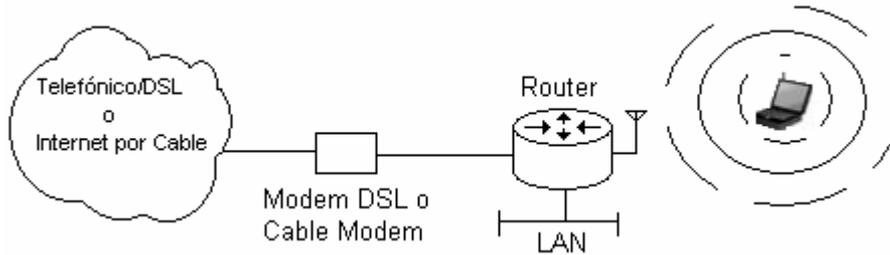


Fig. 4.5 Router inalámbrico con servicio ADSL o Cable MODEM.

Debido a la robustez de un router inalámbrico, se puede eliminar el uso del Access Point en redes pequeñas de uso residencial o en pequeñas oficinas, así disminuyendo el costo y facilitando la implementación de la red, algunos modelos se ilustran a continuación:



Fig. 4.6 Router inalámbrico Linksys.
(Imagen obtenida de la página de Internet www.linksys.com)



Fig. 4.7 Router inalámbrico US Robotics.
(Imagen obtenida de la página de Internet www.usr.com)

4.2.3 MODEM/ROUTER INALÁMBRICO, SERVICIO ADSL

Un MODEM/Router inalámbrico es un dispositivo que provee el acceso a Internet a varios usuarios de la red local de forma simultánea usando una sola cuenta de usuario y una única línea ADSL. Tiene la capacidad de proveer enrutamiento, asignación de direccionamiento dinámico o fijo a los clientes, protección Firewall, cuenta con puertos Ethernet para crear una red local, al mismo tiempo que tiene integrado un Access Point para crear una red local inalámbrica. El alcance inalámbrico va desde unos cuantos metros hasta los 100 metros en línea de vista.

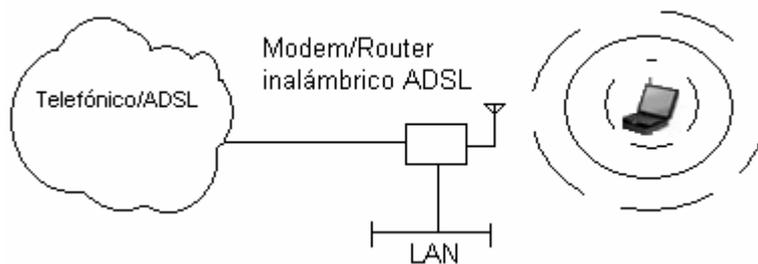


Fig. 4.8 Arquitectura básica de un MODEM / Router.

El servicio de Internet ADSL que se brinda por la línea telefónica es casi siempre de uso residencial o para pequeños negocios, empleándose MODEM/routers ADSL que no tienen una cobertura tan amplia como los dispositivos antes mencionados, sin embargo funcionan adecuadamente para redes pequeñas además de ser versátiles igual que los routers inalámbricos.



Fig. 4.9 Modem/Router Inalámbrico 2Wire 1800hg.
(Imagen obtenida de la página de Internet www.2wire.com)

4.3 DISPOSITIVOS DE ACCESO INALÁMBRICO A LA RED (CLIENTES)

4.3.1 TARJETAS INALÁMBRICAS PCMCIA

Estos dispositivos generalmente se usan en las computadoras portátiles ya que en su mayoría éstas son las que cuentan con ranuras de tipo PCMCIA (*Personal Computer Memory Card International Association*), se pueden encontrar en modelos de 11 y 54 Mbps. De igual manera que todos los dispositivos inalámbricos mencionados, trabajan bajo los estándares 802.11 b y g. Cuentan con un software que al instalarse en la estación de trabajo sirve como controlador y para configurar la red, encriptación, dirección IP, etc.



Fig. 4.10 Tarjeta inalámbrica PCMCIA Linksys.
(Imagen obtenida de la página de Internet www.linksys.com)

4.3.2 TARJETAS INALÁMBRICAS PCI

Estas tarjetas son de tipo PCI (*Peripheral Component Interconnect*), se usan principalmente en computadoras de tipo PC y se instalan dentro del CPU, dejando salir una pequeña antena que se usa para conectarse a la red. También cuentan con un software que al instalarse en la estación de trabajo sirve como controlador y para configurar la red, encriptación, dirección IP, etc. Operan bajo los estándares 802.11 b y g. También se pueden encontrar para redes de 11 y 54 Mbps.



Fig. 4.11 Tarjeta inalámbrica PCI Linksys.
(Imagen obtenida de la página de Internet www.linksys.com)

4.3.3 ADAPTADORES USB

Son una variante de adaptadores portátiles de conexión inalámbrica, hay dos tipos, uno se parece mucho a una memoria USB, y otro es un dispositivo con una antena que se conecta mediante un cable a la PC. Se pueden usar tanto en una PC como en una computadora portátil siempre y cuando cuenten con conectores de tipos USB (*Universal Serial Bus*), de igual manera, cuentan con un software y se encuentran para 11 y 54 Mbps.



Fig. 4.12 Adaptador inalámbrico USB SMC.
(Imagen obtenida de la página de Internet www.smc.com)



Fig. 4.13 Adaptador inalámbrico USB Belkin.
(Imagen obtenida de la página de Internet www.belkin.com)

4.3.4 TARJETAS PARA ORGANIZADORES PERSONALES

Estas son muy pequeñas, se insertan en las ranuras para memorias SD (*Secure Digital*) de los organizadores personales, utilizan la tecnología Wi-Fi bajo el estándar 802.11b, con ellas se puede tener acceso a la red inalámbrica local o a cualquier sitio que cuente con Internet inalámbrico público.



Fig. 4.14 Tarjeta Wi-Fi Palm.
(Imagen obtenida de la página de Internet www.palm.com)

CAPITULO 5. ARQUITECTURA FUNCIONAL.

5.1 SOLUCION DE TECNOLOGÍA Y PRODUCTOS

5.1.1 TECNOLOGÍA APLICADA

La tecnología que ha cobrado importancia para el desarrollo de la red inalámbrica es la 802.11b y g del IEEE. Esta tecnología cumple los requisitos demandados por los clientes, tales como flexibilidad, dimensionamiento, prestaciones, seguridad y costos. Las otras tecnologías estudiadas han sido rechazadas por los siguientes motivos:

- a) **Bluetooth:** Los motivos principales para rechazar esta tecnología fueron la escasa velocidad (1Mbps) y su corto alcance (no mayor a 10m). A favor de esta tecnología cabe citar la amplia acogida en el mercado (Bluetooth agrupa a 1200 miembros en su SIG) y el bajo costo en relación a las demás alternativas. Además se están desarrollando puntos de acceso que permitirán ofrecer coberturas de hasta 100m y se está trabajando para que la versión 2 de este estándar soporte transmisiones a 4 Mbps. Actualmente se usan en dispositivos personales como PDA, celulares y computadoras portátiles implementado redes de tipo PAN.
- b) **HomeRF:** Los motivos principales para la desestimación de esta tecnología fueron su escasa velocidad (2 Mbps) y el enfoque de dirigir los productos al hogar.
- c) **HiperLAN 2:** Esta tecnología es la más avanzada actualmente (junto con 802.11), disponiendo de las velocidades de transmisión más altas (54 Mbps), equiparándose a las redes cableadas convencionales. A pesar de ello, todavía es una tecnología muy reciente y solo algunas pocas compañías disponen de productos para el mercado. Los costos también son algo elevados, aunque se espera que a medida que se vaya incorporando al mercado estos bajen.

Las características ofrecidas en 802.11 permiten, no solo cumplir con las expectativas del cliente, sino disponer de prestaciones adicionales. A continuación vinculamos las necesidades del cliente con las características disponibles en 802.11 (b y g).

- a) Velocidad de transmisión equiparable a redes convencionales de cable, que permitirá en la zona de almacenaje actualizar de manera rápida los datos de inventario, y en las oficinas y sala de juntas disponer de los datos actualizados en cualquier momento, siendo las velocidades de 11 Mbps para 802.11.b y de 54 Mbps para 802.11g.
- b) Rango de cobertura de 100m que proporcionará conectividad a la red en cualquier punto del edificio.
- c) Topología de estrella que permitirá la administración de la red desde un único punto (al igual que los hubs en las redes cableadas), además de minimizar el impacto derivado del fallo de un equipo de un usuario final.
- d) Roaming que permitirá estar continuamente conectado a la red en cualquier lugar del interior del edificio o del campus.
- e) Seguridad en las comunicaciones, maximizando la confidencialidad de los datos de la compañía que viajan por la red.
- f) Interoperabilidad con redes Ethernet, que permitirá el acceso a los recursos de la red Fast Ethernet ya existentes, sin suponer un costo adicional en equipamiento de interconexión.
- g) Bajo consumo, que concede mayor autonomía a los equipos portátiles.
- h) Soporte de voz y vídeo, pese a no ser una necesidad del cliente, éste puede verse beneficiado por una instalación de este tipo.

5.1.2 ELECCIÓN DE PRODUCTOS

Se han encontrado 4 posibles soluciones para la implementación de un punto de acceso a la red inalámbrica: 3Com® Wireless 8760, Linksys Wireless-G, ORINOCO AP-4000 y Cisco Aironet 1230AG. La siguiente tabla, resume sus características.

INGENIERIA EN TELECOMUNICACIONES



UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

	3Com® Wireless 8760 Dual-Radio 11a/b/g Access Point	Linksys Wireless-G Access Point	ORINOCO AP-4000	Cisco Aironet 1230AG Series 802.11A/B/G Access Point
Distribuidor	3COM	Linksys	ORINOCO	CISCO
Especificación	IEEE 802.11b/g	IEEE 802.11b/g	IEEE 802.11a/b/g	IEEE 802.11a/b/g
Certificación Wi-Fi	Sí	Sí	Sí	Sí
Soluciones disponibles				
Punto de Acceso	3CRWE876075	WAP54GP	8670-US	AIR-AP1232AG
Adaptador PC Card	3CRXJK10075	WPC54G	8470-FC	AIR-PCM352
Adaptador PCI	3CRDAG675B	WMP54G	8482-FC	AIR-PCI352
Características de Radio				
Banda de Frecuencias	ISM	ISM	ISM	ISM
Tipo de Señal	DSSS y OFDM	DSSS y OFDM	DSSS y OFDM	DSSS y OFDM
Tasa de transferencia				
Ajuste dinámico	Sí	Sí	Sí	Sí
11 Mbps	Sí	Sí	Sí	Sí
5.5 Mbps	Sí	Sí	Sí	Sí
2 Mbps	Sí	Sí	Sí	Sí
1 Mbps	Sí	Sí	Sí	Sí
Modo de transmisión	Half duplex	Half duplex	Half duplex	Half duplex
Acceso al medio.	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA
Modulación				
CCK a 5.5 y 11 Mbps	Sí	Sí	Sí	Sí
DQPSK a 2 Mbps	Sí	Sí	Sí	Sí
DBPSK a 1 Mbps	Sí	Sí	Sí	Sí
Topologías				
Punto a punto	Sí	Sí	Sí	Sí
Punto de acceso	Sí	Sí	Sí	Sí
Encriptación				
WEP (Wired Equivalent Privacy) (40-128 bits)	Sí	Sí	Sí	Sí
WPA/WPA2 (Wi-Fi Protected Access) (128 bits)	Sí	Sí	Sí	Sí
Software				
Punto de acceso	Sí	Sí	Sí	Sí
Cliente	Sí	Sí	Sí	Sí
Reglamentaciones				
FCC 15 Subpart C	Sí	Sí	Sí	Sí
NOM-019- SCFI	Sí	Sí	Sí	Sí
EN/IEC 60950-1	Sí	Sí	Sí	Sí
Sistemas Operativos				
Windows XP	Sí	Sí	Sí	Sí
Windows 2000	Sí	Sí	Sí	Sí
Características del punto de acceso				
Interfaz de red	10BASET/100BASE-TX	10BASET/100BASE-E-TX	10BASET/100BASE-TX	10BASET/100BASE-TX



Nº máx. de clientes	128	64	64	64
Diversidad de antena	Sí	Sí	Sí	Sí
Alimentación a través de línea Ethernet	Sí	Sí	Opcional	Opcional
Precio				
Punto de acceso	\$4,003.35M.N.	\$2,627.00M.N.	US \$426.52	US \$ 597.07
Adaptador PC Card	\$565.50M.N.	\$676.94M.N.	US\$126.20	US \$197.91
Adaptador PCI	\$694.30M.N.	\$676.94M.N.	US\$151.10	US \$232.05

Tabla 5.1 Características de Productos

Finalmente, el dispositivo 3Com® Wireless 8760, parece tener ventajas sobre los demás de acuerdo a las siguientes características fundamentales:

- a) **Costo medio:** Superior a Linksys pero inferior a Orinoco y Cisco.
- b) **Disponibilidad de productos:** Puntos de acceso, tarjetas para portátiles, tarjetas PCI y dispositivos USB para equipos de escritorio. Además 3COM tiene presencia en Latinoamérica.
- c) **Prestaciones:** Un mayor número de usuarios respecto a las otras marcas.
- d) **Experiencia de la compañía:** 3COM como empresa líder en equipamiento de red.

A continuación vinculamos las características disponibles en los productos 3Com® Wireless 8760 con las ventajas proporcionadas al cliente.

- a) **Balanceo de carga:** permitiendo maximizar el ancho de banda en presencia de dos o más puntos de acceso en una planta el edificio.
- b) **PowerBASE-T:** ofreciendo una instalación muy sencilla del punto de acceso cuya alimentación será proporcionada por el cable de red Ethernet, sin tener que disponer de una toma de AC.
- c) **Un mayor número de usuarios:** superior a las necesidades del cliente incluidas las previsiones de futuro.
- d) **Listas de control de acceso:** que permitirá al administrador especificar los permisos de acceso a la red inalámbrica en función de las direcciones MAC de los equipos inalámbricos.
- e) **DHCP:** que proporcionará una dirección IP válida de la red local a cualquier usuario que se haya autenticado contra el punto de acceso.

- f) **Soporte para IPSec:** que ofrece la posibilidad de aumentar la seguridad WEP (Wireless Equivalent Privacy) proporcionada por el estándar 802.11b.
- g) **Certificado Wi-Fi:** que garantiza la interoperabilidad con equipos inalámbricos de otras compañías que estén bajo el estándar 802.11b.
- h) **Software para sistemas operativos Windows:** que son los que actualmente emplea la empresa, con la ventaja de que al ser dispositivos PnP, su instalación es muy sencilla.

5.2 CÁLCULOS DEL DISEÑO DE LA RED

5.2.1 BASES DEL DISEÑO

Los parámetros básicos para el diseño de la red inalámbrica son:

- Características del sitio
- Número de usuarios con acceso inalámbrico.
- Prestaciones necesarias de la red.
- Integración e interoperabilidad con otras redes.

A continuación entraremos en detalle en cada una de ellos para determinar las características de la red a diseñar.

5.2.2 CARACTERÍSTICAS DEL SITIO

El edificio que albergará la red inalámbrica consta de un piso, con muros de un espesor estándar de 12 cm. Este tipo de edificación se encuadra dentro del entorno estándar de oficina, en el que se basan los fabricantes de productos inalámbricos a la hora de realizar los cálculos de cobertura de éstos.

Las antenas de los productos 3Com® Wireless 8760 vienen optimizadas para realizar comunicaciones a lo largo de un plano, es decir, si situamos un punto de acceso en una planta del edificio, éste dará cobertura a los equipos inalámbricos de dicha planta.

En la siguiente tabla, se resumen los radios de cobertura de los productos Airconnect de 3COM, en función del entorno donde se ubiquen.

Entorno	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Entorno abierto	185 m	300 m	420 m	640 m
Entorno semi-abierto	55 m	80 m	100 m	115 m
Entorno cerrado	35 m	48 m	55 m	80 m

Tabla 5.2 Cobertura de productos Airconnect de 3COM.

Enmarcaremos la planta baja del edificio dentro del grupo de “entorno cerrado” y la planta inferior en el grupo de “entorno semi-abierto”. Si en ambos casos queremos disponer de las tasas máximas de velocidad (11 Mbps), en la planta baja la distancia no debe superar los 55m. Dadas las características de tamaño de cada planta (36.6m x 15.9m), la ubicación del punto de acceso en la zona central proporcionará cobertura a un equipo inalámbrico localizado en cualquier punto de la planta, tal y como se ve en el siguiente esquema.

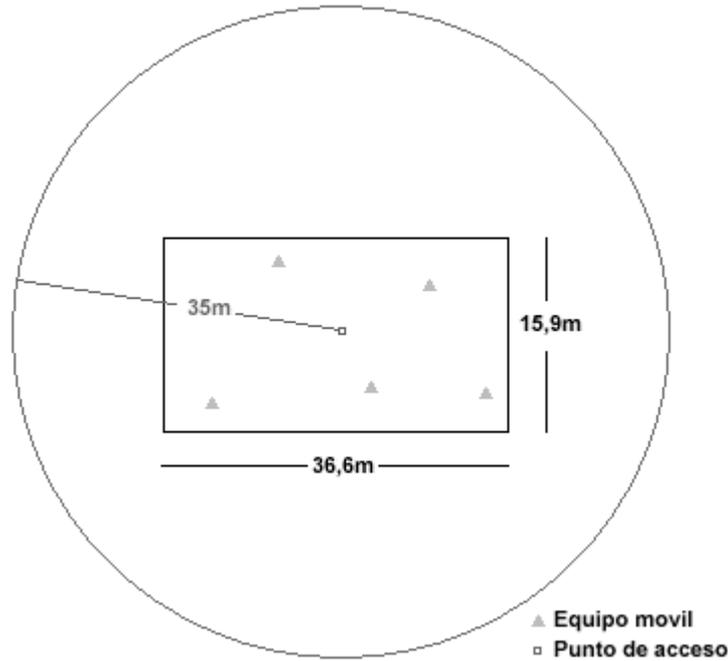


Fig. 5.1 Cobertura a 11Mbps en entorno cerrado.

5.2.3 NÚMERO DE USUARIOS CON ACCESO INALÁMBRICO

En los requerimientos del cliente, se especifica un número de usuarios con acceso inalámbrico a la red, divididos por zonas y con una previsión de crecimiento a medio plazo. En la siguiente tabla se resume estas especificaciones.

Planta baja	
Cobertura	Zona de gestión y dirección. Extensión a la zona de administración a medio plazo.
Equipos inalámbricos	25 (11 equipos de sobremesa + 14 equipos portátiles)
Previsión de crecimiento	80% (+ 20) (9 equipos de sobremesa + 11 equipos portátiles)
Total dimensionamiento	45 (20 equipos de sobremesa + 25 equipos portátiles)

Tabla 5.3 Usuarios con acceso inalámbrico



Para la planta baja el número total de usuarios inalámbricos a medio plazo es de 45, con cobertura para la zona de gestión y dirección inicialmente y una posterior extensión a la zona de administración. Atendiendo a los rangos de cobertura del punto de acceso, incluida la zona de administración. En cuanto al número de usuarios, podemos indicar que un solo punto de acceso podría dar conectividad a todos, dado que la capacidad máxima de éste es de 64 usuarios.

5.2.4 PRESTACIONES NECESARIAS DE LA RED

Cada punto de acceso dispone de un ancho de banda de 11Mbps, pudiendo colocar hasta 3 puntos de acceso con sendos canales que no se solapen, para obtener hasta un total de 33Mbps.

La tecnología de acceso al medio empleada por los puntos de acceso es CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), que atendiendo a datos empíricos suelen ofrecer un rendimiento de un 40-50% sobre el total del ancho de banda. En nuestro caso el ancho de banda en la práctica será de unos 4.4 - 5.5Mbps.

Según los datos del fabricante, la capacidad máxima de usuarios soportados por cada punto de acceso, vienen determinados por el uso que hagan éstos de la red:

- a) 50 usuarios que se encuentran ociosos a menudo y que solo acceden a su correo electrónico.
- b) 25 usuarios que hacen uso intensivo del correo electrónico, páginas web y transmiten/reciben ficheros de tamaño medio.
- c) 10-20 usuarios que hacen un uso constante de la red y transmiten/reciben ficheros de gran tamaño.

De los 45 usuarios inalámbricos previstos para la planta baja, la mayor parte de ellos queda encuadrada en el grupo b), por lo que un único punto de acceso no sería suficiente. Con dos puntos de acceso empleando sendos canales no solapados, se daría conectividad a un total de 50 usuarios tipo b), satisfaciendo los requisitos del cliente.

5.2.5 INTEGRACIÓN E INTEROPERABILIDAD CON OTRAS REDES

La planta baja dispone actualmente de una red cableada Fast Ethernet (100Mbps). Los concentradores o hubs se encuentran situados en las salas de máquinas de cada piso y existe una troncal que comunica ambos pisos. Al conectar los puntos de acceso de cada piso con los hubs correspondientes, se podrán compartir los recursos existentes de la red cableada: servidores de fichero, correo electrónico, servidor web, impresoras, etc.



Gracias a la interfaz Ethernet (10Mbps) disponible en puntos de acceso 3COM, la interconexión entre la red inalámbrica y la red cableada es muy sencilla.

Además el producto viene provisto con un módulo PowerBASE-T para alimentar el punto de acceso a través de la línea 10Base-T con tensión de corriente directa, por lo que se elimina la necesidad de disponer de una toma de AC cerca de su ubicación. La alimentación a través del cable Ethernet elimina el riesgo de posibles interferencias con la red de alterna.

CAPITULO 6

EL FUTURO DE LAS REDES INALÁMBRICAS

6.1 INTRODUCCIÓN

Debido a la introducción masiva de Wi-Fi en nuestras vidas, se están detectando deficiencias que restringen al usuario, Wi-Fi esta diseñado para Redes de Área Local, como alternativa del cableado estructurado en aquellos edificios donde no se puede implementar una red Ethernet tradicional, cabe destacar que presenta beneficios como movilidad del usuario y fácil implementación, pero aun así se limita a un área determinada y en ocasiones se tienen debilidades en la señal de acuerdo a los tipos de materiales de la obra civil donde se encuentra la red.

Hoy en día esta naciendo una nuevo estándar, el IEEE 802.16, conocido como WIMAX (Worldwide Interoperability for Microwave Access). De acuerdo a sus características, WIMAX viene para complementar la funcionalidad de Wi-Fi, ampliando las redes inalámbricas locales hacia una forma metropolitana, sirviendo como extensión de las propias redes locales de Wi-Fi; o en su caso puede sustituir por completo a las redes de tipo local teniendo una cobertura alrededor de los 50 Km. de diámetro, ofreciendo en un futuro posibles productos mas económicos y exponiendo un panorama muy atractivo para los ISP's y la industria, llegando a una extinción total de Wi-Fi para Internet publico. Cabe señalar que el estándar 802.11 difícilmente dejara de operar, esto se debe a que no únicamente se emplea en México para sitios de acceso a Internet en aeropuertos o restaurantes, sino también esta teniendo un gran auge en las rede locales en los hogares y oficinas, para lo cual WIMAX no esta diseñado.

6.2 CARACTERÍSTICAS DE WIMAX

WIMAX (Worldwide Interoperability for Microwave Access) es el nombre comercial de un grupo de tecnologías desarrolladas para operar bajo el estándar IEEE 802.16, en el cual se describe una Red Metropolitana de Banda Ancha de tipo inalámbrica, permitiendo la conexión de varios puntos sin necesidad de línea de vista. WIMAX pretende complementar la tecnología Wi-Fi proporcionando tasas de transferencia de hasta 100 Mbps y permitiendo tener cobertura de ciudades o zonas rurales donde el acceso por cable se ve limitado, brindando cobertura de aproximadamente 50 Km. desde la estación base, se presenta como alternativa y/o extensión a otras tecnologías de banda ancha usadas en la última milla, tales como ADSL, cablemodem y satelital, ofrece servicios a empresas y usuarios residenciales de Acceso a Internet, telefonía y conectividad con grandes anchos de banda. WIMAX destaca por su capacidad como tecnología portadora, ya que puede transportar IP, TDM, T1/E1, ATM, Frame Relay y voz.

A pesar de que este concepto tiene poco de haberse escuchado, el estándar 802.16 tiene sus orígenes a finales de la década de 1990, surgiendo el 802.16, el cual operaba en la banda de frecuencias de 10 – 66 GHz, posteriormente nació en el 2003 el 802.16a que opera en las bandas de frecuencias de 2 – 11 GHz. Sin embargo el constante desarrollo de este estándar y la lucha por incrementar su mercado, ha llevado al olvido al 802.16a, creándose en el 2004 el 802.16 – 2004, conocido también como 802.16RevD o simplemente 802.16d, este estándar está orientado a redes fijas inalámbricas. Por otro lado WIMAX también cuenta con una versión móvil, IEEE 802.16e, pensada para implementarse en vehículos o simplemente para la conexión con computadoras portátiles u organizadores personales.

6.3 WIMAX FIJO Y WIMAX MÓVIL

El estándar 802.16 – 2004 de la IEEE está diseñado para el acceso fijo, básicamente este concepto se define como fijo debido a que el usuario final tiene una antena en su lugar de trabajo, ya sea en el exterior del edificio o en el interior de la habitación, por supuesto no tan robusta como las antenas usadas en el exterior. 802.16 – 2004. WIMAX de acceso fijo opera en las bandas de frecuencias de 2.5 GHz licenciada, y 3.5 GHz y 5.8 GHz de uso libre. Puede operar bajo líneas de vista (LOS) o sin líneas de vista (NLOS), soporta el tipo de modulación multi-portadora OFDM con 256 portadoras. Con WIMAX 802.16 – 2004 se pueden tener conexiones Punto – Punto o conexiones de tipo Punto – Multipunto. Como se ha mencionado, WIMAX 802.16 – 2004 se puede considerar como un complemento de 802.11, podemos tener una red Wi-Fi en nuestro hogar u oficina, y para tener conexión a Internet se puede tener un servicio WIMAX fijo, en éste escenario se observa que las redes pueden convivir sin ver afectada alguna de ellas por la sustitución de servicios.

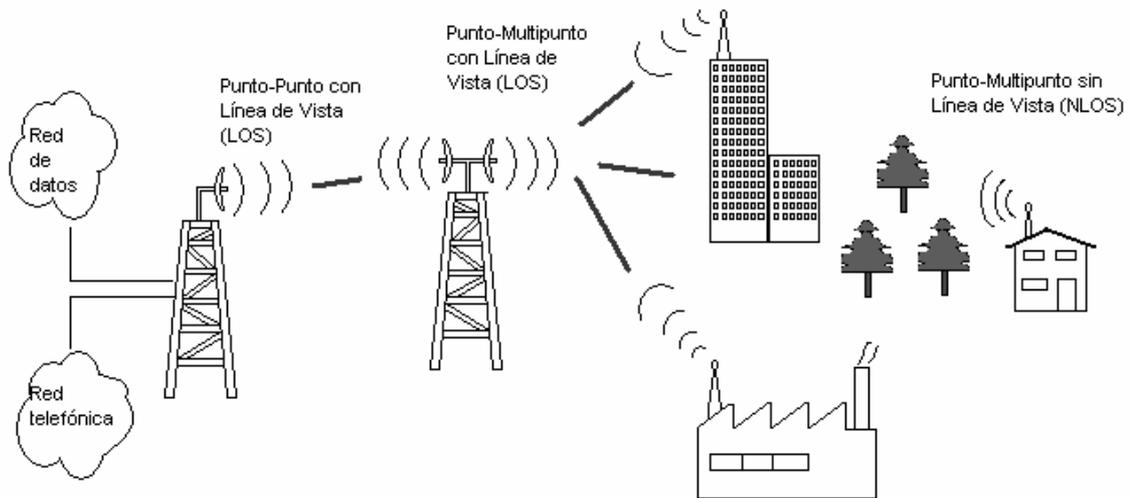


Fig. 6.1 Conexión Punto-Punto y Punto-Multipunto con WIMAX fijo.

Una variante del estándar 802.16 es 802.16e, el cual ofrece una característica clave de la que carece el 802.16 – 2004: la movilidad del usuario, ésta solución requiere de una plataforma de hardware y software distinta, ya que no es compatible con 802.16 – 2004. La idea de 802.16e es implementar una Red Metropolitana Inalámbrica destinada a usuarios con movimiento, es decir, el usuario puede tener conexión a la red desde su automóvil, o tener acceso a Internet en cualquier jardín, parque, o en la calle de toda la zona de cobertura. 802.16e usa Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), brindando la ventaja sobre OFDM de que una sola estación cliente del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión, o los múltiples clientes podrían transmitir simultáneamente usando cada uno una porción del número total de subcanales. Podemos considerar que en futuro 802.16e desplace por completo los Hot Spots, teniendo como ventaja sobre estos el hecho de que el cliente no se verá obligado a entrar a un restaurante o, a pesar de que se trata de una tecnología móvil, el usuario tiene que permanecer dentro de la cobertura del Hot Spot.

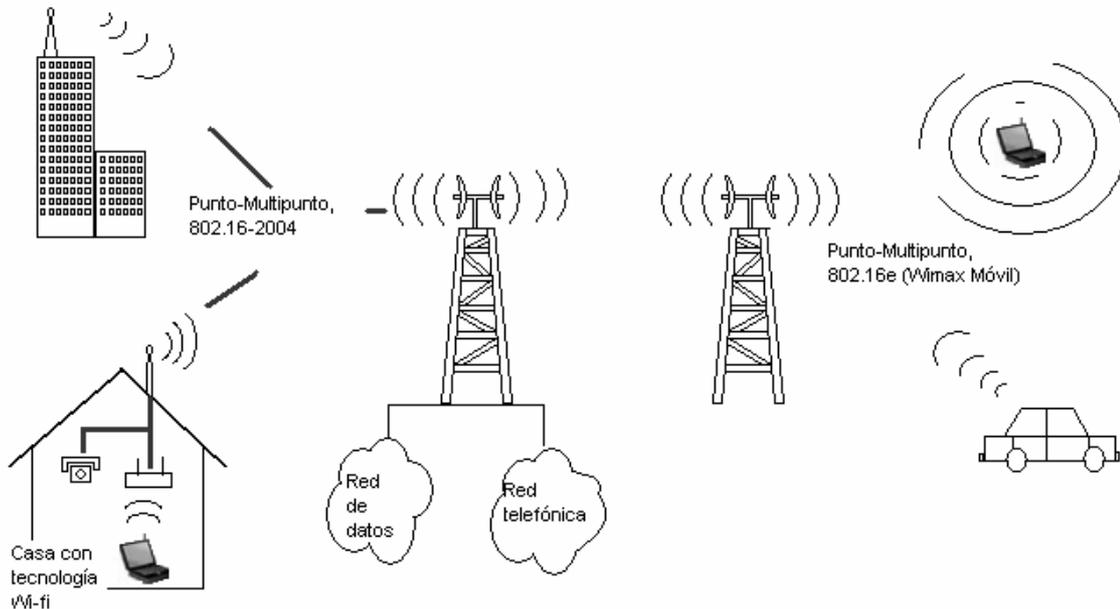


Fig. 6.2 Panorama de WIMAX fijo y WIMAX móvil.

6.4 COMPARACIÓN DE WIMAX FIJO Y WIMAX MÓVIL

WIMAX Fijo y WIMAX Móvil tienen diferentes requerimientos para su implementación, de acuerdo a las distintas aplicaciones de esos dos segmentos del mercado: las redes fijas y las redes móviles. Las redes fijas se pueden ver sustancialmente beneficiadas de acuerdo a las características de los productos implementados en las redes WIMAX, tales como:

- Modulación menos compleja: OFDM es una técnica de modulación simple que es bastante adecuada en ambientes donde no se requiere movimiento.
- Bandas licenciadas y no licenciadas: los servicios móviles requieren de un ancho de banda licenciado para proveer la cobertura en ciertas áreas. De lo contrario, para los servicios fijos, generalmente se usan exitosamente anchos de banda no licenciados en áreas donde los niveles de interferencia son aceptables.
- Mercado amplio: se pueden encontrar más fácilmente dispositivos para redes fijas.

De lo contrario, muchas personas se orientan más hacia 802.16e de acuerdo a las siguientes razones:

- Soporte de movimiento: 802.16e está diseñado para que el cliente no este fijo en un solo lugar.



- Gran flexibilidad en la administración del espectro de frecuencias: la subcanalización permite alojar en una red tantos usuarios como requieran el servicio, resultando en un mejor uso del espectro destinado, permitiendo una mejor cobertura en el interior, y en su mejor caso reduciendo el costo de la implementación
- Variedad de dispositivos: mientras que en un panorama fijo, solo se tienen equipos de escritorio o computadoras personales con tarjetas PCMCIA, en el caso de 802.16e se pueden tener incluso organizadores personales, teléfonos celulares. La variedad de dispositivos permite al ISP extender sus servicios a nuevos mercados.

6.5 EL MERCADO DE WIMAX

Se ha estado haciendo común en gran parte del planeta el uso de la tecnología WIMAX, ya son bastantes los países que lo han adoptado. En Europa los operadores que disponen de licencias para la implementación de WIMAX son: Iberbanda, France Telecom, Neo-Sky y Banda Ancha (antes Aló 2000), sin embargo el primero de ellos fue el pionero en todo el continente, que desde el año 2004, gracias a su trabajo en la implantación de una de las principales redes con una tecnología que podría denominarse pre-Wimax permite hoy en día una cobertura del 25% del territorio nacional de España. La evolución de WIMAX en España se fue dando paulatinamente, comenzando con 802.16-2004, esperando que a inicios del 2008 ya pueda dar servicio móvil. Hoy en día, brindado hoy en día servicios de acceso a Internet de alta velocidad, telefonía, transmisión de datos y servicios de valor añadido en red. Como otro ejemplo del uso de WIMAX, entre tantos proyectos, Venturi, una compañía de automóviles eléctricos, en el 2005 propuso la introducción de WIMAX en uno de sus modelos, para que tenga comunicación con una estación remota y tener un mejor desempeño al registrar datos de temperatura del motor y la carga de la batería, y así poder darle mantenimiento remoto, incluso cargar la batería desde la estación base.

Latinoamérica no se queda atrás, ya son varios los países donde se adoptó esta tecnología para brindar servicios de Internet Banda Ancha, VoIP y telefonía en zonas rurales como alternativa del uso del cable de cobre. Cabe mencionar los siguientes ejemplos:

- Colombia brinda en servicio a través de la empresa Orbitel principalmente en las ciudades de Cúcuta, Cali, Cartagena, Manizales, Barranquilla, Medellín y Bogotá. Además, Telebucaramanga provee una red mixta de WiMAX-WiFi en la ciudad de Bucaramanga desde el año 2005, siendo la primera en estar en el país y Latinoamérica.
- En Paraguay, la empresa Telecel, empezó a actualizarse en la tecnología en Noviembre de 2005 dando cobertura primeramente en área metropolitana y seguidamente expandiéndose en todo el territorio.

- En Chile, Telmex inició oficialmente la comercialización de planes de Internet Banda Ancha y Telefonía, a través de la primera red inalámbrica nacional, con tecnología WiMAX. Telmex recibió la autorización que le ha permitido desarrollar la infraestructura necesaria para ofrecer esta tecnología en Chile. Desde hoy la empresa inicia su campaña para comercializar Internet Banda Ancha y Telefonía Inalámbrica en las ciudades de Santiago, Concepción, Talcahuano, Curicó, Iquique, La Serena, Coquimbo, Linares, Ovalle, Rancagua, Talca, Temuco, Valdivia, Valparaíso y Viña del Mar. Y en las próximas semanas, Telmex estará operando en Calama, Osorno, Puerto Montt, Requinoa y Punta Arenas. De esta forma, para fines del presente año la tecnología inalámbrica de Telmex estará en el 91 por ciento de las comunas de Chile.
- En México, AXTEL pertenece a WiMAX Forum y esta en vías de implementación. En la ciudad de Monterrey, Nuevo León, habrá más de 100 puntos de acceso a Internet inalámbrico de banda ancha gratuitos en parques, jardines y bibliotecas. Además, el Parque Fundidora y la Macro Plaza, ya cuentan con conexión a Internet gratis. Por otro lado, Ultrahot2go, ha puesto en marcha un servicio de este tipo entre Puebla, Veracruz y Aguascalientes. Todo ello basado en WiMAX con el estándar 802.16e.
- Ecuador: Intel ha firmado un acuerdo con la Estación Científica Charles Darwin en Galápagos, Ecuador, para implementar un proyecto piloto de interconexión WiMAX entre las diferentes islas que conforman el archipiélago.
- En República Dominicana, Tricom, empresa telefónica de capital privado, ha anunciado la implementación del servicio WiMAX exclusivamente a sus clientes de negocios en su primera etapa; la misma estará disponible en Bavaro, Haina y Santo Domingo Norte, Oeste y Distrito Nacional.

Como podemos observar, WiMAX cada día esta acaparando el mercado, en algunos países ya se ha desarrollado por completo, y en otros va paso a paso, abriendo oportunidades en el mercado, tanto para el consumidor, como para los fabricantes de equipos. No podemos descartar que en México se dé este crecimiento, y más en zonas rurales donde el tendido de cableado es muy costoso o donde no hay línea de vista para implementar radios de microondas convencionales.

CAPITULO 7 CONCLUSIONES

La presente tesis tuvo como objetivo describir la tecnología con mayor auge para el acceso inalámbrico a Internet, siendo ésta el estándar de la IEEE 802.11, claro sin dejar a un lado los conceptos básicos, la teoría general y los antecedentes de las redes cableadas. Haciendo una revisión de las tecnologías de acceso inalámbrico a una red, pudimos ir descartando aquellas que no son tan robustas, y por eso se utilizan para redes de tipo personal, como en el caso de la comunicación infrarroja, ésta no le permite tener movimiento al cliente ya que si existe un objeto entre los dos dispositivos se pierde la comunicación; o como el caso de Bluetooth, donde no podemos comunicarnos a más de 10 metros de distancia y además cuenta con una tasa de transferencia muy pobre.

Al avanzar en el contexto de la tesis nos dimos cuenta que las redes inalámbricas brindan ciertas ventajas y características interesantes sobre las redes tradicionales, sobre todo para el acceso a Internet, es más cómodo y eficiente tener un Punto de Acceso en un aeropuerto donde se pueden conectar 30 usuarios de forma inalámbrica a tener 30 nodos y llenar el recinto de cableado, facilita la implantación de la red y como se tratan de entes independientes no se ven afectados otros dispositivos en el aspecto físico, nos referimos a este punto partiendo de una computadora que teniendo problemas en su puerto Ethernet puede dañar, a través del cable, el puerto de switch de donde se conecta. Obviamente existen limitantes de cobertura y tasa de transferencia siendo un poco pobre, 54 Mbps a comparación de la Fast Ethernet de 100 Mbps, pero determinamos, que para tratarse de una red de tipo local, funciona de manera óptima.

Partiendo de que la red inalámbrica es inmediatamente después del cliente, se pretende aclarar que ésta tecnología se emplea como un punto de acceso y plantear a la red tradicional como un back bone que concentra y transmite los datos hacia otras redes inalámbricas del mismo sitio. Deducimos que la tendencia de las redes inalámbricas es crecer cada vez más en el mercado y así facilitar a los ingenieros la implementación de redes de tipo local, proponemos que usando este tipo de redes se tienen más ventajas sobre las tradicionales tomando en cuenta que lo más importante es el servicio que se le brinda al cliente. Exponiendo los equipos de acceso a la red tanto de infraestructura como los que usa el cliente, cubrimos un objetivo más, pretendiendo que esta tesis sirva como referencia al usuario de una red para determinar que tipo de equipo puede implementar en su red local.

ANEXO GLOSARIO

ASCII (American Standard Code for Information Interchange). Es un código de caracteres basado en el alfabeto latino, utiliza 7 bits para representar los caracteres, aunque inicialmente empleaba un bit adicional (bit de paridad) que se usaba para detectar errores en la transmisión.

ATM (Asynchronous Transfer Mode). Modo de transferencia asíncrona. Norma internacional en el cual se transmiten múltiples tipos de servicio (como voz, video, o datos) en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de celdas tenga lugar en el hardware, lo que reduce los retrasos en el tránsito. ATM está diseñada para aprovechar medios de transmisión de alta velocidad como E3, SONET, y T3.

Backbone. Se refiere a las principales conexiones troncales de una red. Está compuesta de un gran número de routers de gran capacidad interconectados que llevan los datos a todos los segmentos de redes que se conectan a este.

Bit. Es el acrónimo de Binary digit. (Dígito binario). Un bit es un dígito del sistema de numeración binario. El bit es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información.

BRI (Basic Rate Interface). Provee dos canales B de 128 Kbps y un canal D de 16 Kbps para el control de las comunicaciones.

Byte. Término empleado para referirse a una serie de dígitos binarios consecutivos sobre los cuales se opera como una unidad, un byte tiene 8 bits.

CPE (Customer Premises Equipment). Equipo que se encuentra bajo la administración del cliente.

CRC. Los códigos cíclicos también se llaman CRC (Códigos de Redundancia Cíclica) o códigos polinómicos. Su uso está muy extendido porque pueden implementarse en hardware con mucha facilidad y son muy potentes. Estos códigos se basan en el uso de un polinomio generador $G(X)$ de grado r , y en el principio de que n bits de datos binarios se pueden considerar como los coeficientes de un polinomio de orden $n-1$. Por ejemplo, los datos 10111 pueden tratarse como el polinomio $x^4 + x^2 + x^1 + x^0$. A estos bits de datos se le añaden r bits de redundancia de forma que el polinomio resultante sea



divisible por el polinomio generador. El receptor verificará si el polinomio recibido es divisible por $G(X)$. Si no lo es, habrá un error en la transmisión. Los bits de datos se dividen en bloques (llamados frames en inglés), y a cada bloque se le calcula r , que se denomina secuencia de comprobación de bloque (Frame Check Sequence, FCS, en inglés). Los polinomios generadores más usados son:

- **CRC-12.** $x^{12} + x^{11} + x^3 + x^2 + x + 1$. Usado para transmitir flujos de 6 bits, junto a otros 12 de redundancia. Es decir, usa bloques de 6 bits, a los que les une un FCS que genera de 12 bits.
- **CRC-16.** $x^{16} + x^{15} + x^2 + 1$. Para flujos de 8 bits, con 16 de redundancia. Usado en Estados Unidos, principalmente.
- **CRC-CCITT.** $x^{16} + x^{12} + x^5 + 1$. Para flujos de 8 bits, con 16 de redundancia. Usado en Europa, principalmente.
- **CRC-32.** $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$. Da una protección extra sobre la que dan los CRC de 16 bits, que suelen dar la suficiente. Se emplea por el comité de estándares de redes locales (IEEE-802) y en algunas aplicaciones del Departamento de Defensa de Estados Unidos.

DNS (Domain name system). Sistema de nombres de dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. (Ej. `www.render.es` pasa a `195.76.16.131`).

E1. Define el estándar PDH europeo, definido por la ITU pero que es utilizado en el resto del mundo, incluyendo México. E1 consiste de 30 canales de 64 Kbps (canales E0) y 2 canales reservados para la señalización y sincronía, la capacidad total nos da 2.048 Mbps. Pero también están disponibles E1s fraccionales.

EBCDIC (Extended Binary Coded Decimal Interchange Code). Es un código binario que representa caracteres alfanuméricos, controles y signos de puntuación. Cada carácter está compuesto por 8 bits = 1 byte, por eso EBCDIC define un total de 256 caracteres.

Frame Relay. Es un protocolo de la capa de enlace de datos que administra varios circuitos virtuales utilizando una encapsulación HDLC entre dispositivos conectados. Es especialmente adecuado para redes en forma de malla con alta conectividad entre sus nodos, Frame Relay está diseñado fundamentalmente para aplicaciones de entorno de red de área local, es decir, transporte de datos a alta velocidad, bajo retardo, transporte conjunto de diferentes tipos de tráfico y múltiples protocolos, también permite el transporte de voz.

Gateway. Es un equipo configurado para dotar a las máquinas de una red (LAN) de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP. Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Maskerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a

los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. Se podría decir que un gateway, o puerta de enlace, es un router que conecta dos redes.

Handoff. Es el proceso de transferir la llamada de una celda a otra sin que el cliente pierda señal.

Hardware. Es el conjunto físico, y materiales que componen un dispositivo, una computadora y/o elemento de red.

Impedancia Característica. La impedancia característica de una línea de transmisión es la relación de la diferencia de potencial aplicada entre la corriente que circula por el medio. La impedancia característica es independiente de la frecuencia de la tensión aplicada y de la longitud de la línea de transmisión. La impedancia característica de una línea de transmisión depende de los denominados parámetros primarios de la misma que son: Resistencia, Capacitancia, Inductancia y Conductancia (inversa de la resistencia de aislamiento entre los conductores que forman la línea). La fórmula que relaciona los anteriores parámetros y que determina la impedancia característica de la línea es:

$$Z_o = \sqrt{\frac{R + jL\omega}{G + jC\omega}}$$

Z_o = Impedancia característica en ohms.

R = Resistencia de la línea en ohms.

C = Capacidad de la línea en faradios.

L = Inductancia de la línea en henrios.

G = Conductancia de la línea en siemens.

$\omega = 2\pi f$, siendo f la frecuencia en hercios

j = Factor imaginario

ISDN Integrated Services Digital Network). Estándar internacional de telecomunicaciones para la transmisión de voz, video y datos a través de líneas digitales que corren a 64 Kbits/seg. ISDN emplea canales portadores conmutados por circuitos (canales B) para transportar voz y datos, y usa un canal de datos separado (canal D) para controlar señales a través de una red conmutada por paquetes. Este canal D fuera de banda permite características como envío y espera de llamadas, y asesoría en tarifas. Basic Rate Service (BRI) y Primary Rate Service (PRI).

J1. Define el estándar PDH japonés para una velocidad de transmisión de 1.544 Mbps, consistente de 24 canales de 64 Kbps (canales DS-0), aunque también están disponibles J1 fraccionales. La longitud de la trama del estándar J1 es de 193 bits (24 x 8 bit, canales de voz/datos más un bit de sincronización), el cual es transmitido a una tasa de 8000 tramas por segundo. Así, 193 bits/trama x 8000 tramas/segundo = 1,544,000 bps o 1.544 Mbps.

Kbps. Kilobits por segundo, unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada kilobit esta formado por mil bits.

Mbps. Megabits por segundo, unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada megabit esta formado por un millón de bits.

MODEM. Modulador-Demodulador. Dispositivo que convierte señales digitales y analógicas. En el punto de origen, un módem convierte señales digitales a una forma apropiada para la transmisión por facilidades de comunicación analógica. En el punto de destino, las señales analógicas se recuperan a su forma digital. Los módem permiten la transmisión de datos por líneas telefónicas de grado voz.

Multiplexación. Técnica que permite la transmisión de varias señales lógicas simultáneamente a lo largo de un único canal físico.

Multiplexación estadística. Técnica por la cual la información proveniente de múltiples canales lógicos puede transmitirse a través de un único canal físico. La multiplexación estadística asigna dinámicamente anchos de banda sólo a los canales de entrada activos, aprovechando los anchos de banda disponibles y permitiendo conectar más dispositivos que con otras técnicas de multiplexación.

NIC (Network Information Center). Es la organización encargada de la administración del nombre de dominio territorial, el código de dos letras asignado a cada país. Principalmente en México, entre sus funciones están el proveer los servicios de información y registro para .mx así como la asignación de direcciones de IP y el mantenimiento de las bases de datos respectivas a cada recurso.

OC (Optical Carrier). Define las velocidades de transmisión de SONET para señales ópticas en incrementos de 51.84 Mbps.

Página Web. Es un documento de la World Wide Web, típicamente, incluye texto, imágenes y enlaces hacia otros documentos de la red, pudiendo además contener animaciones, sonidos, programas en Java, y cualquier otro tipo de documento, por medio de plugins y otras tecnologías. Actualmente las páginas web ya no están únicamente enfocadas para ser visionadas, sino que cada vez son más dinámicas permitiendo que el visitante participe en ellas mediante menus interactivos, encuestas, votaciones, etc.

PDA (Personal Digital Assistant). Es un dispositivo portátil, originalmente diseñado como agenda personal, hoy en día se ha convertido en una computadora de mano, y dispositivo multimedia para ver películas, fotografías, escuchar música, etc.

PDH. Define un conjunto de sistemas de transmisión que utiliza dos pares de cables (uno para transmitir, otro para recibir) y un método de multi-canalización por división de tiempo (TDM) para interpolar múltiples canales de voz y datos digitales. Existen tres conjuntos diferentes de estándares PDH utilizados en las telecomunicaciones mundiales, T1, E1 y J1.

PRI (Primary Rate Interface). Provee 23 canales B y un canal D de 64 Kbps for controlling communications, equivalente a T1. Europa usa 30 canales B y un canal D, equivalente al servicio europeo E1.

Protocolo. En un conjunto de reglas y convenciones que indican cómo es el intercambio de la información a través del medio de transmisión.

Puente. es un dispositivo de interconexión de redes que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete. Un bridge conecta dos redes como una sola red usando el mismo protocolo de establecimiento de red. Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual. La principal diferencia entre un bridge y un hub es que el segundo pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio el primer sólo pasa las tramas pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil. Para hacer el bridging o interconexión de más de 2 redes, se utilizan los switches.

Rack. Es una estructura metálica que se dispone de forma vertical, sirve de soporte para acomodar equipos de red y paneles de parcheo para cableado en las salas de transmisión,

Roaming. Es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra. Es una palabra de procedencia inglesa que significa vagar o rondar.

Router. Es un dispositivo que interconecta redes de computadoras, opera en la capa tres (nivel de red) del modelo OSI. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del

router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo de enrutamiento que se utilice.

Sitio Web. Un sitio web (en inglés: website) es un conjunto de páginas web, típicamente comunes a un dominio de Internet o subdominio en la World Wide Web en Internet. Todos los sitios web públicamente accesibles constituyen una gigantesca "World Wide Web" de información. Algunos sitios web requieren una suscripción a acceder a algunos o todos sus contenidos. Un sitio web puede ser el trabajo de una persona, una empresa u otra organización y está típicamente dedicada a algún tema particular o propósito. Un sitio web está alojado en un sistema de ordenador conocido como servidor web.

Software. Es el equipamiento lógico, es decir, el conjunto de programas y procedimientos que son necesarios para realizar una tarea en especial.

SONET. Es el estándar norteamericano (Estados Unidos/Canadá) de transmisión de fibra óptica, mientras que SDH es el estándar europeo. Los sistemas de transmisión SONET/SDH son diseñados para sobrellevar las deficiencias de compatibilidad de los sistemas de transmisión PDH. La estructura escalable de SDH/SONET permite también la incorporación de otras tecnologías de redes ópticas y de banda ancha.

Los niveles de servicio de SDH/SONET incluyen: OC, STS ATM.

STM (Synchronous Transport Mode). Define las velocidades de transmisión de SONET para señales eléctricas y ópticas en incrementos de 155.52 Mbps.

STS (Synchronous Transport Signal). Define las velocidades de transmisión de SONET para señales eléctricas en incrementos de 51.84 Mbps.

T1. Define el estándar PDH de Norteamérica que consiste de 24 canales de 64 Kbps (canales DS-0) dando una capacidad total de 1.544 Mbps. También están disponibles T1s fraccionales.

REFERENCIAS BIBLIOGRAFICAS.

- 1.- "Arquitecturas de enrutamiento en Internet", Halabi Sam y McPherson Dhabi, 2° edición, PEARSON EDUCACIÓN, S.A., Madrid, 2001
- 2.- "Apuntes de redes de datos", Universidad de Concepción, Facultad de Ingeniería, Dpto. de Ingeniería Eléctrica
- 3.- "MCSE Training Guide TCP/IP", Emmett Dulaney, Sherwood Lawrence, Edit. New Riders, E.U.A 1998
- 4.- "Manual de referencia, redes", Osborne Media, Craig Zacker, Edit. McGraw-Hill, España 2002
- 5.- "Digital and analog communication systems", Leon W. Couch II, 4ª edición, Macmillan Publishing Company, USA 1993
- 6.- "Communication systems", Simon Haykin, 3ª edición, John Wiley & Sons Inc. USA 1994
- 7.- "Ley Federal de Telecomunicaciones"
- 8.- www.unincca.edu.co/boletin/indice.htm
- 9.- www.arrakis.es/~sergilda/wlan/
- 10.- www.webopedia.com/quick_ref/WLANStandards.asp
- 11.- www.wlana.org
- 12.- www.bluetooth.com
- 13.- www.homerf.org
- 14.- www.hiperlan2.com
- 15.- www.manta.ieee.org/groups/802/11
- 16.- www.glosarium.com
- 17.- <http://ciberhabitat.com/museo/cerquita/redes/ethernet/06.htm>
- 18.- www.htmlweb.net/redes/osi/osi_1.html
- 19.- www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp
- 20.- www.um.es/~gtiweb/fjmm/ttsite-plan2/modelos.htm#5-1
polaris.lcc.uma.es/~eat/services/fddi/fddi.htm#link52
- 21.- www.sct.gob.mx
- 22.- www.cofetel
- 23.- www.wimaxforum.org
- 24.- www.ceditec.etsit.upm.es
- 25.- www.blogwimax.com
- 26.- www.80216news.com
- 27.- www.wimax.com/education/wimax/wireless_architectures

ÍNDICE DE TABLAS.

CAPITULO 1.	PAG.
Tabla 1.1 Tecnología DSL.	11
CAPITULO 2.	
Tabla 2.1 Comparativa de topologías.	22
Tabla 2.2 Características de Ethernet 10Base-T.	24
Tabla 2.3 Características de Ethernet 100Base-T.	25
Tabla 2.4 Características de Ethernet 1000Base-T.	25
CAPITULO 3.	
Tabla 3.1 Tasas de transferencia.	72
Tabla 3.2 Características de tecnología inalámbrica.	80
CAPITULO 5.	
Tabla 5.1 Características de productos.	91
Tabla 5.2 Cobertura de productos Airconnect de 3COM.	92
Tabla 5.3 Usuario con acceso inalámbrico.	92

ÍNDICE DE IMÁGENES.

CAPITULO 2.	PAG.
Fig. 2.1 Capas del Modelo de Referencia OSI.	16
Fig. 2.2 Información de control.	17
Fig. 2.3 Cable coaxial.	18
Fig. 2.4 Cable par trenzado.	19
Fig. 2.5 Cable de fibra óptica.	19
Fig. 2.6 Topologías de red.	21
Fig. 2.7 Trama de Ethernet.	26
Fig. 2.8 Topología de una red Token-Ring.	27
Fig. 2.9 Topología de una red FDDI,	29
Fig. 2.10 Modelo de Referencia de TCP/IP.	33
Fig. 2.11 Octetos del direccionamiento en una clase A.	35
Fig. 2.12 Octetos del direccionamiento en una clase B.	35
Fig. 2.13 Octetos del direccionamiento en una clase C.	36
Fig. 2.14 Trama de IPv6	40
Fig. 2.15 Paquete básico de DHCP	49
Fig. 2.16 Negociación de dirección IP en DHCP.	52
Fig. 2.17 Alcance de los equipos sobre el Modelo de Referencia OSI.	53
 CAPITULO 3.	
Fig. 3.1 WLAN Peer – Peer.	58
Fig. 3.2 WLAN con un AP.	59
Fig. 3.3 WLAN con varios AP's.	59
Fig. 3.4 WLAN con puntos de extensión.	60
Fig. 3.5 WLAN con antena direccional.	60
Fig. 3.6 Transmisor FHSS.	66
Fig. 3.7 Señal transmitida con FHSS.	66
Fig. 3.8 Dispersión en el espectro de una modulación DSSS.	67
Fig. 3.9 Transmisor DSSS.	68
Fig. 3.10 OFDM	69
Fig. 3.11 Modo infraestructura.	71
Fig. 3.12 Modo Adhoc o Peer – Peer.	71
Fig. 3.13 802.11 y el Modelo de referencia OSI.	72
Fig. 3.14 Roaming y Handoff.	76
Fig. 3.15 Mapa de cobertura.	76
 CAPITULO 4.	
Fig. 4.1 Arquitectura de Access Point.	82
Fig. 4.2 Access Point Cisco Aironet 1230.	82



Fig. 4.3 Access Point Cisco Aironet 1100.	83
Fig. 4.4 Arquitectura básica de un router inalámbrico.	83
Fig. 4.5 Router inalámbrico con servicio ADSL o Cable Modem.	84
Fig. 4.6 Router inalámbrico Linksys.	84
Fig. 4.7 Router inalámbrico US Robotics.	84
Fig. 4.8 Arquitectura básica de un Modem / Router.	85
Fig. 4.9 Modem/Router Inalámbrico 2Wire 1800hg.	85
Fig. 4.10 Tarjeta inalámbrica PCMCIA Linksys.	86
Fig. 4.11 Tarjeta inalámbrica PCI Linksys.	86
Fig. 4.12 Adaptador inalámbrico USB SMC.	87
Fig. 4.13 Adaptador inalámbrico USB Belkin.	87
Fig. 4.14 Tarjeta Wi-Fi Palm.	87

CAPITULO 5.

Fig. 5.1 Cobertura a 11 Mbps en entorno cerrado.	93
--	----

CAPITULO 6.

Fig. 6.1 Conexión Punto-Punto y Punto-Multipunto con WIMAX fijo	98
Fig. 6.2 Panorama de WIMAX fijo y WIMAX móvil	99



“Por mi raza hablará el espíritu”
UNAM