UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

COMUNICACION DE DATOS EN REDES CELULARES GSM

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA
P R E S E N T A:

BENITO OSWALDO CHAVERO CHAVEZ

ASESOR: ING. JOSE LUIS RIVERA LOPEZ

CUAUTITLAN IZCALLI, EDO. MEX. 2006

AGRADECIMIENTOS:

Primero debo agradecer a mi madre, pues además de traerme al mundo, siempre me apoyo y ayudo para alcanzar todas y cada una de mis metas, y aunque lamentablemente ya no está en éste mundo, siempre estará conmigo.

Ma. Cristina Chávez Saldivar †

También debo agradecer a mis tres hermanos, Ma. Del Consuelo, José Alberto y José Oscar, quienes de manera sincera y firme siempre me han apoyado para lograr todas las empresas que he iniciado.

Por supuesto debo agradecer a la Universidad Nacional Autónoma de México, a la Facultad de Estudios Superiores Cuautitlán y a todos y cada uno de mis profesores, pues gracias a su apoyo y dedicación, muchas personas al igual que yo hemos logrado superarnos en lo academico y personal hasta llegar a ser profesionistas.

Un agradecimiento especial a mi asesor el Ing. José Luis Rivera López, por su apoyo tanto para realizar éste trabajo de tesis, como por su gran interés y compromiso en el aula.

Un agradecimiento y a la vez un reconocimiento a todos mis compañeros de la FES-C, Jorge Luis García, Juan Ramírez, Juan Carlos Romero, Eduardo Becerril, Adrián Gutiérrez, Carlos Villafaña, Jaime Olivas, Elia Galván, Daniel Novoa, y muchos más; pues además de compartir el privilegio de cursar una carrera universitaria, siempre estuvieron ahí cuando necesite de su ayuda.

Quisiera también mencionar y agradecer al Matemático y profesor del CCH Oriente Felipe Patiño Santander por su gran interés y apoyo en la superación academica y personal de todos y cada uno de los alumnos que tuvimos el privilegio de pasar por su aula.

Benito Oswaldo Chavero Chávez

Septiembre 2006

ÍNDICE

Prólogo

La comunicación para los seres vivos y en particular para los seres humanos ha sido a lo largo de la historia pieza fundamental para el desarrollo y sobre vivencia de la especie; desde las señales de humo y sonidos guturales, hasta los modernos y eficientes teléfonos móviles y las redes de datos, la evolución de dichos medios de comunicación ha sido enorme.

Desde que la tecnología entro en el campo de la comunicación entre los seres humanos, ésta ha despertado gran interés tanto a nivel gobierno como a nivel comercial, y su desarrollo ha sido desde relativamente lento –sistemas electromecánicos- hasta a pasos agigantados gracias a el desarrollo de los sistemas de computo y software.

Hoy en día para nosotros es común el comunicarnos desde casi cualquier punto dentro y fuera de las ciudades ya sean grandes o pequeñas, además de que la tecnología de comunicación cada día es más barata y flexible. Desafortunadamente para los Mexicanos que día a día vemos llegar tecnologías novedosas y cada vez más sofisticadas el panorama general del desarrollo tecnológico es bastante desalentador, pues mientras que en otros países se invierten cantidades importantes de dinero para el desarrollo tecnológico, en nuestro país seguimos siendo dependientes de lo que se desarrolle en otros lugares, por lo que el nivel de investigación y desarrollo tecnológico –con excepciones como el de nuestra Universidad- es prácticamente nulo en comparación con el de otros países con los que queremos competir.

Por lo que considero importante que más allá del fundamental aprendizaje técnico y científico que se imparte en las diferentes escuelas de ciencias e ingeniería en nuestro país, se debe dar un enfoque especial por parte de los ingenieros y los futuros ingenieros a la historia del desarrollo tecnológico en países donde éste ha sido pieza clave en el desarrollo de sus economías y por ende en el mejoramiento del nivel de vida de sus ciudadanos, pues dichos países han apostado gran cantidad de su capital económico y humano al desarrollo científico y tecnológico por lo que hoy día son considerados además de potencias tecnológicas, países con altos niveles de vida.

Por ejemplo, muchos descubrimientos científicos han sido obra de la casualidad, cuando se estaba investigando una cosa y se descubría otra; pero también han habido investigaciones especificas por parte de gobiernos o de empresas en donde se enfoca un grupo de científicos e ingenieros en desarrollar tecnología para aplicaciones especificas y aun cuando no todas han cumplido con su cometido, ha habido una importante cantidad de investigaciones exitosas que han ayudado al desarrollo de los países que apuestan a una mayor independencia tecnológica.

Concluyendo, creo que es necesario exigir a nuestros gobiernos un mayor apoyo al desarrollo científico y tecnológico, pues no nos sirve de mucho el ser un país "moderno" que prácticamente es dependiente de otros en lo referente a ciencia y tecnología.

Benito Oswaldo Chavero Chávez

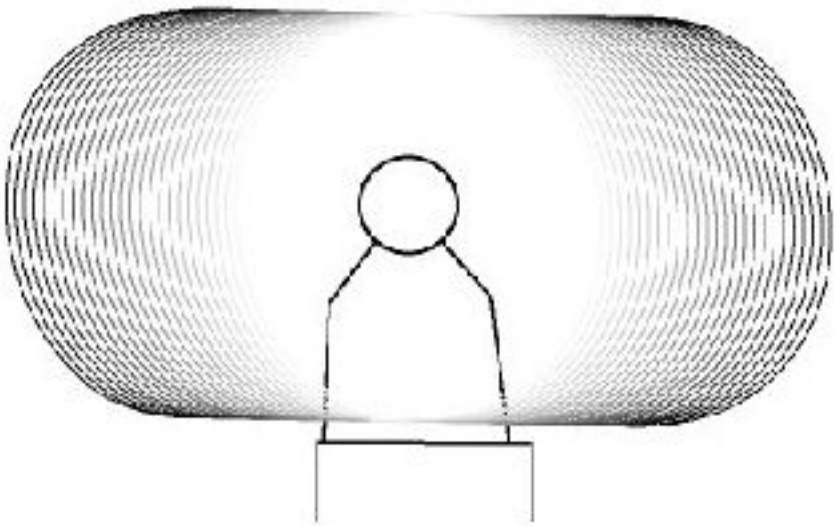
Septiembre 2006

INTRODUCCIÓN

Las Telecomunicaciones durante el último medio siglo han tomado una importancia muy significativa para la gran mayoría de países en el mundo, esto debido en gran medida a los avances científicos y tecnológicos que se han dado en distintos rubros. Desde la comunicación vía satélite hasta los servicios Wreless, las telecomunicaciones inalámbricas han tomado una importancia cada vez mayor debido a la versatilidad que estos servicios proporcionan al usuario, pues cada vez es más fácil estar comunicado casi en cualquier parte del planeta; uno de los servicios inalámbricos que han tomado una importancia trascendental es el servicio de Comunicaciones Celulares, que en los últimos 5 años ha crecido de manera exponencial, debido a la mejora en cuanto a tecnología tanto de servicios como de terminales, pero también debido al crecimiento de la cobertura que proporcionan a los usuarios finales, a continuación se hará un pequeño análisis de las tecnologías y servicios de las redes Celulares GSM.

CAPÍTULO 1

BREVE HISTORIA DE LAS TELECOMUNICACIONES



1.1 INTRODUCCION A LAS TELECOMUNICACIONES

El desarrollo de la civilización, hasta llegar al punto en que se encuentra hoy en día, se debe en gran medida a la habilidad del ser humano para intercambiar información e ideas gracias a los sentidos de la vista, el oído y a través de la palabra y la escritura mediante alguna forma de lenguaje o código. Desde los albores de la civilización la gente ha buscado constantemente medios para transmitir información a distancias muy lejanas. Cualquiera conoce o está familiarizado con métodos como las señales de humo que hacían los indios, los faros alumbrados con hogueras o los semáforos que señalan con banderas.

Vale la pena mencionar el significado de las dos derivaciones de la palabra Telecomunicaciones: *tele* se deriva del griego y quiere decir *a distancia* ; *fono* significa *sonido*, y *grafos* significa *escritura o dibujo*, de estas palabras se desprenden los siguientes términos:

- Telecomunicación: comunicar a distancia
- Teléfono: Hablar a distancia
- Televisión: Ver a distancia
- Telégrafo: Escribir a distancia

Telecomunicación es, por tanto, el proceso de transmitir información en forma de energía a grandes distancias con la ayuda de medios electrónicos. La información en forma de energía es enviada a su destino ya sea por medio de alambres conductores apropiados para éste fin, llamados líneas de transmisión, o en forma inalámbrica a través de la atmósfera por enlaces de radio.

El uso directo de la electricidad o la energía eléctrica en las tareas diarias es bien conocido; por ejemplo, en hornos, luces, motores, etc. En cada caso, la energía eléctrica es transformada en otras formas de energía a efecto de realizar una tarea especifica. En telecomunicaciones, una cierta forma de "información" o energía "inteligente" es convertida en energía eléctrica para poder de éste modo enviarla a un punto distante. Ya en su destino, la energía eléctrica se convierte de nuevo en su forma original. Este uso particular de la energía eléctrica para transmitir información es parte de la electrónica. Algunas formas familiares de energía que contienen información son los sonidos que produce la voz humana, la música, las fotografías fijas o en movimiento, entre otras.

Como es bien sabido por todos los primeros sistemas de telecomunicaciones fueron implementados a través de redes de cable, primero con el uso de un alambre telegráfico, después se incremento el número de cables ya no para transmitir códigos, sino para transmitir voz, hasta llegar a la necesidad de comunicación móvil, o donde era muy difícil la instalación de la red de cable. Móvil significa en términos de telecomunicaciones el hecho de estar en movimiento, ya sea a pie o en algún tipo de vehículo, pero como se menciono anteriormente hay sitios donde implementar una red de cable resulta muy complicado y costoso, por lo que las redes inalámbricas o móviles resultan más practicas de implementar. A continuación se hará un pequeño análisis de los principios de funcionamiento de las telecomunicaciones inalámbricas, así como de algunos conceptos fundamentales para el funcionamiento de dichas redes de telecomunicaciones.

1.2 BREVE HISTORIA DE LAS COMUNICACIONES INALÁMBRICAS

1.2.1 La síntesis de Maxwell

El experimento de Oersted (1820) había demostrado la existencia de efectos magnéticos debidos a cargas en movimiento. Los descubrimientos de Faraday (1831) habían puesto de manifiesto que campos magnéticos variables con el tiempo dan lugar a un movimiento de cargas eléctricas en los conductores. Además, la explicación de Faraday de estos fenómenos llamados de inducción había introducido por primera vez en la historia de la física la noción de campo magnético representado por un conjunto de líneas de fuerza. Medio siglo antes, Charles Coulomb (1785) había descrito en forma de ley el modo en que las cargas eléctricas se atraen entre sí. Estos cuatro elementos fundamentales sirvieron de base a Maxwell para iniciar la síntesis de los fenómenos eléctricos y de los fenómenos magnéticos entonces conocidos y su explicación dentro de una amplia teoría conocida como *teoría del electromagnetismo.*

Apoyado en una enorme habilidad matemática, Maxwell empezó dando forma de ecuaciones a las observaciones de Faraday y a su noción de campo magnético. Las fuerzas entre cargas en reposo se beneficiarían pronto de una representación semejante en forma de campos eléctricos o electrostáticos. Este proceso de elaboración teórica le permitió finalmente describir lo esencial de los fenómenos electromagnéticos en cuatro ecuaciones, que se denominan *ecuaciones de Maxwell.* La primera describe cómo es el campo eléctrico debido a cargas en reposo; la segunda traduce en forma matemática la imposibilidad de separar los polos magnéticos de un imán; la tercera expresa en términos de campos magnéticos y corrientes eléctricas el descubrimiento de Oersted y la cuarta recoge la aportación de Faraday. La virtud de tales ecuaciones es que en ellas aparecen a primera vista los campos eléctricos **E** y magnético **B** y su forma simple y rica a la vez permite relacionarlas entre sí para obtener nuevos resultados y predecir nuevas consecuencias.

Además de resumir en un solo cuerpo de conocimientos la electricidad y el magnetismo, la teoría de Maxwell abrió nuevos caminos al conocimiento de la naturaleza y a sus aplicaciones. Las ondas electromagnéticas, que son la base de las actuales telecomunicaciones, como la radio o la televisión, constituyeron la predicción más interesante de esta síntesis de Maxwell.

1.2.2 Las ondas electromagnéticas

De las ecuaciones de Maxwell se deduce que el campo magnético y el campo eléctrico pueden estar interactuando permanentemente si uno de ellos varía con el tiempo. Así, el movimiento acelerado de un sistema de cargas produce un campo magnético variable, el cual a su vez genera campos eléctricos. Pero, si éstos se producen, tuvieron que partir de cero; tal variación del campo eléctrico produce a su vez un campo magnético y así repetidamente. Esta sucesión oscilante de campos eléctricos y magnéticos viajando por el espacio se denomina *onda electromagnética.*

A partir de sus ecuaciones, Maxwell anticipó que las ondas electromagnéticas deberían propagarse en el vacío a una velocidad igual a la velocidad de la luz. Las predicciones de Maxwell fueron confirmadas experimentalmente por Hertz, quien generó y detectó este tipo de ondas, observando que su comportamiento era idéntico al de las ondas luminosas de la óptica.

Desde las ondas de radio hasta los rayos gamma, pasando por las ondas luminosas, una amplia gama de ondas electromagnéticas constituyen el llamado espectro electromagnético hoy conocido. Todas ellas tienen la misma naturaleza y sólo se diferencian en su frecuencia, es decir, en el número de oscilaciones que se producen en cada segundo en estos campos viajeros. La energía de las ondas electromagnéticas es tanto mayor cuanto mayor es su frecuencia. La luz con sus colores constituye simplemente la porción limitada del espectro electromagnético, al cual el ojo humano es sensible.

1.2.3 El Experimento de Hertz

El montaje experimental que permitió a Heinrich Hertz en 1888 producir y detectar ondas electromagnéticas constaba de un circuito eléctrico, capaz de producir tensiones eléctricas oscilantes, y de un detector. Dicho circuito, formado, en esencia, por un transformador y unas placas metálicas a modo de condensadores, se conectaba a dos esferas metálicas pulimentadas separadas entre sí por una pequeña región de aire. Cuando la tensión entre las dos esferas alcanzaba su valor máximo, el aire intermedio se electrizaba y saltaba una chispa. Este proceso se repetía periódicamente generando, cada vez, según la predicción de Maxwell, un conjunto de ondas electromagnéticas.

Para comprobar que, en efecto, un campo electromagnético viajero se estaba propagando por el espacio, Hertz preparó un detector (o antena), conocido también como resonador, que consistía en un alambre corto doblado en forma de circunferencia, pero con una pequeña abertura intermedia. Las ondas electromagnéticas, si existían, serían detectadas porque la variación del campo magnético de la onda al atravesar el resonador daría lugar a una fuerza electromotriz inducida que provocaría una chispa entre sus extremos.

Con el fin de analizar el fenómeno más cómodamente, situó en su laboratorio una superficie reflectora que le permitiría confinar las ondas producidas en el espacio comprendido entre el circuito emisor y la placa. Así, y con la ayuda del resonador, fue capaz de descubrir las características de las ondas generadas mediante su aparato emisor y de medir una longitud de onda de 66 cm. Las previsiones teóricas de Maxwell fueron confirmadas y Hertz demostró experimentalmente que las ondas electromagnéticas se reflejaban, se retractaban y sufrían interferencias al igual que las ondas luminosas. En su honor recibieron el nombre de ondas hertzianas.

1.3 ALGUNAS DEFINICIONES IMPORTANTES

1.3.1 Radiación Electromagnética

Ondas producidas por la oscilación o la aceleración de una carga eléctrica. Las ondas electromagnéticas tienen componentes eléctricos y magnéticos. La radiación electromagnética puede ordenarse en un **espectro** que se extiende desde ondas de frecuencias muy elevadas (longitudes de onda pequeñas) hasta frecuencias muy bajas (longitudes de onda altas).

1.3.2 Espectro

Serie de colores semejante a un arco iris (por este orden: violeta, azul, verde, amarillo, anaranjado y rojo) que se produce al dividir una luz compuesta como la luz blanca en sus colores constituyentes. El arco iris es un espectro natural producido por fenómenos meteorológicos. Puede lograrse un efecto similar haciendo pasar luz solar a través de un prisma de vidrio.

Cuando un rayo de luz pasa de un medio transparente como el aire a otro medio transparente, por ejemplo vidrio o agua, el rayo se desvía; al volver a salir al aire vuelve a desviarse. Esta desviación se denomina refracción; la magnitud de la refracción depende de la longitud de onda de la luz. La luz violeta, por ejemplo, se desvía más que la luz roja al pasar del aire al vidrio o del vidrio al aire. Así, una mezcla de luces roja y violeta se dispersa al pasar por un prisma en forma de cuña y se divide en dos colores. Se diferencian en su frecuencia y longitud de onda. Dos rayos de luz con la misma longitud de onda tienen la misma frecuencia y el mismo color. La longitud de onda de la luz es tan corta que suele expresarse en nanómetros (nm).

Los científicos descubrieron que más allá del extremo violeta del espectro podía detectarse una radiación invisible para el ojo humano pero con una marcada acción fotoquímica; se la denominó radiación ultravioleta. Igualmente, más allá del extremo rojo del espectro se detectó radiación infrarroja que aunque era invisible transmitía energía, como demostraba su capacidad para hacer subir un termómetro. Como consecuencia, se redefinió el término *espectro* para que abarcara esas radiaciones invisibles, y desde entonces se ha ampliado para incluir las ondas de radio más allá del infrarrojo y los rayos X y rayos gamma más allá del ultravioleta.

Por orden decreciente de frecuencias figura 1.1, u orden creciente de longitud de onda tabla 1.1, el espectro electromagnético está compuesto por rayos gamma, rayos X duros y blandos, radiación ultravioleta, luz visible, rayos infrarrojos, microondas y ondas de radio. Los rayos gamma y los rayos X duros tienen una longitud de onda de entre 0,005 y 0,5 nanómetros (un nanómetro, o nm, es una millonésima de milímetro). Los rayos X blandos se solapan con la radiación ultravioleta en longitudes de onda próximas a los 50 nm. No existen límites definidos entre las diferentes longitudes de onda, pero puede considerarse que la radiación ultravioleta va desde los 350 nm hasta los 10 nm. El ultravioleta, a su vez, da paso a la luz visible, que va aproximadamente desde 400 hasta 800 nm. La longitud de onda de la luz violeta varía entre unos 400 y 450 nm, y la de la luz roja entre unos 620 y 760 nm. Los rayos infrarrojos o "radiación de calor" se solapan con las frecuencias de radio de microondas, entre los 100.000 y 400.000 nm. Desde esta longitud de onda hasta unos 15.000 metros, el espectro está ocupado por las diferentes ondas de radio; más allá de la zona de radio, el espectro entra en las bajas frecuencias, cuyas longitudes de onda llegan a medirse en decenas de miles de kilómetros.

Rayos	**Gamma**	**X duros**	**X blandos**		**Ultra-violeta**	**Visibles**				**Infra-rojos**		**Micro-ondas**	**Radio**
						Violeta		**Rojo**					
1 (nm)	**.005**	**0.5**	**10**	**50**	**350**	**400**	**450**	**620**	**760**	**800**	**100 000**	**400 000**	**15000 x10^3**

Tabla 1.1 Espectro electromagnético y longitud de onda

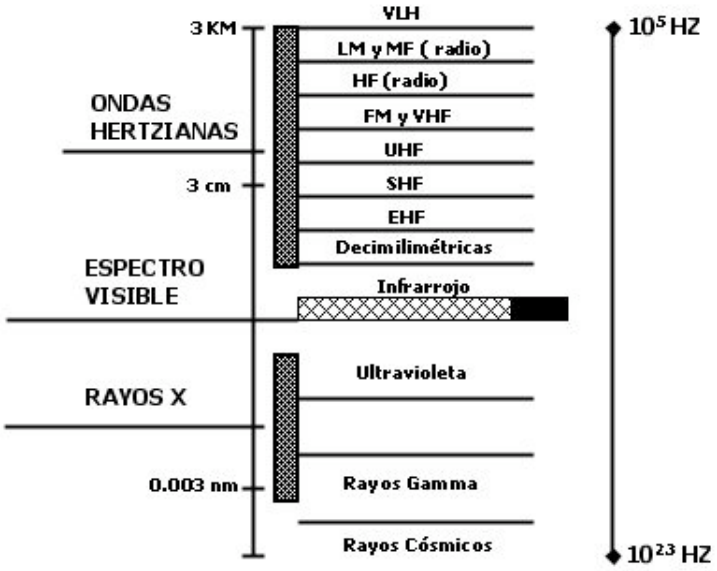


Figura 1.1 Espectro electromagnético y sus frecuencias

1.3.3 Propiedades

Las ondas electromagnéticas no necesitan un medio material para propagarse. Así, estas ondas pueden atravesar el espacio interplanetario e interestelar y llegar a la Tierra desde el Sol y las estrellas. Independientemente de su frecuencia y longitud de onda, todas las ondas electromagnéticas se desplazan en el vacío a una velocidad c = 299.792 km/s. Todas las radiaciones del espectro electromagnético presentan las propiedades típicas del movimiento ondulatorio, como la difracción y la interferencia. La longitud de onda va desde billonésimas de metro hasta muchos kilómetros, es importante para determinar su energía, su visibilidad, su poder de penetración y otras características. y se expresa mediante la ecuación:

l x f = c

l: longitud de onda

f: frecuencia

c: velocidad de propagación de la luz

Una onda electromagnética con una longitud de onda de 1 nm tiene una frecuencia de aproximadamente 300 millones de GHz.

Los físicos sabían que la luz se propaga como una onda transversal (una onda en la que las vibraciones son perpendiculares a la dirección de avance del frente de ondas). Sin embargo, suponían que las ondas de luz requerían algún medio material para transmitirse, por lo que postulaban la existencia de una sustancia difusa, llamada éter, que constituía el medio no observable. La teoría de Maxwell hacía innecesaria esa suposición, pero el concepto de éter no se abandonó inmediatamente, porque encajaba con el concepto newtoniano de un marco absoluto de referencia espaciotemporal. Un famoso experimento realizado por Michelson y Morley socavó el concepto del éter, y fue muy importante en el desarrollo de la teoría de la relatividad. De este trabajo concluyó que *la velocidad de*

la radiación electromagnética en el vacío es una cantidad invariante, que no depende de la velocidad de la fuente de radiación o del observador.

1.3.4 Cuantos de radiación

Los físicos se dieron cuenta de que la teoría ondulatoria no explicaba todas las propiedades de la radiación. Planck demostró que la emisión y absorción de radiación se produce en unidades finitas de energía denominadas **cuantos**. Einstein consiguió explicar algunos resultados experimentales sorprendentes en relación con el efecto fotoeléctrico externo postulando que la radiación electromagnética puede comportarse como un chorro de partículas.

Hay otros fenómenos de la interacción entre radiación y materia que sólo la teoría cuántica explica. Así, los físicos modernos se vieron obligados a reconocer que la radiación electromagnética se comporta unas veces como partículas y otras como ondas. El concepto paralelo que implica que la materia también puede presentar características ondulatorias además de corpusculares fue desarrollado por De Broglie.

1.3.5 Rayos X

Radiación electromagnética penetrante, producida bombardeando un blanco (generalmente de volframio) con electrones de alta velocidad. Los rayos X fueron descubiertos por Roentgen mientras estudiaba los rayos catódicos en un tubo de descarga gaseosa de alto voltaje. A pesar de que el tubo estaba dentro de una caja de cartón negro, Roentgen vio que una pantalla de platino cianuro de bario, que casualmente estaba cerca, emitía luz fluorescente siempre que funcionaba el tubo. Tras realizar experimentos adicionales, determinó que la fluorescencia se debía a una radiación invisible más penetrante que la radiación ultravioleta.

La longitud de onda de los rayos X va desde unos 10 nm hasta 0,001 nm. Cuanto menor es la longitud de onda de los rayos X, mayores son su energía y poder de penetración. Los rayos de mayor longitud de onda, cercanos a la banda ultravioleta del espectro electromagnético, se conocen como *rayos X blandos*. Los de menor longitud de onda, que están más próximos a la zona de rayos gamma, se denominan *rayos X duros*. Los rayos X formados por una mezcla de muchas longitudes de onda diferentes se conocen como rayos X "blancos", para diferenciarlos de los rayos X monocromáticos, que tienen una única longitud de onda.

Tanto la luz visible como los rayos X se producen a raíz de las transiciones de los electrones atómicos de una órbita a otra. La luz visible corresponde a transiciones de electrones exteriores y los rayos X a transiciones de electrones interiores. En el caso de la radiación de frenado, los rayos X se producen por el frenado o deflexión de electrones libres que atraviesan un campo eléctrico intenso. Los rayos gamma, cuyos efectos son similares a los de los rayos X, se producen por transiciones de energía en el interior de núcleos excitados.

1.3.6 Rayos Ultravioletas

Radiación electromagnética cuyas longitudes de onda van aproximadamente desde los 400 nm, el límite de la luz violeta, hasta los 15 nm, donde empiezan los rayos X. La radiación ultravioleta puede

producirse artificialmente mediante lámparas de arco; la de origen natural proviene principalmente del Sol.

La radiación ultravioleta con longitudes de onda inferiores a 300 nm se emplea para esterilizar superficies porque mata a las bacterias y los virus. En los seres humanos, la exposición a radiación ultravioleta de longitudes de onda inferiores a los 310 nm puede producir quemaduras; una exposición prolongada durante varios años puede provocar cáncer de piel.

La atmósfera terrestre protege a los organismos vivos de la radiación ultravioleta del Sol. Si toda la radiación ultravioleta procedente del Sol llegara a la superficie de la Tierra, acabaría probablemente con la mayor parte de la vida en el planeta. La capa de ozono de la atmósfera absorbe casi toda la radiación ultravioleta de baja longitud de onda y gran parte de la de alta longitud de onda. Sin embargo, la radiación ultravioleta no sólo tiene efectos perniciosos; gran parte de la vitamina D que las personas y los animales necesitan para mantenerse sanos se produce cuando la piel es irradiada por rayos ultravioleta.

1.3.7 Rayos Infrarrojos

Emisión de energía en forma de ondas electromagnéticas en la zona del espectro situada inmediatamente después de la zona roja de la radiación visible. Oscila entre aproximadamente 10-6 y 10-3 metros. La radiación infrarroja puede detectarse como calor, para lo que se emplean instrumentos como el bolómetro.

Los rayos infrarrojos se utilizan para obtener imágenes de objetos lejanos ocultos por la bruma atmosférica, que dispersa la luz visible pero no la radiación infrarroja. Hay dispositivos infrarrojos que permiten ver objetos en la oscuridad. Estos instrumentos consisten básicamente en una lámpara que emite un haz de rayos infrarrojos, a veces denominados *luz negra*, y un telescopio que recibe la radiación reflejada por el objeto y la convierte en una imagen visible. En astronomía se utilizan los rayos infrarrojos para estudiar determinadas estrellas y nebulosas.

Para las fotografías infrarrojas de alta precisión se emplea un filtro opaco que sólo deja pasar radiación infrarroja, pero generalmente basta un filtro corriente anaranjado o rojo claro, que absorbe la luz azul y violeta. La teledetección mediante fotografía infrarroja aérea y orbital se ha empleado para observar las condiciones de la cosecha y el daño por insectos y enfermedades en grandes zonas agrícolas, así como para localizar depósitos minerales. En la industria, la espectroscopia de infrarrojos es una parte cada vez más importante de la investigación de metales y aleaciones, y la fotografía infrarroja se emplea para regular la calidad de los productos.

1.3.8 Microondas

Ondas electromagnéticas de radio situadas entre los rayos infrarrojos y las ondas de radio convencionales. Su longitud de onda va aproximadamente desde 1 mm hasta 30 cm. Las microondas se generan con tubos de electrones especiales como el clistrón o el magnetrón, que incorporan resonadores para controlar la frecuencia, o con osciladores o dispositivos de estado sólido especiales. Las microondas tienen muchas aplicaciones: radio y televisión, radares, meteorología, comunicaciones vía satélite, medición de distancias, investigación de las propiedades de la materia o cocinado de alimentos.

Los hornos de microondas funcionan excitando las moléculas de agua de los alimentos, lo que hace que vibren y produzcan calor. Las microondas entran a través de aberturas practicadas en la parte superior de la cavidad de cocción, donde un agitador las dispersa de forma homogénea por todo el horno. Las microondas no pueden penetrar en un recipiente de metal para calentar la comida, pero sí atraviesan los recipientes no metálicos.

Las microondas pueden detectarse con un instrumento formado por un rectificador de diodos de silicio conectado a un amplificador y a un dispositivo de registro o una pantalla. La exposición a las microondas es peligrosa cuando se producen densidades elevadas de radiación, como ocurre en los *maceres.* Pueden provocar quemaduras, cataratas, daños en el sistema nervioso y esterilidad. Todavía no se conocen bien los posibles peligros de la exposición prolongada a microondas de bajo nivel.

1.3.9 ESPECTRO LUMINOSO / VENTANA OPTICA

Es la parte del espectro electromagnético comprendido entre 300 y 1500 nm. Aquí englobamos el espectro visible y el espectro luminoso no visible. El espectro visible, llamado también ventana óptica, comprende desde los 380 nm, aproximadamente, hasta los 780 nm. Por encima de los 780 nm tenemos las radiaciones infrarrojas y por debajo de los 380 nm tenemos las ultravioletas.

1.3.10 MOVIMIENTOS ONDULATORIOS

Propagación de una perturbación en un medio elástico

Sí en un punto de un medio elástico producimos una perturbación que dé lugar a una deformación local, se observa que esta perturbación se trasmite a todo el medio, propagándose por él a una determinada velocidad. Cuando se produce esta perturbación en un punto, dando lugar a un desplazamiento de la posición de equilibrio de las partículas, éstas empezaran a vibrar, transmitiendo su movimiento a las partículas más próximas y estas a su vez a otras, dando lugar a que la perturbación se propague por todo el medio. Pero esta perturbación se amortigua no solo por la perdida de energía debida al rozamiento de unas partículas con otras, sino que también esta energía, que en principio correspondía a unas pocas partículas, se extiende a un número mucho mayor. Y sirve como ejemplo para clarificar este hecho el efecto que produce una piedra cuando se arroja a un estanque de agua, la perturbación provocada por la piedra en el lugar de la caída se transmite a las partículas de agua próximas, propagándose en todas direcciones en forma de ondas circulares que se van amortiguando a medida que se van alejando del centro perturbador.

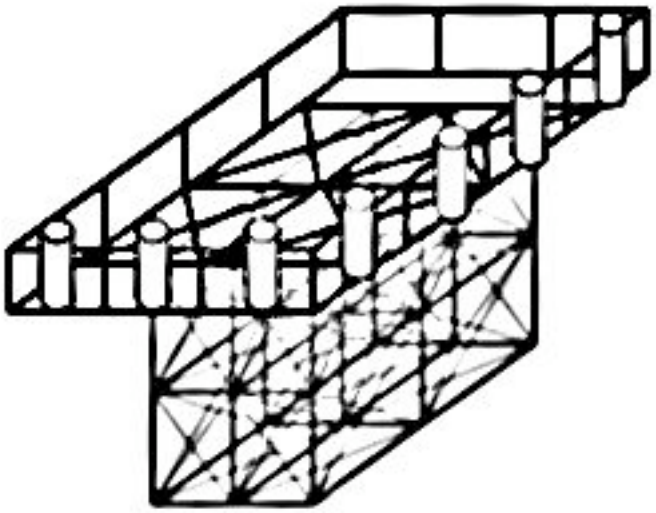
1.3.11 Ondas Longitudinales y Transversales

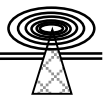
Ondas Transversales: Las partículas del medio oscilan en ángulos rectos con respecto a la dirección en la que viaja la onda, es decir, con respecto a su dirección de propagación. Ejemplo. Onda en el agua, radiación electromagnética.

Ondas Longitudinales: Las partículas oscilan a lo largo de la línea que representa la dirección en la que la onda está viajando. Ejemplo: sonido

CAPÍTULO 2

BREVE HISTORIA DE LA TELEFONÍA CELULAR





2.1 INICIOS DE LA TELEFONÍA MÓVIL EN ESTADOS UNIDOS

La radio móvil se utilizó por primera vez en 1921, cuando el Departamento de Policía de Detroit utilizó un sistema de radio móvil que operaba a una frecuencia cercana a los 2 MHz. Mucho más tarde, en 1940, la Comisión Federal de Comunicaciones (FCC) dispuso nuevas frecuencias para la radio móvil en la banda de frecuencia de 30 a 40 MHz. Sin embargo, no fue hasta que los investigadores desarrollaron técnicas de modulación en frecuencia (FM) en sustitución de las de modulación de amplitud (AM), para mejorar la recepción en presencia de ruido electrónico y desvanecimiento de señales, que la radio móvil se convirtió en algo verdaderamente útil.

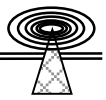
El primer sistema de telefonía móvil comercial en los Estados Unidos se estableció, en 1946, en St. Louis (Missouri), cuando la FCC proporcionó seis canales de telefonía móvil de 60 kHz, en el rango de frecuencias de 150 MHz. Esos sistemas tenían cierto parecido con los sistemas celulares de hoy. Típicamente, constaban de una estación base, tan elevada como fuera posible, con un potente transmisor y seis canales. Los "Teléfonos" iban montados en automóviles o camiones y eran grandes transeptores con también grandes baterías adjuntas. Su movilidad dependía de las de los vehículos en los que iban.

Aquellos sistemas satisfacían una necesidad, pero tenían serias limitaciones. La necesidad de transmitir una señal fuerte desde los vehículos requería baterías pesadas, que tenían que ser recargadas a menudo. Además, los sistemas hacían un uso muy ineficaz del espectro. Un sistema con seis canales podía manejar unos 200 abonados. Un mayor número de abonados implicaba el uso de más frecuencias, y las frecuencias portadoras tenían que estar bien distanciadas para evitar interferencias entre si.

La frecuencia existente es limitada, y la demanda supera casi siempre a la oferta. El servicio suministrado por las redes móviles estaba solamente a disposición de un número comparativamente pequeño de personas, y competía por la frecuencia con la Televisión, con su audiencia de millones que formaban un grupo de presión mas bien ruidoso. Para poder convencer a la FCC de que les asignara más frecuencias, las compañías involucradas –AT&T, Motorola, GE y las demás- tenían que encontrar una mejor forma de usar el espectro.

En 1947, AT&T había resuelto el problema. La solución era el *concepto celular,* que permite la reutilización de las frecuencias. Este concepto divide toda la zona que se vaya a cubrir, en cierto número de células. Cada célula tiene su propia estación base, con el número de frecuencias de onda portadora asignadas que corresponda al número estimado de abonados a quienes se vaya a servir en el área de la célula. Las células adyacentes tienen frecuencias de onda portadora distintas, para evitar interferencias, pero las células más alejadas pueden usar las mismas frecuencias que la primera célula –el espectro es así reutilizado-. Las células más pequeñas reducen también la potencia transmisora requerida.

Todo lo que se necesitaba era un sistema para pasar la llamada de una célula a la siguiente mientras avanzaba ("Hand-off"). AT&T tenía una solución teórica, pero dependía de un alto nivel de



"inteligencia" en el sistema, que no podía ser incorporado a un sistema práctico en los tiempos antes de los transistores, la microelectrónica y la tecnología informática.

Habrian de pasar más de 30 años antes de que los principios del sistema pudieran ser realizados. Los trabajos de AT&T llamaron demasiado la atención como para pasar desapercibidos, y, en todo caso, tuvieron su paralelo en otros países. Las décadas de 1950 y 1960 vieron nacer varios sistemas tempranos no celulares, que funcionaron de forma rentable.

La empresa Sueca Televerket fue una de las primeras instancias competidoras. A finales de 1950 se instaló en Estocolmo un sistema de prueba, con una sola antena de estación base colocada encima de la torre de agua Lindigö, isla próxima a la capital Sueca. El sistema llevaba dos canales de radio, dúplex, y servia a cinco estaciones móviles. Los resultados fueron alentadores y condujeron al montaje de dos sistemas, en Estocolmo y en Gotemburgo, completamente equipados para su operación comercial, si bien no fue hasta 1956 cuando esas redes móviles entraron en funcionamiento. El sistema recibió el nombre de MTA y permaneció en servicio hasta finales de la década siguiente, con unos 125 abonados en total.

La labor de Televerket con el sistema MTA fue seguida muy de cerca por la industria de la radio, incluido Ivar Ahlgren, director gerente de SRA. Fue ésta empresa la que construyó la primera estación móvil para el MTA, en 1956.

La segunda generación, el sistema MTB, fue montada sobre una base experimental en 1961 y entro en servicio a partir de 1965 en Estocolmo, Gotemburgo y Malmö, con unos 2000 abonados. SRA fue también uno de los fabricantes de las estaciones móviles para el MTB. La respuesta de los clientes al nuevo servicio fue favorable, a pesar de que, por razones obvias, los costes de los equipos y de las tarifas eran altos. Sin embargo, ampliar la cobertura resultaría costoso y requeriría bloques de espectro radioeléctrico tremendos. Televerket comprendió que la tecnología disponible conduciría a un callejón sin salida.

2.2 El ESTÁNDAR NMT

A pesar de todo, Televerket ya había decidido abordar aquellas dificultades, y así, en 1964, nombró un grupo de estudio bajo la dirección de Carl Gösta Åsdal (posteriormente jefe de las operaciones de telefonía móvil de Televerket), al que se encargo de investigar "todos los aspectos" de ésta telefonía. El grupo presento su informe en 1967 y recomendó el desarrollo de un servicio nacional de telefonía móvil celular, junto con un sistema nacional de radio búsqueda y un nuevo sistema de radio móvil terrestre.

Estos dos últimos sistemas fueron ejecutados con éxito, conforme a las recomendaciones dadas, y los laboratorios de Televerket comenzaron a trabajar sobre el sistema de telefonía celular. Sin embargo, en 1969, Åsdal presentó también el informe al pleno de la conferencia Nórdica de Telecomunicaciones, y sugirió que la telefonía móvil podría ser un tema digno de consideración para la cooperación pan nórdica. La propuesta fue aceptada con entusiasmo, y se creó un grupo de trabajo conjunto con representantes de las PTT nórdicas. Ese grupo se convirtió en el NMT, el grupo de telefonía móvil Nórdica, cuyo primer informe apareció en 1970.

Dicho informe recomendaba el desarrollo de un nuevo sistema pan nórdico de telefonía móvil, pero también sacaba la conclusión de que terminar un programa así llevaría alrededor de diez años, ya que dependería de nueva tecnología –en especial, la microelectrónica- aún no disponible. Por tal motivo, recomendaba asimismo el establecimiento de un sistema manual y provisional de telefonía móvil según un estándar común escandinavo, que atendiera la creciente demanda, y el desarrollo del mercado. Asi, en 1971, se introdujo el MTD, que duro hasta 1987.

El citado informe implicó igualmente una de las primeras grietas en la armadura monopolista de las administraciones Nórdicas de telecomunicación; presentó fuertes argumentos a favor de que las futuras estaciones móviles, los terminales instalados en los vehículos, fueran propiedad de los abonados, que los comprarían a fabricantes competidores en un mercado abierto. Ello ayudaría a reducir los precios y a estimular el crecimiento.

A partir de 1971, el grupo NMT mantuvo a los fabricantes pertinentes, incluido SRA, al corriente de los adelantos y, en 1973, invito a comentar y a hacer sugerencias sobre la especificación del sistema y las propuestas de diseño, así como sobre un cálculo preliminar de costos. La contribución central de SRA se centro en el interfaz aéreo, la forma de tratar el intercambio de información entre la estación móvil y las estación base. Las soluciones imperantes se basaban en el uso de señalización de tonalidad, pero SRA adujo, con éxito, que para manejar las cantidades necesarias de información a una velocidad suficiente, el sistema debía emplear tecnología informática –la señalización digital-.

Resulta interesante pensar que, hace tan solo 32 años, los operadores tenían la posibilidad, bien es verdad que con derechos exclusivos al mercado, de dedicar 10 años a la planificación y el desarrollo de una nueva red móvil!

Las cosas fueron bien, y en 1977-1978, se realizó una prueba de campo en Estocolmo de forma satisfactoria. De esto se otorgo el mérito a Thomas Haug, de Televerket, que fue entonces presidente del grupo NMT, y al Östen Mäkitalo, responsable en gran parte del diseño, la construcción y la realización de la prueba.

En 1977, se invito a los fabricantes a que presentaran ofertas para el suministro de estaciones base y de conmutadores MTX, que habrían de ser instalados en los distintos países.

2.3 El Estándar AMPS

En Estados Unidos, en 1947 se estableció un sistema móvil público en la autopista entre la ciudad de Nueva York y Boston que operó en el rango de frecuencia de 35 a 40 MHz.

En 1949, La FCC autorizó seis canales móviles adicionales a las portadoras de radio comunes, para ser utilizadas por compañías que hasta entonces no proporcionaban un servicio telefónico público. También, incrementó el número de canales de 6 a 11, reduciendo el ancho de banda a 30 kHz y espaciando los nuevos canales entre los viejos. En 1950, la FCC agregó 12 canales nuevos en la banda de 450 MHz.

Hasta 1964, los sistemas de telefonía móvil operaban sólo en el modo manual; una operadora del teléfono móvil especial manejaba cada llamada, de y hacia cada unidad móvil. En 1964, se pusieron en servicio los sistemas selectores de canales automáticos para los sistemas de telefonía móvil, lo que

eliminó la necesidad de la operación oprimir-para-hablar (push-to-talk) y le permitió a los clientes marcar directamente sus llamadas, sin la ayuda de una operadora. La instalación de marcación automática se extendió a la banda de 450 MHz, en 1969, y los sistemas de telefonía móvil mejorados (IMTS), se convirtieron en el servicio de telefonía móvil estándar de Estados Unidos. Los sistemas MTS sirven a un área de aproximadamente 60 km a la redonda y cada canal opera similarmente a una línea compartida. Cada canal puede asignarse a varios suscriptores, pero sólo uno puede utilizarlo a la vez y si el canal preasignado está ocupado se debe esperar hasta que se desocupe, antes de hacer o recibir una llamada.

La demanda creciente en el espectro de frecuencia de telefonía móvil saturado impulsó a la FCC a buscar un modo de proporcionar una eficiencia del espectro de frecuencia mayor. En 1971 AT&T hizo una propuesta sobre la posibilidad técnica de proporcionar respuesta a lo anterior; se comenzaba a delinear el principio de la radio celular, que entraría en servicio en distintos países a principios de los 80, con AMPS, NMT, ETACS, etc.

El 1974, la FCC proporcionó un ancho de banda de 40 MHz adicionales para el servicio de radio celular (825 a 845 MHz y 870 a 890 MHz). Estas bandas de frecuencias fueron previamente asignadas a los canales de televisión 70 a 83 de UHF. En 1975, se concedió a AT&T la primera licencia para operar un servicio de radio celular en desarrollo, en Chicago, AT&T subsecuentemente creó el Servicio de Telefonía Móvil Avanzado (AMPS).

El sistema celular AMPS usa una banda de frecuencia de 20 MHz compuesta de 666 canales con espacios entre canales de 30 kHz. Para las unidades móviles, el canal 1 tiene una frecuencia de transmisión de 825,03 MHz y el canal 666, en 889,98 MHz. Un espectro de frecuencias de 5 MHz adicional, se aumentó posteriormente a la banda de 20 MHz existente, lo cual incrementa el número total de canales disponibles a 832. El estándar celular TACS, estándar en Europa, utilizaba una banda de frecuencia de 15 MHz que abarca 600 canales con un espacio, entre canales, de 25 kHz.

Si nos centramos en Estados Unidos, en 1980, la FCC decidió dar una licencia de dos portadoras comunes por área de servicio. La idea era eliminar la posibilidad de un monopolio y proporcionar las ventajas que generalmente acompañan un ambiente competitivo. Subsecuentemente, surgieron dos sistemas de distribución de frecuencia, cada uno con su propio grupo de canales, sistema A y sistema B, para compartir el espectro de la frecuencia distribuida. El sistema A se definió para las compañías sin líneas fijas y el sistema B se definió para las compañías con líneas fijas, como se muestra en la figura 2.1.

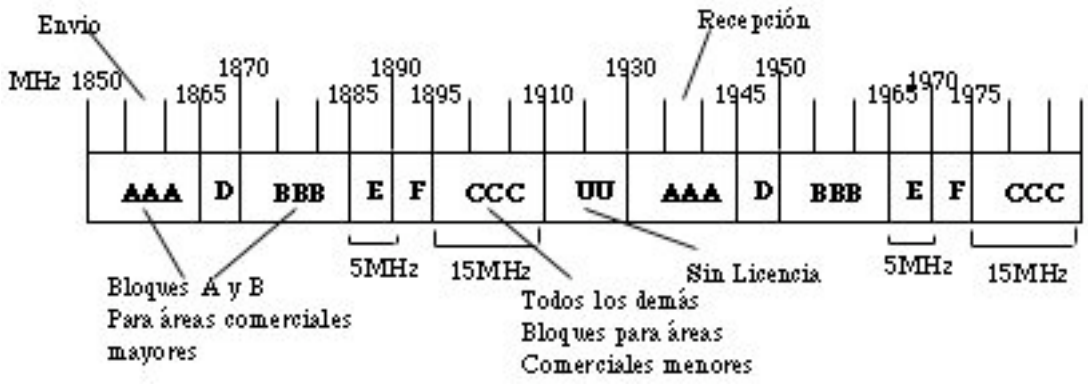


Figura 2.1 Sistema A y sistema B.

2.4 El ESTÁNDAR TACS

En Estados Unidos, Buffalo entro en servicio en abril de 1984. Nueve meses después, entro a su vez en servicio la primera red Móvil en el Reino Unido, por la empresa Vodafone, cuyo proveedor de servicio fue la empresa Sueca Ericsson.

A pesar de la rapidez con que siguió ésta red con respecto a la de Buffalo, la situación en el Reino Unido era distinta a la de Estados Unidos, y tenía algunas características propias importantes.

Mientras en Estados Unidos se daba el concurso para ver que proveedor suministraría la red móvil, el Reino Unido decidía sobre sus propios arreglos de telefonía móvil. En el invierno de 1981-1982, el gobierno Británico estableció un panel consultivo sobre la liberalización de servicios de valor agregado, con lo que nació el concepto de dúo polio. En éste dúo polio, BT (que iba a ser separada ya pronto de la división postal de la GPO) iba a ser uno de los operadores móviles, por medio de una filial llamada Cellnet, cuya propiedad compartiría con un co-propietario en minoría. Las solicitudes para la segunda licencia se sacaron a licitación.

Entre los solicitantes se encontraba Racal, que podía aportar una larga historia en el campo de la radio, y una empresa de riesgo conjunto con una compañía estadounidense llamada Millicom, ya involucrada en un ensayo de telefonía móvil en Estados Unidos. Racal fue elegida y se estableció con el nombre de Vodafone.

Luego se produjo una larga disputa entre BT y Vodafone por los estándares. BT favorecía el sistema de Siemens, mientras que Vodafone quería una variación del estándar estadounidense AMPS, con una separación de 25 KHz entre canales, en lugar de los 30 kHz estadounidenses. Vodafone comprendía que, para el abonado, el costo de entrada –representado en su mayor parte por el costo del teléfono- sería crítico. Su razonamiento era que éste último sería mas bajo si pudiera compartir su caparazón y una gran parte de sus componentes electrónicos con cualquier teléfono que fuera producido en serie para los Estados Unidos.

BT propuso una idea Francesa como alternativa, pero fue bloqueada de nuevo por Vodafone. BT sugirió entonces el estándar Nórdico NMT 450, pero Vodafone se mantuvo firme por considerar (con bastante certeza) que los volúmenes de NMT nunca podrían compararse con los de AMPS, y que el volumen reduciría el costo de la infraestructura y también el de los teléfonos. Además, abrigaba ciertas

dudas sobre la seguridad del sistema NMT. Al final, BT cedió, con lo que se adopto una versión Británica del AMPS, llamada TACS (Sistema de Comunicaciones de Acceso Total). Actualmente, Cellnet admite que fue la decisión correcta.

Después, Vodafone se puso a buscar su proveedor de infraestructuras. Poco a poco, redujo los contendientes a AT&T, Motorola y Ericsson, y eligió a ésta última debido a la gran capacidad del conmutador AXE. Creía que las mayores ciudades británicas necesitaban un conmutador grande, lo que disminuiría las transferencias de llamada y la señalización entre conmutadores. En aquella época, los conmutadores de AT&T y Motorola eran relativamente pequeños.

Vodafone, que había obtenido su licencia un año después que Cellnet, metió fuertes prisas a Ericsson, y la operación pudo comenzar el 1 de enero de 1985.

Un resultado interesante del enfoque del dúo polio en el Reino Unido fue el surgimiento del proveedor de servicios independiente; ni Cellnet ni Vodafone tenían permitido en un principio el acceso directo a los clientes, por lo que, en su lugar, se crearon una serie de empresas que se hicieran cargo de las conexiones, la venta y el servicio de los teléfonos móviles.

2.5 El ESTÁNDAR D-AMPS

También conocido como Servicio Digital de Telefonía Móvil Avanzado, DAMPS, es una segunda generación del servicio celular telefónico AMPS, solo que ahora es agregado el servicio digital, pues sigue funcionando la parte analógica de la red; al igual que su antecesor D-AMPS fue desarrollado en Estados Unidos, y en realidad fue una actualización de la red AMPS para incrementar la calidad y la capacidad de las redes celulares.

DAMPS usa las mismas bandas de frecuencia que AMPS (800 y 900 MHz), pero cada canal de 30 KHz creado con FDMA (Acceso Múltiple por División de Frecuencias) se divide en tres, usando TDMA (Acceso Múltiple por División de Tiempo), con lo cuál se triplica el número de canales, y en consecuencia el número de llamadas.

DAMPS, GSM y PDC, son tres tecnologías inalámbricas digitales que usan versiones no compatibles de TDMA.

El estándar digital del Japón se conoce por PDC, Personal Digital Cellular, y fue puesto en un principio en la banda de los 800 MHz , pero, poco después, se concedieron licencias a nuevos operadores regionales para introducir un servicio PCN Japonés en la banda de 1.5 a 1.6 GHz. El grupo Japonés Digital Phone , con Japan Telecom y PacTel como socios, tenían intereses en varias compañías que operaban a nivel regional y que ofrecían PCN, y eligió a la empresa Sueca Ericsson como proveedor. El 1 de marzo de 1994, antes del plazo contractual, entro en funcionamiento la primera red, que fue inaugurada el 15 de abril.

2.6 El ESTÁNDAR GSM

En lo referente a telefonía móvil en Europa existían dos estándares analógicos distintos, NMT y TACS, que luego se convirtió en ETACS (Sistema de Comunicaciones de Acceso Total Mejorado). El primero proporcionó en realidad el seguimiento del abonado entre los países nórdicos y algunos otros, como Suiza. Si embargo fue la CEPT, Conferencia Europea de las Administraciones y Telecomunicaciones, en sus preparativos para el importante paso en la telefonía Móvil Digital, la que

primero comprendió la necesidad de crear un estándar único paneuropeo –el estándar que se convirtió en GSM (que recibió en un principio el nombre de Grupo Especial Móvil, es decir, el grupo de trabajo de la CEPT)-. Esta norma europea fue creada para asegurar, por una parte, que cualquier abonado pueda usar su teléfono móvil en cualquier país de Europa y, por otra parte, que tanto los operadores como los abonados puedan comprar equipos y teléfonos móviles en un mercado abierto.

¿Qué ofrecía GSM que no tuvieran los sistemas analógicos?

Tiene varias ventajas, desde una mayor claridad de la voz, y el estar libre de escuchas furtivas hasta un mejor uso de las frecuencias. Con todo la ventaja principal es que la especificación de GSM ha sido desarrollada como estándar internacional, en sus orígenes paneuropeo, pero con una difusión rápida a la mayor parte del mundo.

El seguimiento internacional del abonado fue incorporado a la especificación técnica de GSM, sí bien mucho más importante aún fue el esfuerzo hecho por diversos organismos para conseguir la adhesión de todos los operadores europeos.

La primera necesidad fue una banda de frecuencias común. Ya en 1978, la CEPT había reservado dos bloques de 25 Mhz en la banda de 900 MHz. En 1982, creó un grupo de trabajo sobre normalización para la segunda generación móvil, el Grupo Especial Móvil (GSM), con representantes de 11 PTT´s europeas. El número de participantes y de aportaciones fue en aumento y, en 1985, el grupo fue dividido en cinco grupos menores de trabajo dedicados a aspectos específicos del sistema. En 1986 se formó una secretaría, llamada "el núcleo permanente".

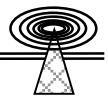
En 1988, todas las actividades del grupo CEPT sobre GSM fueron transferidas a una nueva organización, el Instituto Europeo de Normas de Telecomunicaciones ETSI. La participación en él no se limita a la PTT´s , sino que incluye miembros de otros operadores, grupos de usuarios –y fabricantes-. Da la casualidad de que el grupo GSM ya había invitado a una gama similar de representantes para que participara a partir de 1987.

Una característica clave de GSM es el principio de interfaz "abierto".

Con interfaces abiertos entre los componentes de un sistema, pueden ser integrados en éste los componentes de cualquier fabricante, a condición de que sus interfaces correspondan a las especificaciones publicadas. Lo que pase dentro del componente, no importa, y ello permite a cada fabricante incorporar tecnología y funcionalidad patentadas, siempre y cuando los interfaces se adapten al conjunto.

La finalidad de GSM fue crear condiciones para conseguir una red internacional de telefonía móvil sin costuras, así como disponer el escenario para la competencia y para una adquisición abierta, con objeto de impedir que un fabricante, u operador, imponga una solución patentada en todo el mercado, y cree así, un monopolio.

La incorporación de interfaces abiertos en la estructura del sistema GSM fue una política oficial de la Comunidad Europea, diseñada para fomentar la competencia entre proveedores de sistemas y operadores, asi como, es preciso señalarlo, para permitir que los pequeños fabricantes pudieran entrar también en el mercado GSM.



Los operadores europeos firmaron un acuerdo, el MoU de GSM, en Copenhague en 1987, que fue una respuesta a la necesidad de cooperación en cuestiones comerciales y operacionales, tales como la programación temporal para adquisición y despliegue de redes; la compatibilidad de planes de numeración y encaminamiento; la armonización de la introducción del servicio; y los procedimientos de tarifación y contabilidad. Una vez terminadas las especificaciones de GSM en 1988, los operadores comenzaron a enviar solicitudes de ofertas.

2.7 El ESTÁNDAR CDMA

CDMA (Code Division Multiple Access, acceso múltiple por división de código) es un nuevo concepto en las comunicaciones radiofónicas. Ha ganado una aceptación general por los operadores de sistemas radio celulares como una actualización que incrementará notablemente la capacidad del sistema y la calidad del servicio. Este sistema ha sido elegido por la mayoría de los ganadores de las subastas de licencias que se han hecho en EEUU para dar servicios celulares.

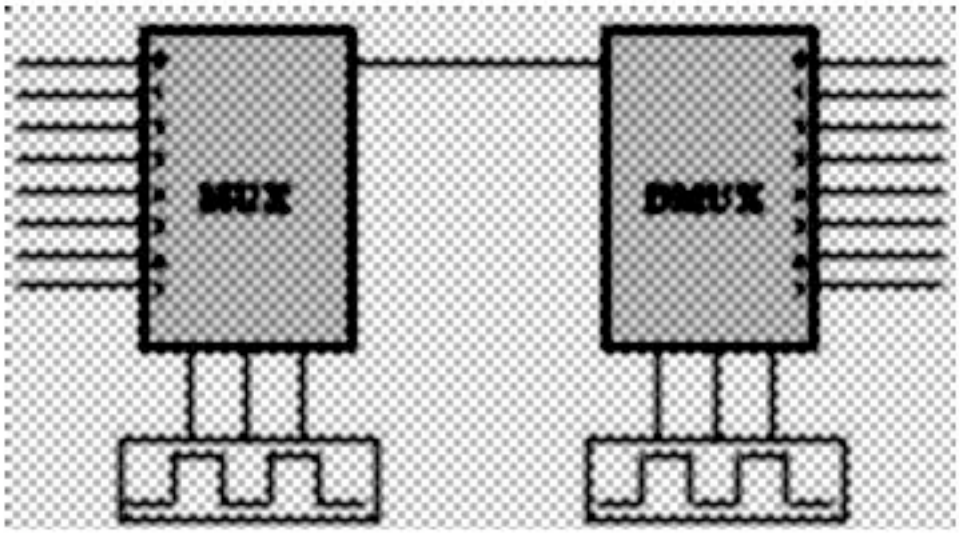
Al principio no estaba muy claro si CDMA era una mejor opción que las otras dos técnicas tradicionales: TDMA (sistema de acceso utilizado por GSM) y FDMA. Viterbi comparó la capacidad de CDMA en aplicaciones para satélites con las otras dos técnicas y no quedó claro cual era mejor. Pero esto cambió al observar que CDMA era robusto ante las interferencias. Este factor provoca un aumento en la capacidad del sistema y que viene muy bien en aplicaciones de voz.

El origen de esta tecnología está en las comunicaciones militares, al tratar de rechazar enérgicamente las interferencias provocadas, superponiéndose a ellas y asegurando las comunicaciones mediante códigos, lo que por otro lado no es sino lo que se desea alcanzar en las comunicaciones móviles celulares.

El primer punto a considerar es que en CDMA todos los usuarios, mientras duran sus comunicaciones, ocupan la totalidad del ancho de banda asignado a cada estación base, que puede ser de varios Mhz. Tanto en FDMA como en TDMA hay una separación de las señales de cada usuario, bien en frecuencia o bien en tiempo, mientras que en CDMA todos los usuarios en comunicación se están interfiriendo mutuamente, como grupos de parejas hablando en una recepción en la que mientras todo el mundo está hablando a un determinado nivel de volumen, cada persona se concentra en lo que dice su interlocutor, al menos que sobrevenga alguna información excepcional.

CAPÍTULO 3

TECNOLOGÍAS DE ACCESO



Como consecuencia del aumento en el número de abonados, el tamaño de las redes telefónicas y su infraestructura creció de manera significativa, por lo que el número de cables en los postes de las calles se incrementaba a grado tal que era prácticamente imposible un crecimiento mayor dentro del espacio de una ciudad, por muy grande que ésta fuera. El problema entonces era reducir la infraestructura de transmisión, por lo que se recurrió a la técnica llamada Multiplexaje, donde varias llamadas telefónicas comparten un medio de transmisión común. Y puede ser por medio del Multiplexaje por división de frecuencias, por división de tiempo o por división de código. Estas técnicas de multiplexaje no solo son usadas en las redes de cable, también son empleadas en redes celulares para compartir los canales de radio; a continuación se detallan tres de las técnicas de multiplexaje de mayor uso en las redes tanto fijas como celulares.

3.1 FRECUENCY DIVISION MULTIPLEXING ACCESS

En FDMA, el espectro de frecuencias se divide entre los canales lógicos, donde cada uno de los usuarios posee una banda de frecuencias en exclusiva.

En la figura 3.1 se muestra como tres canales de calidad telefónica se multiplexan mediante FDMA. Unos filtros delimitan el ancho de banda útil a cerca de 3000 Hz por canal de calidad telefónica. Cuando se multiplexan varios canales, se asignan 4000 Hz a cada canal, con objeto de mantener una buena separación entre ellos. Primero, se eleva la frecuencia de los canales de voz, en diferente grado para cada uno de ellos. Después, se pueden combinar, dado que ahora ningún par de canales ocupan la misma parte del espectro. Nótese que aun cuando existen intervalos (es decir, bandas de seguridad) entre los canales, hay un solape entre canales adyacentes, pues los filtros no tienen caídas abruptas en sus extremos. Este solape significa que un parásito grande, en el extremo de un canal, se sentirá en el adyacente, como ruido no térmico.

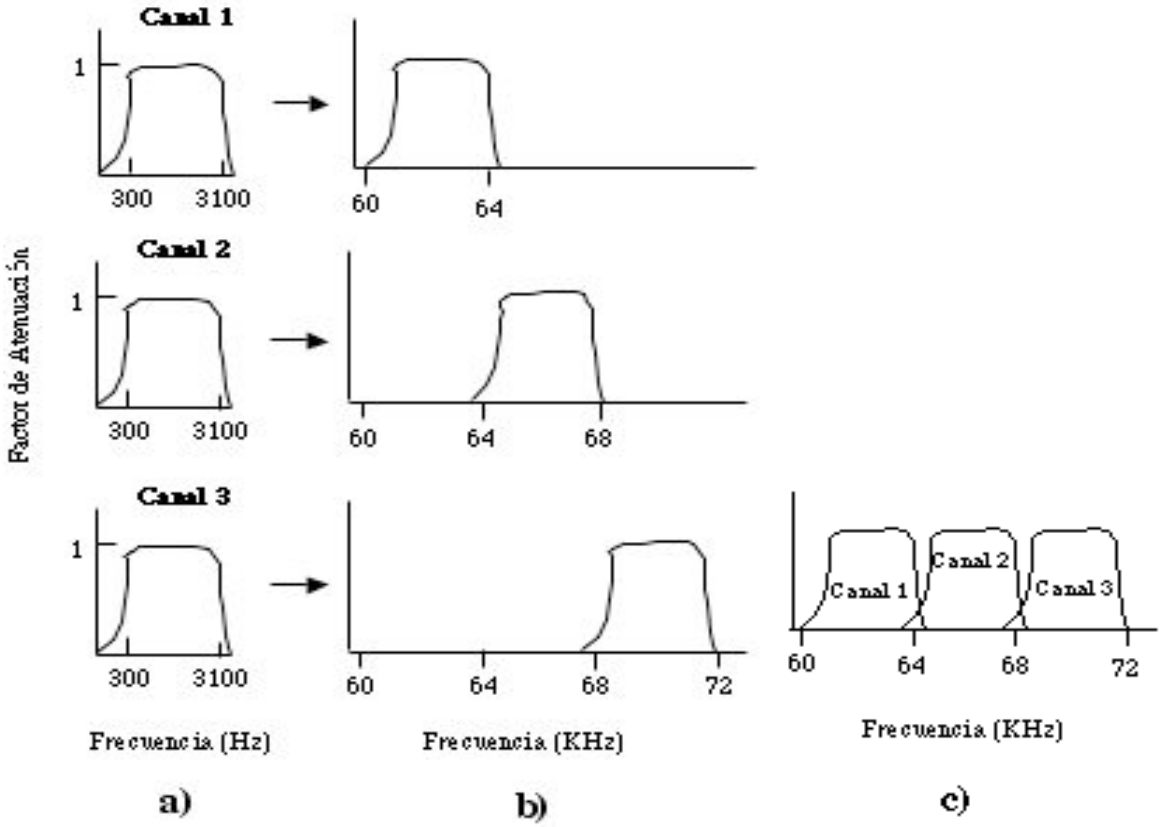
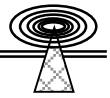


Figura 3.1 Multiplexaje por división de frecuencia, a) Anchos de banda originales, b) Los anchos de banda elevados en frecuencia, c) El canal Multiplexado.

Los esquemas de FDMA que se utilizan en el mundo entero están, hasta cierto grado, normalizados. Una norma de gran uso es la correspondiente a 12 canales de voz de 4000 Hz (de los cuales 3000 Hz son del usuario, más dos bandas de seguridad de 500 Hz cada una), multiplexados en la banda de los 60 a los 108 kHz. A esta unidad se le llama *grupo.* Algunas veces, la banda de 12 a 60 kHz se llega a utilizar para otro grupo. Muchos proveedores de servicios portadores ofrecen a sus clientes una línea alquilada de 48 a 56 kbps, basada en un grupo. Se pueden multiplexar cinco grupos (60 canales de voz), para formar un supergrupo. La siguiente unidad es el *grupo maestro,* que esta constituido por cinco súper grupos (de acuerdo con la norma del CCITT), o por diez súper grupos (de acuerdo a Bell System). Existen otras normas hasta un máximo de 230000 canales de voz.

Los primeros sistemas de multiplexaje por división de frecuencias se diseñaron para usar el ancho de banda de cables portadores tipo cuartos, para comunicación de larga distancia. El ancho de banda de dichos cables era mayor que el de los cables usados para redes locales y de junción y, por tanto, eran más caros. Además, se necesitaba amplificadores para la comunicación de larga distancia, por lo que era esencial que esos circuitos caros de larga distancia pudieran manejar simultáneamente más de un circuito de comunicación, por razones económicas.

En los primeros sistemas portadores se ensamblaban grupos de 12 canales, como se ilustra en la figura 3.2, ocupando un ancho de banda de 60 a 108 kHz. Este grupo de 12 canales podía usarse



para modular la amplitud de una frecuencia de 120 kHz portadora de grupo, y la banda lateral inferior filtrada, para que los canales originales fueran ensamblados en un ancho de banda de 12 a 60 kHz, y así transmitirlos en el cable portador como un sistema de multiplexaje de 12 canales.

Sin embargo, un segundo grupo de canales podía ensamblarse en el ancho de banda de 60 a 108 kHz, como se ilustra en la figura 3.2 y agregarse a los 12 canales originales para dar un sistema de multiplexaje por división de frecuencia de 24 canales en el ancho de banda de 12 a 108 kHz.

Número de Canal	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Frecuencia Portadora (kHz)	108	104	100	96	92	88	84	80	76	72	68	64
Banda lateral inferior (kHz)	104.6 –107.7	100.6-103.7	96.6 -99.7	92.6 -96.7	88.6 -91.7	84.6 -87.7	80.6 -83.7	76.6 -79.7	72.6 -75.7	68.6 -71.7	64.6 -67.7	60.6 -63.7

Figura 3.2 FDMA; Tabla de frecuencias y canales originales.

3.2 TIME DIVISION MULTIPLEXING ACCESS

En la década de los 50´s, AT&T Bell labs y Western Electric Manufacturing introdujeron un nuevo sistema de portadora (carrier) a ser usado tanto en redes telefónicas locales así como en redes telefónicas de larga distancia. Este nuevo sistema de portadora (carrier) , llamado "portadora-T" (T-carrier), utiliza transmisión digital en lugar de analógica.

Debido a los muchos avances en la electrónica de estado sólido y los circuitos integrados para manipular señales digitales, los sistemas telefónicos se orientan en dirección de redes completamente digitales. El nuevo sistema convierte voz e información de señalización analógica a señales digitales para su transmisión.

Hay tres técnicas empleadas para la transmisión digital de señales digitales: Pulse Amplitud Modulation (PAM) Modulación por Amplitud de Pulsos, Pulse Code Modulation (PCM) Modulación por Codificación de Pulsos, y Time Division Multiplexing Access (TDMA) Multiplexaje por División en el Tiempo.

3.2.1 Pulse Amplitud Modulation PAM

La voz humana puede ser desplegada por medio de un osciloscopio, y se ve como una onda o función senoildal. Una muestra de ésta señal u onda senoidal, tomada en un instante de tiempo, puede

cercanamente representar la señal en cualquier lado del punto de muestra para el mismo instante de tiempo.

Si la señal es muestreada al doble rango del componente de la frecuencia más alta en la señal, las muestras contendrán toda la información contenida en la señal original.

En el caso de la señal telefónica, desde que el ancho de banda para el canal de voz fue definido en 4000 Hz, el rango de la muestra de 8000 muestreos por segundo fue suficiente para reproducir la señal.

La señal obtenida por éste tipo de muestreo consistirá de pulsos de frecuencia constantes. La amplitud de estos pulsos será igual a la amplitud de la señal muestreada, en el momento del muestreo. Estos pulsos son modulados en amplitud, y éste proceso es llamado Modulación por Amplitud de Pulsos (PAM por sus siglas en Inglés).

Estos pulsos muestreados pueden ser enviados en un canal digital, y cuando ésta pasa al final de su camino por un filtro, se obtiene la señal original de entrada antes del muestreo.

Sin embargo, PAM tiene algunos problemas durante la transmisión de la señal. Cualquier distorsión o ruido introducido no puede ser corregido durante el viaje de la señal, y, a la salida de la señal, los pulsos se dispersan e interfiere con otras señales. Este problema hace que la señal sea difícil de recuperar.

En la figura 3.3 se muestra en diagramas de bloque el proceso de muestreo realizado para Modular una señal por Pulsos.

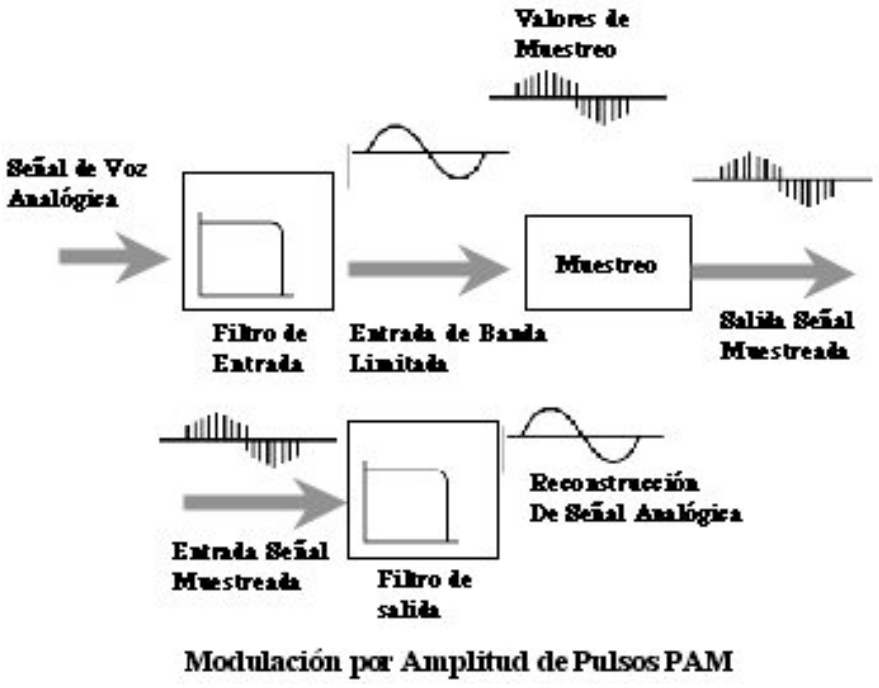


Figura 3.3 Muestreo de PAM.

3.2.2 Pulse Code Modulation

Ahora, cuando la información contenida en la amplitud de la señal muestreada se convierte en un número, o cuantificada, ese número puede ser entonces codificado en bits para ser transmitidos.

Nota: Un bit es la cantidad mínima de información procesada o almacenada de manera digital, y puede ser representado por medio de un "1" o un "0", en algunos textos se identifica como "HIGH" o "LOW" o sea "NIVEL ALTO" o "NIVEL BAJO".

Cuando la información es codificada en dígitos binarios (bits), y no en amplitud, entonces aunque la amplitud de los pulsos varíe, no afectara la información; en la fig. 3.4 se muestra PCM.

3.2.3 Cuantización

Un circuito llamado cuantizador toma una muestra de la señal analógica y produce un equivalente numérico (número) de la misma señal. Ahora, éste número es usualmente un valor aproximado del valor real de la señal, la diferencia entre los dos valores es conocido como error de cuantizacion, este error causa un "ruido de cuantizacion" que puede ser escuchado en el auricular telefónico como cuando se habla arrastrando la letra "s", también conocido como "hissing".

3.2.4 Codificación

Una vez que la muestra de señal analógica es cuantificada en un número, dicho número debe ser traducido en un número binario. Este circuito que traduce o convierte el numero cuantificado en un número binario se conoce como codificador (encoder o coder). Y el circuito que realiza la función contraria, o sea, convertir un número binario en un número cuantificado se conoce como decodificador (decoder). La combinación de ambos circuitos es conocida como CODEC (Codec-DECoder) CODificador / DECodificador.

El CODEC también ajusta el intervalo de la señal cuantificada en relación a la señal de entrada, lo cuál da como resultado una señal comprimida a la salida. Al final del proceso el CODEC COMPANDER (COMpressor / exPANDER).

-Compresor / Decompresor- restaura la señal, lo cuál reduce el ruido de cuantización.

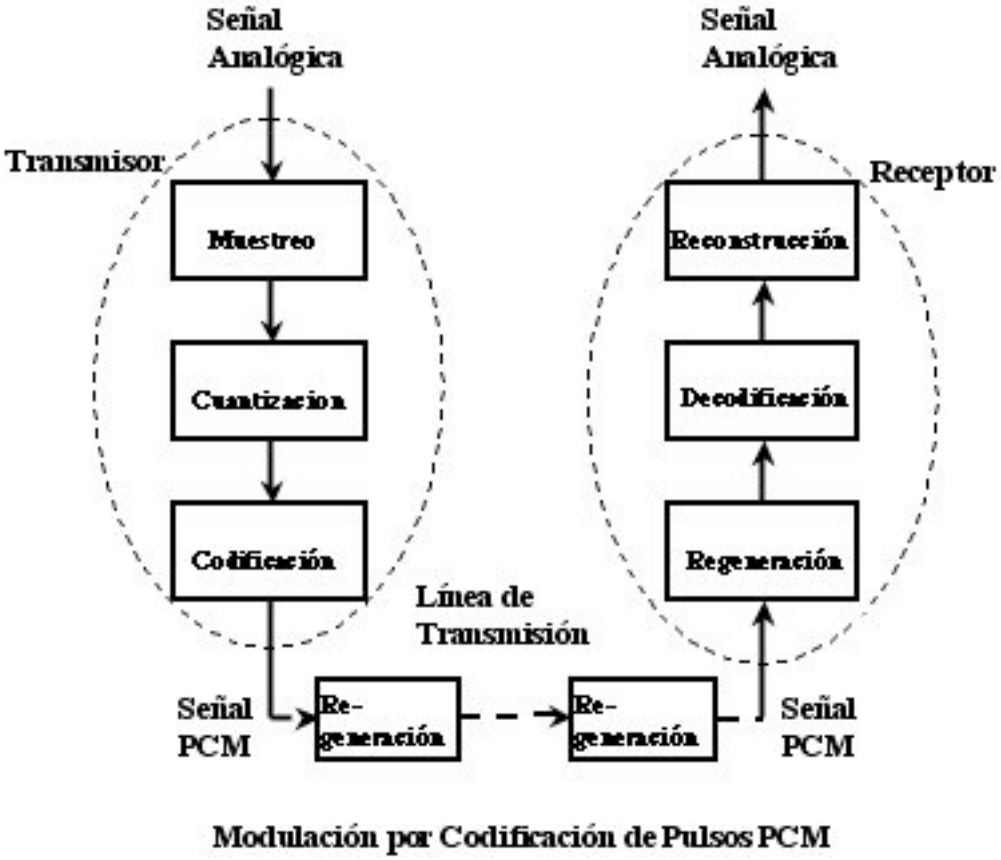


Figura 3.4 Modulación por Codificación de Pulsos (PCM).

3.2.5 Time Division Multiplexing Access

Una vez que la señal de voz ha sido muestreada, cuantificada y codificada en forma digital, es tiempo de transmitirla a su destino. El Multiplexaje por División de Tiempo (TDMA) figura 3.5, divide la capacidad de transmisión del canal en periodos muy cortos de tiempo, dejando pasar las diferentes señales en cada uno de estos periodos, de forma tal que por un solo canal es posible transmitir varias señales sin necesidad de variar la frecuencia; esto gracias a que los periodos de tiempo (del orden de los milisegundos ms) son tan pequeños que, por ejemplo, por un canal pueden estar pasando 20 llamadas telefónicas a la vez sin que exista interferencia alguna entre ellas; y esto es posible gracias a que el oído humano es incapaz de percibir los cambios "switch" de señal que ocurren mientras escucha la llamada telefónica, por ende para el oído humano estos cambios son imperceptibles.

TDMA trabaja con señales binarias provenientes de pulsos, en forma de ceros "0" y unos "1". Estos pulsos pueden ser de una muy corta duración y seguir representando la información deseada.

Los códigos binarios (señales digitales) pasan serialmente bit por bit. En lugar de que una sola señal analógica ocupe la totalidad de un canal, varias señales digitales serán mezcladas por un patrón definido (TDMA) en un solo canal.

El canal 2 es multiplexado detrás del canal 1, el canal 3 será multiplexado detrás del canal 2, el canal 4 será multiplexado detrás del canal 3 y asi seguirán el proceso un canal detrás de otro, sin nunca llegar a mezclarse.

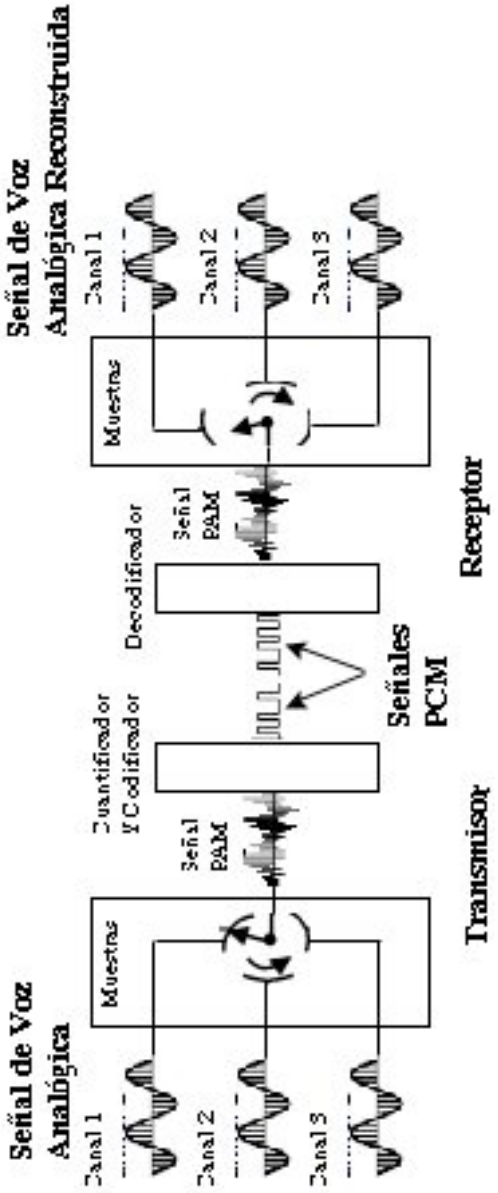


Figura 3.5 Time División Multiplexing Access TDMA.

3.2.6 Convertidores

Los convertidores se encuentran en cada extremo de la transmisión digital de canales en la Red Telefónica Pública de Circuitos Conmutados (PSTN-Public Switched Telephone Network). Estos convertidores realizan el muestreo, la cuantización y la codificación necesaria para transformar la señal analógica de voz en bits.

En la PSTN muchos canales digitales deben usar un esquema común para las conversiones análogo-digital. Este esquema es llamado la ley-μ.

De acuerdo a ésta ley el codificador producirá una salida de 8-bits, con un bit usado como bit de señalización ("1" para positivo, "0" para negativo), quedando los restantes 7 bits como el valor absoluto de la señal de entrada.

Partiendo de que el rango de muestreo es de 8000 muestras por segundo, el rango de datos para un canal individual de voz usando codificación por la ley-μ es:

8000 muestras por segundo X 8 bits por muestra = 64000 bits por segundo. El rango de transmisión de muchas facilidades digitales es mucho más alto que éste, porque muchos canales son multiplexados juntos.

El sistema de convertidores de la compañía Bell Labs es llamado tipo-D (D-type) donde la "D" es por digital y forma la fundación por una completa serie de multiplexores.

3.2.7 Convertidores Tipo-D

Un convertidor "D", figura 3.6, multiplexa 24 canales de voz, para formar una señal "DS-1". La salida de un convertidor tipo-D es una señal digital de 1.544 Mbps llamada "DS-1". La señal "DS-1" contiene la secuencia de bits con la señal de voz.

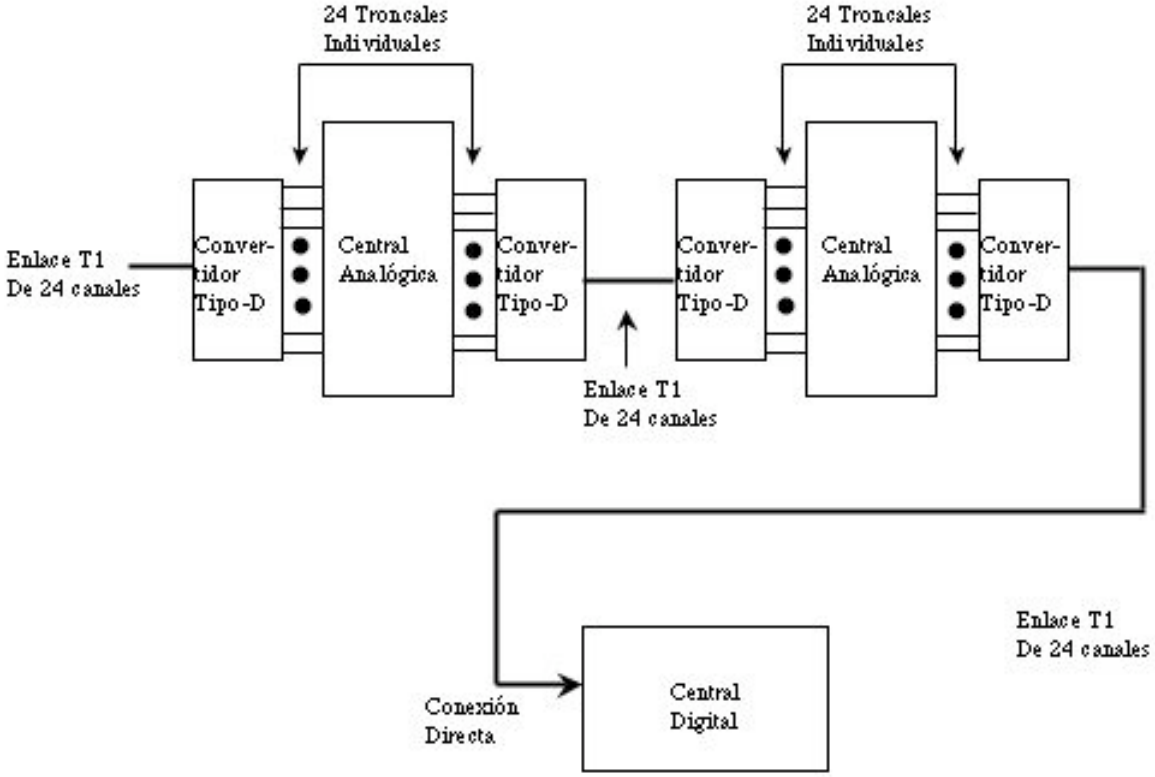


Figura 3.6 Convertidor Tipo-D.

3.2.8 Sistemas de Portadora-T (T-Carrier Systems)

La señal "DS-1" es usada en los sistemas digitales de Portadora "T1", figura 3.7, de Bell Labs (1962). Portadora Digital es lo mismo que PCM.

Las líneas digitales son catalogadas por el número de bits transmitidos por segundo.

Para la línea de transmisión T1:

- Cada uno de los 24 canales recibidos contienen palabras de 8 bits

  8 X 24 = 192

- Después de cada trama (frame) de 192 bits, es insertado 1 bit, para sincronización.
  192 + 1 = 193
- Hay 8000 tramas (frames) por segundo
  8000 X 193 = 1544000 bits

Por simplificación, el rango de transmisión de una línea "T1", es manejado como 1.544 Mega bits por segundo (1.544 Mbp/s). Esto representa el máximo número de bits que pueden ser transmitidos en cada segundo si todas las posiciones en la línea fueran utilizadas.

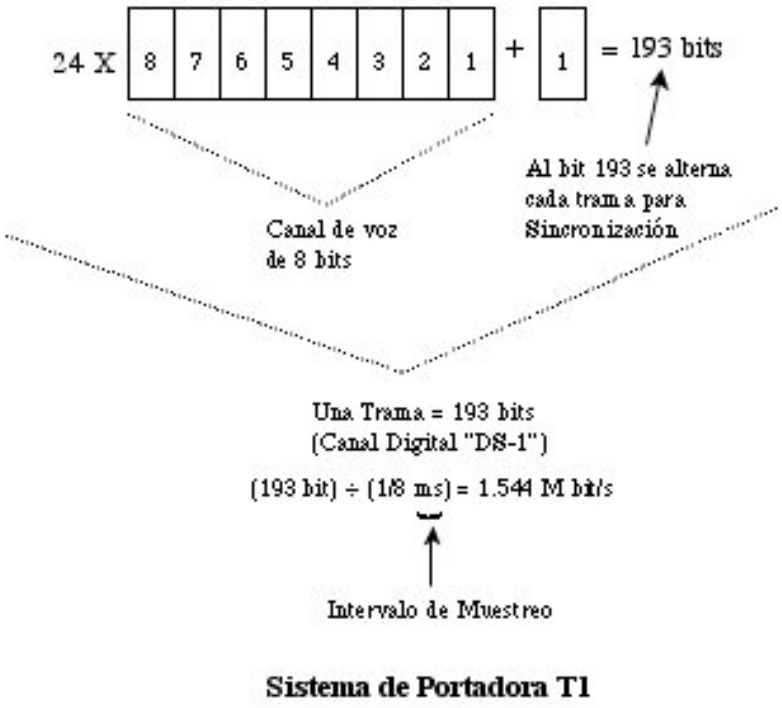


Figura 3.7 Sistema de Portadora T1 (T1 Carrier System).

Portadora T1

La portadora (carrier) digital T1, tiene 24 canales de voz, y es usada para comunicación Inter-centrales o Inter-oficinas, que están separadas por una distancia no mayor a 80 Km (50 millas). Repetidores regenerativos de la señal son requeridos aproximadamente cada 1.6 Km (1 milla). Cada línea T1 opera a un rango de datos (bit rate) de 1.544 Mbps.

Portadora T2

La portadora (carrier) digital T2, tiene 96 canales de voz y es usada para enlazar puntos separados hasta por 800 Km (500 millas). Los repetidores se necesitan aproximadamente cada 4.8 Km (3 millas).

Para lograr un T2 se utilizan 4 señales TDMA DS-1, que nos dan una señal digital DS-2, que es usada como una portadora T2. Cada línea T2 opera a un rango de datos (bit rate) de 6.312 Mbps.

Portadora T3

Una portadora T3 está compuesta de 28 señales TDMA DS-1, que a su vez forman una señal DS-3, que tiene 672 canales de voz. Cada línea T3 opera a un rango de datos (bit rate) de 44736 Mbps.

Portadora T4M

La portadora (carrier) digital T4M tiene 4032 canales de voz y es típicamente usada en rutas de 800 Km (500 millas) o menos de distancia; en la figura 3.8 se muestra completa la jerarquía TDMA.

Una portadora T4M está compuesta de 6 señales TDMA DS-3, que a su vez forman una señal digital T4M. Cada línea T4M opera a un rango de datos (bit rate) de 274.176 Mbps.

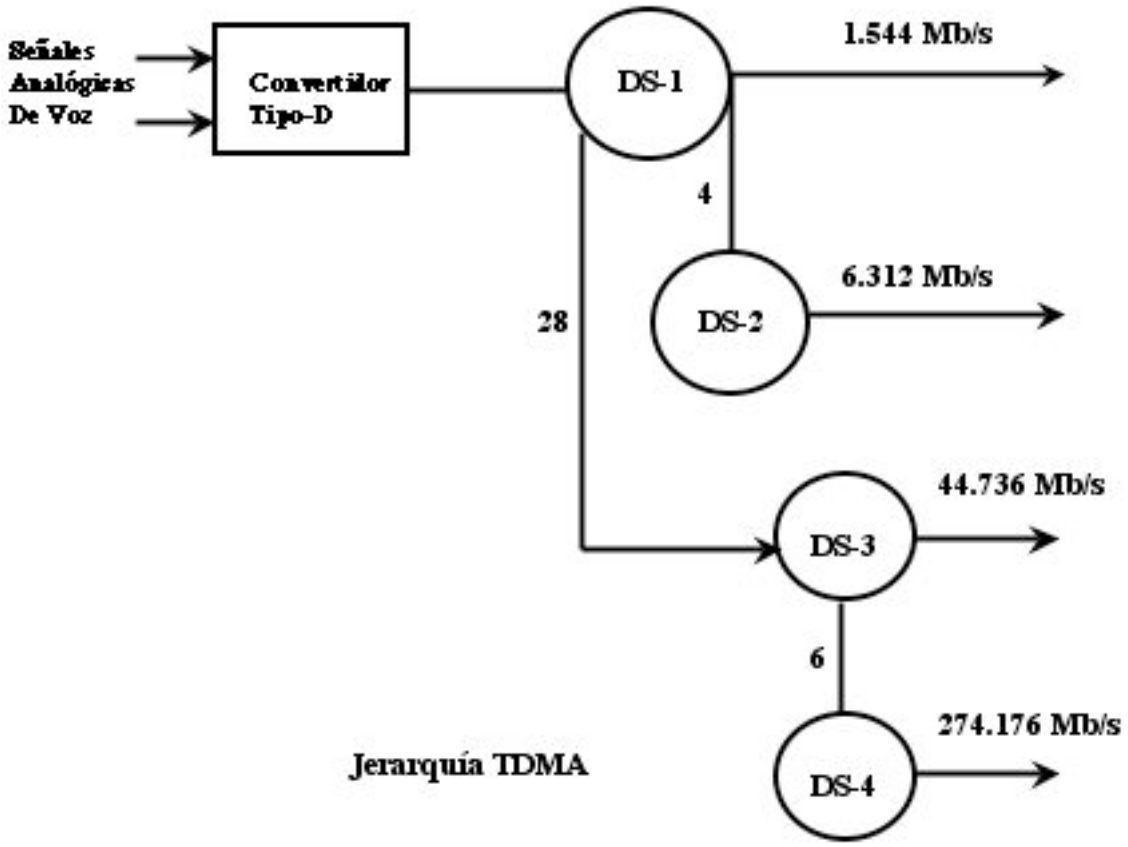


Figura 3.8 Jerarquía TDMA

3.2.9 Sistema de Portadora-E (E-Carrier System)

E1 (o E-1) es un formato de transmisión digital Europeo legado por la ITU-TS y nombrado por la Conference of European Postal and Telecommunication Administration (CEPT). Es el equivalente del formato Norteamericano de portadora T (T Carrier).

Los E2 hasta los E5 son portadoras (carriers) que se incrementan como múltiplos del E1.

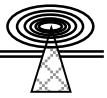
El rango de transmisión del formato de señal E1 es de 2048 millones de bits por segundo (Mbps) y puede manejar 32 canales de 64 Kbps cada uno.

E1 maneja rangos de información más altos que T1 (el cual maneja 1544 Mbps), y esto es porque, a diferencia de T1, no hace bit-robbing y los 8 bits por canal son usados para codificar la señal. E1 y T1 pueden ser usados en interconexiones internacionales.

E2 (E-2) es una línea que pede manejar 4 señales E1 multiplexadas con un rango de datos de 8448 Mbps.

E3 (E-3) puede manejar 16 señales E1 con un rango de datos de 34368 Mbps

E4 (E-4) maneja cuatro canales E3 con un rango de datos de 139264 Mbps.



E5 (E-5) maneja cuatro canales E4 con un rango de datos de 565148 Mbps.

3.3 CODE DIVISIÓN MULTIPLEXING ACCESS

CDMA (Code Division Multiplexing Access) es un nuevo concepto en las comunicaciones radiofónicas. Ha ganado una aceptación general por los operadores de sistemas radio celulares como una actualización que incrementará notablemente la capacidad del sistema y la calidad del servicio.

Al principio no estaba muy claro si CDMA era una mejor opción que las otras dos técnicas tradicionales: TDMA (sistema de acceso utilizado por GSM) y FDMA. Viterbi comparó la capacidad de CDMA en aplicaciones para satélites con las otras dos técnicas y no quedó claro cual era mejor. Pero esto cambió al observar que CDMA era robusto ante las interferencias. Este factor provoca un aumento en la capacidad del sistema y que viene muy bien en aplicaciones de voz.

El origen de esta tecnología está en las comunicaciones militares, al tratar de rechazar enérgicamente las interferencias provocadas, superponiéndose a ellas y asegurando las comunicaciones mediante códigos, lo que por otro lado no es sino lo que se desea alcanzar en las comunicaciones móviles celulares.

El primer punto a considerar es que en CDMA todos los usuarios, mientras duran sus comunicaciones, ocupan la totalidad del ancho de banda asignado a cada estación base, que puede ser de varios Mhz. Tanto en FDMA como en TDMA hay una separación de las señales de cada usuario, bien en frecuencia o bien en tiempo, mientras que en CDMA todos los usuarios en comunicación se están interfiriendo mutuamente, como grupos de parejas hablando en una recepción, en la que mientras todo el mundo está hablando a un determinado nivel de volumen, cada persona se concentra en lo que dice su interlocutor, al menos que sobrevenga alguna información excepcional.

Si cada pareja hablara y entendiera un único idioma, su capacidad de dialogar, con un alto nivel de interferencia, sería mucho mayor, debido a la exclusividad del lenguaje. Este es el principio de supresión de interferencia utilizado en CDMA, donde las comunicaciones de cada móvil, con su estación base se produce con una particular codificación semejante al uso de un solo idioma. Si además la codificación fuera ortogonal y las comunicaciones sobre un canal ideal, los usuarios ignorarían totalmente cualquier interferencia intercelular.

Se ha dicho que cada usuario transporta su señal utilizando la totalidad del ancho de banda disponible en su emplazamiento y como éste ancho de banda es mucho mayor que la señal del mensaje del usuario, se produce un proceso de ensanchamiento del espectro, inevitable debido al uso de un código único asignado a cada usuario.

Típicamente una señal de voz será una codificación binaria seguida por una codificación de canal y el entrelazado. El código único asignado a cada usuario consta de impulsos binarios denominados CHIP. La duración del código es idéntica a la duración de

los bits del mensaje codificado y hay "G" CHIPS en cada uno de estos. Cada bit codificado se reemplaza por el código si el bit codificado es un 1 lógico, o cada CHIP en el código tiene su polaridad invertida si el bit codificado es un 0 lógico.

El ancho de banda de la señal codificada se multiplica aproximadamente por "G", asumiendo la modulación binaria, con lo que "G" se constituye en un factor de ganancia. Aunque el ancho de banda de la señal ha sido ensanchado por el proceso de codificación, la densidad espectral de potencia PSD, en W/Hz consecuentemente se ha estrechado y la señal es más parecida a un ruido. Cuanto mayor sea "G", más ancho de banda y menor PSD, con lo que aumenta la posibilidad de convivir con la interferencia. De ésta manera, cada uno de los usuarios tendrá sus propios bits de codificación de mensaje representado por "G" CHIPS, y el código reside en el esquema binario de CHIPS.

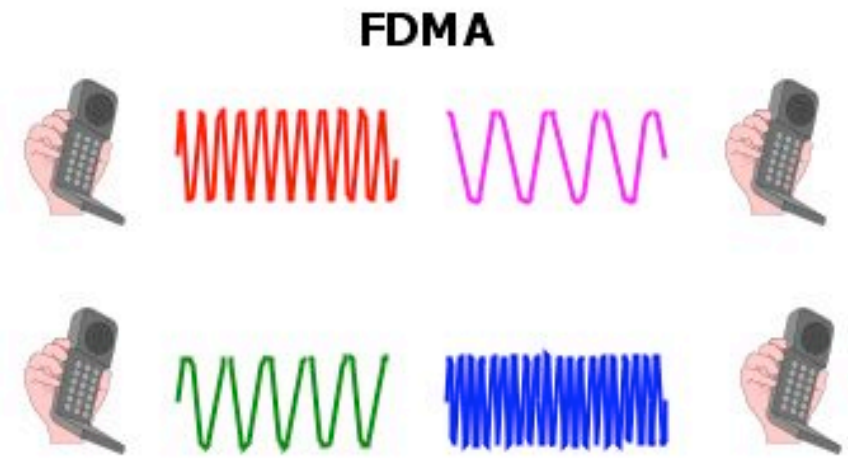
Para las comunicaciones desde la estación base hacia los móviles, las señales ensanchadas de cada usuario se combinan y aplican a un modulador. Un determinado móvil, después de demodular la señal de RF se presenta junto con todas las demás señales CDMA, y de la misma manera en los enlaces móvil-base, ésta recibe todas las señales CDMA y decodifica cualquiera de ellas en presencia de todas las demás. Mezclando la totalidad de las señales con el código único asignado a un móvil determinado, resulta que la señal de este móvil aparece reconstruida. Para apreciar esta reconstrucción se supone que el código tiene chips cuyos niveles de voltaje son +/- 1 y son multiplicados por sí mismo. El resultado es un nivel de voltaje 1, es decir, no hay cambios mientras dura el código. Evidentemente esta técnica precisa de un perfecto sincronismo entre las señales de entrada CDMA con el código generado en el receptor.

Mientras que la señal deseada ha sido reconstruida gracias a la recuperación de la señal del mensaje original, todas las otras señales CDMA han sido multiplicadas por medio de un código compuesto por muchos chips que mantienen su amplio ancho de banda. El resultado es que sólo aquellos componentes de frecuencia del amplio ancho de banda que interfieren a las señales CDMA que están en la banda del mensaje de la señal deseada, causan interferencia, que equivale a decir que las interferencias de los otros usuarios del espectro han sido divididas por G.

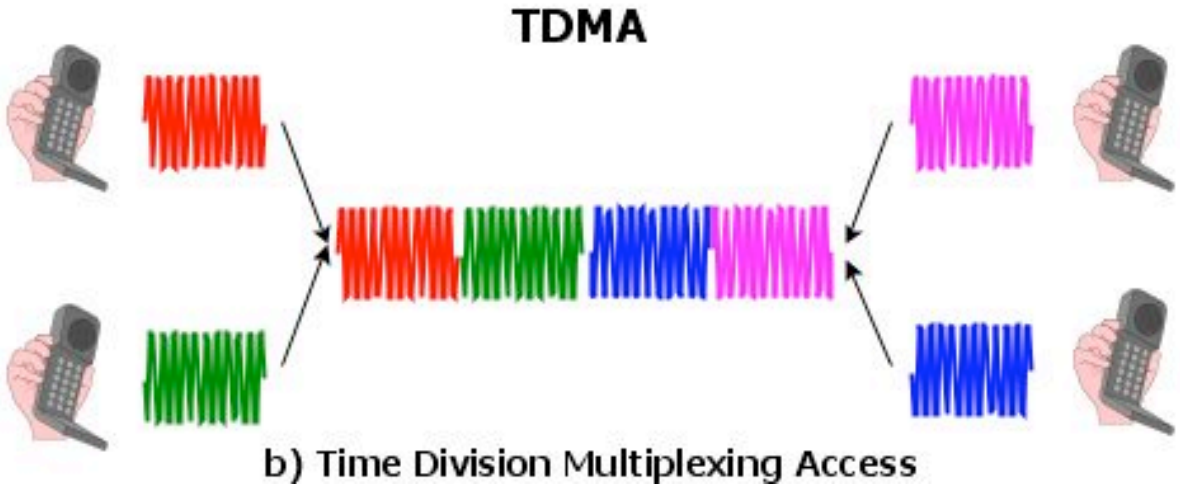
La tecnología CDMA permite usar retículas con una sola célula, es decir, no tener retículas sino sólo células, lo que bajo un punto de vista de eficiencia espectral resulta inmejorable. Pero es más, si se utiliza la sectorización, todos los sectores en cada célula pueden utilizar las mismas frecuencias, y ello produce un incremento fenomenal de la capacidad del sistema. Las interferencias procederán de otros sectores y células, pero las pérdidas de capacidad debidas a estas interferencias están más que compensadas por el aumento de capacidad generado por el uso de una célula por retícula y por la sectorización, eliminando además la planificación de frecuencias.

Otra característica de CDMA es la forma en que efectúa el handover (traspaso entre células), que es siempre blando (soft handover), ya que no hay cambios de frecuencia durante el proceso, de forma que en la frontera de las células, dos estaciones base comunican simultáneamente con la estación móvil que se desplaza, lo que resulta más favorable para las comunicaciones y proporciona mejor calidad de voz en los extremos de las células comparado con los sistemas FDMA y TDMA.

En la figura 3.9 se muestra la forma en que cada tecnología de acceso maneja las señales de información.



a) Frecuency Division Multiplexing Access



b) Time Division Multiplexing Access

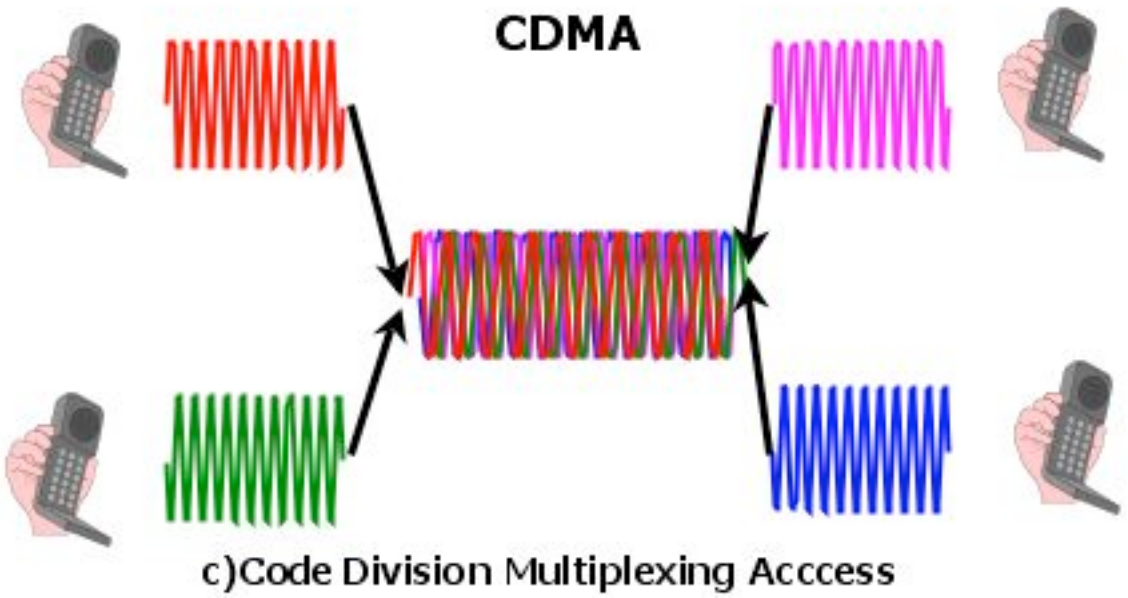
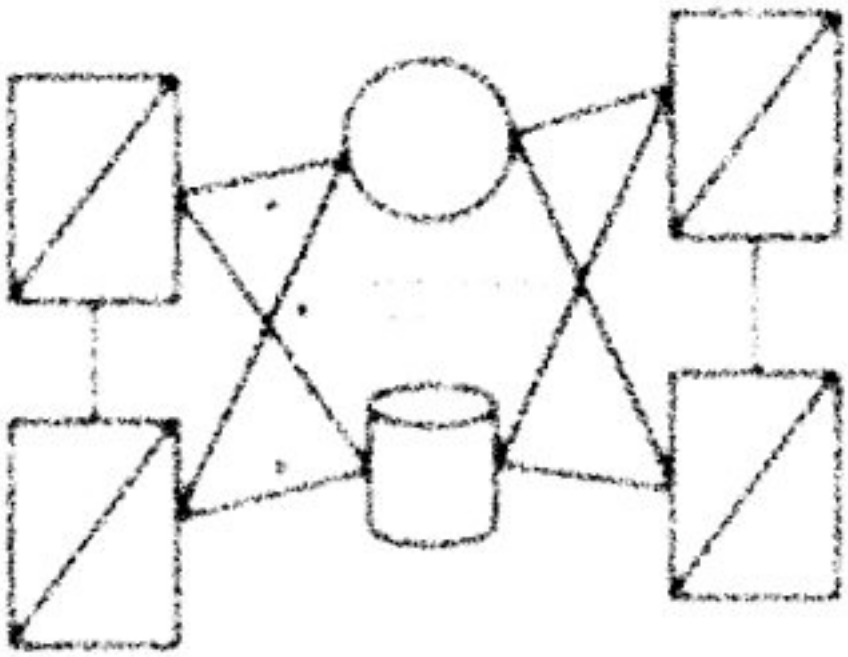


Figura 3.9 Tecnologías de Multiplexaje; a) FDMA Frecuency Division Multiplexing Access (pag. Anterior) b) TDMA Time Division Multiplexing Access (pag. Anterior) c) Code Division Multiplexing Access.

CAPÍTULO 4

SEÑALIZACIÓN



SEÑALIZACIÓN

4.1 Introducción

La principal función de la señalización en las redes de telecomunicaciones modernas, donde diferentes nodos (equipos) de red deben cooperar y comunicarse entre si, es habilitar y controlar la transferencia de información entre dichos nodos con:

- El establecimiento, la supervisión y la liberación de conexiones y servicios en redes de telecomunicaciones (llamadas de voz, datos, etc.) figura 4.1a
- Requerimientos de servicios específicos en bases de datos, el servicio de Roaming en redes celulares, actualizaciones en las bases de datos, etc. figura 4.1b
- Procedimientos de manejo de red. Figura 4.1c

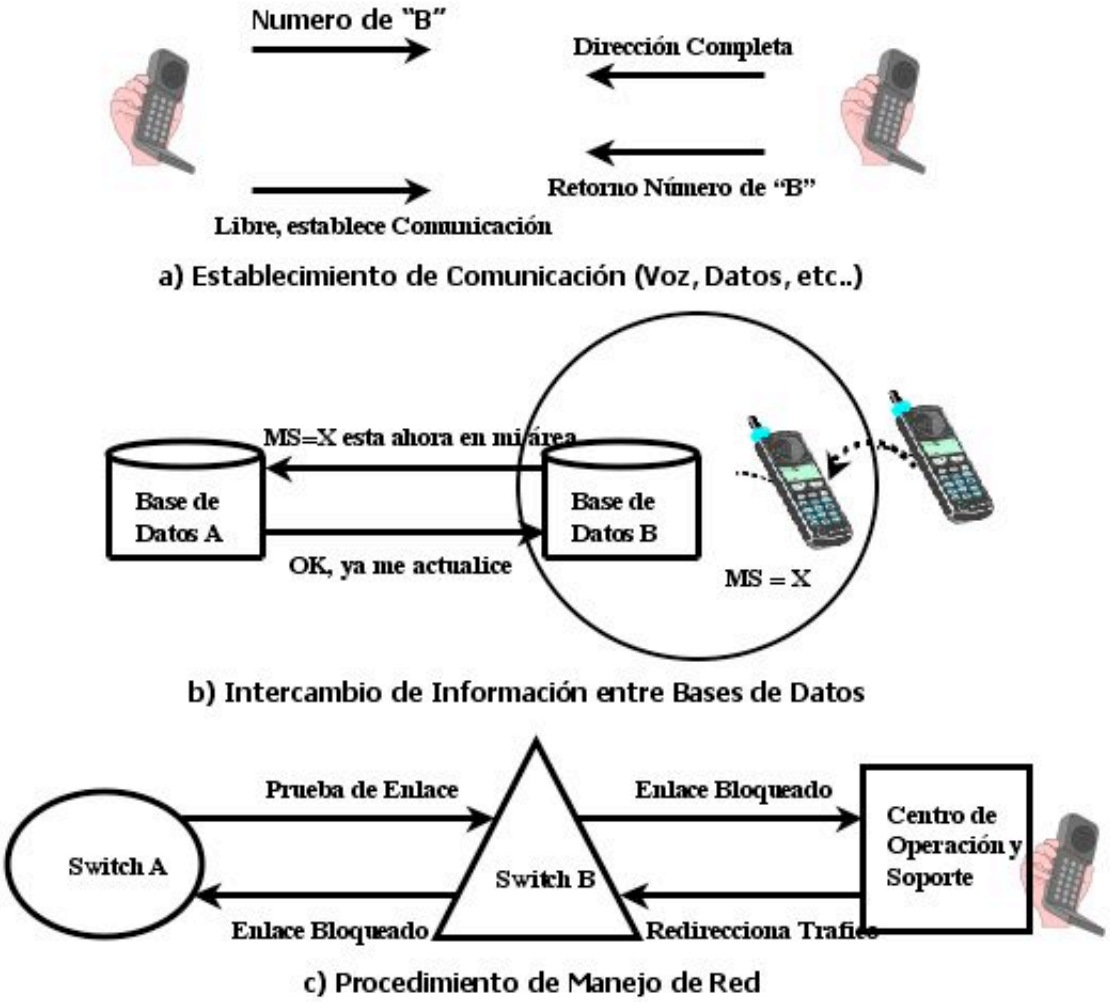


Figura 4.1 Diferentes usos de la Señalización.

La información de señalización a ser transferida depende del tipo de conexión que se desee establecer (Voz, datos, Texto e Imágenes) y de los requerimientos específicos de la aplicación que se usara. El procedimiento de establecimiento de comunicación siempre requerirá de la transferencia de la información de direcciones. Por ejemplo para una llamada de Voz, la información de direcciones es

transferida de la parte que inicia la llamada (usualmente conocida como lado o suscriptor A) a la parte que recibe la llamada (usualmente conocida como lado o suscriptor B). Todo intercambio de información que es utilizado en el establecimiento de la llamada necesita de ésta información de direcciones para poder establecer y seleccionar una conexión adecuada entre las dos partes.

Además de la información de direcciones, algunos servicios necesitan información especifica, como por ejemplo bearer capability, la cual deberá ser enviada como parte de la señalización durante el establecimiento de la comunicación. Después de que el lado "B" ha sido encontrado e identificado, alguna información de señalización será transferida de regreso (al lado A) indicando el estado del lado "B" (libre, ocupado, congestión, etc.). En otras palabras, la rutina de uso de señalización es de todos los días en el establecimiento de la comunicación entre usuarios o partes de la redes de telecomunicaciones.

La señalización también es usada durante la liberación de una conexión para indicar el fin de la misma, detener el proceso de cobro por la comunicación y preparar recursos para nuevas conexiones.

Diferentes tipos de bases de datos han sido sucesivamente implementados como parte de las funciones de redes de telecomunicaciones modernas, con objeto de soportar servicios de redes inteligentes "IN" (tarjetas de crédito, números de acceso universal, y otros tipos de comunicaciones). Lo cual implica el constante intercambio de información de señalización entre las bases de datos (también conocidas como Service Control Points – SCP y Service Data Points – SDP) y los nodos de red (Service Switching Points – SSP), estos nodos de red pueden ser por ejemplo centrales telefónicas.

En redes celulares, existe una gran necesidad por el uso de señalización, por ejemplo entre las bases de datos HLR (Home Locator Register) y VLR (Virtual Locator Register) con las terminales móviles (teléfonos celulares). Esta señalización es necesaria para ubicar la posición geográfica de cada estación móvil (mejor conocido como Roaming) y también para el establecimiento y liberación de las llamadas. Otros ejemplos del uso de la señalización en el manejo de procedimientos de redes celulares son: mensajes indicando cambios temporales en la red, bloqueo o desbloqueo de equipo de switcheo, re-enrutamiento de trafico, etc.

La señalización es utilizada por todo tipo de telecomunicaciones que requieran de intercambio de señales; ahora, para detallar un poco más esto, se dará un acercamiento a la estructura funcional de las redes de telecomunicaciones. La actual división entre las facilidades de red (bearer networks) ilustra el amplio rango de actividades, servicios, etc. en las telecomunicaciones y la necesidad de señalización. En estos días la funcionalidad en redes de telecomunicación es de dos tipos principalmente: circuitos conmutados (circuit-switched) y paquetes conmutados (packet-switched). Los principales usuarios de funciones de señalización en las redes basadas en circuitos conmutados son:

- PSTN – Public Switched Telephone Network con teleservicios para intercambiar voz, texto y datos. Servicios suplementarios como desvió de llamada y llamada en espera también son provistos por la señalización.
- CSPDN – Circuit Swtched Public Data Network con teleservicios para Circuit Switch Data (datos por circuitos conmutados – vía MODEM).

  Las aplicaciones típicas son en agencias de viajes, gasolineras de auto-servicio, etc.

- ISDN – Integrated Services Digital Network que permite a los usuarios el acceso a servicios integrados de voz, datos, texto e imágenes desde un solo punto de conexión.
- PLMN – Public Land Mobile Network con teleservicios para voz, fax y datos para terminales móviles y servicios suplementarios relacionados a las mismas.

Existen diferencias significativas en el manejo y transferencia de información de señalización en las redes de circuitos conmutados, en comparación con los procedimientos correspondientes usados en las redes de paquetes conmutados, ver figura 4.2. En las redes de circuitos conmutados la información de señalización es manejada y distribuida por un equipo especifico de señalización, funciones y canales de señalización. Esta amplia gama de versiones y tipos de equipos de sistemas de señalización, especialmente en aplicaciones de telefonía, crean problemas entre las redes algunas veces.

La razón de la existencia de un largo número de sistemas de señalización se debe en gran medida al largo desarrollo en los sistemas de telefonía (más de un siglo). Diferentes culturas y diferentes filosofías en el desarrollo tecnológico son otros factores que influenciaron la situación actual. Sin embargo, los organismos de estandarización como ITU-T (anteriormente CCITT) han definido y estandarizado un número limitado de sistemas de señalización, los cuales se encuentran ahora en amplio uso en redes de telecomunicación locales e internacionales. Y en el caso de las redes basadas en paquetes conmutados se utilizan protocolos de señalización, lo cual simplifica de manera importante el tamaño de las redes, asi como su diseño.

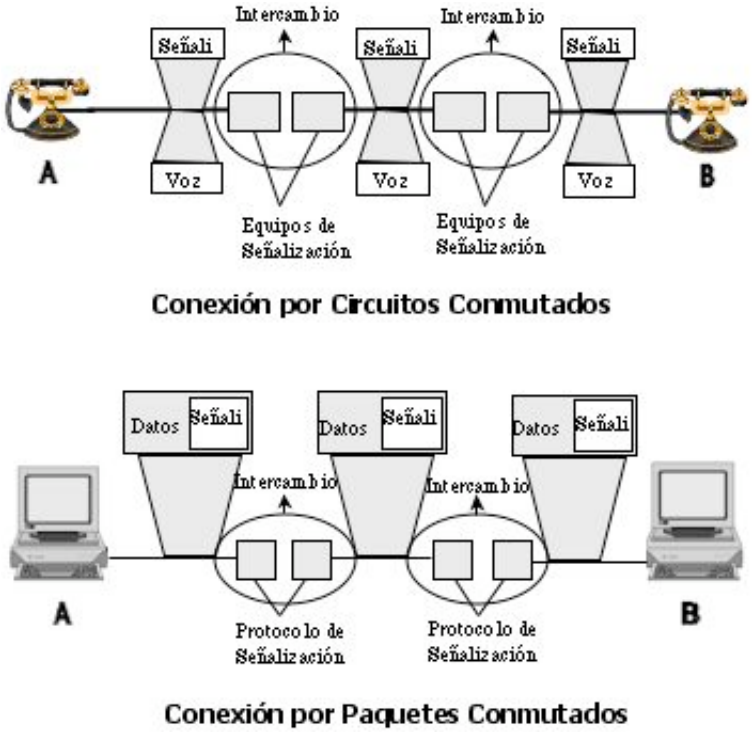


Figura 4.2 Ejemplificación gráfica de los distintos procesos de señalización en Circuitos Conmutados y Paquetes Conmutados.

4.2 ESTRUCTURA GENERAL DE LA SEÑALIZACIÓN SS7

El sistema de señalización SS7 juega hoy en día un muy importante papel en la gran mayoría de las redes de circuitos conmutados, y probablemente éste sistema de señalización será desarrollado más fuertemente para aplicaciones futuras de mayor ancho de banda.

4.2.1 Señalización No. 7 (SS7)

SS7 está basado en protocolos de señalización que semejan de manera cercana otras formas de protocolos de comunicación de datos en los cuales toda la información es transferida en mensajes etiquetados. Esto es debido a que toda la información de señalización es transferida en un canal separado (conocido como time slot en la transmisión digital), que es independiente de los canales de comunicación de trafico, el uso de ruteo flexible en los mensajes de señalización sobre enlaces alternos es muy seguro. El resultado es alta confiabilidad; por ejemplo, si un enlace de señalización falla, el tráfico de señalización podrá entonces ser re-enrutado por el enlace alterno (también llamado redundancia). SS7 ha sido diseñado con el fin de proveer diferentes grupos de usuarios con su propio arreglo (set) de mensajes. Esto facilita la implementación de nuevos mensajes para un grupo de usuarios especifico, sin afectar otros grupos de usuarios en el sistema. Los grupos típicos de usuarios en aplicaciones de telecomunicaciones utilizando señalización SS7 son servicios PSTN, ISDN, PLMN e IN, asi como servicios de comunicación de datos tanto para redes fijas como para redes celulares.

Conceptos Básicos de Señalización

Una de las mas distintivas y ventajosas características de SS7 es la eliminación de toda la información de señalización de las troncales de voz y la creación de canales específicamente diseñados para llevar señalización. En SS7 la separación entre tráfico y señalización es posible gracias al uso de la Señalización de Canal Común (Common Channel Signaling). Para entender mejor estos conceptos, se analizaran los dos tipos básicos de señalización: Señalización por Canal Asociado (Channel Associated Signaling -CAS) y Señalización por Canal Común (Common Channel Signaling –CCS).

4.2.2 Señalización por Canal Asociado (CAS)

La señalización por canal asociado, es la vieja forma de señalizar. Bajo éste sistema, tanto la información de voz como la información de señalización se transportaba por una sola troncal de comunicación. La gran desventaja de éste tipo de señalización es que la troncal de voz debe estar reservada mientras la señalización establece la llamada. Si el abonado al que se llama esta ocupado o por alguna razón se encuentra no disponible, la llamada deberá ser pagada ya sea por proveedor de servicio o por el usuario, debido a que la troncal de voz ya había sido reservada, o sea se ocupa de todas formas. No hay forma de saber el estado del abonado al cual se llama para de esta forma no tener que reservar una troncal de voz y tener que incurrir en un costo. Aunque CAS fue usado ampliamente entre centrales telefónicas, ha sido reemplazado casi en su totalidad por CCS.
CAS es comúnmente referido a la señalización In-Band.

4.2.3 Señalización por Canal Común (CCS)

En la señalización por canal común (CCS), señalización y voz son transmitidos por canales separados de un mismo enlace. Una troncal de voz nunca portara ninguna información de señalización. El uso de CCS permite a la red saber el estado del abonado con el que se desea establecer una

comunicación antes de asignar un canal de voz, y a diferencia de CAS, esto permite que los costos bajen de manera importante.

Aunque es obvio que CCS es mas eficiente en términos económicos, hay algunas otras ventajas que no son tan evidentes. Por ejemplo, como las troncales de voz no son requeridas a menos que la llamada sea completada, el número de troncales de voz puede ser reducido, reduciendo los costos aun más. Otro beneficio a considerar es la reducción de tiempo para el establecimiento de la llamada. Debido a la velocidad de los enlaces de señalización (de hasta 64 Kbps), el tiempo total usado para establecer una llamada (determinado por el estado del abonado que recibe la llamada y el tiempo de transmisión de los dígitos marcados) es considerablemente menor en CCS en comparación con CAS.

CCS es algunas veces mencionado como señalización Out-Band, debido a que dicha señalización es transmitida por un canal diferente al que transmite el trafico.

4.3 FUNCIONES DE TRANSFERENCIA DE LOS MENSAJES DE SEÑALIZACIÓN

4.3.1 Formatos de Mensajes de Señalización

Un mensaje creado por ISUP (ISDN User Part) esta basado en reglas predefinidas por la ITU. En SS7 una parte de la información relativa al mensaje es definida como una Unidad de Señal del Mensaje (Message Signal Unit MSU). El MSU es enviado desde ISUP a el MTP, quien agrega información adicional de cabecera necesaria por el receptor MTP/SP para controlar el proceso de transferencia del mensaje. De ésta forma la información de señalización relativa al mensaje junto con la información de cabecera forman la estructura final de un MSU en la cual cada mensaje de señalización es transferido entre dos partes sobre un enlace común de señalización. En la parte que recibe el mensaje la información de cabecera es usada por el MTP para controlar el proceso y la información relativa al mensaje es direccionada al TUP.

La Parte de Transferencia del Mensaje (MTP)

La parte de transferencia del mensaje (Message Transfer Part MTP) provee las funciones básicas que habilitan la parte significativa de la información del usuario a ser transferida a través de la red SS7 del SP (Signalling Point) que envía al SP que recibe. Funciones adicionales son incluidas para asegurar que todos los mensajes sean transferidos libres de error, en el orden correcto y sin pérdidas o duplicación de la misma. Sobretodo el MTP es diseñado para funcionar solo en transferencias de señalización en redes de telefonía basadas en circuitos conmutados como especificación inicial de SS7 (1980).

La funcionalidad de la arquitectura de SS7 se ilustra por un modelo de referencia de cuatro niveles. En éste modelo el MTP se refiere a los niveles del 1 al 3. Las funciones principales de los niveles del MTP son definidas a continuación:

- Nivel 3: Funciones de Señalización de la Red (Signalling Network Functions)
- Nivel 2: Funciones de Señalización del Enlace (Signalling Link Functions)
- Nivel 1: Funciones de Señalización del Enlace de Datos (Signalling Data Link Functions)

El nivel 3 define dos funciones principales:

- Funciones para manejo de MSU´s entrantes y salientes

- Funciones de manejo de señalización de la red.

Basado en sus direcciones, los MSU´s entrantes son clasificados como MSU´s finales o MSU´s para transferencias futuras. Los MSU´s finales son entregados al receptor del mensaje que los requiere. Los MSU´s restantes son direccionados a un enlace de señalización saliente para transferencias futuras. Las funciones de manejo, administran la señalización de la red (pruebas iniciales, envio de mensajes de manejo a MTP´s involucrados, etc.). El nivel 2 define todas las funciones necesarias para manejar cada enlace de señalización, funciones que aseguran la transferencia libre de error en el orden correcto y sin pérdidas o duplicación de MSU´s. La señalización terminal (o final) también pertenece a este nivel. Pero además la información de cabecera de los MTP mencionada anteriormente es agregada a (o retirada de) los MSU´s en éste nivel. El nivel 1 define las funciones de las interfaces mecánicas y eléctricas para conexión de la señalización terminal (o final) a la otra parte, para la conexión de un enlace en la red, etc.

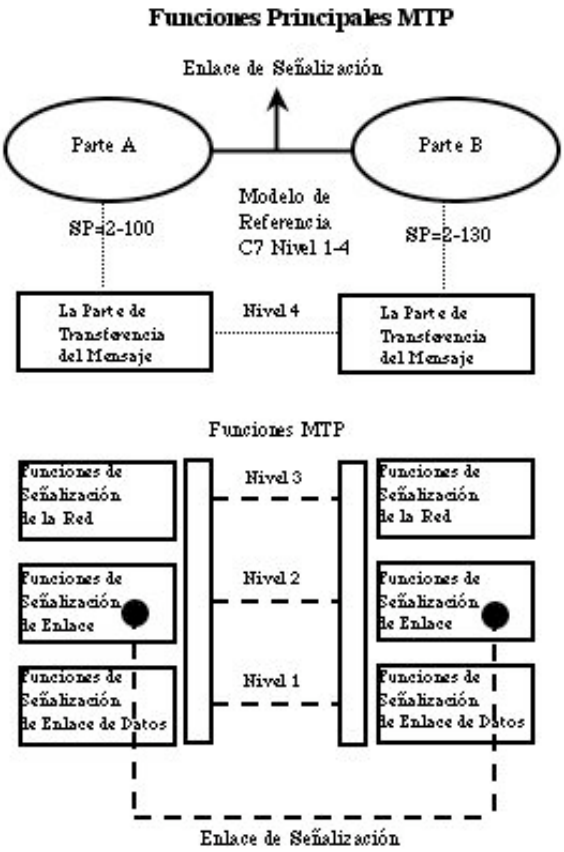


Figura 4.3 La parte de Transferencia de Mensaje MTP

Signalling Connection Control Part (SCCP)

A medida que han surgido nuevos requerimientos, para transferencia de información de señalización no relacionada a circuitos, servicios de red orientados a conexión y para más funciones avanzadas de ruteo y direccionamiento en la red de señalización, ha sido necesario agregar nuevas funciones a el MTP.

En lugar de cambiar las especificaciones iniciales de el MTP, los diseñadores han definido y estandarizado funciones adicionales conocidas como Signalling Connection Control Part SCCP, (parte de

señalización de control de conexión), la cual fue especificada en su primera versión en 1984. La SCCP complementa la MTP proveyendo ambos servicios de red, "connectionless" y "connection-oriented" para la transferencia de información de señalización orientada a conexión y no orientada a conexión. Las funciones SCCP son usadas para la interacción de bases de datos en la red (por ejemplo Home Location Register HLR y Visitor Location Registers VLR, para redes celulares). Otro ejemplo es la interacción entre un Service Switching Point (SSP) y un Service Control Point (SCP) para el manejo de los servicios en una IN (Inteligent Network). En el modelo de referencia SS7 el SCCP esta relacionado al nivel 4, el cual desde el punto de vista de el MTP es un User Part (TUP, ISUP, etc.). Pero el SCCP puede ser también relacionado al modelo de referencia OSI. En éste modelo el SCCP contribuye con la capa 3 del modelo de referencia OSI en la red de servicio.

El SCCP se especifica en las recomendaciones de la ITU-T´s Q.711 , Q.714 y Q.716.

La parte de Servicio de Red (Network Service Part - NSP)

El MTP define la plataforma básica para transferencia de todo tipo de mensajes de señalización y es siempre requerido. Pero algunas aplicaciones también necesitan las funciones provistas por el SCCP, lo cual quiere decir que tanto las funciones del SCCP como del MTP cooperaran en este tipo de aplicaciones.

La combinación de estos dos conceptos define la plataforma completa que provee la transferencia de mensajes de señalización, tanto orientada a conexión como no orientada a conexión, usando servicios de red "connectionless" o "connection-oriented". Esta combinación de MTP+SCCP es llamada la Network Service Part NSP.

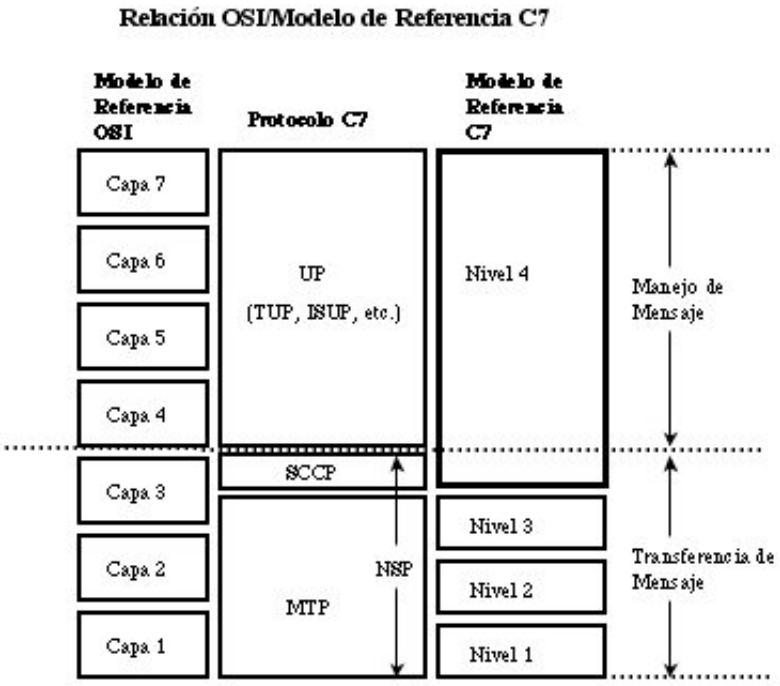


Figura 4.4 Relación OSI / Modelo de Referencia SS7

4.3.2 Unidades de Señalización (Signal Units SU)

El sistema de señalización SS7 esta basado en una estructura de comunicación de paquetes de datos, lo que significa que los mensajes de señalización son transferidos en la red de señalización en la

forma de paquetes de datos. En el sistema SS7 estos paquetes de datos son usualmente llamados Unidades de Señalización (Signal Units SU). Una unidad de señalización es por definición una porción de información. La estructura de esta información puede variar dependiendo de donde fue originalmente generada. La unidad de Señalización pueden ser generadas en el nivel 4 por un user part, o también pueden ser generadas en el nivel 3 (mensajes de manejo de / hacia el MTP).

Una característica común de todas las unidades de señalización es la estructura principal, la cual divide el contenido de la información en:

- Información de Señalización relativa al mensaje
- Información del mensaje relativa a la cabecera

Tres tipos de unidades de señalización han sido definidas:

a) Message Signal Unit (MSU)
b) Link Status Signal Unit (LSSU)
c) Fill in Signal Unit (FISU)

Unidades de Mensaje de Señalización (Message Signal Unit - MSU)

La versión de la unidad de señalización usada por los mensajes del user Part (del / hacia el nivel 4) y para los mensajes de manejo del MTP o mensajes de prueba y mantenimiento (de / hacia el nivel 3) es conocido como Message Signal Unit (MSU). Este mensaje de señalización esta definido por todos los parámetros en el campo de la información de la señalización (Signalling Information Filed SIF) de el MSU. Para habilitar a el MTP a transferir sobre un enlace de señalización todo tipo de US´s libres de error, en el orden correcto y sin pérdida o duplicación; información extra para las funciones del enlace debe ser añadida en el nivel 2 de cada unidad de señalización. Esto es reflejado por los parámetros principales añadidos. Los cuales se agregan a cada unidad de señalización antes de ser enviada por el enlace físico (the signalling data link).

4.3.3 Funciones de Manejo de Mensajes de Señalización (Signalling Message Handling Functions)

El establecimiento, supervisión y liberación de las conexiones de tráfico, asi como los procedimientos relacionados a servicios suplementarios, son las acciones principales entre las partes que establecerán una comunicación. Por ésta razón es necesario el intercambio de información. Esta información que es producida principalmente por el tráfico o los procedimientos del manejo del servicio dentro del intercambio de información, es empaquetado en mensajes de señalización y transmitido sobre la red de transmisión entre las partes comunicadas o también conocidas como MSU´s.

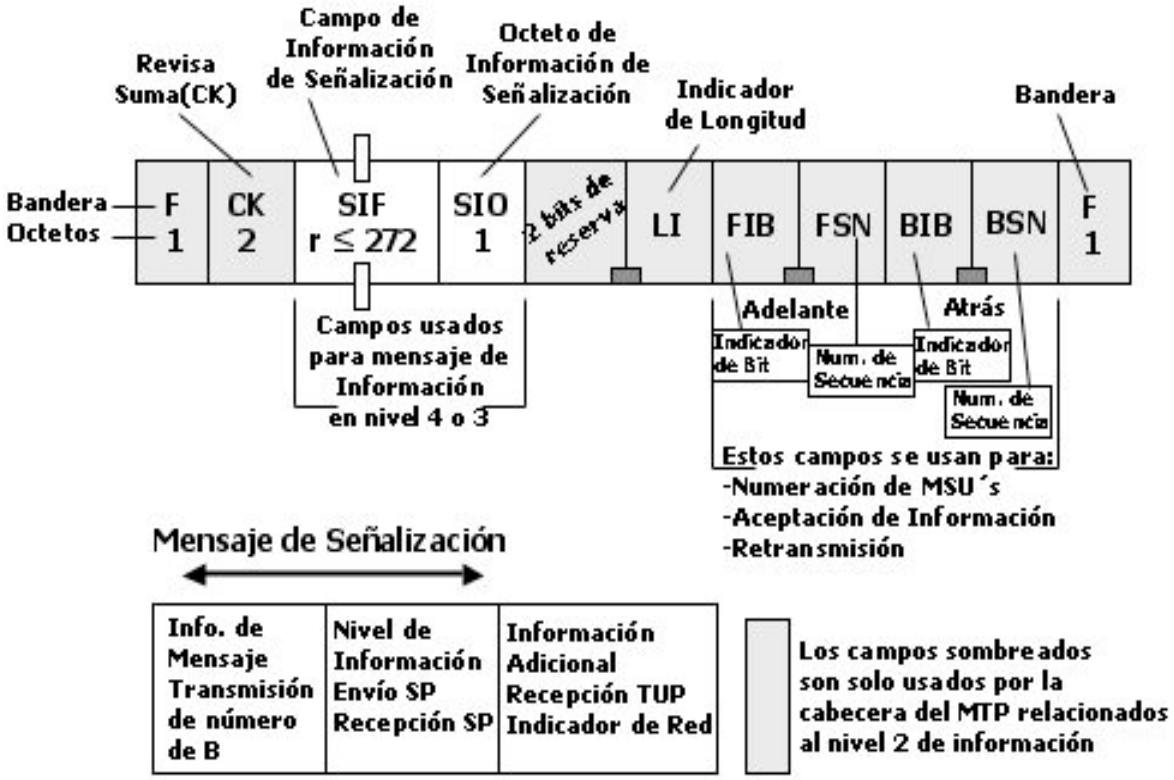


Figura 4.5 Estructura de las Unidades de Mensaje de Señalización (Message Signal Unit – MSU).

Unidades de Estado de Enlace de Señalización (Link Status Signal Units - LSSU)

Se encarga de llevar 1 o 2 octetos de información sobre el estado del enlace entre los puntos de señalización en ambos lados del enlace. El estado del enlace para controlar el alineamiento del mismo y para indicar el estado de un punto de señalización a otro punto remoto de señalización.

Unidades de Señalización de Relleno (Fill in Signal Units - FISU)

Se encarga básicamente de transportar la información del nivel 2. Se utiliza para señalizar el estado de desocupado cuando no hay ninguna señal MSU para enviar.

La Parte de Protocolos de Usuario (User Part Protocols)

Algunos protocolos SS7 son responsables del manejo de los mensajes de señalización. Este conjunto de protocolos es llamado "User Part Protocols" y corresponde a las funciones del nivel 4 en el modelo de referencia SS7 (OSI capas 4-7). Ejemplos típicos son el Telephone User Part (TUP) y el ISDN User Part (ISUP). Sin embargo, versiones más recientes de SS7 también contienes protocolos como TCAP (Transaction Capabilities Application Part). Este protocolo es usado exclusivamente en señalización no orientada a conexión. El protocolo TCAP se relaciona con la capa 7 en el modelo de

referencia OSI. Los protocolos de manejo de mensaje en la señalización SS7 son conjuntamente responsables de lo siguiente:

- Empaquetamiento de mensajes de señalización salientes y des-empaquetamiento de mensajes de señalización entrantes (cada mensaje tiene una estructura específicamente definida con parámetros principales y opcionales)
- Comunicación interna con funciones relativas a manejo de tráfico, provisión de servicio y manejo de circuitos en un intercambio (intercambio de señales definidas de software entre las funciones del User Part y los procedimientos internos en un intercambio).
- Comunicación interna con el MTP o el NSP (intercambio de señales definidas de software entre las funciones del user Part y el MTP o el NSP)

Cada User Part Protocol tiene un único conjunto de mensajes de señalización el cual es usado en secuencias de señalización para tráfico y control de servicio asi como para manejos y mantenimiento (información de cambios de estado que afectan a los equipos de conmutación, etc.). Un mensaje completo de señalización contiene dos partes básicas: una parte de mensaje y una parte de dirección.

4.3.4 Los protocolos SS7

El SCCP es usado solo por ciertas áreas de aplicación o usuarios.

Hasta donde concierne a los servicios ISDN, el SCCP puede ser usado en conexión con el servicio de mensajes cortos (SMS-Short Message Service), el cual puede ser ejecutado sobre un canal-D y la red SS7. Aquí, todo el ruteo y transferencia de los mensajes cortos es manejada por el SCCP, el MTP e ISUP exclusivamente.

SS7 puede ser dividido en dos partes funcionales principales:

-Funciones de Manejo de Mensaje TUP, ISUP, etc. (Message Handling Functions)

-Funciones de Transferencia de Mensaje MTP y SCCP (Message Transfer Functions)

El MTP y el SCCP conjuntamente forman el NSP, el cual provee tanto señalización orientada a conexión como señalización no orientada a conexión y los caminos de las señales SS7 "connectionless o connection-oriented" son transferidos como estructuras de paquetes de datos llamados Message Signal Units (MSU´s). Los protocolos de manejo de mensajes TUP, ISUP, etc. son responsables de el empaquetamiento / des-empaquetado de mensajes de señalización entrantes y salientes, asi como de la comunicación interna con otros sistemas. Los intercambios de información que usan SS7 son llamados Puntos de Señalización (SP´s-Signalling Points) y se les da un código único de identificación en la red SS7.

4.4 Establecimiento de Llamada con ISUP

Desde el punto de vista del MTP y el TCS, el establecimiento de llamada con ISUP es similar al establecimiento de llamada con TUP. Sin embargo, la estructura de ISUP es muy diferente a la de TUP. El procedimiento del establecimiento de llamada en el nivel 4 en ISUP tiene sus variantes con respecto al establecimiento de llamada con TUP. El mensaje con ISUP puede llevar un poco mas de información que el mensaje con TUP.

El mensaje ISUP es estructurado de forma distinta que el mensaje TUP, a pesar de que ambos ISUP y TUP, usan las mismas funciones MTP.

4.4.1 La estructura de ISUP-MSU

Las funciones ISUP pueden ser usadas en intercambios de voz, o enviando mensajes ISUP de señalización. El uso actual de estos mensajes y sus parámetros pueden diferir de un mercado a otro. Cada mensaje ISUP es llevado en un MSU desde el MTP.

La trama completa ISUP es llamada ISUP-MSU. El MTP puede al mismo tiempo llevar otros mensajes de otra partes pertenecientes al nivel 4, TUP-MSU y SCCP-MSU.

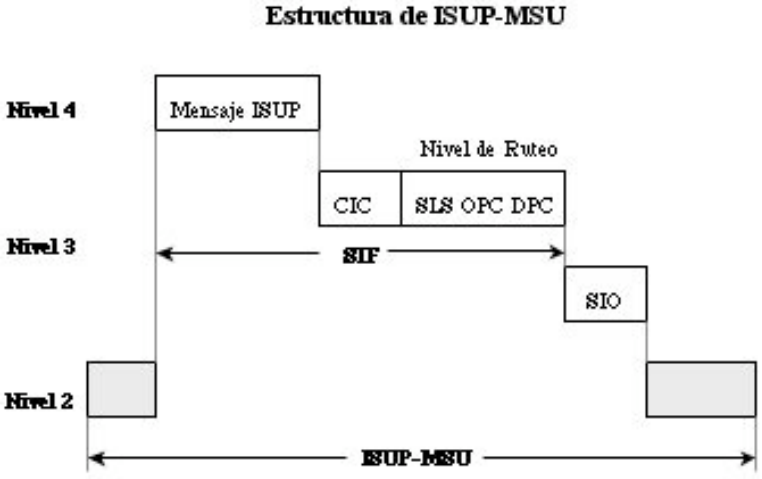


Figura 4.6 Estructura de ISUP-MSU

Octeto de Información de Servicio (Service Information Octet (SIO) Field)

El campo (Field) SIO contiene un indicador de servicio de 4 bit´s (Service Indicator SI), y el campo de sub-servicio (Subservice Field SSF), el cual es también de 4 bit´s de longitud. El indicador de servicio para ISUP es 5.

El indicador de servicio es leído por el nivel 3 del MTP, e indica a que User Part será dirigido el mensaje. El campo de sub-servicio contiene el indicador de red (Network Indicator NI) que es contenido en 2 bit´s, y que tiene también 2 bit´s de repuesto.

Los códigos correspondientes al Indicador de Red (Network Indicator):

00 Red Internacional (International Network)

01 Repuesto (para uso internacional solamente)

10 Red Nacional (national network)

11 Reservado (Para uso nacional solamente)

El indicador de red es usado por las funciones de manejo de mensajes de señalización y sirve para diferenciar entre mensajes nacionales e internacionales.

Estructura del Service Information Octet

Campo de Sub-Servicio	Indicador de Servicio
NIXX	0101

Figura 4.7 Estructura del Octeto de Información de Servicio (Service Information Octet – SIO)

El Campo de Información de Señalización (Signalling Information Field - SIF)

El SIF consiste de las siguientes partes:

- Nivel de Ruteo (Routing Level)
- Código de Identificación de Circuito (Circuit Identification Code CIC)
- Mensaje

El tamaño máximo de un SIF en un MSU es de 272 octetos

El nivel de Ruteo (Routing Level)

El nivel de ruteo contiene información para el ruteo de los mensajes en la red de señalización. El nivel 3 de el MTP lee ésta información para comprobar que el mensaje entrante corresponde a un intercambio, o deberá ser re-enrutado a otro intercambio de información. El nivel de ruteo consiste de tres campos, el código de punto destino (Destination Point Code DPC), del código de punto originado (Originating Point Code OPC) y de la Selección de enlace de Señalización (Signalling Link Selection SLS).

El Código de Identificación de Circuito (The Circuit Identification Code)

El campo CIC (Circuit Identification Code) es un número que identifica el canal de tráfico actual. Los 4 bit´s menos significativos de éste campo pueden ser usados como Signalling Link Selection (SLS). De otra manera, se utiliza el campo SLS del nivel ISUP.

La opción de utilizar un campo SLS separado de el campo CIC comparado con el MTP "rojo". Cuando el campo SLS es usado, es posible especificar con datos de ruteo que todos los ISUP-MSU´s para una ruta sean enviados en el mismo canal de señalización.

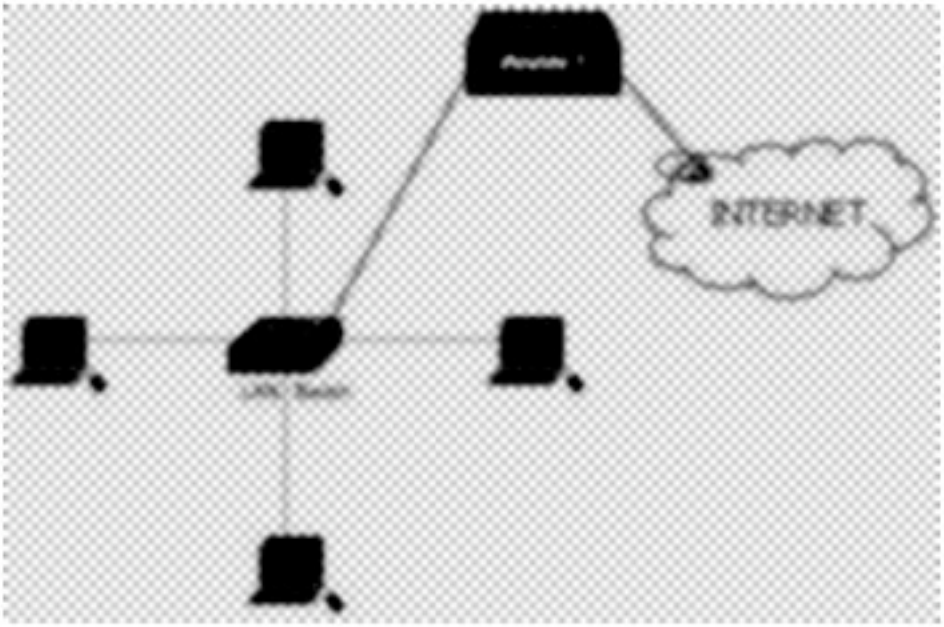
Para cada conexión individual del circuito, el mismo nivel de ruteo debe ser usado para cada mensaje que es transmitido por esa conexión.

El Tipo de Código de Mensaje (The Message Type Code)

El tipo de código de Mensaje, es un octeto codificado que únicamente identifica los mensajes ISUP. Este campo es de alto valor jerárquico para todos los mensajes.

CAPÍTULO 5

INTRODUCCIÓN A LAS REDES DE DATOS



5.1 DEFINICIONES BÁSICAS

Redes de Área Local (Local Area Network - LAN)

Una red de área Local (LAN-Local Area Network) es la interconexión de dispositivos de cómputo que pueden comunicarse entre si y compartir un grupo de recursos comunes, como impresoras, discos, etc. Normalmente, están limitadas en distancia (5 Km), por lo que pueden abarcar desde un departamento hasta un edificio, o todo un campus universitario. En general, el hecho de trabajar dentro de una red de área local es sencillo y garantiza accesos seguros a quienes se encuentran interconectados a través de su alta velocidad.

Red de Área Metropolitana (Metropolitan Area Network - MAN)

Se considera una red de área metropolitana a la interconexión de dispositivos de cómputo que pueden comunicarse entre si dentro de una ciudad, de ahí el término metropolitana.

Red de Área Extensa (Wide Area Network - WAN)

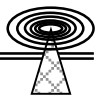
Una red de área extensa, es una red que interconecta redes mas pequeñas, y el ejemplo más claro de una red de área extensa es *internet*, debido a que ésta interconecta muchas redes más pequeñas que ella, en un área muy extensa.

Distancia	Lugar	Tipo de Red
0.1 m	La tarjeta de cto.	LAN
1 m	El Sistema	
10 m	La habitación	
100 m	El edificio	
1 Km	La Universidad	
100 Km	La ciudad	MAN
1000 Km	El país	WAN
+ de 10000 Km	El mundo	

Figura 5.1 Identificación de redes LAN, MAN y WAN.

5.2 Interconexión de Sistemas Abiertos (Modelo OSI - Open Systems Interconection)

Los estándares tienen un papel muy importante en las redes de área local modernas. Si éstos no existieran, los usuarios estarían obligados a comprar equipos y redes propietarias de un solo fabricante, por lo que si alguna compañía o fabricante desapareciera, o bien descontinuara alguna línea de producto, generaría altos costos para los usuarios de dichas redes y un bajo rendimiento. Es por eso que durante muchos años el Departamento de Defensa de los Estados Unidos y diversas organizaciones



internacionales han estado trabajando en el desarrollo de un conjunto de estándares para los equipos de comunicaciones de datos en general (DCE), y en particular para las redes de área local (LAN), donde los beneficios que incluye una estandarización son: reducción de costos en los equipos, facilidad de interconectar y configurar tanto el hardware como el software de diferentes marcas de equipo.

En 1984 la Organización de Estándares Internacionales (ISO-International Standards Organization), junto con el CCITT (Consultative Committee on International Telegraphy and Telephony) desarrollaron el modelo OSI (Open Systems Interconnection), que consiste en un conjunto de niveles funcionales, en los que cada nivel tiene sus propios protocolos de comunicaciones para facilitar las comunicaciones entre las redes de computadoras.

El modelo OSI considera siete niveles funcionales, como se muestra en la figura 5.2, con los que se diseña el software de comunicaciones. La instauración de dicho modelo, aparte de los beneficios que trae consigo, facilita el reemplazo de piezas, la escalabilidad de los equipos y la administración de los recursos que conforman a las redes de área local (LAN).

OSI fue conceptualizado como el software que maneja la transmisión de los mensajes de una terminal o programa aplicativo, con otra terminal o programa aplicativo, separados e interconectados en una red.

Está basado en el concepto de aplicaciones distribuidas cooperativas. En éste modelo un sistema se compone de una computadora, todo su software y cualquier periférico conectado a ella. Incluyendo terminales tontas. Una aplicación distribuida es cualquier actividad que involucre el intercambio de información entre dos sistemas abiertos.

Este modelo esta dirigido al intercambio de información entre dos sistemas abiertos, como se dijo anteriormente, más que al funcionamiento internos de los mismos. La visión para el futuro del modelos OSI es poder conectar cualquier equipo de comunicación de datos y cualquier tipo de software con otros equipos y software, sin importar que compañía los fabricó, y así poder minimizar el trabajo del usuario final y la complejidad al momento de la interoperabilidad de las redes y de los sistemas actuales.

7. Nivel de Aplicación
6. Nivel de Presentación
5. Nivel de Sesión
4. Nivel de Transporte
3. Nivel de Red
2. Nivel de Datos
1. Nivel Físico

Figura 5.2 Capas del Modelo OSI.

5.2.1 Aplicación del Modelo OSI

El propósito de los siete niveles del modelo OSI es poder segmentar las diversas funciones que se requieren para transportar la información cuando dos computadoras se comunican.

En el modelo OSI el objetivo de cada nivel funcional es proporcionar los servicios necesarios para el nivel superior inmediato. Los niveles son abstractos, de tal forma que cada nivel asegura la comunicación con el nivel asociado en la computadora remota. En realidad, cada nivel se comunica con sus niveles adyacentes en una misma computadora.

Excepto por el nivel más bajo en el modelo, ningún nivel proporciona información directamente a su contraparte en la computadora remota. La información generada en la computadora emisora tiene que pasar por todos los niveles del modelo, del 7 al 1; después, dicha información se transmite a través del cable de red hasta la computadora receptora y de igual forma ésta tiene que pasar por todos los niveles en orden inverso.

La interacción entre los niveles adyacentes se llama **interfaz**. La interfaz define qué servicios ofrecen los niveles inferiores de redes a los niveles superiores y, además, la forma en que estos servicios serán accedidos; cada nivel en una computadora actúa como si se estuviera comunicando directamente con su nivel asociado en la computadora remota. El conjunto de normas usadas para comunicarse entre los niveles se llama **protocolo**.

A continuación se describe la función de los siete niveles del modelo OSI y la identificación de los servicios que proporcionan los niveles adyacentes entre si.

1. Nivel Físico (Physical Layer)

El nivel físico es el encargado, primordialmente, de la transmisión de los bits de datos (ceros o unos) a través de los circuitos de comunicaciones. Este es el nivel de comunicación física de los circuitos. En éste nivel se revisan tareas básicas como el acoplamiento de los niveles de voltaje, los factores de tiempo (por ejemplo, transmitir 1200 bits por segundo es igual a 833 mseg por bit [1 seg / 1200 bps = 833 mseg]), definir si la comunicación es en serie o paralelo, full duplex o half duplex, reglas para iniciar y establecer la comunicación, así como para terminarla, y estándares en los tipos de conectores como el RS-232(A-F) o RS449.

El propósito principal del nivel físico es definir las normas para garantizar que cuando la computadora emisora transmita un bit "1", la computadora receptora verifique que el bit "1" fue recibido y no un bit "0". En éste nivel los bits por si solos no tienen ningún significado.

Es fundamental recordar que el nivel 1 es la base de la conexión, la más importante y por donde la información se transmite proveniente de y hacia todos los niveles. El nivel 1 está relacionado únicamente con hardware, mientras que los niveles 2 al 7 están relacionados solo con software.

El nivel físico define la forma en la que el cable se conecta a la tarjeta de red; por ejemplo, cuántos pines debe tener el conector y la función de cada uno de ellos. También define la técnica de transmisión que se usará para enviar la información a través del medio de transmisión de la red.

2. Nivel de Datos (Data Link Layer)

El nivel de datos es donde los bits tienen algún significado en la red y puede equipararse con el departamento de recepción y envio de una compañía manufacturera, el cual debe tomar los paquetes que recibe del nivel de red (Network Layer) y prepararlos en la forma correcta (tramas) para poder enviarlos (Transmitirlos) por el nivel físico.

De igual forma sucede cuando recibe paquetes (bits) del nivel físico y tiene que ponerlos correctamente (Trama) para verificar si la información que está recibiendo está libre de errores, si los paquetes vienen en orden, si no faltan algunos de ellos, etc., para poder entregarlos al Nivel de Red (Network Layer) sin ningún error.

Dentro de sus funciones se incluyen la de notificar al emisor (la computadora remota) si algún paquete (trama) se recibió en mal estado (basura), o si se omitieron algunas de las tramas y se requiere que sean enviadas nuevamente (retransmisión); de igual manera se debe notificar si una trama está duplicada o si llego sin problemas. Es responsable de saber en donde comienza la transmisión de la trama y dónde termina, así como de garantizar hasta qué punto tanto la computadora emisora como la receptora están sincronizadas y si emplean el mismo sistema de codificación y decodificación.

El nivel de datos tiene a su cargo la integridad de la recepción y el envio de la información.

Figura 5.3 Un ejemplo de tramas de datos.

Cuando el nivel de datos envía una trama, siempre espera una respuesta (acknowledgment) de la computadora receptora. Si ésta encuentra problemas en alguna trama durante la transmisión, solamente se retransmiten las tramas que fueron identificadas con problemas.

3. Nivel de Red (Network layer)

Este nivel determina la ruta del mensaje desde la computadora emisora hasta la computadora receptora, dependiendo de las condiciones de la red.

El nivel de red es el responsable del direccionamiento de mensajes y de la conversión de las direcciones y de los nombres lógicos a físicos.

Dentro de las funciones de enrutamiento de mensajes evalúa el mejor camino que debe seguir el paquete dependiendo del tráfico en la red, el nivel de servicios, etc. Los problemas de tráfico que controla tienen que ver con el enrutamiento (routing), intercambio (switching) y congestionamiento de paquetes en la red.

El nivel de red maneja pequeños paquetes de datos juntos para su transmisión a través de la red, así como la reestructuración de grandes tramas de datos en paquetes pequeños. En la computadora receptora se reensamblan los paquetes en su estructura de datos original (trama).

A la información proveniente del nivel de transporte (transport layer) se le añaden componentes apropiados para su enrutamiento en la red y para mantener un cierto nivel en el control

de errores. La información se presenta según el método de comunicaciones utilizado para acceder a la red de área local, la red de área extendida como los enlaces T1 o E1, la conmutación de paquetes (packet switching) como X25, etc. Por ejemplo, el protocolo IP (Internet Protocol) es uno de los protocolos que se usa en éste nivel de red.

4. Nivel de Transporte (Transport Layer)

Este nivel es llamado ocasionalmente nivel de host-to-host o nivel de end-to-end. En particular los niveles 4 a 7 son conocidos como niveles end-to-end y los niveles 1 a 3 son conocidos como niveles de protocolo.

En el nivel de transporte se establecen, mantienen y terminan las conexiones lógicas para la transferencia de información entre usuarios.

El nivel de transporte provee un mecanismo de intercambio de información muy confiable entre las computadoras, debido a que es el responsable del manejo, de la detección y corrección de errores.

El nivel de transporte se relaciona en mayor medida con los beneficios de end-to-end, como son el manejo de las direcciones de la red, el establecimiento de circuitos virtuales los procedimientos de entrada y salida de ésta. Solamente al alcanzar el nivel superior de transporte (sesión) se podrán observar los beneficios notorios para el usuario final.

Este nivel puede incluir las especificaciones de los mensajes de difusión (Broadcast), los tipos de datagramas, los servicios de correo electrónico, las prioridades de los mensajes, la recolección de la información y su administración, la seguridad, los tiempos de respuesta, las estrategias de recuperación en caso de falla y la segmentación cuando el paquete excede su tamaño máximo según el protocolo.

Cuando recibe información del nivel de red, el nivel de transporte verifica que la información éste en el orden adecuado y revisa si existe información duplicada o extraviada. Si la información recibida ésta en desorden, lo cual es posible cuando se enrutan las tramas en redes grandes, el nivel de transporte corrige el problema y transfiere la información al nivel de sesión en donde se le dará un proceso adicional. Por ejemplo, el protocolo TCP (transmisión Control Protocol) usa éste nivel del modelo OSI.

5. Nivel de Sesión (Session Layer)

Este nivel es el que permite que dos aplicaciones en diferentes computadoras establezcan, usen y finalicen la conexión llamada sesión. El nivel de sesión maneja el diálogo que se requiere en la comunicación de dos dispositivos. Establece reglas para poder iniciar y finalizar la comunicación entre dispositivos y puede brindar el servicio de recuperación de errores; es decir, si la comunicación falla y esto es detectado, el nivel de sesión puede retransmitir la información para poder completar el proceso en la comunicación.

El nivel de sesión es el responsable de iniciar, mantener y terminar cada sesión lógica entre usuarios finales.

Para poder entender mejor éste nivel, se puede hacer una comparación con el sistema telefónico. Cuando uno levanta el auricular del teléfono, espera el tono y marca un número, en ese momento se está creando una conexión física que va desde el nivel 1 (Físico) como un protocolo de persona a red. Al momento de hablar con la persona en el otro extremo del teléfono, uno se encuentra

en una sesión persona a persona. En otras palabras, la sesión es el dialogo de las dos personas que se transporta por el circuito del teléfono. En éste nivel se ejecutan funciones de reconocimiento de nombres para el caso de seguridad relacionado con aplicaciones que requieren comunicarse a través de la red.

6. Nivel de Presentación (Presentation Layer)

En éste nivel se traduce o transfiere la información recibida en el formato del nivel de aplicación a un formato intermedio reconocido. En la computadora receptora la información se traduce o transfiere del formato intermedio al formato usado en su propio nivel de aplicación.

El nivel de presentación maneja beneficios como la administración de la seguridad en la red; por ejemplo, la codificación y decodificación, el encriptado, la compresión y descompresión, el cifrado y descifrado. También brinda las normas para la transferencia de información (Data Transfer) y comprime datos para reducir el número de bits que necesitan ser transmitidos.

El nivel de presentación define el formato en que la información será presentada al usuario e intercambiada entre ellos, así como la sintaxis usada entre las aplicaciones.

7. Nivel de Aplicación (Application Layer)

Este nivel es el nivel más alto y sirve como una ventana para los procesos de la misma índole al acceder a los servicios de la red.

El nivel de aplicación representa el servicio que soporta directamente las aplicaciones del usuario.

Entre éstas aplicaciones se encuentran el software para transferencia de archivos (File Transfer), accesos a bases de datos y correo electrónico.

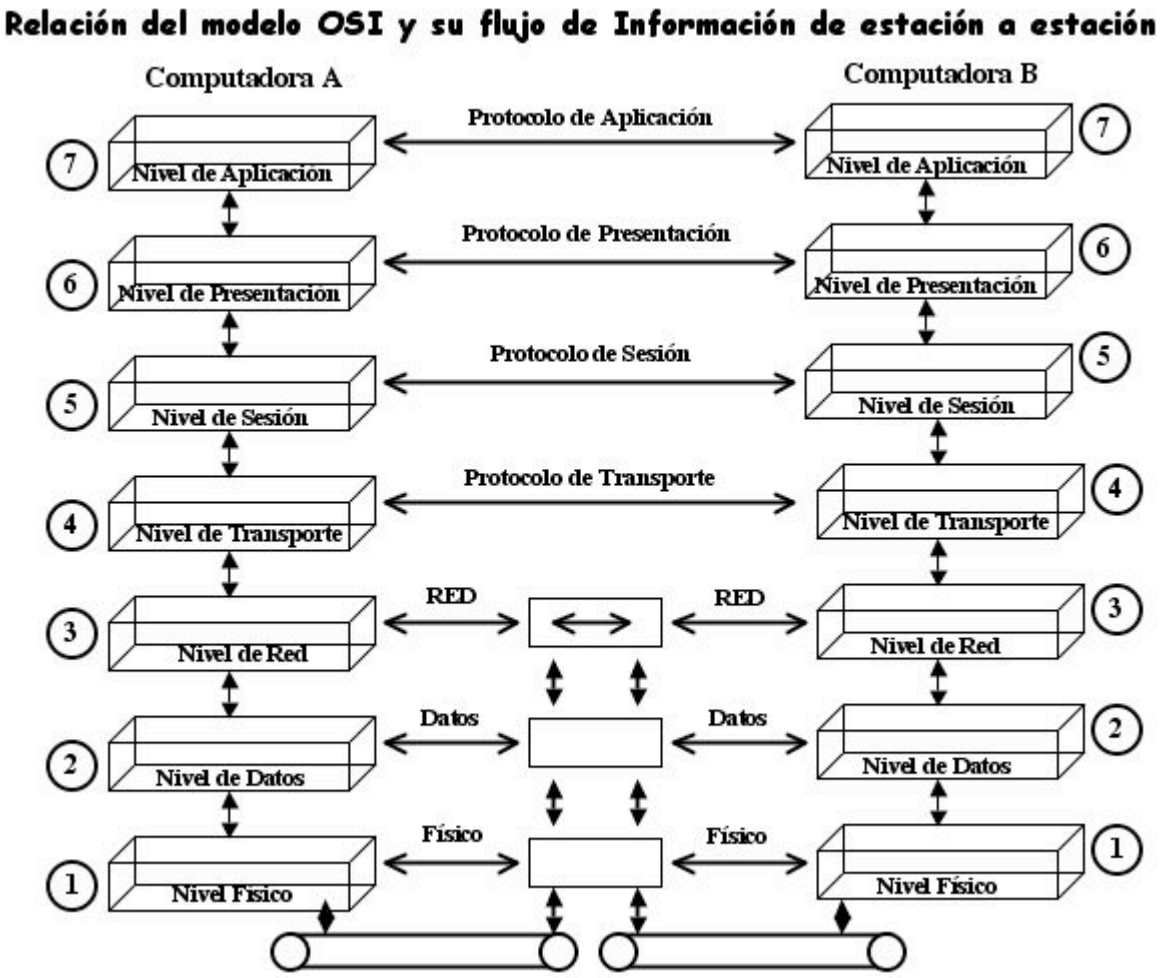


Figura 5.4 Relación del modelo OSI y su flujo de Información de estación a estación.

5.3 MODELO IEEE 802

El instituto de Ingenieros Eléctricos y Electrónicos (IEEE-Institute of Electrical Electronic Engineers) es una de las organizaciones que establece estándares para diversas áreas técnicas. Por ejemplo, el proyecto para la estandarización de las redes de área local (LAN), el cual se denomino 802, debido al año y mes en que fue puesto en operación (febrero de 1980) figura 5.5.

El proyecto 802 definió los estándares de las redes para los niveles físico y de datos del modelo OSI. Aunque las publicaciones de los estándares de la IEEE 802 actualmente preceden a las de los estándares del modelo OSI, ambos fueron desarrollados en el mismo periodo y compartieron la misma información, lo que condujo al desarrollo de dos modelos compatibles.

En éste modelo diferentes métodos de acceso están a cargo de varios grupos de trabajo. Los **grupos de trabajo** son identificados por el sufijo numérico; por ejemplo: 3, 4, etc.

La lista que se presenta a continuación contiene los diferentes grupos de trabajo del proyecto 802.

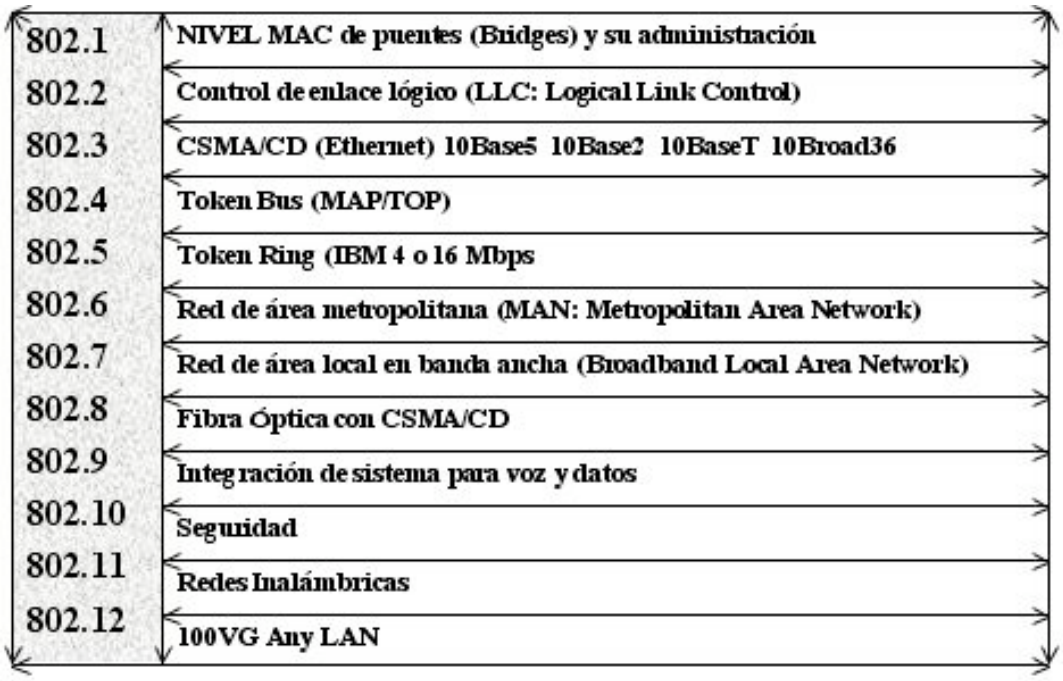


Figura 5.5 Estándares de la IEEE 802.

La figura 5.6 es una representación gráfica de cómo se relacionan los estándares IEEE 802.1 al 802.5.

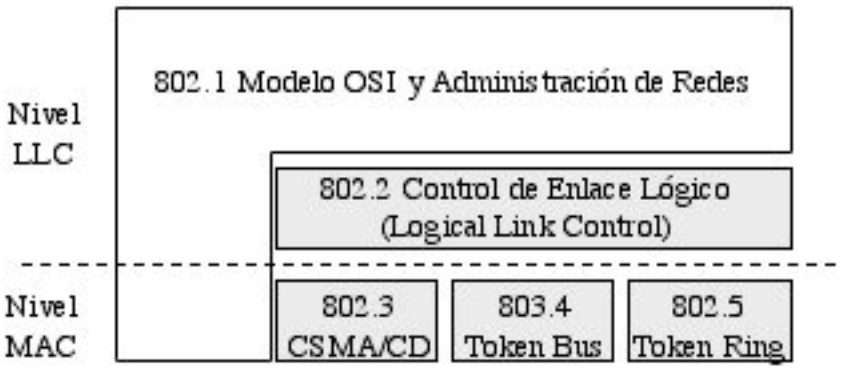


Figura 5.6 Estándares del 802 relacionados con los niveles LLC y MAC.

El comité de estándares del proyecto 802 estuvo de acuerdo con el modelo OSI, pero decidió que requería de mayor detalle en el nivel de datos. El proyecto 802 dividió el nivel de datos en dos subniveles: el control de acceso al medio (MAC) y el control de enlace lógico (LLC).

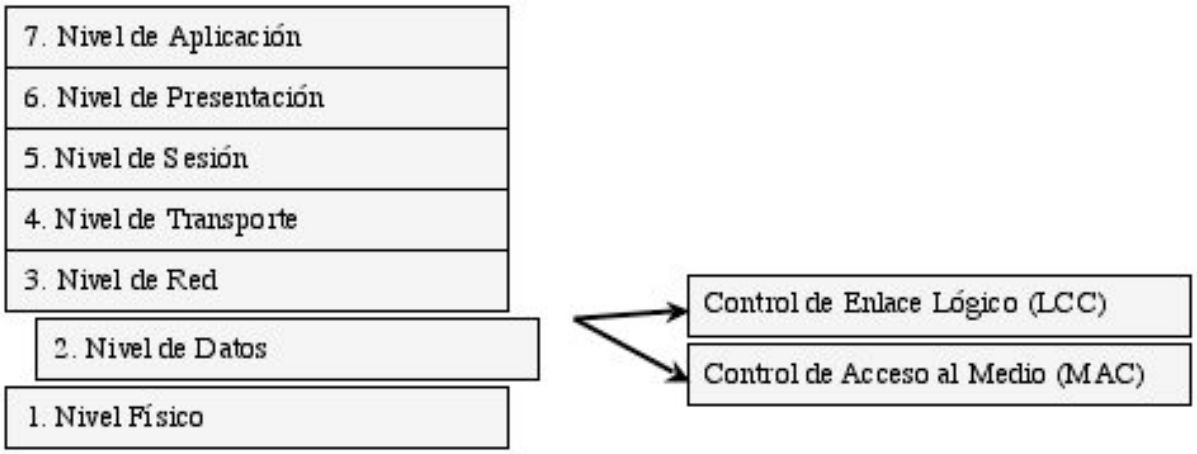


Figura 5.7 IEEE 802 (LLC y MAC).

Como puede apreciarse en la figura 5.7, el MAC es el subnivel inferior y proporciona a la tarjeta de red de la computadora un acceso compartido hacia el nivel físico. El subnivel MAC se comunica directamente con la tarjeta de red y es responsable de la entrega de datos sin errores entre dos computadoras en la red.

El LCC administra la liga de comunicaciones y define el uso de puntos lógicos de interfaz llamados SAP (Service Access Points) que la computadora remota puede referenciar y utilizar para la transferencia de información desde el subnivel LLC hasta el nivel 7 del modelo OSI.

El proyecto 802 de la IEEE definió los subniveles de control lógico y control de acceso al medio. También se generó una serie de documentos, de los cuales los tres mas importantes para los estándares de las topologías de red fueron:

802.3 Define los estándares para las redes en bus, como Ethernet, que usa el método de acceso CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

802.4 Define los estándares para las redes Token Passing.

802.5 Define los estándares para las redes Token Ring.

La IEEE definió las funciones para el nivel LLC en el estándar 802.2 y definió las funciones del nivel MAC y el nivel Físico en los estándares 802.3, 802.4 y 802.5.

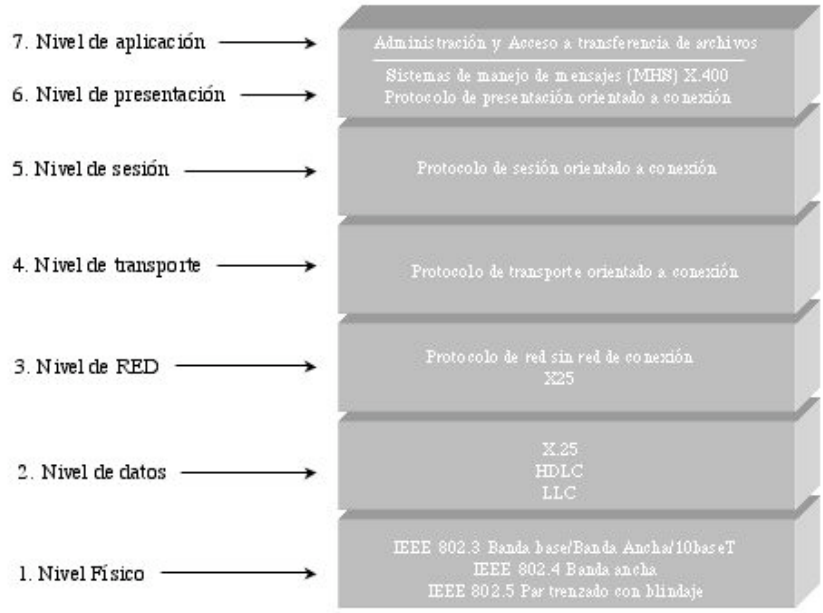


Figura 5.8 Protocolos asociados con los niveles del modelo OSI.

5.4 TOPOLOGÍAS DE REDES DE DATOS

En el nivel físico, cada red de área local ha definido sus propias características. A continuación se analizaran las topologías de redes de datos, los tipos de cableados y medios y las técnicas de transmisión usadas en estas redes.

A la forma en que se conectan las computadoras en una red se le llama **Topología**. Actualmente existen una gran cantidad de topologías, como son la topología en bus, en estrella, en anillo y, en el caso de las redes complejas, topologías mixtas o híbridas, dependiendo de la flexibilidad y / o complejidad que se quiera dar al diseño.

Tipos de Conexión

Existen dos tipos de conexión a una red: la conexión **punto a punto** y la conexión **multipunto**. La conexión Punto a Punto es una conexión de dos dispositivos entre ellos y nadie más. Por ejemplo, una conexión de dos computadoras mediante fibra óptica o par trenzado (Twisted pair).

Figura 5.9 Conexión Punto a Punto.

La conexión multipunto utiliza un solo cable para conectar más de dos dispositivos. Por ejemplo, un cable que tiene varios dispositivos conectados al mismo medio de transmisión, como es el caso del cable coaxial.

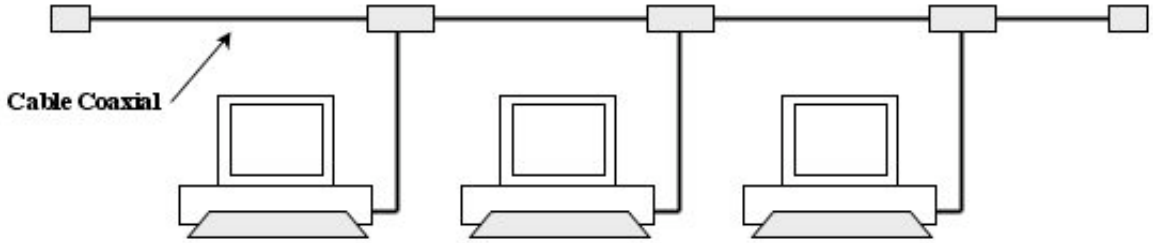


Figura 5.10 Conexión Multipunto.

5.4.1 Topología en Bus

La topología en bus es una topología de red multipunto, en la cual los dispositivos se conectan a un mismo cable, uno tras otro.

En la topología de bus, todos los dispositivos comparten el mismo **medio**, que en éste caso es el cable coaxial; por ésta razón, los mensajes que se transmiten a través de éste medio son atendidos por todos los demás dispositivos que lo comparten.

La topología en bus se considera como una carretera por la que transitan todos los vehículos (paquetes o tramas) y que está limitada en distancia, dependiendo del tipo de cable y los conectores que se utilicen. Los conectores son resistencias que sirven para mantener constante la impedancia del cable para poder transmitir la información.

En la topología en Bus existen dos formas de conectar los dispositivos y éstas dependen del tipo de cable que se quiera usar. Los tipos de cable son conocidos como cable coaxial grueso y cable coaxial delgado, y la diferencia entre ellos es que uno puede transmitir información a un máximo de hasta 500 m, mientras que el otro solamente puede transmitir información a un máximo de 1.85 m. Existen reglas sobre la distancia mínima que debe dejarse entre un dispositivo y otro. Para el caso del cable coaxial grueso, la distancia entre dispositivos es de 2.5 m, mientras que para el cable coaxial delgado es de 1 m.

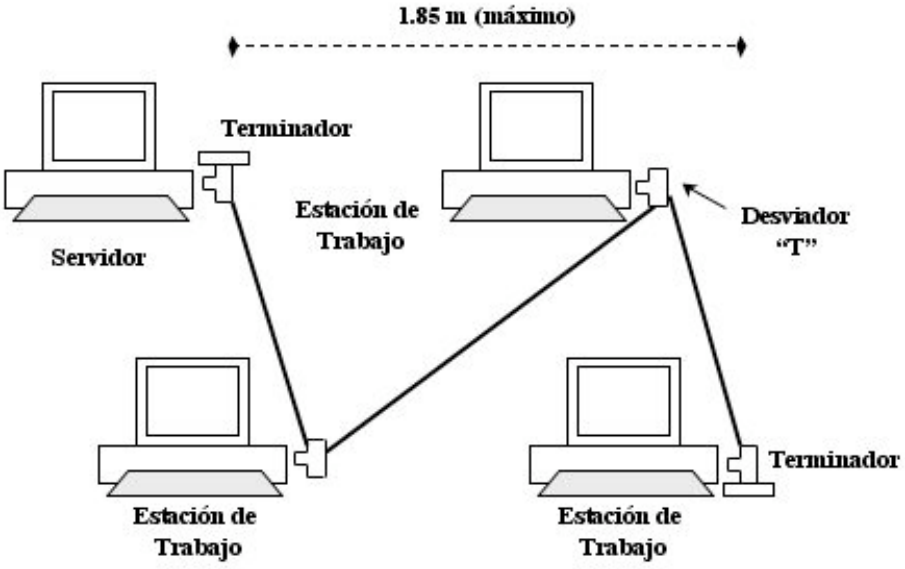


Figura 5.11 Topología en Bus con cable coaxial delgado (Thin Coax).

En la figura anterior se muestra cómo se construye una topología en Bus, con cable coaxial delgado, en la que se encuentran terminadores y derivadores "T", los cuales se utilizan para poder seguir expandiendo la red cuando se requiera, con una resistencia interna para mantener la impedancia. En éste tipo de conexión, la "T" se conecta directamente a la tarjeta de red y se requieren dos terminadores por segmento de red. La impedancia que debe tener el segmento es de 50Ω. Un segmento de red es la distancia que hay entre dos terminadores; o bien, es el espacio que ocupa una red donde todos los dispositivos pueden interconectarse sin necesidad de usar ningún tipo de equipo adicional para unirlos.

El número máximo de computadoras o dispositivos conectados a éste tipo de topología es de 30; esto se debe al método de acceso que utiliza Ethernet, el cual será revisado más adelante.

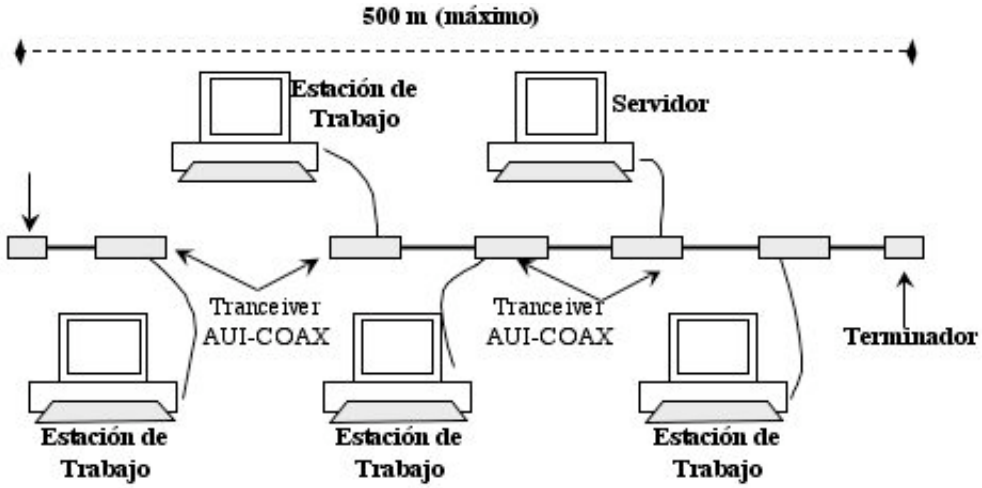


Figura 5.12 Topología en Bus con cable coaxial grueso (Thick Coax).

En la figura anterior se pueden apreciar dos diferencias entre éste tipo de topología y la topología en Bus de cable coaxial delgado. La primera consiste en que con cable coaxial grueso se puede abarcar más lugares, debido a que su distancia máxima es de 500 m. La segunda es que en éste tipo de conexión no se usan "T´s" , sino transceivers (transmisor-receptor). Sin embargo, tienen algo en común, y es el uso de terminadores. Al igual que con el cable coaxial delgado, se requiere de dos terminadores para poder transmitir la información, y estos terminadores también son de 50Ω, aunque de mayor tamaño.

El número máximo de dispositivos o computadoras conectadas a éste tipo de topología es de 100, esto se debe al método de acceso que utiliza Ethernet.

Ventajas	Desventajas
La falla en una computadora no afecta a la red	Frágil. Si el cable se desconecta o se troza, la red deja de funcionar en su totalidad por pérdida de impedancia.
Las conexiones a la red son sencillas y flexibles.	Limitada en distancia y número de dispositivos conectados.
Es una topología barata en cuestión de cable, conectores, "T" y terminadores	Difícil de aislar cuando hay problemas de cableado.
	Degradación del desempeño de la red con el crecimiento de dispositivos.

Tabla 5.1 Ventajas y desventajas de la topología en Bus.

5.4.2 Topología de Anillo

La topología en anillo es una red punto a punto donde los dispositivos se conectan en un circuito irrompible formado por un concentrador, que es el encargado de formar eléctricamente el anillo en la medida en que se insertan los dispositivos. En la topología en anillo, el mensaje viaja en una sola dirección y es leído por cada una de las computadoras individualmente y retransmitido al anillo en caso de no ser el destinatario final del mensaje.

Esta topología se usa generalmente por Token Ring y Token Passing, en donde el Token (testigo) da a cada estación la oportunidad de transmitir, cuando el token es liberado, pasa a la siguiente computadora que desee transmitir, y así sucesivamente.

No se sabe que haya un número máximo de dispositivos conectados en éste tipo de topología debido a que no se comparte el medio como en al caso de la topología en Bus.

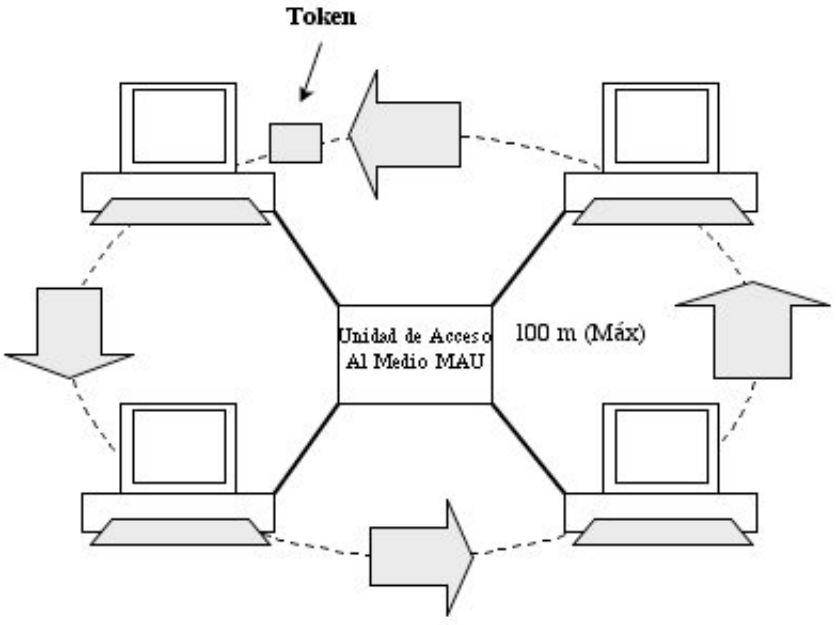


Figura 5.13 Topología en Anillo.

Ventajas	Desventajas
Si el cable de un dispositivo falla, no afecta la integridad del anillo.	Un alto costo en el cableado y las conexiones, asi como en el concentrador.
Igualdad de acceso a todos los dispositivos.	Si el concentrador falla en anillo se rompe.
El desempeño de la red esta garantizado.	

Tabla 5.2 Ventajas y desventajas de la topología en anillo.

5.4.3 Topología en Estrella

La topología en estrella es una topología en red punto a punto, ya que los dispositivos se encuentran conectados a un concentrador. Generalmente se le denomina topología de concentradores.

La topología en estrella concentra a todos los dispositivos en una estación centralizada que enruta el tráfico al lugar apropiado. Tradicionalmente, ésta topología es un acercamiento a la interconexión de dispositivos en la que cada dispositivo se conecta por un circuito separado a través del concentrador.

Esta topología es similar a la red de teléfonos, en donde existe un conmutador (PBX) y cada llamada que se hace tiene que pasar por el PBX para poder llegar a su destino.

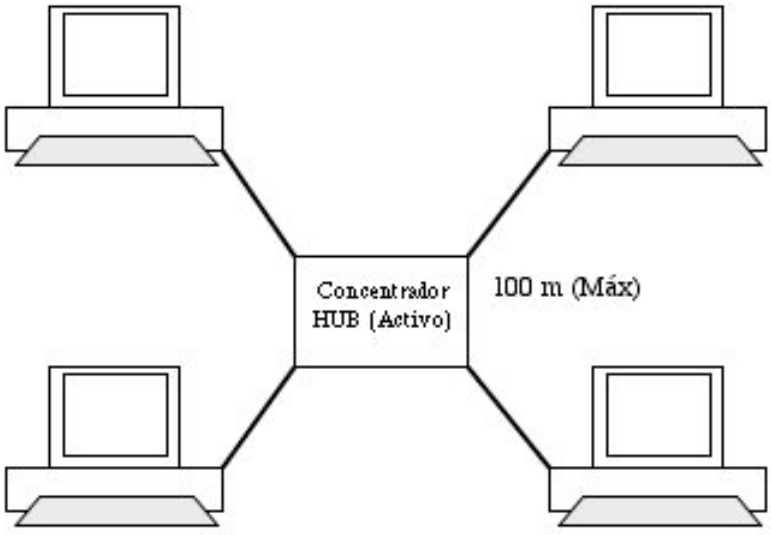


Figura 5.14 Topología en Estrella.

Al igual que la topología en anillo, no existe un número máximo de conexiones debido a que los concentradores son cada vez más poderosos y soportan mayor número de dispositivos con un nivel de servicio muy alto. En general, el número de estaciones que se pueden conectar al concentrador depende del tráfico que se genere entre ellas, y cuando éste es excesivo la red se divide mediante un dispositivo adicional cuya función es aislar el tráfico de un segmento a otro.

Tipos de Acceso

Las topologías en estrella y anillo físicamente tienen forma de estrella, pero dependiendo del concentrador que se instale permanecen con esta forma o se genera un anillo. En éste caso existen dos formas de comunicar los dispositivos con el concentrador o estación controladora de la topología: **poleo y contención.**

El tipo de **acceso de poleo** consiste en contar con una estación , la cual es la asignada de encargar permisos a cada dispositivo dentro del segmento; es decir, si el dispositivo tiene permiso de enviar su información, éste comienza su transferencia a su destinatario, de lo contrario tiene que esperar su turno. Cada dispositivo tiene una cantidad de tiempo igual a los demás, por lo que existe igualdad de acceso al medio. En este tipo de acceso no se puede enviar información si no se tiene el permiso para hacerlo.

En el tipo de **acceso de contención** cada dispositivo envía su información solo cuando nadie en la red esta enviando información; es decir, *solo un dispositivo a la vez puede enviar información*, y el concentrador es el encargado de administrar el tráfico y enrutarlo de la mejor manera posible. Este tipo de acceso permite un mayor número de paquetes y mejor rendimiento en la red.

Ventajas	Desventajas
Si el cable de un dispositivo falla no afecta la integridad de la red.	Alto costo en el cableado, las conexiones y el concentrador.
Facilidad para añadir nuevos dispositivos.	Si el concentrador falla, la red entera deja de funcionar.
Administración y monitoreo centralizado.	

Tabla 5.3 Ventajas y desventajas de la topología en estrella.

5.4.4 Topología Híbrida

La topología híbrida es el conjunto de todas las anteriores. Su implementación se debe a la complejidad de la solución de red, o bien al aumento en el número de dispositivos, lo que hace necesario establecer una topología de éste tipo. Las topologías híbridas tienen un costo elevado debido

a su administración y mantenimiento, ya que cuentan con segmentos de diferentes tipos, lo que obliga a invertir en equipo adicional para lograr la conectividad deseada.

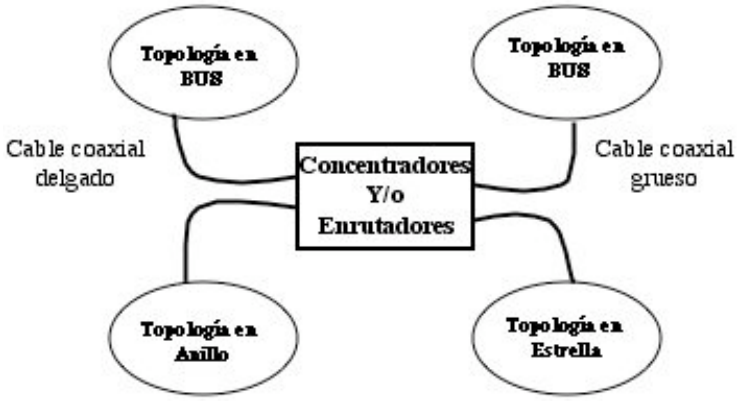


Figura 5.15 Topología Híbrida

5.5 MEDIOS DE TRANSMISIÓN DE DATOS

El medio de transmisión es utilizado para transportar las señales de la red de un punto a otro. Las redes de área local pueden conectarse usando diferentes tipos de medios. La industria de redes de área local ha estandarizado, principalmente , tres tipos de medio físico: coaxial, UTP (Unshielded Twisted Pair) y fibra óptica. Los niveles de transmisión que soporta cada tipo de medio físico se miden en millones de bits por segundo o Mbps.

5.5.1 Estándares EIA/TIA 568

La asociación de industrias electrónicas (EIA – Electronic Industries Association) es una asociación de estándares acreditada por el ANSI (American National Standars Institute) que desarrolla una variedad de estándares, incluyendo equipo. Por ejemplo, el estándar RS-232. La EIA generó los estándares para el cable y el conector, así como para otros conectores como el RS-449, etc.

El estándar EIA/TIA 568 se desarrolló para la instalación de cableados de telecomunicaciones en edificios comerciales. Los puntos principales de éste estándar son:

- Definir un sistema genérico de cableado, tanto para voz como para datos, que soporte múltiples productos y fabricantes.
- Proporcionar el diseño de telecomunicaciones con base en productos internacionalmente comercializados.
- Planear e instalar el cableado en un edificio con el conocimiento previo de los productos de telecomunicaciones que se instalaran.

El panorama que plantea éste medio es:

- Reconocimiento del Medio
- Topología
- Distancia de cableado y rendimiento
- Facilidad del cableado
- Rendimiento del Hardware
- Administración

Los elementos del cableado que propone son:

- Cableado Horizontal
- Cableado del circuito principal
- Las áreas de trabajo
- Los cuartos de telecomunicaciones
- El cuarto de equipos
- Facilidades de entrada
- Especificaciones del cable
- Las salidas del cableado de telecomunicaciones
- La conexión con el hardware
- Administración

Como puede apreciarse, el estándar EIA/TIA 568 cubre una gran variedad de aspectos que deben tomarse en cuenta antes de diseñar, construir o comprar una solución de cableado.

Métodos de Transmisión

Existen dos métodos de transmisión en las redes modernas: **banda base y banda ancha.**

El método de transmisión de **banda base** define que solamente una señal digital puede viajar por el medio y que su velocidad no puede ser mayor a 100 Mbps. La información es puesta en el medio sin ningún tipo de modulación y cada señal transmitida utiliza el ancho de banda total del medio.

El cable UTP, la fibra óptica y el cable coaxial para banda base son los más comunes para éste tipo de transmisión.

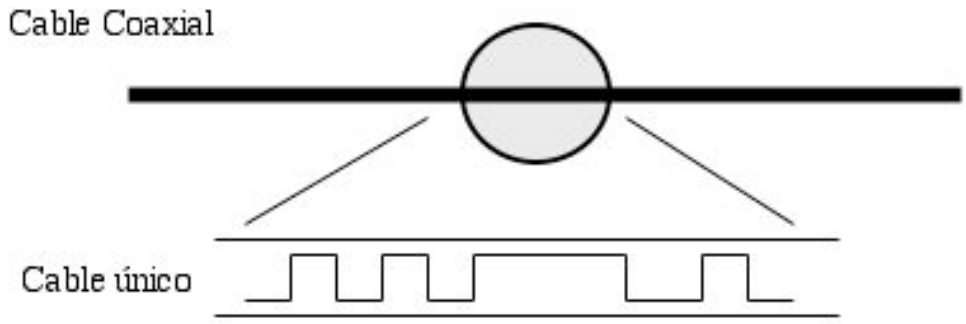


Figura 5.16 Transmisión en Banda Base (Baseband).

El método de transmisión en banda ancha permite que varias señales puedan viajar al mismo tiempo por el medio, por ejemplo, un CATV coaxial cable con un ancho de banda de 500 MHz puede llevar 80 canales de televisión de 6 MHz de ancho de banda cada uno (el 6 MHz no es limitante de velocidad). Estas transmisiones requieren de un mayor ancho, o rango de frecuencias, para poder permitir varias frecuencias en el mismo cable. La información se modula antes de transmitirla. El sistema de televisión es el mejor ejemplo de que varios canales pueden verse a través de un solo cable.

Los cables de fibra óptica y coaxial para banda ancha son los más comunes para éste tipo de transmisión.

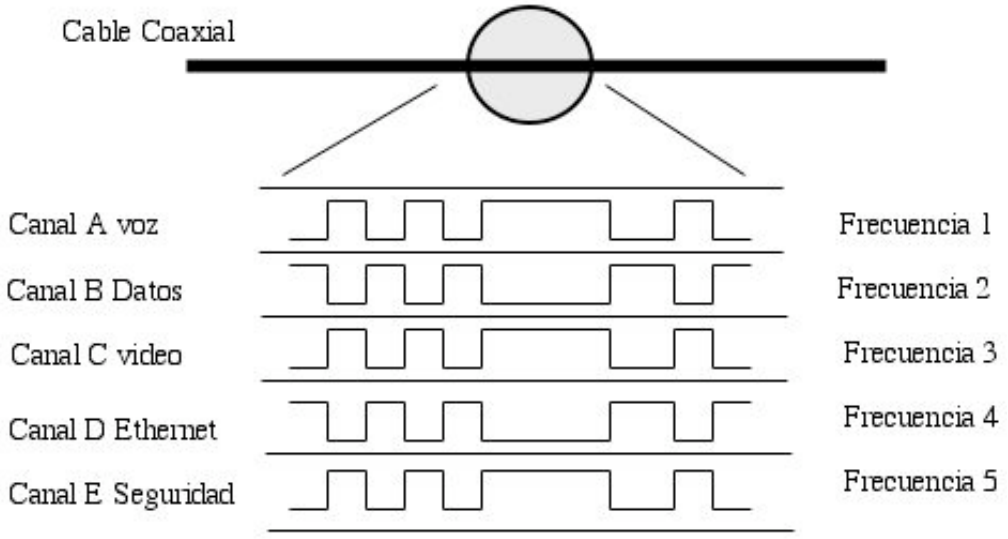


Figura 5.17 Transmisión en banda Ancha (Broadband).

Cable Coaxial

El cable para banda base y el cable coaxial para banda ancha son muy parecidos en su construcción, pero sus principales diferencias son: la cubierta del cable, los diámetros y la impedancia.

El cable coaxial para banda base es de 3/8 de pulgada y utiliza una cubierta de plástico, mientras que el cable coaxial para banda ancha es de 1/2 pulgada y está cubierto de una malla o tela de aluminio y una funda protectora de plástico.

Ethernet, por ejemplo, puede trabajar con ambos cables, pero lo más común es con banda base.

	Banda base	**Banda ancha**
Tipo de Cable	RG-58 A/U	RG-59 o RG-6
Velocidad Máxima de transferencia	10 Mbps	6 MHz
Impedancia	50 Ω	75 Ω
Distancia máxima de segmento	185-500 m	3600 m
Costo	Bajo	Alto
Inducción de ruido	Baja	Alta

Tabla 5.4 Comparativa entre banda base (baseband) y banda ancha (broadband).

5.5.2 IEEE 802.3 10Base5

Este tipo de cable es conocido como cable coaxial grueso, opera en la transferencia de datos a 10 Mbps en una sola banda (banda base) y alcanza distancias máximas de 500 m (10=velocidad en Mbps, Base = una sola banda y 5 = 5 multiplicado por 100 = 500). La impedancia de éste tipo de cable es de 50 Ω y requiere de un terminador en cada extremo para poder enviar información.

El tipo de conectores utilizados en este tipo de cable se conoce como conectores tipo "N".

5.5.3 IEEE 802.3 10Base2

Este tipo de cable se conoce como cable coaxial delgado, opera en transferencias de datos a 10 Mbps en una sola banda. La impedancia de éste cable es de 50 Ω y requiere de un terminador en cada extremo para que la información pueda transmitirse.

Los conectores que utiliza este cable se conocen como conectores tipo BNC.

A diferencia del coaxial delgado que utiliza "T" para conectar los dispositivos al mismo cable, el coaxial grueso utiliza *transceivers* y un tipo de cable conocido como AUI (Attachment Unit Interface), el cual parte del Transceiver al dispositivo que se desea conectar.

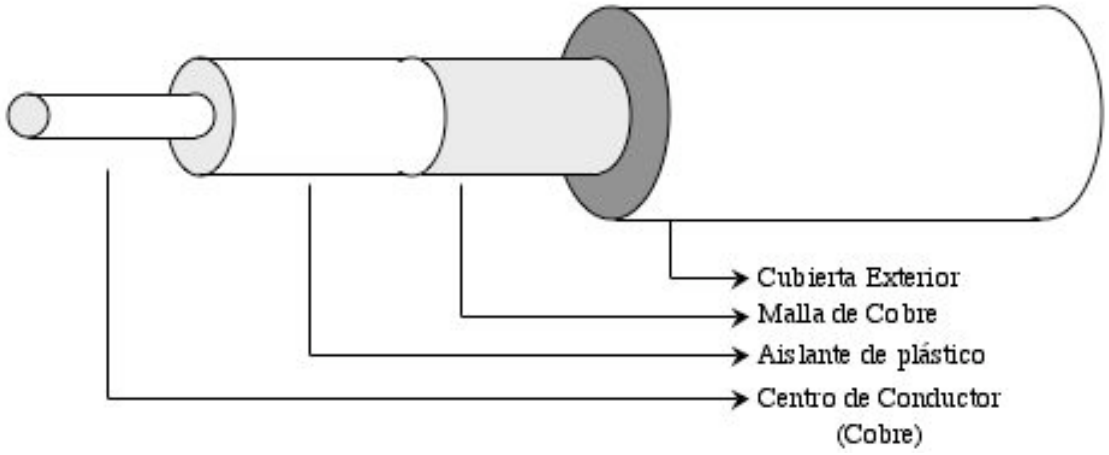


Figura 5.18 Cable Coaxial.

El cable delgado se usa para conectar a un grupo pequeño de dispositivos, los cuales no cambian de lugar con frecuencia. Es ideal para departamentos pequeños o grupos de personas que comparten la misma área física.

El cable coaxial para banda base tiene una cubierta y una malla que evita que las señales externas afecten a la conductividad, como es el caso del cable UTP.

Pueden adquirirse dos tipos de cable coaxial: con cubierta de PVC y Plenum. Estos difieren entre ellos en que la recubierta de PVC lo hace más flexible, mientras que el plenum es más rígido. El plenum soporta mayores temperaturas de calor y llega a resistir en casos de incendio; además, cuando llega a quemarse no genera tanto humo como el PVC y no es tan tóxico.

Ventajas	Desventajas
Bajo costo de mantenimiento	Limitado en distancia y topología
Fácil de instalar y conectar	Poca seguridad. Se daña fácilmente
Mayor resistencia al ruido y a la inducción de otras señales	Mayor dificultad a l efectuar cambios en el cableado

Tabla 5.5 Ventajas y desventajas del cable coaxial.

5.5.4 UTP (Unshielded Twisted Pair) IEEE 10BaseT

El cable de par trenzado se compone de dos cables de cobre con centro sólido, formando una trenza entre ellos.

El cable UTP se utiliza comúnmente en oficinas para los sistemas telefónicos. Por lo general, viene en pares de cuatro, cubiertos por una funda de plástico, y algunas veces tienen cubiertas de aluminio para ayudar a incrementar las velocidades de transmisión de datos y protegerlos del ruido exterior.

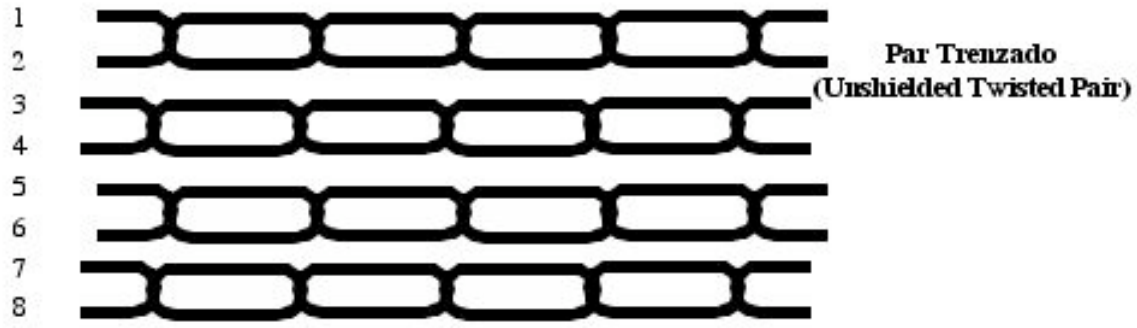


Figura 5.19 Par trenzado.

El cable STP (Shielded Twisted Pair) está sujeto a menor interferencia eléctrica y soporta altas velocidades a través de grandes distancias. Como se mencionó, existen dos tipos de cable: el UTP y el STP, en los cuales la diferencia principal es el recubrimiento que tienen para aislar el ruido, ganar mayores distancias y obtener altas velocidades.

El instituto de ingenieros eléctricos y electrónicos (IEEE) logró generar el estándar 10BaseT, el cual ha tenido mucha aceptación por los administradores de redes y compañías de cableado, ya que éste tipo de cable es mucho más fácil de manejar que el coaxial.

Este cable se recomienda por los estándares de la EIA/TIA 568 para las instalaciones de cableados horizontales. Para este tipo de cableado se requiere del uso de dos pares (cuatro hilos). Se usan dos hilos para la transferencia y dos para la recepción.

Actualmente existen varios niveles en este tipo de cable y la razón es que el nivel del cable se escoge, dependiendo de la velocidad a la que se quiera transmitir; los niveles actuales son los siguientes:

Nivel 3: Este nivel se usa para soportar hasta 10 Mbps y distancias de 90 m. Generalmente se utiliza en redes Ethernet que no pretender utilizar altos volúmenes de transferencia, como pudieran ser imágenes, video, etc.

Nivel 4: Este nivel se utiliza para garantizar hasta 20 Mbps y distancias de 100 m. Este tipo de cable puede utilizarse para las tecnologías de Ethernet y / o Token Ring 4/16 Mbps. Al igual que el anterior, no soporta grandes transferencias de información, como se menciono en el nivel anterior.

Nivel 5: Este nivel es el más utilizado en la actualidad, debido a que garantiza hasta 100 Mbps y 100 m de estación a estación. Es el que se recomienda para la transferencia de imágenes, video, videoconferencia, etc. Entre mayor sea el nivel, también lo son los costos. La diferencia entre cada uno de los niveles es el número de trenzas por pulgada con que cuenta el cable, además del recubrimiento que se le da a cada uno de ellos.

Usar cable que no éste trenzado genera grandes problemas en la comunicación de datos, por ejemplo, problemas de diafonía (cross talk), pérdida de información, etc.

Las especificaciones técnicas del cable son:

- Distancia máxima de 100 m.
- Impedancia de 100 Ω
- Mínimo dos Pares
- Cable de 24 AWG
- Máxima velocidad de transferencia entre 10 y 100 Mbps.

El tipo de conectores que se utilizan en éste tipo de cable son los RJ-45, los cuales tienen un costo muy bajo, al igual que la herramienta necesaria para instalarlos.

Ventajas	Desventajas
Tecnología bien asimilada	Susceptible al ruido
Facilidad al añadir dispositivos nuevos	Limitación en el ancho de banda
Bajo costo	Limitantes de distancia
Puede utilizarse el mismo cable para la red de teléfonos	

Tabla 5.6 Ventajas y desventajas del par trenzado

5.5.5 Fibra Óptica

Los cables de fibra óptica se usan para transmitir señales digitales de datos en forma de pulsos modulados de luz. La fibra óptica consiste en un cilindro de vidrio extremadamente delgado, llamado core (centro) y recubierto de vidrio conocido como cladding.

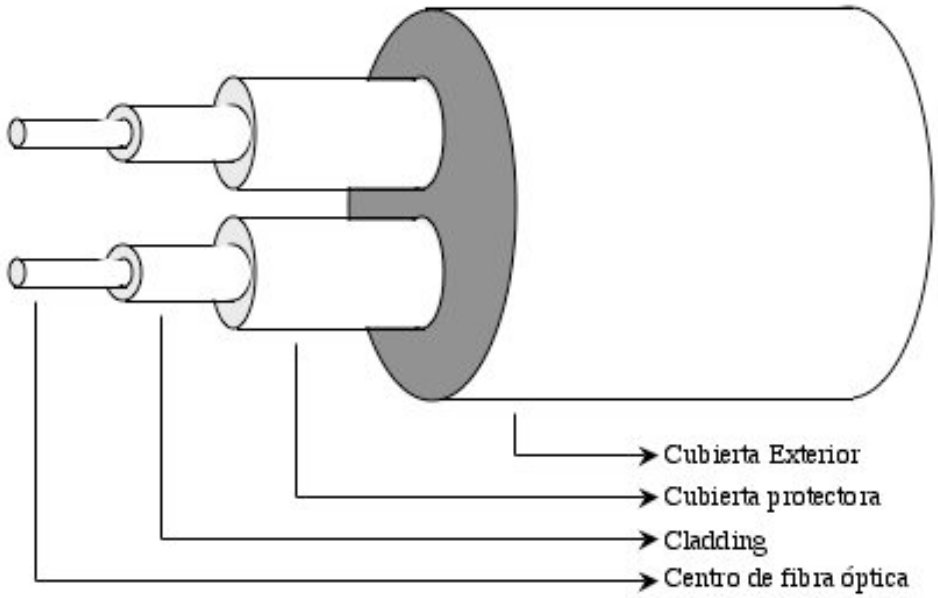


Figura 5.20 Fibra óptica.

La fibra óptica se usa tanto para la transmisión de banda base como para la de banda ancha. Los anchos de banda de tres gigahertz son accesibles con este cable, mientras que los de 400 y 500 MHz los son con el cable coaxial. Debido a los amplios anchos de banda que soporta éste tipo de fibra, se utiliza cada vez más en muy variadas aplicaciones.

Con el cambio constante en la tecnología, la única parte de la red que tiene que actualizarse son los componentes electrónicos y no la fibra; esto también depende de que el tipo de fibra instalado sea el adecuado. Existen dos fibras por cable, una para la transmisión y otra para la recepción. La fibra puede transmitir a 100 Mbps y se ha demostrado que puede llegar a alcanzar velocidades de hasta 200 000 Mbps. Este tipo de cable no esta sujeto a interferencias de ningún tipo.

Debido a su construcción puede alcanzar grandes distancias que van desde los 1000 m hasta los 10 Km. La distancia máxima recomendada por la IEEE es de 1000 m.

Construcción de la Fibra Óptica

Como se menciono anteriormente, la fibra está formada por tres componentes que son: el centro o core, el cladding y el buffer. El core es el centro de la fibra y está fabricado de vidrio, el cladding recubre al core y ayuda a mantener la luz dentro de éste. El buffer es la cubierta de plástico que le da a la fibra una rigidez adicional.

Cada fibra es reconocida por el tamaño del core en relación con el cladding. Por ejemplo, la fibra 62.5/125μ tiene un diámetro de 62.5 micrones en el core y 125 micrones en el cladding. Un micrón es la millonésima parte de un metro. Para tener una idea, cada hoja de papel de un cuaderno tiene, aproximadamente, 25 micrones de grueso.

Tipos de Fibra Óptica

Existen dos tipos de fibra en la actualidad: unimodo (single mode) y multimodo (multimode). La fibra unimodo se utiliza principalmente en telefonía y en telecomunicaciones para alcanzar grandes distancias, esto se debe a que su espectro de luz recorre varios miles de metros antes de requerir algún repetidor. Este tipo de fibra generalmente se maneja con rayo láser, permitiendo la entrada al core de un solo rayo de luz, lo que brinda una clara y fina señal hasta el final del cable.

Nota: Debido a que se utiliza el láser como emisor de luz para enviar la información, si no se maneja con cuidado puede dañar a quien la maneja o instala, ya que la luz de láser es altamente dañina al ojo humano cuando se ve directamente, por lo que su manejo es muy delicado.

La fibra multimodo se usa generalmente en aplicaciones donde las distancias son pequeñas (por ejemplo 10 Km), como es el caso de las redes de área local. Este tipo de fibra es mucho más barata que la anterior y se ilumina con un LED. Debido a que el ancho del core en éste tipo de fibra es mayor, admite que varios rayos entren al core al mismo tiempo, lo que provoca un decremento en el ancho de banda soportado por la fibra.

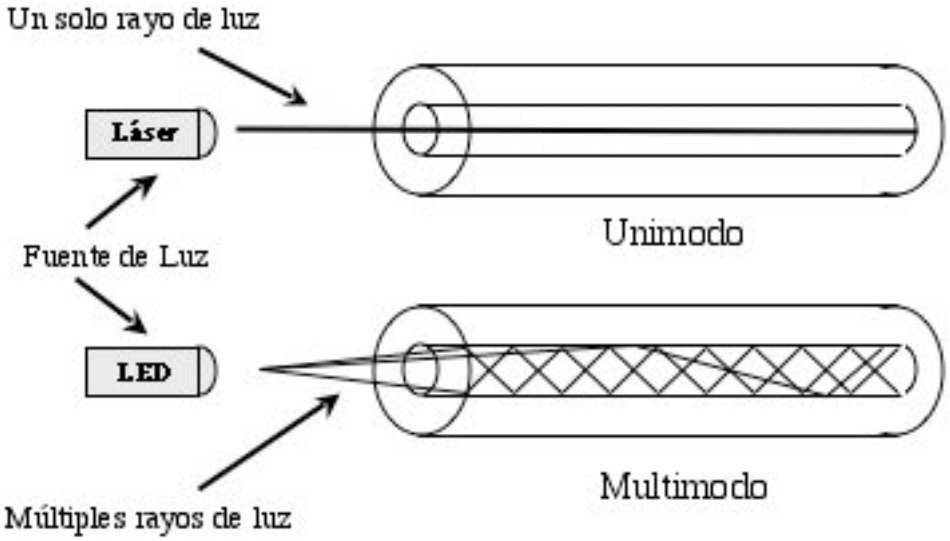


Figura 5.21 Tipos de fibra óptica.

Actualmente existen dos tipos de fibra multimodo en el mercado, que son: step index y grade index. Las fibras step index tienen un gran cambio en el índice de refracción que va del core hacia el cladding, mientras que la fibra de grade index presenta un índice de refracción que decrece gradualmente partiendo del core hacia el cladding.

Nota: La luz utilizada en éste tipo de fibra no daña al ojo humano, por lo que se puede ver directamente al cable sin temor a perder la vista.

El tipo de fibra usada en Ethernet es la fibra multimodo grade index, 62.5/125μ. Aunque existen varios tipos en el mercado, ésta fibra es la más usada por las compañías que fabrican productos para redes de área local.

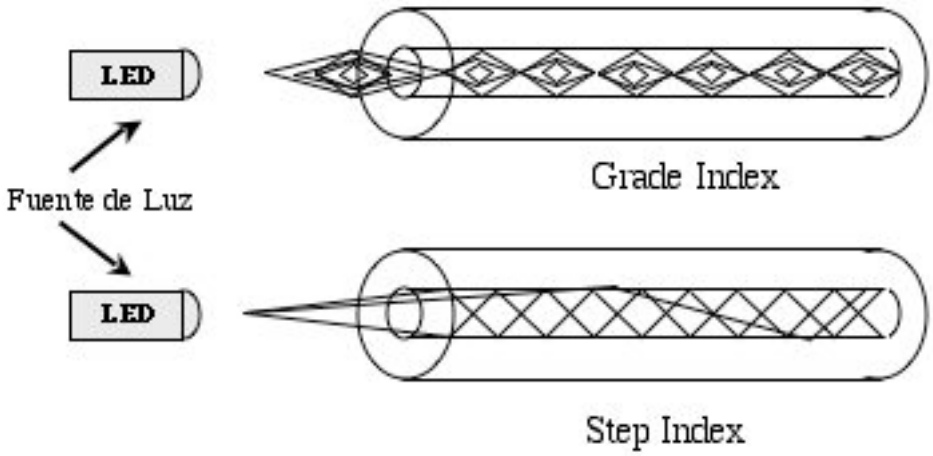


Figura 5.22 Tipos de transmisión en Fibra óptica.

Características Técnicas de la Fibra Óptica

- Precio compatible con el coaxial para banda base.
- Altos niveles de transferencia de datos. 50 Gbps en distancias de 1 Km y 10 Mbps en distancias de 2 Km.
- Grandes distancias. En el caso de Ethernet se pueden tener nodos remotos a distancias de hasta 2 Km sin necesidad de un repetidor.
- No es susceptible al ruido.
- Relativamente difícil de encontrar, es escaso en el mercado. Requiere de herramientas especiales para el armado de los conectores.
- El equipo de pruebas es demasiado costoso.
- La fibra óptica es un enlace punto a punto. Con la tecnología no es posible tener ningún tipo de transferencia multipunto.

Tipos de Conectores

En la actualidad, existen varios conectores para fibra. Algunos de los más populares son: Biconic, FC, Mini-BNC, ST y SMA. Los conectores ST y SMA son los dos más usados en la industria para las redes de área local, y el **conector ST** se ha convertido en el más común y confiable de los dos.

El conector ST es denominado "keyed" twist. Es decir, éste tipo de conector se ensambla con la entrada a la fibra en la misma forma en que se inserta la llave a un auto y se gira para abrir el seguro. Al igual que solo hay una forma de quitar el seguro al coche, de igual forma solo hay una manera de instalar el conector; así, se obtiene una consistencia en la forma de conectar y desconectar la fibra.

El conector SMA, por otro lado, es un conector que se atornilla, lo cual tiene como consecuencia que dependiendo de la persona que realice la actividad, el core puede quedar ya sea centrado con el equipo o bien un poco desfasado, pero lo suficiente para provocar problemas de acoplamiento en la transferencia. Este tipo de conectores se encuentra por lo general en equipos viejos que utilizan Ethernet.

Ventajas	Desventajas
Altas velocidades	Más caro que otros tipos de cables
No es susceptible al ruido	No está dentro de los estándares de la IEEE (draft)
Se utiliza como Backbone de redes de área local	Limitado (prácticamente) a altas velocidades, punto a punto
Soporte a datos, video y voz	Requiere de personal capacitado para su instalación y mantenimiento

Tabla 5.7 Ventajas y desventajas de la fibra óptica.

5.5.6 AUI (Attachment Unit Interface)

Este tipo de cable es conocido como el cable para transceiver. Es del tipo STP y se usa principalmente para la tecnología Ethernet. El conector utiliza el DB-15 definido por la IEEE, aunque sólo ocupa 4 pines para lograr la conectividad, dos para transmisión y dos para recepción. La impedancia de éste tipo de cable es de 78Ω.

Hay dos formas de utilizar este tipo de cable que son: el cable AUI de oficina y el cable IEEE 802.3 AUI. El cable AUI para oficina es relativamente más flexible y fácil de manejar, además de que al conectarse en la parte posterior de las computadoras su instalación es mucho más sencilla, comparándolo con el cable IEEE 802.3. El hecho de tener un cable más manejable también reduce sus características técnicas.

El cable AUI es el único cable que además de transmitir información, también puede conducir corriente eléctrica o potencia suficiente para hacer que el transceiver funcione.

IEEE 802.3 AUI	AUI de Oficina
Cable STP de 20 AWG	Cable STP de 28 AWG (más flexible)
Distancia máxima de 50 m	Distancia máxima de 16.5 m
Relativamente más caro que el cable telefónico	Menos caro que el IEEE 802.3 AUI
Pins out bajo el estándar IEEE 802.3	Pins Out bajo el estándar IEEE 802.3
Impedancia de 78Ω	Impedancia de 78Ω

Tabla 5.8 Comparativa entre AUI 802.3 y AUI de Oficina.

Estándares de Cableado

El sistema de cableado es el tipo de material que se utiliza para cumplir con los estándares de la EIA en relación con el tipo de cable, velocidad de transmisión, número de hilos por cable, impedancia y distancias máximas; en la actualidad existe una gran variedad de sistemas para cableados que cada proveedor o fabricante pone a la venta. Dentro de éstos, los más usados son: el sistema Systimax PDS de la compañía AT&T, el de la compañía Simeón y el de ModTap.

En general, todos los sistemas de cableado se componen de cables de cobre y de fibra óptica, bloques de interconexión, bloques y terminales protectoras, adaptadores, dispositivos de interfaz electrónica y equipo estándar para el cableado en edificios (EIA/TIA 568).

La gran mayoría de las instalaciones con estos sistemas de cableado utiliza una topología en estrella, llegando a un cuarto de cableado (MDF o IDF) en donde se encuentran los denominados Patch panel, liu, cables de parcheo, etc.

Los sistemas de cableado se utilizan para administrar eficientemente la instalación, ya que se lleva un estricto control de los puertos que se están utilizando y al mismo tiempo se usan para la puesta en marcha de las redes de voz y datos y se llaman sistemas de cableado estructurado.

5.6 TECNOLOGÍAS LAN

En la actualidad existe una gran variedad de tecnologías de redes de área local, como las tecnologías Ethernet, Token Ring, FDDI y ATM. Cada una de éstas tecnologías opera de manera diferente debido a que fueron desarrolladas en distintos ambientes y con métodos de acceso diferentes.

Ya que cada tecnología se desarrollo por una compañía diferente, las organizaciones internacionales como la ISO, IEEE, etc. generaron reglas de la forma en que deben operar éste tipo de tecnologías en cualquier ambiente.

5.6.1 Ethernet

La tecnología Ethernet es la más usada en la actualidad, su primera implementación fue en la empresa Xerox, por Robert Matcalfe, a principios de 1970, para conectar hasta 100 computadoras en un área de 100 Km, con una transferencia de información de 2.94 Mbps. Ha sido la ideal en la industria y oficinas donde no es obligatorio un tiempo de respuesta determinístico.

En 1978 se publico la primera norma, como un trabajo conjunto de las empresas Digital, Intel y Xerox. Esta es la base del estándar ANSI/IEEE 802.3 publicado en 1983 por la IEEE. La norma internacional ISO 8802/3 también está basada en la especificación de 1978.

La tecnología Ethernet se utiliza principalmente en las topologías en BUS y Estrella, y puede ser usada en banda base (baseband) o en banda ancha (broadband), en donde el estándar para ésta última es el IEEE 10Broad36. El método de acceso a la red es el CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Este funciona de forma que primero tiene que escuchar el medio para asegurarse de que nadie esté transmitiendo en ese momento. Si nadie lo está haciendo, comienza la transmisión; por otro lado, en el caso de que el medio esté siendo ocupado por otro dispositivo, espera un tiempo aleatorio y vuelve a intentar. Si llegara a suceder que dos dispositivos escucharan el canal al mismo tiempo y comenzaran a transmitir, la información chocaría en un punto de la red, lo que

originaria una Colisión (Collision); esto se debe a que existen tiempos de propagación de la información, por lo que el dispositivo no solo escucha el canal para poder transmitir información, sino que también lo hace mientras está transmitiendo y cuando se llevan a cabo colisiones. Debido a esto, cada dispositivo puede retransmitir su información, pero antes de hacerlo espera un tiempo aleatorio dado por un algoritmo, con lo que se minimiza el número de colisiones en una red.

Esto es algo parecido a lo que sucede cuando se esta en una junta de trabajo y de pronto dos personas empiezan a exponer sus ideas al mismo tiempo, lo cual origina una degradación en la conversación. Después de un rato, ambas guardan silencio y escuchan si nadie está hablando, y en éste momento otra persona comienza a hablar. De la misma manera en que se entablan conversaciones en los grupos de personas se establecen comunicaciones en las redes con el método de acceso CSMA/CD. La forma en que las redes Ethernet transmiten sus datos se llama **Datagrama o Trama**.

La información que se envía de la computadora emisora a la receptora se pone en datagramas, y cada datagrama contiene parte de la información. La información que viaja en cada trama que se transmite a la red es la siguiente:

	Preámbulo	SFD	Destino	Fuente	Longitud	Información	FCS
Bytes:	7	1	6	6	2	46-1500	4

IEEE 802.3

	Preámbulo	SFD	Destino	Fuente	Longitud	Información	FCS
Bytes:	7	1	6	6	2	46-1500	4

Ethernet

Figura 5.23 Trama Ethernet

5.6.2 Token Ring

Cuando IBM coloco en el mercado las redes Token Ring, inmediatamente se convirtió en el competidor número uno de las redes Ethernet 802.3. El comité de la IEEE 802.5 ha desarrollado estándares para las redes Token Ring, así como algunos de sus componentes. Conocer a fondo la funcionalidad de las redes 802.5 permite tener un mejor panorama del comportamiento de las redes cuando se habla de Bridges (puentes) y Routers (enrutadores).

Las redes Token Ring, a diferencia de las redes Ethernet, son determinísticas y no probabilísticas. El método de acceso que utiliza éste tipo de tecnología se conoce como Token Passing, el cual está diseñado para operar en redes con topología en anillo, aunque físicamente son cableadas en forma de estrella, utilizando una unidad MSAU (Multistation Access Unit). Las estaciones de trabajo transmiten su información en paquetes llamados **tramas**. El comité 802.5 publico un conjunto de especificaciones sobre la trama Token Ring. Originalmente, está tecnología transmitía a 4 Mbps, y después de varios años un conjunto de empresas, incluida IBM, logró alcanzar velocidades de 16 Mbps.

La forma en que la información viaja de una estación a otra es por medio de un Token. El Token es el mecanismo por el cual se puede transmitir información. Si una estación de trabajo posee el Token, puede transmitir; si no cuenta con él, tiene que esperar su turno. Debido a que la información viaja en forma de anillo, el Token recorre cada una de las estaciones conectadas a él, de tal forma que al momento de recibirlo, cada una de las estaciones lee el paquete para saber si le corresponde; en caso negativo, lo retransmite al anillo, de la misma forma que trabaja un repetidor, por lo que cada vez que una estación de trabajo lee el mensaje y lo regresa a la red, es un paquete nuevo con la misma información. Este proceso de leer y enviar el paquete es lo que determina que no exista un número máximo de nodos conectados al anillo.

Cuando el Token regresa a la estación que origino el mensaje, ésta verifica que la información haya sido entregada correctamente y entonces libera el Token a la siguiente estación de trabajo. Debido a éste fenómeno es posible garantizar tiempos de respuesta en las redes, por lo que se les denomina redes deterministicas.

Las redes 802.5 difieren de las redes IBM, debido a que el estándar IEEE 802.5 no ha podido igualar las reglas de funcionamiento de las redes Token Ring de IBM, por lo que se debe tener cuidado al momento de juntar redes 802.5 y redes IBM. De alguna forma, IBM sigue empleando algún tipo de interrupción relacionado con las tarjetas de red (hardware), por lo que es importante saber si la tarjeta se está comprando tiene el chip de IBM o solamente está bajo los estándares 802.5. Algunas de las diferencias entre las redes IBM y las rede 802.5 radican en el empleo de memoria (buffering), el software de comunicaciones y la calidad de los controladores de software (drivers).

5.6.3 FDDI

La necesidad de transmitir a mayores velocidades fue debido al requerimiento de transmitir aplicaciones gráficas y de video, las cuales necesitan enviar millones de bits en tiempos muy cortos, lo que obliga a tener redes de altas velocidades como son las redes FDDI (Fiber Distributed Data Interface), que transmiten a 100 Mbps.

FDDI es un conjunto de estándares que definen la compartición del medio a 100 Mbps, con fibra óptica como transporte (unimodo o multimodo) o similares al IEEE 802.5, en el que es posible usar el cable UTP. El proceso de estandarización comenzó en 1982 y logró su estabilidad a finales de los 80. FDDI utiliza una tecnología de Token y fue desarrollada para poder soportar la interconexión con las redes de área local, aunque en sus inicios se consideraba el uso de ésta tecnología solamente para el backbone (columna vertebral de la red) en edificios o campus. En la actualidad, existen empresas que han llevado ésta tecnología a cada una de las estaciones que forman la red de área local.

Las redes FDDI se componen de un anillo doble, el cual ayuda a mantener un nivel de tolerancia a las fallas en el caso de que se presenten en alguna parte de la red. Uno de los anillos es el encargado de transmitir datos, mientras que el otro se utiliza para transmitir tramas de control.

Los estándares definen los componentes de las redes que se deben incluir, éstos son: SAS (Single Attachment Station), DAS (Dual Attachment Station) y sus conectores respectivos. Las estaciones que usan SAS están conectadas a un concentrador con topología en estrella. Las ventajas y

desventajas que esto trae consigo son las mismas que se mencionaron cuando se explicó la tecnología en estrella; entre las principales se pueden mencionar las que siguen.

1) La falla en una de las estaciones, tanto en cableado como hardware, no afecta el funcionamiento de la red.
2) La falla en el concentrador provoca que la red entera deje de funcionar. Las estaciones conectadas en DAS, por lo general, forman una topología en anillo.

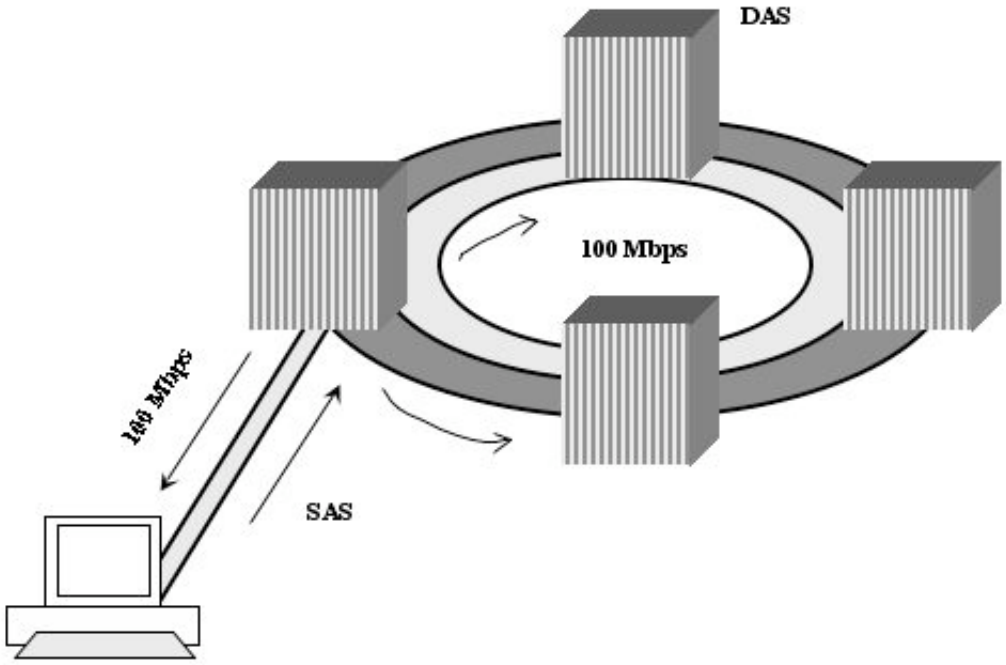


Figura 5.24 FDDI

Las redes FDDI pueden alcanzar distancias entre 3 y 40 Km, dependiendo del tipo de fibra que se emplee. En el caso de fibra óptica, el tipo 62.5/125 µm es una de las más usadas. El método de acceso utilizado en FDDI es Token Passing, al igual que en las redes Token Ring. Sin embargo, en éste tipo de tecnología se pueden tener múltiples tramas al mismo tiempo en el anillo, sin que éstas tengan que ser reconocidas por sus destinatarios; además, utiliza transferencia de información asíncrona, lo que genera una mayor velocidad de transferencia. La trama de FDDI tiene un tamaño máximo de 4500 bytes, lo que es ideal para transferir grandes volúmenes de información.

5.6.4 ATM

ATM (Asynchronous Transfer Mode) es el nuevo acrónimo en la nomenclatura de redes. Las redes ATM son consideradas redes de tercera generación, debido a que rompen con el esquema que se venia utilizando en la transferencia de información. La tecnología ATM usa un método bastante flexible para poder transportar diferentes tipos de información (por ejemplo: voz, datos y video) entre los dispositivos de una red de área local (LAN) o red de área amplia (WAN). La tecnología utilizada para transportar los datos se conoce como intercambio de celdas (Cell Switching), las cuales son de tamaño fijo.

ATM fue propuesto originalmente por la industria de las telecomunicaciones. La primera recomendación fue hecha por la CCITT en 1988, proponiendo a ATM y la red óptica síncrona SONET

(Synchronous Optical Network) como las base de B-ISDN (Broadband-Integrated Services Digital Network).

Se llama modo de transferencia a una de las técnicas de telecomunicaciones usada para transportar información de un punto a otro. El primer modo de transferencia se hizo en forma de intercambio de mensajes. En éste, el paquete tenía una dirección destino, una dirección fuente y el mensaje mismo. La estrategia en éste modo de transferencia está basada en las operaciones de los seres humanos, quienes deciden que hacer con cada mensaje.

Las redes ATM son redes orientadas a conexión (connection-oriented); debido a esto, lo primero que hacen es establecer una conexión con la estación con la que desean intercambiar información y validar que dicha conexión sea exitosa. Una de las principales diferencias entre el modo de transferencia de conmutación de paquetes (packet switching) y la conmutación de celdas (cell switching) es que ésta última mantiene un circuito abierto permanente con la estación remota hasta que termina la comunicación, y aun cuando no se éste transmitiendo, permanece abierto; por otro lado, el modo de transferencia de conmutación de paquetes establece un circuito con la estación remota solamente cuando necesitan intercambiar información, lo que ayuda a mantener un tráfico estable. La diferencia entre cerrar el circuito o dejarlo abierto, depende del tipo de información que se desee transmitir; por ejemplo, en el caso de transmitir video o voz, el hecho de abrir el circuito y cerrarlo ocasiona un cierto retraso que provoca que la información no llegue bien, como pérdida de cuadros de video, descontinuados o vacíos en la voz. ATM es una nueva tecnología con la capacidad de soportar cualquier tipo de tráfico a las más altas velocidades dentro de una red.

Como se menciono en párrafos anteriores, ATM ésta basado en la conmutación de celdas. Este concepto combina los beneficios de la conmutación de circuitos y paquetes usando la conmutación rápida de paquetes FPS (Fast Packet Switching). FPS utiliza la alta confiabilidad de la tecnología para la transmisión digital y la alta calidad en la transmisión del medio, lo suficiente para no tener que detectar y corregir errores en cada nodo de la red, por lo que se ahorra tiempo. La información es empaquetada en pequeñas tramas de longitud fija llamadas celdas. Cada celda tiene una longitud de 53 bytes, de los cuales 5 bytes se utilizan para el encabezado y 48 bytes para el resto de la información (datos).

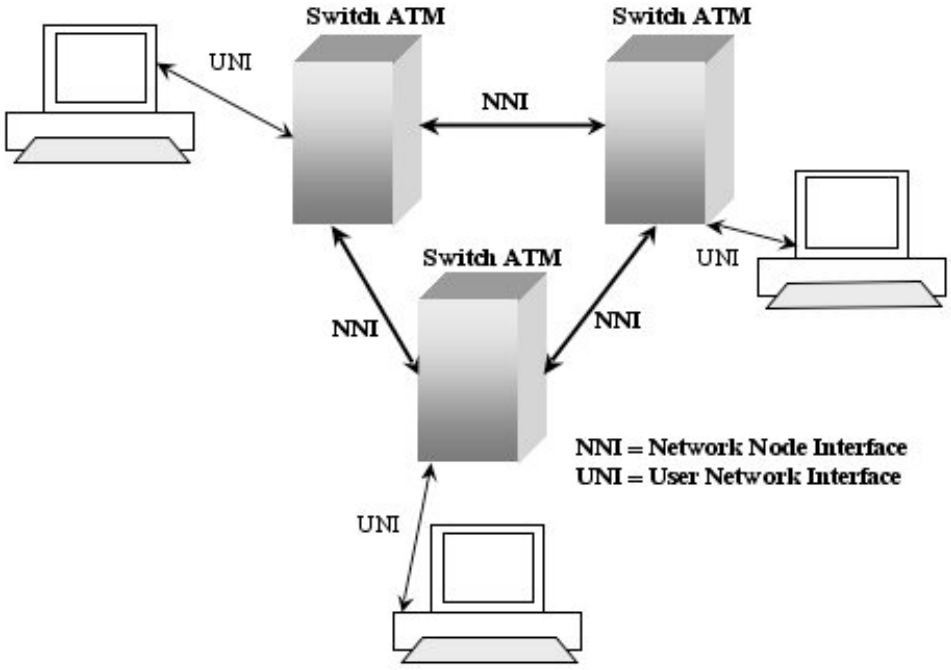


Figura 5.25 Red ATM.

5.7 PROTOCOLOS DE COMUNICACIÓN

Un protocolo es el conjunto de normas o procedimientos necesarios para iniciar y mantener una comunicación.

En el caso de las redes de computadoras, un protocolo es un conjunto de normas que permiten que dos o más computadoras puedan comunicarse. El protocolo consta de una sintaxis, una semántica y un tiempo. La **sintaxis** en un protocolo define los conjuntos de bits (una serie de unos y ceros) divididos en campos. Por ejemplo, los primeros 48 bits son la dirección fuente y los siguientes 48 son la dirección destino. La **semántica** define el significado exacto de los bits dentro del campo. Por ejemplo, una dirección de 48 bits iguales (unos), significa que es una dirección Broadcast; es decir, que puede ser leída por todas las computadoras de la red. El **tiempo** define la relación entre el rango de los bits dentro de los campos y las pausas entre reconocimiento de los mismos.

5.7.1 TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) es probablemente uno de los protocolos de comunicación más antiguos en los estándares de Inter-redes (redes interconectadas). TCP/IP se desarrollo por la Agencia de Proyectos de Investigación Avanzada de la Defensa de los EUA (DARPA-Defense´s Advanced Research Project Agency), DARPA convierte todos los viejos sistemas ARPANET para correr o ejecutar los protocolos de Internet.

El protocolo de comunicaciones es flexible y permite la transmisión de tramas sin errores entre diferentes sistemas, ha estado funcionando ya desde hace varios años. Debido a que es un protocolo de transferencia de información, puede enviar grandes volúmenes de información a través de redes no confiables, garantizando que ésta será recibida sin errores al momento de alcanzar su destino final.

Cuando se utiliza TCP/IP, la información viaja en segmentos creados por TCP entre emisor y receptor para poder acceder a alguna aplicación. Los segmentos creados por TCP son encapsulados en IP, ésta encapsulación se le llama **Datagrama IP**. El datagrama IP permite que los segmentos TCP que fueron creados por alguna aplicación puedan ser transmitidos o enrutados en la red de área local o en la red de área extendida.

Las redes TCP/IP permiten que la información pueda enviarse de un sistema a otro, sin que éstos tengan que ser del mismo fabricante; por ejemplo, una estación con Windows NT, de Microsoft, puede intercambiar información con una computadora con Pathworks, de Digital, siempre y cuando utilicen el mismo protocolo de comunicaciones, como en éste caso es TCP/IP.
TCP/IP, al igual que OSI, tiene niveles funcionales, los cuales se muestran en la siguiente figura:

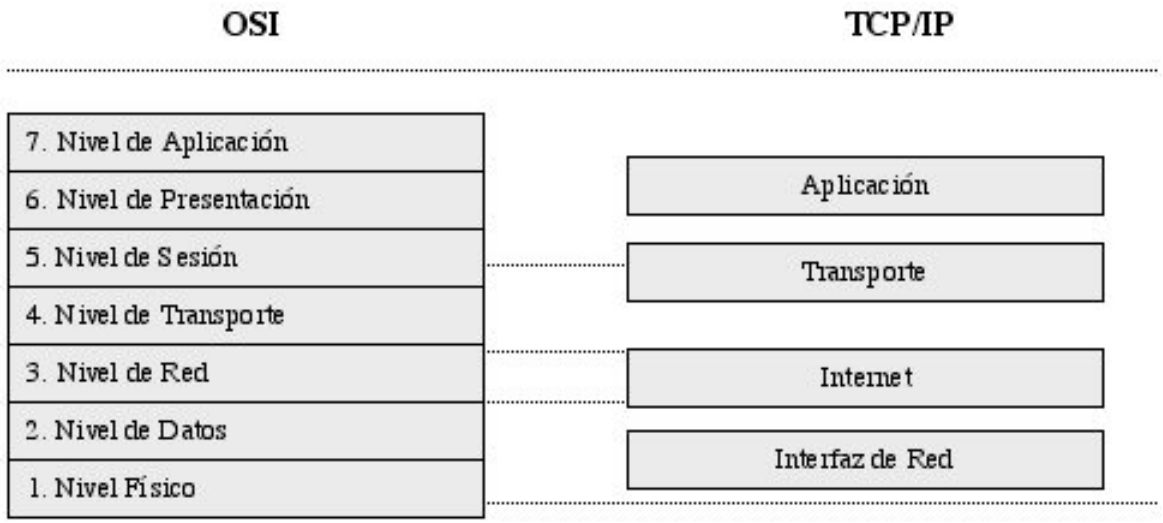


Figura 5.26 Comparación de los niveles de TCP/IP con los de OSI.

5.7.2 SNA

Las redes SNA (System Network Architecture) han sido el punto principal en la estrategia de redes de IBM desde el momento en que se introdujeron a l mercado en 1974. Este tipo de redes se ha implementado en una gran variedad de productos, tanto de IBM como de otras marcas. Aunque el desarrollo de SNA es controlado por IBM, su impacto ha sido muy positivo a través de una gran variedad de estándares en la industria de la computación. IBM estima que existen más de 300 000 redes SNA en todo el mundo. Las redes SNA son particularmente importantes en grandes corporaciones. Por ejemplo, la mayoría de las empresas del Fortune 1000 tiene instalaciones SNA.

El alcance de SNA no esta limitado a la línea de productos IBM. Virtualmente, la mayoría de las industrias de computadoras incluye compatibilidad con SNA en sus productos de redes y en sus líneas de computadoras. Aunque SNA fue diseñado originalmente para implementaciones con IBM, se ha convertido en el estándar de facto en la industria de redes.

Las redes SNA se encuentran posicionadas en las redes de comunicaciones abiertas, como las redes TCP/IP, OSI y DEC. En la actualidad, la importancia de las redes SNA es cada vez mayor, debido

a que las grandes instituciones requieren de conectividad entre éste tipo de redes y otras más del mercado. Los niveles funcionales de SNA comparados con OSI se muestran a continuación:

OSI	SNA
7. Nivel de Aplicación	Servicios Transaccionales
6. Nivel de Presentación	Servicios de Presentación
5. Nivel de Sesión	Control de Flujo de Datos
4. Nivel de Transporte	Control de Transmisión
3. Nivel de Red	Control de la Ruta
2. Nivel de Datos	Control de Enlace de Datos
1. Nivel Físico	Control Físico

Figura 5.27 Comparación de los niveles de SNA con los de OSI.

5.7.3 NetBEUI

NetBEUI proviene de una extensión de la interfaz al usuario de NetBIOS y fue introducido principalmente por IBM en 1985 como un protocolo pequeño, eficiente y rápido.

NetBEUI fue desarrollado en 1985 asumiéndose que las redes de área local tendrían segmentos de 20 a 200 estaciones y que todas ellas formarían grupos de trabajo. También existirían compuertas (gateways) que permitirían unir varios segmentos de redes de área local y / o la conexión con los mainframes.

NetBEUI fue optimizado para obtener mayor rendimiento al usuario de redes departamentales o en segmentos de redes a redes. Actualmente, las redes de la casa de software Microsoft utilizan éste protocolo de comunicaciones para interconectar sus redes. Microsoft ha desarrollado varias versiones del protocolo, siendo la última la versión 3.0, en la cual se corrigieron algunas limitantes, como son:

- NetBEUI 3.0 junto con el nivel TDI (Transport Drive Interface) elimina la limitante de 254 estaciones como máximo en la tarjeta de red del servidor.
- NetBEUI es completamente autoconfigurable.
- NetBEUI proporciona mejor rendimiento en redes y conexiones de baja velocidad.

En realidad, NetBEUI 3.0 no es el original, es una trama de protocolo de forma NetBIOS (NBF). Utiliza las interfaces de NetBIOS en los niveles superiores, pero NBT conforma la interfaz de los controladores de trasporte TDI.

Ventajas:

- Protocolo rápido en segmentos departamentales.
- Uso de poca memoria

Desventajas:

- No es enrutable

- Tiene un rendimiento inferior en redes WAN

5.7.4 IPX/SPX

IPX/SPX (Internetwork Packet Exchange/Sequent Packet Exchange) es el protocolo de comunicaciones de las redes NetWare de Novell.

El protocolo de comunicaciones es propietario y se usa solamente en redes NetWare. Debido a su gran aceptación en el mercado, ha logrado ser uno de los sistemas operativos de red de área local más populares, por lo que las compañías que fabrican y diseñan equipos han logrado enrutar el protocolo independientemente de que éste no sea enrutable.

Su comportamiento en redes de área local pequeñas es aceptable y aun en redes grandes su rendimiento es bueno. Los equipos de enrutamiento envían tramas de una red a otra utilizando un puente de información (bridge) en lugar de enrutarlas.

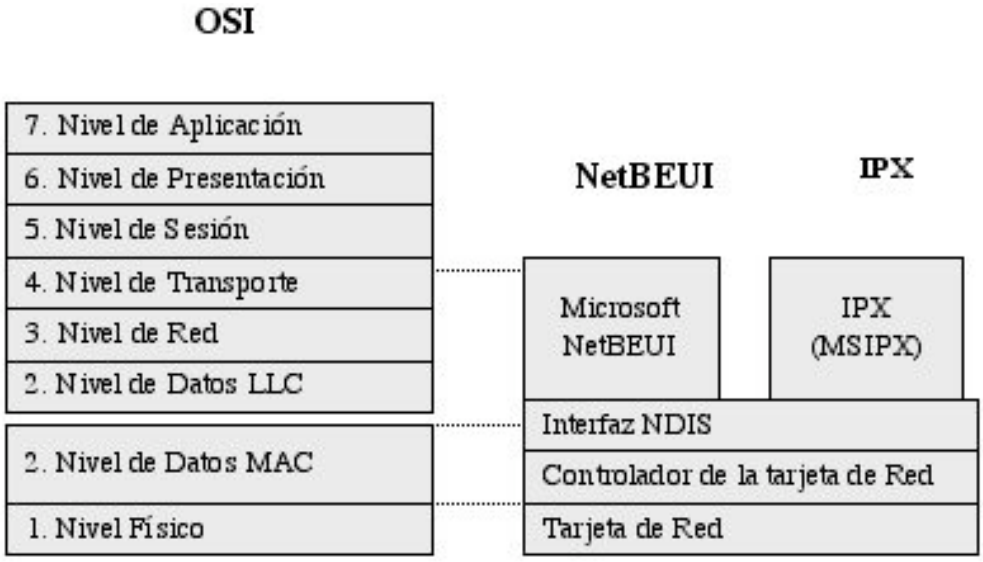


Figura 5.28 Comparación de los niveles OSI con NetBEUI e IPX.

5.8 EQUIPOS DE COMUNICACIÓN

Los diferentes componentes que interconectan a las redes de área local para poder extenderlas, administrarlas, combinar tecnologías, etc. son conocidos como equipos de comunicación.

Dentro de los equipos de comunicaciones más usuales se encuentran los módems, los encriptores, concentradores inteligentes, repetidores, puentes (bridges), enrutadores (routers) y las tarjetas de PC.

5.8.1 Concentradores Inteligentes (HUB)

Los concentradores inteligentes son dispositivos electrónicos capaces de concentrar grandes volúmenes de computadoras en áreas pequeñas. Los concentradores son cajas de circuitos, tarjetas y conectores electrónicos, en los cuales se insertan las tarjetas de red de la tecnología que se quiera utilizar; por ejemplo, Ethernet, Token Ring, FDDI, etc.

Dentro del concentrador existe una tecnología de conmutación de paquetes (packet switching), en la que se puede obtener una alta concentración de paquetes por segundo.

Esta clase de equipo es muy utilizado en compañías que tienen muchos nodos y desean concentrarlos en un solo lugar, sin romper las limitantes de distancia de los cables UTP. La mayoría de los concentradores posee herramientas de administración y monitoreo, para verificar y diagnosticar constantemente las condiciones de la red.

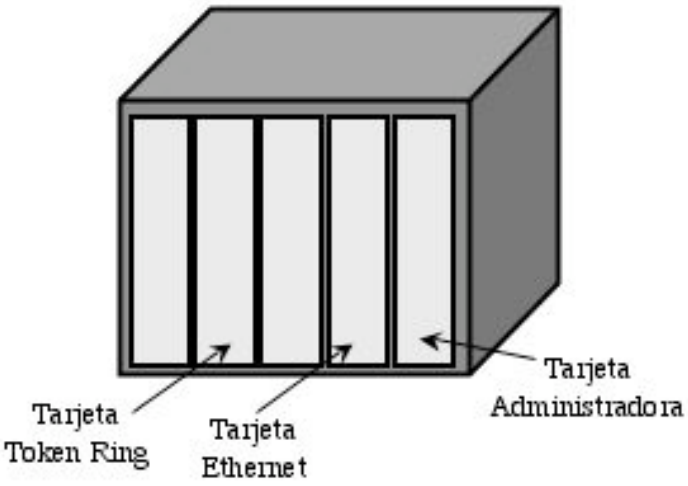


Figura 5.29 Concentrador Inteligente (HUB)

5.8.2 Repetidores

Los repetidores son equipos diseñados específicamente para redes broadcast, como es el caso de Ethernet, y como su función principal es amplificar la señal que recibe en su entrada y amplificarla a su salida. Debido a que los repetidores amplifican las señales, también amplifican el ruido, por lo que debe tenerse cuidado al momento de seleccionar alguno de ellos. La relación de éste equipo con el modelo OSI, es que el repetidor trabaja en el nivel Físico.

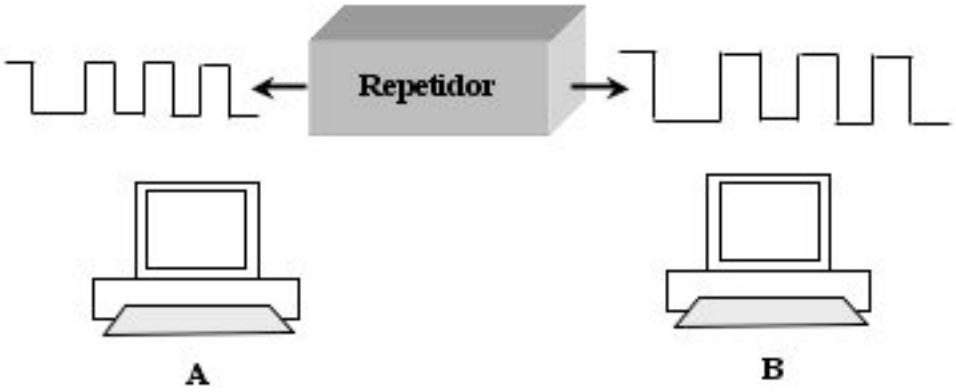


Figura 5.30 Repetidor

5.8.3 Puentes (Bridges)

Los puentes de redes de área local constan de un hardware y un software necesarios para unir dos o más tipos de redes. A diferencia de los repetidores, los puentes pueden unir dos tipos de redes diferentes debido a que no sólo están compuestos de hardware, sino que requieren de software para conectarlos.

Los puentes más simples del mercado examinan las direcciones físicas de los paquetes que viajan en la red y comparan éstas con las direcciones que tienen almacenadas en una tabla para

verificar si la dirección destino se encuentra en el mismo segmento. Si es así, el paquete no es enviado al otro lado de la red.

Al proceso de examinar las direcciones físicas de destino y decidir si los paquetes son transmitidos al otro lado de la red, sin que el usuario tenga que hacer ningún tipo de programación a los equipos, se le llama **puenteo transparente** (transparent bridging). Esta técnica se utiliza por todos los puentes Ethernet y por algunos Token Ring.

Algunos puentes generan sus propias tablas, las cuales son almacenadas en memoria RAM, lo que hace que las comparaciones de direcciones sean más rápidas. Los puentes no toman en cuenta los protocolos de niveles altos. Su función está localizada en el sub-nivel MAC del nivel de datos del modelo OSI. Mientras ambas redes de los puentes sean estándares con la IEEE 802.2 LLC (Logical Link Control), el puente puede segmentar las redes independientemente del tipo de medio y método de acceso que estén utilizando.

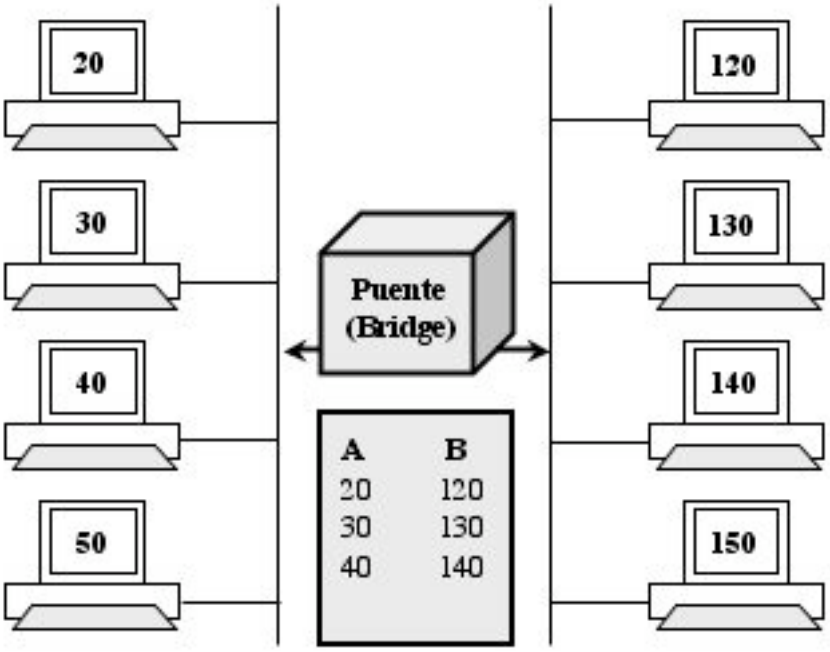


Figura 5.31 Puente (bridge).

5.8.4 Ruteadores

Los ruteadores operan principalmente en el nivel 3 (capa de red: Network layer) del modelo OSI. Mientras los puentes no toman en cuenta los protocolos de los niveles superiores, los enrutadores si lo hacen. Están diseñados para soportar ciertos tipos de protocolos como son TCP/IP, XNS, NetBIOS, DEC, etc.

Estos protocolos utilizan los esquemas de direccionamiento, verificación de errores y técnicas de enrutamiento que caracterizan a cada uno de ellos. Algunos enrutadores sofisticados son capaces de manejar enrutamiento de paquetes de una red a otra, independientemente del tipo de redes que se esté utilizando, por ejemplo: una red Ethernet puede intercambiar mensajes con una red Token Ring y viceversa.

Los Ruteadores requieren de software más sofisticado y, en consecuencia, de mayor conocimiento para utilizarlos y operarlos.

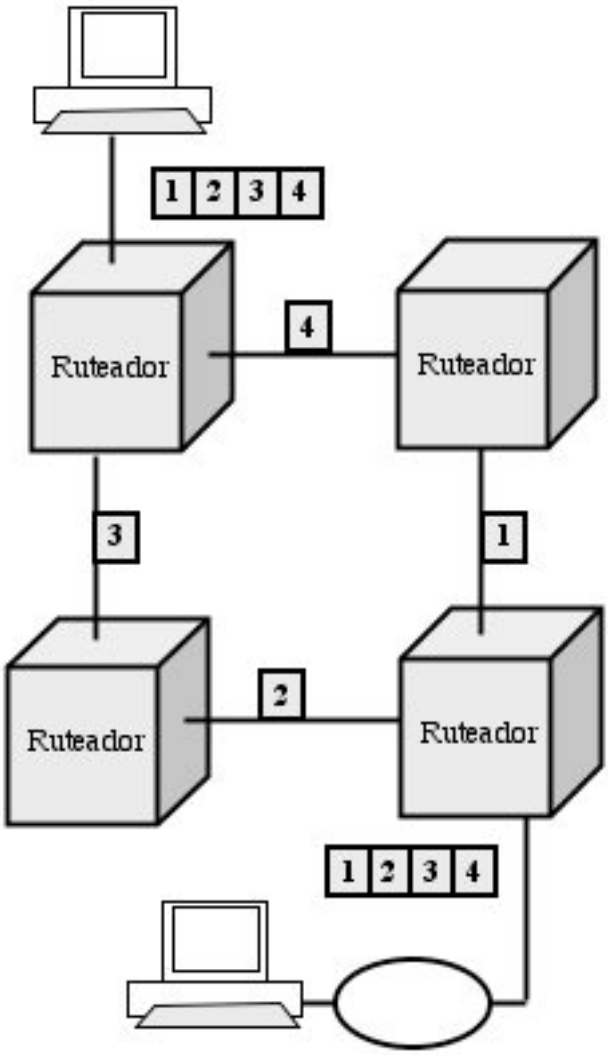


Figura 5.32 Ruteador (Router).

CAPÍTULO 6

EL PROTOCOLO TCP/IP

6.1 DESCRIPCIÓN GENERAL DE LOS SERVICIOS TCP/IP

El protocolo TCP/IP es ampliamente utilizado, debido a su capacidad para conectar redes locales y extensas redes heterogéneas que lo convierten en un buen integrador. Igualmente importante es que sirve de base para las comunicaciones Par a Par y ofrece servicios genéricos sobre ésta base. Además, TCP/IP se diseño desde el principio para permitir interacciones cliente / servidor.

Comunicación entre Aplicaciones

Existen dos estilos de interacción entre aplicaciones. La comunicación orientada a conexión resulta apropiada cuando las aplicaciones necesitan un flujo continuo de información. Al contrario, las aplicaciones implicadas en una comunicación no orientada a conexión intercambian mensajes independientes. La comunicación no orientada a conexión es más apropiada para las interacciones esporádicas con intercambio de pequeñas cantidades de datos.

6.1.1 Comunicación Orientada a Conexión de TCP

La parte TCP de TCP/IP significa Protocolo de Control de Transmisión, y ofrece comunicaciones "par a par", fiables y orientadas a conexión. Las sesiones de conexión remota y transferencia de archivos utilizan TCP.

6.1.2 Comunicación no Orientada a Conexión de UDP

Algunas interacciones de datos no requieren una interacción continua. Por ejemplo, supongamos una base de datos en un servidor de la red que contiene los nombres del personal de la compañía y sus números de teléfono. Se podría buscar un número de teléfono enviando un mensaje de petición al servidor con el nombre de la persona. El servidor podría responder con un mensaje que contuviese el número del teléfono.

El Protocolo de Datagramas de Usuario UDP (User Datagram Protocol) ofrece éste tipo de interacción.

Interfaz de Programación de Conectores

Los sistemas que disponen de TCP/IP normalmente disponen de una interfaz de programación de comunicaciones para los desarrolladores de software. La mayoría utilizan una interfaz de programación de conectores, definida inicialmente para el sistema operativo Unix de Berkeley. La interfaz de programación de conectores incluye:

- Subrutinas básicas para crear, transmitir y recibir los mensajes independientes que se usan en las comunicaciones de UDP no orientadas a conexión.
- Rutinas para establecer una conexión de TCP, enviar y recibir datos y cerrar la conexión.

Interfaz de Programación de Llamadas a Procedimientos Remotos

Aunque no tan relevante como la interfaz de programación de conectores, la interfaz de programación cliente / servidor Llamadas a procedimientos remotos (RPC – Remote Procedure Call) está muy extendida.

Un cliente que use una interfaz RPC invoca a una subrutina que automáticamente hace que se envíe una petición a un servidor. El servidor ejecuta la subrutina y devuelve al cliente los parámetros de la salida de la subrutina. Este escenario se llama apropiadamente una Llamada a procedimiento

remoto ya que un procedimiento al que se invocó localmente se ejecuta en un sistema remoto. Por ejemplo, la aplicación de búsqueda de número de teléfono, descrita anteriormente, podría haberse escrito con rutinas de RCP.

6.1.3 Servicios Básicos

Transferencia de Archivos

Se espera que las implementaciones de TCP/IP ofrezcan al menos tres servicios de aplicación: transferencia de archivos, conexión remota y correo electrónico. Muchos productos incluyen clientes y servidores de World Wide Web. También suele ser normal incluir una función de impresión remota.

La transferencia de archivos fue uno de los primeros servicios añadidos a TCP/IP. El protocolo de transferencia de archivo (FTP – File Transfer Protocol) permite a los usuarios copiar archivos completos desde un sistema a otro. FTP también permite al usuario acceder a un sistema remoto para realizar tareas básicas como cambiar el nombre a un archivo, borrarlo o crear nuevos directorios.

Terminal Virtual

A principios de los años setenta, la mayoría de los fabricantes de computadoras construían terminales propietarias que sólo se podían usar con sus propios sistemas de cómputo. El departamento de Defensa de los EU (DOD) compraba sistemas de muchos fabricantes diferentes y quería que cualquier usuario fuera capaz de conectarse a cualquier host de la red desde un mismo terminal. Para hacerlo posible se creo el protocolo de terminal virtual "Telnet". Desde entonces se ha mejorado para que funcione con una larga lista de tipos de terminales y sistemas operativos.

Correo

Muchos usuarios finales se han sentido atraídos hacia TCP/IP por el correo. Se han normalizado dos aspectos del correo:

- El formato del correo intercambiado entre los usuarios. Existen formatos para texto sencillo y para mensajes multimedia y con múltiples partes.
- Los mecanismos necesarios para la transferencia directa o con almacenamiento y reenvío del correo entre host. Desde los primeros momentos de Internet se ha usado el Protocolo Simple de Transferencia de Correo (SNMP – Simple Mail Transfer Protocol). Recientes extensiones le han añadido nuevas funciones.

Se han conectado al correo de Internet otros sistemas de correo propietario, haciendo crecer la comunidad de potenciales destinatarios del correo.

Servicio World Wide Web

La World Wide Web es la más versátil de todas las aplicaciones cliente / servidor de TCP/IP. Los usuarios pueden ver atractivos documentos a los que se han añadido imágenes y sonidos, navegar sin esfuerzo de un lugar a otro con un "clic" del ratón y buscar en gigantescas bases de datos información de todo tipo.

Servicios Adicionales

Acceso a Archivos

Los servidores de archivos permiten que un usuario acceda a archivos remotos como si fuesen locales. Se hicieron populares en primer lugar en los entornos LAN de computadoras personales como mecanismo para compartir valiosos recursos de disco y centralizar las tareas de mantenimiento y copias de seguridad.

Muchos productos de TCP/IP incluyen el sistema de archivos de red (NFS – Network File System). Los productos permiten una o dos de las siguientes funciones de NFS:

- *Cliente de acceso a archivos*. Permite que una computadora acceda a archivos remotos como si fueran locales. Los usuarios y los programas no tienen que preocuparse de la localización de dichos archivos.
- *Servidor de Archivos*. Mantiene los directorios a los que pueden acceder determinadas computadoras de la red.

Noticias

La aplicación de noticias electrónicas empezó como un mecanismo para disponer de acceso local a los tablones de anuncios electrónicos y distribuir dicha información a muchos lugares. Muchas organizaciones usan software de noticias gratuito para realizar publicación electrónica de información interna. Otros acceden a los grupos de noticias de Internet donde se discuten temas que van desde los deportes a la física del plasma. Este software también se usa para acceder a los servicios de noticias comerciales como Reuters, AP y UPI.

Servicio de Nombres del Sistema de Nombres de Dominio

Para poder utilizar un servicio de red hay que poder identificar las computadoras remotas. Los usuarios y los programas pueden identificarlas por su nombre, que es fácil de recordar y escribir.

Para establecer una comunicación con un host hay que traducir su nombre a una dirección numérica. En los inicios, cada host de TCP/IP mantenía una tabla completa con la lista de todos los nombres y direcciones de todos los host en su red. Era imposible mantener estas listas actualizadas en una red en crecimiento dinámico como Internet, con cientos, después cientos de miles y después millones de host.

Para resolver éste problema se desarrollo el Sistemas de Nombres de Dominio (DNS – Domain Name System). El sistema de nombres de dominio es una base de datos de nombres y direcciones de host distribuida por miles de servidores. Los protocolos de DNS permiten que un usuario envíe una consulta a una base de datos local y reciba una respuesta que pudo haberse conseguido de un servidor remoto.

Además de traducir entre nombres de host y direcciones, los servidores de DNS también ofrecen información necesaria para encaminar el correo electrónico a su destino.

Software Comercial

Muchos terceros fabricantes han desarrollado aplicaciones que se ejecutan sobre TCP/IP. Por ejemplo, los fabricantes de bases de datos conectan a clientes con sus servidores mediante TCP/IP.

Administración de Red

Durante estos años, se han desarrollado muchas herramientas de gestión de red para el protocolo TCP/IP. Por ejemplo, existen comandos que permiten al administrador de red ver qué sistemas están activos, ver su carga actual, obtener la lista de usuarios conectados y la lista de servicios disponibles.

Estos comandos son muy útiles, pero se necesitaba mucho más para proporcionar una plataforma consistente y comprensible para una administración de red centralizada. La comunidad de Internet desarrolló el Protocolo Simple de Administración de Red (SNMP) para administrar cualquier cosa, desde un dispositivo simple a un sistema operativo de un host o el software de aplicación.

6.2 ARQUITECTURA DE TCP/IP

TCP/IP se diseño para un entorno que resultaba bastante poco usual en los años 70 pero que ahora es el habitual. El protocolo TCP/IP debía conectar equipos de distintos fabricantes. Debía ser capaz de ejecutarse en diferentes tipos de medios y enlaces de datos. Debía unir conjuntos de redes en una única Internet, de forma tal que todos sus usuarios pudiesen acceder a un conjunto de servicios genéricos.

Más aún, los patrocinadores académicos, militares y gubernamentales de TCP/IP querían poder conectar nuevas redes a sus internet sin interrumpir el servicio del resto de la red.

Estos requisitos conformaron la arquitectura del protocolo. La necesidad de independencia de la tecnología del medio y la conexión automática a una red en crecimiento, condujo a la decisión de transmitir los datos por una internet troceándolos en piezas y encaminando cada pieza como una unidad independiente.

Las funciones que garantizan una transmisión de datos fiable se situaron en los host origen y destino. Por ello, los fabricantes de ruteadores pueden centrar sus esfuerzos en mejorar el rendimiento y mantenerse en las nuevas tecnologías de comunicaciones. Al hacerlo así, los protocolos de TCP/IP consiguieron escalarse muy bien, ejecutándose en sistemas que iban desde las grandes computadoras a las PC. De hecho, un útil subconjunto de administración de red se traslada a dispositivos de la red –sin inteligencia- como los puentes, multiplexores y conmutadores.

6.2.1 Estructura en Capas

Para conseguir un intercambio fiable de datos entre dos computadoras, se deben llevar a cabo muchos procedimientos separados.

- Empaquetar los datos
- Determinar el camino que deben seguir
- Transmitirlos por el medio físico
- Regular la tasa de transferencia de acuerdo con el ancho de banda disponible y la capacidad del receptor para absorber los datos

- Ensamblar los datos entrantes para que se mantengan en la secuencia correcta y no haya pérdida de trozos
- Comprobar los datos entrantes para ver si hay trozos repetidos
- Notificar al emisor los datos que se han recibido correctamente
- Entregar los datos a la aplicación correcta
- Manejar eventos de errores y problemas

El resultado es que el software de comunicaciones es complejo. Con un modelo en capas resulta más sencillo agrupar funciones relacionadas e implementar el software de comunicaciones de forma modular.

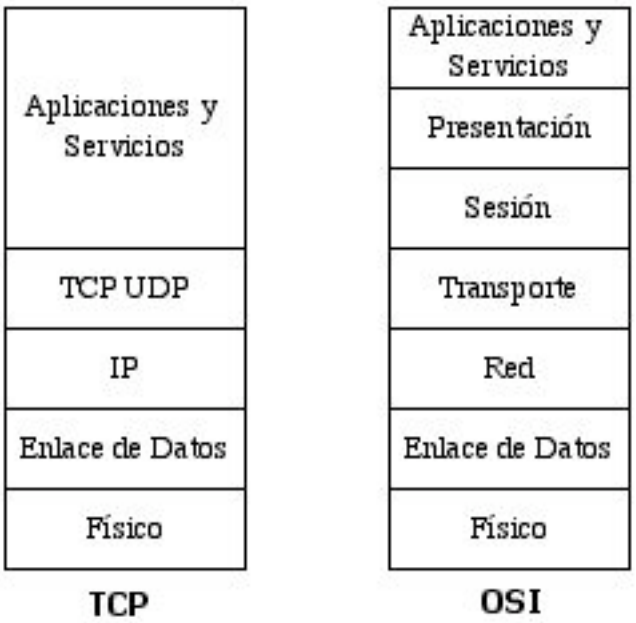


Figura 6.1 Capas de TCP/IP y OSI.

La estructura concreta seleccionada para los protocolos de TCP/IP proviene de requisitos que evolucionaron en las comunidades académicas y de defensa. IP hace lo necesario para agrupar distintos tipos de redes en una internet, y TCP proporciona transferencia fiable de datos.

El modelo de comunicación de datos de OSI se vio influido fuertemente por el diseño de TCP/IP. Las capas de OSI y la terminología de OSI se ha convertido en una parte estándar de la cultura de la comunicación de datos.

Capa Física

La capa física trata con el medio físico, los conectores y las señales que representan los ceros (0) y los unos (1). Por ejemplo, las tarjetas de interfaz de red de Ethernet y Token Ring y los cables implementan las funciones de la capa física.

Capa de Enlace de Datos

En la capa de enlace, los datos se organizan en unidades llamadas tramas. Cada trama tiene una cabecera que incluye una dirección e información de control y una cola que se usa para la detección de errores.

La cabecera de una trama de red de área local (LAN) contiene las direcciones físicas del origen y del destino, identificando las tarjetas de interfaz de red del origen y el destino de la LAN. La cabecera de una trama que se transmite por una red de área extensa (WAN) contiene un identificador de circuito en su campo de dirección.

Hay que recordar que un enlace es una red de área local, una línea punto a punto o alguna otra facilidad de área extensa por la que se pueden comunicar los sistemas mediante un protocolo de la capa de enlace de datos.

Capa de Red

El protocolo de Internet realiza funciones de la capa de red. IP encamina datos entre sistemas. Los datos pueden atravesar un enlace único o pueden reenviarse por varios enlaces de una internet. Los datos se transportan en unidades llamadas datagramas.

Un datagrama tiene una cabecera de IP que contiene información de direcciones de la capa 3. Los ruteadores examinan la dirección de destino de la cabecera de IP, para dirigir los datagramas al destino.

La capa de IP se denomina no orientada a conexión ya que cada datagrama se encamina de forma independiente e IP no garantiza una entrega fiable, ni en secuencia, de los mismos. IP encamina su tráfico sin tener en cuenta la relación entre aplicaciones a las que pertenece de un determinado datagrama.

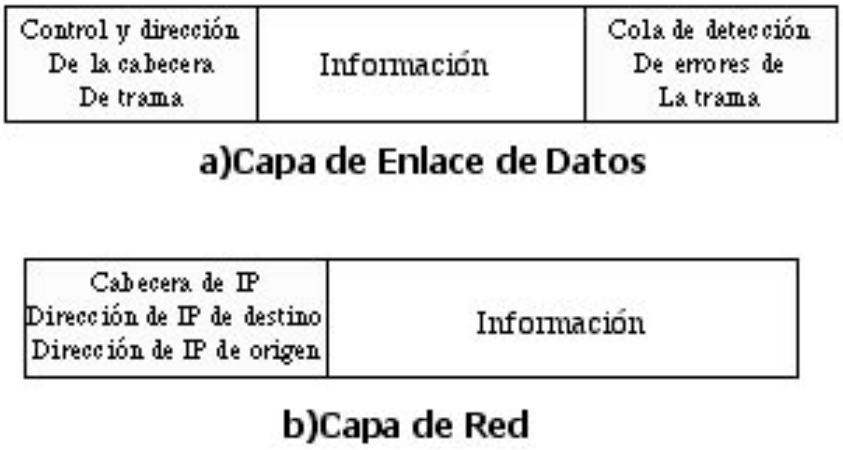


Figura 6.2 a) Capa de enlace de datos: cada trama tiene una cabecera que incluye una dirección e información de control y una cola que se usa para la detección de errores; b) Capa de red: Un datagrama tiene una cabecera de IP que contiene información de direcciones de la capa 3.

Capa de Transporte: TCP

El protocolo de control de transmisión realiza funciones de la capa de transporte. TCP proporciona a las aplicaciones servicios de conexión fiable de datos. TCP dispone de los mecanismos que garantizan que los datos se entregan sin errores, sin omisiones y en secuencia.

Una aplicación, como la de transferencia de archivos, transmite datos a TCP. TCP le añade una cabecera creando una unidad denominada un segmento.

TCP envía segmentos pasándoselos a IP, quien los encamina hacia su destino. TCP acepta segmentos entrantes por IP, determina la aplicación de destino y traslada los datos a la aplicación en el orden a que fueron enviados.

Capa de transporte UDP

Una aplicación envía un mensaje independiente a otra aplicación mediante el protocolo de datagramas de usuario (UDP). UDP añade una cabecera creando una unidad denominada datagrama de UDP o mensaje de UDP.

UDP traslada los mensajes de UDP salientes a IP. UDP acepta mensajes de UDP entrantes de IP y determina la aplicación de destino. UDP es un servicio de comunicaciones no orientado a conexión que suele usarse en aplicaciones de búsquedas simples en bases de datos.

Servicios de Aplicación

El protocolo TCP/IP incluye un conjunto de servicios de aplicación estándares como el terminal virtual, la transferencia de archivos, el acceso al servidor de archivos del sistema de archivos de red (NFS), correo electrónico, noticias, la World Wide Web (WWW) y la búsqueda de direcciones del sistema de nombres de dominio.

Empaquetado de Datos para su Transmisión

El término genérico para la información junto con una cabecera apropiada de una capa es Unidad de datos del Protocolo (PDU). Por ejemplo, un segmento de TCP es una PDU de la capa de transporte y un datagrama de IP es una PDU de la capa de red.

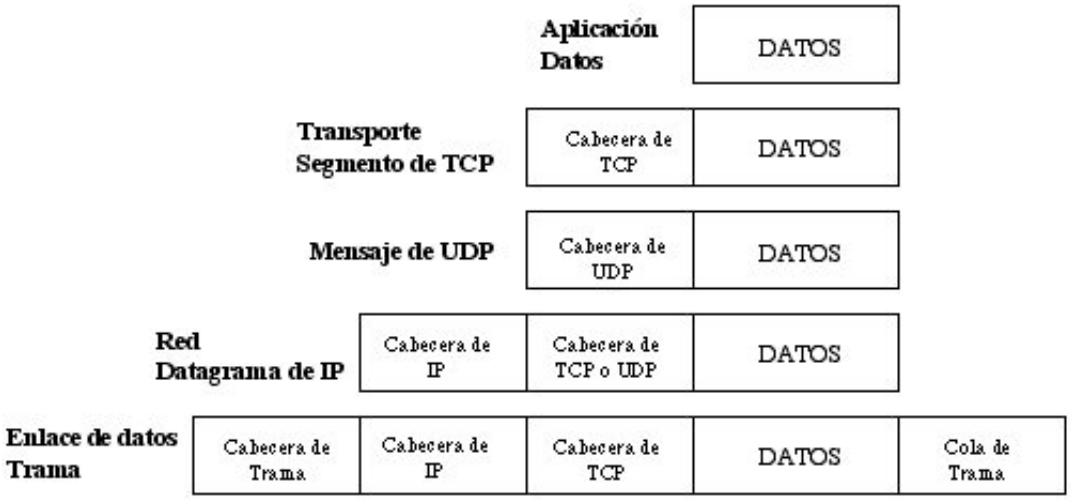


Figura 6.3 Empaquetamiento de datos para su transmisión.

6.2.2 Descripción General del Protocolo

Aunque no se han normalizado formalmente las interfaces textuales de las interfaces de usuario para la transferencia de archivos, el terminal virtual ni la traducción de nombre a dirección del sistema de nombres de dominio, la mayoría de los fabricantes suelen ofrecer un conjunto de comandos, copia de las interfaces de usuario de Unix de la distribución de software de Berkeley. Para los usuarios que

trabajen en el modo textual en dos tipos de host distintos resulta muy útil que las interfaces de usuario permanezcan casi iguales al cambiarse de sistema.

Existen muchas interfaces gráficas de usuario (GUI) para los sistemas Windows y Macintosh. Aunque difieren en los detalles, siguen las convenciones del sistema operativo y normalmente se pueden usar sin un entrenamiento especial.

Los clientes de World Wide Web, noticias, transferencia de archivos (FTP), correo electrónico y terminal virtual (telnet) se comunican con sus servidores mediante conexiones fiables de TCP. La mayoría de los clientes de archivos de NFS intercambian mensajes de UDP con sus servidores, aunque algunas implementaciones de NFS se pueden ejecutar tanto sobre UDP como sobre TCP.

Las búsquedas de directorio del sistema de nombres de dominio utilizan mensajes de UDP. Las estaciones de administración del protocolo simple de gestión de red (SNMP) obtienen información de los dispositivos de red mediante mensajes de UDP.

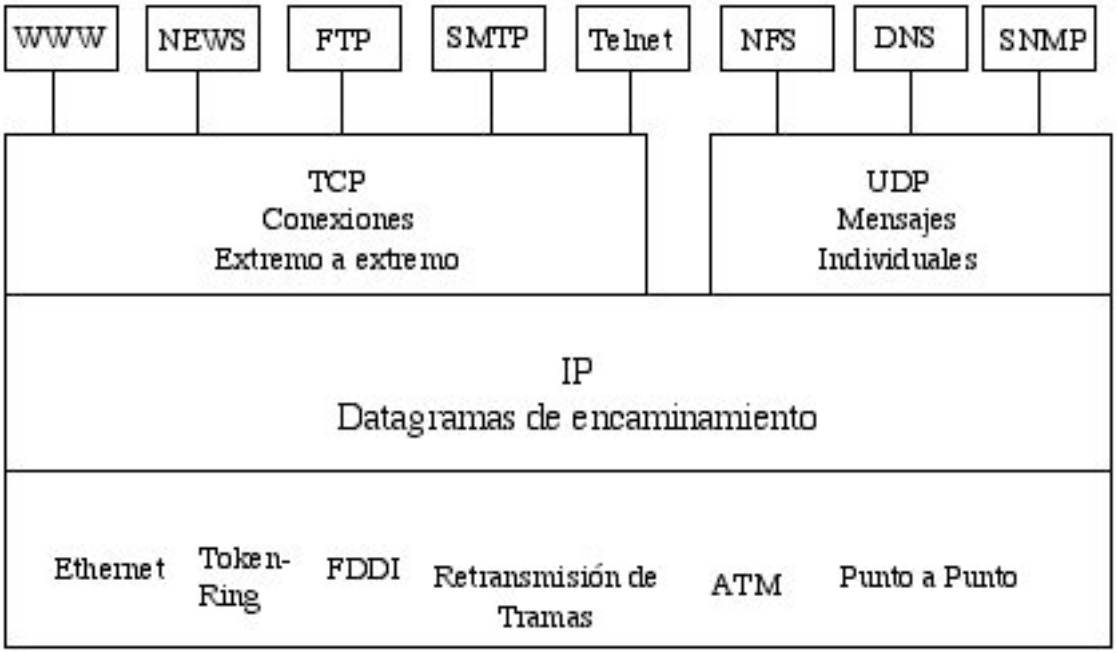


Figura 6.4 Componentes del conjunto de protocolos de TCP/IP.

6.2.3 Ruteadores y Topología

El conjunto de protocolos TCP/IP se puede utilizar en LAN y WAN independientes o en complejas "internet" creadas por la unión de muchas redes. Cualquier host con TCP/IP se puede comunicar con otro por LAN, con una línea punto a punto o una red de paquetes de área extensa.

Las redes se pueden interconectar en una internet con ruteadores de IP. Los modernos productos de encaminamiento disponen de múltiples ranuras de interfaz hardware configurables según las necesidades de conexión del usuario: Ethernet, Token Ring, FDDI, conexión punto a punto sincronía, retransmisión de tramas u otros.

Las internet se pueden construir con cualquier mezcla de topología. Sin embargo, cuando la internet tiene una estructura coherente, a los ruteadores les resulta más sencillo realizar su trabajo eficientemente y reaccionar rápidamente a fallos en cualquier lugar de la red, cambiando los caminos

de los datagramas para evitar los puntos conflictivos. Un diseño lógico fácil de entender ayuda a los administradores de red a diagnosticar, localizar y reparar fallos en la red.

El robusto y competitivo mercado de ruteadores de IP ha promovido la arquitectura de TCP/IP. Los fabricantes de ruteadores implantan rápidamente las tecnologías de LAN y WAN, ampliando las opciones de conectividad de sus clientes. La relación precio / rendimiento de un ruteador se ha reducido continuamente durante los últimos años.

Ruteo de IP

El software de IP se ejecuta en host y en ruteadores de IP. Si el destino de un datagrama no está en el mismo enlace que el host de origen, el IP del host dirige el datagrama a un ruteador local. Si el ruteador no está directamente conectado con el enlace de destino hay que enviar el datagrama a otro ruteador. Este proceso continúa hasta que se alcanza el enlace de destino.

IP rutea hacia lugares remotos buscando la red de destino en una tabla de ruteo. Una entrada de la tabla de ruteo identifica el ruteador del siguiente salto que debe seguir el tráfico para conseguir llegar a su destino.

Protocolos de Ruteo

En una internet estática y pequeña, las tablas de ruteo se pueden mantener y crear manualmente. En internet los ruteadores grandes mantienen sus propias tablas actualizadas intercambiando información unos con otros. Los ruteadores pueden descubrir dinámicamente:

- Si se ha añadido una nueva red a la internet.
- Que el camino a un destino ha fallado y que ya no se puede alcanzar dicho destino.
- Se ha añadido un nuevo ruteador a la internet. Este ruteador proporciona un camino más corto a ciertos lugares.

No existe una única norma para el intercambio de información entre ruteadores. La libertad de elección del protocolo más apropiado ha estimulado la competencia y ha conseguido una gran mejora en estos protocolos.

Las funciones de red bajo el control de una organización se denomina un sistema autónomo (AS – Autonomous System). Una organización puede elegir el protocolo de intercambio de información de ruteo que desee para su propio sistema autónomo. El protocolo de intercambio de información de ruteo dentro de un sistema autónomo se denomina Protocolo Interior de Pasarela (IGP – Interior Gateway Protocol).

El Protocolo de Información de ruteo (RIP – Routing Information Protocol) es un estándar muy usado del protocolo de pasarela interior. RIP es muy popular por su sencillez y por su gran disponibilidad. Sin embargo, el nuevo protocolo Primero el Camino Abierto más Corto (OSPF – Open Shortest Path First) dispone de un conjunto más rico de funciones.

Aunque todos los ruteadores disponen de uno o más protocolos estándar, algunos fabricantes de ruteadores también proporcionan un protocolo propietario para el intercambio de información entre ruteadores. Muchos productos de ruteo pueden ejecutar varios protocolos de ruteo simultáneamente.

Arquitectura de TCP

TCP se implanta en host. La entidad de TCP en cada extremo de una conexión debe asegurar que los datos se entreguen a su aplicación local de forma:

- Precisa
- En secuencia
- Completa
- Libre de duplicados

El mecanismo básico para conseguirlo se ha utilizado desde el inicio de las comunicaciones de datos. El TCP emisor:

- Numera los segmentos
- Fija un temporizador
- Transmite el segmento

El TCP receptor tiene que mantener informado al emisor del número de datos correctos recibidos mediante una confirmación (ACK). Si no llega el ACK para un segmento dentro del plazo del temporizador, TCP reenvía el segmento. Esta estrategia se denomina Retransmisión de Confirmación Positiva. A veces la retransmisión puede causar que se entreguen segmentos repetidos al TCP receptor.

El TCP receptor debe reordenar los segmentos entrantes en el orden correcto, descartando los repetidos. TCP entrega los datos a la aplicación en orden, sin pérdida de trozos.

Hasta aquí parece como si hubiese un lado que envía y el otro que recibe. TCP es un protocolo dúplex, es decir, ambos extremos pueden enviar y recibir a la vez, por lo que de hecho se están transmitiendo dos flujos de datos. TCP juega el papel de transmisor y receptor simultáneamente.

Arquitectura de UDP

UDP se implanta en el host. UDP no promete ni garantiza la entrega y es responsabilidad de las aplicaciones que intercambian la información confirmar si los datos han llegado correctamente. Una aplicación que quiere enviar datos UDP traslada un bloque de datos a UDP. UDP simplemente añade una cabecera a dicho bloque y lo transmite.

Una aplicación que participa en una comunicación de UDP puede enviar y recibir mensajes de datagramas de usuario en cualquier momento. Es responsabilidad de los clientes y de los servidores que utilizan UDP mantener un registro de cualquier relación entre los datagramas de usuario intercambiados.

6.2.4 Conceptos de Seguridad

TCP/IP se comporta muy bien en el establecimiento de comunicaciones de computadoras en una LAN, a través de una red de puntos o incluso globalmente. Pero la conectividad alcanza un nuevo interés en cuanto a la seguridad de la información.

Los temas básicos de seguridad en un entorno de red son los mismos que se encuentran en un host central.

- Autenticación de los usuarios
- Integridad, es decir, asegurar que los datos no han cambiado
- Confidencialidad, es decir, evitar que nadie pueda observar la información

Autenticación

Un aspecto importante de la seguridad de las computadoras es saber quién es quién. En el pasado se confiaba en los identificadores de usuario (ID) y en las contraseñas para identificar a los usuarios interactivos. Se confiaba en el campo "FROM:" de un mensaje de correo electrónico para identificar al emisor. Pero las contraseñas se pueden capturar mediante una escucha silenciosa y el correo electrónico se puede falsificar.

Si se van a realizar transacciones serias sobre redes TCP/IP, se necesita algún mecanismo para identificar de forma fiable al emisor. La identificación fiable de un emisor se denomina autenticación.

Tecnología de Clasificación de Mensajes

Una tecnología de autenticación sencilla, pero eficaz utiliza clasificación de mensajes (Message Digests). Una clasificación de mensajes es el calculo que se realiza con un mensaje usando una clave secreta. La clasificación de mensajes 5 (MD5) se usa mucho actualmente.

El Challenge Handshake muestra una forma de uso de la clasificación de mensajes. Como ocurre en la autenticación convencional, un usuario da su contraseña registrada en un host. Sin embargo, la contraseña no se envía nunca por la red. En lugar de ello, el sistema del usuario realiza un cálculo MD5 utilizando la contraseña como clave secreta.

1. El usuario envía un identificador de usuario al host
2. El host envía un mensaje aleatorio al usuario
3. El host y el sistema del usuario realizan un cálculo MD5 del mensaje aleatorio y la contraseña secreta del usuario.
4. El sistema de usuario envía la respuesta al host.
5. El host compara las respuestas. Si el sistema del usuario envía la respuesta correcta, se autentica al usuario.

Integridad de los Mensajes

También se pueden usar MD5 y una clave secreta para detectar si han cambiado los datos durante su transmisión; y se debe de hacer lo siguiente:

1. Se realiza un calculo MD5 con los datos y la clave secreta.
2. Se envían al otro extremo los datos y el mensaje clasificado.
3. El otro extremo realiza un calculo MD5 de los datos y la clave secreta.
4. El otro extremo compara la respuesta con el mensaje clasificado. SI coinciden, significa que los datos no han cambiado.

Se debe de tener en cuenta que sin conocer la clave secreta, un fisgón no puede falsificar o modificar los datos. Este mecanismo se usa en el correo electrónico seguro y en las transacciones cliente / servidor que se deben proteger.

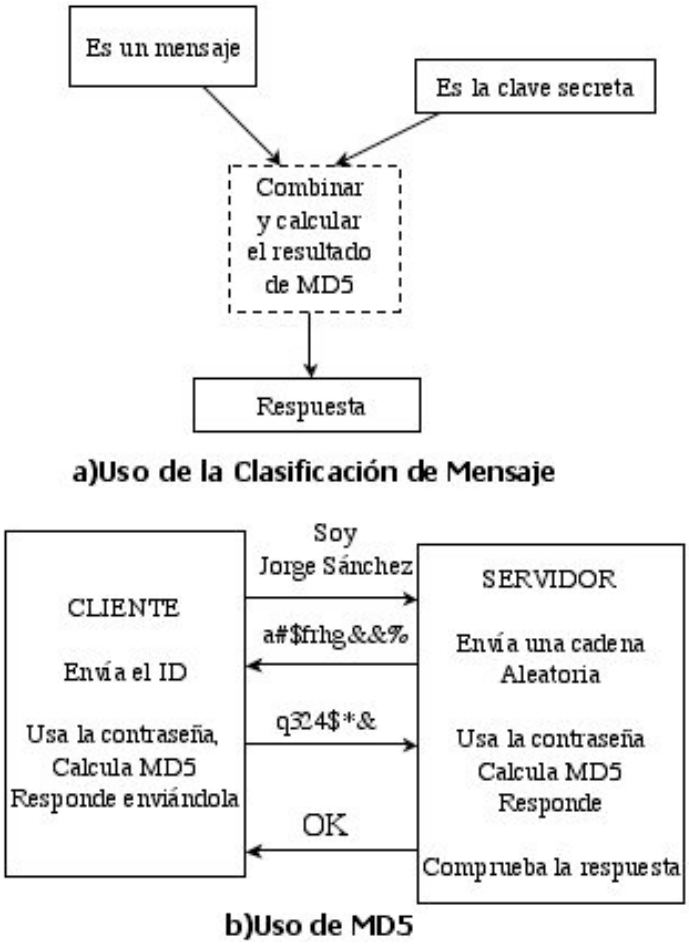


Figura 6.5 Autenticación; a) Uso de la clasificación de mensaje; b) Uso de MD5 en un Challenge handshake.

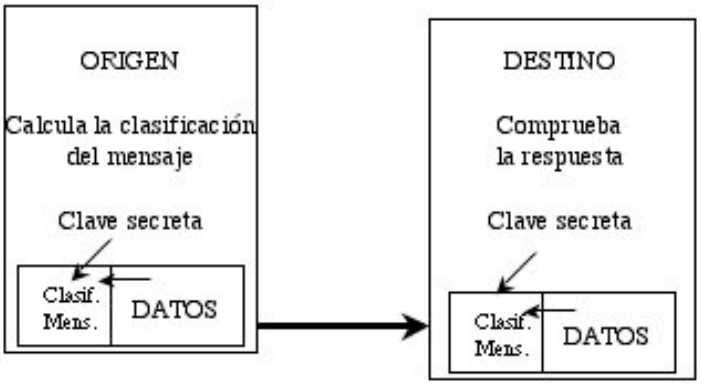


Figura 6.6 Integridad de los mensajes; Protección de los datos de un mensaje con una clasificación de mensajes MD5.

Confidencialidad Usando Cifrado Simétrico

Para evitar que los fisgones lean y utilicen los datos, éstos deben ir cifrados. La manera clásica de hacerlo es que el emisor y el receptor estén de acuerdo en la clave secreta. Los datos se cifran antes de enviarse esta clave. A menudo, se añade una clasificación de mensaje de manera que el receptor pueda que el mensaje recibido se corresponda exactamente con el emitido. Una vez que se han cifrado los datos parecen una cadena de basura.

Este es el método tradicional de cifrado simétrico. El cifrado simétrico usa la misma clave para cifrar y para descifrar los datos. Los usuarios deben conocer y guardar la clave secreta. Las desventajas de éste método son:

- Por seguridad, se necesita una clave distinta para cada par de entidades que se comunican.
- Es difícil actualizar las claves..

Figura 6.7 Cifrado simétrico

Cifrado asimétrico con Clave Pública

Actualmente, han aparecido métodos que realizan un cifrado asimétrico. El cifrado asimétrico utiliza claves diferentes para cifrar y descifrar los datos. Para comprenderlo, podemos suponer que se tiene una caja con dos llaves diferentes, A y B, como se muestra en la siguiente figura.

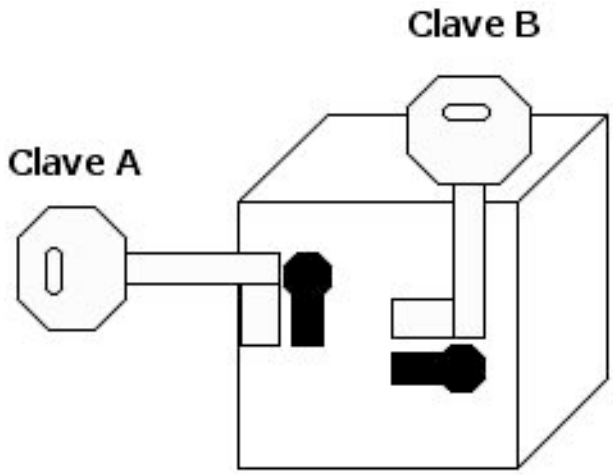


Figura 6.8 Uso de distintas llaves para abrir y cerrar (cifrar y descifrar)

- Se cierra la caja usando la llave A, debe abrirla con la llave B.
- Se cierra la caja usando la llave B, debe abrirla con la llave A.

El cifrado asimétrico también se denomina cifrado de clave pública ya que permite administrar las claves de una forma muy conveniente. La clave A puede ser la clave pública. Se le puede dar a los amigos o ponerla en un directorio.

- Cualquiera puede usar la clave pública para cifrar datos que va a enviar.
- Nadie conoce tu clave privada, por lo que nadie más puede descifrar los datos que te envíen.

La administración de claves pública / privada es mucho más sencilla que las claves simétricas. Pero, aún así, se necesita una autoridad de registro en quien confiar que asegure que la clave que aparece como "Clave pública de Blanca S." realmente pertenece a Blanca S., y no a una impostora.

Cifrado Combinado

El cifrado combinado funciona de la siguiente forma:

1. Se selecciona una clave simétrica aleatoria
2. Se cifran los datos con dicha clave
3. A continuación la clave aleatoria se cifra usando la clave pública del receptor y se incluye en el mensaje. Es como poner la nueva clave aleatoria dentro de un contenedor que se ha cerrado con la llave pública del receptor
4. El receptor descifra la clave aleatoria temporal y la usa para descifrar los datos

Como se muestra en la figura 6.9, la clave pública se usa para poner un envoltorio alrededor de la clave aleatoria. El receptor es el único que puede abrir éste envoltorio.

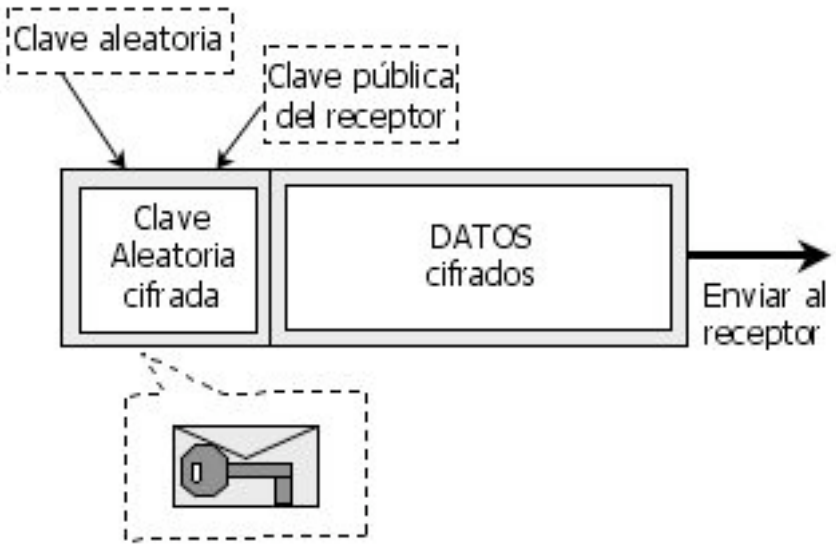


Figura 6.9 Guardando una clave para descifrar un mensaje

6.3 TECNOLOGÍA FÍSICA Y DE ENLACE DE DATOS

Durante los últimos años ha aparecido un número sin precedente de tecnologías innovadoras de LAN y de WAN que han absorbido rápidamente el mercado. Se ha introducido el uso del par trenzado y la fibra a un ritmo que nadie hubiese podido predecir. Red Digital de Servicios Integrados (RDSI), Retransmisión de tramas T1, T1 fraccional, T3, SONET, línea de fibra óptica. Servicio conmutado de datos multimegabit (SMDS), conexiones de cable y modo de transferencia asíncrono (ATM), todos ellos prometen conexiones de área extensa más rápidas y baratas.

Según han surgido nuevas tecnologías, el Internet Engineering Task Force (IETF) ha respondido rápidamente, escribiendo las especificaciones para ejecutar IP, junto con otros protocolos , sobre el nuevo medio. A continuación, sin casi retraso, los fabricantes de ruteadores ha desarrollado las interfaces hardware y los controladores software que ha permitido a los usuarios aprovechar la nueva tecnología.

Los esfuerzos del IETF se pueden seguir en la larga serie de documentos "Petición de Comentarios" (RFC – Request for Comment) con títulos como:

The Point to Point Protocol (PPP) for the transmssion of Multiprotocol Datagrams over Point to Point Links

Standard for the Transmission of IP datagrams over IEEE 802 Networks

Transmission of IP and ARP over FDDI Networks

Classical IP and ARP over ATM

6.3.1 Funciones de la Capa Física, MAC y de Enlace de Datos

A continuación se describe cómo funciona "I+P" encima de varias tecnologías de capas inferiores.

La capa física especifica los cables, los conectores y las características eléctricas del medio. También corresponde a la capa física las reglas para insertar ceros (0) y unos (1) individuales en el medio.

Para dar sentido a los datos transmitidos, se empaquetan en unidades que se llaman tramas. Una trama transporta información por un único cable. Para alcanzar el destino final, un datagrama de IP puede que necesite viajar por varios enlaces.

La descripción del formato de la trama puede ser diferente dependiendo de la tecnología subyacente del enlace. El formato de la cabecera depende de la tecnología utilizada.

Tecnologías de Red

Las tecnologías de red se pueden dividir en cuatro grandes categorías:

1. Líneas punto a punto de área extensa
2. LAN
3. Servicios de área extensa de envío de paquetes
4. Servicios de conmutación de células

Para cada tecnología se necesitan mecanismos para:

- Identificar el destino cuando una única interfaz conecta con múltiples sistemas, por ejemplo una interfaz de LAN
- Detectar errores cuando los datos se corrompen durante su tránsito

En la actualidad, tanto los entornos locales como de área extensa son multiprotocolo. Como se muestra en la figura 6.10, a menudo un enlace lo comparten varios protocolos, como TCP/IP, Novell, IPX/SPX, DECnet, Vines e incluso tráfico entre puentes. Los host y ruteadores multiprotocolo necesitan mecanismos para ordenar los distintos tipos de tráfico, por lo que se necesitan mecanismos para:

- Identificar el tipo de protocolo de cada unidad de datos del protocolo (PDU) que va en cada trama

La identificación de un tipo de protocolo no parece que debiera de ser difícil. Bastaría con tomar un cuerpo de normas y realizar una lista de protocolos , asignar un número a cada uno y poner éste número en un campo de la cabecera de la trama.

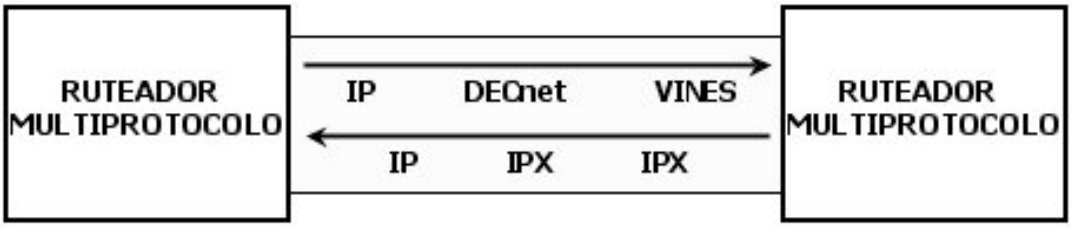


Figura 6.10 Múltiples protocolos compartiendo un mismo medio.

Y es así de fácil, excepto por el hecho de que varios organismos de normalización ya han realizado el trabajo y cada uno introduce números diferentes en los campos y números diferentes para identificar los protocolos.

Re-empaquetamiento

Existe un evento olímpico en el que un atleta nada un tramo, toma una bicicleta, pedalea otro tramo y corre un tercero. IP funciona de la misma forma. Los diseñadores de Internet construyeron IP de manera que los datagramas pudiesen pasar de un medio a otro hasta llegar a su destino.

Antes de transmitir un datagrama por un enlace, se empaqueta en una trama apropiada para dicho enlace. Cuando un ruteador recibe una trama:

- Elimina el empaquetamiento de la trama y extrae el datagrama
- Mira la dirección IP de destino del datagrama y elige el medio del próximo salto
- Reempaqueta el datagrama con un nuevo empaquetado de trama para su viaje por el siguiente enlace y transmite el datagrama

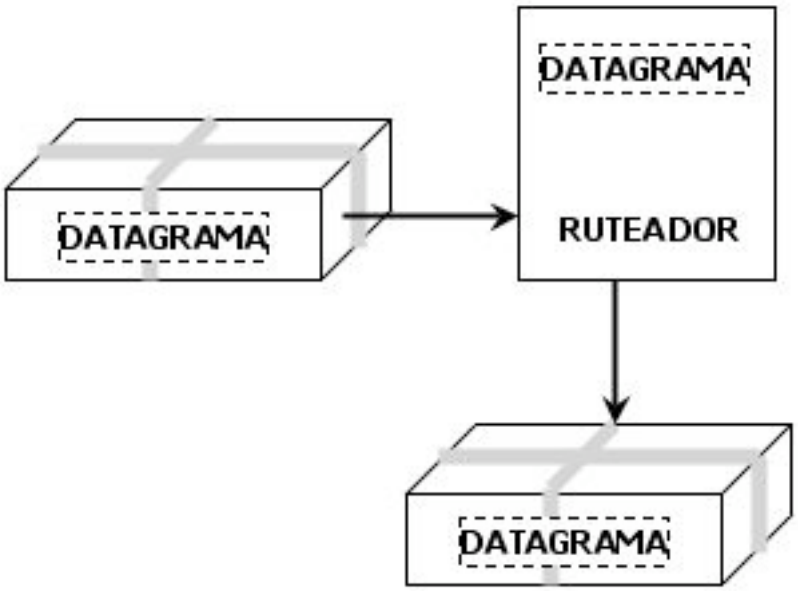


Figura 6.11 Reenpaquetamiento de Datagramas

6.3.2 Protocolos Punto a Punto

Los datagramas de IP se pueden enviar por un enlace punto a punto entre dos Host, dos ruteadores o un host y un ruteador. IP transmitirá los datagramas para muchas interacciones diferentes de UDP y TCP por un único enlace punto a punto.

IP no sabe si se preocupa de la identidad de las aplicaciones de origen o de destino. Cada vez que IP maneja un datagrama saliente, transmite el datagrama en cuanto puede. Como se muestra en la figura 6.12, el tráfico de muchas interacciones cliente / servidor comparten un enlace, al igual que muchos coches comparten una misma carretera.

En la actualidad, el tráfico de IP se transmite por enlaces punto a punto empaquetado de varias formas diferentes:

- Con una de las versiones convencionales del protocolo punto a punto; Control de Enlace de Datos de Alto Nivel (HDLC – High-Level Data Link Control).
- Mediante el protocolo punto a punto (PPP – Point to Point Protocol) estándar en internet.
- Mediante el protocolo de interfaz de línea serie (SLIP – Serial Line Interface Protocol).

Poco a poco las implementaciones van migrando al estándar de internet PPP, que ofrece muchas funciones avanzadas.

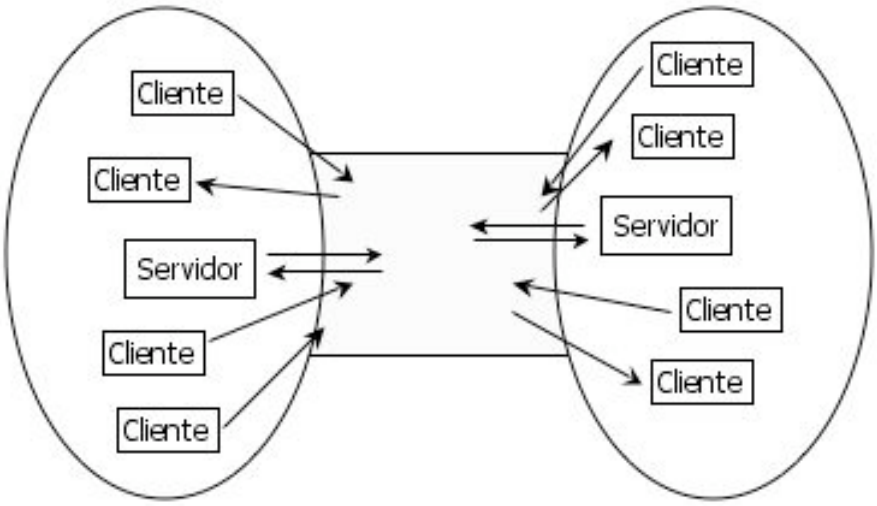


Figura 6.12 Múltiples clientes y servidores comparten un enlace.

6.3.3 HDLC

El protocolo de control de enlace de datos de alto nivel (HDLC) es una norma internacional para enlaces punto a punto escrita en los años 60. HDLC envía datos serie como un flujo de bits con reloj que se trocea en tramas. Las tramas se delimitan con un patrón especial:

0111110

Para reconocer éste patrón es necesario evitar que el patrón aparezca en los datos del usuario. Para ello, tras transmitir el patrón de inicio, el hardware de envío inserta un cero (0) cada vez que

encuentra cinco bits consecutivos a uno en los datos. Este procedimiento se llama inserción de bit cero o compresión de bits a uno (1), (1 bit Stuffing).

En la parte receptora del enlace, tras reconocer el comienzo de una trama, el hardware de recepción elimina los ceros que aparecen tras cinco unos consecutivos en la trama.

Formato de Trama de HDLC

En la figura 6.13 se muestra un pequeño ejemplo de datos antes y después de ejecutar la inserción de bits.

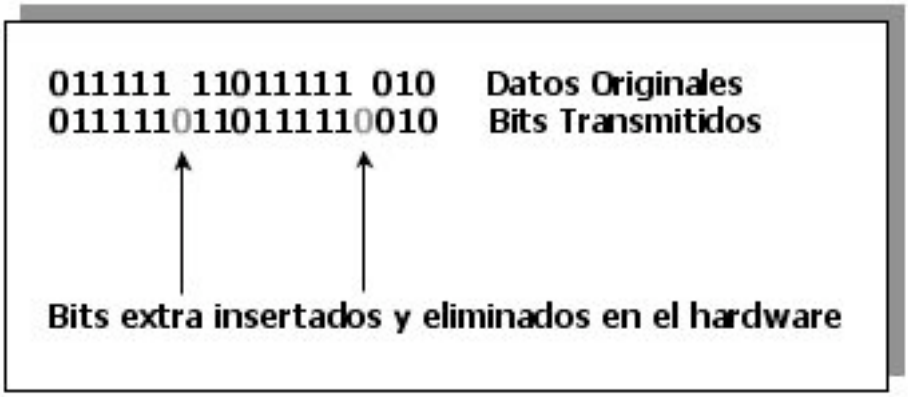


Figura 6.13 Inserción de Bits en HDLC

El protocolo HDLC establece un esquema básico que ha influido en todos los formatos de tramas posteriores. Como se muestra en la figura 6.14, una trama de información de HDLC está compuesta por una cabecera, algunos datos y al final una cola que contiene una Secuencia de Comprobación de Trama (FCS – Frame Check Secuence). Se usan octetos bandera para delimitar el comienzo y final de la trama.

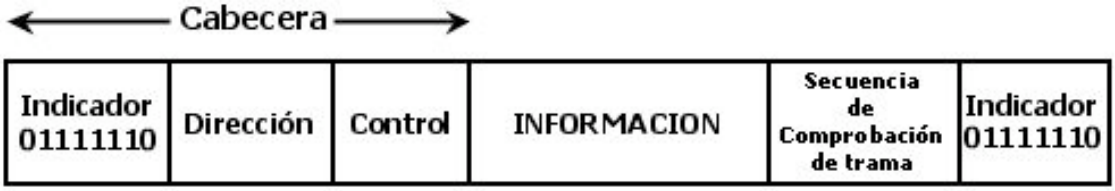


Figura 6.14 Formato de una trama de HDLC con sus delimitadores

La secuencia de comprobación de trama es el resultado de un cálculo matemático que se realiza con la trama en el origen. Ese mismo cálculo se realiza en el extremo destino del enlace. Si la respuesta no coincide con el valor del campo FCS, es que algunos bits de la trama han cambiado durante su transmisión y por ello la trama se descarta.

La idea de usar una secuencia de comprobación de trama para detectar errores de transmisión fue una gran idea. Existen campos para un FCS en todas las tramas excepto en una para LAN y WAN.

La cabecera de la trama de HDLC contiene un campo dirección de destino. Este campo es necesario en las versiones multiprotocolo de HDLC, como el control de enlace de datos síncrono, o

SDLC, de IBM, que permite que muchos sistemas puedan compartir una única línea. Se asigna a cada sistema una dirección y el tráfico se dirige a cierto sistema colocando su dirección en la cabecera.

IP no utiliza la tecnología de líneas multipunto; los datagramas de IP se transmiten en una trama de HDLC cuya dirección tienen el valor binario 11111111 (X´FF en hexadecimal) que se conoce como dirección "a todas las estaciones" (All stations), o de difusión.

La cabecera de la trama de HDLC también tiene un campo de control. Algunos protocolos de envío sitúan números de trama y de reconocimiento en el campo de control. Estos protocolos de enlace retransmiten las tramas numeradas que no consiguen una confirmación dentro de un cierto periodo de tiempo.

Las tramas que llevan IP, y muchos otros protocolos, como IPX y DECnet, no requieren numeración ni confirmación . Para IP, y para esos otros protocolos, el campo de control se establece en X´03 que identifica una trama HDLC de información sin numerar.

Es decir, un datagrama de IP empaquetado en una trama de HDLC tiene el formato que se muestra en la figura 6.15.

Para resumir, cuando una trama de HDLC lleva un datagrama de IP:

- Se usa la dirección "a todas las estaciones - X´FF".

El campo de control se establece en X´03, que significa información sin numerar.

Figura 6.15 Formato de una trama de HDLC con un datagrama de IP.

Problemas de HDLC

Que HDLC sea una "Norma" no significa que se puede usar una línea punto a punto entre cualesquiera dos interfaces HDLC y que se comuniquen una con otra.

Existen muchas opciones en la norma de HDLC, y muchas implementaciones de versiones diferentes de la "Norma" de HDLC. Y para confundir más las cosas, muchos fabricantes han implementado sus propias versiones de las interfaces punto a punto de HDLC.

El resultado, durante mucho tiempo, fue que no había un único estándar para las comunicaciones punto a punto, de manera que era difícil la interconexión de equipos de distintos fabricantes.

HDLC se diseño antes de existir las redes multiprotocolo. Actualmente, las líneas punto a punto suelen llevar tráfico de varios protocolos. Ello causa otro problema. Se propuso a un comité del IETF el trabajo de resolver estos problemas.

6.3.4 Protocolo Punto a Punto de Internet

La solución del grupo de trabajo de IETF fue el protocolo punto a punto, llamado normalmente PPP. PPP se puede utilizar sobre cualquier circuito dúplex, ya sea síncrono orientado a bit, o asíncrono orientado a byte (parada y arranque). Se puede usar por líneas telefónicas lentas, líneas rápidas

alquiladas, RDSI o incluso en líneas de fibra óptica de SONET. Además, PPP se diseño para llevar PDU de varios protocolos, IP, IPX, DECnet, ISO y otros. PPP puede llevar incluso datos de puentes. PPP incluye varios sub-protocolos. Por ejemplo:

- El protocolo de control de enlace establece, comprueba, configura y cierra un enlace.
- Los protocolos de control de red se usan para inicializar, configurar y terminar el uso de un protocolo de red concreto. Se define un protocolo de red distinto para cada IP, IPX, DECnet, ISO y otros.

Un escenario típico de PPP es el siguiente:

1. El PPP de origen envía una trama de Control de Enlace para empezar. Las dos partes intercambian tramas de control adicionales de control de enlace para establecer las opciones de uso del enlace.
2. Se intercambian tramas del Protocolo de Control de Red para seleccionar y configurar los protocolos de la capa de red que se van a usar.
3. Se envían datos de los protocolos seleccionados por el enlace en tramas de PPP. Cada trama incluye un campo de cabecera que identifica el tipo de datos del protocolo que se envía.
4. Se usan tramas de Control de Red y del Protocolo de Control de Enlace para cerrar el enlace.

Una cabecera de una trama de PPP se parece a una cabecera de PPP con su campo adicional que identifica el protocolo de la siguiente capa. En la figura 6.16 se muestra el formato de una trama de PPP que contiene un datagrama de IP.

El campo de dirección contiene X´FF "a todas las estaciones" y el campo de control contiene X´03 "Información sin numerar". El campo de protocolo adicional contiene X´00-21, valor que índica que la trama lleva un datagrama de IP. Los números de protocolos que se usan en PPP los publica la autoridad de asignación de números de Internet (IANA – Internet Assigned Numbers Authority) en su documento RFC Assigned Numbers.

Compresión de PPP

Puede parecer un derroche incluir los mismos octetos de dirección y de control en todas las tramas. De hecho las partes de cada extremo de un enlace PPP pueden negociar el funcionamiento en el modo compresión que elimina estos campos.

El valor del campo protocolo indica si el contenido de la información es un mensaje de control del enlace, un mensaje de control de red o información, como por ejemplo un datagrama de IP. Durante el establecimiento de un enlace de PPP, el campo protocolo empieza con un tamaño de 16 bits, pero se puede negociar el tamaño del campo protocolo cuando se transmita información para reducirlo a 8 bits. Por tanto, un datagrama se puede empaquetar en un paquete eficiente como el que smuestra en la figura 6.16.

Figura 6.16 Trama de PPP con un formato comprimido

Otra opción de PPP que permite ahorrar ancho de banda durante las sesiones de TCP es la compresión de Van Jacobson. Las cabeceras de IP y de TCP juntas suponen una sobrecarga de 40 o más bytes. La compresión de Van Jacobson reduce una combinación típica de 40 bytes a solo 3, 4 o 5 bytes, lo que significa un considerable ahorro.

Funciones Adicionales de PPP

PPP se suele usar para conectar a un teletrabajador o a un usuario de viaje a una red de IP mediante una conexión telefónica. A veces se usan las conexiones telefónicas para conectar a un grupo de trabajo a una LAN mediante un ruteador desde la filial a las oficinas centrales.

Antes de permitir que un sistema externo se conecte a la red mediante un enlace telefónico, se debería autenticar a ese sistema. Actualmente, PPP dispone de dos métodos de autenticación:

- El Protocolo Simple de Autenticación de Contraseña (PAP – Password Authetication Protocol). Se envía una trama con el texto del identificador del usuario y su contraseña durante el establecimiento del enlace.
- El Protocolo de Autenticación Challenge Handshake (CHAP – Challenge Handshake Authentication Protocol).

El Challenge Handshake fue revisado anteriormente con el nombre MD5.

Cada vez que se establece un enlace, un curioso vería diferentes bytes de información. Cuando se utilizan buenas contraseñas de 16 bytes, resulta virtualmente imposible adivinar la contraseña mirando el enlace.

Control Automático de la Calidad del Enlace

A menudo se usa PPP entre dos ruteadores. A veces la calidad del enlace se degrada por alguna razón . Resultaría de gran ayuda tener un aviso de las condiciones del enlace para tomar automáticamente alguna acción. Por ejemplo, un ruteador podría terminar la conexión y volver a marcar. O, si los problemas ocurren en una línea alquilada, el ruteador podría avisar al personal de administración y, posiblemente, desviar el tráfico a un enlace temporal alternativo.

PPP proporciona una forma muy simple y efectiva de comprobar la calidad de un enlace. El proceso de control del enlace simplemente cuenta el número de tramas y octetos enviados y recibidos. También se cuentan las tramas descartadas y los errores. Periódicamente, se envía un informe a el otro extremo del enlace.

Esta información presenta una buena imagen de lo que ocurre en el enlace. Por ejemplo, si se han enviado 100,000 octetos durante un cierto intervalo de tiempo, pero el otro extremo informa que sólo ha recibido 50,000 correctamente, algo esta pasando en el enlace.

6.3.5 Protocolo de Interfaz de Línea Serie

El protocolo de Interfaz de línea serie (SLIP) se invento antes que PPP y proporciona un método rudimentario para la transmisión de datagramas de IP por enlaces serie.

Seguramente, SLIP sea el protocolo más primitivo que se haya inventado. Sencillamente se transmite un datagrama de IP, byte a byte, por una línea serie. SLIP marca el inicio y final de un datagrama con el byte delimitador 11000000 (X´C0). ¿Qué ocurre cuando aparece un X´C0 dentro de un datagrama? El SLIP de transmisión usa una secuencia de escape que el SLIP de recepción vuelve a traducir a los datos realmente enviados.

C0 en los datos -- > DB DC

DB en los datos -- > DB DD

Normalmente, se usa SLIP para conectar una PC, una Macintosh o una computadora UNIX a una red de IP mediante un enlace de acceso telefónico. Hay que tomar en cuenta que SLIP no proporciona secuencia de comprobación de trama y deja la comprobación de errores a las capas superiores. SLIP no puede llevar ningún protocolo que no sea IP.

SLIP comprimido (CSLIP) es una versión mejorada de SLIP que comprime las cabeceras de TCP/IP usando el algoritmo de Van Jacobson. CSLIP proporciona un rendimiento del enlace mucho mejor que SLIP.

SLIP se puede utilizar para las comunicaciones entre host, host a ruteador o entre ruteadores. En la figura 6.17 se muestra un servidor de comunicaciones que admite tanto terminales ASCII "sin inteligencia" como acceso telefónico con SLIP. El dispositivo actúa como un ruteador de IP para el tráfico de SLIP.

La característica más atractiva de SLIP es que se utiliza ampliamente. Su peor característica es que el usuario de una máquina tiene que escribir un programa interpretado (`script`) que lea los indicativos que envía el servidor de comunicaciones y envíe el identificador de usuario, la contraseña y otra información en los momentos apropiados del dialogo. PPP es más funcional, no necesita programas interpretados y prácticamente ha sustituido a SLIP.

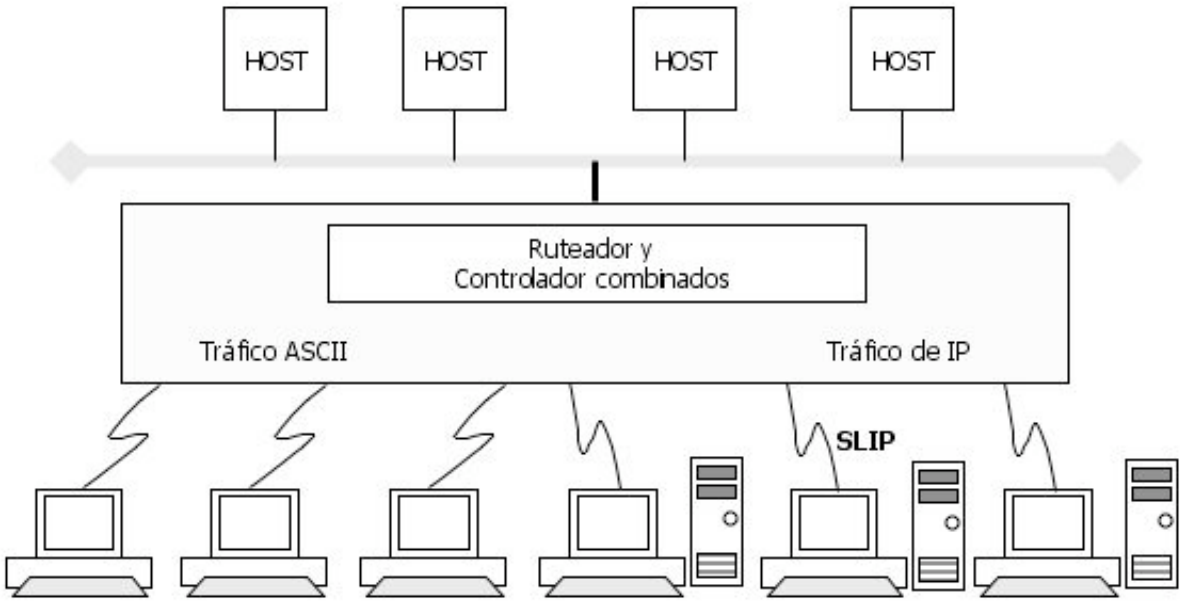


Figura 6.17 Terminal ASCII y conexiones SLIP

6.4 PROTOCOLO DE INTERNET

Se toma en cuenta que una Internet es un conjunto de redes interconectadas con ruteadores y el protocolo de Internet es un protocolo de la capa de red que rutea los datos por una internet. Los investigadores y diseñadores que crearon IP respondían a los requisitos del Departamento de Defensa (DOD) de Estados Unidos de crear un protocolo que pudiese.

- Usarse en host y ruteadores de distintos fabricantes
- Seguir el crecimiento de distintos tipos de redes
- Permitir que la red crezca sin interrumpir el servicio
- Admitir sesiones de nivel superior y servicios orientados a mensajes

La arquitectura de la capa de red de IP se diseñó para cubrir estas necesidades.
Resulto que IP también daba a los creadores de redes exactamente lo que necesitaban para integrar las redes de área local (LAN) que se habían extendido por sus organizaciones como islas. Más aún, las nuevas islas se podían conectar sin tener que interrumpir las que ya había.

Estas características hicieron que IP se convirtiese en el protocolo de red elegido por la agencias gubernamentales, universidades y empresas.

6.4.1 Datagramas de IP

El protocolo de IP ofrece los mecanismos necesarios para transportar unidades, llamadas Datagramas de IP, por una internet. Como se muestra en la figura 6.18, un datagrama de IP está constituido por una cabecera de IP y un trozo de datos a entregar.

IP es un protocolo de "lo mejor que se pueda". Significa que IP no garantiza que el datagrama se entregue a su destino. Todo lo que garantiza es que se hará lo mejor que se pueda. Un datagrama se puede destruir en el camino debido a:

- Errores de los bits durante su transmisión por el medio

- Que un ruteador congestionado descartó el datagrama debido a falta de espacio en el búfer.
- Temporalmente, no había camino hasta el destino.

Todas las funciones que aseguran la fiabilidad se han concentrado en la capa TCP. La recuperación de datos destruidos depende de las acciones de TCP.

Figura 6.18 Formato de un datagrama

La función principal de IP es aceptar datos de TCP o del protocolo de datagramas de usuario (UDP), crear un datagrama, rutear por la red y entregarlo a una aplicación de destino.

Cada datagrama de IP se rutea de forma independiente. IP confía en dos herramientas que le ayuden a rutear los datagramas:

- La mascara de subred
- La tabla de ruteo de IP

6.4.2 Uso de la Macara de Subred

Supongamos que una computadora tiene la dirección IP 130.15.12.131 y está conectada a una LAN. Si tiene datos que enviar:

Desde: 130.15.12.131

A: 130.15.12.22

Puede suponer que ambos sistemas están en la misma subred. Sin embargo, la computadora debe comprobar si es cierto o no. Se hace comprobando la máscara de subred. Suponga que su host tiene la máscara de subred:

255.255.255.0

Significa que la máscara tiene 24 unos y 8 ceros:

11111111 11111111 11111111 00000000

Se debe recordar que los unos de la máscara de subred identifican la parte de red y subred de la dirección. Como tanto la parte de red y subred de las direcciones de origen y destino es 130.15.12 ambas están en la misma subred.

La computadora, realmente, realiza un AND lógico entre la máscara y cada una de las direcciones de IP. El efecto de que los ceros de la máscara de subred ponen a cero la parte de host de la dirección, dejando sólo las partes de red y subred.

En éste ejemplo, el ruteador es directo. Significa que hay que envolver el datagrama en una trama y transmitirlo directamente a su destino en la LAN, como se muestra en la figura 6.19.

La dirección de destino que se pone en la cabecera de la trama debe ser la dirección física del sistema de destino. Se comprueba la tabla del protocolo de resolución de direcciones (ARP) para

comprobar si existe una entrada que tenga la dirección física 130.15.12.22. Si todavía no existe una entrada, se usa el protocolo ARP para crear una.

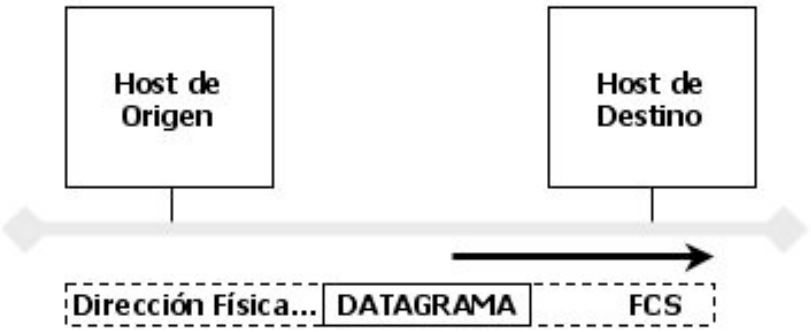


Figura 6.19 Colocación de una trama y transmisión del datagrama

6.4.3 Tabla de Ruteo de Host de IP

Supongamos que se tienen datos que enviar:

Desde 130.15.12.131

A: 192.45.89.5

Una rápida comprobación de la máscara de subred muestra que el destino no está en la subred local. En éste caso, IP debe consultar su tabla local de ruteo.

La tabla de ruteo del host, normalmente, es muy simple; Si el destino no se encuentra en la red local, el host no tiene elección. La única forma de abandonar la red local es a través del Ruteador.

Cada host y computadora personal de la LAN contienen una tabla de ruteo que indica a IP cómo rutear los datagramas hacia sistemas que no estén conectados a la LAN. Para indicar el camino hacia lugares remotos, la tabla de ruteo solo necesita una entrada default, por ejemplo: 130.15.12.1.

Es decir, envía cualquier datagrama a maquinas remotas al Ruteador por defecto, que tiene la dirección IP 130.15.12.1. Hay que tomar en cuenta que la dirección de destino 0.0.0.0 se usa en las tablas de ruteo para indicar "por defecto".

6.4.4 Ruteo de Salto Siguiente

La razón por la que las tablas de ruteo pueden ser tan simples es que IP no necesita conocer la ruta completa que se seguirá hasta el destino. Sólo necesita descubrir cuál es el siguiente salto y enviar allí el datagrama.

Para enviar un datagrama a la interfaz del Ruteador en 130.15.12.1, hay que envolver el datagrama en una trama cuya cabecera contenga la dirección física de la tarjeta de interfaz del Ruteador.

Cuando el Ruteador recibe la trama, elimina la cabecera y la cola de la trama y examina la cabecera del datagrama de IP para decidir hacia donde debe ir a continuación.

Regla para la Búsqueda en la Tabla de Ruteo

Cada entrada en la tabla de ruteo ofrece información sobre el ruteo a un destino individual. Un destino de la tabla de ruteo puede ser un host concreto, una subred, una superred o default.

Existe una regla general que se aplica a la forma en que IP usa la tabla de ruteo, si la tabla se encuentra en un host o en un Ruteador. La entrada que se elige debería basarse en la coincidencia más precisa con la dirección de IP de destino. En otras palabras, cuando IP busca la dirección de un host de destino es, conceptualmente, como sigue:

- Se busca primero en la tabla para ver si hay una entrada que coincida completamente con la dirección de IP. Si existe se usa dicha entrada para rutear el tráfico.
- Si no existe, se busca en la tabla una entrada que corresponda a la subred de destino.
- Si no existe, se busca en la tabla una entrada con la red de destino.
- Si no existe, se busca en la tabla si existe una entrada con un prefijo de ruteo.
- Si no existe, se usa el ruteador por defecto.

En realidad, en una implementación real sólo se busca en la tabla una sola vez, eliminando una entrada cuando se encuentra otra que es más precisa.

Tablas de Ruteo del Ruteador

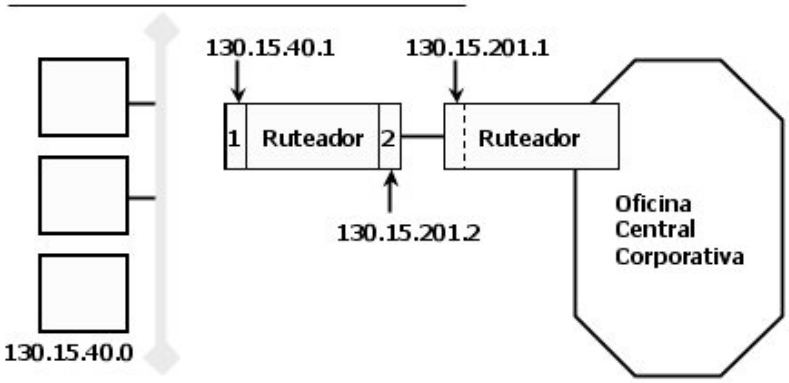
Las tablas de ruteo de un host pueden ser muy sencillas, pero las tablas de los ruteadores suelen contener más información. Un Ruteador tiene dos o más interfaces y hay que transmitir cada datagrama a la interfaz apropiada. Puede que el Ruteador tenga que registrar la selección del siguiente salto para muchas redes y subredes distintas.

Tabla de Ruteo de la Filial

Algunos ruteadores tienen tablas de ruteo muy simples. Por ejemplo, el Ruteador de la filial de la figura 6.20 dirige el tráfico entrante de la oficina central a la LAN del lugar y reenvía todo el tráfico saliente hacia el enlace de área extensa al Ruteador de la oficina central.

Este Ruteador tiene dos interfaces:

Interfaz	Dirección IP
1	130.15.40.1
2	130.15.201.2



La información de la tabla de ruteo incluiría:

Destino	Interfaz	Siguiente Salto	Tipo	Protocolo
130.15.40.0	1	130.15.40.1	Directo	Manual
0.0.0.0	2	130.15.201.1	Indirecto	Manual

Figura 6.20 Ruteo de la Filial

La primera entrada describe, únicamente, la conexión directa a la subred conectada localmente, 130.15.40.0. Se llega a la subred directamente por su propia interfaz.

La segunda entrada es el camino por defecto para el resto de las redes. Para el Ruteador su siguiente salto es 130.15.201.1 y se alcanza por la interfaz 2. Los destinos de la oficina central se alcanzaran indirectamente, a través del Ruteador de siguiente salto. Ambos ruteadores se han introducido manualmente.

6.4.5 Operaciones Globales de Ruteo

En la figura 6.21 se muestra una operación global de ruteo de IP.

Cuando TCP o UDP desde el host A quiere enviar datos al otro extremo en el host B, el origen pasa los datos a IP junto con la dirección del host de destino. IP añade a los datos una cabecera que contiene la dirección IP de destino.

- IP en el host A examina la dirección de destino para determinar si el destino se encuentra en la subred local. Si no es así, IP busca en la tabla de ruteo.
- La tabla indica que el siguiente salto es el ruteador "X" . Se añade una trama al datagrama y en la cabecera de la trama se pone la dirección física de la LAN del ruteador "X".
- Cuando llega un datagrama al ruteador "X", se elimina la trama. El IP del ruteador "X" compara la dirección de IP de destino con todas sus direcciones de IP (usando las máscaras de subred) para comprobar si el destino se encuentra en una subred conectada localmente.
- No es así, por lo que IP realiza una búsqueda en la tabla de ruteo. El siguiente salto es el ruteador "Y". Se añade una trama al datagrama para su transmisión en serie y se envía al ruteador "Y".
- Cuando el datagrama llega al ruteador "Y" se elimina la trama. El IP del ruteador "Y" compara la dirección de IP de destino con todas sus direcciones de IP (usando las máscaras de subred) para comprobar si el destino se encuentra en una subred conectada localmente. Lo está y, por tanto, el ruteador "Y" añade una trama al datagrama para entregarlo al host B.

Esta ruta desde el host A hasta el host B tiene tres saltos: de "A" a "X", de X a "Y" y de "Y" a "B".

6.4.6 Características de IP

IP dispone de ciertas características que contribuyen a dotarle de flexibilidad y capacidad para adaptarse a muchos entornos diferentes. Entre ellas están el ruteo adaptativo de datagramas y la fragmentación y reensamblado.

Ruteo Adaptativo

Normalmente, el ruteo de los datagramas es adaptativo. Es decir, en todo momento se realiza la mejor elección para el siguiente salto comprobando la tabla de ruteo del nodo actual. Las entradas de la tabla de ruteo pueden cambiar en cualquier momento dependiendo de las condiciones de la red.

Según la figura 6.22, por ejemplo, si un enlace deja de funcionar se enviarán los datagramas por otra ruta diferente, si existe.

Un cambio en la topología de la red puede hacer que los datagramas se re-enruten automáticamente. El ruteo adaptativo es la base de la flexibilidad y la robustez de IP.

Por otra parte, una cabecera de IP puede contener una ruta concreta que hay que seguir hasta un destino. Se puede hacer para rutear tráfico sensible por un camino seguro.

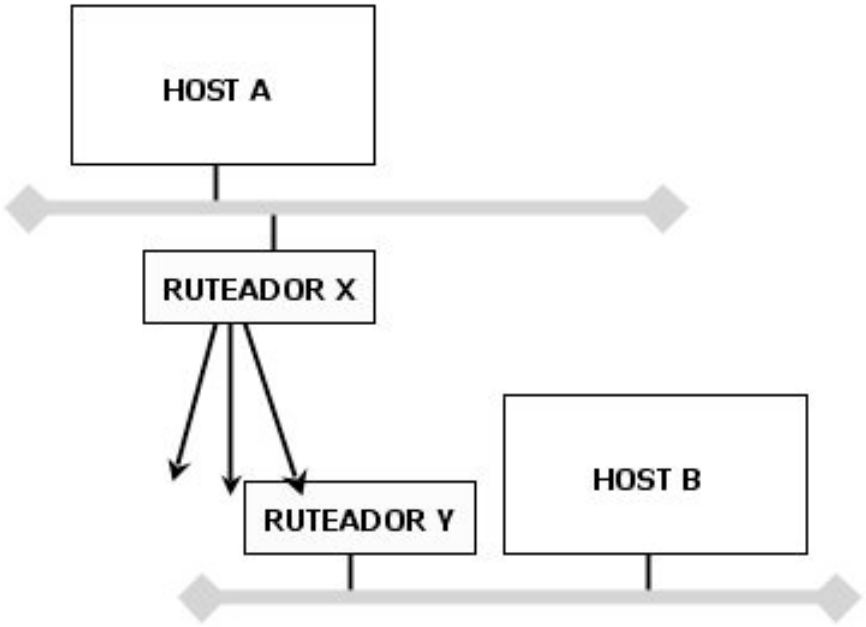


Figura 6.21 Ruteo Global

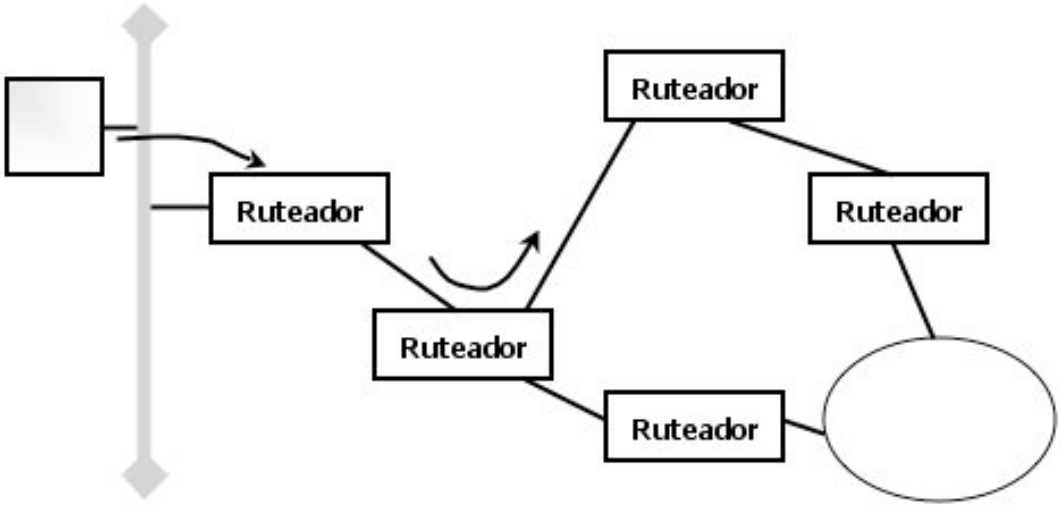


Figura 6.22 Ruteo Adaptativo

6.4.7 MTU, Fragmentación y Reensamblado

Como se muestra en la figura 6.23, antes de transmitir un datagrama por un salto de red, debe encapsularse por las cabeceras de la capa 2 dependiendo de la tecnología de red. Por ejemplo, para atravesar una red 802.3 u 802.5, se añade una cabecera de control lógico del enlace (LLC), una subcabecera del protocolo de acceso a la subred (SNAP), una cabecera de control de acceso al medio (MAC) y una cola MAC.

Como ya se ha visto, cada tecnología de LAN y WAN impone límites diferentes al tamaño de tramas. Un datagrama debe caber en una trama, por lo que el tamaño máximo de trama restringe el tamaño de los datagramas que se pueden enviar por un medio.

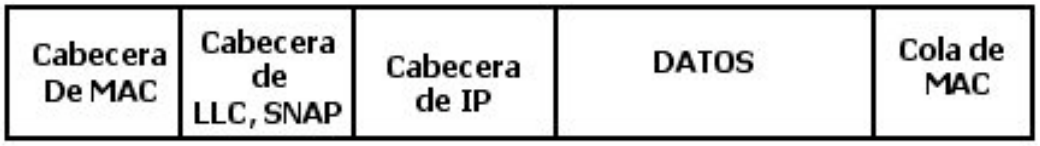


Figura 6.23 Formato de transmisión de una trama de LAN

El tamaño máximo de un datagrama por un medio se calcula restando el tamaño de la cabecera de la trama , la cola de la trama y la cabecera de la capa de enlace de datos del tamaño máximo total de la trama.

Máximo tamaño de trama – tamaño de la cabecera – tamaño de la cola de la trama – tamaño de la cabecera de enlace de datos.

Se debe recordar que el mayor tamaño de un datagrama por un medio se denomina Unidad Máxima de transmisión (Maximum Transmission Unit – MTU). Por ejemplo, DIX Ethernet tiene un MTU de 1500 octetos.

802.3 tiene una MTU de 1492 octetos, la interfaz distribuida de datos por fibra (FDDI) tiene una MTU de 4352 octetos y el servicio de conmutación de datos Multimegabit (SMDS) tiene una MTU de 9180 octetos.

En una internet grande, un host origen puede que no conozca los límites de tamaño con que se va a encontrar un datagrama en el camino. ¿Qué ocurre si el host origen ha enviado un datagrama que es demasiado grande para algún nodo intermedio?

Cuando llega el datagrama al ruteador conectado a la red intermedia, IP resuelve el problema de tamaño dividiendo el datagrama en varios datagramas menores llamados fragmentos. Es responsabilidad del IP del host de destino recoger los fragmentos y reconstruir el datagrama original.

La fragmentación se suele realizar en los ruteadores. Sin embargo, una aplicación de UDP podría iniciar un mensaje muy grande que hiciese que el host origen dividiese en fragmentos un datagrama.

6.5 PROTOCOLO DE CONTROL DE TRANSMISIÓN

IP es simple para que la capa de red se centre en una importante función, el ruteo de datos desde el emisor hacia el destino. La función de TCP es convertir el intercambio de datagramas en una conexión de datos entre aplicaciones sólida y fiable, que se implementa en el host final. Los servicios como World Wide Web (WWW), conexión a terminales remotas, transferencia de archivos y transferencia de mensajes se efectúan con conexiones TCP.

6.5.1 Principales Servicios de TCP

Se puede pensar en TCP como si ofreciera llamadas de datos, de forma similar a las llamadas telefónicas de voz. Quien efectúa la llamada identifica el destino. En el otro extremo, se avisa a una aplicación que esta escuchando que existe una llamada entrante y acepta la conexión. Los dos

extremos intercambian información durante cierto tiempo. Cuando han terminado, ambos dicen "adiós" y cuelgan.

IP utiliza una entrega de datagramas lo mejor que se pueda, pero puede que algunos se destruyan en el camino y otros lleguen desordenados. Puede que un datagrama esté en la red durante un largo periodo de tiempo y llegue inesperadamente. Es tarea de TCP asegurar que los datos se entreguen fiablemente, en secuencia y sin confusiones o errores.

Una aplicación rápida, en un host potente, puede saturar a un receptor lento de datos. TCP proporciona control de flujo lo que permite al receptor regular la cantidad de datos a la que el emisor debe enviarlos. TCP también dispone de mecanismos que le permiten responder a las condiciones de la red, ajustando su propio comportamiento para optimizar el rendimiento.

TCP y el Modelo Cliente / Servidor

TCP funciona de manera muy natural en un entorno cliente/ servidor. Una aplicación servidora escucha solicitudes entrantes de conexión. Por ejemplo, los servidores de World Wide Web, transferencia de archivos y terminal virtual escuchan a los clientes. Una aplicación cliente inicia la comunicación TCP invocando las rutinas de comunicación que establecen una conexión con un servidor. El "cliente" puede ser realmente otro servidor, por ejemplo, un servidor de correo se conecta a otro servidor de correo para transferir el correo entre dos computadoras.

6.5.2 Conceptos de TCP

¿De que forma traslada una aplicación datos a TCP? ¿De que forma TCP traslada datos a IP? ¿Cómo se identifican las conexiones entre aplicaciones a las que pertenecen las unidades de datos? Estas preguntas se responderán a continuación.

Flujos de Datos de Entrada

El modelo conceptual de una conexión es que una aplicación envía un flujo de datos a otra aplicación pareja. Al mismo tiempo, recibe un flujo de datos de la otra. TCP proporciona un servicio dúplex que maneja simultáneamente los dos flujos de datos, como se observa en la figura 6.24.

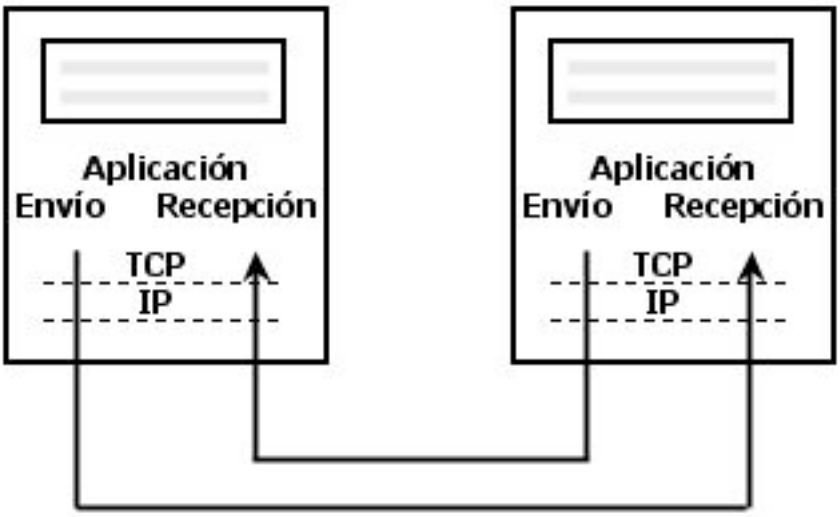


Figura 6.24 Aplicaciones Intercambiándose flujos de Datos

Segmentos

TCP debe convertir los flujos de datos salientes de una aplicación de forma que se puedan entregar como datagramas lo que se explica a continuación:

La aplicación traslada los datos a TCP y TCP sitúa estos datos en un búfer de envío. TCP toma un trozo de los datos y le añade una cabecera, creando un segmento. TCP traslada el segmento a IP para que lo entregue como un único datagrama. El empaquetado de datos en trozos del tamaño adecuado permite usar de manera eficiente los servicios de transmisión, por lo que TCP debería esperar a recoger una cantidad razonable de datos antes de crear un segmento.

Push

Pero, a veces no resultan apropiados para una determinada aplicación trozos de datos grandes y eficientes. Por ejemplo, supongamos un programa cliente que ha iniciado una sesión interactiva con un servidor remoto y el usuario ha tecleado un comando, y pulsado enter.

El programa cliente requiere que TCP sepa que los datos deberían enviarse al host remoto y entregarse a la aplicación del servidor inmediatamente. Esto es posible con la función Push.

Si se observa un trazo de una sesión interactiva, se podrá observar muchos segmentos que contienen muy pocos datos y probablemente se pueda ver una señal de push en cada uno de ellos. Por otra parte, no se debería usar push durante una transferencia de archivos (excepto por el último segmento), para que TCP pueda empaquetar los datos en segmentos de la forma más eficiente posible.

Datos Urgentes

Recordando que la transmisión de datos de una aplicación se modela como un flujo ordenado de bytes hacia su destino. Pero siguiendo con el ejemplo de una sesión interactiva suponga que un usuario ha pulsado una tecla de aviso o interrupción. La aplicación debería ser capaz de saltarse los bytes intermedios y avisar lo antes posible.

Existe un mecanismo de Datos Urgentes para marcar un segmento concreto como urgente, TCP puede avisar al otro extremo de que un segmento contiene datos urgentes y puede indicar cuales son los datos. El TCP del otro extremo puede trasladar esta información a la aplicación de destino.

Puertos de Aplicación

Un cliente debe identificar el servicio que desee. Esto se realiza especificando la dirección de IP del host y su número de puerto de TCP. Al igual que para el protocolo de datagramas de usuario (UDP) los números de puerto de TCP están en el intervalo "0 a 65535". Recordando que los puertos en el intervalo "0 a 1023" ya están asignados y se usan para acceder a servicios estandarizados.

En la tabla 6.1 se ofrece una lista de algunos puertos de TCP y sus aplicaciones. Discard en el puerto 9 y Chargen en el puerto 19 son las versiones de TCP de los servicios de utilidad descritos para UDP. Recordemos que el tráfico que se envía al puerto 9 de TCP está totalmente separado del tráfico que se envía al puerto 9 de UDP.

¿Pero y los puertos que usan los clientes? Existen algunos casos en que un cliente trabaja con un puerto distinto de uno de los estandarizados, pero la mayor parte de la veces, un cliente que quiere

una conexión pide al sistema operativo que le asigne un número de puerto en desuso, sin reservar. Al finalizar la conexión, el cliente devuelve el puerto al sistema y lo puede utilizar otro cliente. Como existen más de 63000 puertos sin reservar, los clientes no tienen ningún problema de uso de puertos.

Puerto	Aplicación	Descripción
9	Discard	Descartar todos los datos entrantes
19	Chargen	Intercambiar flujos de caracteres
20	FTP-Data	Puerto de transferencia de datos para la transferencia de archivos
21	FTP	Puerto de diálogo para la transferencia de archivos
23	TELNET	Puerto de conexión remota mediante Telnet
25	SMTP	Puerto del protocolo simple de transferencia de correo
110	POP3	Servicio de recuperación de correo de PC
119	NNTP	Acceso a las noticias de red

Tabla 6.1 Puertos de TCP estandarizados y sus aplicaciones

Dirección de Conectores

Recordando que la combinación de una dirección IP y el puerto que se usa en la comunicación se denomina una dirección de conector (socket). Una aplicación TCP queda completamente definida mediante las direcciones de los conectores de ambos extremos. En la figura 6.25 se muestra una conexión entre un cliente con una dirección de conector (128.36.1.24, puerto=3358) y un servidor con una dirección de conector (130.42.88.22, puerto=21).

Figura 6.25 Direcciones de Conectores

Todas las cabeceras de un datagrama contienen las direcciones de IP del emisor y del receptor. Los números de puerto del emisor y del destino están en la cabecera del segmento de TCP.

Normalmente, un servidor es capaz de manejar muchos clientes a la vez. Todos los clientes deben acceder simultáneamente a la dirección del conector único del servidor, como se muestra en la figura 6.26.

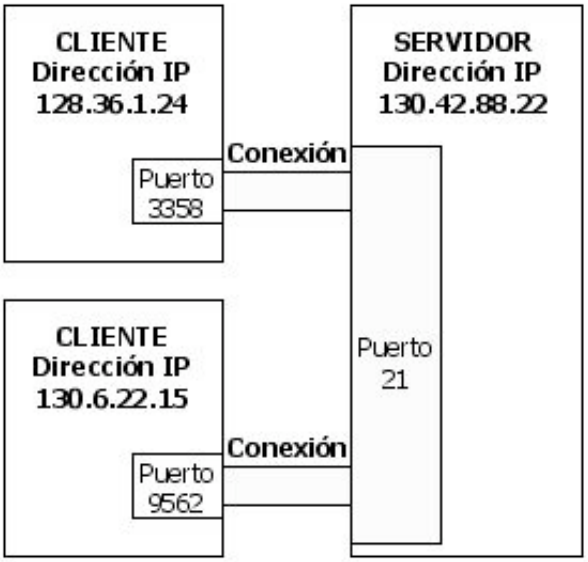


Figura 6.26 Múltiples clientes conectándose a una dirección de conector de un servidor

Como un datagrama transporta un segmento para una conexión concreta de TCP e identifica ambas direcciones de IP y ambos puertos, resulta sencillo que el servidor mantenga conexiones con múltiples clientes.

6.5.3 Establecimiento de una Conexión

¿Cómo se inicia una conexión entre dos aplicaciones? Antes de poder comunicarse, cada parte llama a una subrutina que crea un bloque de memoria para almacenar los parámetros de TCP y de IP durante la conexión, como las direcciones de los conectores (sockets), los números actuales de secuencia, el valor inicial de IP para el tiempo de vida y otros.

La aplicación servidora espera a los clientes. Un cliente que desee acceder al servidor lanza una solicitud de conexión mediante la dirección de IP y el puerto del servidor.

Hay un aspecto técnico. En lugar de empezar a numerar los bytes en 1, cada parte genera un número inicial de secuencia aleatoria.

Escenario de Conexión

El procedimiento de conexión se denomina un acuerdo en tres pasos, ya que intercambian tres mensajes para establecer la conexión, llamadas SYN, SYN y ACK.

Durante el establecimiento de la conexión se intercambian importantes elementos de información. Cada parte notifica a la otra:

1. Del espacio disponible en su búfer para recibir datos
2. La cantidad máxima de datos que puede llevar un segmento
3. El número inicial de secuencia que se usará para numerar los datos de salida

Se debe tener en cuenta que cada parte usa los elementos 1 y 2 para establecer los límites de lo que puede hacer la otra parte. Una PC podría tener un pequeño búfer de recepción, mientras una súper computadora podría tener un búfer muy grande. La estructura de memoria de una PC podría limitar el

tamaño de los trozos de datos a 1K, mientras que una súper computadora podría manejar segmentos de datos de mayor tamaño.

La posibilidad de controlar cómo la otra parte envía los datos, es una característica importante para la escalabilidad de TCP/IP.

En la figura 6.27 se muestra un escenario simple de conexión. Se muestran los números de secuencia inicial, para facilitar su lectura. Hay que tener en cuenta que en este ejemplo, el cliente es capaz de recibir mayores segmentos que el servidor. Los pasos son:

1. El servidor se inicializa y está listo para aceptar conexiones de clientes. A esto se le denomina apertura pasiva (Passive Open).
2. El cliente solicita a TCP que abra una conexión con un servidor en una determinada dirección y puerto de IP. A esto se denomina una apertura activa (Active Open).
3. El TCP cliente recoge un número inicial de secuencia, 1000 en el ejemplo. El TCP cliente envía un segmento de sincronización. Llamado SYN, con éste número de secuencia, el tamaño de la ventana de recepción (4K) y el tamaño de mayor segmento que puede recibir el cliente (1460 bytes).
4. Cuando llega SYN, el TCP servidor genera su número inicial de secuencia (3000). EL TCP servidor envía un segmento SYN con su número inicial de secuencia (3000), un ACK 1001, que significa que el primer byte de datos enviados por el cliente debería tener un número 1001, el tamaño de su ventana de recepción (4K) y el tamaño de mayor segmento de datos que puede recibir (1024 bytes).
5. Cuando el TCP cliente recibe el mensaje SYN/ACK del servidor, envía de vuelta un ACK 3001, lo que significa que el primer byte de datos enviado por el servidor debería tener el número 3001.
6. El TCP cliente notifica a su aplicación que la conexión esta abierta.
7. Cuando el TCP servidor recibe el ACK de TCP cliente, el servidor notifica a su aplicación que la conexión esta abierta.

El cliente y el servidor han anunciado sus reglas para la recepción de datos, han sincronizado sus números de secuencia y están listos para intercambiar datos.

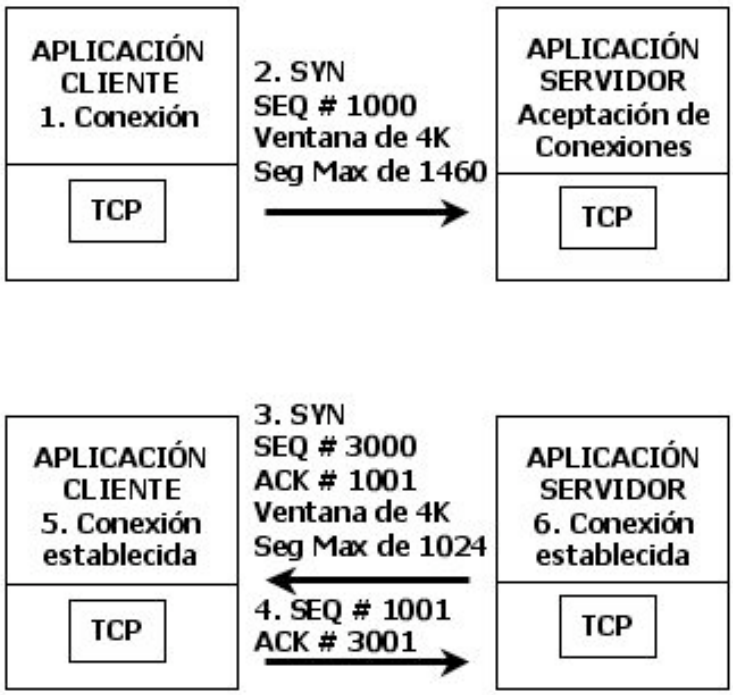


Figura 6.27 Establecimiento de una conexión

6.5.4 Configuración de Parámetros de IP

La llamada de programación que establece una conexión puede fijar parámetros de los datagramas de IP que transportarán los datos de la conexión. Cuando no se dan valores concretos, se usan los valores por defecto del sistema.

Por ejemplo, una aplicación puede pedir una Precedencia o tipo de servicio de IP concretos. Como cada extremo de una conexión elige su propia Precedencia o tipo de servicio de forma independiente, en teoría, podrían ser diferentes en cada sentido de flujo de datos. En la práctica, normalmente se usan los mismos.

Cuando las aplicaciones usan la opción de seguridad de IP del gobierno / militar, ambos extremos de la conexión deben trabajar con el mismo nivel de seguridad o, si no, la conexión termina.

Transferencia de Datos

La transferencia de datos comienza después de terminar el establecimiento en tres pasos. En la figura 6.28 se muestra un intercambio directo de datos. Para que la numeración resulte sencilla, se usan mensaje de 1000 bytes. Todas las cabeceras de los segmentos de TCP llevan un campo ACK que identifica el número de secuencia del siguiente byte que se espera del otro extremo.

El primer segmento que envía el cliente contiene los bytes del 1001 al 2000. Su campo ACK anuncia que el número de secuencia del siguiente byte que espera del servidor es 3001.

El servidor responde con un segmento que contienen 1000 bytes de datos que empieza en el 3001. El campo ACK de la cabecera de TCP indica que se han recibido correctamente los bytes 1001 a 2000, por lo que el número de secuencia que se espera del siguiente byte del cliente es 2001.

A continuación, el cliente envía segmentos que empiezan en los bytes 2001, 3001 y 4001. Hay que tener en cuenta que el cliente no tiene que esperar a que llegue el ACK de cada segmento. Se pueden enviar datos al otro extremo siempre que disponga de espació no utilizado en el búfer. El servidor ahorra ancho de banda si se usa un único ACK para indicar que todos los segmentos se recibieron correctamente.

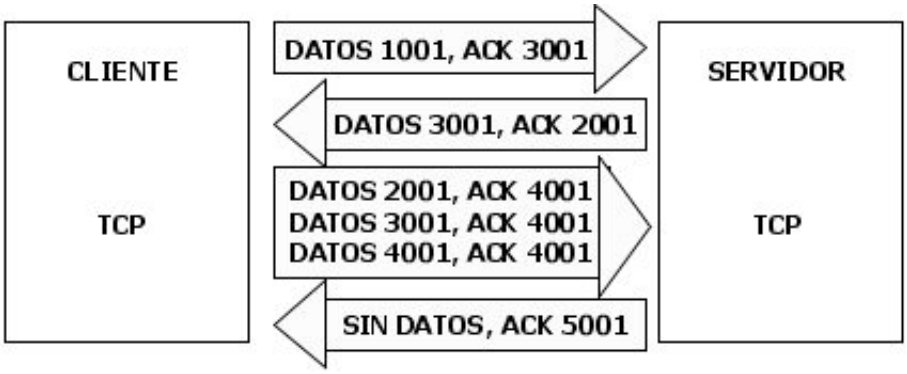


Figura 6.28 Flujo sencillo de datos y sus ACK.

En la figura 6.29 se muestra una transferencia en la que se pierde el primer segmento. Tras un cierto plazo, el segmento se vuelve a transmitir. Se debe tener en cuenta que una vez que llega el segmento perdido, el receptor puede enviar un único ACK que confirma que ambos segmentos han llegado correctamente.

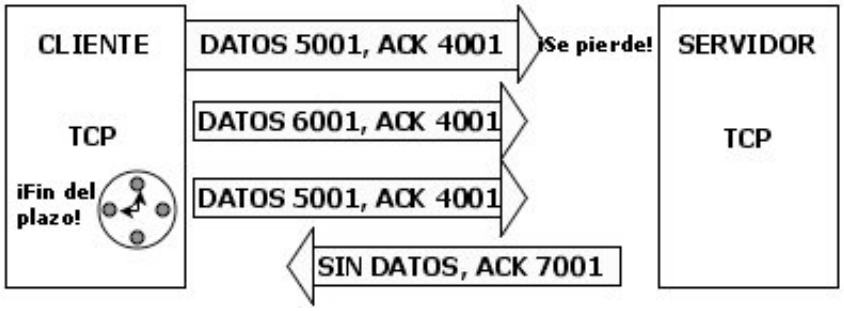


Figura 6.29 Pérdida de datos y su retransmisión.

Terminación de Conexión

La terminación normal de una conexión se lleva a cabo mediante un proceso en tres pasos similar al del establecimiento. Cualquiera de las partes puede lanzar el proceso de terminación, que suele ser como sigue:

A: "He terminado. No tengo más datos para enviar"

B: "OK"

C: "Yo también he terminado"

A: "OK"

También es válida la siguiente secuencia, aunque raramente se usa:

A: "Ya he terminado. No tengo más datos para enviar"

B: "OK, pero yo tengo algunos datos…"

B: "Yo también he terminado"

A: "OK"

En el ejemplo, el servidor empieza a cerrar la conexión, como suele ocurrir en una interacción real cliente / servidor. Por ejemplo, tras una sesión de telnet el usuario escribe "log-out", el servidor invoca a una llamada para cerrar la conexión.

1. La aplicación servidora índica a TCP que termine la conexión.
2. El TCP servidor envía un segmento final (Final Segment) (FIN), informando a la otra parte que no va a enviar más datos.
3. El TCP cliente envía un ACK del segmento FIN.
4. El TCP cliente notifica a su aplicación que el servidor quiere terminar.
5. La aplicación cliente indica a TCP que termine.
6. El TCP cliente envía un mensaje FIN.
7. El TCP servidor recibe el FIN del cliente y responde con un ACK.
8. El TCP servidor notifica a su aplicación que la conexión se ha terminado.

Ambas partes pueden iniciar la terminación simultáneamente. En éste caso la terminación normal se completa cuando cada una de las partes ha enviado un ACK.

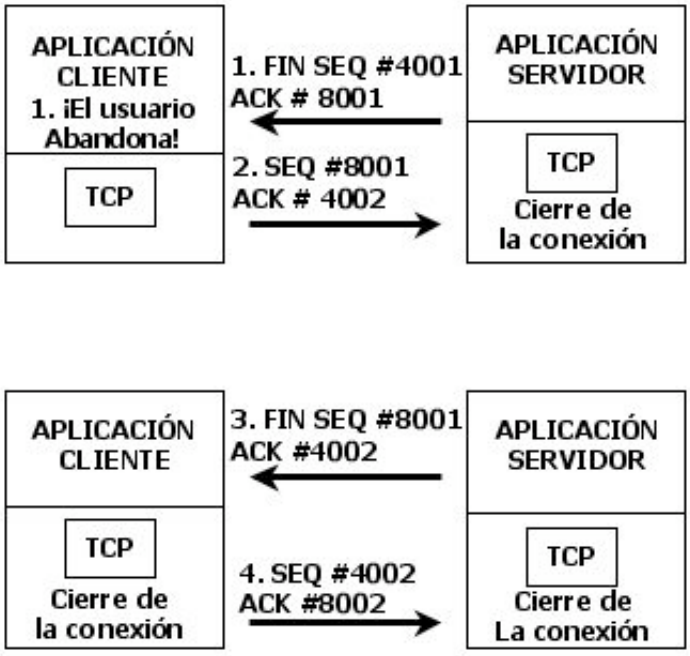


Figura 6.30 Terminación de una conexión.

Terminación Abrupta

Cualquiera de las partes puede invocar una terminación abrupta. Puede realizarse si una aplicación quiere abortar una conexión o si TCP ha detectado un problema serio en la comunicación que no se puede resolver. Se solicita una terminación abrupta enviando uno o más "reset" al otro extremo. El "reset" se indica mediante una bandera de la cabecera de TCP.

Control de Flujo

El TCP que recibe los datos se encarga del flujo de los datos de entrada. El receptor decide cuántos datos desea aceptar y el emisor debe actuar dentro de estos límites. A continuación se describe lo que ocurre desde un punto de vista conceptual. Los fabricantes pueden implantar estos mecanismos de la forma que les sea más conveniente.

Durante el establecimiento de la conexión, cada parte asigna espacio para los Búfer de recepción para esa conexión y lo comunica "Este es el número de bytes que puedes enviarme". Este número suele ser un múltiplo entero del tamaño máximo de segmento.

El flujo de datos llega al búfer de recepción y permanece ahí hasta que lo recoge la aplicación asociada a éste puerto de TCP. En la figura 6.31 se muestra un búfer de recepción que puede almacenar 4K.

El espacio del búfer se utiliza según llegan los datos. Cuando la aplicación recoge los datos del espacio se libera para los próximos datos de entrada.

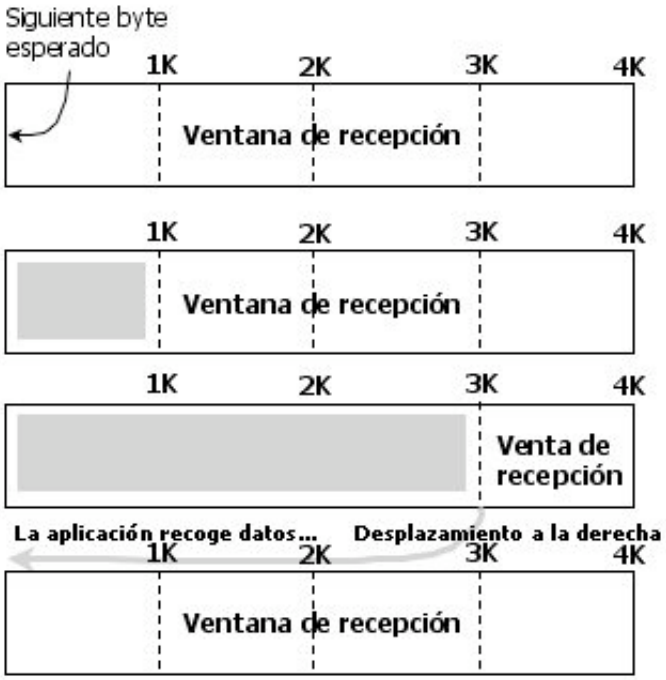


Figura 6.31 Ventana de recepción del búfer de recepción.

6.5.5 Ventana de Recepción

La ventana de recepción es cualquier espacio del búfer de recepción que no está ocupado. Los datos permanecen en el búfer de recepción hasta que la aplicación a la que van dirigidos los recoge. ¿Por qué puede una aplicación no recoger los datos inmediatamente?

Se puede explicar con un escenario sencillo. Por ejemplo, que un cliente envía un archivo a un servidor de transferencia de archivos que se ejecuta en una computadora multiusuario muy ocupada. El programa del servidor de transferencia de archivos leerá los datos del búfer de recepción y los escribirá a disco. Cuando el servidor realice la entrada / salida a disco, el programa ha de esperar a que termine. Durante ese tiempo, otros programas entraran a ejecutarse de acuerdo con el sistema

operativo. Mientras el proceso de transferencia de archivos del servidor está esperando a ejecutarse de nuevo, pueden llegar más datos.

La ventana de recepción se extiende desde el último byte que se ha confirmado hasta el final del búfer. En la figura 6.31 está libre todo el búfer, por lo que hay una ventana de recepción de 4K. Llega 1K de datos y la ventana de recepción se reduce a 3K. Llegan dos segmentos más de 1K, con lo que la ventana se reduce a 1K.

Finalmente la aplicación absorbe los 3K de datos del búfer, con lo que el espacio libre para más datos aumenta. Se puede ver cómo una ventana que se desplaza hacia la derecha. En éste momento los 4K del búfer están libres.

Los ACK del receptor contienen una actualización del estado de la ventana de recepción. El flujo de datos desde el emisor se regula de acuerdo con éstas actualizaciones de la ventana.

La mayor parte del tiempo, el búfer de recepción que se establece durante el establecimiento de la conexión se mantiene durante la misma. Sin embargo, la norma de TCP no restringe de qué forma una cierta implementación controla sus búfer. El búfer de recepción puede crecer o reducir, siempre que el receptor no "se vuelva atrás" de lo que ha concedido al emisor.

¿Qué ocurre cuando llegan segmentos qué están dentro de la ventana, pero llegan desordenados? Virtualmente todas las implementaciones guardan todos los datos que se encuentren dentro de la ventana y asienten con ACK el bloque completo de datos contiguos cuando llegan los datos que faltan. Es una ventaja, pues tirar datos puede conducir a una caída del rendimiento.

6.5.6 Ventana de Envío

El transmisor de los datos controla dos cosas: Cuántos datos le han enviado y ya se han asentido y el tamaño actual de la ventana de recepción del otro lado. El espacio de *envío* activo va desde el primer octeto sin asentir hasta la parte derecha de la ventana de recepción actual. La parte de la ventana de recepción de este espacio índica cuantos datos adicionales se pueden enviar hasta el otro lado.

El número de secuencia inicial y el tamaño inicial de la ventana de recepción se obtienen durante la fase de establecimiento de la conexión. Con un ejemplo (ver figura 6.32), se pueden ver algunos de los mecanismos de la transmisión de datos.

1. El emisor comienza con una ventana de envío de 4K
2. El emisor transmite 1K. Hay que mantener una copia de dichos datos hasta que llegue el asentimiento, ya que puede ser necesario retransmitirlos.

3. Llega un ACK para los primeros 1K y se envían otros 2K de datos. El resultado se muestra en la tercera parte de la figura 6.32. Hay que mantener los 2K.

4. Finalmente, llega un ACK que indica que todos los bytes transmitidos se han recibido. El ACK también actualiza la ventana del receptor a 4K.

Hay que destacar algunas características interesantes:

- El emisor no tiene que esperar un ACK para cada segmento de datos transmitidos. La única limitación para la transmisión es el tamaño de la ventana de recepción. Por ejemplo, el emisor podría transmitir 4096 segmentos de 1 byte.

Suponga que el emisor tiene que retransmitir datos que se enviaron utilizando segmentos muy pequeños (por ejemplo de 80 bytes). Los datos se pueden volver a empaquetar de una manera más eficiente, por ejemplo en un único segmento.

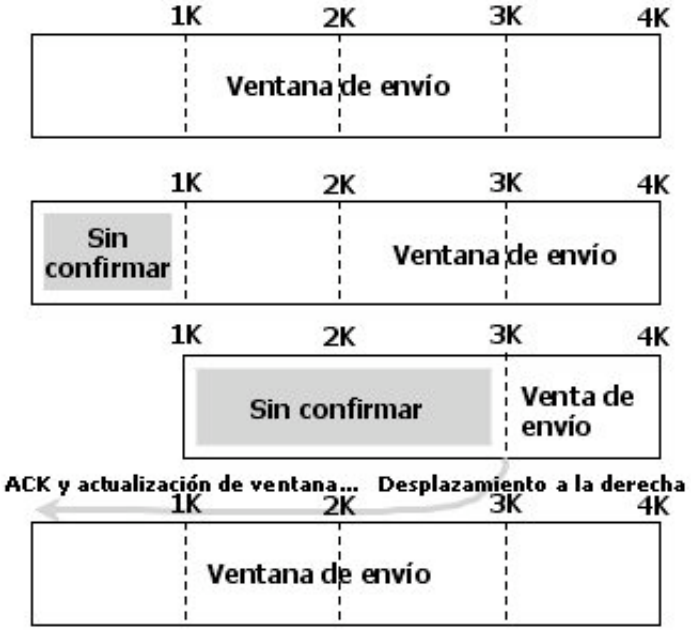


Figura 6.32 Ventana de envío.

6.6 PROTOCOLO DE DATAGRAMA DE USUARIO

El protocolo de datagramas de usuario (UDP) es muy directo. UDP permite que las aplicaciones se envíen entre si mensajes individuales.

¿Porque definir este tipo de servicio? Existen muchas aplicaciones que se pueden construir usando los datagramas de usuario de manera muy natural. Por ejemplo, un simple intercambio de datagramas se puede usar para ejecutar una consulta rápida en una base de datos. Se evita la sobrecarga de enviar y recibir los múltiples mensajes necesarios para establecer y cerrar una conexión, mediante un simple mecanismo de petición y respuesta. UDP también es una pieza perfecta para construir funciones de monitor, depuración, gestión y prueba.

UDP es un servicio muy básico, solamente envía mensajes individuales a IP para su transmisión. Como IP no es fiable, no se garantiza su entrega. Si una aplicación envía una petición en un datagrama de UDP y no llega una respuesta en un tiempo razonable, es responsabilidad de la aplicación el retransmitir la petición.

A veces éste esquema hace que aparezcan peticiones duplicadas en el servidor. Si la aplicación incluye un identificador de transacción con su mensaje de petición, el servidor puede reconocer los duplicados y descartarlos. Este mecanismo es responsabilidad de la aplicación, no de UDP.

6.6.1 Difusión y Multienvío

Otra ventaja de UDP es que lo pueden usar las aplicaciones que necesitan mensajes de difusión o multienvío. Por ejemplo, un cliente de BOOTP difunde una petición de parámetros de inicialización.

Puertos de las Aplicaciones

¿Qué ocurre con los datos cuando llegan a un host de destino? ¿cómo se entregan al proceso apropiado? Como se muestra en la figura 6.33 para cada capa, existe un identificador de protocolo que indica qué hacer con los datos entrantes. En la capa 2 en tipo Ethernet de X´08-00 en una cabecera de la trama indica que la trama se debe pasar por IP. En la capa 3, el campo protocolo de la cabecera IP identifica el protocolo de la capa 4 al que hay que trasladar los datagramas, por ejemplo 6 para TCP, 17 para UDP.

Se puede esperar que un host participe en muchas comunicaciones simultáneas en un cierto momento. ¿Cómo se ordenan y se entregan apropiadamente los datagramas de UDP a los procesos de la capa de aplicación? La respuesta es que a cada extremo de una comunicación de UDP se le asigna un identificador de 16 bits llamado número de puerto.

Los números de puerto del 0 al 1023 están reservados para servicios estándar. Los puertos estándar se llaman puertos públicos (well-Known). El uso de puertos públicos permite que los clientes identifiquen el servicio al que se desea acceder. Por ejemplo, al servicio de nombres de dominio usando UDP se accede por el puerto público 53.

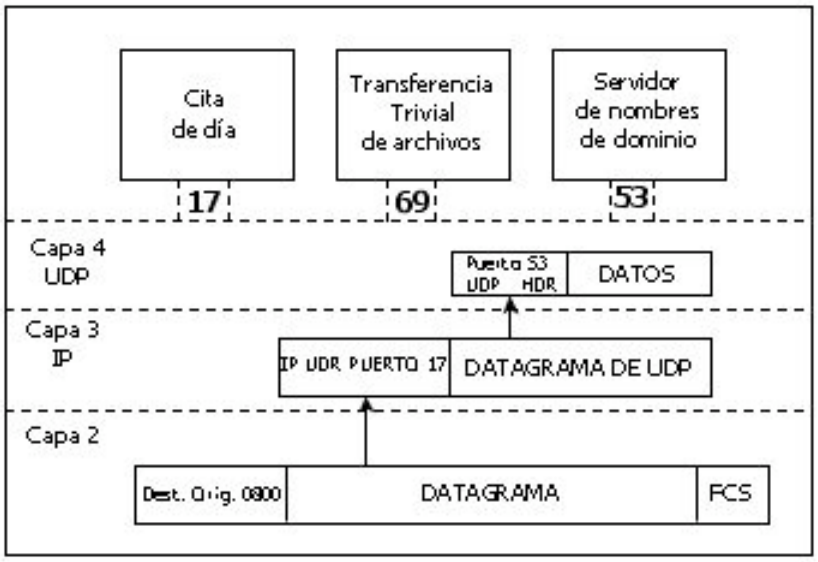
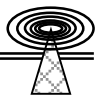


Figura 6.33 Paso de los datos hacia arriba a la capa de aplicación.

¿Cómo se asignan los puertos públicos? Como es de suponer, la autoridad de asignación de números de Internet (IANA – Internet Assigned Numnbers Authority) se encarga de ésta función. Los números de puerto para aplicaciones concretas están registrados por la IANA y publicados en el documento RFC Assigned Numbers. Una lista parcial de los puertos de UDP tomada del documento de RFC actual de Assigned Numbers se muestra en la tabla 6.2.



Algunos de estos servicios proporcionan bloques para probar, depurar y medir. Por ejemplo, el servicio eco en el puerto 7 hace lo que su nombre indica, devuelve cualquier datagrama que se le envía. Descartar en el puerto 9, por otro lado, tira los datagramas. Un generador de caracteres responde a cualquier mensaje con un datagrama que contiene entre 0 y 512 bytes. El número se elige aleatoriamente.

El servicio "cita del día" responde a cualquier datagrama enviando de vuelta un mensaje, por ejemplo, alguna frase de la sabiduría para tenerla en cuenta durante el día tras cerrar la sesión. En muchos sistemas se puede ejecutar el comando fortune que responde con una cita:

> fortune

Churchill´s Commentary on Man:

Man will occasionally stumble over the truth, but most of the time he will pick himself up and continue on.

Servicio	Puerto/ Protocolo	Descripción
Eco (Echo)	**7/UDP**	**Eco del datagrama de usuario de vuelta al emisor**
Descartar (Discard)	**9/UDP**	**Descartar el datagrama de usuario**
Fecha y hora (daytime)	**13/UDP**	**Indica la hora de manera sencilla para el usuario**
Cita (Quote)	**17/UDP**	**Devuelve una cita del día**
Carácter Gen. (Chargen)	**19/UDP**	**Generador de caracteres**
Servidor de Nombres (Nameserver)	**53/UDP**	**Servidor de nombres de dominio**
Bootps	**67/UDP**	**Puerto del servidor usado para descargar la información de configuración.**
TFTP	**69/UDP**	**Puerto del protocolo trivial de transferencia de archivos**
SunRPC	**111/UDP**	**Llamada a procedimientos remotos de SUN**
NTP	**123/UDP**	**Protocolo de tiempo de red**
SNMP	**161/UDP**	**Usado para recibir las peticiones de gestión de red**
SNMP-trap	**162/UDP**	**Usado para recibir los informes de problemas de red**

Tabla 6.2 Ejemplos de puertos públicos de UDP.

Un servidor de fecha y hora responde a cualquier datagrama con un mensaje que contiene la fecha y hora actual en un formato ASCII legible. Por otra parte, el protocolo de tiempo de red (NTP – Network Time Protocol) proporciona un método robusto para sincronizar los relojes de las computadoras de una red.

El servidor y el cliente de BOOTP se usan para inicializar un dispositivo sin configuración. Una estación de trabajo puede descubrir su dirección de IP, su máscara de dirección, la situación de su ruteador por defecto, la dirección de servidores importantes y, si lo necesita, el nombre y ubicación de un archivo de descarga de software desde el servidor de arranque. El software de la estación de trabajo se descarga mediante el protocolo trivial de transferencia de archivos.

Además de los números asignados oficialmente, cualquier sistema que ejecuta TCP/IP puede reservar un intervalo de números para servicios y aplicaciones de red importantes. El resto de los números de red, por encima del 1023, se asigna a los clientes mediante un software de red según se necesitan. El siguiente escenario indica lo que ocurre:

1. Un usuario invoca un programa cliente, por ejemplo nslookup.

2. El proceso cliente ejecuta una rutina del sistema que dice: "Quiero una comunicación de UDP, dame un puerto".
3. La rutina del sistema elige un puerto no usado de los puertos disponibles y se los da al proceso cliente.

Los números de TCP y de UDP son independientes unos de otros. Un proceso puede enviar mensajes por el puerto 1700 de UDP a la vez que otro esta manteniendo una sesión en el puerto 1700 de TCP. Existen algunos servicios que necesitan acceder tanto a TCP como a UDP. En éste caso, el IANA intenta asignar el mismo número a los puertos asignados al servicio de UDP y de TCP. Sin embargo, como extremos de la comunicación siguen estando en "lugares" diferentes.

6.6.2 Direcciones de los Conectores

A la combinación de una dirección IP y de puerto para una comunicación se le llama una dirección de conector. Hay que tener en cuenta que una dirección de conector ofrece toda la información que necesita un cliente o un servidor para identificar a su otro extremo. La cabecera de IP contiene las direcciones de IP de origen y de destino. Las cabeceras de UDP o de TCP contienen los números de puertos de origen y de destino. Por tanto, cada mensaje de UDP o de TCP contiene las direcciones de conector de su origen y de su destino.

6.7 TELNET Y FTP

¿De qué sirve una red con una rica oferta en aplicaciones si los usuarios no pueden acceder a las distintas computadoras, y usar sus aplicaciones? TCP ofrece conectividad entre computadoras, pero existen otros problemas. Durante mucho tiempo dio la impresión de que cada fabricante de computadoras estaba decidido a lanzar al mercado un entorno totalmente propietario. Sólo se podía acceder a una aplicación en el host del fabricante desde terminales especiales manufacturados por él mismo.

El protocolo TELNET (Terminal Networking) vence las diferencias entre fabricantes y permite a un usuario, conectado a un host de una red, comunicarse con cualquier otro host. La emulación de terminal de TELNET fue la primera aplicación de TCP/IP. El protocolo telnet se diseño, además, como base para comunicaciones entre aplicaciones en general. Conforme las organizaciones se han ido alejando de la herencia de las aplicaciones basadas en terminal, se ha usado cada vez más telnet como herramienta para la creación de aplicaciones cliente / servidor. De hecho, telnet es el soporte de las interacciones cliente / servidor en la transferencia de archivos, el correo electrónico y la World Wide Web (WWW).

Uso de TELNET para Conexiones

Telnet permite la emulación de varios tipos de terminal, por lo que se puede acceder a computadoras UNIX, sistemas VAX/VMS o grandes computadoras de IBM. Algunas implementaciones de telnet disponen de procedimientos especiales de autenticación.

Si se ejecuta telnet desde un sistema multiusuario, probablemente se manejará una sencilla interfaz de usuario de texto. La utilización de un cliente telnet de texto es muy fácil. Basta con teclear:

> telnet hostname

A menudo, la emulación de IBM 3270 se suministra por separado y se accede a los host de IBM tecleando:

>tn3270 hostname

Acceso a un Puerto Concreto

por medio de TELNET

El puerto 23 es el puerto público normalizado para el terminal virtual de telnet. Cuando un cliente se conecta al puerto 23, la respuesta es un cursor para introducir un ID de conexión y una contraseña.

Pero, puesto que telnet se diseño como herramienta general de comunicaciones entre aplicaciones, incluye una "alfombra mágica" que puede llevar al cliente a cualquier puerto. La posibilidad de acceder con telnet ha cualquier puerto ha demostrado ser muy convincente. También se ha convertido en una potencial fuente de problemas de seguridad cuando los piratas invaden un lugar a través de un programa deficientemente, que se ejecuta en algún puerto sin restricciones.

6.7.1 Modelo de Emulación de Terminal TELNET

Como se muestra en la figura 6.34, un usuario en un terminal real interacciona con el programa cliente de telnet local. El programa cliente de telnet tiene que aceptar las pulsaciones del teclado del usuario, interpretarlas y mostrar la salida en la pantalla del usuario de forma consistente con la emulación en uso. El cliente telnet abre una conexión de TCP con el servidor telnet, al que se accede por el puerto público 23. El servidor telnet interacciona con las aplicaciones y asiste en la emulación de un terminal nativo.

Terminal Virtual de Red

Para conseguir iniciar una sesión, ambos extremos intercambian información utilizando un protocolo muy sencillo llamado terminal Virtual de red (NVT – Network Virtual Terminal).

El protocolo NVT se modeló en un antiguo teclado semidúplex y una impresora funcionando línea a línea. NVT posee unas características bien definidas:

- Los datos de NVT se componen de caracteres USASCII de 7 bits aumentados a 8 bits por medio de un cero "0" inicial.
- Los datos se envían línea a línea.
- Cada línea termina con una combinación de caracteres ASCII de retorno de carro (CR – Carriage Return) y salto de línea (LF – Linefeed).
- Los bytes cuyo bit inicial (más significativo) es "1" se usan para códigos de comandos.

El protocolo es "semidúplex". Después de enviar una línea, el cliente espera hasta recibir una línea del servidor. El servidor envía sus datos y, a continuación, un comando "adelante" (Go ahead), indicando al cliente que ya puede enviar otra línea.

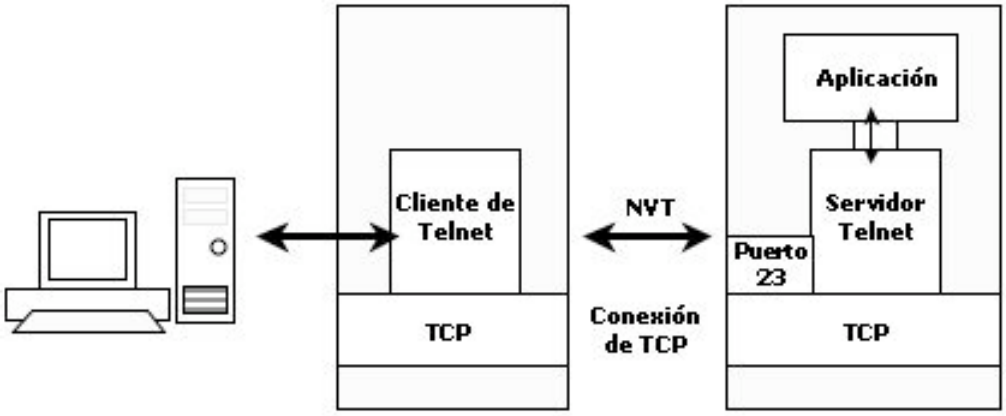


Figura 6.34 Cliente y servidor Telnet.

6.7.2 Protocolo de Transferencia de Archivos FTP

En un entorno de red, es natural que se quiera copiar archivos entre distintas computadoras. ¿Por qué a veces es tan complicado? Los fabricantes de computadoras han ideado cientos de sistemas de archivos. Estos sistemas difieren en docenas de detalles menores, ¡y también en unos cuántos detalles importantes! No es solo un problema de que haya múltiples fabricantes. A veces, es difícil copiar archivos entre dos tipos diferentes de computadoras de un mismo fabricante. Cuando se trabaja en un entorno multi-sistema pueden aparecer, entre otros, los siguientes problemas:

- Convenciones diferentes para nombrar los archivos
- Reglas diferentes para recorrer los sistemas de directorios
- Restricciones de acceso a archivos
- Formas diferentes de representar texto y datos dentro de los archivos

Los diseñadores del conjunto de protocolos de TCP/IP no trataron de crear una solución general muy complicada que resolviera cualquier problema de transferencia de archivos. En lugar de ello, crearon un Protocolo de Transferencia de Archivos (FTP – File Transfer Protocol) bastante básico, pero elegante, útil y fácil de usar.

El protocolo de transferencia de archivos se ha diseñado para su uso de forma interactiva por usuarios finales o por programas de aplicación. Aquí se limitara la explicación al servicio FTP de usuario final interactivo más familiar, disponible en todas las implementaciones de TCP/IP.

La interfaz de usuario desarrollada para el cliente de transferencia de archivos del UNIX Berkeley se ha implementado en muchos tipos de computadoras multiusuario. Las funciones esenciales de transferencia de archivos permiten a los usuarios copiar archivos de un sistema a otro, ver listados de directorios y realizar tareas normales, como cambiar de nombre o borrar archivos. Esas funciones forman parte del conjunto de protocolos normalizados de TCP/IP.

6.7.3 FTP Público y Privado

Normalmente los sistemas de computadoras piden al usuario que introduzca un ID de conexión y una contraseña para poder ver o manipular los archivos. Sin embargo, a veces es útil crear un área

pública de archivos. El FTP ofrece dos tipos de servicio para adaptarse tanto al acceso de información pública compartida como al acceso de archivos privados:

- Acceso a archivos públicos por medio de conexiones "anónimas"
- Acceso a archivos privados, restringido a usuarios que poseen un identificador de conexión al sistema y una contraseña.

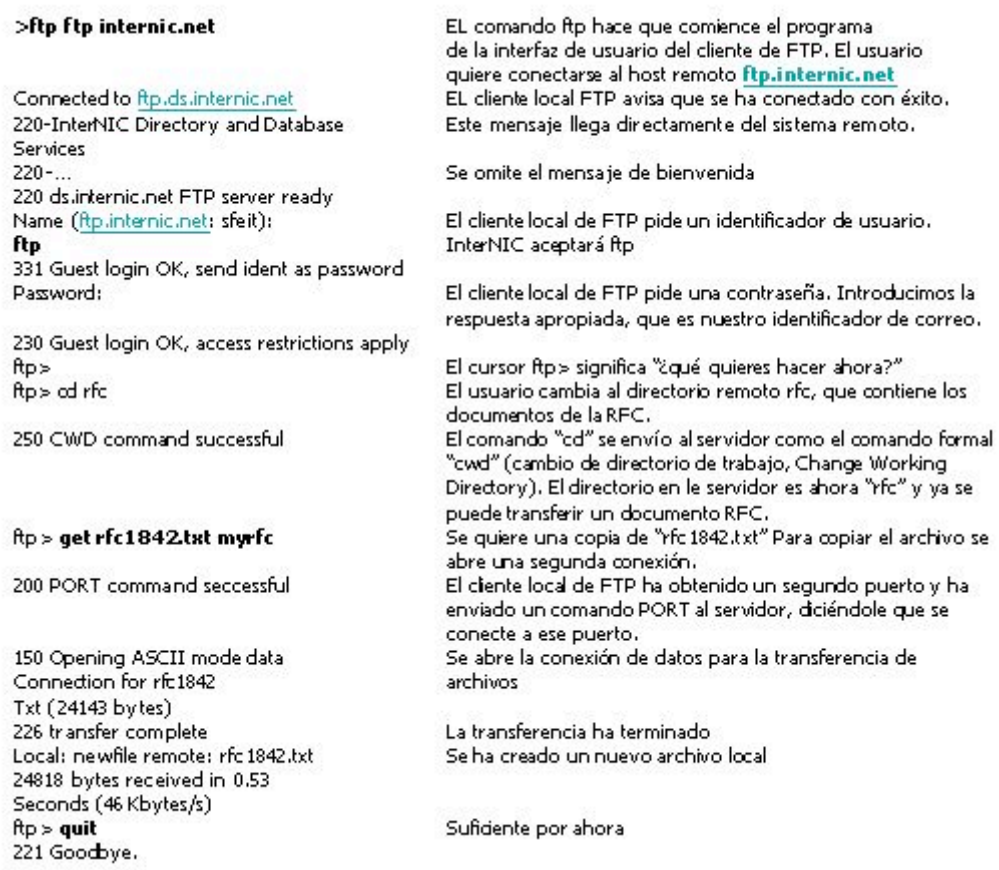
Dialogo Introductorio

El dialogo que aparece a continuación demuestra cómo se puede copiar un archivo del repositorio público de documentos de RFC, situado en el servicio de datos de InterNIC de AT&T.

Actualmente muchas personas disponen de interfaces gráficas de usuario (GUI-Graphical User Interface) para la transferencia de archivos. Sin embargo, la interfaz de texto ofrece una excelente idea de la forma real de operar del protocolo.

El registro de archivos de InterNIC es público y se puede acceder con el indicador ftp. Tradicionalmente, los sistemas públicos se configuraban para que aceptasen el identificador de acceso anonymous (anónimo). En la actualidad la mayoría acepta ftp, que es más sencillo de escribir. Los servidores de transferencia de archivos públicos esperan que se introduzca el identificador de correo electrónico como contraseña.

Cada vez que la aplicación de FTP local espera una entrada del usuario aparece el cursor ftp>. Las líneas que comienzan por números contienen mensajes del servidor de archivos remoto.



>ftp ftp internic.net	EL comando ftp hace que comience el programa de la interfaz de usuario del cliente de FTP. El usuario quiere conectarse al host remoto **ftp.internic.net**
Connected to ftp.ds.internic.net	EL cliente local FTP avisa que se ha conectado con éxito.
220-InterNIC Directory and Database Services	Este mensaje llega directamente del sistema remoto.
220-...	Se omite el mensaje de bienvenida
220 ds.internic.net FTP server ready	
Name (ftp.internic.net: sfeit):	El cliente local de FTP pide un identificador de usuario. InterNIC aceptará ftp
ftp	
331 Guest login OK, send ident as password	
Password:	El cliente local de FTP pide una contraseña. Introducimos la respuesta apropiada, que es nuestro identificador de correo.
230 Guest login OK, access restrictions apply	
ftp>	El cursor ftp> significa "¿qué quieres hacer ahora?"
ftp> cd rfc	El usuario cambia al directorio remoto rfc, que contiene los documentos de la RFC.
250 CWD command successful	El comando "cd" se envío al servidor como el comando formal "cwd" (cambio de directorio de trabajo, Change Working Directory). El directorio en le servidor es ahora "rfc" y ya se puede transferir un documento RFC.
ftp > **get rfc1842.txt myrfc**	Se quiere una copia de "rfc1842.txt" Para copiar el archivo se abre una segunda conexión.
200 PORT command seccessful	El cliente local de FTP ha obtenido un segundo puerto y ha enviado un comando PORT al servidor, diciéndole que se conecte a ese puerto.
150 Opening ASCII mode data Connection for rfc1842 Txt (24143 bytes)	Se abre la conexión de datos para la transferencia de archivos
226 transfer complete	La transferencia ha terminado
Local: newfile remote: rfc1842.txt 24818 bytes received in 0.53 Seconds (46 Kbytes/s)	Se ha creado un nuevo archivo local
ftp > **quit**	Suficiente por ahora
221 Goodbye.	

Dialogo Introductório de FTP

Con el primer comando se ha pedido al servidor que cambie al directorio "rfc". Después se ha copiado el documento remoto "rfc1842.txt" en un archivo local llamado "myrfc". Si no hubiese indicado un nombre de archivo, se le habría asignado el mismo nombre que al archivo remoto.

FTP permite escribir nombres de archivos remotos igual que lo habrían hecho los usuarios de ese host remoto. Cuando se copia un archivo a la computadora local, se le puede asignar un nombre local. Si no se hace, FTP traducirá el nombre de archivo remoto, si es necesario, a un formato aceptable por el host local. A veces esto puede originar que algunos caracteres se conviertan a mayúsculas o que halla que truncar los nombres.

El protocolo de transferencia de archivos tiene un estilo peculiar de funcionamiento. Cada vez que se necesita copiar un archivo se abre una segunda conexión para la transferencia de datos. En el dialogo precedente, después del comando "get", el cliente local de FTP consiguió un puerto adicional y le índico al servidor que abriera una conexión con ese puerto. No se vio ese comando de salida, pero si la respuesta.

200 PORT command successful

150 Opening ASCII mode data connection for rfc1842.txt (24143 bytes).

6.7.4 Modelo de FTP

Como se puede observar del diálogo anterior, un usuario interacciona con un proceso del cliente local de FTP. El software del cliente local entabla una conversación formal con el proceso del

servidor remoto de FTP a través de una conexión de control. Cuando el usuario final introduce un comando de transferencia o de gestión de archivos, el comando se traduce a uno de los acrónimos especiales de la conexión de control.

En el fondo, la conexión de control no es más que una simple sesión del NVT de telnet. El cliente envía comandos al servidor a través de la conexión de control y el servidor envía respuestas de vuelta al cliente a través de la misma.

Si el usuario pide una transferencia de archivos, se abre una conexión de datos independiente y el archivo se copia a través de dicha conexión. También se utilizan conexiones de datos para transmitir los listados de directorios. En la figura 6.35 se muestra el modelo FTP. El servidor utiliza normalmente el puerto 20 para su extremo de la conexión de datos.

Durante el diálogo de la sección anterior, el usuario final solicitó un cambio de directorio para copiar un archivo. Esta petición se convirtió en un comando formal de FTP y se envió al servidor remoto de FTP a través de la conexión de control. La transferencia del archivo se realizó por la conexión de datos independiente que se creó para tal efecto.

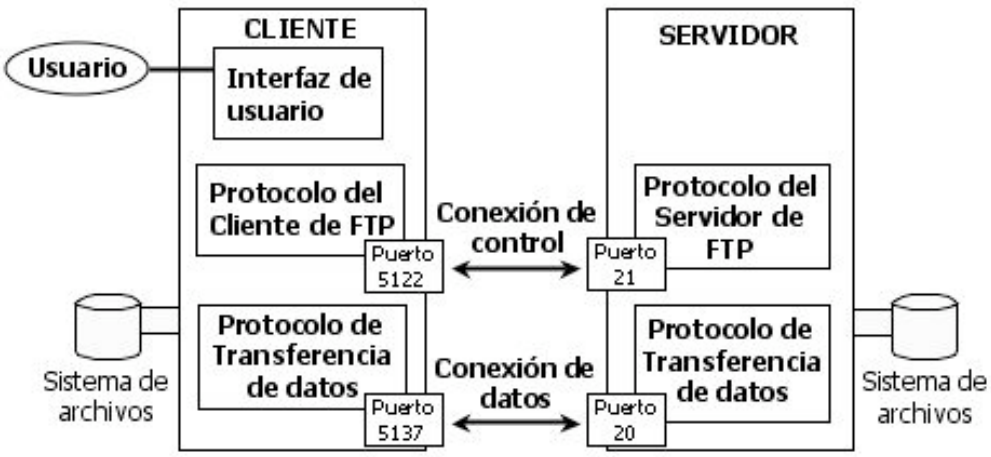


Figura 6.35 Conexiones de control y de datos de FTP.

Hay comandos de transferencia de archivos que permiten al usuario:

- Copiar un único archivo de un host a otro.
- Copiar varios archivos de un host a otro.
- Añadir un archivo local a un archivo remoto.
- Copiar un archivo y añadir un número al nombre para que sea un nombre único.

Hay comandos de control que permiten al usuario:

- Indicar si se va a transferir texto ASCII, texto EBCDIC o datos binarios.
- Establecer si el archivo está estructurado como una serie de bytes o como una secuencia de registros.
- Descubrir cómo se va a transferir el archivo, por ejemplo, como un flujo de octetos.

Los comandos que se envían a través de la conexión de control tienen un formato normalizado. Por ejemplo, el comando "RETR" se usa para copiar un archivo desde un servidor al lugar donde se encuentra el cliente.

FTP no impone restricciones al tipo de interfaz de usuario que pueda suministrar un vendedor y, como ya se ha visto, los sistemas de escritorio proporcionan ingeniosos clientes de fácil manejo. De éste modo, acciones como teclear "get", arrastrar un icono o pulsar sobre un nombre de archivo se pueden traducir a un comando "RETR".

La interfaz de usuario incluye, en general, comandos adicionales que permiten al usuario personalizar su entorno local, como:

- Pedir a FTP que emita un sonido al final de una transferencia.
- Para una interfaz de usuario de tipo texto, pedir a FTP que imprima el símbolo "#" por cada bloque de datos que se transfiera.
- Establecer la traducción automática de letras mayúsculas a minúsculas o viceversa en un nombre de archivo o crear una tabla para traducir automáticamente los caracteres de los nombres de los archivos transferidos.

Se puede obtener el conjunto completo de funciones disponibles en un host dado, por medio de la opción de ayuda del cliente de FTP.

6.8 CORREO ELECTRÓNICO

De todas la aplicaciones de TCP/IP, el correo electrónico es la que atrae la mayor cantidad de gente. Cuando una organización ofrece un buen acceso al correo, su utilización aumenta de forma explosiva. El correo atrae a usuarios que nunca pensaron que utilizarían una computadora.

El correo electrónico es una buena forma de contactar con la gente, y de fácil manejo. El dialogo que aparece a continuación muestra una interacción muy sencilla con un programa muy simple de correo de UNIX. El programa pregunta por el asunto (subject) y el usuario señala el fin del mensaje escribiendo un punto como único carácter de una línea.

> **mail fred**
Subject: Nuevos Materiales
Los manuales han llegado
Discutámoslos la siguiente semana.
.

Existen programas de correo mucho más elegantes, con interfaces de usuario de pantalla completa donde las opciones se seleccionan con un "clic" del ratón. Por ejemplo, el software "Outlook" para PC, o el software "Eudora" para Macintosh.

El nombre formal para un programa de correo de usuario final es Agente de Usuario (UA – User Agent). Se espera que un agente de usuario realice varias tareas como:

- Mostrar información de los mensajes de correo de entrada que esperan en el buzón del usuario.

- Guardar los mensajes de entrada o de salida en carpetas o en archivos locales.
- Disponer de un buen editor para componer el texto de los mensajes.

El estilo de agente de usuario que prefiere cada individuo ha sido considerado siempre una cuestión de gusto personal y no está sujeto a normalización. Lo importante es que el resultado final sea siempre el mismo, que se envíen y entreguen los mensajes de correo.

Retomando la transacción de correo anterior. Todo parece muy sencillo, pero hay gran actividad escondida entre bastidores. Resulta que "fred" es un seudónimo o alias definido en la agenda de direcciones privada. Cundo el agente de usuario hace la consulta, descubre que el identificador real del destinatario es fred@micosoft.com.

Este identificador tiene el formato típico del correo de Internet. Sin embargo, los fabricantes de software de correo electrónico propietario y los proveedores de servicio de correo han demostrado mucho individualismo al diseñar sus propios formatos de destinatario. Existen "gateways" de correo muy ocupadas realizando conversiones entre esos formatos.

¿Cómo se entrega el correo? Al comienzo, el correo se transfería a través de una conexión TCP/IP directa entre el host origen y el host destino. Pero hoy es más habitual que el correo se reenvíe por medio de uno o varios host intermedios.

6.8.1 Protocolos de Correo de Internet

El correo es muy utilizado y son muchos los protocolos de internet que se han evolucionado para satisfacer las necesidades de los usuarios de correo electrónico. En la figura 6.36 se describen los protocolos de correo de internet.

El Protocolo Simple (o único) de Transferencia de Correo (SMTP – Simple Mail Transfer Protocol) es el estándar clásico de internet para la transferencia de correo entre computadoras. SMTP se diseño para transportar sencillas notas de texto y se implemento sobre una simple sesión de terminal virtual de Telnet.

Al llegar el correo, un agente de usuario tiene que interpretar algunos elementos del mensaje, como el identificador del remitente, fecha de envío, asunto y la parte de la información del mensaje. El venerable Estándar para el Formato de Mensajes de texto en Internet de ARPA, proporciona el formato para mensajes sencillos de correo de texto de Internet.

Un conjunto más reciente de normas define las extensiones de SMTP (ESMTP), que permiten transportar cualquier tipo de información. Recientemente se han descrito los cuerpos de mensajes que constan de varias partes en las normas de extensiones de correo multipropósito de Internet (MIME – Multipurpose Internet Mail Extensions). Pueden entregarse muchos tipos de información, como documentos creados por procesadores de texto, archivos Binhex de Macintosh, imágenes, video, sonidos codificados, hojas de cálculo, código ejecutable o cualquier otra cosa. Los nuevos tipos MIME se definen según se necesitan y los registra la autoridad de asignación de números de Internet.

Se ha diseñado otro conjunto de normas adaptadas a la forma de trabajo actual de mucha gente. El Protocolo de Oficina de Correos (POP – Post Office Protocol).

Permite a un cliente obtener correo de un servidor de correo. Como alternativa, el Protocolo de Acceso a Correo de Internet (IMAP – Internet Message Access Protocol), permite que un usuario lea, copie o borre los mensajes almacenados en un servidor, pero el servidor es el depositario autorizado de los mensajes. Resulta útil para los usuarios que quieren beneficiarse de los servicios administrativos, como la copia de seguridad diaria, evitar el uso de espacio en disco local o tener acceso a su correo cuando están de viaje. El correo se entrega a un servidor por medio de SMTP o de ESMTP.
Algunas organizaciones reenvían correo por medio de los protocolos X.400 de OSI.

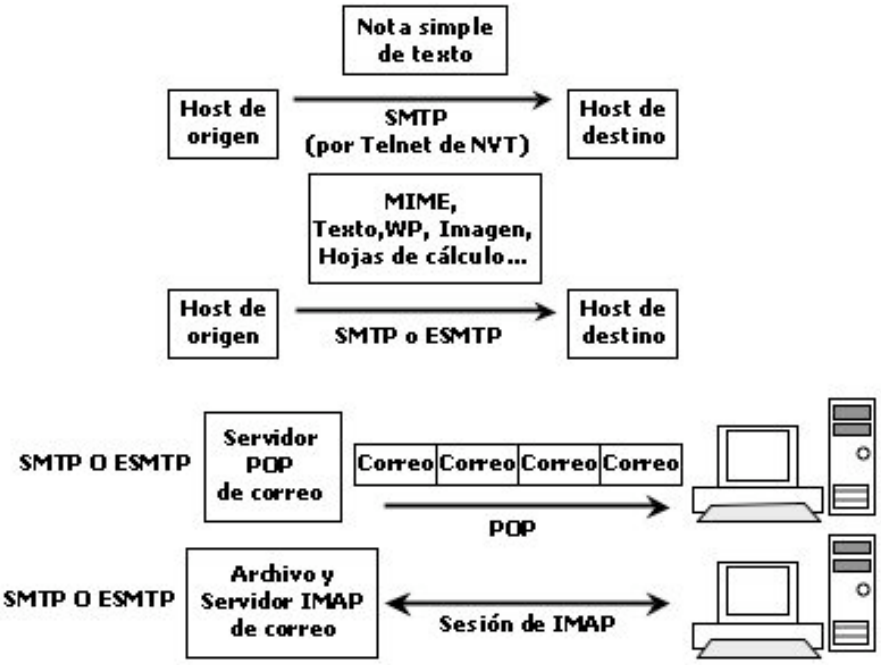


Figura 6.36 Protocolos de Correo de Internet.

6.8.2 Modelo para la Transmisión de Correo

En la figura 6.37 se muestran los elementos de un sistema de correo. El correo se prepara con la ayuda de un aplicación de agente de usuario. El agente de usuario normalmente pone el correo en la cola de otra aplicación, llamada agente de transferencia de mensajes (MTA – Message Transfer Agent), que es responsable de establecer la comunicación con el host remoto y transmitir el correo. Agente de Usuario y Agente de Transferencia de Mensajes son términos que se utilizan en las normas del sistema de mensajes de X.400, pero esos términos describen componentes válidos también para el correo de SMTP.

Se puede enviar el correo directamente entre los MTA remitentes y destinatario y reenviarse por medio de MTA intermedios. Cuando se reenvía un mensaje de correo, se transmite el mensaje completo a un host intermedio, donde se almacena hasta el momento en que se pueda reenviar. Los sistemas que utilizan reenvió se denominan sistemas de almacenamiento y envío (Store-&-Forward).

En el host de destino se coloca el correo en una cola de entrada para después transferirlo a una zona de almacenamiento de buzones de usuario. Cuando un destinatario llama a un programa de

agente de usuario, el agente de usuario suele mostrar un resumen del correo de entrada que espera en el buzón.

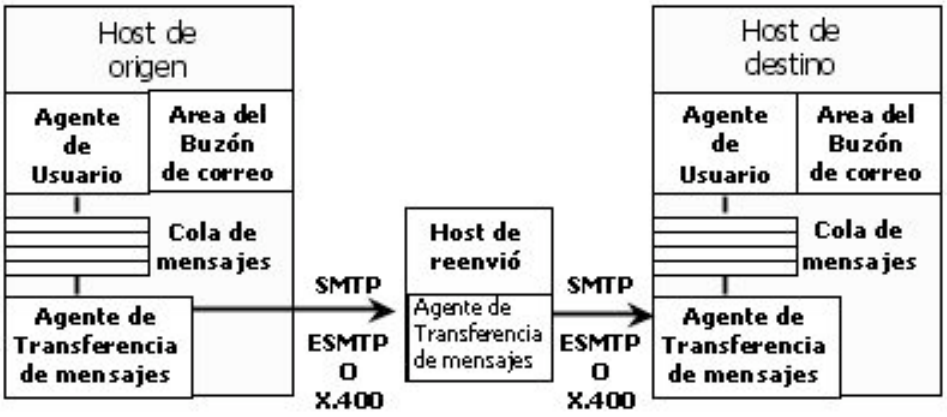


Figura 6.37 Componentes de un sistema de correo electrónico.

6.8.3 Escenario de Reenvío de Correo

Para ver por qué el estilo de almacenar y enviar está tan extendido, fíjese en el escenario que se describe en la figura 6.38. Pedro, que trabaja en la industria ABC, envía un mensaje de correo a Maria, que trabaja en computadoras JCN. La computadora de Pedro es una estación de trabajo de LAN que esta apagada casi siempre. La estación de trabajo envía y recibe correo por medio de un servidor de reenvío de la LAN.

Tanto industrias ABC como computadoras JCN están muy preocupados por la seguridad. Solamente permiten intercambio de correo con el mundo exterior a través de un host de reenvío. Intercambiador de Correo (Mail Exchanger) determinado. Ambas compañías se comunican con el mundo exterior por medio de un ruteador que bloquea todo el tráfico excepto las conexiones al puerto de correo, el 25, del intercambiador de correo de la compañía.

En la LAN de Pedro se utiliza un producto propietario de correo electrónico de LAN. En donde trabaja Maria se utilizan protocolos TCP/IP de correo electrónico.

Como se muestra en la figura 6.38, el correo se transfiere desde la computadora de Pedro a un servidor de LAN utilizando el protocolo propietario de correo. El servidor de LAN tiene software de Gateway que traduce el formato propietario de correo al formato de mensajes de Internet. Entonces se envía el correo del intercambiador de correo de ABC. Desde ahí se transmite a través de una red externa, por ejemplo, Internet, hasta el intercambiador de correo de JCN. Se reenvía de nuevo al servidor de correo electrónico de la LAN de Maria, donde se almacena hasta que Maria se conecta y recoge su correo por medio del protocolo de oficina de correos.

Este escenario muestra que el reenvío ofrece multitud de beneficios:

- Las PC y estaciones de trabajo cuentan con un sistema de servidores de LAN para enviar el correo de salida y mantener el correo electrónico de llegada.
- Los empleados de la compañía pueden utilizar el correo electrónico manteniendo la seguridad, al canalizar el correo a través de un intercambiador de correo.
- Se puede ahorrar dinero agrupando correo de reenvío en los horarios más favorables.

El reenvío de correo puede realizar traducciones de formato de correo.

6.9 SEGURIDAD DE IP

Con la necesidad de desarrollar una nueva versión de IP se creó un estimulo adicional para resolver los problemas de seguridad de TCP/IP. Los mecanismos propuestos introducen la seguridad en la capa de IP. Se han diseñado para su uso tanto con la versión 4 como con la versión 6.

Todo el mundo está de acuerdo en que se necesita la seguridad, pero ¿por qué en la capa de IP?, ¿Por qué no utilizar la capa de aplicación?. De hecho, es probable que muchas aplicaciones añadan sus propios mecanismos de seguridad. Pero en un entorno en que los fisgones pueden capturar tráfico fácilmente, usarlo todo o parte para repetirlo posteriormente falsificando sus direcciones de IP cuando lo hacen, no se puede estar seguro de que cualquier datagrama sea válido.

¿Por qué no utilizar la capa física? Se podría cifrar todo el tráfico de los enlaces. Ello resolvería los problemas de las escuchas, pero se necesitaría que todos los ruteadores descifrarán el tráfico automáticamente. En la actualidad no hay ninguna razón para confiar en los ruteadores.

Y ello no resolvería los problemas de autenticación. Podría causar graves problemas de cuello de botella en el tráfico de alta velocidad, aunque el cifrado y descifrado se realice por hardware. Más aún, todas las tarjetas de interfaz deberían ser capaces de cifrar y descifrar y ello sería muy costoso.

6.9.1 Elementos de Seguridad

Autentícación: Validación de la identidad de los usuarios, de los procesos cliente o las aplicaciones servidoras.

Integridad: Asegurar que los datos no han cambiado.

Confidencialidad: Evitar que la información sea vista por quien no debe verla.

Estrategia de Seguridad

La integración de la seguridad en IP es uno de los trabajos más espinosos que ha tenido que afrontar el Internet Engineering Task Force (IETF). La necesidad de autenticación, integridad de datos y confidencialidad es inmediata y de amplio uso. La estrategia de seguridad es:

- Promover la intercomunicación, empezar con mecanismos bien conocidos y ya implantados por la autenticación, integridad y confidencialidad.
- Diseñar un marco de seguridad que haga posible cambiar a otros mecanismos.
- Clasificación de mensajes 5 (MD5 – Message Digest 5) para la autenticación y seguridad de datos.
- Cifrado simétrico con el modo de encadenamiento de bloques de cifrado, correspondiente al estándar de cifrado de datos de Estados Unidos (CBC-DES) para la confidencialidad.

Se puede usar clave pública para la distribución de claves.

Elementos del Protocolo de Seguridad

Para permitir que un host de origen se comunique de manera segura con un host de destino, tanto el origen como el destino necesitan almacenar un conjunto de parámetros, como:

- Direcciones de Origen
- Los algoritmos de integridad y autenticación que se usan.
- El algoritmo de confidencialidad que se usa.

- Las claves secretas y cualquier otra información que necesite el algoritmo.
- El tiempo de vida de las claves.
- El límite de tiempo de vida de la asociación segura.
- El nivel de sensibilidad, por ejemplo "Sin clasificar" ó "Alto secreto".

Una asociación de seguridad se define formalmente como el conjunto de parámetros de seguridad de que dispone una comunicación en un sentido entre un origen y un destino.

- Un host de origen debería de usar un único conjunto de parámetros cuando envía datos a un destino.
- Alternativamente, un host podría tener varias asociaciones seguras que usa para enviar datos a un host de destino. La asociación elegida puede hacerse de acuerdo con el ID de usuario de origen, el rol o la sensibilidad.

A cada uno de los conjuntos de parámetros para un destino dado, se asigna un identificador numérico, denominado índice de parámetros de seguridad. Se pueden reutilizar los mismos números para distintos destinos.

Es muy probable que los conjuntos de parámetros para (destino=A, SPI=300) y (destino=B, SPI=300) sean diferentes. Es decir, los conjuntos de parámetros se localizan tanto por el destino como por el SPIc.

La cabecera de autenticación de IP y la cabecera de encapsulado de seguridad de la carga útil se usan para implementar la seguridad de las versiones 4 y 6 de IP.

6.9.2 Cabecera de Autenticación

Cuando se usa la clasificación de mensajes para la autenticación, la cabecera de autenticación sirve para un doble propósito:

- Valida al origen, ya que el origen conoce las claves secreta que se usan para calcular la clasificación del mensaje.
- Indica que los datos no han cambiado durante su transmisión.

En la figura 6.38 se muestra el formato de la cabecera de autenticación. El receptor usa el índice de parámetros de seguridad para buscar el protocolo y la clave de autenticación. El receptor usa la clave de autenticación para realizar los cálculos MD5.

El cálculo de la autenticación MD5 se realiza con todos los campos del datagrama de IP que no cambian durante la transmisión. Los campos que se modifican, como la cuenta de saltos o en la versión 6 de IP el apuntador de encaminamiento se tratan en los cálculos como si fuesen ceros. La respuesta del receptor se compara con el valor del campo Datos de autenticación. Si son diferentes, el datagrama se descarta.

Figura 6.38 Formato de la cabecera de Autenticación.

6.9.3 Modo de Transporte y Modo de Encapsulado

Ahora se vera como se implementa la confidencialidad. En la figura 6.39a se muestra el formato de un datagrama de la versión 6 de IP, cuya carga útil de la capa superior está cifrada. A éste formato se le llama modo de transporte.

En la figura 6.39b se muestra el formato de modo de encapsulado. Se cifra el datagrama completo, incluyendo todas sus cabeceras. Se añade una nueva cabecera para poder reenviar el datagrama. Se debe tener en cuenta que el encapsulado de un host a otro puede tener problemas si en la ruta entre ellos existe el filtro de un firewall. El firewall puede querer comprobar la información de las direcciones de origen y de destino y los puertos, que se encuentran ocultos dentro del mensaje cifrado.

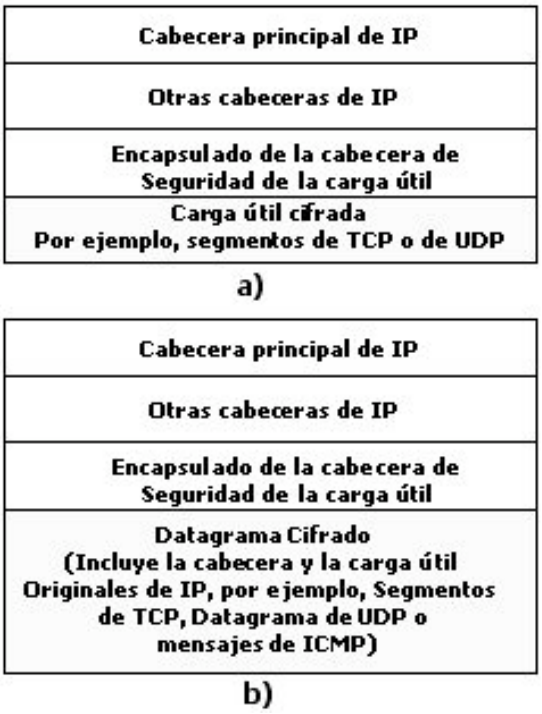


Figura 6.39 Cifrado a) en modo de transporte; b) en modo encapsulado.

Encapsulado de Seguridad de la Carga Útil

La cabecera de encapsulado de seguridad de IP de la carga útil se usa tanto para el cifrado en modo de transporte como en modo encapsulado.

En la figura 6.40a se muestra el formato de la cabecera de encapsulado de seguridad de la carga útil. El receptor usará el Índice de parámetros de seguridad para buscar el algoritmo y la(s) clave(s) que ha de utilizar. El resto de los datos depende del algoritmo elegido.

En la figura 6.40b se muestra el formato de la cabecera de encapsulado de seguridad de la carga útil y el resto del mensaje, cuando se usa el CBC-DES. El vector de inicialización es un bloque de datos necesarios para empezar el algoritmo CBC-DES, El área sombreada es transmitida cifrada. Tipo = 4 significa que la carga útil encapsula un datagrama completo (modo encapsulado).

Aunque se espera que los sistemas usen inicialmente CBC-DES, se espera que los futuros protocolos de encapsulado de seguridad de la carga útil combinen la autenticación e integridad de datos con el cifrado.

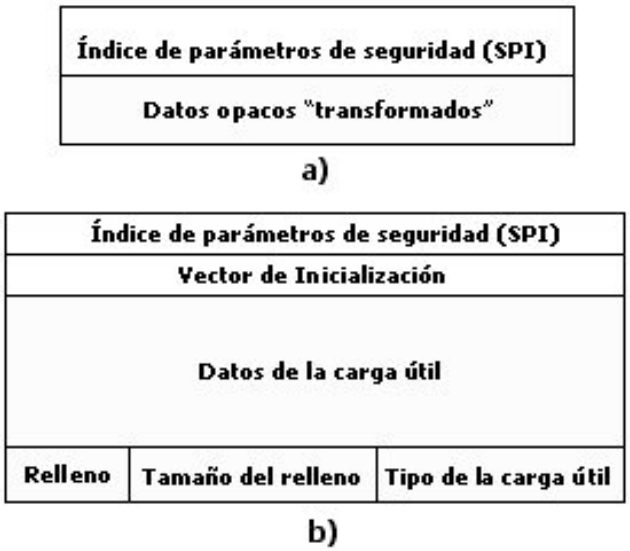


Figura 6.40 Encapsulado a) Una cabecera de encapsulado de seguridad de la carga útil; b) Cabecera y carga útil cuando se usa CBC-DES.

Uso de la Autenticación en el Modo Encapsulado

Se deberían incluir dos cabeceras separadas de autenticación cuando se usa el cifrado en el modo encapsulado entre ruteadores de frontera. Una debería ser la cabecera original del datagrama, que debería ir cifrada y oculta durante toda, o parte, de la ruta. Esta cabecera debería proporcionar autenticación extremo a extremo. La otra cabecera de autenticación debería formar parte de la cabecera de IP en abierto que se usa entre los ruteadores de frontera. Esta cabecera proporcionaría autenticación entre fronteras.

6.9.4 Administración de Claves

Como ya se ha visto, un amplio uso de la seguridad de IP requiere la distribución de muchas claves secretas a un gran número de nodos. Se necesita cambiar las claves periódicamente y hay que sincronizar la correspondencia entre claves.

La literatura sobre la administración de claves crece día a día. No existe ningún método estándar obligado de administración de claves, y se está experimentando con ello.

El uso de claves pública / privada en lugar del CBC-DES simétrico puede reducir significativamente el número de claves que hay que administrar.

CAPÍTULO 7

SERVICIOS DE MENSAJERÍA MÓVIL

7.1 MENSAJERÍA SOBRE IP (SHORT MESSAGE SERVICE - SMS)

El servicio de mensajes cortos (SMS – Short Message Service), tiene el potencial de contribuir de manera significativa con el tráfico de información que fluye día con día en una red móvil -por ende aumenta las ganancias del operador de red-. Para muchos usuarios el servicio de Mensajes Cortos puede convertirse en una parte esencial de su vida, ya sea personal o de negocios.

El servicio de Mensajería sobre IP (MoIP SMS) es un poderoso elemento de las redes móviles, que basa su éxito en el Servicio de Mensajes Cortos (SMS). Como ya se comento el MoIP SMS incrementa el tráfico en la red móvil, reduce costos de operación y mantenimiento de la red, mejora la confianza y lealtad de los clientes y da a estos mayor beneficios en sus comunicaciones personales y de negocios.

MoIP SMS no solo provee los medios para introducir el servicio de Mensajes Cortos (SMS) a la red móvil, también proporciona una confiable migración hacia aplicaciones más avanzadas, como el Servicio de Mensajería Multimedia (MMS) que se vera más adelante; por ende éste es un servicio escalable y altamente flexible, y esto es debido a que se implementa tanto con protocolos estándar como con interfaces propietarias. Este servicio puede ser adaptado a las necesidades del usuario final o del operador de la red, de tal manera que ambos puedan recibir y / o enviar mensajes cortos a y desde terminales móviles o computadoras personales.

MoIP SMS utiliza servidores UNIX comerciales, que a su vez proporcionan escalabilidad, redundancia y software de mensajería independiente. Estándares y protocolos abiertos como TCP/IP, SMTP, SMPP, TAP, CAPII y SNMP proveen la flexibilidad para manejar robustas aplicaciones y servicios de valor agregado que marcaran la diferencia en el mercado de operadores de redes móviles.

MoIP SMS cumple de manera cabal con las recomendaciones ANSI y ETSI y puede funcionar solo como una solución SMS (stand alone) o como parte de una completa e integrada solucion de mensajería IP.

Entonces ¿Qué es MoIP SMS? Es la primera aplicación para redes móviles que combina los beneficios de una red móvil con los beneficios de una red IP como internet. El servicio de Mensajes Cortos (SMS) nos servirá para enviar y recibir mensajes cortos de texto a y desde terminales móviles o entre terminales móviles y computadoras. Este servicio SMS es proporcionado por un SMS-C (Short Message Service – Center) o dicho de manera más coloquial por un servidor basado en UNIX.

7.1.1 Historia del SMS

La primera generación del servicio SMS servia principalmente para notificaciones de texto sobre nuevo correo de voz, para enviar e-mail, para servicios de información referentes a el clima, deportes, horóscopos, la broma del día, e información financiera; además los operadores de red usaban el servicio SMS para promocionar otros servicios propios de la red telefónica móvil a sus usuarios.

La segunda generación del SMS, además de los servicios antes mencionados, mejoro significativamente el tráfico en la red, y permitió el intercambio de mensajes entre redes D-AMPS, CDMA y GSM, además de agregar servicios como WAP (Wireless Aplication Protocol) y mejorar las terminales con teclados "QWERTY' como los de las maquinas de escribir o las PC.

7.1.2 Características del Servicio SMS

- Solo se puede implementar el servicio en redes móviles digitales
- Total de caracteres permitidos en las redes TDMA: 150
- Total de caracteres permitidos en las redes GSM: 160
- Por sus características de funcionamiento (solo basado en señalización) es más barato enviar un mensaje de texto que hacer una llamada de voz.
- Envío y recepción de e-mail, entre terminales móviles.
- Envío de mensajes de manera masiva, o sea, el operador de red, o incluso un usuario, puede enviar un mensaje corto a varios usuarios al mismo tiempo (broadcast).

Servicios de Telemetría, por ejemplo, un camión de carga con un equipo especial con capacidad de enviar SMS puede avisar a una central si el motor del camión esta fallando, o incluso si el camionero abre la puerta en el transcurso del camino, ya sea por robo o algún otro percance.

Alcances del SMS para TDMA 3.0

- Rango de manejo de hasta 200 mensajes por segundo con un solo SMS-C (Servidor SMS). Esto es que un solo servidor puede almacenar y entregar exitosamente hasta 200 mensajes por segundo
- Recibir y enviar mensajes desde los teléfonos móviles, así como enviar notificaciones de correo de voz.
- Activación en el aire (Over The Air (OTA) Activation) para TDMA (OAA y OATS)
- Servicios de Activación en el aire (OTA Activation) para CDMA

Alcances del SMS para TDMA 3.1

- Rango de manejo de hasta 400 mensajes por segundo con un solo SMS-C (Servidor SMS). Esto es que un solo servidor puede almacenar y entregar exitosamente hasta 400 mensajes por segundo.
- Opción Multi-carácter, esta opción permite a los usuarios elegir el lenguaje en que enviaran sus mensajes cortos. En esta versión de software de SMS se incluyeron lenguajes como el español, el chino, el portugués y el ruso.
- Bases de Datos Inteligentes para el Servicio de Roaming (IRDB – Intelligent Roaming Database). Posibilita al proveedor de servicio la habilidad de actualizar las terminales móviles con la información de nuevos acuerdos de roaming, en el aire.
- Soporte para Convertir MIN/MDN. El MDN es el número que el usuario marca para contactar a otro abonado y el MIN el número usado dentro de la PLMN para identificar al suscriptor. Para soportar la portabilidad de la numeración, los operadores se han dado cuenta de la necesidad de traducir los MIN a MDN dentro del centro de mensajes.

Alcances de SMS para CDMA TMC 3.1

- Rango de manejo de hasta 400 mensajes por segundo con un solo SMS-C (Servidor SMS). Esto es que un solo servidor puede almacenar y entregar exitosamente hasta 400 mensajes por segundo.

- Opción Multi-carácter, esta opción permite a los usuarios elegir el lenguaje en que enviaran sus mensajes cortos.
- Servicio en el Aire, (OTA - Over the Air Services), Proporciona acceso al los proveedores de servicio para bajar datos como información de roaming o directorios telefónicos.

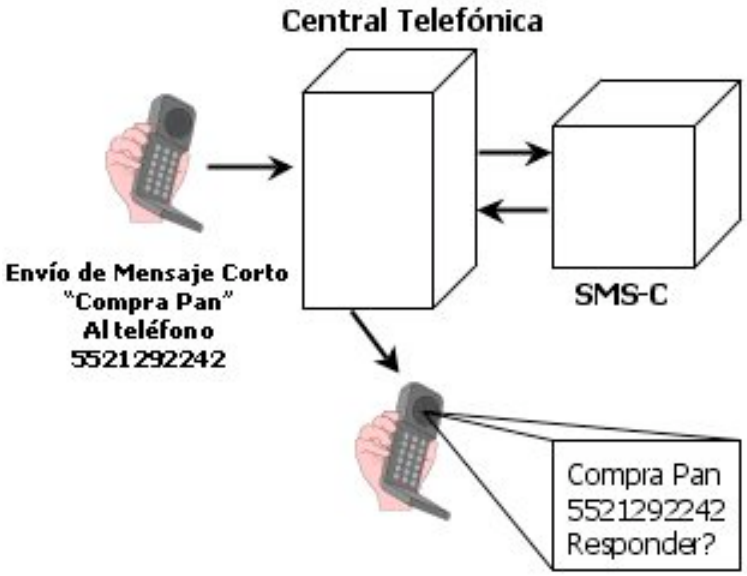


Figura 7.1 Red SMS básica.

En la figura 7.1 observamos los elementos básicos que intervienen en el funcionamiento del servicio de mensajes cortos, una central telefónica móvil, un servidor (SMS-C) con el software SMS y con un sistema operativo basado en UNIX (por ejemplo, Solaris) y las terminales involucradas en el intercambio de mensajes.

En la figura 7.2 observamos los mismos elementos de el servicio de mensajes cortos SMS, pero ahora desde la perspectiva de que una PC envía un mensaje a una terminal móvil. Cabe mencionar que el funcionamiento es prácticamente el mismo, solo que ahora se involucra además una conexión a internet y también se debe mencionar que se debe de contar con software especial en la computadora para enviar los mensajes a las terminales móviles; hoy en día existen sitios WEB desde los cuales es posible enviar los SMS, con un cargo al receptor del mensaje.

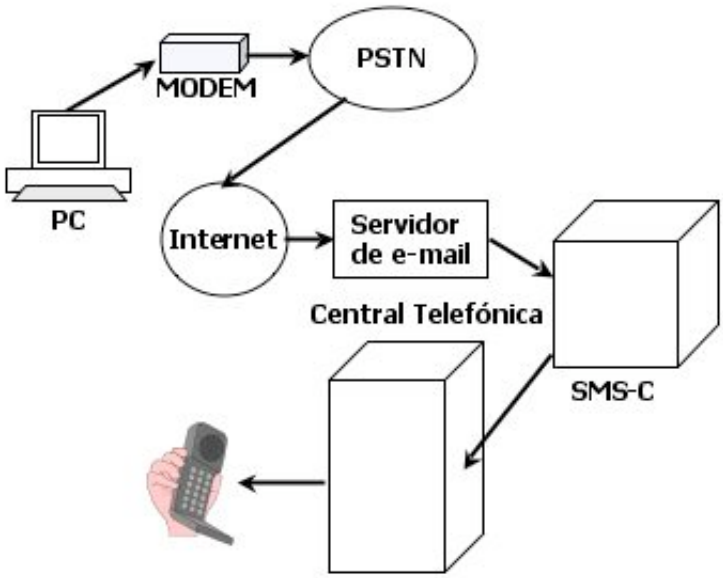


Figura 7.2 SMS enviado desde una PC.

Existen algunas otros servicios que utilizan los mensajes cortos, por ejemplo, en algunos países se proporciona el servicio de "Broadcast" de un mensaje de voz, esto es que una persona se puede comunicar a un número telefónico, y proporcionar a el personal el mensaje que quiere que se difunda a varios teléfonos suscritos al servicio, y que por ende aceptan publicidad en sus terminales, ésta opción es muy usada para anuncios comerciales por SMS.

También en algunos países la gente se puede suscribir a algunos servicios desde su terminal móvil por medio de SMS.

7.1.3 Funcionamiento del SMS

El servicio de mensajes cortos SMS es en si muy simple, y esto es gracias a que, por un lado al ser mensajes de 160 caracteres máximo, el ancho de banda requerido para el servicio no tiene que ser muy grande, y en segundo lugar porque se basa en el protocolo TCP/IP. En pocas palabras lo que éste servicio hace, es recibir un mensaje de una terminal móvil o PC, almacenarlo mientras el HLR le informa a la Central Telefónica el estatus actual de la terminal a la cual se enviara el mensaje, y en caso de que la terminal esté encendida, lo envía; una ves que la Central Telefónica le confirma que el mensaje ha sido recibido con éxito por la terminal, entonces el SMS-C lo borra. Pero analicemos con más detalle lo que sucede con un ejemplo:

Envío de SMS Móvil a Móvil

En éste ejemplo se analizara el envío de un SMS desde un terminal móvil a otro terminal móvil; suponemos que ambos terminales móviles están encendidos y configurados correctamente, por ende pueden recibir y enviar SMS.

- El propietario de la terminal A escribe el mensaje que desea enviar a la terminal B.
- Elige o teclea el número de la terminal B y ordena a la terminal enviar el mensaje corto.

- El mensaje pasa por la radiobase y por la BSC (ver apéndice A), y llega a la central telefónica, la cual al identificarlo como un SMS, lo envía al Short Message Service – Center (SMS-C).
- Una vez que la Central telefónica ya envio el mensaje corto al SMS-C, pregunta al HLR-VLR (ver apéndice A) por el estado del móvil, y en el caso de que este disponible, entonces avisa al SMS-C.
- El SMS-C recibe el mensaje corto, y hasta que es notificado de el estatus de "disponibilidad de la terminal B" por parte de la MSC, envía el mensaje corto a la central telefónica.
- La central telefónica ubica la ruta por la que el SMS será enviado, y procede a enviar el SMS, pues ya sabe que dicha terminal se encuentra disponible para recibir el SMS en ese momento.

En el segundo ejemplo se analizara el envío de un SMS también de móvil a móvil, solo que ahora se supondrá que el móvil B esta apagado.

- De la misma forma el propietario de la terminal A escribe el mensaje que desea enviar a el terminal B, confirma el número y ordena a la terminal su envío.
- La Central telefónica lo envía al SMS-C, y pregunta al HLR-VLR (ver apéndice A) por el estado del terminal B.
- En este caso particular el HLR-VLR envía el estado de no disponible a la MSC; este estado puede darse ya sea porque la terminal B este apagada, o porque se encuentre fuera del área de cobertura de la red Móvil.
- Entonces el SMS-C, al recibir un estado de "no disponibilidad de la terminal destino" del mensaje corto, por parte de la Central telefónica, lo almacena en alguno de sus discos duros, etiquetándolo con los datos de la fecha y hora en la que el mensaje fue enviado, además de los datos de la terminal que origino el mensaje, y obviamente el dato del destinatario al que deberá ser entregado en el momento en que el móvil se encuentre disponible.
- Una vez que el terminal B se encuentra disponible, el HLR-VLR (ver apéndice A) avisa a la central telefónica para que ésta revise si existe algún mensaje corto almacenado para esta terminal.
- Entonces la Central telefónica informa al SMS-C que el terminal B ya esta disponible, por lo que el SMS-C procederá a enviar el mensaje almacenado a la central telefónica, para que ésta a su vez proceda a entregar dicho mensaje corto a la terminal B; y el SMS-C no borra el mensaje hasta que no recibe la confirmación por parte de la Central Telefónica de que el mensaje ha sido entregado a la terminal B con éxito.

En realidad éste procedimiento se realiza para cada terminal que es encendida, o regresa al área de cobertura de la red celular, y el HLR-VLR (ver apéndice A) siempre informa a la central telefónica, para que ésta pregunte al SMS-C, o al Correo de Voz sobre posibles mensajes almacenados que tengan los suscriptores del servicio.

Envío de SMS de PC a Móvil

Para éste ejemplo, supondremos que el móvil esta encendido, pues en el caso de que se encuentre apagado o fuera del área de cobertura de la red Móvil, sucederá lo mismo de el caso anterior, o sea, será almacenado hasta que el terminal esté disponible.

- La persona que va a enviar el mensaje corto desde su PC, abre el software para envío de mensajes cortos, o en su caso el sitio WEB.
- Puede estar conectado a Internet por medio de MODEM, o por medio de una LAN.
- Se escribe el mensaje –que no puede exceder de 160 caracteres-, se teclea el número al cuál va a ser enviado dicho mensaje y se envía.
- En éste caso el mensaje va a viajar seguramente primero por la red telefónica pública como trama TCP/IP y después se incorporara a Internet.
- Una vez en Internet, el mensaje será enrutado a el servidor de correo electrónico pre-establecido por el proveedor de servicio de la red Móvil.
- Una vez que llega al servidor de e-mail, éste enviara el mensaje corto al SMS-C, quien lo recibirá, e informará a la central telefónica de éste mensaje.
- En este caso la central no recibe el mensaje hasta que el HLR-VLR (ver apéndice A) confirme que la terminal a la cuál va dirigido el mensaje corto esta disponible.
- Una vez que la central telefónica recibe la confirmación del HLR-VLR de que la terminal esta disponible, entonces pide al SMS-C el mensaje corto y lo envía al terminal destino, y de igual manera el SMS-C no borrará el mensaje hasta que la central telefónica confirme que dicho mensaje ha sido recibido con éxito.

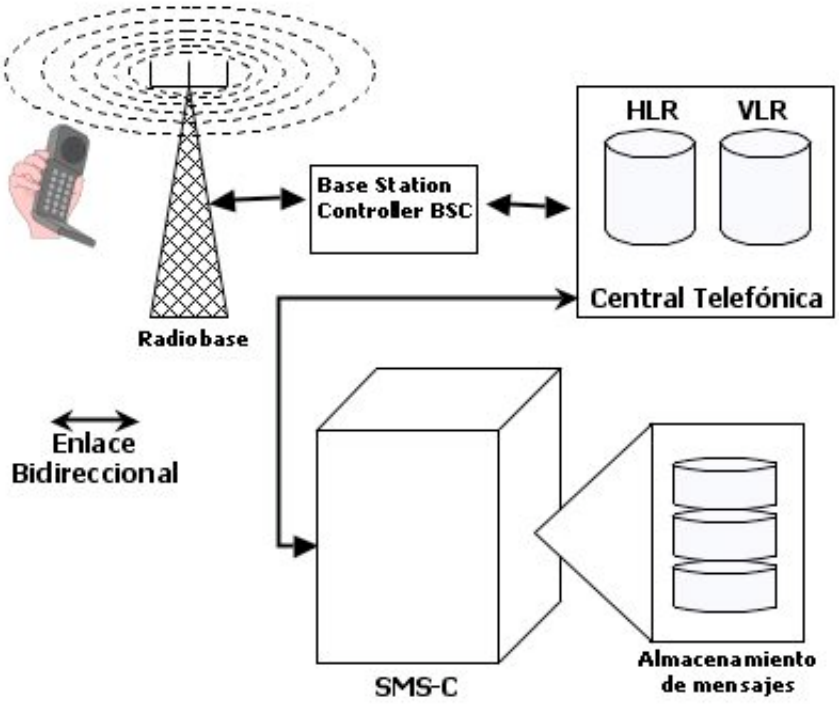


Figura 7.3 Envío, recepción y almacenaje del servicio de mensajes cortos SMS.

7.1.4 Instalación Típica de una Red SMS-C

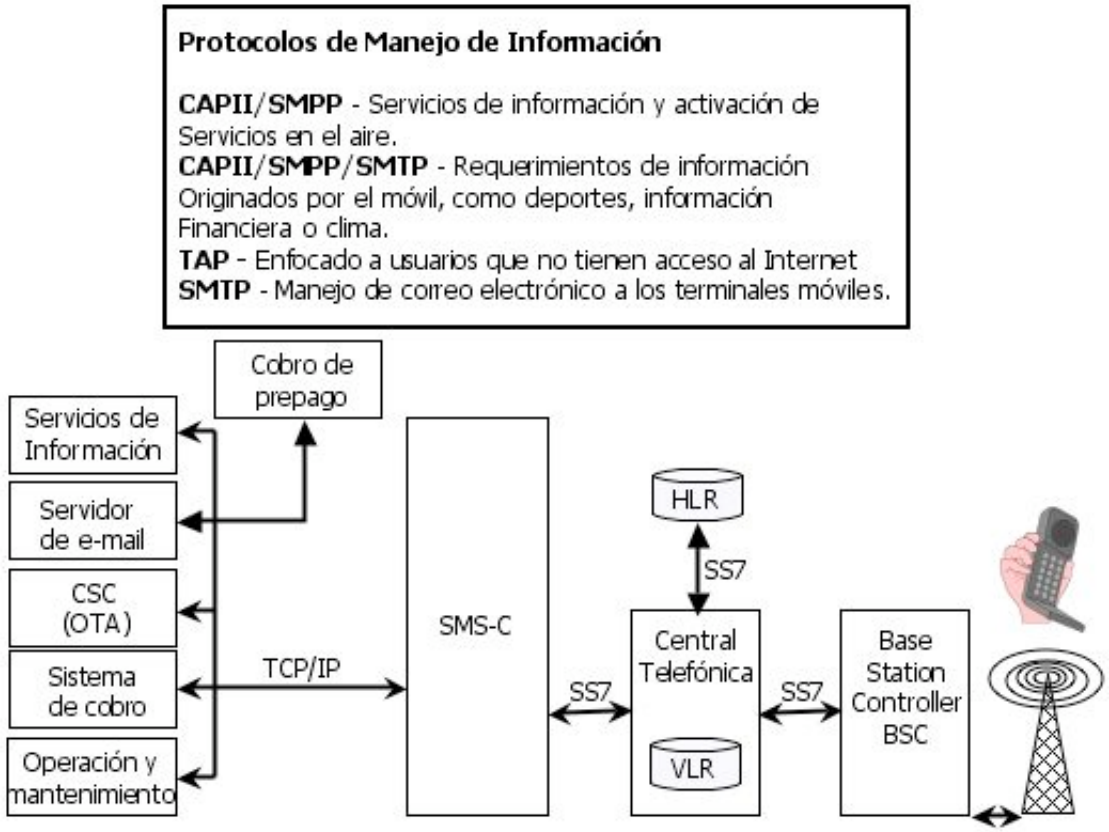


Figura 7.4 Instalación Típica de una red SMS-C.

Como se ve en la figura 7.4, el servicio SMS se comunica con la central Telefónica por medio de señalización número 7 (SS7), y en realidad en la implementación del servidor SMS-C, solo se utilizan enlaces de señalización 7; y cuando se comunica con servidores de correo y / o internet, lo hace por medio de protocolos basados en TCP/IP, de ahí se deriva que el servicio SMS es muy económico y hasta cierto punto muy sencillo de implementar. Ahora cuando hablamos de la recuperación de la inversión de éste servicio, se concluye que es un gran negocio, pues la demanda del servicio en México (Noviembre del 2005) ha sido tan elevada que se habla de varios millones de pesos cada 5 minutos solamente por el servicio de SMS.

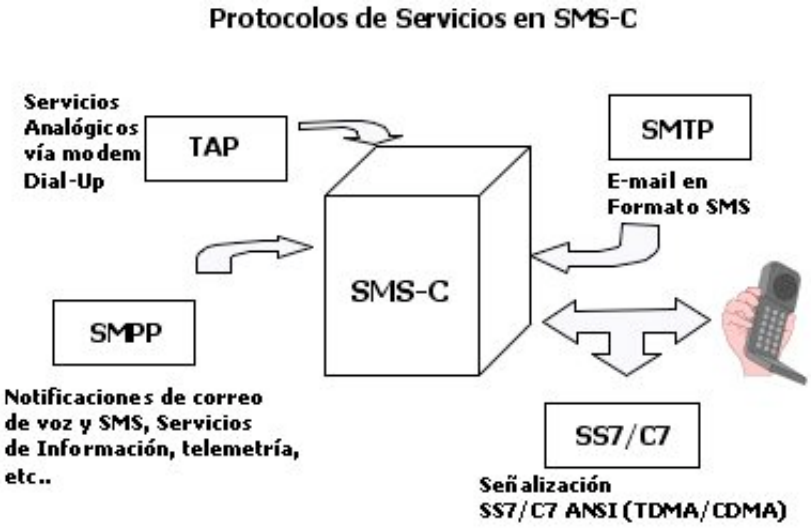


Figura 7.5 Protocolos usados en el SMS-C dependiendo el servicio que se requiera.

El software SMS puede ser instalado en varias marcas de servidores, lo que se requiere básicamente del servidor es que tenga cargada alguna versión del sistema operativo UNIX. A continuación se presentan los subsistemas principales del SMS-C, y un diagrama de bloques que muestra éstas funciones.

- Subsistema de Procesamiento Principal.- Este es el procesador del SMS-C. Soporta el arreglo de discos duros, la o las fuentes de alimentación y los demás procesadores; además provee las interfaces internas necesarias entre los subsistemas.
- Subsistema de Almacenamiento.- Consiste de varios discos duros en espejo, lo cuál asegura que todos los mensajes puedan ser enviados y recibidos incluso en caso de que alguno de éstos discos falle.
- Interfaz de Señalización SS7/C7.- Esta es una tarjeta que provee la interfaz con la red fija o móvil. Esta interfaz provee la ruta para recibir y enviar mensajes a el SMS-C; por ejemplo se pueden utilizar tarjetas ADAX y hasta 2 E1´s o T1´s por tarjeta.
- Subsistema de Operación y mantenimiento.- Provee al operador de una sencilla y fácil de usar Interfaz Grafica de Usuario (GUI – Graphical User Interface) para el control, el monitoreo y la supervisión del sistema.
- Interfaz de Conexiones Externas.- En caso de que se requiera el servidor tiene capacidad para algunos servicios más, pero para el caso del SMS no se requiere de ésta interfaz.

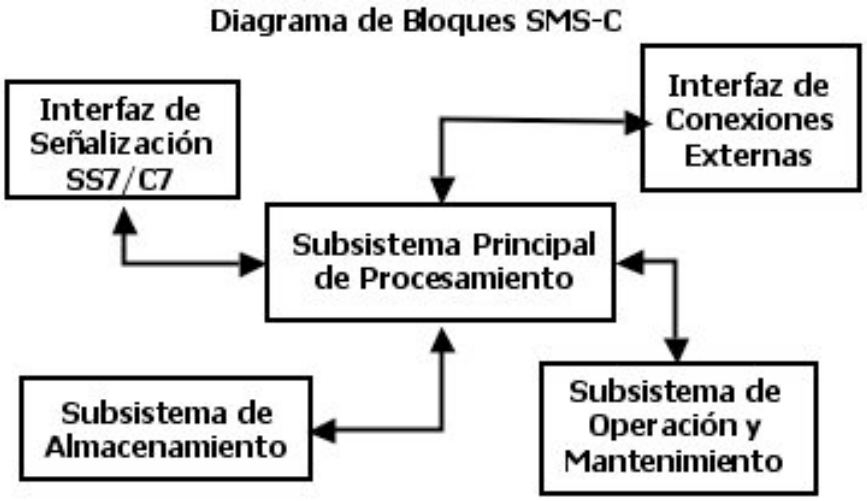


Figura 7.6 Diagrama de bloques del SMS-C.

A continuación se muestra en un diagrama de bloques en forma más detallada un SMS-C sobre una red IP.

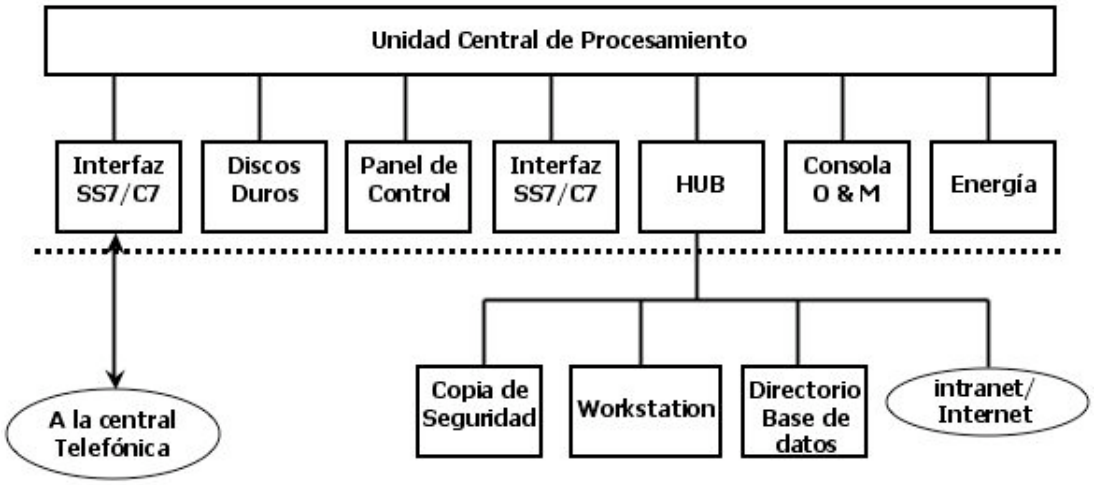


Figura 7.7 MoIP SMS-C.

La función de los discos duros es:

- Almacenar el sistema Operativo
- El software de aplicación (SMS)
- Almacenar todos los mensajes
- Almacenamiento de los archivos de configuración (*CFG Files*)

La función de la copia de seguridad es:

CD-ROM Drive

- Carga y actualización del software de Sistema Operativo.
- Carga y actualización del software de Aplicación (SMS).

DAT Drive

- Back-up y recuperación de los archivos de configuración o de los mensajes. Los mensajes son almacenados en DAT solo cuando se realiza una actualización del sistema, o cuando se cambia de servidor.

Nota: Cuando se opera el servidor de manera normal los mensajes no se almacenan en el drive DAT, sino en los discos duros del propio servidor.

La función del modulo de Energía es:

- Convierte el voltaje alterno (CA) en voltaje directo (CD)
- Provee a los diferentes módulos de voltaje (CD)
- Gracias a que el modulo de energía consta de dos fuentes, éste provee de redundancia en caso de que una fuente falle.

La función del modulo de interfaz de Red es:

- Proveer la interfaz física "a y de" la Central telefónica; tarjetas de señalización de Canal Común (CCS – Common Channel Signaling) E1 o T1 redundantes.
- Conversión serial a paralela entre el Span/Link y los discos duros.

El modulo HUB Ethernet se encarga de:

- Provee la interfaz entre la red LAN Ethernet y el CPU.
- Provee la interfaz a la Intranet o a Internet.
- Permite a otras estaciones de trabajo múltiples y simultáneos accesos al sistema.
- Usa Protocolos 10/100 baseT Ethernet y TCP/IP.

La función de administración remota se encarga de:

- Proveer la interfaz persona-maquina.
- Provee la Interfaz Gráfica de Usuario.
- Actúa como un cliente stand-alone
- Puede proveer acceso remoto al sistema vía MODEM.

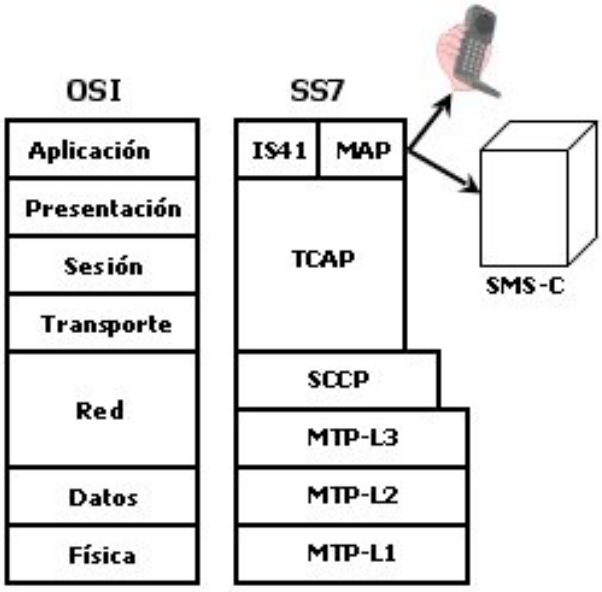


Figura 7.8 Comparación entre el las capas del modelo OSI y las capas del modelo SS7; durante el envío de texto.

7.2 Enhanced Message Service EMS

El servicio de mensajeria mejorado está basado en la plataforma SMS (Short Message Service). Este servicio habilita a las terminales móviles para enviar y recibir, además de mensajes de texto, imágenes, animaciones, efectos de sonido y sonidos de timbrado. Cabe mencionar que tanto las imágenes como las animaciones que maneja el servicio EMS no son a color.

EMS es un estándar ampliamente aceptado desarrollado para 3GPP. Los items manejados por el servicio EMS pueden ser intercambiados entre terminales móviles sin importar el modelo o marca siempre y cuando las terminales soporten el servicio EMS. Las terminales que no soporten el servicio EMS, solo recibirán la parte de texto, por lo que las imágenes o las animaciones no serán desplegadas.

7.2.1 Formatos Soportados por EMS

- Formatos de Texto.- EMS no solo soporta texto plano, como SMS, sino que también soporta texto alineado a la derecha, izquierda o al centro, además de diferentes tamaños de letra, y tipos de letra como **bold**, Underline, *italic*, y texto strikethrough. El servicio SMS es usado para finalizar el envío de EMS.
- Imágenes.- El formato EMS soporta tres formatos de imágenes: pequeñas 16x16 pixeles, largas 32x32 pixeles o incluso imágenes de tamaño variable, dependiendo de la terminal móvil, aunque el estándar recomienda un tamaño máximo de imágenes de hasta 96x64 pixeles. Múltiples imágenes pueden ser recibidas en el terminal y serán desplegadas en la pantalla de la terminal como animaciones. Las imágenes no son en color, sin escala de grises ni variaciones de tono.
- Sonidos.-El servicio EMS tiene 10 sonidos predefinidos diferentes, desde bajos y altos tonos hasta acordes como Ding, TaDa, Claps, Drum and Notify. Adicionalmente los usuarios pueden definir sonidos, que a su vez puede transferir por medio de EMS. Dentro del servicio EMS iMelody es usado como estándar para definir sonidos. Un tono del estándar iMelody es una representación melódica basada en mensaje de texto.
- Animaciones.- Las animaciones serán soportadas por el servicio EMS, en dos tamaños: 8x8 pixeles y 16x16 pixeles. Los fabricantes de terminales deberán implementar el software necesario para dar animación a dichas imágenes.

El soporte para el servicio EMS se logra al extender el largamente establecido y ampliamente usado User Data Header (UDH), común en SMS. En SMS el UDH hace posible el incluir datos binarios en un mensaje corto con mayor prioridad que el propio texto del mensaje. El servicio EMS tiene muy poco o prácticamente ningún impacto en el SMS-C. El servicio del EMS deberá ser totalmente transparente a el SMS-C, ya que también soporta el User Data Header (UDH).

Concatenación de SMS

Uniendo varios mensajes cortos será la clave para el servicio EMS por la simple razón de que implementar complejos servicios de EMS como enviar cada carácter de forma alternada en un formato de letra rellena (**Bold**) ocuparía muchos octetos en el User Data Header (UDH), por ende la concatenación es más practica y necesaria.

7.3 Multimedia Message Service MMS

La convergencia entre Internet y la telefonía móvil, esta resultando en innovaciones revolucionarias en el mercado móvil, cambiando la idea generalizada de que la telefonía móvil solo era factible para transmisión de voz; de esta forma esta convergencia hoy día representa una forma de comunicación mucho más completa que satisface el manejo de una mayor cantidad de tipos de información.

El servicio de mensajería multimedia MMS, es el siguiente paso en la evolución de servicios de mensajería. El MMS es una aplicación clave en las redes móviles con una significativa mejora en el ancho de banda, como sucede en EDGE, GPRS y UMTS. El servicio de mensajería multimedia permite a los usuarios enviar y recibir mensajes explotando la amplia gama de archivos multimedia que existen hoy en día; texto, imágenes, audio, e-mail, video; incluso esta diseñado para crecer al margen de nuevas aplicaciones futuras.

MMS no esta limitado a usarse en redes 3G (tercera generación de redes móviles). El servicio MMS tiene la capacidad de operar con una gran variedad de tecnologías (GPRS, CSD, HSCSD), dentro del estándar de redes de 2.5G (Generación 2.5 de redes móviles); obviamente esta preparado para redes UMTS de 3G. El transporte del servicio MMS es manejado de manera transparente por el protocolo WAP (Wireless Aplication Protocol). El buen funcionamiento del servicio de mensajería multimedia MMS dependerá de el ancho de banda con que cuente la red móvil. El MMS representa una solución total que consiste de la terminal habilitada para soportar MMS y del Centro de Mensajeria Multimedia (MMC), más –dependiendo del proveedor de servicio móvil- aplicaciones adicionales MMS.

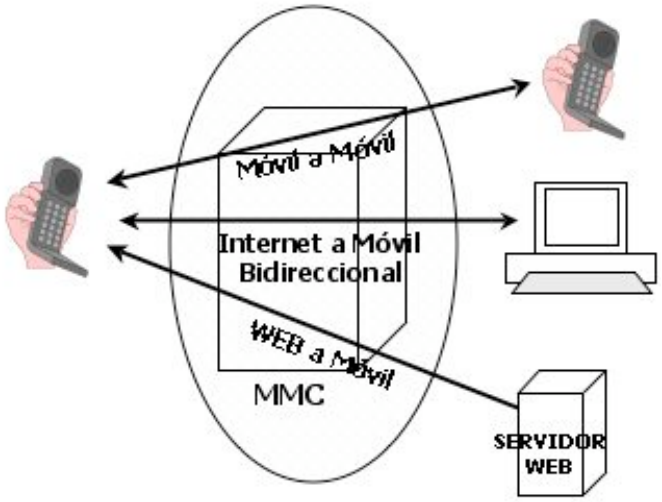


Figura 7.9 Diferentes aplicaciones MMS.

7.3.1 Características del Centro de Mensajería Multimedia MMC

El MMC es un sistema altamente flexible, que puede ser adaptado a las necesidades de los operadores de telefonía móvil, y particularmente a los usuarios finales del servicio. El MMC maneja diferentes tipos de información hacia y desde las terminales móviles, soportando un amplio rango de interfaces estándar. El uso de estándares abiertos y protocolos como SMTP y HTTP permiten al

operador servicios adicionales que dan un valor agregado al servicio, y de ésta manera ofrecer un servicio competitivo en el cambiante mundo de las telecomunicaciones de hoy.
Las principales características del MMC incluyen:

- Intercambio de mensajes multimedia de usuarios móviles, usuarios de e-mail y servidores de aplicaciones basados en internet.
- Entrega de mensajes multimedia a usuarios móviles y a sitios de Internet. La entrega a la terminal destino es iniciada vía WAP (Wireless Aplication Protocol)

El MMC ofrece también funcionalidades como el almacenamiento y envío, garantía de entrega, preferencias del suscriptor, requerimientos del operador, información del costo del servicio, etc.

Todos los componentes de la red de mensajería son diseñados para funcionar en hardware comercial y escalable. Lo cuál significa que el equipo puede ser seleccionado para satisfacer las necesidades de desempeño del operador. Esto también significa que el operador tiene la oportunidad de tomar ventaja en la creciente industria de la tecnología de la información, y de ésta manera seleccionar el mejor equipo en cuanto a desempeño / precio disponible en el mercado. Además mientras el número de usuarios del servicio MMS crece, el MMC puede ser fácilmente expandido para cumplir con las necesidades de mayor capacidad. Una óptima combinación de hardware redundante, arquitectura distribuida, Simple Network Management Protocol (SNMP), monitoreo y almacenaje de mensajes seguro, aseguran que el MMC cumplirá de forma correcta las demandas del operador.

Entrega de Mensajes Multimedia a Terminales Móviles

Los mensajes multimedia son entregados a las terminales que soportan el servicio MMS usando el siguiente procedimiento; Cabe mencionar que el procedimiento es automático y no requiere de intervención alguna por parte del usuario final. La secuencia de los eventos en la cuál se entregan los MMS es como sigue:

- El MMC notifica a la terminal móvil de un mensaje entrante.
- La terminal móvil envía un requerimiento al MMC para que le envíe el mensaje multimedia.
- El MMC envía el mensaje multimedia a la terminal móvil.

En el caso de que el primer intento de entrega falle, el mensaje quedara en una fila de espera donde se reintentara entregar de nueva cuenta y de acuerdo con una configuración de reintentos de entrega previamente hecha por el operador. Este proceso garantiza la entrega segura de los mensajes multimedia a las terminales móviles. Cabe mencionar que en éste caso el HLR / VLR y la MSC (ver apéndice A) realizan la misma labor que en el caso del SMS.

Entrega de Mensajes Multimedia a Internet

Los mensajes multimedia que van a Internet se entregan usando el protocolo SMTP. En éste caso los mensajes multimedia son enviados usando una dirección de e-mail.

Depósito de Mensajes

El MMC soporta el depósito o almacenaje de mensajes de varias fuentes: terminales móviles, usuarios de e-mail y aplicaciones multimedia basadas en Internet. Mientras recibe el mensaje en el disco duro, el MMC revisa que el mensaje sea soportado. Si el mensaje multimedia pasa la prueba

entonces se envía a la fila para su posterior entrega al destinatario. De otra manera el mensaje es rechazado y se envía una notificación de rechazo a la fuente de donde se trato de enviar el mensaje.

7.3.2 Almacenamiento y Envío de Mensajes

Una característica clave del MMC es su mecanismo de envío y almacenaje, el cual asegura que ningún mensaje será perdido. Cuando un mensaje es enviado, el MMC lo almacena en alguno de sus discos duros que se encuentran en un arreglo de espejo, antes de confirmar que el receptor recibió el mensaje correctamente. El procedimiento es prácticamente igual al del SMS, es decir, que hasta que no recibe la confirmación por parte de la terminal de que el mensaje fue recibido correctamente, no procede a borrar el mensaje de su disco duro. Y si a esto agregamos una combinación de componentes poco susceptibles a fallar, fuentes de poder redundantes y los ya mencionados arreglos en espejo de discos duros, entonces el método de almacenamiento y envío aseguran la entrega fiable de los mensajes aun en escenarios de falla, incluyendo pérdida de energía y el colapso de algún disco duro.

Direccionamiento

El MMC soporta diferentes formatos de direccionamiento para identificar al origen y al destino de un mensaje. El MMC soporta el uso de direcciones de e-mail o MSISDN para direccionar al destino de un mensaje multimedia. En el caso de direcciones de e-mail el ruteo de mensajes de internet estándar será usado. El uso de MSISDN para direccionar a un destinatario un mensaje en un MMC de otro proveedor de servicio, es posible. Por esa razón la traducción de MSISDN a una dirección ruteable ha sido identificada. El MSISDN a mapa de dominio (Domain mapping) para el MSISDN a el destinatario correcto MMC esta sobre desarrollo para posteriormente estandarizarse.

Envío a Múltiples Destinos

Esta característica habilita al usuario a enviar mensajes a múltiples usuarios o múltiples direcciones. De forma similar a el servicio de correo electrónico que se usa en internet, el servicio de mensajes multimedia contiene campos de dirección que especifican "A" (To), Copia al carbón (CC – Carbon Copy) y Copia al Carbón Ciega (BCC – Blind Carbon Copy); lo cuál permite al usuario utilizar su tiempo de manera eficiente en lugar de forzarlo a enviar el mismo mensaje de uno en uno a varios terminales destino.

Información del Servicio al Sistema de Cobro

El Centro de Servicio de Mensajes Multimedia provee de una muy completa información sobre el uso del servicio al sistema de cobro del operador de la red móvil, por medio de la tarificación; el MMC genera información para tarificar en las siguientes situaciones:

- Al recibir mensajes multimedia de un cliente MMS
- El recibir mensajes de otro proveedor del servicio MMS
- El recibir mensajes multimedia de un servicio de e-mail
- Envío de mensajes multimedia a otro proveedor de servicio MMS
- Al entregar mensajes multimedia a los clientes propios del proveedor
- Al notificar de un nuevo mensaje multimedia
- Al dar el reporte sobre los mensajes multimedia
- Al enviar mensajes multimedia a servidores de e-mail

- Si el mensaje multimedia es rechazado, no fue posible entregarlo o si ya expiro.

Directorio de Preferencias del Usuario

El directorio de preferencias de usuario contiene la configuración de preferencias de cada uno de los usuarios, y consiste de información que controla la funcionalidad y las características de la configuración del manejo de los mensajes multimedia del usuario; por ejemplo se le podría permitir o no enviar mensajes multimedia a un servidor de e-mail. Una interfaz con el equipo permite al operador manejar las preferencias del usuario, según los planes que el proveedor de servicio maneje para su red.

Directorio de Servicios del Operador

El directorio de servicios del operador contiene la configuración de las preferencias de los usuarios en general –aunque también puede ser en particular-, y consiste de información para la configuración de el tamaño de los mensajes manejados por el MMC, la cantidad de los mensajes, el tiempo de retención de los mensajes o los intervalos para reintentar el envío de los mensajes cuando por alguna razón no pueden ser recibidos por el destinatario.

Grupo de Caracteres y letras Soportado en los Mensajes Multimedia

Los mensajes multimedia pueden estar conformados por uno o más grupos de caracteres y / o tipos de letra. Para el MMC estos grupos de caracteres o tipos de letra en los mensajes multimedia son transparentes. Los grupos de caracteres y tipos de letra deberán ser soportados por las terminales multimedia.

Las terminales multimedia deberán ser capaces de soportar grupos de caracteres y tipos de letra que son ampliamente usados en las redes de datos actuales de Internet, como archivos de audio AMR y tipos de imágenes como JPEG, GIF87A, GIF89A o WBMP.

Los grupos de caracteres que generalmente son soportados por las terminales son:

- Arábico (ASMO708) ASMO-708
- Arábico ISO iso-8859-6
- Báltico (ISO) iso-8859-4
- Europeo Central (ISO) iso-8859-2
- Chino Simplificado (EUC) EUC-CN
- Chino Simplificado (GB 2312) gb2312
- Chino Simplificado (HZ) hz-gb-2312
- Chino Tradicional (Big5) big5
- Chino Tradicional (CNS) x-Chinese-CNS
- Chino Tradicional (Eten) x-Chinese-Eten
- Cyrillic (ISO) iso-8859-5
- Cyrillic (KO18-R) koi8-r
- Cyrillic (KO18-U) koi8-u
- Europa x-Europa
- Alemán (IA5) x-IA5-Alemán
- Griego (ISO) iso-8859-7

- Hebreo (ISO-Lógico) iso-8859-8-i
- Hebreo (ISO-Visual) iso-8859-8
- Japonés (EUC) euc-jp
- Japonés (JIS) iso-2022-jp
- Japonés (JIS-permite 1 byte kana) iso-2022-jp
- Japonés (Shift-JIS) shift_jis
- Japonés (JIS-permite 1 byte Kana) csISO2022JP
- Coreano (EUC) euc-kr
- Coreano (ISO) iso-2022-kr
- Latín 3 (ISO) iso 8859-3
- Latín 9 (ISO) iso-8859-15
- Noruego (IA5) x-IA5-Noruego
- Sueco
- Turco (ISO) iso-8859-9
- Unicode unicode, utf-16
- Unicode (Big-Endian) unicodeFFFE
- Unicode (UTF-7) utf-7
- Unicode (UTF-8) utf-8
- US-ASCII us-ascii
- Europeo del Este (ISO) iso-8859-1
- Europeo del Este (IA5) x-IA5

7.3.3 Configuración de la Red

EL MMC puede ser instalado en cualquier red telefónica móvil. La figura 7.10 muestra un ejemplo de cómo puede ser conectado un MMC en una red telefónica móvil.

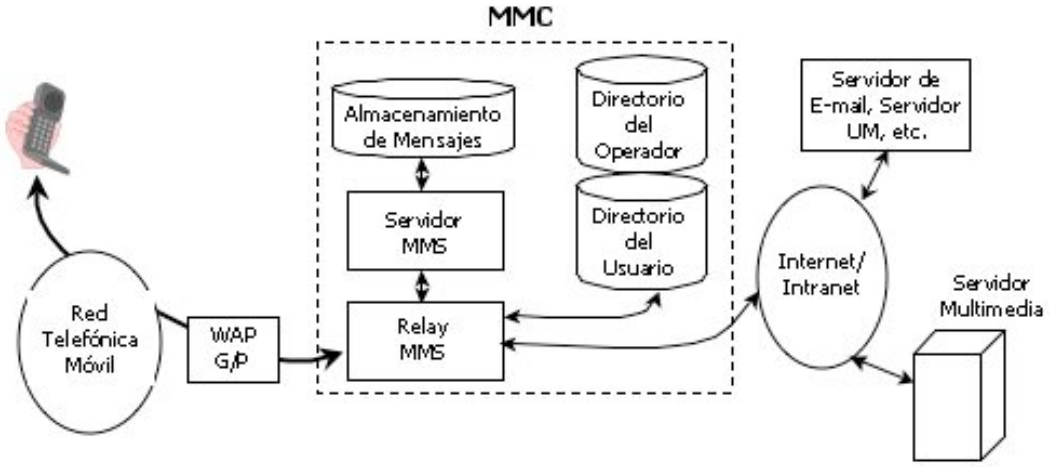


Figura 7.10 Descripción lógica de un MMC en una red telefónica móvil.

Servidor MMS

El servidor MMS provee al MMC de la maquina de procesamiento y de la aplicación de servicios multimedia. El componente del servidor MMS es responsable de la función de "Almacenamiento y re-envío" del sistema MMC.

Almacenamiento de Mensajes

El almacenamiento de mensajes como su nombre lo índica, se encarga de almacenar todos los mensajes multimedia, dándole prioridad a la entrega de los mismos en sus respectivos recipientes. Dicho almacenamiento se basa en las bases de datos Oracle® la cual esta bajo control del manejador de volumen de Veritas®.

Relay MMS

El relay MMS es el elemento que da la cara del sistema. Este componente provee la interfaz a las varias conexiones y protocolos de la red IP, permitiendo a los suscriptores acceso a los servicios de almacenamiento y envio de los mensajes multimedia.

Directorio de Usuario (Preferencias del Suscriptor)

El directorio de usuarios contiene el perfil (profiles) de todos los suscriptores. Los operadores de red son quienes generan estos perfiles (profiles), y por conveniencia, se generan al menos tres perfiles generales para diferentes planes de servicio; el servicio esta preparado también para que el usuario pueda configurar un perfil a su gusto, pero no es algo común. La integridad y disponibilidad del directorio de usuario esta protegida por cinco discos duros en arreglo de espejo.

Directorio del Operador (Servicios del Operador)

El directorio del operador provee al operador del servicio con una amigable y fácil de usar interfaz gráfica de usuario (GUI) para la configuración de los parámetros del MMS, y al igual que el directorio de usuario esta protegido por un arreglo de cinco discos duros en espejo.

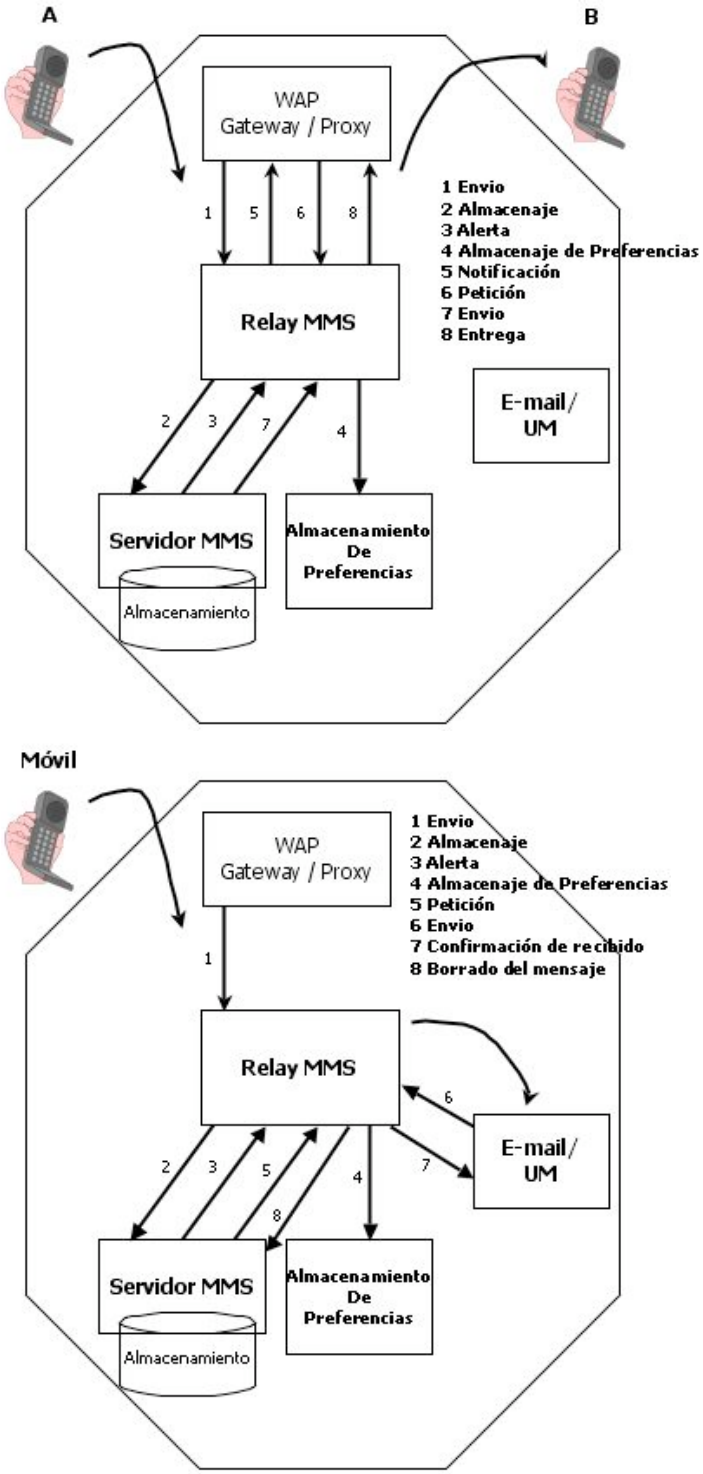


Figura 7.11 Seguimiento de llamada de MMS; de móvil a móvil y de móvil a e-mail.

7.3.4 Configuración LAN

Las interfaces entre el MMC y las computadoras que envían y de las que accede a los mensajes y aplicaciones son vía un cable UTP 100 baseT, en una red LAN TCP/IP, que provee simple y eficiente integración. La red MMC consiste de las siguientes redes internas Ethernet 100 baseT:

- LAN interna de tráfico

- LAN interna de operación y mantenimiento
- LAN primaria de operación y mantenimiento
- Consola interna de sistema

La red MMC consiste de las siguientes conexiones de red para nodos y redes externas:

- LAN externa de mantenimiento
- LAN primaria de operación y mantenimiento
- LAN de tráfico externo

Estas redes son usadas para la comunicación entre los nodos de un único MMC de dominio y los nodos funcionales externos requeridos. El punto de conexión para los nodos internos consiste de una o más redes Ethernet 100 baseT. Las redes externas pueden consistir de las siguientes redes con sus respectivas funciones:

- La red del Gateway de WAP (http)
- La red Inter e Intranet (SMTP)
- La conectividad FTP a el Gateway de cobro (Billing Gateway)
- La conectividad FTP al nodo de estadísticas (XML)
- Sistema de provisionamiento a el MMC
- Conectividad NTP a otros nodos
- La red de manejo de conectividad a la red de manejo de sistema (NMS)
- La red MMC Inter-dominio (SMTP)

Interfaces

El MMC conecta el entorno de internet con el entorno de la telefonía móvil, valiéndose de diferentes protocolos e interfaces para lograr dicha comunicación. Estas interfaces y protocolos se describen a continuación:

Interfaces WAP

Protocolo de Acceso de Empuje (Push Access Protocol - PAP)

El protocolo de acceso de empuje (PAP) es usado entre el MMC y el gateway de WAP para enviar las notificaciones concernientes a nuevos mensajes a usuarios móviles.

Protocolo de Transferencia de Hipertexto (HTTP)

El protocolo de Transferencia de Hipertexto (HTTP) es usado para depositar y entregar mensajes a los usuarios móviles entre el MMC y el gateway de WAP.

Interfaces de Mensajes Multimedia

Protocolo Simple de Transferencia de Correo (SMTP)

El Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol- SMTP) habilita a los usuarios a enviar y / o recibir mensajes multimedia a y de terminales móviles vía un sistema de e-mail de internet.

Interfaz de Operación y Mantenimiento

Protocolo Ligero de Acceso al Directorio LDAP

El protocolo Ligero de Acceso al Directorio (LDAP – Light Weight Access Protocol) es un protocolo de internet que lee y escribe a los servidores directorio. El protocolo LDPA puede ser usado para acceder la información en los servidores directorio que se encuentran fuera del sistema, asi como permitir a los directorios externos consultas en el sistema.

Protocolo Simple de Manejo de Red SNMP

La integración del SNMP (Simple Network Management Protocol – SNMP) provee compatibilidad con una gran variedad de aplicaciones funcionales de computo para operación y mantenimiento. Esto permite al proveedor de servicio administrar y mantener todos los elementos de la red móvil, incluyendo por supuesto el MMC, en una locación centralizada. En suma, esta compatibilidad permite que el MMC tenga una administración y mantenimiento desde el NOC (Network Operation Center), que es el lugar desde donde se da Operación y Mantenimiento (O&M) a los elementos IP de las redes móviles.

Protocolo RADIUS

El protocolo RADIUS provee la compatibilidad a la interfaz para aplicaciones funcionales de computo para el cobro del servicio. Esto permite al proveedor de servicio administrar y mantener todas las estadísticas y cambios de los elementos de mensajería multimedia de la red, que se encuentren centralizados en una locación. El protocolo RADIUS es usado internamente en el MMC para proveer la información necesaria para el cobro del servicio.

7.3.5 Desempeño y Capacidad del MMC

El rango de manejo de mensajes por parte del MMC se mide en el número de mensajes por segundo (mps), donde los mensajes son definidos como "mensajes multimedia" exitosamente almacenados y entregados al primer intento, por el Centro de Mensajería Multimedia (Multimedia Messaging Center – MMC).

Procesamiento de Mensajes

Basando en las condiciones que se mencionan abajo, el máximo manejo de mensajes de un sistema consistente por un solo nodo a la hora de mayor tráfico de mensajes multimedia es de 360 000 mensajes por hora, ó 50 mensajes por segundo (50 mensajes por segundo de entrada y 50 mensajes por segundo de salida de manera simultanea).

- Los mensajes fueron originados desde un usuario móvil y entregados a una terminal móvil.
- Todos los mensajes fueron entregados exitosamente en el primer intento de entrega, y por ende no fue necesario reintentar la entrega del mensaje.
- La cantidad de mensajes de entrada a el MMC y de salida desde el MMC fue igual (carga balanceada).

Los mensajes son de 50 Kbytes de tamaño.

Suscriptores

La capacidad de suscriptores es en promedio de 1.8 millones de usuarios, dependiendo el modelo de tráfico usado. Y puede almacenar un máximo de 850 000 mensajes, también dependiendo el modelo de tráfico.

Estándares y Especificaciones del MMS

El MMS ésta especificado en los forums 3GPP y WAP. Los principales estándares y especificaciones son:

- 3G TS 22.140, versión 1.2.0 (1999-11). 3 rd Generation Partnership Project. Technical Specification Group Services and System Aspects; Stage 1 Multimedia Messaging Service.
- 3G TS 23.140, versión 1.3.0. 3 rd Generation Partnership Project; Technical Specification Group Terminal; Multimedia Messaging Center (MMS); Functional Desciption Stage 2.
- WAP-205-MMS Architecture Overview; Wireless Application Protocol; MMS Architecture Overview.
- WAP-205-MMS Messaging Service; Wireless Application Protocol; MMS Service Specification.
- WAP-205MMS Encapsulation; Wireless Application Protocol; WAP Multimedia Messaging Service; Message Encapsulation.

El servicio MMS debe ser implementado en una red GSM versión R8 en adelante.

7.3.6 Gateway / Proxy WAP

El MMC requiere al menos del siguiente soporte WAP de el Gateway / Proxy: WAP de junio del 2000 (también conocido como WAP 1.2.1), WAP push, WTP-SAR Large Data Transfer.

El Gateway / Proxy WAP requiere ser conectado al SMS-C, para la entrega de las notificaciones WAP push.

Los datos antes mencionados se basan en el software MMC que comercializa la empresa Ericsson.

Módulos de Aplicación de Software

Agente de Empuje WAP

El agente de empuje WAP (WAP Push Agent) se comunica con el Gateway / Proxy de WAP para el envío y la entrega de los mensajes. Además provee codificación / decodificación de partes HTTP, corrección básica de los mensajes, etc.

Agente SMTP

El agente SMTP se encarga de la comunicación con los sistemas externos de e-mail, servidores de contenido y servidores de mensajería unificada. Convierte la cabecera SMTP a y desde cabecera MMS. El agente SMTP esta dividido en dos sub-módulos de software, el manejador SMTP y el despachador SMTP. El manejador SMTP es responsable de manejar mensajes entrantes. El despachador MSTP es responsable de procesar los mensajes de salida. El módulo de software SMTP fue dividido para el rápido procesamiento de los mensajes. También, permite que el sistema sea fácilmente escalable en cuanto a su arquitectura y también actualizado sin afectar las funciones de trabajo de otros módulos de software.

Agente de Prepago

El agente de prepago es la interfaz de comunicación con el sistema de prepago. El agente de prepago es diseñado para ser usado en base a los protocolos IP y protocolos SS7.

Conversión de Mensajes

El módulo de conversión de mensajes es responsable de la conversión del arreglo final SMIL, conversión de mensajes de contenido, conversiones de tipo multimedia, conversión de formato, codificación de caracteres alfa-numéricos y adecuación del tamaño de imágenes.

Maquina de Estado Real

La maquina de estado real (Real State Machine) es la autoridad de decisiones centrales en lo que a disposición de mensajes se refiere. En escenarios de prepago, por ejemplo, realiza las verificaciones de los datos que se envían al sistema de prepago. Esta verificación se realiza primordialmente en lo referente al almacenaje del lado del operador y en lo referente a las notificaciones del lado de la terminal. En suma, ejecuta el regreso de crédito a la terminales para los casos de mensajes no entregados y genera CDR´s.

Configuración de la Base de Datos del Operador

Permite control total sobre el manejo de la información por parte del operador. Permite gran funcionalidad a las necesidades del operador.

Ruteo de Mensaje

El ruteo de mensaje realiza todas las decisiones de ruteo, incluyendo el ruteo de mensajes fuera del Home Relay. La búsqueda de un suscriptor en la base de datos determina el ruteo de mensaje.

El manejador de Licencia

El módulo manejador de licencia administra la capacidad de manejo de mensajes, la capacidad de almacenamiento y el número de suscriptores en la base de datos.

Contexto de Mensaje

El módulo de contexto de mensaje contienen la información de cabecera de los mensajes. Es usado para toda la información referente a notificaciones, provee los URI a la maquina servidora de estado con el contenido del contexto de mensaje. Esta información es utilizada para el desarrollo de estadísticas, logs, etc.

Maquina Servidora de Estado

La maquina servidora de estado (Server State Machine) es responsable de el seguro almacenamiento de los mensajes. También envía los mensajes al lugar correcto de almacenaje. Ejecuta un único estado en múltiples recipientes de entrega, como mensajes con CC (Carbon Copy) y BCC (Blind Carbon Copy). En suma, es responsable de obtener los mensajes requeridos, responsable de correlacionar todos los mensajes "a y de" un suscriptor en particular, decisiones de reintento y expiración de mensajes, además inicia las entregas que deben hacerse en el momento o en el futuro y es utilizada en almacenaje (backup) y restauración de los mensajes.

7.3.7 Seguimiento de Mensaje Multimedia

A diferencia de los mensajes cortos que requieren de un ancho de banda muy pequeño, los Mensajes Multimedia requieren de un ancho de banda mucho más grande, por lo que es necesario que sean canalizados por una red de datos ya sea dentro de la red de circuitos conmutados (CSD y HSCSD), o por medio de una red de paquetes conmutados (GPRS); el canalizar un MMS por una red de circuitos conmutados tiene como inconveniente que cada que se quiera enviar o recibir un MMS será necesario hacer una llamada para, primero, establecer el camino de datos, y segundo poder enviar o recibir el MMS.

La otra opción para canalizar un MMS es por medio de una red de paquetes conmutados (GPRS), en este caso, el usuario estará conectado de manera permanente al servicio de paquetes conmutados, por lo que el envio o recepción de un MMS no requerirá de realizar ninguna llamada adicional.

A continuación se describirán dos casos: el primero es el envio de un MMS desde una terminal móvil hacia otra terminal móvil; y el segundo será el envio de un MMS desde una computadora hacia una Terminal móvil; se da por hecho que las terminales están encendidas y correctamente configuradas para el envio de mensajes multimedia, además de que cuentan con las categorías para el envió de MMS, la PC esta conectada a internet y en una página desde donde es posible enviar mensajes multimedia; y por último que existe una red GPRS implementada y funcionando correctamente.

1. Una vez que el mensaje multimedia está listo en la terminal 1 para ser enviado a la terminal 2, se procederá a presionar la tecla adecuada para su envio desde la terminal 1.

2. Una vez que la red detecta que se intenta enviar un MMS automáticamente direcciona dicho MMS a la red de datos GPRS, por medio de la cual viaja el mensaje multimedia para su entrega en el Servidor de Mensajes Multimedia.

3. Una vez que el mensaje ha sido recibido por el servidor MMS, procede a avisar al SMS-C para que éste a su vez envíe un mensaje corto a la Terminal 2 informándole que tiene un MMS esperando a ser aceptado.

4. Si la terminal 2 acepta el MMS, entonces el SMS-C informa al servidor MMS para que este envíe el MMS a la terminal 2 por medio de la red GPRS. Ahora, quien se encargara de ubicar físicamente a la terminal 2 será la red GPRS, que es la que tiene contacto con la central telefónica y por ende con el VLR (ver apéndice A).

5. En el caso de que la terminal rechace el mensaje multimedia o la terminal se encuentre fuera del área de servicio, entonces el servidor de mensajes multimedia lo almacenara hasta que lo logre enviar exitosamente, o si llegara a pasar más tiempo del seleccionado por el proveedor de servicio para mantener los mensajes almacenados, entonces el servidor de mensajes multimedia borrara dicho mensaje.

Envío de un MMS de una PC a un Móvil

1. Se accede a la página WEB desde la cuál es posible el envío de mensajes multimedia, se realiza el mensaje y/o se adjunta el archivo a enviar y se envía el mensaje; generalmente son páginas WEB que o son de los proveedores de servicio móvil, o tienen algún convenio con las mismas, por lo

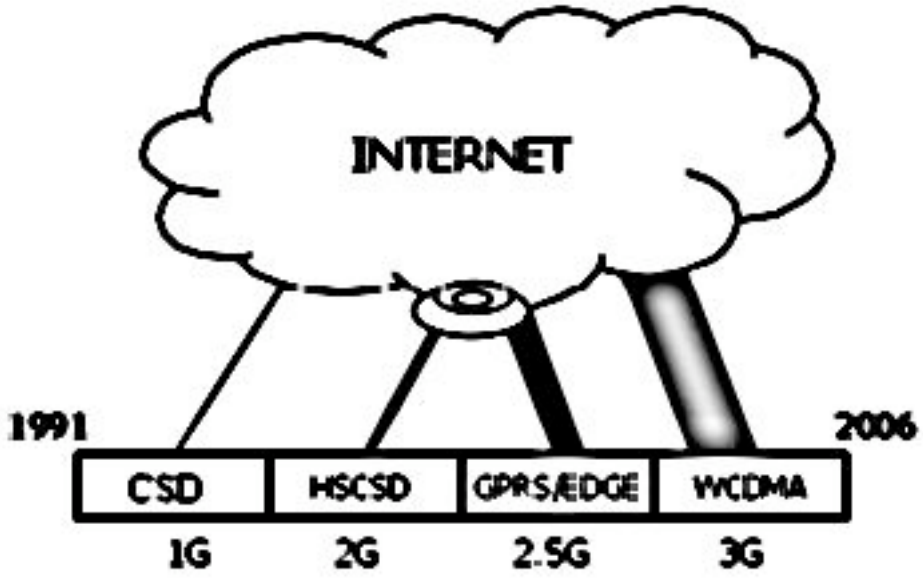
que ya tienen las direcciones IP de los servidores de red de los proveedores de servicio móvil, quienes desde su red re-direccionan el mensaje multimedia al servidor MMS.

2. Una vez que el mensaje multimedia ha llegado al servidor MMS, entonces se realizan los pasos 3 a 5 del procedimiento de envío entre terminales móviles.

SEGUIMIENTO DE LLAMADA MMS

CAPÍTULO 8

SERVICIOS DE INTERNET MÓVIL



SERVICIOS DE INTERNET MOVIL

A finales de los 80 y durante la década de los 90 se observo el desarrollo de Internet como una red pública de comunicación de datos a nivel global, alcanzando un mayor impacto con la introducción de la World Wide Web a principios de la década de los 90. El rápido crecimiento del mercado de las computadoras personales y los nuevos alcances de las tecnologías de MODEM creo un mercado de masas para los servicios en línea Dial-up, lo que vio el nacimiento de los Proveedores de Servicios de Internet (ISP´s – Internet Service Providers). Internet es ahora un fenómeno realmente global, respaldado por una gran expectación y un gran avance tecnológico. El desarrollo de Internet ha continuado a un paso tal que se ha duplicado en tamaño desde 1997 en términos de número de host, usuarios, dominios, etc.

La práctica de conectar sistemas de cómputo vía conexiones Dial-up sobre la red telefónica pública ha sido usada por décadas. El rápido desarrollo dentro del campo de las comunicaciones de datos para circuitos conmutados y acceso a Internet ha conducido a redes de mayor desempeño y capacidad, pero también al fácil uso y manejo de dichas redes. Soluciones de sistemas sostenibles y protocolos estándar han sido desarrollados para el crecimiento global de la red.

Desde la perspectiva de un Operador de Telecomunicaciones el acceso a intranets o a Internet genero un problema de red: La red de Circuitos Conmutados. Velocidad y aplicaciones de software fueron dramáticamente improvisados, pero la comunicación esencial de datos permanece siendo manejada como llamadas de voz en la red telefónica.

La red telefónica pública no fue dimensionada ni optimizada para lo que el tráfico de datos significa. La comunicación de datos es transportada por redes orientadas a conexión (Circuitos Conmutados), pero dicha comunicación es mejor manejada por redes de paquetes conmutados. En cuanto se decrementa el tráfico de datos, los efectos de los tiempos de espera en las conexiones Dial-up pueden ser descuidados. Sin embargo, con el acceso vía Dial-up, como mercado masivo, los efectos sobre la red de telecomunicaciones son claramente vistos. Redes de Telecomunicación en buen estado están bien preparadas para manejar el incremento en la capacidad de transporte, pero resulta obvio que la infraestructura total de centrales telefónicas y redes de transporte pueden ser usadas de una manera más eficiente, en Inter-operación con redes nuevas o ya existentes de paquetes conmutados.

8.1 Comunicación de Datos por Circuitos Conmutados (Circuit Switch Data – CSD)

Circuit Switch Data, como su nombre lo índica es un servicio de datos que funciona en redes de circuitos conmutados, lo que quiere decir que los datos viajaran por redes telefónicas, y por ende usaran para las conexiones de datos circuitos diseñados específicamente para manejar llamadas de voz. Estas redes dentro de la telefonía fija han sido y son hasta la fecha muy usadas por la gran mayoría de la gente que requiere servicios de comunicación de datos e Internet; pero no se han limitado a las redes de telefonía fija, también han sido desarrolladas para las redes de telefonía móvil, y eso es lo que a continuación se intentara explicar en lo relativo a su estructura y funcionamiento.

8.1.1 Elementos de CSD en una Red Móvil

Para que una central telefónica móvil pueda manejar llamadas de datos por medio del servicio CSD es necesario que contenga los siguientes elementos de hardware:

- Tarjeta de manejo de Señalización (RPG2E): Esta tarjeta es hardware adicional que se agrega a la central telefónica (si no cuenta con ella), y se encarga de intercambiar toda la información necesaria para establecer la llamada de datos, con el equipo de ruteo por medio de señalización.
- Data Transmisión Internetworking DTI: Este es también hardware que se debe agregar (si es que no existe) a la central telefónica, y su función principal es manejar los parámetros de velocidad de conexión, tipo de conexión de datos (analógica o digital) y tipo de llamada de datos (sincrona o asíncrona); ademas el DTI se conecta por medio de enlaces E1 con el ruteador; se debe crear una ruta en la central telefónica para que las llamadas de datos sean direccionadas a éste elemento de la red.
- Ruteador: El propósito fundamental de un ruteador es al igual que en otras redes el dar a las llamadas de datos salida a los servicios WEB, FTP, Telnet, etc.; y en éste caso se agrega el servicio WAP.
- Gateway de WAP: El gateway de WAP es un servidor que se encarga de dar acceso a las terminales móviles a páginas especialmente hechas bajo el protocolo WAP, que pueden ser vistas en las pequeñas pantallas de las terminales móviles. Además, en el gateway de WAP se deben de dar de alta los números de abonado de los usuarios móviles para que éstos tengan acceso a los servicios de páginas WAP.
- Servidor de Autenticación (RADIUS): Este servidor es en el que se validaran las cuentas del servicio de datos, pues como es bien sabido para que un usuario tenga acceso a Internet, necesita una cuenta que contenga "el nombre de usuario" y el "password".

8.1.2 Descripción de Servicios en CSD

En CSD existen varios tipos de servicios de datos, y a continuación se describen algunos de ellos.

- Conexión de datos entre computadoras: CSD permite que se conecten dos computadoras usando las terminales móviles como MODEM (se debe cargar el driver de la terminal móvil en la computadora para que ésta pueda emular un FAX/MODEM), e intercambien datos por medio de aplicaciones de software como Hyperterminal®; en éste tipo de llamada solo se utiliza el DTI para el establecimiento de la misma. En el caso de Hyperterminal®, se utilizan comandos "AT" para establecer la comunicación y posteriormente se puede emplear el intercambio de archivos entre las dos computadoras vía Hyperterminal®.
- Llamadas de Fax: CSD también permite el intercambio de Fax (se debe cargar el driver de la terminal móvil en la computadora para que ésta pueda emular un FAX/MODEM), puede enviar Fax entre computadoras usando terminales móviles (siempre y cuando existan

software de Fax en las mismas), de terminal Móvil a Fax fijo y de Fax fijo a terminal Móvil; en éste caso de igual manera que en el anterior caso solo se ocupa el DTI.

- Llamadas WEB: En éste tipo de llamada se utiliza la terminal móvil conectada por medio de un cable o del puerto infrarrojo a la computadora, (se debe cargar el driver de la terminal móvil en la computadora para que ésta pueda emular un FAX/MODEM) el siguiente paso es configurar en la computadora una conexión "Dial-up" con el numero de teléfono al cuál se debe marcar, seleccionar el driver de la terminal como MODEM, además de el nombre de usuario y el password; una vez que se establece la llamada se puede hacer uso de el browser de la computadora para navegar en internet, o se pueden hacer conexiones vía FTP. Por supuesto también se puede consultar el correo electrónico, o hacer conexiones Peer-to-Peer. En éste tipo de llamada ya se involucra al ruteador, al RADIUS y el DTI.
- Llamadas WAP: El protocolo Wireless Aplication Protocol es un protocolo específicamente diseñado para que permita que se vean páginas de internet (como yahoo o google) en las terminales móviles, claro que las páginas deben estar en WAP y no en HTML. En éste tipo de llamada se involucran al ruteador, al servidor de autenticación, al gateway de WAP y por supuesto al DTI.

El servicio CSD maneja velocidades de conexión de 2400 bps, 4800 bps y 9600 bps.

Cabe mencionar que tanto al ruteador como al Gateway de WAP y al servidor de autenticación, se les asignan direcciones IP, por lo que no es necesario que exista una conexión física entre estos tres elementos para que se comuniquen.

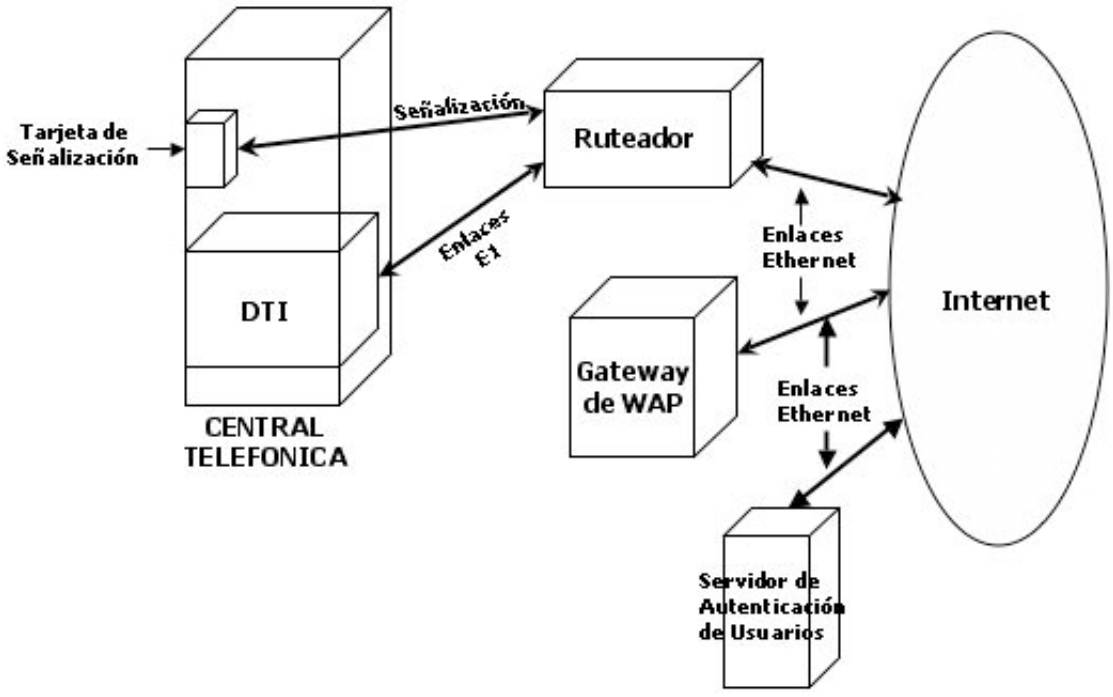


Figura 8.1 Conexión y elementos del servicio CSD.

Lo que se menciono anteriormente es muy importante, debido a que en el caso del DTI, el ruteador y la tarjeta de señalización es necesaria la instalación de éste trío de elementos en cada

central telefónica móvil, y en el caso del servidor de autenticación (RADIUS) y el gateway de WAP, no es necesario que se instalen en cada central telefónica, de hecho varias centrales telefónicas habilitadas para el servicio CSD, pueden trabajar con un solo servidor de autenticación (RADIUS) y un gateway de WAP. También es necesario señalar que al ruteador, al servidor de autenticación (RADIUS) y al gateway de WAP se les asignan direcciones IP independientes para su funcionamiento dentro de la red, por lo que no necesitan estar en lugares cercanos, o en una sola intranet.

También es importante mencionar que para que una terminal móvil pueda proporcionar el servicio CSD, su SIM Card (Suscriber Identity Module) debe contar con las categorías en el HLR correspondientes a dicho servicio, además de que –como se menciono anteriormente- para que puedan acceder al servicio WAP, los números de abonado de los usuarios deben ser dados de alta en el gateway de WAP, de otra manera aunque tengan las categorías en el HLR y se encuentren bien configuradas no podrán acceder a dicho servicio.

8.1.3 Seguimiento de una Llamada de Datos en CSD

Para éste ejemplo se va a analizar una llamada de CSD solicitando el servicio WEB utilizando una terminal móvil como MODEM; se da por hecho que en la PC se ha cargado el driver de FAX / MODEM de la terminal, y se ha configurado un "Dial-up" correctamente, además de que la tarjeta SIM de la terminal tiene asignadas las categorías de CSD en el HLR y que la terminal esta encendida.

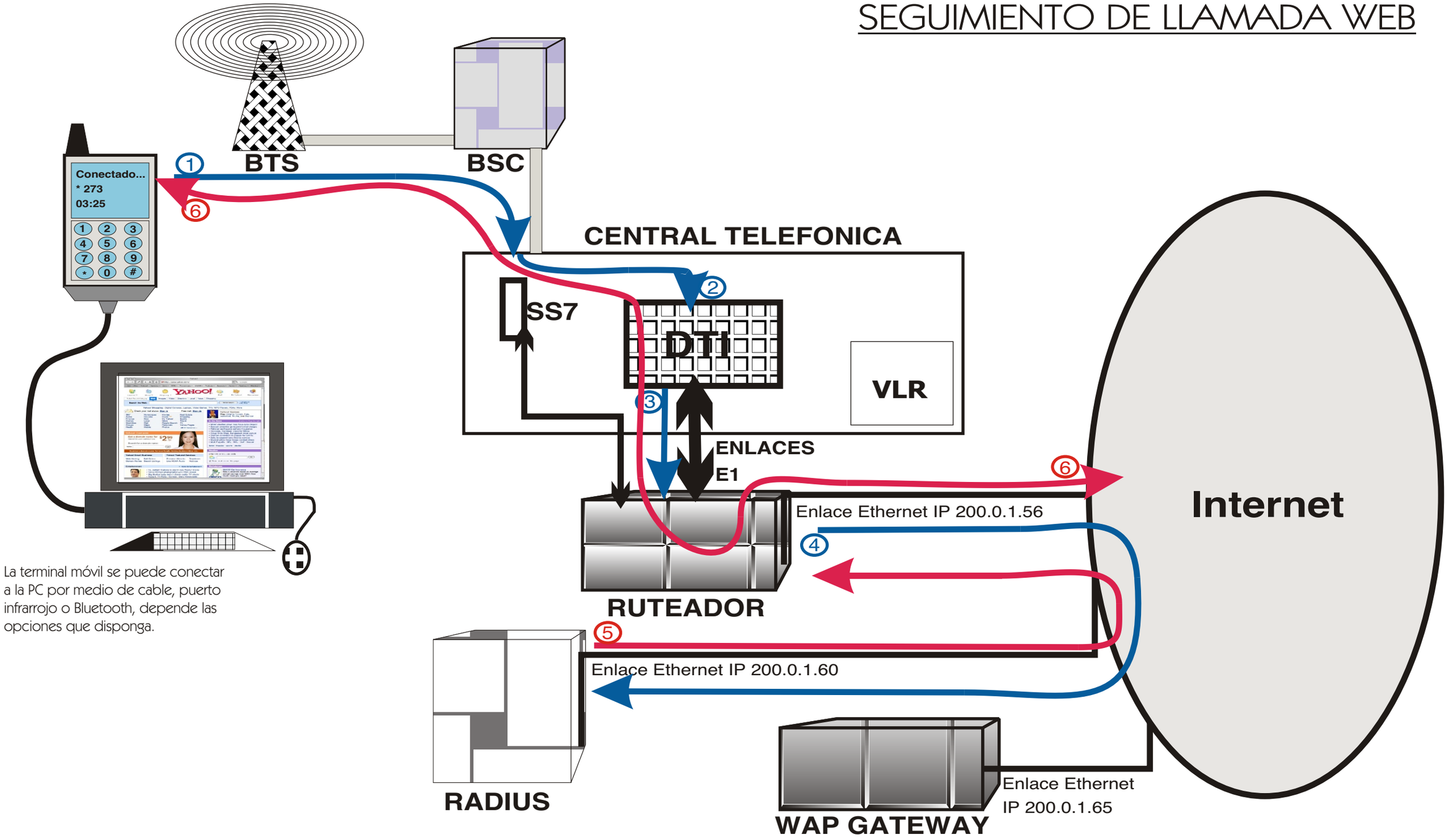
1. Se inicia el proceso de conexión, la terminal móvil marca el número preconfigurado en el "Dial up" para acceso a CSD.
2. La central telefónica analiza el número que fue marcado por la terminal móvil y lo identifica como llamada de datos del servicio CSD, y procede a enrutarla al DTI.
3. En el DTI, se le asigna velocidad de transmisión, tipo de llamada y tipo de conexión, y se envía al ruteador. Por señalización el DTI y el ruteador se comunican y realizan el Handshaking y se procede al siguiente paso.
4. En el ruteador, se recibe la llamada y se desempaqueta la información, recibiendo primero la información de Identificación de Usuario y password; ésta información es enviada al servidor de autenticación (RADIUS) por medio de un enlace Ethernet.
5. Si la información de Identificación de usuario es correcta el servidor de autenticación "Valida" al usuario, se avisa entonces al ruteador y se procede al siguiente paso.
6. Una vez que el usuario es "Validado", entonces se avisa al ruteador, y se procede a establecer el circuito de datos entre el ruteador y la red celular; en éste momento ya es posible abrir páginas WEB, FTP, o correo electrónico.

En el caso de que el usuario no sea "Validado" por el servidor de autenticación, entonces el ruteador avisara al DTI de la falla en la autenticación del usuario, enviando al mismo el aviso de que el password o el nombre de usuario fue incorrecto, e inmediatamente después de que se recibió el mensaje por parte del usuario, la central telefónica termina la llamada y envía el mensaje de error por señalización.

Para el caso de una llamada que solicite el servicio WAP, el procedimiento es exactamente el mismo que para una llamada WEB, solo que en éste caso el gateway de WAP, a solicitud del ruteador,

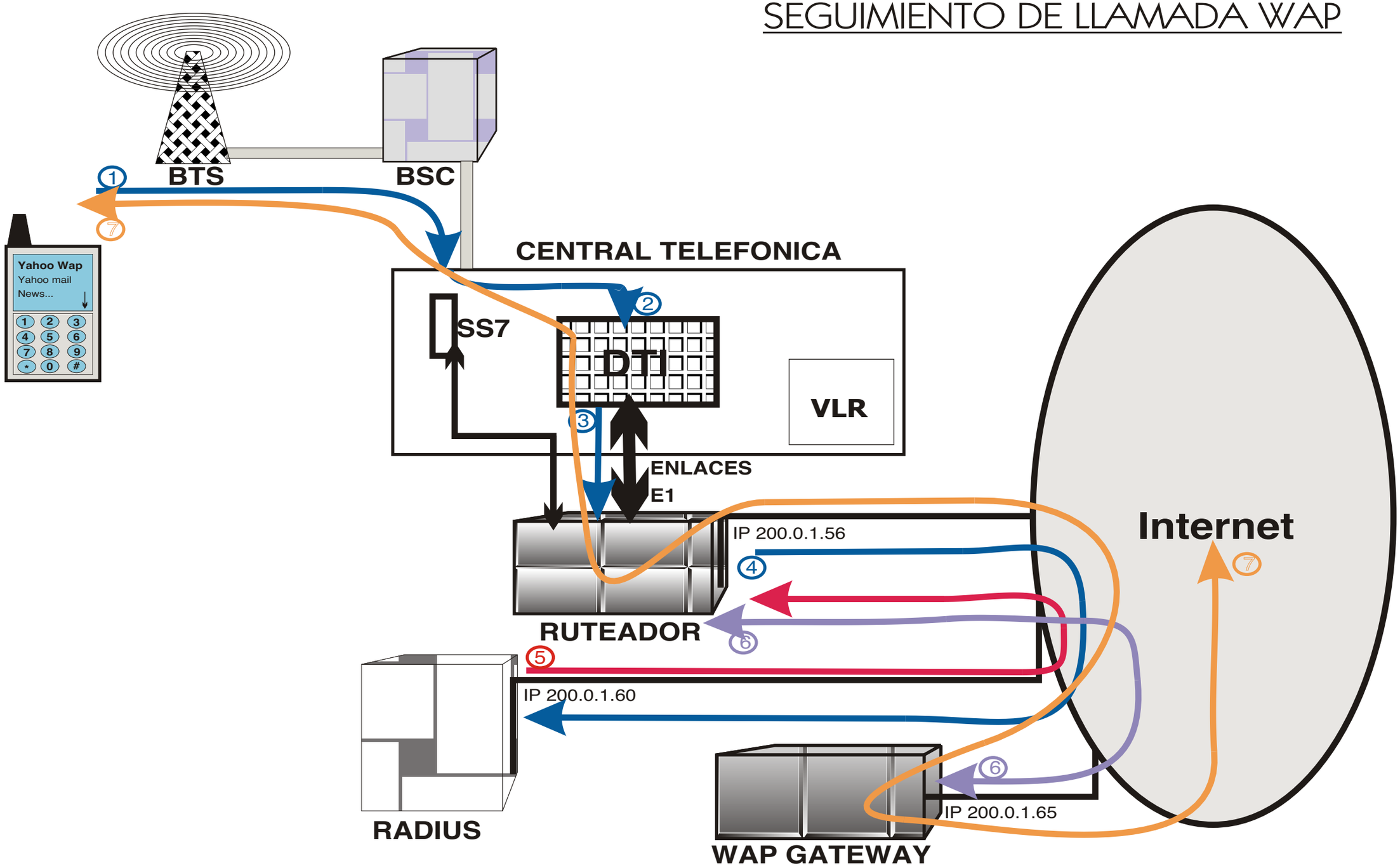
se encargara de convertir la página HTML en una página WAP, y viceversa (paso número 7 diagrama de Seguimiento de llamada WAP); además de que en el gateway de WAP se darán de alta los números de abonado de los usuarios que tendrán acceso al servicio. Esto es debido a que las pantallas de las terminales móviles son muy pequeñas, por lo que es necesario que las páginas de internet HTML se adapten a éstas, y esto se logra por medio del gateway de WAP.

SEGUIMIENTO DE LLAMADA WEB



La terminal móvil se puede conectar a la PC por medio de cable, puerto infrarrojo o Bluetooth, depende las opciones que disponga.

SEGUIMIENTO DE LLAMADA WAP



8.2 High Speed Circuit Switch Data (HSCSD)

La creciente demanda de los servicios de datos, obliga a el incremento en el ancho de banda de los servicios de redes fijas y móviles a nivel usuario, dando como resultado anchos de banda mayores empleando aún redes de circuitos conmutados.

En el caso especifico de las redes móviles basadas en la tecnología de acceso TDMA –como las redes GSM-, el incrementar el ancho de banda tiene que ver con el uso de más de un solo "Time-slot" en los radios de las antenas (Radiobases).

Para que se implemente el servicio HSCSD en una red móvil GSM, se necesita que la red móvil cuente con las siguientes características:

- Debe tener implementado y funcionando de manera correcta el servicio CSD a 9600 bps mínimo.
- Deben ser implementadas dos features en la Central telefónica, la feature HSCSD, y la feature 14400 bps.
- Además se debe habilitar la feature multislot en la BSC.

El funcionamiento de cada una de la features se describen a continuación:

La feature HSCSD permite al servicio poder tomar hasta cuatro "Time-slots" de una Radiobase, para de esta forma poder multiplicar el ancho de banda de 9600 bps por 4 "Time-slots", lo cual nos da un ancho de banda total de 38400 bps; Ahora, esta feature también permitirá de manera automática que el servicio en casos de congestionamiento de la Radiobase en la que se encuentre el usuario del servicio limite el número de "Time-slots" a 3, 2 o hasta 1 solo "Time-slot" para que otros usuarios que requieran servicios de voz o incluso de datos no se queden sin servicio porque una sola llamada de datos este absorbiendo 4 "Time-slots" ella sola (en condiciones de congestionamiento la feature HSCSD no cortara la llamada, sino que la limitara a 1 "Time-slot). Y si se descongestiona la Radiobase antes de que la llamada de HSCSD que originalmente tenia 4 "Time-slots" asignados, entonces la feature regresara los 3 "Time-slots" (o los que pueda regresar 1 o 2) a el usuario del servicio de HSCSD. Esto quiere decir que una llamada de HSCSD dependiendo del congestionamiento de las radiobases, tendrá un ancho de banda variable que va desde los 9600 bps con un solo "Time-slot", 19200 bps con dos "Time-slots", 28800 bps con tres "Time-slots" o 38400 bps con cuatro "Time-slots"; Esta feature solo permite como máximo el uso de cuatro "Time-slots" por llamada de datos.

La Feature 14400 habilitara a la BSC para que pueda manejar "Time-slots" específicamente para llamadas de datos (no de voz) de hasta 14400 bps por cada "Time-slot" en las radiobases.

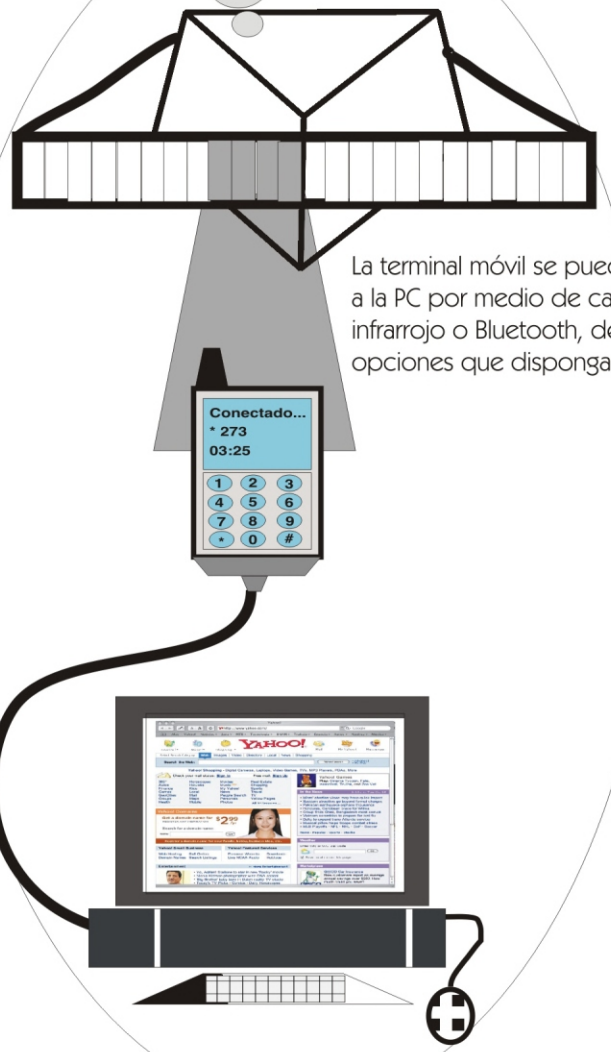
La feature Multislot, permitirá que la BSC controle de manera eficiente el manejo de "Time-slots" para el servicio HSCSD.

Entonces el servicio HSCSD, ya con las tres features habilitadas (HSCSD, 14400 y Multislot), funcionara con anchos de banda desde los 14400 bps con un "Time-slot", 28800 bps con dos "Time-slots", 43200 bps con tres "Time-slots" y hasta 57600 bps con cuatro "Time-slots". Y como se menciono antes la velocidad de transmisión de datos estará controlada por la feature HSCSD y dependerá de el congestionamiento que exista en las radiobases o Radiobase en donde se este dando el servicio HSCSD.

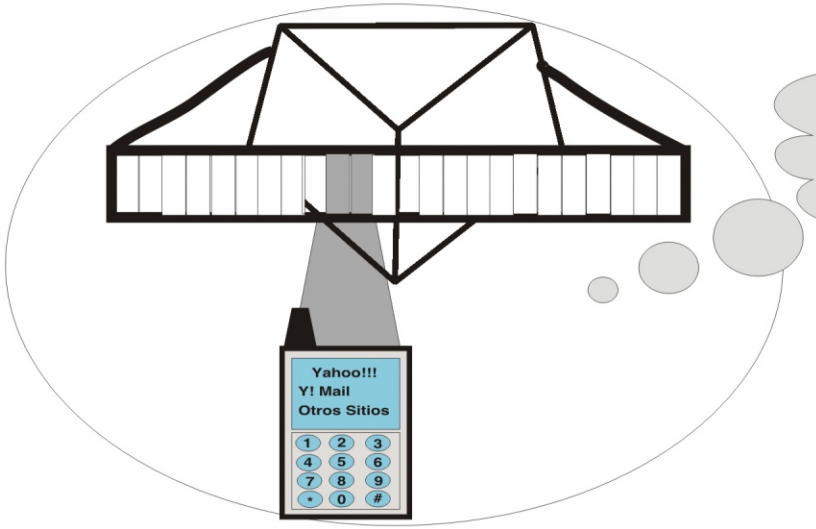
Para el caso de llamadas de datos ya sea con CSD o con HSCSD, que se encuentren en movimiento (ya sea que el usuario se encuentre caminando o circulando en un vehículo) la red móvil manejara las llamadas de datos como maneja las llamadas de voz, o sea, que el "Hand off" pasará la llamada entre radiobases, entre BSC´s o entre Centrales Telefónicas (ver Hand Off en el apéndice A).

HSCSD

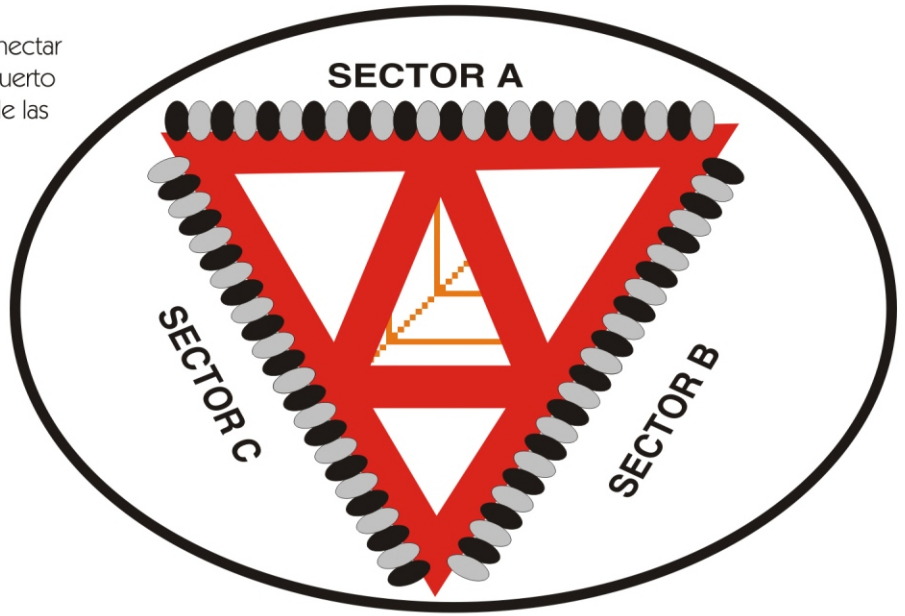
Llamada WEB HSCSD a 57600 Kbps, utilizando 4 Timeslots de un sector de la Antena.

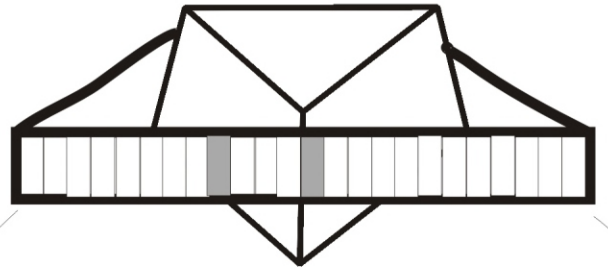


La terminal móvil se puede conectar a la PC por medio de cable, puerto infrarrojo o Bluetooth, depende las opciones que disponga.



Llamada WAP HSCSD a 28800 bps, utilizando 2 Timeslots de un sector de la Antena.





Cada sector de la antena permite la instalación de radios, que a su vez soportan 8 Timeslot cada uno, generalmente se instalan 3 radios por sector de la antena lo cual da un total de 24 Timeslot; estos Timeslot se emplean de manera individual para llamadas de voz o de datos; y en el caso del servicio HSCSD una llamada ya sea WEB o WAP, puede ocupar 1 ó hasta 4 Timeslots por llamada; También puede por ejemplo tomar 2 Timeslots en el sector "A" y 2 Timeslots en el sector "B", por lo que no se limitara a un solo sector de la antena.

VISTA SUPERIOR DE LOS 3 SECTORES DE UNA TORRE

NOTA: Los Timeslot representados en éste diagrama por rectángulos y ovalos negros y grises, en la realidad no se ven, pues son lógicos , no físicos. Además se consideran 3 radios de 8 Timeslots por cada sector de la antena, lo que da un total de 24 Timeslots por sector.

8.3 Global Packet Radio Service GPRS

Los estándares móviles digitales existentes continúan siendo desarrollados para incrementar su capacidad, cobertura, calidad y velocidad de transmisión de datos. Existen una serie de desarrollos en progreso con el objetivo de mejorar la funcionalidad de las redes GSM. Acorde con la primer mejora para incrementar la velocidad de transmisión de datos (HSCSD). La siguiente mejora es Global Packet Radio Service GPRS, que es un servicio de datos basado en paquetes conmutados, que permite una completa movilidad y área de cobertura. Además el servicio EDGE (Enhanced Data rates for the GSM Evolution) usara una modulación mejorada y técnicas relacionadas a mejorar de manera importante en el futuro el ancho de banda de los servicios de datos móviles.

El servicio UMTS (Universal Mobile Telecommunications System), también conocido como WCDMA, incluye servicios de segunda y tercera generación, lo último de lo que será un servicio multimedia de alta velocidad de transmisión de datos.

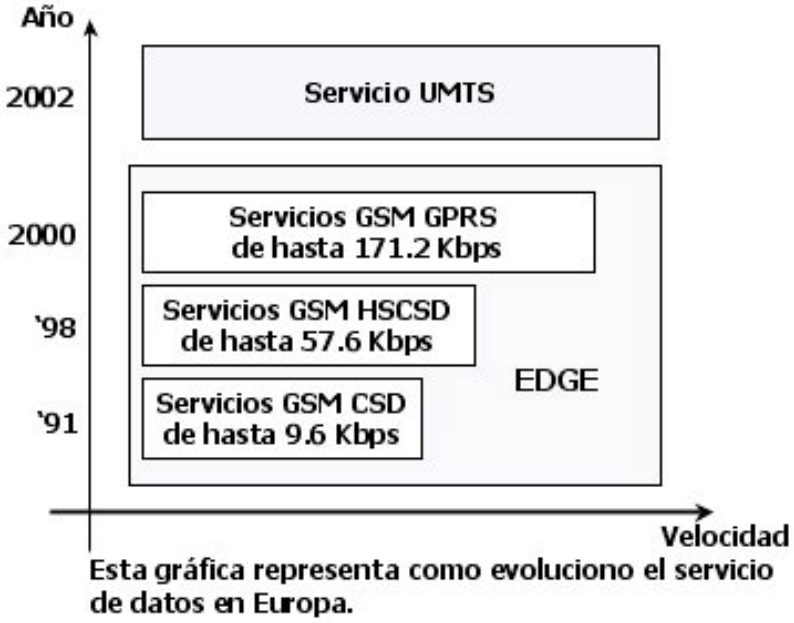


Figura 8.2 Evolución de los servicios de datos en las redes móviles GSM.

8.3.1 Circuitos Conmutados y Paquetes Conmutados

Para la comunicación en los sistemas basados en circuitos conmutados, la red habilita una conexión vía aire, alojándola en un canal de radio (Timeslot) a una terminal móvil para transmitir los datos a través de la red móvil. Incluso, si solo se transmitirán pequeñas cantidades de información, el canal de radio (Timeslot) es ocupado por la terminal móvil durante la conexión. Lo cuál implica que el usuario deberá pagar por el tiempo total de conexión, asi haya estado transmitiendo datos durante todo el periodo, o solo por ratos durante el mismo periodo; recordemos que el tiempo de conexión en la telefonía móvil es mucho más caro que en la telefonía fija.

Los sistemas basadas en circuitos conmutados son convenientes para tráfico de datos en alguna de las siguientes situaciones:

- Flujo de datos constante, ocupando el total del ancho de banda.
- Cuando la información es sensible incluso a pequeños retardos en la conexión.

Por ejemplo, el servicio basado en circuitos conmutados será útil para videoconferencia, y esto es debido a que éste servicio es muy sensible a retardos en la conexión, además requieren de ancho de banda constante.

Para el caso de los sistemas basadas en paquetes conmutados la red entregara paquetes con información solo cuando sea solicitado. Gracias a esto la interfaz aire (Timeslot) puede ser compartido por varias terminales móviles de manera simultanea. Cuando una terminal móvil genera un paquete de información, la red direcciona dicho paquete a el canal de radio (Timeslot). Desde que el tráfico de datos consiste comúnmente de ráfagas de datos (bursts), los canales de radio se usan de manera más eficiente.

Los sistemas basados en conmutación de paquetes son convenientes para tráfico de datos en alguna de las siguientes situaciones:

- Cuando la información es enviada en ráfagas de datos (bursts).
- Cuando la información no es sensible a retardos.

Por ejemplo, el servicio basado en paquetes conmutados será útil para aplicaciones de telemetría y correo electrónico.

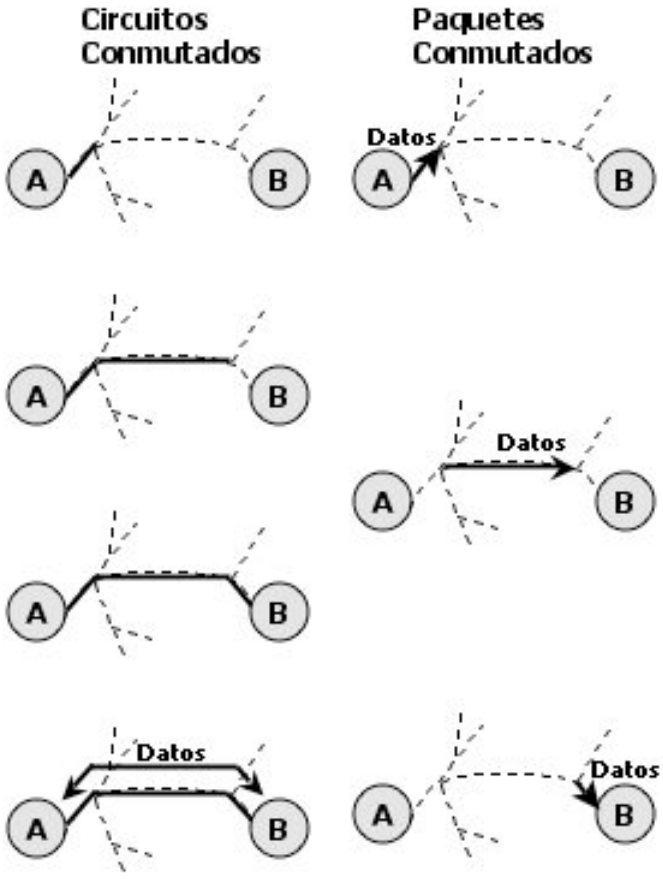


Figura 8.3 Comparación del manejo de datos entre circuitos conmutados y paquetes conmutados.

8.3.2 Ventajas de GPRS

El sistema GPRS provee una solución básica para las comunicaciones que utilizan el Protocolo de Internet (IP) entre terminales móviles y Servidores de Internet o redes LAN corporativas.

Y esto es gracias a:

- El uso eficiente de los no muy abundantes canales de radio (Timeslots).
- Un servicio flexible, que puede ser cobrado en base a el volumen de datos enviado y recibido por la terminal móvil.
- Rápido acceso al servicio.
- Transporte eficiente de paquetes a través de la red GSM.
- Coexistencia simultanea entre la red GSM y la red GPRS sin problemas.
- Conectividad con redes externas de paquetes de datos usando el protocolo de Internet (IP).

La solución de comunicaciones IP entre la terminal móvil y los Servidores de Internet permite servicios más allá de los que la red GSM puede proveer por si misma.

Comunicación de Ráfagas (bursts) y de Ancho de Banda

En la figura 8.4 se muestran la áreas en las que se utilizan los servicios de datos dependiendo su tipo, ya sea que se maneje información por ráfagas (bursts), o por consumo de ancho de banda. Ahora, dependiendo del tipo de servicio se tomara la decisión de que servicio es el más conveniente para la aplicación que se valla usar; pues puede ser el basado en circuitos conmutados o en paquetes conmutados, y de esto dependerá el costo del servicio para el usuario final.

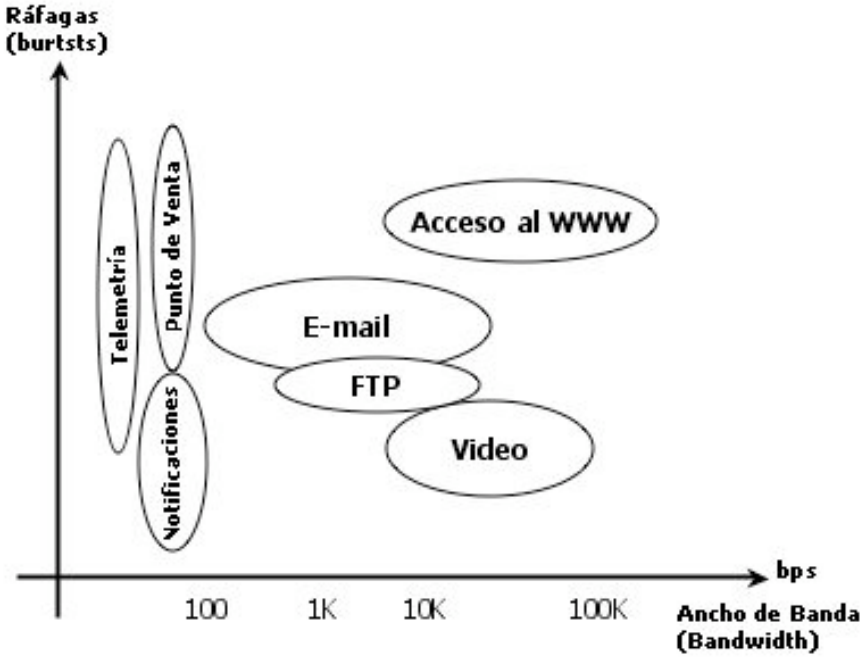


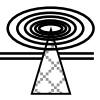
Figura 8.4 Gráfica de áreas de uso de los servicios de datos de acuerdo a su consumo en ancho de banda.

8.3.3 Aplicaciones de Paquetes de Datos

GPRS soporta el uso de Internet e Intranets mediante el uso de GSM/DCS (Digital Communication System)/PCS (Personal Communication System) y la terminal móvil como dispositivo de conexión. Las diferentes aplicaciones se caracterizan por ser horizontales o verticales.

Aplicaciones Horizontales

Las aplicaciones horizontales son aplicaciones adaptadas para resolver comunicaciones persona a persona, por ejemplo:



- E-mail
- Navegadores World Wide Web (WWW)
- Chats de Internet
- Transferencia de archivos usando el protocolo FTP
- Puntos de venta (lectores de tarjetas de crédito)
- Búsquedas en bases de datos
- Mensajería de dos Vías

Aplicaciones Verticales

Las aplicaciones verticales son aplicaciones adaptadas a resolver requerimientos específicos de comunicación de datos corporativos, por ejemplo:

- Ventas en campo
- Aplicaciones bancarias
- Aplicaciones de Telemetría (Maquinas de venta)
- Sistemas de optimización de distribución
- Servicios de despacho (Policía, taxis, etc.)

8.3.4 Estaciones Móviles GPRS

Equipos Terminal (Terminal Equipment – TE)

Los equipos terminal son en realidad equipos de computo donde el usuario trabaja. Y son los componentes usados por GPRS para transmitir y recibir los paquetes de datos, por ejemplo, un TE puede ser una Laptop, una Palm, etc.

Terminal Móvil (Mobile Terminal – MT)

La terminal móvil es quien desempeña todas las funcionalidades GPRS. La MT establece un enlace lógico a un SGSN, el cual realiza la actualización de la ubicación y la transferencia de datos al usuario sobre la interfaz aire. La red GPRS provee conectividad IP entre la TE e Internet o redes corporativas. Desde el punto de vista de el TE es posible comparar la MT con un MODEM, que conecta el TE con la red de datos.

Como en el caso de CSD la terminal móvil puede ser usada como un MODEM para conectarse a la red, o con el navegador WAP puede visualizarse la información que se recibe y que se envía.

Estación Móvil (Mobile Station – MS)

La combinación entre un equipo terminal (TE) y una terminal móvil (MT) es llamado una estación móvil (MS). Comúnmente en el documento conocido como ETSI GSM Standard for GPRS, el termino MS es usado cuando se discuten las posibilidades (features) de GPRS.

Clases de Estaciones Móviles en GPRS

Las estaciones móviles GPRS pueden operar en tres modos diferentes:

- Clase A, soporta simultáneamente tráfico de circuitos conmutados y de paquetes conmutados.

- Clase B, soporta tráfico de circuitos conmutados o paquetes conmutados, pero no ambos simultáneamente.
- Clase C, esta clase trabaja ya sea como paquetes conmutados o como circuitos conmutados.

La estación móvil también cuenta con la siguientes especificaciones:

- Potencia de Radiofrecuencia (RF – máxima potencia en transmisión)
- Capacidad de servicio de Mensajes Cortos (SMS)
- Frecuencia de operación (900,1800 o 1900; ya hay terminales tri-banda)
- Capacidad para bajar y subir información por multislot (por ejemplo, un MS 3+1 puede manejar como máximo 3 timeslots para bajar información y 1 timeslot para subir información).

8.3.5 Comparación entre GPRS y WCDMA

Los componentes de las redes GSM que llevan a cabo el manejo de paquetes en la red GPRS son el Servidor Nodo de Soporte GPRS (Serving GPRS Support Node – SGSN) y el gateway nodo de soporte GPRS (Gateway GPRS Node Support – GGSN). El SGSN provee ruteo de paquetes a y desde el área geográfica de servicio del SGSN. El GGSN maneja la interfaz hacia las redes IP de datos externas. Tanto el SGSN como el GGSN son equipos físicamente separados de la red móvil de circuitos conmutados. Los otros elementos a usar en la red GSM son la BSC y la Radiobase (ver apéndice A).

Ahora, para cuando se quiere usar GPRS en una red WCDMA, el primer paso que se debe realizar es cambiar la BSC por su equivalente RNC y la Radiobase (BTS) por el nodo B (Node B).

Sistema Estación Base (Base Station System – BSS)

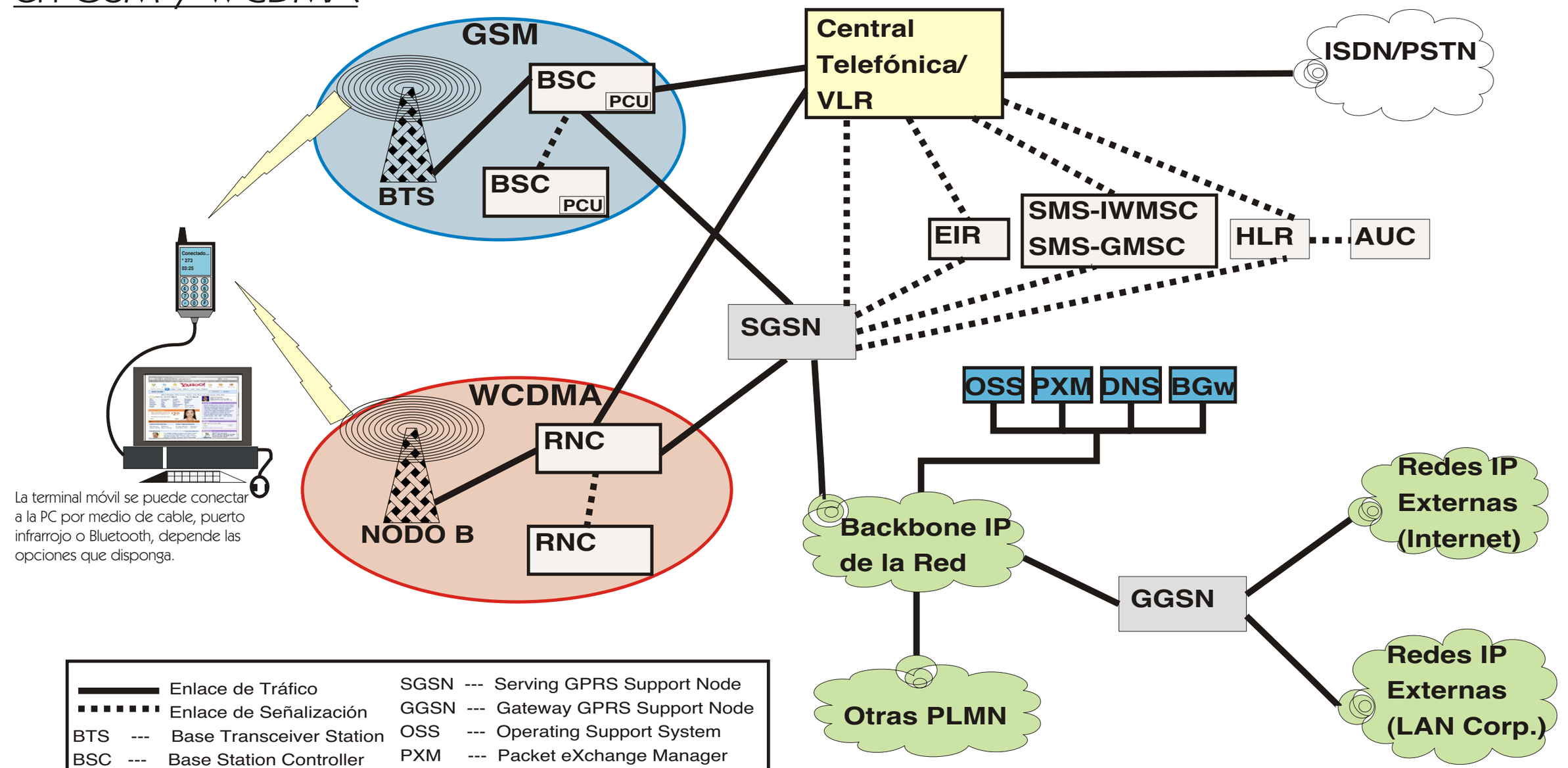
El sistema estación base (BSS) consiste de una Estación Base Controladora (BSC – Base Station Controller) y de una Estación Base receptora/transmisora (BTS – Base Transceiver Station) mejor conocida como Radiobase. La BTS es el equipo de radio que recibe y transmite información sobre la interfaz aire, y que permite a la BSC comunicarse con las estaciones móviles en su área de servicio. Un grupo de BTS´s es controlado por una BSC; la BTS debe contener software y hardware especifico para GPRS.

La BSC provee todas las funciones relativas a el servicio de radio. Además puede establecer, supervisar y desconectar llamadas de circuitos conmutados o de paquetes conmutados; es un switch de alta capacidad que provee funciones que incluyen hand-off, configuración de datos en la célula y asignación de canales de radio. La BSC debe ser equipada con hardware y software especifico para operar con GPRS. Una o varias BSC´s trabajan para una central telefónica, y varias BSC´s trabajan para un SGSN.

La BTS separa las llamadas de circuitos conmutados de la de paquetes conmutados antes de que lleguen a la BSC, quien a su vez envía las llamadas de circuitos conmutados a la central

telefónica/HLR y las llamada de paquetes conmutados a el SGSN. Protocolos GSM estándar son usados con la BSC para alcanzar la compatibilidad deseada.

Estructura de Red GPRS en GSM y WCDMA



La terminal móvil se puede conectar a la PC por medio de cable, puerto infrarrojo o Bluetooth, depende las opciones que disponga.

Enlace de Tráfico
Enlace de Señalización

BTS --- Base Transceiver Station
BSC --- Base Station Controller
PCU --- Packet Control Unit
HLR --- Home Locator Register

SGSN --- Serving GPRS Support Node
GGSN --- Gateway GPRS Support Node
OSS --- Operating Support System
PXM --- Packet eXchange Manager
NTP --- Network Time Protocol
Bgw --- Billing Gateway
RNC --- Radio Network Controller

8.3.6 Elementos de Red: La Central Telefónica (Switch)

La central telefónica se encarga de las funciones de conmutación de circuitos en la red GSM, asi como el SGSN se encarga de las funciones de la conmutación de paquetes de tráfico. Controla las llamadas "a y desde" otros sistemas telefónicos y de datos, como la Red Telefónica Pública Conmutada (PSTN – Public Switch Telephone Network), la Red Digital de Servicios Integrados (ISDN – Integrated Service Digital Network), la Red Pública Móvil (PLMN – Public Land Mobile Network), la Red Pública de Datos (PDN – Public Data Network) y hasta puede llegar a controlar algunas redes privadas.

El área de ruteo del SGSN (RA – Routing Area) es un sub-segmento de el área de locación (LA) de la Central Telefónica (CS). El área de locación de una Central Telefónica es un grupo de células BSS. El sistema usa las áreas de locación (LA´s) para buscar abonados activos. Una LA es el área en la red donde una terminal móvil (MS) puede moverse sin necesidad de reportar su locación a la red.

Un área de servicio (SA) está conformada por la Central Telefónica y el VLR (ver apéndice A) y agrupa un número de LA´s. El área de servicio (SA) es la parte de la red a la cuál da cobertura una Central Telefónica.

Pueden existir muchas Centrales Telefónicas asociadas a un solo SGSN. Una Central Telefónica puede también estar asociada a varios SGNS´s. La configuración es un asunto de dimensionamiento dependiendo del tráfico que exista, o que se tenga contemplado en el diseño de la red GPRS.

Gateway Mobile Services Switching Center GMSC

El Gateway GMSC realiza la conmutación de circuitos entre la red GSM y la red PSTN**,** que no es otra más que la red Telefónica Fija, entonces, soporta la función de ruteo de llamadas entrantes a la Central Telefónica donde los suscriptores móviles están registrados. Normalmente la Central Telefónica y el VLR están integrados en el mismo nodo. El GMSC no cambia su función por el uso del servicio GPRS.

Home Locator Register HLR

El HLR es la base de datos que almacena la información personal de cada uno de los suscriptores de la red GSM/GPRS. El HLR almacena información de la comunicación de la red de circuitos conmutados y de la de paquetes conmutados. La información que almacena el HLR incluye, por ejemplo, servicio suplementarios, parámetros de autenticación, Nombres de Punto de Acceso (APN – Access Point Name) como la suscripción de Proveedor de Servicios de Internet así como una dirección IP estática es alojada para una terminal móvil (MS).

En suma, el HLR incluye información sobre la locación de las terminales móviles. Para GPRS, la información del suscriptor es intercambiada entre el HLR y el SGSN. Hay que notar que la información de autenticación para el servicio GPRS es requerida al HLR por parte del SGSN, lo que significa que ésta información no pasa por la Central Telefónica/VLR como sucede en el caso de circuitos conmutados.

La información del suscriptor que va de el HLR al SGSN ha sido dada de alta por el operador de la red, o ha sido recibida con anterioridad de otro SGSN. Esta transferencia de información se realiza cuando el operador cambia la información del suscriptor, o cuando un nuevo SGSN necesita la información de un suscriptor después de haber sido dado de alta o por el servicio de Roaming. Los SGSN ya existentes también son informados por el Roaming. La información que va desde el SGSN

hacia el HLR es la información de ruteo que es transferida por el movimiento de las terminales móviles, por ejemplo en el caso del roaming. Para que exista el roaming de una terminal móvil, el HLR debe estar en una PLMN diferente que el SGSN que sirve a dicha terminal.

Visitor Locator Register VLR

El VLR es una base de datos que contiene información sobre todas las terminales móviles que se encuentran en un área de locación LA de la Central Telefónica o en el área de ruteo del SGSN, respectivamente. El SGSN actualmente contiene la funcionalidad del VLR para la comunicación de paquetes conmutados.

El VLR contiene la información del suscriptor que la central Telefónica o el SGSN necesitan para proveer el servicio correspondiente a los suscriptores, solo que esta información es temporal mientras el suscriptor se mantiene dentro de el área de servicio de la Central Telefónica o del SGSN.

Cuando una terminal móvil cambia del área de locación de la Central Telefónica o de el área de ruteo del SGSN, el VLR de la Central Telefónica o del SGSN solicita información al HLR sobre la terminal móvil, la cuál la almacenara temporalmente mientras la terminal móvil se mantenga dentro del área de locación de la central o del área de ruteo del SGSN. Si la terminal móvil hace una llamada ya en la nueva área de locación o área de ruteo, la información necesaria para dicha llamada ya se encuentra disponible de manera inmediata en el VLR.

El VLR de GPRS consiste de software en el SGSN. El VLR contiene la información sobre el SGSN que será usada. Para el sistema GPRS, el HLR, en lugar de la Central Telefónica/VLR, es usado de manera directa para el procedimiento de autenticación de las terminales móviles. De una u otra manera, el SGSN obtiene la información de autenticación de el HLR.

Equipment Identity Register EIR

El Registro de Identidad de equipo EIR es una base de datos que mantiene la información de identidad de las terminales móviles, el cual ayuda a bloquear llamadas de terminales móviles robadas, sin autorización o defectuosas.

Authentication Center AUC

El centro de Autenticación es una entidad especificada en el estándar GSM que provee las herramientas tecnológicas necesarias para autenticar y cifrar procesos utilizados internamente en las redes GSM. La autenticación tanto para usuarios GPRS como GSM es la misma. El cambio en seguridad para GPRS es solo relacionado al cifrado, y cuando se agrega el servicio GPRS a una red GSM no se requiere ninguna actualización en el AUC.

Short Message Service-Interworking MSC (SMS-IW-MSC)

El servicio de mensajes cortos SMS permite a las terminales móviles que cuentan con el servicio GPRS enviar mensajes cortos sobre los canales de radio GPRS.

Short Message Service Gateway MSC (SMS-GMSC)

El Gateway de Mensajes Cortos habilita a las terminales que cuentan con el servicio GPRS a recibir SMS sobre los canales de radio GPRS. Cuando el SMS-GMSC va a enviar un mensaje corto a una terminal móvil, éste recibe la ubicación de el HLR.

Serving GPRS Node Support SGSN

El SGSN es un componente primario en la red GPRS, y es un nuevo componente en la red GSM. El SGSN provee ruteo de paquetes y transferencia "a y desde" el área de servicio de el SGSN. El SGSN da servicio a todos los suscriptores GPRS que están localizados físicamente dentro del área de servicio del SGSN. Un usuario GPRS puede ser atendido por cualquier SGSN en la red, todo depende de su ubicación física. El tráfico se enruta entre el SGSN y la terminal móvil vía la BSS (BSC/BTS).

El SGSN también provee de:

- Cifrado y autenticación.
- Manejo de Sesión.
- Manejo de Movilidad.
- Manejo de enlaces lógicos hacia las terminales móviles.
- Conexión a el HLR, la Central Telefónica, la BSC, el GGSN y otros nodos.
- Manejo de Información de cobro del servicio.

El SGSN colecta la información de cobro de cada terminal móvil relacionada a el uso de los canales de radio de la red. Tanto el SGSN como el GGSN colectan información de cobro sobre el uso de los recursos de la red GPRS.

Gateway GPRS Node Support GGSN

Como el SGSN, el GGSN es un componente primario de la red GPRS, y es un componente nuevo.

El GGSN provee de:

- La interfaz hacia las redes externas IP de paquetes. El GGSN, por tanto, es quien se encarga del manejo de las interfaces con Proveedores de Servicio de Internet (ISP – Internet Service Provider), y se conecta a, por ejemplo, otros ruteadores o a servidores RADIUS, los cuales son usados para la locación segura de direcciones IP. Desde el punto de vista de las redes IP externas, el GGSN actúa como un ruteador para todas las direcciones IP de todos los suscriptores de la red GPRS. El GGSN, de una u otra forma, intercambia información de ruteo con redes IP externas.
- Manejo de la sesión GPRS, inicio de la comunicación hacia redes IP externas.
- Habilidad para asociar a los suscriptores con el SGSN que les corresponde para entregar información de redes IP externas.
- Manejo de información de cobro. Como se menciono anteriormente el GGSN colecta la información de cobro para cada terminal móvil que use la red de datos.

Packet Exchange Manager PXM

La interfaz de usuario PXM se basa en un navegador WEB y un ambiente java instalado sobre una plataforma UNIX o Windows. La aplicación PXM es implementada en el nodo GSN (SGSN-GGSN).

Esto significa que las páginas HTML y los applets de java, leídos con éste navegador WEB, serán almacenados en el nodo. Las páginas serán transferidas sobre TCP/IP en el Backbone IP.

Todas las actividades de Operación y Mantenimiento (O&M) hacia un GSN son manejadas a través de está Interfaz Gráfica de Usuario java (java based GUI).

Domain Name Server DNS

El DNS maneja una base de datos. La base de datos contiene un mapeo entre el nombre de las redes de datos externas y las direcciones IP de el GGSN permitiendo el acceso a dichas redes.

Billing Gateway BGw

El Gateway de cobro (BGw) facilita la introducción del servicio GPRS en una red móvil, ofreciendo funciones que simplifican el manejo de el cargo por el servicio GPRS en los sistemas de cobro.

El criterio de cargo usado para un servicio de paquetes conmutados, como GPRS, es fundamentalmente diferente de el principio usado para el servicio de circuitos conmutados; éste (GPRS) se basa en el volumen de los datos manejados en lugar de en el tiempo total de conexión (CSD o HSCSD).

La información de cobro es colectada por los nodos GPRS (SGSN y GGSN) y es transformada para ser más fácilmente interpretada por los sistemas de cobro.

Operation Support-System OSS

Para el manejo de las redes móviles existe una herramienta llamada Sistema de Operación y Soporte (OSS). El OSS incluye aplicaciones para la supervisión, configuración y manejo de desempeño en redes móviles. En suma a las aplicaciones de manejo de la red móviles, el OSS provee funciones básicas, por ejemplo, manejo de alarmas y transferencia de archivos.

De manera semejante a la interfaz de usuario PXM, el OSS permite la supervisión simultanea de todos los nodos GSN de la red GPRS.

8.3.7 Interfaz Aire GPRS

En GPRS la interfase aire es llamada Um como en GSM. La trama TDMA siempre se usa, pero los canales físicos (mejor conocidos como canales de radio) se manejan de forma diferente.

Canales Físicos Dedicados y por Demanda GPRS

La totalidad de canales físicos disponibles en una célula es compartida por los servicios de circuitos conmutados y GPRS **.** Estos canales físicos GPRS serán fijos (llamados Dedicados) o dinámicos (llamados por Demanda). Un canal físico que transporta tráfico GPRS es llamado PDCH (Physical Data Channel).

Los PDCH dedicados son dados de alta y liberados vía comandos por el operador.

Los PDCH por demanda, sirven temporalmente como recursos dinámicos GPRS, y se dan de alta y liberan dependiendo la demanda de tráfico GPRS.

PDCH Dedicados

Los PDCH dedicados solo pueden ser usados por el servicio GPRS. El operador puede especificar desde cero hasta ocho PDCH dedicados por célula.

Los PDCH dedicados aseguran que siempre habrán recursos de radio para el servicio GPRS en una célula. El operador puede especificar el rango donde los PDCH dedicados serán ubicados en la célula.

PDCH por Demanda

1. Los PDCH por demanda serán asignados de el pool de canales físicos de los circuitos conmutados, también llamado CSD (Circuit Switch Domain), solo cuando halla necesidad de más PDCH para tráfico de Paquetes Conmutados (PS).

Una supervisión de tráfico será implementada para ello, en una célula con o sin PDCH dedicados, nuevos PDCH por demanda serán asignados cuando el número de usuarios GPRS sea muy alto con respecto al numero de PDCH existentes en la célula, siempre y cuando hallan canales de tráfico libres disponibles.

2. Los PDCH por demanda serán asignados solo de manera temporal para el servicio GPRS y serán regresados a CSD cuando no fueron reservados por un tiempo determinado.

Los PDCH que no son usados por tráfico GPRS, son colocados en una lista Dominio de Paquetes Conmutados (PSD – Packet Switch Domain) listos para ser usados. Después de un tiempo límite en la lista PSD, los PDCH son reasignados de la PSD y regresados a CSD.

Un parámetro PILTIMER es usado para la asignación de el temporizador de la lista de paquetes disponibles. Cuando un PDCH por demanda pasa a ser disponible es colocado en dicha lista por el Dominio de Paquetes Conmutados PSD y el PILTIMER se inicializa. Cuando el PILTIMER expira para un PDCH el canal es regresado al Dominio de Circuitos Conmutados.

4. El PDCH por demanda es regresado al Dominio de Circuitos Conmutados cuando dicho dominio lo necesite. Recordemos que las llamadas de voz son parte primordial del Dominio de Circuitos Conmutados, por lo que si se requiere uno o varios canales aire para llamadas de voz, y estos canales están siendo ocupados por llamadas de datos, se reasignaran para las llamadas de voz de manera automática.

Si existe falta de canales de tráfico en CSD, un requerimiento de canales PDCH será enviado a el PSD, en el caso de que existan PDCH por demanda en la célula. Un PDCH por demanda será regresado a CSD.

8.3.8 Posibilidades de Envío y Recepción de Información por los Recursos de Radio (Uplink & Downlink)

EN GPRS los recursos de radio para el envío (uplink) y la recepción (downlink) de la información pueden ser alojados separadamente para diferentes terminales móviles. Por ejemplo, en la figura 8.5 se muestra que en el Timeslot número 7 se ocupa para enviar información de la terminal 1, y para la recepción de información de la terminal 2.

Varios Timeslots pueden ser elegidos para la misma terminal. En la misma figura 8.5 se muestran los Timeslots 5, 6 y 7 recibiendo información para la terminal 2.

En un mismo Timeslot pueden ser alojadas varias terminales. En la figura 8.5, el Timeslot 3 recibe información para la terminal 3 en $T=T_0$. Pero en un periodo posterior $T=T_1$, en la misma trama TDMA, el Timeslot 3 es usado por la terminal 4. Y de nueva cuenta, unos periodos después el Timeslot 3 será usado por la terminal 3.

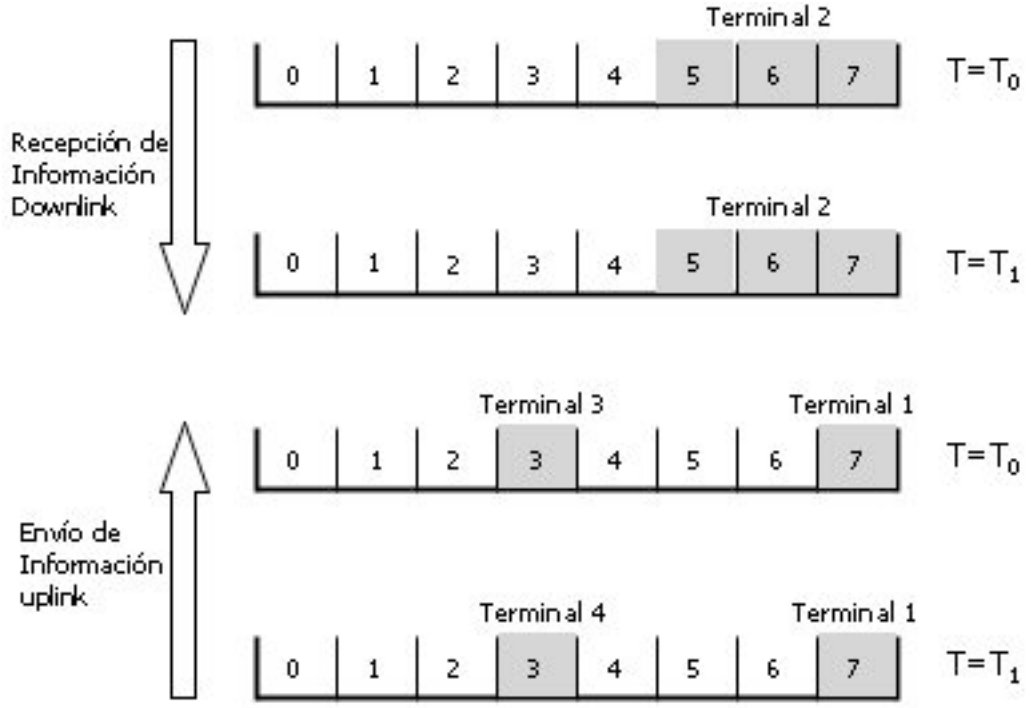


Figura 8.5 Recursos de radio enviando (uplink) y recibiendo (downlink) información de terminales móviles; considerando un radio de 8 Timeslots.

Ubicación de los Recursos de Radio de Recepción (Downlink) de Información

Cuando la Unidad Controladora de Paquetes (PCU – Packet Control Unit) recibe tramas desde el SGSN, la PCU se cerciora si la dirección de la terminal esta inmiscuida en la transferencia de paquetes:

Si la terminal ya tiene asignados recursos de recepción de información, las nuevas tramas de datos son puestas en cola junto con las otras tramas que van hacia esa terminal.

Si la terminal no tiene asignados recursos de recepción de información, una asignación de recepción de paquetes es enviada a la terminal. Este mensaje contiene los Timeslots que serán usados para la recepción de la información, además de una identidad temporal para la terminal llamada TFI. Esta identidad es necesaria debido a que varias terminales pueden compartir un mismo Timeslot.

En la figura 8.6, la PCU se encuentra recibiendo una trama de datos para la terminal 2, mientras que una transferencia se encuentra en progreso a la terminal 1; debido a que la terminal 2 no esta involucrada en la recepción de información, entonces la PCU aloja la terminal 2 en el Timeslot 6 y le asigna el TFI 23.

Si el SGSN no conoce la célula donde la terminal esta alojada, envía un requerimiento por medio del Paging. Entonces la PCU difunde el mensaje de Paging a todas las células pertenecientes a el área indicada por el SGSN para localizar la célula que corresponde a la terminal y de esa manera poder enviarle la información.

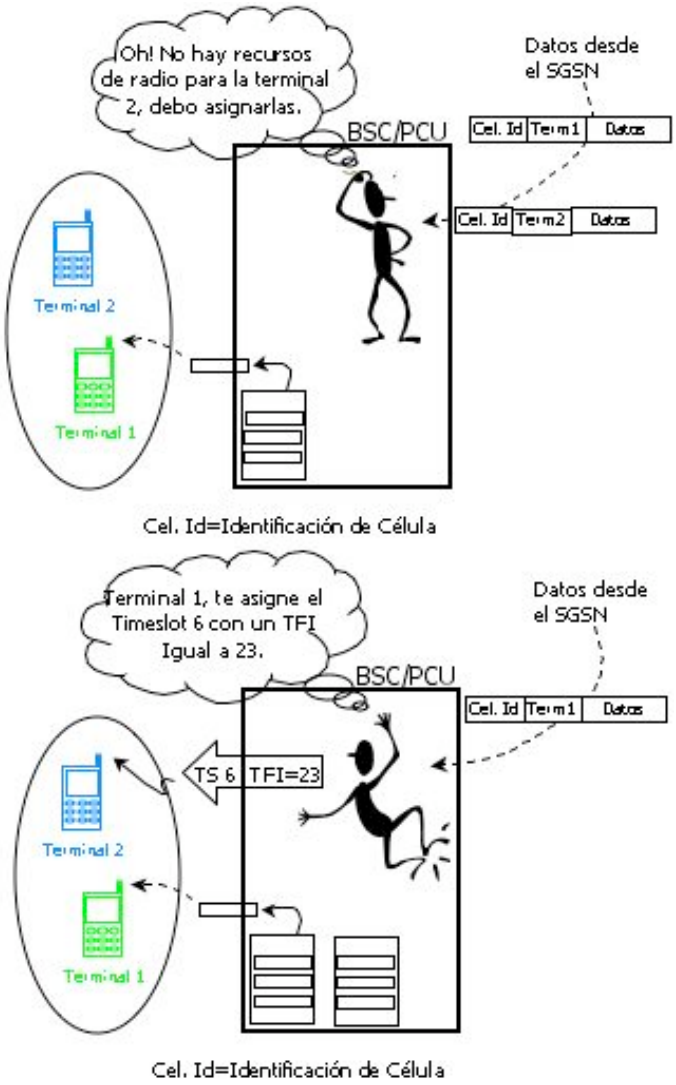


Figura 8.6 Alojamiento de recursos de radio para recepción de información.

Recepción de Datos (Downlink Transfer)

Una vez que la terminal ha recibido el mensaje de asignación de recepción de paquete (PDAM - Packet Downlink Assignment Message) con la lista de Timeslots y el TFI, éste lee el encabezado de la trama enviado por el Timeslot.

Si el TFI presente en el encabezado de la trama es el mismo que el TFI alojado en la terminal, entonces la información que viene en el bloque le pertenece a esa terminal. Si no, la terminal ignora la información contenida en el bloque.

En la figura 8.7 el Timeslot 6 es compartido por la terminal 2 y la terminal 3. Los segmentos PCU de la trama provienen del SGSN y son almacenados en el buffer de transmisión del Timeslot 6. La PCU también agrega la cabecera incluyendo el TFI.

El bloque que se envía por la interfaz aire contiene el TFI número 23, así que el dueño de ese bloque es la terminal 2. El siguiente bloque será para la terminal 3.

Cuando no hay más tramas que transmitir a una terminal en la PCU, los recursos de recepción (downlink) son liberados. Si una nueva trama llega, un nuevo mensaje de asignación de recepción de paquete (PDAM) es enviado a la terminal.

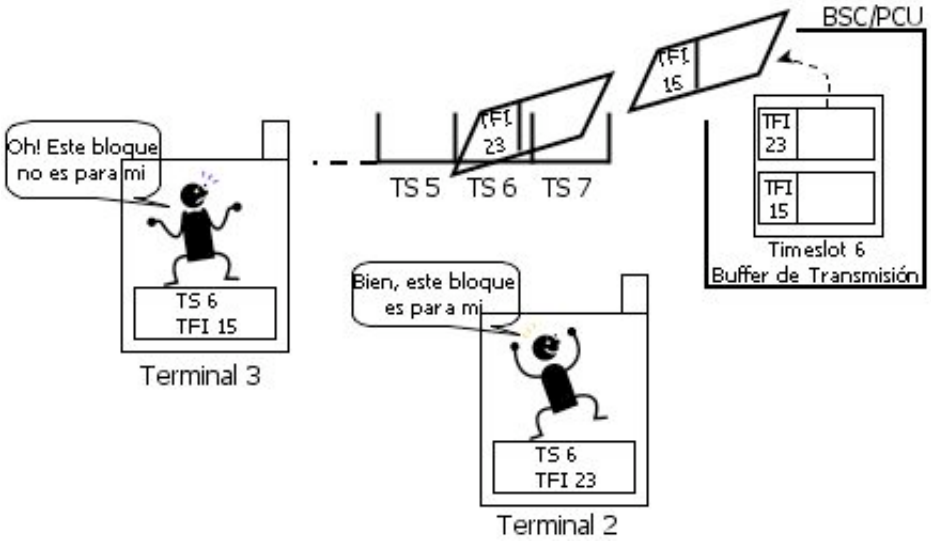


Figura 8.7 Recepción de Datos (Downlink Transfer).

Alojamiento de Recursos de Radio para Envío de Información

Cuando una terminal necesita enviar tramas de datos a la red, envía un mensaje de requerimiento de canal para transmitir paquetes (PCRM – Packet Channel Request Message) a la PCU. Y la PCU contesta a la terminal con un mensaje de asignación de paquete de envío (PUAM – Packet Uplink Assignment Message).

Este mensaje contiene una lista de Timeslots que podrán ser usados para enviar información, una identidad temporal llamada TFI, además de un número USF para cada Timeslot incluido en la lista. El USF índica a una terminal cuando debe transmitir.

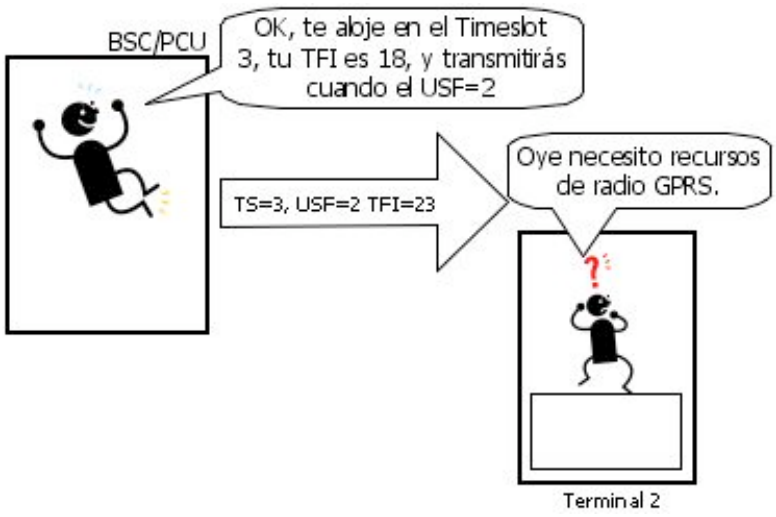


Figura 8.8 Alojamiento de Recursos de Radio para Envío de Información

Envío de Datos (Uplink Transfer)

Una vez que la terminal ha recibido mensaje de asignación de paquete de envío (PUAM), con la lista de Timeslots, el USF para cada Timeslot y el TFI, leerá la cabecera de los bloques de recepción enviados a sus Timeslots asignados para saber cuando deberá enviar información.

Si el USF presente en la cabecera es el mismo que el USF alojado en la terminal, entonces la terminal sabe que esta autorizado a enviar el siguiente bloque de datos por el canal de radio. Este mecanismo evita conflictos en el envío de datos cuando el mismo Timeslot es compartido por varias terminales.

En la figura 8.9 el Timeslot 3 es compartido por la terminal 2 y la terminal 3. Ambas terminales leerán los USF presentes en los bloques de datos de recepción enviados por el Timeslot 3. En el bloque que es enviado por el Timeslot 3, el USF es 2. Por lo tanto la terminal 2 deberá transmitir su siguiente bloque de datos.

La terminal 2 envía en la cabecera del bloque de datos su TFI. La PCU usa el TFI para identificar el bloque del que envía de entre los bloques almacenados en el buffer de recepción del Timeslot 3.

Cuando una terminal solo tiene unas pocas tramas que enviar, esto es notificado a la red y un procedimiento de conteo descendente comienza. Después de que todos los bloques de datos has sido enviados, los recursos de envío son liberados. Si la terminal tiene más tramas que transmitir después de que el procedimiento de conteo descendente se ha iniciado, nuevos recursos de radio deberán ser habilitados para estas tramas de datos. A la terminal no se le permite continuar enviando más paquetes de los que tenia una vez que se inicio el procedimiento de conteo descendente.

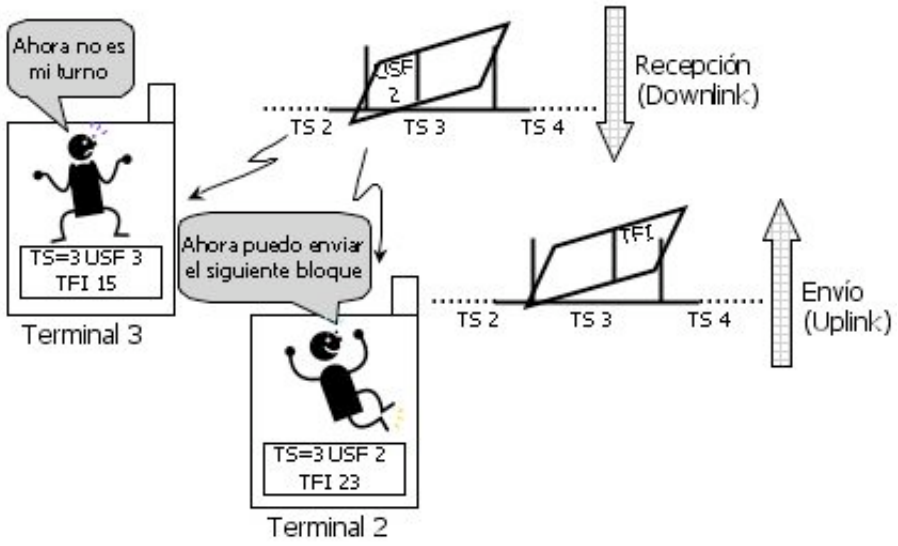


Figura 8.9 Envío de Datos (1) (Uplink Transfer)

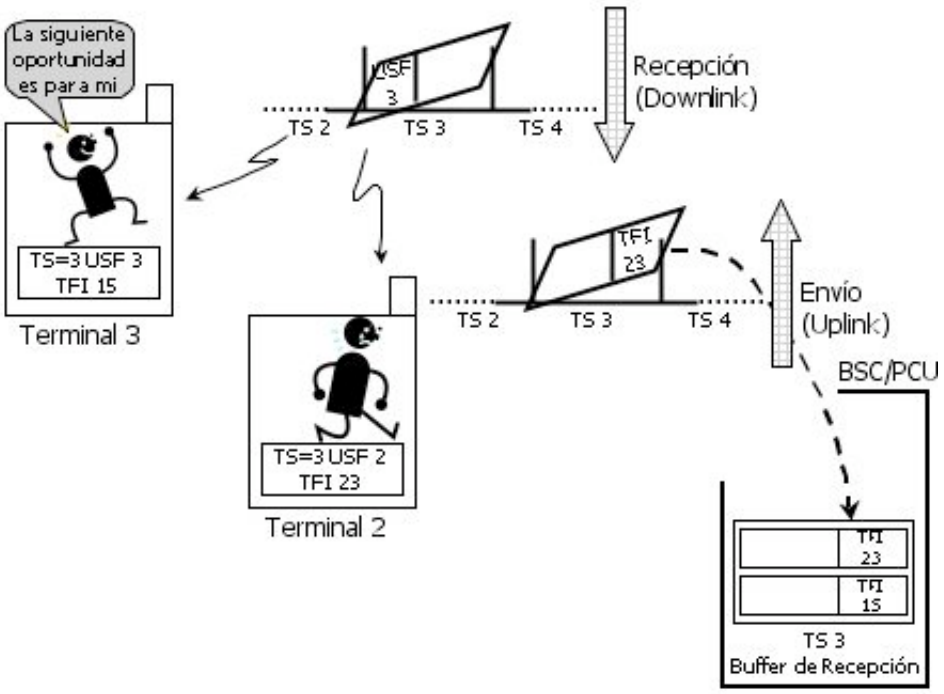


Figura 8.10 Envío de Datos (2) (Uplink Transfer)

8.3.9 Impactos de GPRS

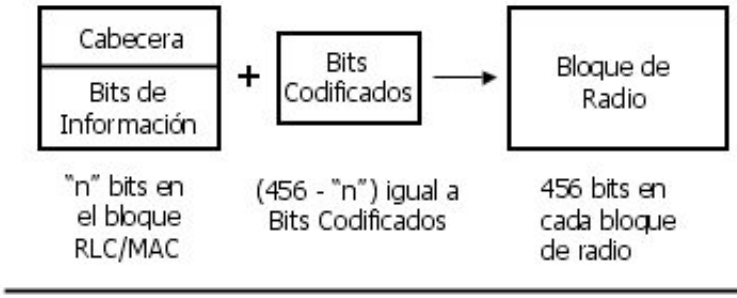
Los bloques de radio que contienen la información, y que son transmitidos sobre interfaces aire sufren una degradación debido a interferencias y atenuación en la señal.

Información redundante es agregada a la información transmitida para detectar, y eventualmente corregir errores que aparecen durante la transmisión por la interfaz aire de radio. Estos bits de información redundante son llamados bits codificados.

El tamaño de los bloques de radio siempre es de 456 bits. Por lo tanto, para incrementar el número de bits codificados, el número de bits de información debe ser reducido. En GPRS 4 (CS – Coding Schemes) los esquemas de codificación han sido definidos correspondiendo a radios diferentes, el de bits codificados y el de bits de información.

Entre más bits codificados ión decrece.

Por lo tanto, el esquema de codificación 1 es el más seguro, pero provee una baja tasa de transmisión de información (9.04 Kbps). Mientras que el esquema de codificación 4 es el menos seguro, pero provee la tasa de transmisión mas alta (21.4 Kbps).



Esquema de Codificación	Máx. No. De Bits de Información	Tasa Máx de Transf. (Kbps)	Target C/I (dB)
CS 1	181	9.05	-6
CS 2	268	13.4	-9
CS 3	312	15.6	-12
CS 4	428	21.4	-17

Figura 8.11 Estructura del Bloque de Radio

8.4 ENHANCED DATA FOR GSM EVOLUTION EDGE

EDGE es una mejora para el sistema móvil GSM. Como su nombre los indica EDGE permite el manejo de datos sobre redes GSM (TDMA) a mayores velocidades de transmisión (hasta 384 Kbps). EDGE también es conocido como EGPRS o dicho en términos más simples, es un GPRS mejorado.

Como se menciona en el párrafo anterior, para que EDGE pueda ser implementado, es necesaria la anterior implementación de GPRS en la red móvil. Una vez que GPRS ha sido implementado y funciona de manera correcta, entonces la implementación de EDGE puede incrementar poco más de 3 veces la velocidad manejada con GPRS (115 Kbps), y esto se debe a que EDGE adopta una nueva forma de modulación. GSM utiliza la modulación conocida como Gaussian Minimum Shift Keying (GMSK-ver Apéndice A), y EDGE cambia a la modulación 8PSK (ver Apéndice A), por lo cuál puede incrementar significativamente la tasa de transferencia de datos en la red móvil.

Bajo el sistema GPRS original, un circuito puede ser usado para proporcionar al usuario transmisión de voz o datos, esto es bueno para las llamadas de voz, pues el ancho de banda que demanda es suficiente, pero para aplicaciones de datos que demandan un ancho de banda considerable, no es suficiente. Para hacer más eficiente el uso de las redes móviles, se emplea la tecnología de paquetes conmutados, donde paquetes de datos individuales son enrutados al usuario, habilitando el canal o canales a ser compartido por varios usuarios.

En términos de implementación el servicio EDGE requiere de hardware adicional (EDGE tranceiver Unit) que será instalado en cada Radiobase, además de la actualización de software para su correcto funcionamiento. La actualización de software en la Radiobase y en la BSC puede ser implementado de manera remota, no necesariamente en los sitios.

Como es de imaginarse la implementación de EDGE requiere de una inversión considerable, pues al agregar hardware adicional a cada Radiobase es necesario el desplazamiento de personal especializado para realizar dicha implementación, por lo que esta actualización se hace por un periodo de tiempo determinado.

Es importante mencionar que tanto GSM, GPRS y EDGE pueden co-existir en la misma red móvil. Pero no todas las terminales móviles soportan los tres servicios de manera conjunta, por lo que es lógico que una terminal GPRS no necesariamente soporte EDGE.

Como se menciono anteriormente la razón por la que EDGE puede manejar mejores tasas de transferencia de datos, es por el tipo de modulación que utiliza. Mientras GPRS utiliza la modulación usada por GSM (GMSK), la cuál limita los canales de radio (Timeslots) a 9.6 Kbps –Si la feature 14400 no esta habilitada-, EDGE utiliza el tipo de modulación 8 PSK. 8 PSK (8 Phase Shift Keying) es un tipo de modulación donde pueden ser usados 8 estados de fase. La ventaja es que puede transmitir datos a tasas de transferencia mayores, pero el problema que tiene es que no es totalmente inmune al ruido y las interferencias. Y esta es una de las razones por las que EDGE es usualmente adoptado como un servicio temporal, además de que ya existen redes donde se esta probando la tercera generación móvil (WCDMA).

8.5 TERCERA GENERACION

WIDE CODE DIVISION MULTIPLEXING ACCESS - WCDMA

Debido a la creciente demanda de ancho de banda por parte de los servicios de datos, y a pesar de que la gran mayoría de redes móviles en el mundo se basan en la tecnología de multiplexaje TDMA, los grandes proveedores de tecnología móvil (Ericsson®, Nokia® y algunos otros) han concluido que la tercera generación de telefonía móvil estará basada en una mezcla entre las tecnologías TDMA y CDMA.

WCDMA es la tecnología de acceso de radio que soportara todos los servicios multimedia que estarán disponibles a través de los terminales de 3era Generación. WCDMA soporta eficientemente tasa de datos entre 144 a 512 Kbps para coberturas de áreas amplias y pueden llegar hasta 2Mbps para mayor cobertura local. Esto adicionalmente complementara la amplia cobertura y el roaming internacional de GSM para proveer la capacidad requerida para servicios personales multimedia.
Entre los aspectos técnicos están: soporta protocolo IP, los terminales son menos difícil de fabricar, hace uso de la técnica de duplexación FDD. Utiliza muy eficientemente el espectro de radio disponible mediante la reutilización de cada celda. Los enlaces desde la red de acceso WCDMA y en el núcleo de red GSM utilizan el más reciente protocolo de transmisión ATM de mini-celdas, conocido como Capa de Adaptación ATM 2 (AAL2). El rango de frecuencia para servicios de área amplia: WCDMA, haciendo uso del acceso FMA2 está entre 1920 a 1980 y de 2110 a 2170 MHz. WCDMA usa una tasa de chip de 4.096 Mcps. Entre los últimos estudios sobre WCDMA están: Cancelación de Interferencia, Cancelación de Interferencia Gradual, Gerencia de Recurso Dinámico en Sistemas Multimedia Inalámbricos, Técnicas de Codificación, entre otros.

8.5.1 Aspectos Técnicos de WCDMA:

WCDMA ofrece flexibilidad en los servicios, combinando conmutación de paquetes y conmutación de circuitos en el mismo canal con un promedio de velocidad entre 8 Kbps hasta 2 Mbps.
Utiliza muy eficientemente el espectro de radio disponible, mediante la reutilización de cada celda, la cual requiere de 2 a 5 MHz por cada capa, lo que quiere decir que una red necesitará de 2 a 15 MHz, en un espectro común de banda de 2GHz.
Los terminales WCDMA son menos difíciles de fabricar, debido a que requieren muy poca señal de procesamiento, ayudando a mantener bajo costos en los terminales.
WCDMA soporta conectividad IP (Internet Protocol), permitiendo accesos más rápidos en Internet. La natural sinergia entre las comunicaciones móviles y el acceso a Internet, ha estimulado que estas sean integradas. La tecnología fundamental sobre la cual trabaja IP es Conmutación de Paquetes. El camino para la evolución de GSM hacia WCDMA, incluye un estado denominado GPRS (General Packet Radio Service) que provee conmutación de paquetes hasta 115 Kbps.

Los enlaces desde la red de acceso WCDMA y el núcleo de red GSM utilizan el más reciente protocolo de transmisión ATM de mini-celdas, conocido como Capa de Adaptación ATM 2 (AAL2). Esta es la forma más eficiente de manejar paquetes de datos incrementando la capacidad de un estándar. Con ATM 2 las líneas E1/T1 pueden manejar aproximadamente 300 conexiones de voz, comparado con 30 de las redes de hoy. Los ahorros por costos de transmisión, están en el orden del 50 %.

El nuevo estándar WCDMA utiliza canales de radio con un ancho de banda de 5 MHz y hace una utilización muy eficiente del espectro radioeléctrico consiguiendo alcanzar un flujo de datos de hasta 2 Mbps en áreas locales, que queda reducido a 384 kbps en áreas de gran extensión, un valor aún muy superior a los 9,6 Kbps actuales que se alcanzan en GSM o incluso a los 115 Kbps que se estima debe alcanzar la red GPRS.
El concepto de WCDMA está basado en una nueva estructura de canales en todas las capas (L1 – L3) construido sobre tecnología como canales de paquete de datos y servicio de multiplexación. Esta tecnología incluye símbolos pilotos y estructura de ranuras de tiempo.

La tecnología de Tercera Generación establece para sus sistemas, el uso de los denominados FRAMES (Future Radio Wideband Multiple Access Systems), estos son Sistemas de Acceso Múltiple para Futuro Radio de Banda Ancha, los cuales trabajan con dos tipos de acceso:
FMA 1: TDMA Banda Ancha con o sin esparcimiento, con un espaciado de la portadora de 1.6 MHz
FMA 2: WCDMA, con espaciado de la portadora de 4.4. a 5.0 MHz.
El objetivo general de los FRAMES es definir una especificación de una interfaz de aire de acceso múltiple UMTS (WCDMA), la cual servirá como un inicio para el proceso de estandarización del UMTS y tomar toda la compatibilidad de aspectos anteriores para su consideración dentro de GMS/DCS.
Los FRAMES están estructurados en dos núcleos de tareas principales:

El núcleo de sistemas de tareas (CTSYS), el cual dirige las especificaciones del sistema, las cuales incluyen los requerimientos y la síntesis en el orden de enlace con operadoras UMTS potenciales. Adicionalmente este núcleo define la interfaz de aire, funciones de la red de aire e implicaciones en las redes de acceso.

El núcleo demostrador de tareas (CTDEMO) se encarga del diseño e implementación de los demostradores basados en especificaciones de trabajo hechos por el núcleo CTSYS. Un enlace externo y la estandarización de páginas de trabajo forman la interfaz hacia los demás proyectos ACTS, de manera de definir interfaces comunes para pruebas de sistemas.

Para la interfaz de aire WCDMA, el ETSI (European Telecommunications Standards Institute), establece el uso de la técnica de duplexación, distribuidas según las bandas de frecuencia de la siguiente manera:

- WCDMA: FDD (Frecuency Division Duplexing), para operación en bandas de frecuencia pares. El FDD, provee dos bandas distintas de frecuencias por cada usuario. La banda delantera provee el trafico desde la estación de base hacia el móvil y la banda reversa provee el trafico desde el móvil hacia la base.
- TD/CDMA: TDD (Time Division Duplexing), para operación en bandas de frecuencia impares. El TDD utiliza tiempo en vez de frecuencia para proveer tanto los enlaces delantero como hacia atrás, provee dos ranuras de tiempo simplex en la misma frecuencia.

Se ha considerado los distintos acercamientos a los sistemas de banda ancha de Tercera Generación, especialmente los propuestos TD/CDMA y WCDMA. En virtud del espectro y la frecuencia las consideraciones compartidas son más críticas a mayor densidad de usuarios. Para los ambientes urbanos TD/CDMA, podría ser la opción preferida en ambientes de microceldas, mientras que WCDMA, podría proveer cobertura de macroceldas. TD/CDMA, podría ser usado para servicios asimétricos, tales como acceso a internet debido a un buen aspecto de la duplexación por división de tiempo (TDD) el cual permite que se pueda ajustar el radio de cuanto espectro será usado para envío (uplink) y recepción (downlink) de información.

El rango de frecuencia para servicios de área amplia: WCDMA, haciendo uso del acceso FMA2 es:

- 1920 a 1980 MHz (uplink)
- 2110 a 2170 MHz (downlink)

El rango de frecuencia para internos o privados: TD/CDMA, haciendo uso del acceso FMA1 es:

- 1900 a 1920 MHz
- 2100 a 2025 MHz

Objetivos del acceso FMA2 de WCDMA:

- Soporta alta velocidad de datos (mayor a 384 kbps en cobertura de área amplia y hasta 2mbps para cobertura local o interna.
- Alta flexibilidad con soporte de servicios múltiples paralelos de tasa variable en cada conexión.
- Acceso eficiente de paquetes
- Alta capacidad inicial y cobertura con soporte interno instalado para futura capacidad, albergando tecnologías mejoradas, tales como las antenas inteligentes y las estructuras de receptores avanzados.
- Soporte para entrega interfrecuencia por operaciones con estructuras de celdas jerárquicas.

- Fácil implementación de terminales de modo dual UMTS/GSM, así como entrega entre UMTS y GSM.

Características técnicas de la interfaz de radio WCDMA:

Tasa básica de chip de 4.096 Mcps con espaciado de portadora desde 4.4 a 5 MHz dependiendo del escenario o situación.

Espaciado múltiple de la portadora de 200 KHz para la capacidad de la Segunda Generación (2G).

- Más altas tasa de chip con 8.192 y 16.384 Mcps.
- Tasa variable de esparcimiento para ambas direcciones
- Bajas y medias tasas de bit con un código simple
- Altas tasas de bit con soluciones multicódigo
- Detección coherente en ambos enlaces: hacia arriba y hacia abajo
- Longitud de la trama de 10 milisegundos (ms)
- Operación asíncrona
- Códigos cortos de esparcimiento y dispersación con códigos opcionales largos en el uplink
- Esparcimiento híbrido (factor variable de esparcimiento más multicódigo) para soportar transmisión a tasa variable
- Soporte flexible para servicios de tasa variable
- Separación de datos en la capa 1 y control en diferentes canales físicos
- Tasa de información explícita
- Rápido control de energía para ambos enlaces: hacia arriba y hacia abajo

8.5.2 Elementos de la Red WCDMA

Los elementos principales de la red WCDMA (UMTS) se basan en la combinación de elementos de la red de conmutación de circuitos usados por GSM y elementos de la red de paquetes conmutados empleados por la red GPRS y EDGE. Por ende el núcleo (Core) de la red WCDMA se divide en el dominio de circuitos conmutados y en el dominio de paquetes conmutados. Los elementos principales del dominio de circuitos conmutados son la Central Telefónica y el VLR, y los elementos principales del dominio de paquetes conmutados son el SGSN y el GGSN. El HLR es un elemento que comparten ambos dominios, por lo cuál no es considerado dentro de ninguno de los dos dominios.

El modo de Transferencia Asíncrono (ATM) es especificado para la transmisión entre los elementos del núcleo (Core). La arquitectura del núcleo de la red puede cambiar cuando nuevos servicios y nuevas opciones (features) son implementadas. El número Portátil de la Base de Datos (NPDB – Number Portability DataBase) será usado para habilitar al suscriptor para cambiar de proveedor de servicio manteniendo el mismo número telefónico. El Gateway de Locación de Registro (GLR – Gateway Locator Register) podrá ser utilizado para optimizar el manejo del suscriptor entre los límites de la red. La central Telefónica, el VLR y el SGSN pueden ser considerados como el núcleo (Core) de la red WCDMA (UMTS).

La capa física de WCDMA es totalmente diferente de la empleada por GSM. Esta emplea un espectro de transmisión de radio más de la forma de CDMA que de TDMA. Además también usa diferentes frecuencias que GSM.

8.5.3 Frecuencias

Existen seis bandas de frecuencia especificadas para WCDMA (UMTS), aunque la operación en otras frecuencias no es imposible. Sin embargo el enfoque de frecuencia para UMTS se aloja alrededor de los 2 GHz. En la conferencia mundial de Administración de Bandas de Frecuencia que se llevo a cabo en 1992, las bandas 1885-2025 y 2110-2200 MHz fueron reservadas para uso de sistemas de banda ancha a nivel mundial por parte de quienes querían implementar Telecomunicaciones móviles a nivel global (IMT-2000). El propósito fue que reservando espectro radioeléctrico para sistemas de banda ancha facilitaría el uso del servicio de Roaming para WCDMA (UMTS).

Dentro de estas bandas las porciones han sido reservadas para diferentes usos:

1920-1980 y 2110-2170 MHz Duplexaje por División de Frecuencia (FDD-Frecuency Division Duplex , WCDMA), respectivamente para envío (Uplink) y recepción (Downlink), con un espaciamiento de canal de 5 MHz y 200 KHz para raster. Un operador necesita de 3-4 canales (2x15 MHz o 2x20 MHz) para ser capaz de implementar una red de alta capacidad, y por ende de alta velocidad.

1900-1920 y 2010-2025 MHz Duplexaje por División de Tiempo (TDD – Time Division Duplex, TD/CDMA), con un espaciamiento de canal de 5 MHz y un raster de 200 KHz. El envío y recepción de la transmisión no están separados en frecuencia.

1980-2010 y 2170-2200 MHz se ocupan para el envío (Uplink) y la recepción (Downlink) vía satélite. Las frecuencias de la portadora son designadas por el UTRA Absolute Radio Frecuency Channel Number (UARFCN). Este puede ser calculado a partir de:

UARFCN = 5 x (la frecuencia en MHz)

APÉNDICE A

ELEMENTOS DE UNA RED CELULAR

Apéndice A Elementos de una Red Celular

La Central Telefónica

La central telefónica se encarga de las funciones de conmutación de circuitos en la red GSM. Controla las llamadas "a y desde" otros sistemas telefónicos además de algunas llamadas de datos, como la Red Telefónica Pública Conmutada (PSTN – Public Switch Telephone Network), la Red Digital de Servicios Integrados (ISDN – Integrated Service Digital Network), la Red Pública Móvil (PLMN – Public Land Mobile Network), la Red Pública de Datos (PDN – Public Data Network) y hasta puede llegar a controlar algunas redes privadas.

El área de locación de una Central Telefónica es un grupo de células BSS. El sistema usa las áreas de locación (LA´s) para buscar abonados activos. Una LA es el área en la red donde una terminal móvil (MS) puede moverse sin necesidad de reportar su locación a la red.

Un área de servicio (SA) está conformada por la Central Telefónica y el VLR y agrupa un número de LA´s. El área de servicio (SA) es la parte de la red a la cuál da cobertura una Central Telefónica.

Gateway Mobile Services Switching Center GMSC

El Gateway GMSC realiza la conmutación de circuitos entre la red GSM y la red PSTN, que no es otra más que la red Telefónica Fija, entonces, soporta la función de ruteo de llamadas entrantes a la Central Telefónica donde los suscriptores móviles están registrados. Normalmente la Central Telefónica y el VLR están integrados en el mismo nodo.

Sistema Estación Base (Base Station System – BSS)

El sistema estación base (BSS) consiste de una Estación Base Controladora (BSC – Base Station Controller) y de una Estación Base receptora/transmisora (BTS – Base Transceiver Station) mejor conocida como Radiobase. La BTS es el equipo de radio que recibe y transmite información sobre la interfaz aire, y que permite a la BSC comunicarse con las estaciones móviles en su área de servicio. Un grupo de BTS´s es controlado por una BSC.

La BSC provee todas las funciones relativas a el servicio de radio. Además puede establecer, supervisar y desconectar llamadas de circuitos conmutados o de paquetes conmutados; es un switch de alta capacidad que provee funciones que incluyen hand-off, configuración de datos en la célula y asignación de canales de radio. Una o varias BSC´s trabajan para una central telefónica, y varias BTS´s trabajan para una BSC.

Existen dos tipos de BSC´s la Stand Alone y la TRC, la diferencia es que una BSC Stand solo puede manejar Radiobases (BTS´s) y la BSC TRC puede manejar otras BSC Stand Alone ademas de que puede manejar Radiobases (BTS´s).

La BTS separa las llamadas de circuitos conmutados de la de paquetes conmutados antes de que lleguen a la BSC, quien a su vez envía las llamadas de circuitos conmutados a la Central Telefónica / HLR y las llamada de paquetes conmutados a el SGSN. Protocolos GSM estándar son usados con la BSC para alcanzar la compatibilidad deseada.

Home Locator Register HLR

El HLR es la base de datos que almacena la información personal de cada uno de los suscriptores de la red GSM / GPRS. El HLR almacena información de la comunicación de la red de circuitos conmutados y de la de paquetes conmutados. La información que almacena el HLR incluye, por ejemplo, servicio suplementarios, parámetros de autenticación, Nombres de Punto de Acceso (APN – Access Point Name) como la suscripción de Proveedor de Servicios de Internet así como una dirección IP estática es alojada para las terminales móviles (MS).

Visitor Locator Register VLR

El VLR es una base de datos que contiene información sobre todas las terminales móviles que se encuentran en un área de locación LA de la Central Telefónica o en el área de ruteo del SGSN, respectivamente.

El VLR contiene la información del suscriptor que la central Telefónica o el SGSN necesitan para proveer el servicio correspondiente a los suscriptores, solo que esta información es temporal mientras el suscriptor se mantiene dentro de el área de servicio de la Central Telefónica o del SGSN.

Cuando una terminal móvil cambia del área de locación de la Central Telefónica o de el área de ruteo del SGSN, el VLR de la Central Telefónica o del SGSN solicita información al HLR sobre la terminal móvil, la cuál almacenara temporalmente mientras la terminal móvil se mantenga dentro del área de locación de la central o del área de ruteo del SGSN. Si la terminal móvil hace una llamada ya en la nueva área de locación o área de ruteo, la información necesaria para dicha llamada ya se encuentra disponible de manera inmediata en el VLR. Es fácil entender la importancia del VLR, de hecho sin el VLR la telefonía móvil seria algo prácticamente imposible, pues quien identifica la ubicación de los abonados en la red es precisamente el VLR.

Equipment Identity Register EIR

El Registro de Identidad de equipo EIR es una base de datos que mantiene la información de identidad de las terminales móviles, el cual ayuda a bloquear llamadas de terminales móviles que se han reportado robadas, sin autorización o defectuosas.

Authentication Center AuC

El centro de Autenticación es una entidad especificada en el estándar GSM que provee las herramientas tecnológicas necesarias para autenticar y cifrar procesos utilizados internamente en las redes GSM. La autenticación tanto para usuarios GPRS como GSM es la misma. El cambio en seguridad para GPRS es solo relacionado al cifrado, y cuando se agrega el servicio GPRS a una red GSM no se requiere ninguna actualización en el AUC.

Operation Support-System OSS

Para el manejo de las redes móviles existe una herramienta llamada Sistema de Operación y Soporte (OSS). El OSS incluye aplicaciones para la supervisión, configuración y manejo de desempeño en redes móviles. En suma a las aplicaciones de manejo de la red móviles, el OSS provee funciones básicas, por ejemplo, manejo de alarmas y transferencia de archivos.

WCDMA Radio Access Network RAN

El sistema de acceso de radio para redes WCDMA, consiste de dos elementos fundamentales, el Controlador de Canales de Radio (RNC – Radio Network Controller) y el Nodo B. El Nodo B maneja la interfaz aire de los canales de radio, es el equivalente a la Radiobase (BTS) en sistemas GSM. El RNC provee todas las funciones relacionadas al manejo de los canales de Radio, y es el equivalente a la BSC en GSM; el RNC puede establecer, supervisar y desconectar llamadas tanto de circuitos conmutados como de paquetes conmutados.

Domain Name Server DNS

El Servidor de Nombres de Dominio DNS maneja una base de datos, la cual contiene un mapeo entre el nombre de las redes de datos externas y las direcciones IP del GGSN permitiendo el acceso a dichas redes.

Billing Gateway BGw

El Gateway de cobro es el encargado de recibir toda la información referente a tiempos y tipos de llamadas, para poder generar los recibos de cobro del servicio telefónico; ademas facilita la introducción del servicio GPRS en una red Móvil, ofreciendo funciones que simplifican el manejo del cargo por el servicio GPRS en los sistemas de cobro.

Short Message Service-Interworking MSC (SMS-IWMSC)

El SMS-IWMSC permite a las terminales móviles recibir los SMS. Y ademas de ser usado en las redes GSM/GPRS, también será utilizado en las redes WCDMA.

Short Message Service Gateway MSC (SMS-GMSC)

El SMS-GMSC permite originar los SMS. Y ademas de ser usado en las redes GSM/GPRS también será utilizado en las redes WCDMA.

Packet Exchange Manager (PXM)

La interfaz de usuario PXM se basa en un Navegador WEB y un ambiente Java instalado en una plataforma UNIX o Windows, y es una aplicación implementada en el nodo GSN. Esto significa que las páginas HTML (Hyper Text Mark-up Language) y los Applets de Java, interpretadas con éste Navegador WEB, son guardadas en el nodo. Las páginas son transferidas sobre TCP/IP en el Backbone IP. Todas las actividades concernientes a la Operación y Mantenimiento (O&M) relativas al GSN son manejadas a través de ésta Interfaz Gráfica de Usuario (GUI) basada en Java.

8 Phase Shift Keying 8PSK

Esta es una técnica de modulación en la cuál la portadora puede existir en cualquiera de los 8 diferentes estados. Cada estado representa 3 bit´s desde 000 hasta 111. También se le llama algoritmo de modulación de fase; PSK se refiere a la separación que existe entre la fases. PSK es una forma de modulación de fase la cuál se logra por el uso de un discreto número de estados; por lo que 8PSK se refiere a PSK con 8 estados.

GSM Minimum Shift Keying GMSK

MSK es un tipo especial de esquema de modulación FSK ("Frecuency Shift Keying"), con fase continua y un índice de modulación de 0.5. El índice de modulación de una señal FSK es similar al de FM, y se define por kFSK= (2D F)/Rb, donde 2D F es el desplazamiento en frecuencia de pico a pico y

Rb es el bit rate. Un índice de modulación de 0.5 se corresponde con el mínimo espacio en frecuencia que permite que dos señales FSK sean ortogonales coherentes, y el nombre MSK significa la mínima separación en frecuencia que permite una detección ortogonal.

MSK es una modulación espectralmente eficiente. Posee propiedades como envolvente constante, eficiencia espectral, buena respuesta ante los errores de bits, y capacidad de auto sincronización.

GMSK es un esquema de modulación binaria simple que se puede ver como derivado de MSK. En GMSK, los lóbulos laterales del espectro de una señal MSK se reducen pasando los datos modulantes a través de un filtro Gaussiano de pre-modulación. El filtro Gaussiano aplana la trayectoria de fase de la señal MSK y por lo tanto, estabiliza las variaciones de la frecuencia instantánea a través del tiempo. Esto tiene el efecto de reducir considerablemente los niveles de los lóbulos laterales en el espectro transmitido.

El filtrado convierte cada dato modulante que ocupa en banda base un período de tiempo T, en una respuesta donde cada símbolo ocupa varios períodos. Sin embargo, dado que esta conformación de pulsos no cambia el modelo de la trayectoria de la fase, GMSK se puede detectar coherentemente como una señal MSK, o no coherentemente como una señal simple FSK. En la práctica, GMSK es muy atractiva por su excelente eficiencia de potencia y espectro.

Tipos de Hand-Off

El procedimiento llamado "Hand-Off", se realiza cuando una terminal móvil se encuentra en movimiento, lo que significa que dicha terminal cambiara su posición física en una zona determinada; existen 4 tipos de Hand-Off fundamentales, que se explicaran a continuación.

1. Hand-Off Inter-Sectorial.- Este hand-off se realiza cuando una terminal cambia de un sector de la Antena a otro sector de la misma Antena, podría ser por ejemplo que una terminal pase del sector A al sector B de la misma Antena; éste tipo de hand-off Inter-sectorial solo puede efectuarse en una Antena, y es controlado exclusivamente por la BSC.
2. Hand-Off Inter-BTS.- Este hand-off se realiza cuando una terminal cambia su cobertura de una Radiobase a otra Radiobase, por ejemplo pasa de la Radiobase 1 a la Radiobase 2, lo que caracteriza a éste hand-off es que ambas Radiobases pertenecen o están conectadas a la misma BSC, que es quien se encarga de controlar el hand-off.
3. Hand-Off Inter-BSC.- En éste tipo de hand-off la terminal cambiara de BSC, o sea que la terminal pasara por ejemplo de la BSC 1 a la BSC 2, y éste hand-off se caracteriza porque ambas BSC pertenecen o están conectadas a la misma Central Telefónica, que es quien junto con las BSC involucradas controla dicho hand-off.
4. Hand-Off Inter-Centrales.- En éste hand-off la terminal cambiará de Central telefónica, por ejemplo pasará de la CT1 a la CT2, y en éste caso el hand-off estará controlado por las Centrales telefónicas involucradas y por las respectivas BSC involucradas.

Para una mejor apreciación de éste procedimiento ver el diagrama "TIPOS DE HAND-OFF", al final de éste apéndice.

SIM CARD

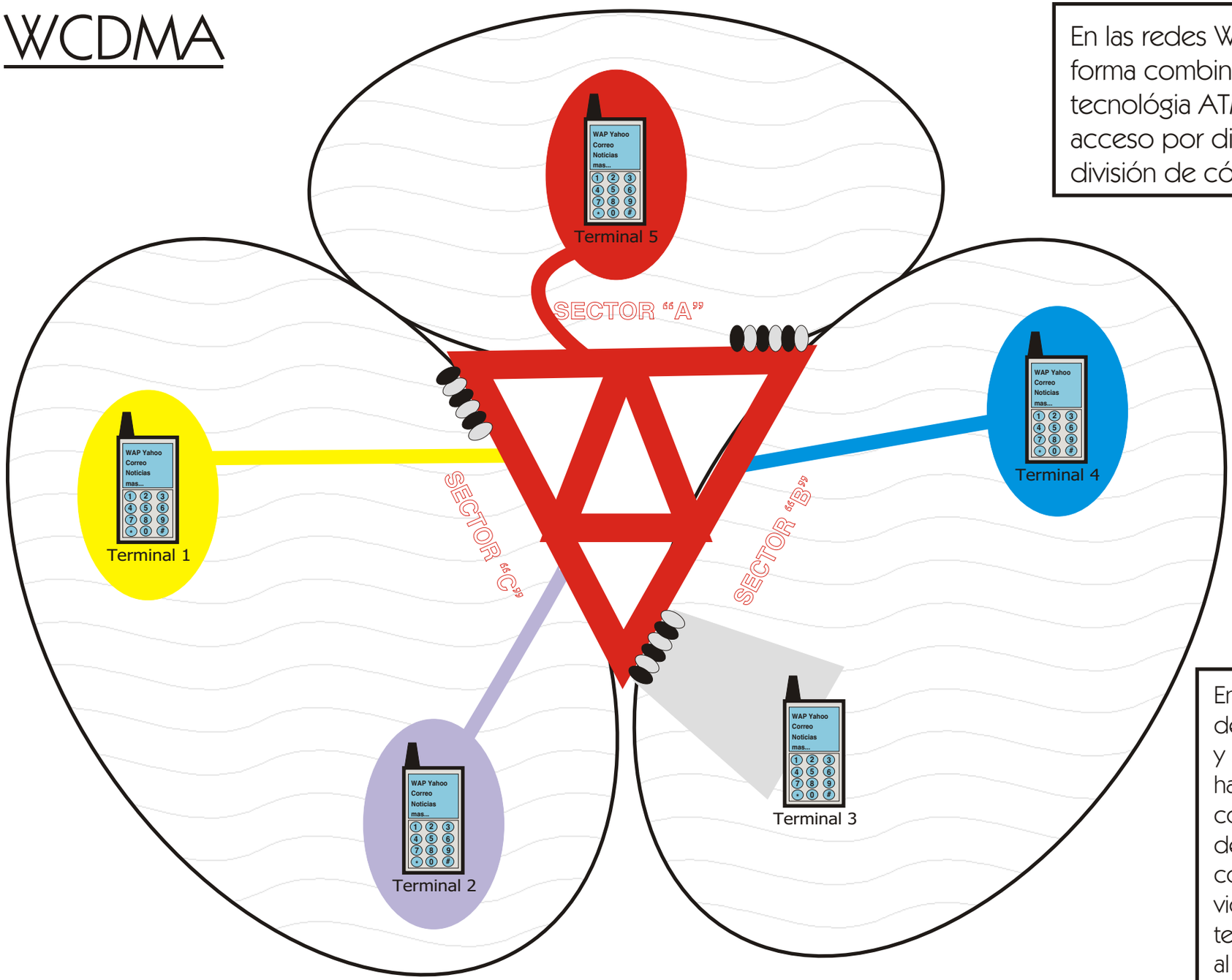
El modulo SIM card (Suscriber Identity Module) esta formada por un microprocesador, y tres memorias del tipo ROM, EEPROM y RAM de diferentes capacidades según sea el fabricante, en las que se encuentran almacenados principalmente:

- IMSI – International Mobile Suscriber Identity éste número es el que se almacena en el HLR, y consta de información relativa al código móvil del país, el código de la red móvil, el código del HLR y el número de serie de la tarjeta SIM card; éste IMSI es al que se asigna un número de abonado, ademas de las categorías de HLR (SMS, GPRS, CSD, etc).
- Nombres y números de teléfono.
- Mensajes SMS recibidos.
- Nombres y números restringidos
- Códigos y algoritmos de autenticación.

La SIM cuenta con un código de seguridad de acceso llamado PIN 1 el cuál esta formado por 4 dígitos y sirve para proteger la terminal del uso de terceros, en caso de que el código PIN 1 sea introducido de forma errónea 5 veces la SIM card se bloquea y la única forma de desbloquearla es por medio de otro código denominado PUK 1; el código PUK 1 sirve para desbloquear la SIM card y consta de 8 dígitos, pero si el código PUK 1 se introduce de forma errónea 10 veces la SIM card quedara bloqueada de manera indefinida. También existe el PIN 2 que sirve para activar la marcación fija, el control de costo y algunas otras restricciones; cabe mencionar que el PIN 2 se comporta de la misma forma que el PIN 1, se bloqueara a los 5 intentos y también existe un PUK 2 para desbloquear el PIN 2, que a los 10 intentos erróneos bloqueara la SIM de manera indefinida.

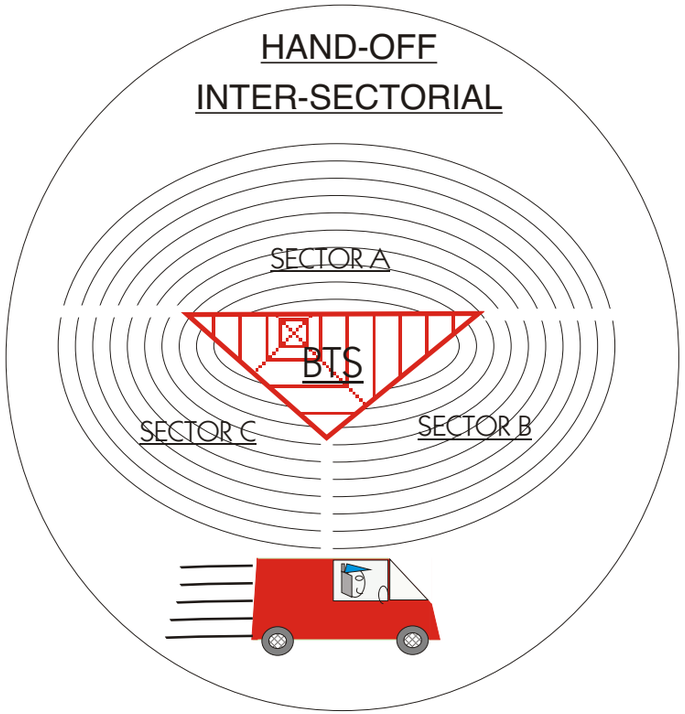
WCDMA

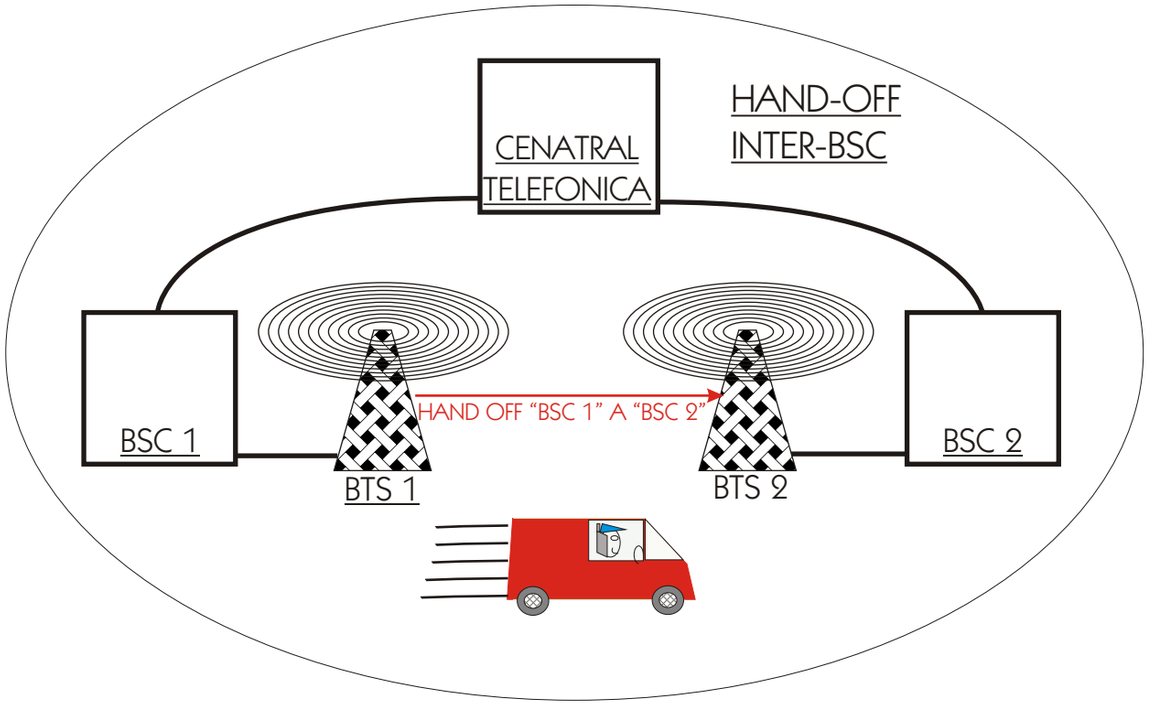
En las redes WCDMA el ancho de Banda se maneja de forma combinada, esto es debido a que se utiliza la tecnológia ATM2, la cuál permite la combinación entre acceso por división de tiempo (TDMA) y acceso por división de código (CDMA).

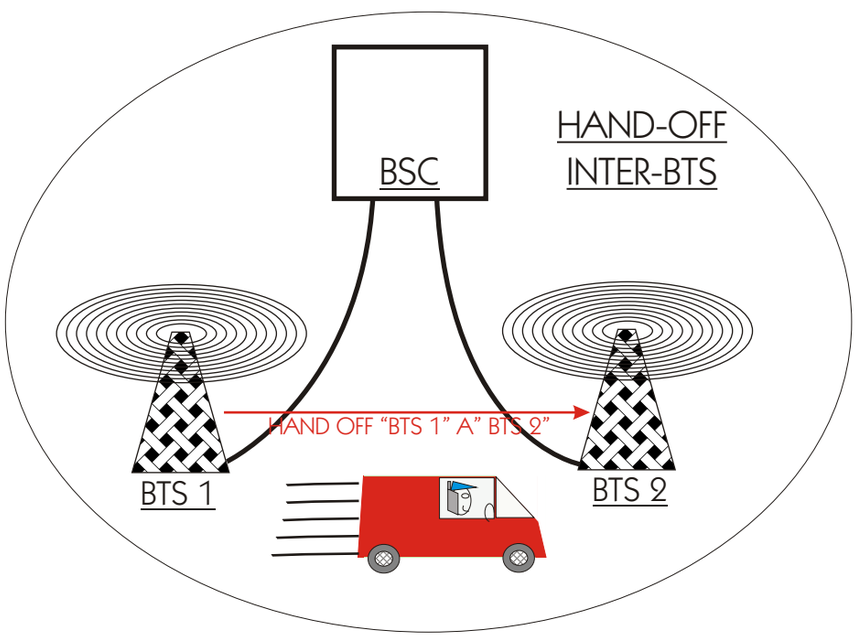


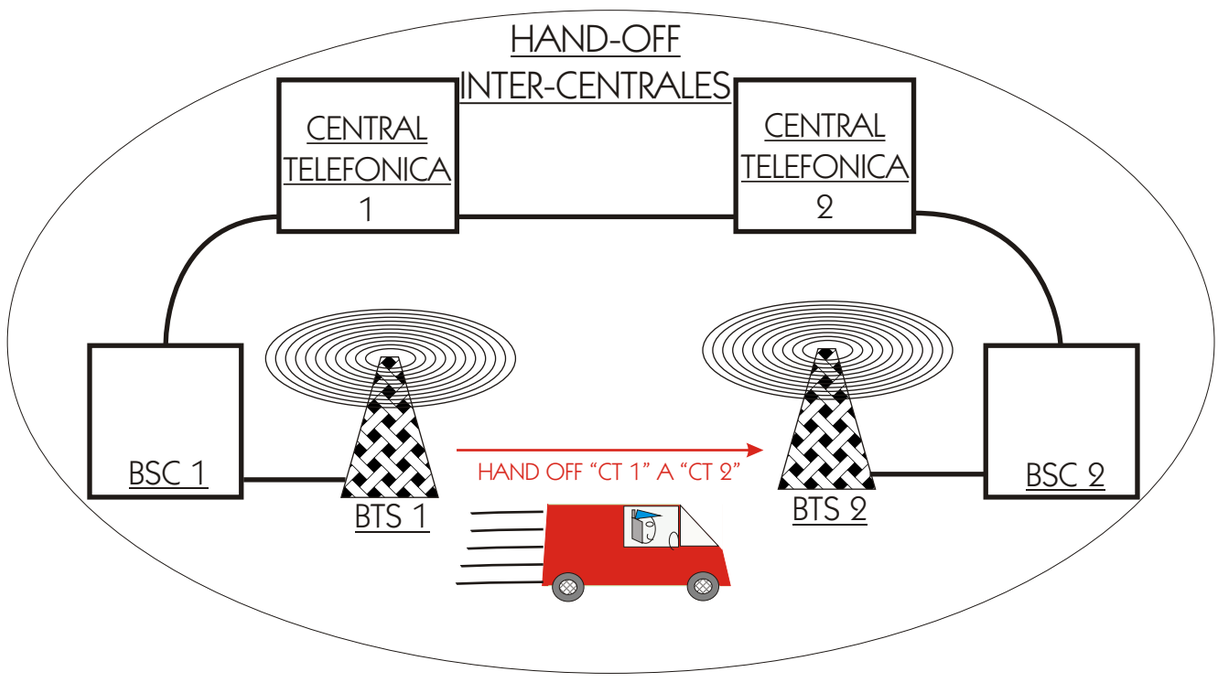
En la figura se busca ejemplificar la combinación de tecnologías de acceso; las terminales 1,2,4 y 5 comparten el ancho de banda total como se hace en CDMA y lo que las diferencia es su código; pero la terminal 3 solicito un enlace dedicado, por lo que se le asignanTimeslots como en TDMA para lo que podria ser una videoconferencia.En el momento en que la terminal 3 concluya su videoconferencia,volvera al esquema de ráfagas de información o dicho de otra forma a CDMA.

TIPOS DE HAND-OFF









La tendencia de las telecomunicaciones en México y el mundo va enfocada en dos sentidos, primero hay que hablar de la convergencia tecnológica de los servicios de voz, datos y entretenimiento (TV y Radio), que dentro de muy poco tiempo serán ya una realidad, y segundo se debe hablar de las ya muy extendidas redes inalámbricas, dentro de las cuales se encuentra la telefonía celular.

Dentro del tema de la convergencia tecnológica es importante señalar a los proveedores de servicio que están preparados para afrontarla, y en ese sentido se debe decir que las redes celulares aunque están un poco en desventaja con respecto a los proveedores de servicio telefónico fijo, a los proveedores de TV por cable y a las redes WiFi, mantienen el desarrollo en nuevos servicios de transmisión de datos como High Speed Downlink Packet Access (Recepción de paquetes de datos a alta velocidad) que promete alcanzar velocidades de hasta 14 Mbps y High Speed Uplink Packet Access (Envío de paquetes de datos a alta velocidad) que prometen aumentar considerablemente la velocidad de envío de información, por lo que en el rubro de la convergencia tecnológica es altamente probable que las tecnologías de servicio celular den una gran batalla a las redes WiFi y quizá hasta a los proveedores de TV por cable quienes en éste momento llevan una gran ventaja a sus competidores en lo que a convergencia se refiere.

En el rubro de redes inalámbricas es un caso distinto, pues quienes tienen una gran cobertura inalámbrica de servicio de voz y datos son precisamente los proveedores de comunicaciones celulares, por lo que en éste rubro (y con mayor razón si funciona correctamente HSDPA y HSUPA) dichos proveedores serán los rivales a vencer, aunque las redes WiFi se encuentran también en constante evolución, por lo que se prevé una dura batalla.

Se prevé una alta competencia en el mercado de las telecomunicaciones a principios del año 2008, y como las reglas fundamentales de la sobre vivencia, la tecnología que esté preparada para afrontar dicha competencia, será quien concentre al mayor número de usuarios y quizá será quien sobreviva.

Esperemos que como país México no solo se integre a la modernidad desde la perspectiva del consumo (que parece ser inevitable), sino además como un generador ciencia y tecnología.

Benito Oswaldo Chavero Chávez
Septiembre 2006

BIBLIOGRAFIA:

ELECTRICIDAD Y MAGNETISMO
Jaramillo / Alvarado
Facultad de Ingeniería UNAM

INTRODUCCION A LAS REDES DE AREA LOCAL
Jorge E. Rodríguez G.
Mc GRAW HILL

REDES DE ORDENADORES
Andrew S. Tanembaum
PRENTICE HALL

TCP/IP
Sidnie Feit
OSBORNE-Mc GRAW HILL

LA HISTORIA DE ERICSSON
John Meurling / Richard Jeans
ERICSSON TELECOM

INTRODUCCION A LOS SISTEMAS DE TELECOMUNICACIONES
P.H. Smale
TRILLAS

Unified Messaging UM (SMS, EMS y MMS)
Curso en Ericsson Telecom
www.palowireless.com/sms/tutorials.asp

CSD, HSCSD y GPRS
Cursos en Ericsson Telecom

REFERENCIAS

EDGE y WCDMA
www.iec.org
www.protocols.com/pbook/umts.htm
www.cdg.org/
www.3gamericas.org/spanish/technology_center/umts_sp.cfm
www.mobile-phone-directory.org/Glossary/D/D-AMPS.html
www.mobile-phone-directory.org/

Además de la experiencia adquirida durante mi estancia laboral en la empresa Ericsson Telecom, en la cuál colabore activamente en la implementación de la red GSM para el proveedor de servicios celulares Telcel; y tuve directamente bajo mi cargo la integración de dos proyectos para dicha red: CSD / HSCSD y SMS / MMS, Además -y aunque no como responsable directo-, también colabore en otros proyectos como GPRS, VMS y las pruebas del Switch (Central Telefónica).

GLOSARIO

AMPS	Advanced Mobile Phone System – Sistema Telefónico Móvil Avanzado
ANSI	American National Standards Institute – Instituto Estadounidense de Estándares
Applets	Aplicaciones implementadas por medio del lenguaje de programación Java que se cargan desde un servidor y se ejecutan en la maquina cliente; y que son considerados mecanismos de seguridad que limitan el acceso a recursos de las máquinas donde se ejecutan.
Åsdal	Carl-Gösta Åsdal; Ingeniero en jefe del sistema Sueco de Radiotelecomunicaciones
AT&T	American Telephone & Telegraph – Teléfonos y Telégrafos Estadounidenses
ATM2	Asynchronous Transfer Mode Versión 2 también conocido como AAL2 – Modo de Transferencia Asíncrono versión 2
AWG	American Wire Gauge, estándar de cables y alambres en función de su diámetro y área.
AXE	Sistema de Conmutación digital de la empresa Ericsson®, usado tanto en redes fijas como en redes móviles. Hoy día considerado una plataforma de comunicaciones.
AuC	Authentication Center – Centro de Autenticación
Bellcore	Bell Communications Research - Centro de Investigación en Comunicaciones Bell
Bell System	Sistema de Telefonía de AT&T
Bearer Capability	Elemento de información de las redes ISDN usado para describir los servicios de portadora como el rango de datos (data rate) y la calidad de voz requeridos por un usuario.
Bit-robbing	Es un tipo especifico de señalización por canal asociado (CAS) usado por las portadoras "T1".
Bluetooth	Estándar inalámbrico desarrollado por la empresa Ericsson y que debe su nombre a un rey Vikingo
BOOTP	Protocolo de arranque de red en TCP/IP
BSC	Base Station Controller – Controlador de Estaciones Base
BT	British Telecommunications Group plc. – Grupo Británico de Telecomunicaciones
BTS	Base Transceiver Station – Estación base Transmisora / Receptora
CAP II	Computer Access Protocol no. 2- Protocolo de Acceso de Cómputo No. 2
CCITT	Comité Consultivo Internacional Telegráfico y Telefónico

CDR´s	Registros generados por la central telefónica que contienen la información necesaria de una llamada y que son empleados por el sistema Billing Gateway para poder cobrar el servicio celular, además los CDR´s pueden servir para resolver problemas en la red.
CDMA	Code Division Multiplexing Access – Multiplexaje por División de Código
CHIP-50	Chip desarrollado por la empresa Qualcomm que mejora la transmisión y desempeño de su generación Chipset 3000 para CDMA.
CSD	Circuit Switch Data – Comunicación de Datos por Circuitos Conmutados
CSMA/CD	Carrier Sense Multiple Access with Collision Detection – Tecnología empleada por Ethernet para acceder al medio de transmisión / recepción de información.
D-AMPS	Digital - Advanced Mobile Phone System – Sistema Telefónico Móvil Avanzado Digital
DCE	Data Circuit Equipment – Equipo de Comunicación de Datos
DTE	Data Terminal Equipment – Terminal de Datos
EDGE	Enhanced Data rate for GSM Evolution – Rango Mejorado de Datos para la Evolución de GSM.
EIR	Equipment Identity Register – Registro de Identidad de Equipos
EMS	Enhanced Message Service – Servicio de Mensajería Mejorado
FCC	Federal Communications Comisión – Comisión Federal de Comunicaciones
FDD	Frecuency Division Duplex – División de Frecuencia Doble
FDMA	Frecuency Division Multiplexing Access – Multiplexaje por División de Frecuencia
FMA2	Frames Multiple Access, Second Versión – Acceso Múltiple a Tramas Versión 2
FTP	File Transfer Protocol - Protocolo de Transferencia de Archivos
GE	General Electric
GMSC	Gateway Mobile Services Switching Center – Centro de Conmutación Móvil
GPO	General Post Office – Oficina de Correos
GPRS	General Packet Radio Service – Servicio General de Paquetes de Datos por Radio
GSN	Nombre que se da al conjunto de elementos SGSN y GGSN en la red GPRS.
Hand Off	Intercambio de llamadas entre elementos de la red GSM y WCDMA.
Hissing	Ruido escuchado durante una llamada telefónica parecido a un silbido.
HSCSD	High Speed Circuit Switch Data – Comunicación de Datos por Circuitos Conmutados de Alta Velocidad

HLR	Home Locator Register – Registro de Usuarios de red Móvil
HTML	HyperText Markup Language – Lenguaje de Marcas de Hipertexto
HTTP	Hypertext Transfer Protocol – Protocolo de Transferencia de Hipertexto
IEEE	Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos
IETF	Internet Engineering Task Force – Grupo de Ingenieros que coordinan las diferentes actividades de Internet
IMTS	Improved Mobile Telephone System – Sistema Telefónico Móvil Mejorado
IP	Internet Protocol – Protocolo de Internet
ISO	International Standard Onganization – Organización Internacional de Estándares
ISUP	Integrated Services Digital Network User Part – Usuario Parte Red Digital de Servicios Integrados
ITU-T	International Telecommunication Union-Standarization Sector – Sector de Normalización de las Telecomunicaciones
Java	Lenguaje de programación orientado a objetos creado por la empresa Sun Microsystems.
LAN	Local Area Network – Red de Área Local
LLC	Logic Link Control – Control de Enlace Lógico
MAC	Medium Access Control – Control de Acceso al Medio
MAN	Metropolitan Area Network – Red de Área Metropolitana
Máseres	Líneas espectrales. Maser "Microwave Amplification by Stimulated Emission of Radiation". El mecanismo de emisión máser es idéntico al del láser, pero con microondas en lugar de luz visible.
Millicom	Empresa Estadounidense de telefonía móvil, que conjuntamente con la británica Racal constituyo la empresa Vodafone en el Reino Unido.
MMS	Multimedia Message Service – Servicio de Mensajes Multimedia
MoU	Minutes Of Use – Minutos de Uso
MSC	Mobile Switching Center - Centro de Conmutación Móvil
MTA, MTB, MTC	Las primeras redes de telefonía móvil Sueca no celular.
MTP	Message Transfer Part – La parte de Transferencia de Mensaje
MTS	Mobile Telephone System – Sistema Telefónico Móvil
MTU	Maximum Transmission Unit – Unidad Máxima de Transmisión

NMT	Red analógica de Telefonía Nórdica
NTP	Network Time Protocol – Protocolo de Sincronización de relojes de Red
OAA	Over the Air Activation – Activación sobre la interfaz Aire
OATS	Over the Air Activation Services – Servicios de Activación sobre la Interfaz Aire
OSI	Open System Inteconection –Sistema de Interconexión Abierto
OSS	Operation Support – System – Sistema de Operación y Soporte
OTA	Over The Air Activation – Activación sobre la Interfaz Aire
Paging	Difundir un mensaje a través de una red para localizar un elemento de radio.
PAM	Pulse Amplitud Modulation – Modulación por Amplitud de Pulso
Pathworks	Software utilizado para cálculos de enlaces de microondas.
PBX	Private Branch Exchange – Centralita Telefónica
PCM	Pulse Code Modulation – Modulación por Codificación de Pulso
PDC	Personal Digital Celular – Comunicación Personal Digital Celular
PLMN	Public Land Mobile Network – Red Pública Móvil
PTT	Post Telegraph and Telephone – Servicio Telefónico y Telegráfico Postal
Racal	Empresa Británica de Radiodifusión, que se involucro en la telefonía móvil con el nombre de Vodafone.
RADIUS	Remote Access Dial-In User Server – Servidor de Autenticación de Usuario
Raster	Técnica gráfica que usa arreglos de píxeles
SCCP	Signalling Connection Control Part – La parte de Control de Conexión de Señalización
SMIL	Synchronized Multimedia Integration Language (lenguaje de integración multimedia sincronizada)
SMPP	Short Message peer-to-peer Protocol – Protocolo de Mensajes Cortos Punto a Punto
SMTP	Simple Mail Transfer Protocol – Protocolo Simple de Transferencia de Correo
SMS	Short Message Service – Servicio de Mensajes Cortos
SMS-IW-MSC	Short Message Service – Interworking – Mobile Switching Service Center
SNMP	Simple Network Management Protocol – Protocolo Simple de Manejo de Red
Span/Link	Enlace Redundante
SRA	Svenska Radioaktiebolaget – Empresa Sueca de Radiodifusión

SS7	Signaling System No. 7 – Sistema de Señalización Número 7
TACS	Total Access Communication System – Sistema de Comunicación de Acceso Total
TAP	Telocator Alphanumeric Protocol, reduce tiempos de espera en sistemas alfanuméricos.
Tasa de Chip	Rango de manejo de datos de los microprocesadores en CDMA
TCS	Traffic Control Subsystem – Subsistema de Control de Tráfico
TCP/IP	Transport Control Protocol / Internet Protocol – Protocolo de Control de Transporte / Protocolo de Internet
TDMA	Time Division Multiplexing Access – Multiplexaje por División de Tiempo
TELNET	Terminal Virtual
Teleservicios	Servicios proporcionados por la red GSM para la comunicación de voz.
Televerket	Administrador de correos del estado Sueco, cuyo nombre completo era Telegrafverket.
Timeslot	Ranura de tiempo en que se divide el ancho de banda en la tecnología TDMA, un Timeslot es un canal aire para una llamada de voz o de datos.
UDH	User Data Header – Cabecera de Datos de Usuario
UMTS	Universal Mobile Telecommunicatios System – Sistema Universal de Telecomunicaciones Móvil
URI	Esquema comparable al "Mail to" de internet para el SMS
Viterbi	Andrew Viterbi, creador de la decodificación Viterbi.
VLR	Visitor Locator Register – Registro Temporal de Usuario
WAN	Wide Area Network – Red de Área Extensa
WAP	Wireless Aplication Protocol – Protocolo de Aplicación Inalámbrico
WAP-205-MMS	Wireless Aplication Protocol Versión 2001 para MMS – Protocolo de Aplicación Inalámbrico Versión 2001 para MMS
WCDMA	Wide Code Division Multiplexing Access – Multiplexaje por División de Código Amplio
X.25	Recomendación de la CCITT para las primeras tres capas del modelo OSI en redes públicas.