ESCUELA POLITÉCNICA DEL EJÉRCITO

FACULTAD DE INGENIERÍA ELECTRÓNICA

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA ELECTRÓNICA

ESTUDIO TÉCNICO ECONÓMICO PARA IMPLEMENTAR SOLUCIONES DE ÚLTIMA MILLA DE SERVICIOS DE ISP EN AMBIENTES RESIDENCIALES

DANNY ERNESTO MORALES BRIONES

SANGOLQUÍ – ECUADOR

2006

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado “Estudio Técnico Económico para Implementar Soluciones de Última Milla de Servicios de ISP en Ambientes Residenciales” ha sido desarrollado en su totalidad por el Sr. Danny Ernesto Morales Briones con C.I. 1717057283, bajo nuestra dirección.

Ing. Rodrigo Silva	Ing. Darío Duque
DIRECTOR	CODIRECTOR

AGRADECIMIENTO

Quiero agradecer:

A mis padres, Rosario y Eduardo por acompañarme a lo largo de mi vida, ser mi principal apoyo y por darme siempre su confianza inquebrantable.

A mis hermanos, Diego y David por compartir las experiencias de crecer juntos y ser mis amigos.

A Giovana, por brindarme su paciencia y cariño.

A mis amigos, con los que se han compartido momentos inolvidables y me han ayudado, a aquellos que ya no están y a los de toda la vida.

A la vida, por mostrarme cada día algo nuevo, por permitirme experimentar los matices del amor, amistad, ternura, esperanza, voluntad y libertad, dando color y significado a cada momento vivido.

DEDICATORIA

A ROSARIO Y EDUARDO

Por su amor, confianza, comprensión y por haberme enseñado a ser un mejor hombre.

PRÓLOGO

El deseo de mantenerse comunicado es una característica que distingue al hombre en el presente, un medio en particular a sido capaz de estrechar las distancias y ofrecer comunicaciones tan variadas como eficientes, este es el Internet, que desde sus inicios a mostrado adaptarse a las necesidades actuales, volviéndose en una necesidad para muchos y una herramienta básica para los demás.

Debido a la carencia de redes de datos dentro de las áreas urbanas de nuestro país, el acceso a los servicios que ofrece un ISP han estado limitados para aquellos que pueden pagar los altos costos de un servicio dedicado, o tener acceso a los mismos pero a bajas velocidades, impidiendo aprovechar las ventajas del Internet y retrasando el avance de las comunicaciones en el país.

La vigencia e importancia del presente estudio crece a medida que el uso del Internet se generaliza en nuestro país, convirtiéndose en una necesidad para las personas; motivo por el cual se buscan soluciones que permitan llegar a usuarios residenciales de manera eficiente y a costos accesibles.

El presente proyecto tiene por intención ser una guía para futuras implementaciones de últimas millas, que permitan dar servicios de ISP a sectores residenciales, para lo cual se han llevado a estudio cuatro tecnologías: Ethernet, xDSL, WiFi y WiMAX.

Nuestro estudio se enfoca en sectores residenciales específicos como son edificios de departamentos y conjuntos habitacionales, para llegar a ellos, se tendrán últimas millas hibridas de dos o un tramo dependiendo de la tecnología usada, las cuales abaratan los costos y el tiempo de despliegue; los primeros tramos son inalámbricos, usando sistemas PMP hasta las inmediaciones de los conjuntos o edificios, y desplegando un segundo tramo con las tecnologías Ethernet, xDSL o WiFi hasta el cliente; en el caso WiMAX se cuenta con un solo tramo inalámbrico gracias a las prestaciones de esta tecnología.

CAPITULO I

INTRODUCCIÓN

1.1 DEFINICIÓN DE INTERNET

1.1.1 Introducción

Estimado lector, dentro de las nuevas tendencias tecnológicas que este nuevo siglo nos trae consigo es la globalización, y exactamente el medio que más ha influido en la globalización es el Internet. Conocido también como la red de redes, es una red global que enlaza no solo ciudades y continentes, sino al mundo entero; de tal manera que quien este conectado al Internet, podrá mantener comunicación con todo posible usuario, en cualquier parte del mundo, que también posea dicha conexión.

Internet, como ya se ha citado previamente es una red de computadoras de extensión global, esta red nos permite transmitir datos, lo que significa que podemos fácilmente enviar documentos, fotos, videos, voz y cualquier otro tipo de información que se presente en forma digital; es precisamente esta gran flexibilidad la que ha hecho posible la expansión del Internet de una forma cada vez mayor a lo largo del planeta.

Debemos también hacer referencia al protocolo que permite a esta red funcionar, este lenguaje es el TCP/IP; es un protocolo compuesto, el primero TCP que significa Transmission Control Protocol; o, en español Protocolo de Control de Transmisión, que es el encargado de establecer conexión entre dos terminales y a su vez garantiza la entrega de la información y su correcto orden; el segundo IP que significa Internet Protocol; o, en español Protocolo de Internet, este protocolo se encarga de establecer en origen y el

destino de los datos a ser transmitidos sin preocuparse del contenido o fiabilidad de lo enviado.

1.1.2 Breve Historia del Internet

El Internet tiene sus inicios a finales de la década de los sesentas, es en 1969 que surge bajo el nombre de ARPANET, esta fue una red creada por ARPA (Advanced Research Projects Agency), una agencia que funcionaba bajo la supervisión del Departamento de Defensa de los Estados Unidos.

El propósito de dicha nueva red era la de ofrecer un medio de comunicación seguro que funcionase independiente, de respaldo del en ese entonces servicio telefónico, que era susceptible de ataques o violaciones por parte de la Unión Soviética, ya que para este particular periodo de tiempo estaba en vigencia la denominada Guerra Fría. Al mismo tiempo los Estados Unidos se ven forzados a buscar nuevas formas de comunicaciones ya que entraba también en servicio la serie de satélites Sputnik que dejaba en cierta medida a este país por detrás de su principal rival.

Arpanet empezó a ser utilizada por Universidades, Instituciones Militares, Instituciones Científicas y por el Departamento de Defensa y sus filiales; de esta manera se fue afianzando poco a poco, y al mismo tiempo empezaba su crecimiento y nuevas implementaciones; ya en 1972, a medida que la red se volvía cada vez más grande y sus avances se hacían sobre la marcha, se implementa el servicio de correo electrónico que es la herramienta más difundida en la actualidad por el Internet.

Algunos años después, en 1983 se integra a esta red el protocolo TCP/IP como el protocolo principal de comunicación, de esta manera Arpanet alcanza nuevas dimensiones, este protocolo fue creado en 1974 por Robert Kahn y Vint Cerf. Finalmente en 1990 se decide constituir oficialmente la red INTERNET; que unía a varias redes, una de ellas las de universidades y demás oficinas y departamentos de investigación a lo largo de los Estados Unidos y el mundo.

1.1.3 Avances y Cambios a través de los Años

En ya diez años como usuario permanente del Internet, he podido notar ciertos cambios que seguramente valen la pena mencionar, y probablemente usted deba tener en cuenta, ya que estos, en algunos casos sutiles y en otros definitivamente notorios, han sido los motores principales de que el Internet se haya difundido, y se vaya adoptando como un medio de comunicaciones cada vez más indispensable en el día a día de esta nueva sociedad de principios de siglo.

Voy a comenzar por citar la forma en la que se veía la información, ya este es uno de los principales cambios a lo largo de la vida del Internet; en un principio el ambiente era totalmente escrito, es decir que nos encontrábamos frente a una pantalla con nada más que información en forma de texto, esto dificultaba en gran medida que los usuarios con pocas nociones de lo que era un Telnet pudiese sacarle provecho a la información que ofrecía la red de redes en sus principios. Después empezó a utilizarse el lenguaje gráfico, dominado por las paginas html, estas páginas nos mostraban la información en pantallas bajo ambientes gráficos, que ofrecían una mejor aceptación y además nos permitían poner y contenidos multimedia junto con la información.

Junto con el advenimiento de esta nueva forma de presentación de la información surgieron nuevos servicios, que tal vez ya no sean conocidos por la mayoría de los usuarios cotidianos de Internet como eran: gopher, wais, www4, etc. El gopher era un sistema que nos permitía hacer uso de los nuevos recursos del Internet sin necesidad de preocuparnos por los programas, el hardware y las direcciones, ya que estas poderosas máquinas se encargaban de correr las aplicaciones, realizaban las búsquedas y nos las presentaban en nuestra maquina. Wais eran un sistema que buscaba por nosotros la información, esto antes de presentarse el monopolio de empresas de software, al igual que el gopher, era un sistema que utilizaba recursos ajenos a los nuestros para poder realizar las búsquedas. Finalmente mencionaré el www4, que era una herramienta que a principios de la era multimedia, nos permitía ver videos y escuchar música (eso si con sus debidas limitaciones) en aquellos equipos que aún no poseían el hardware y el software necesario para mostrar las en ese entonces flamantes páginas Web que ofrecían este contenido; y todo esto no hace más de unos escasos ocho años.

Otra interesante variable es la de la descarga de archivos, en el pasado si se requería de una descarga de algún tipo de archivo o documento, se debía tener conocimientos básicos del uso de los sistemas FTP (File Transfer Protocol), además de la paciencia para poder buscar la información dentro de la terminal mediante medios totalmente ASCII; ahora este tipo de transferencias se pueden hacer de un modo más transparente, ya que las descargas se pueden hacer mediante la página que se encarga de evitarnos los procedimientos de conexión y nos permite directamente la descarga de los datos, o si es necesario conectarse con la terminal, ahora la búsqueda también es bajo un ambiente gráfico en la mayoría de los casos.

Finalmente haré referencia al correo electrónico, que es la herramienta de Internet más usada por los internautas, como es de suponerse, los primeros correos sólo nos permitían enviar datos escritos, pero gracias a su popularidad y uso extendido, en la actualidad a los datos escritos se les puede anexar de forma muy sencilla cualquier tipo de dato, ya sea este imágenes, documentos, hojas de datos, videos, etc. Lo único que nos limita es el tamaño de los datos, pero gracias a conexiones más rápidas el límite se ha vuelto la imaginación.

1.1.4 Protocolo TCP/IP

Como ya se citó anteriormente dentro de este mismo capitulo, el protocolo en el cual se basa el Internet es el TCP/IP, en esta parte, nos detendremos a revisar de forma un poco más detenida el funcionamiento de este protocolo para que se pueda tener una idea más especifica de cómo funciona la red global de la información y porque su reputación de una red de comunicaciones confiable.

1.1.4.1 Orígenes

El protocolo de Internet nace en un principio a la gran necesidad del Departamento de Defensa (DOD de sus siglas en inglés) de los Estados Unidos de Norteamérica por unificar las diferentes redes que poseía en ese momento, así como la de tener esta nueva red a punto para poder resistir los embates de la en ese entonces Guerra Fría.

Cabe mencionar que para ese entonces el Departamento de Defensa tenía a su cargo el desarrollo de la integración de las tres ramas del ejército, que son: la Fuerza Aérea, Fuerza Terrestre, y Fuerza Naval. “Para ese entonces cada una de las tres fuerzas militares puso a concurso de merecimientos sus sistemas de comunicaciones y por supuesto cada una eligió una empresa manufacturera diferente”[1]. El escenario que se encontraba ante el DOD era un poco desalentador, ya que cada empresa manufacturera de los servicios de telecomunicaciones manejaba, como es de esperarse, su propio protocolo el cual no era compatible con el sistema de comunicaciones del Departamento de Defensa, mucho menos con las otras ramas del ejército.

Por lo tanto para poder comunicarse se debía desarrollar un protocolo que pudiera funcionar independientemente del tipo de redes y fabricante; en otras palabras este nuevo protocolo debía ser capaz de establecer la comunicación entre una red manejada y propietaria de IBM y otra con Unisys, algo que para ese entonces implicaba ya un reto de por si, esto sin considerar el otro punto clave que era la seguridad.

Como se mencionó anteriormente, otro de los puntos clave en el desarrollo de este nuevo protocolo era la seguridad, cuando nos referimos a la seguridad nos referimos a la confiabilidad de la red al momento de enviar información, es decir que dicha información debe llegar a su destinatario, ya que en plena Guerra Fría el medio para pasar información era el teléfono, que como es de imaginarse era poco confiable debido a la facilidad para ser interceptada la comunicación y por ser vulnerable a los ataques u otro tipo de sabotajes.

Qué implicaba la creación de esta red segura? En primer lugar garantizar que los datos que se envíen no se pierdan en el camino o que dejen de llegar por falla en alguno de los diferentes puntos de conexión entre las redes de datos; y, que los datos no puedan ser leídos por máquinas a las que no se les remita dicha información; estas condiciones son fundamentales, ya que la expansión del Internet ha ido de la mano con esta seguridad implícita de usar el protocolo TCP/IP, ya que nos ofrece garantías de una entrega de datos pese a daños en ciertos puntos de la red.

[1] http://www.yale.edu/pclt/COMM/TCPIP.HTM

Una vez que se estuvo de acuerdo en las características que debía poseer este nuevo protocolo, el departamento de defensa puso a cargo del proyecto a Robert Khan, quien ya había trabajado en la red conocida como ARPANET, que con el tiempo cambiaría de nombre a Internet; Khan rápidamente pidió ayuda a Vint Cerf de la Universidad de California. Ambos son conocidos como los inventores de la Internet, y sus trabajos llevan el sello de la simplicidad y eficiencia, como la delata una frase muy común: "El producto de Cerf y Khan, correrá sobre dos latas delgadas y una correa"[2].

Desde un principio se observó, que para lograr una unión de las diferentes redes se debía quitar el peso de la correcta transmisión de la información a la red y en cambio hacer responsable a cada host por esta acción, una vez que el rol de la red paso a ser mínimo, se pudo integrar las diferentes redes casi sin mayores inconvenientes; por lo tanto la red previamente diseñada y en uso Arpanet que funcionaba según estos preceptos paso a ser el modelo para el desarrollo de este nuevo protocolo.

Otro de los conceptos que se introdujeron fue el uso de pequeños dispositivos llamados routers que tenían la capacidad de convertirse en la unión entre dos redes, este concepto fue fácilmente adoptado por la mayoría de las redes, en parte debido a que se ajustaba a las necesidades de la mayoría de fabricantes; estos preceptos que en principio son simples fueron la clave para que este nuevo protocolo tuviera éxito, logré unir las diferentes redes y sea adoptado con gran rapidez, además como se verá más adelante brinde robustez y confiabilidad.

En 1983 el flamante protocolo impulsado por Cerf y Kahn bautizado como TCP/IP estuvo terminado y se puso en funcionamiento, Arpanet tuvo su transformación más importante y se convirtió en la primera red capaz de unir a varias redes en una; y proporcionar la confiabilidad en caso de daños que se buscaba, a partir de este momento su crecimiento sería veloz y de gran aceptación.

TCP/IP es un protocolo que se permite recuperarse de fallas en el sistema por caídas o perdida de comunicación con cualquier nodo, estas recuperaciones se realizan de manera automática, lo que implica una reconfiguración de la red en si misma; esto se logra gracias

[2] http://en.wikipedia.org/wiki/Internet_history

a que las tablas de enrutamiento se actualizan en forma dinámica de un router a otro; esta actualización de las tablas de enrutamiento traen consigo como es de esperarse el uso de algún tiempo, y en el transcurso de esta actualización se puede experimentar la perdida de información, pese a esta característica TCP/IP ofrece una confiabilidad como ningún otro protocolo de red.

"TCP es el responsable de la correcta entrega de información entre el cliente y el servidor"[3], o visto de otra manera del un host y otro, también es el encargado de detectar si existen errores o perdidas en la información que se transmite y ordena de forma automática la retransmisión de esta hasta que la entrega de los datos sea la correcta.

IP por su parte es el responsable de mover la información de un nodo a otro, este protocolo se vale de una dirección de destino de 4 bytes, IP opera en máquinas gateways para mover la información y redireccionarla en la ruta correcta.

Debido a que en un principio el desarrollo del Internet y su protocolo le correspondió al gobierno, este protocolo estaba bajo la protección de los artículos de no comercialización y de uso militar y científico, lo que impidió que se vuelva propietario de alguna compañía y por consiguiente se entorpezca la expansión y su generalización. A finales de la década de los 80's la Fundación Nacional de Ciencia o NSF por sus siglas en inglés (Nacional Science Fundation) se unió activamente al DOD y decidió conectar varios de sus centros de investigación al Arpanet, al igual que algunas Universidades.

En 1984 el Departamento de Defensa decide separarse de la red en desarrollo, a finales de los 80's decide que el protocolo de Internet se había desarrollado lo suficiente, por lo que decide retirarse y cerrar el Arpanet; en este punto la NSF una organización civil toma el control de la red y nace el Internet, el DOD terminaría apagando el último núcleo de Arpanet a finales de 1989.

La NSF junto con varias Universidades llevaron el Internet a un rápido crecimiento debido a nuevas mejoras y aplicaciones que tuvieron gran éxito como fueron el Domain Name System (DNS), y el correo electrónico o e-mail, sin embargo el protocolo TCP/IP

[3] OP CIT 1

permaneció sin mayores cambios, dejando en claro su eficiencia. A su vez varias empresas se unieron a esta nueva red, y a principios de 1990 nace el primer Proveedor de Servicios de Internet o ISP por sus siglas en inglés que mediante conexiones Dial-up daba acceso a Internet, que en un principio tenia información de estas Universidades y centros de Investigación.

1.1.4.2 Conceptos Básicos

Antes de poder entrar en detalle acerca del funcionamiento del protocolo de Internet y en especial TCP e IP vamos a revisar varios conceptos básicos que nos ayudarán a comprender como esta dispuesta una red y como funciona el flujo de información a través de estas diferentes redes.

En primera instancia revisaremos ciertos aspectos acerca de una red. A continuación les presento un gráfico básico de una red, la cual me servirá para ilustrar los componentes de la misma.

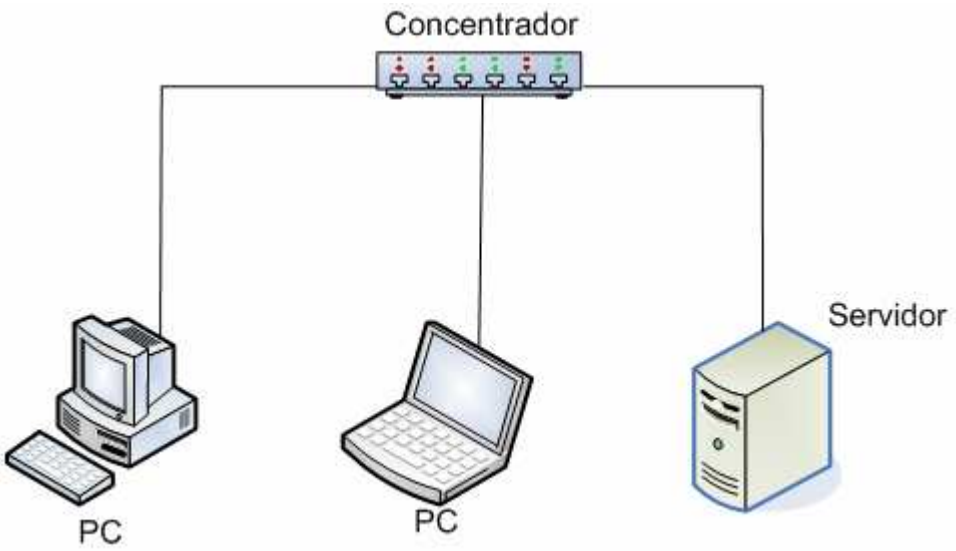


Figura 1.1. Esquema Básico de Red

De la figura se pueden destacar dos tipos fundamentales de equipos, el primer tipo de equipos es el conocido como concentrador, que es un dispositivo diseñado para poder conectar los equipos de la red, toda la información que los equipos de la red generen pasará

por este concentrador; el segundo tipo de equipos son los computadores, estos pueden ser de escritorio, portátiles, e inclusive pueden ser computadores que ofrecen servicio especializados o servidores.

Este esquema que se mostró es el básico de una red, es decir que toda red de datos poseerá al menos de equipos de computación y de concentradores, las diferencias entre redes yacerán en la conexión física, la distribución que tomen los diferentes componentes en la red, y en la forma en que se produce la comunicación. También vale la pena notar que esta red no posee conexión con otra red, es decir que solo se puede establecer comunicación entre los equipos que estén conectados al concentrador.

Existen varios equipos concentradores, entre los más importantes podemos citar al hub que es un equipo con varias terminales a las cuales se conectan varios computadores, la información que entra a este equipo es retransmitida por todas las terminales del hub, lo que significa que si un equipo transmite información, esta le llegará a todos los demás equipos, lo que implica que el canal de comunicaciones se satura con facilidad y provoca en algunos casos perdida de información. Otro concentrador es el switch, que realiza la misma función que el hub, con la diferencia que no retransmite la información por todos sus terminales, el switch es capaz de reconocer a que equipo le es dirigida la información y la retransmite por el terminal más conveniente, esto genera que el canal de comunicación no se sature y se produzcan menos perdidas de información debido a colisiones.

Tal como se mencionó, las redes se diferencian en su conexión física, según la distribución de sus componentes y en la forma en la que se produce la comunicación entre equipos, a continuación les mostrare el esquema de una red Ethernet y otra Token Ring.

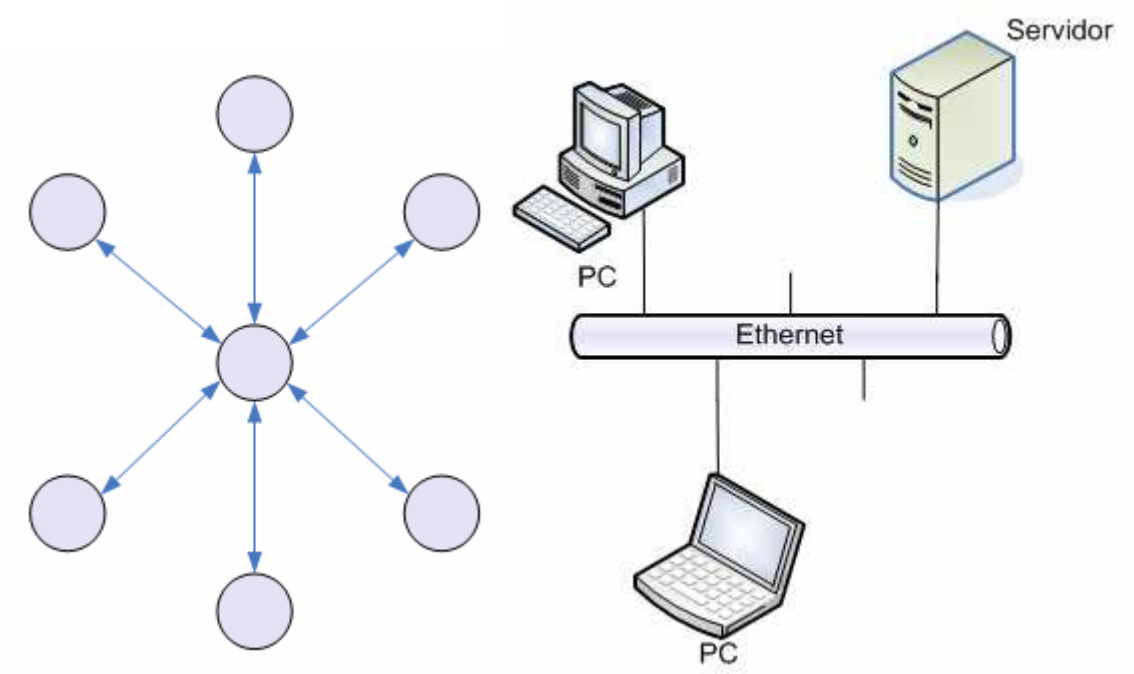


Figura 1.2. Esquema de Red Ethernet

Como se aprecia en el esquema de una red Ethernet, el o los concentradores me sirven para que la red este conectada de tal manera que los equipos se unan a ellos formando una estrella, esto a nivel físico; mientras que a nivel lógico es como si todas las máquinas acceden a un solo canal por el cual viaja la información de la red, en el gráfico se puede ver al lado izquierdo la forma en que los equipos se distribuyen, con el concentrador como punto central y de unión entre equipos; y, a su derecha la representación de la misma red de una manera más lógica.

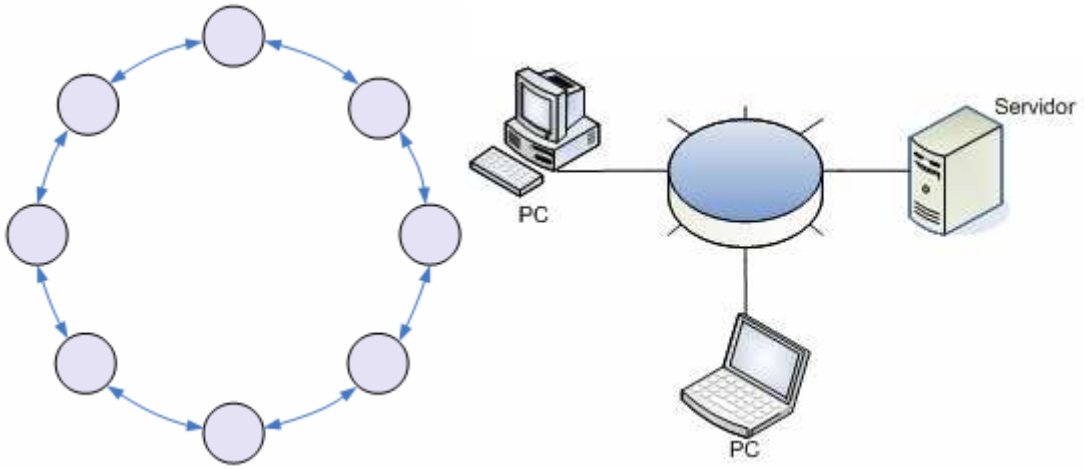


Figura 1.3. Esquema de Red Token Ring

En la figura 3 se aprecia un modelo de la red Token Ring, los concentradores y los equipos están dispuestos de tal manera que a nivel lógico una máquina este conectada con otra formando un anillo, la implementación física de este tipo de red puede ser totalmente diferente, la manera más común es en estrella tal como una red Ethernet, la diferencia es que los concentradores y la forma en que viaja la información dentro de esta red, nos permite que a nivel lógico la red se perciba como un anillo; al lado derecho se puede ver un esquema a nivel lógico de una red Token Ring.

Ya que se tiene claro las diferencias que puede haber entre una red y otra, pasaremos a revisar ciertos componentes y términos que aparecen a raíz de la conexión de varias redes; a continuación les presentamos un gráfico en el cual podremos identificar componentes más importantes para poder comprender el funcionamiento del Internet.

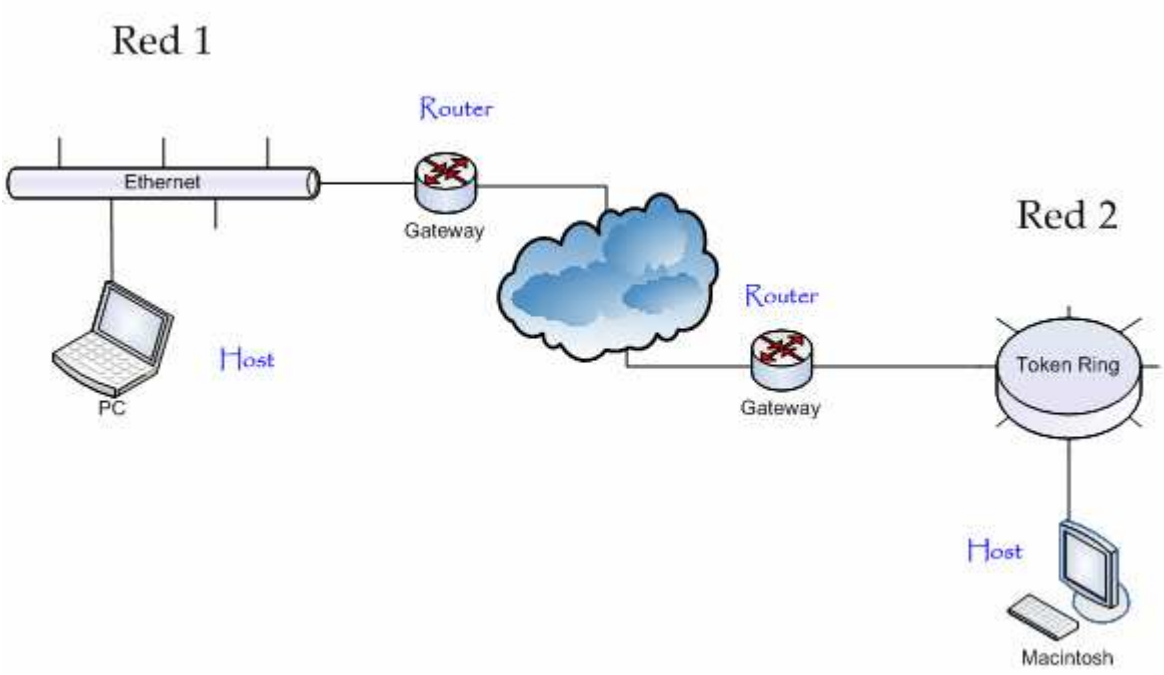


Figura 1.4. Diagrama de Conexión entre Redes

En la figura 4 podemos diferenciar fácilmente dos redes, estas redes están unidas entre si mediante una nube que representa ya sea una conexión transparente (un cable), o puede ser otra red; estas dos redes pueden o no ser del mismo tipo, en el caso representado estas redes son diferentes, nos encontramos con una red Ethernet y otra Token Ring, una con PC's y la otra con equipos Macintosh respectivamente.

A simple vista reconocemos un nuevo equipo en estas redes llamado router, este equipo es una computadora especializada cuya función es la de servir como Gateway o en español Puerta de Enlace, el router cumple con la función de direccional la información por el camino más apropiado para encontrar su destino, toda la información ya sea dentro o fuera de la red pasa por el router, este verifica si el destino esta dentro o fuera de la red, si esta dentro no deja que la información pase a través de si, pero si el destinatario se encuentra fuera de la red este toma la información y la envía por la mejor ruta disponible. El router puede lograr procesos como los descritos anteriormente gracias a que en él corren los protocolos IP y TCP; el router puede tener dos o más interfaces y estas pueden corresponder a varios tipos de conectores según la conexión física lo requiera, esto quiere decir que el router puede adaptarse a cualquier tipo de red y a dos o más al mismo tiempo.

Previamente se mencionó el concepto de gateway o puerta de enlace, gateway no es más que un nodo dentro de la red por el cual la información pasa al momento de querer viajar de una red a otra, el gateway debe cumplir con la tarea de ser un acople a nivel físico de las redes de ser necesario o de ser un interprete de protocolos.

Finalmente el otro concepto que debemos tener en cuenta es el de host, un host es cualquier equipo dentro de una red que envía o recibe información, lo que significa que se puede tener equipos host en una misma red o en diferentes redes dependiendo del origen y el destino de información.

1.1.4.3 Protocolo de Internet

En esta parte nos detendremos a revisar con más profundidad el protocolo de Internet, debemos empezar por citar que el protocolo en el cual se basa el Internet tiene cuatro capas, mediante estas cuatro capas se puede explicar todo el flujo de información de la red mundial de la información y por lo tanto su funcionamiento, en estas capas también encontraremos al protocolo IP y TCP respectivamente.

Empezaremos por citar las cuatro capas del protocolo de Internet mediante el siguiente gráfico:

Figura 1.5. Capas del Protocolo de Internet

En la figura 5 podemos ver las cuatro capas: "Aplicación, Transporte, Internet y Enlace"[4], estas capas se encuentran en orden de acuerdo al flujo que sigue la información para poder llegar desde los programas hasta el medio físico que se encargará de su transmisión; toda la información pasa a través de estas capas y se transforma según pasa por ellas.

Una vez que la información a recorrido su proceso a través de todas las cuatro capas del protocolo de Internet, los datos fueron fragmentándose para poder ser transmitidos, y además se le otorgo identificadores de cada capa en orden ascendente para pueda ser reconocida por cada capa cuando llegue a su destino, los identificadores quedan de la siguiente manera.

Figura 1.6. Orden de los Identificadores de Capa[5]

Cada capa del protocolo de Internet se comunica con su vecina y solo con estas, de tal manera que los datos no pueden saltar ninguna capa, cada capa le entrega la información a la siguiente, se fracciona y se le añade identificadores para poder reconstruir la información al momento de querer realizar el proceso inverso cuando la información le es

[4] http://www.faqs.org/rfcs/rfc793.html
[5] http://www.cs.fit.edu/~mmahoney/cse3103/tcpip.html

entregada a su destinatario, de la misma manera estas capas son capaces de lidiar con la capa superior e inferior formando un sistema simple pero efectivo de entregar información.

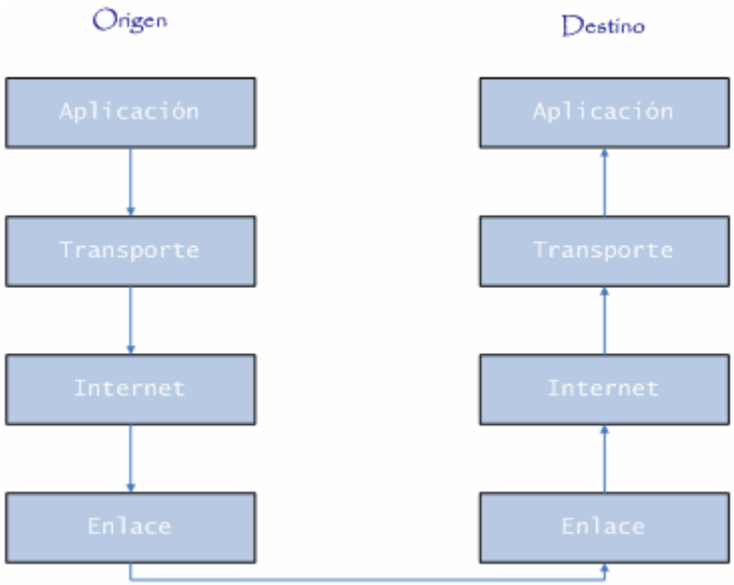


Figura 1.7. Flujo de Información en el Protocolo de Internet

Cada capa del protocolo de Internet se compone por una serie de programas, protocolos o tecnologías. La capa de Aplicación esta compuesta por los programas de alto nivel como los browser, programas de transferencia de documentos o programas de correo electrónico entre otros, estos a su vez manejan protocolos como HTTP (Hyper Text Transfer Protocol), POP3 (Post Office Protocol version 3), FTP (File Transfer Protocol), Telnet, etc.

La capa de Transporte puede estar compuesta por varios protocolos, el más importante y difundido es TCP (Trasmission Control Protocol).

La capa de Internet esta compuesta igualmente por varios protocolos pero el más importante es IP (Internet Protocol) ya sea en su versión 4 o versión 6.

Finalmente la capa de Enlace esta compuesta de varias tecnologías dependiendo del tipo de red, entre las tecnologías más usadas tenemos Ethernet, Token Ring, WiFi, FDDI, WiMAX, entre otras. La siguiente tabla nos muestra de mejor manera la composición de las diferentes capas del protocolo de Internet.

CAPAS DEL PROTOCOLO DE INTERNET	
Aplicación	**HTTP, HTTPS, POP3, FTP, Telnet, IMAP, SMTP, SSL, …**
Transporte	**TCP, UDP, SCTP, …**
Internet	**IPv4, IPv6, …**
Enlace	**Ethernet, Token Ring, WiFi, WiMAX, FDDI, PPP, RS232, …**

Tabla 1.1. Capas del Protocolo de Internet

1.1.4.3.1 TCP (Transmission Control Protocol)

1.1.4.3.1.1 Encabezado TCP

Antes de poder revisar el funcionamiento del Protocolo de Control de Transmisión debemos ver como esta estructurado el encabezado que este protocolo le otorga a cada segmento de datos para que en el host de destino se puedan recibir los datos y de manera segura y sin perdidas o errores. En el siguiente gráfico se vera cada una de las partes de este encabezado de 20 Bytes.

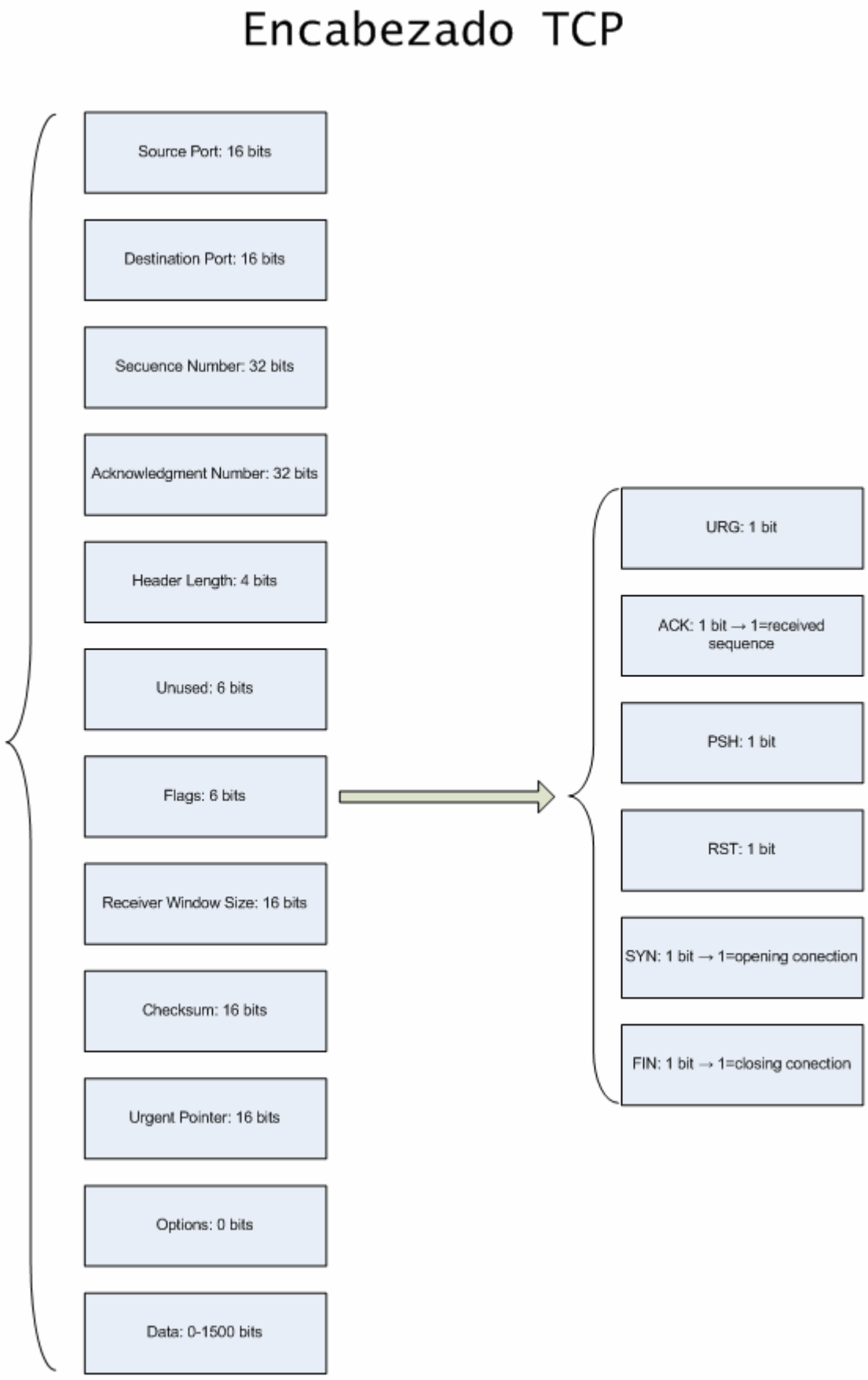


Figura 1.8. Encabezado TCP

A continuación, se procederá a revisar de manera más detenida las diferentes partes que componen este encabezado.

Empezaremos por *Source Port*, o por su nombre en español Puerto de Origen, su longitud es de 16 bits y me indica el número de puerto del que se origina la transferencia de datos.

Destination Port, tiene una longitud de 16 bits y su denotación en español es Puerto de Destino, me indica el número del puerto al cual van destinados los datos.

Sequence Number, posee una longitud de 32 bits, es el número de secuencia del primer octeto de datos en este segmento, si SYN esta activo el número de secuencia es el número inicial de secuencia o por sus siglas en inglés ISN y el primer octeto de datos es ISN+1.

Acknowledgment Number, si el bit de control ACK esta activado este campo contiene el valor del siguiente número de secuencia que el transmisor del segmento esta esperando recibir. Una vez que la conexión esta establecida este campo siempre se envía, tiene una longitud de 32 bits.

Header Length, este campo nos indica el número de 32 palabras bits del encabezado TCP, este nos indica donde los datos comienzan, posee una extensión de 4 bits.

Reserved, tal como su nombre en español indica, este campo se encuentra reservado para posibles usos en el futuro, como se muestra en la figura anterior este campo era de 6 bits[6] en la publicación del RFC793, pero con el paso del tiempo se ha reducido a 3 según la RFC3540[7], pero cabe destacar que estas actualizaciones no están del todo en funcionamiento, por lo que el protocolo original de Cerf y Khan, en el cual se basa la publicación RFC793 aún es la más acertada al momento de realizar una presentación del modelo.

Control Bits o Flags, este campo esta compuesto según la RFC793 por 6 bits y según las nuevas propuestas teóricas por 9 bits, en un principio revisaremos los 6 bits originales y

[6] http://www.faqs.org/rfcs/rfc793.html

[7] http://www.networksorcery.com/enp/rfc/rfc3540.txt

luego veremos como a quedado propuesto este campo y los bits de control que se han aumentado.

- ✓ URG o urgent, es un bit conocido como puntero urgente.
- ✓ ACK que es la abreviación de acknowledgment, es usado como un indicador de reconocimiento.
- ✓ PSH se le conoce como la función presionar.
- ✓ RST usado para indicar un reseteo de la conexión.
- ✓ SYN son los números de la secuencia de sincronía.
- ✓ FIN indica que no se enviarán más datos desde el transmisor.

Ahora bien una vez que se han revisado los seis bits originales y que se encuentran en uso que a su vez constituyen el campo de las banderas, podemos revisar la nueva propuesta teórica presentada en la RFC3540.

Cabe destacar que esta nueva propuesta nace con el propósito de poder mejorar los algoritmos que usa TCP para poder manejar el tráfico de datos; para poder evitar la congestión de los datos se ha desarrollado el ECN o Explicit Congestion Notification que al español nos quiere decir Notificación Explicita de Congestión, que le permite a un router con capacidad ECN en caso de saturación del canal hacer algo más que simplemente botar los paquetes de datos como señal de congestión, estos router pueden activar ciertos bits correspondientes al campo de bits de control que actúan directamente con el parámetro *Receiver Window Size* para poder sincronizar el tamaño de los datos y así mejorar el flujo de datos.

Como es de suponerse estos incrementos de los bits de control implican una reducción en alguno de los otros campos, el campo que se vio afectado es el *Reserved* que pierde 3 bits que son precisamente los necesarios para poder implementar los algoritmos ECN; a continuación les mostramos como queda el campo de las banderas con la adición de estos tres nuevos bits.

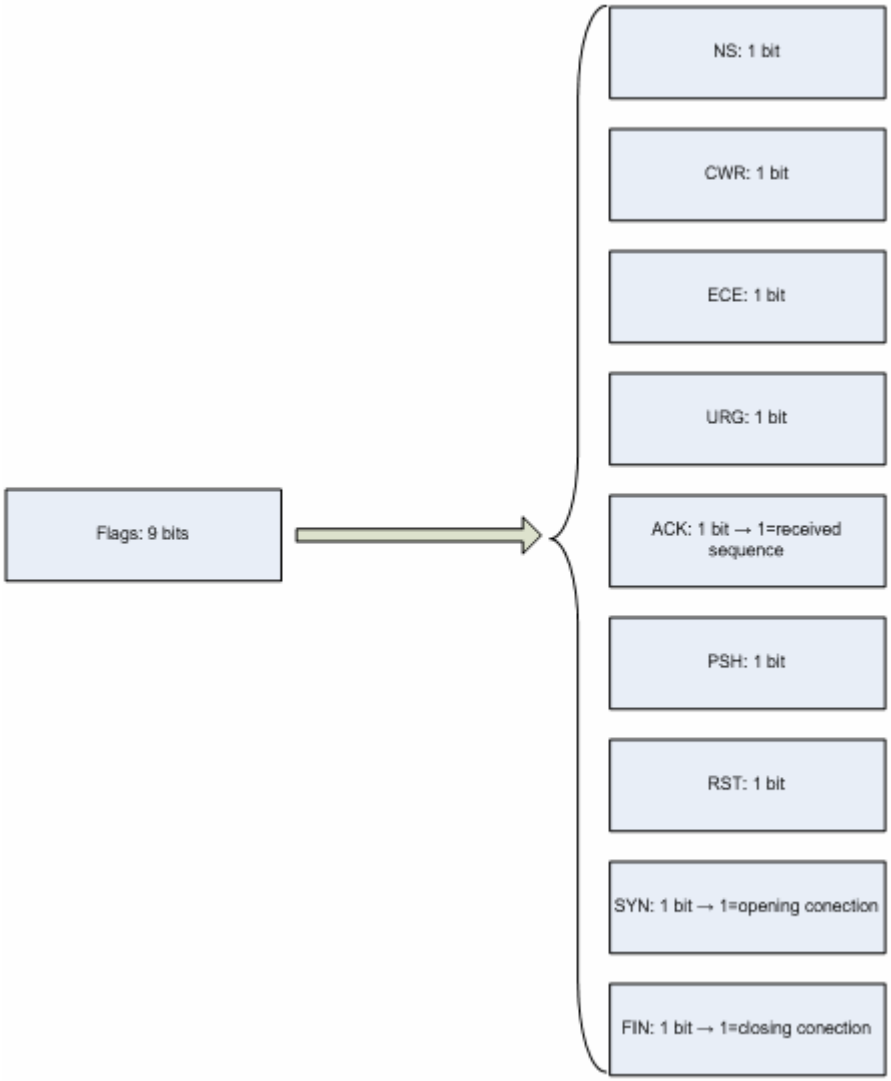


Figura 1.9. Nuevo Esquema para el Parámetro Flags o Control Bits

Una vez que se ha podido observar como queda conformado el parámetro Flags, revisaremos los tres restantes bits que se añaden a los seis revisados anteriormente que conforman el ECN.

- ✓ NS o nonce sum que se envía al recibir paquetes sin marca del ECN.
- ✓ CWR conocido como congestion window reduce que se activa una vez que se ha establecido una congestión del canal y le indica reducir el tamaño de los paquetes a enviarse.
- ✓ ECE que es el explicit congestion codepoint que se activa al sentirse la congestión del canal.

De esta manera terminamos de revisar el parámetro Flags del encabezado TCP.

Receiver Window Size, este parámetro de 16 bits me indica el número de octetos de datos, comenzando con el que esta indicado en el campo de acknowledgment, que el transmisor de este campo esta dispuesto a recibir.

Checksum, es el complemento a uno de 16 bits de la suma del complemento a uno de todas las palabras de 16 bits en el encabezado y texto. Si un segmento contiene un número impar de octetos de encabezado o texto para ser revisados, se coloca un último octeto a la derecha con ceros para propósitos de realizar las operaciones, esta colocación no se transmite como parte del segmento, Mientras se calcula esta revisión el campo mismo de checksum se llena con ceros.[8]

La operación del checksum también incluye un pseudo-encabezado de 96 bits conceptualmente prefijado al encabezado TCP. Este pseudo-encabezado incluye la dirección de origen, dirección de destino, tipo de protocolo y la longitud TCP. Esto le da a TCP una protección en contra de segmentos mal enrutados.

La longitud TCP es el campo header length más la longitud de datos en octetos, y no cuenta los 12 octetos del pseudo-encabezado; a continuación un gráfico del pseudo-encabezado.

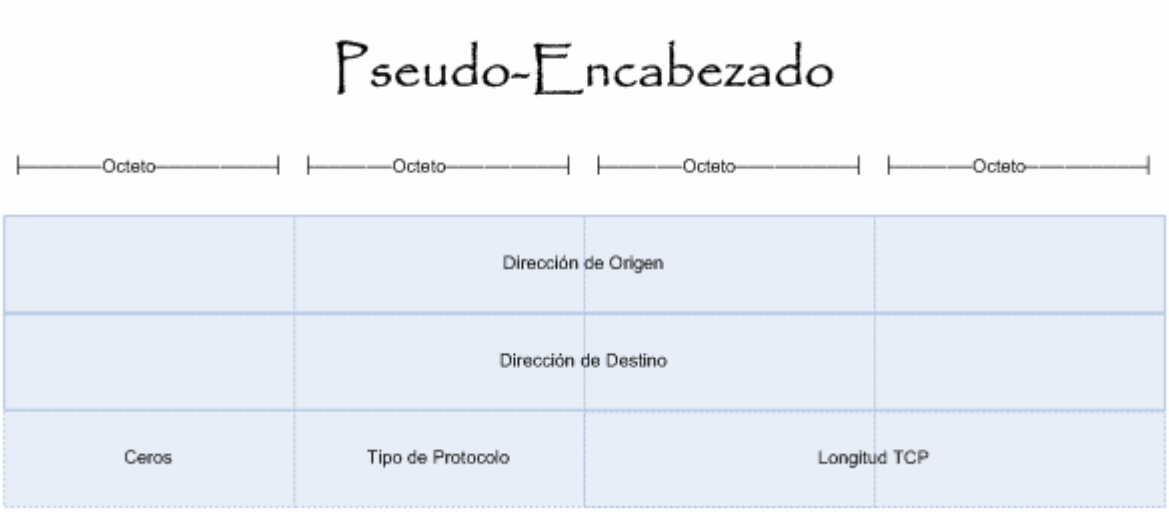


Figura 1.10. Seudo-Encabezado

[8] http://www.faqs.org/rfcs/rfc793.html

Urgent Pointer, es un campo compuesto por 16 bits, comunica el valor actual del puntero de urgencia como un offset positivo desde el número de secuencia en este segmento; este puntero nos indica directamente el número de secuencia del octeto que le sigue al dato urgente. Este dato solo es interpretado en los segmentos que tienen el bit URG activado.

Options, este constituye un campo variable, se lo ejemplifica como un campo de 0 bits ya que también es un campo opcional, va al final del encabezado y debe ser múltiplo de ocho bits de longitud, todas las opciones están incluidas en el checksum, hay dos clases de opciones de formato:

1. Un octeto simple o option-kind
2. Un octeto de option-kind, un octeto de option-length, y los octetos de datos en si u option-data.

El octeto option-length cuenta la longitud de las tres clases de octetos. Se debe también tomar en cuenta que la longitud de la lista de opciones puede ser más pequeña que la que indicada, en cuyo caso se debe completar con ceros.

1.1.4.3.1.2 Proceso de Conexión

En esta parte del presente documento se revisará el proceso de conexión que realiza el protocolo TCP, lo que nos llevará a revisar en primera instancia los estados que pueden presentarse durante la conexión previa a la transmisión de datos.

- LISTEN.- Este estado representa el momento de espera de una petición de conexión desde cualquier Puerto TCP remoto.
- SYN-SENT.- Representa la espera de una respuesta de petición de conexión después de haber enviado una petición de conexión.
- SYN-RECEIVED.- Nos indica la espera de confirmación de reconocimiento de la petición de conexión después de haber recibido y enviado ambos una petición de conexión.
- ESTABLISHED.- Representa una conexión abierta, los datos pueden ser enviados por el usuario. Este es el estado normal para la fase de transferencia de datos de la conexión.

- FIN-WAIT-1.- El presente estado nos indica la espera de un pedido de terminación de la conexión desde el TCP remoto, o un reconocimiento de la petición de terminación de la conexión previamente enviada.
- FIN-WAIT-2.- Este estado similar al anterior representa la espera del pedido de terminación de conexión del TCP remoto.
- CLOSE-WAIT.- Este estado en particular nos indica el periodo de tiempo en espera del pedido de terminación de conexión desde el usuario local.
- CLOSING.- Representa la espera del reconocimiento del pedido de terminación de la conexión de desde el TCP remoto.
- LAST-ACK – Este estado nos indica el periodo de espera por un reconocimiento del pedido de terminación de conexión previamente enviado al TCP remoto (el que incluye un reconocimiento de su pedido de terminación de conexión.).
- TIME-WAIT – Este estado es en si una espera del tiempo necesario para estar seguro que el TCP remoto recibió el reconocimiento de petición de terminación de conexión.
- CLOSED – Esta palabra no representa ningún estado de conexión.

"Una conexión TCP progresa de un estado a otro en respuesta a eventos. Los eventos son las llamadas de usuarios, OPEN, SEND, RECEIVE, CLOSE, ABORT, y STATUS; los segmentos recibidos, en especial aquellos que contienen las banderas de SYN, ACK, RST y FIN; y los timeouts."[9]

Una vez que se han revisado los estados que pueden suscitarse en el proceso de conexión, podemos pasar a revisar el con más detenimiento la conexión y la desconexión.

El proceso mediante el cual se realiza una conexión se llama "Three-Way Handshake", y es normalmente iniciado por un TCP y respondido por otro, se puede producir casos en los cuales dos usuarios pretenden establecer comunicaciones al mismo tiempo, gracias a los debidos usos de las banderas, en especial del RST se pueden evitar problemas de ambigüedad.

[9] http://www.faqs.org/rfcs/rfc793.html

A continuación se mostrara el más simple de los procesos de conexión, en donde un TCP inicia la petición de conexión y el otro le responde de la manera más apropiada para establecer la comunicación.

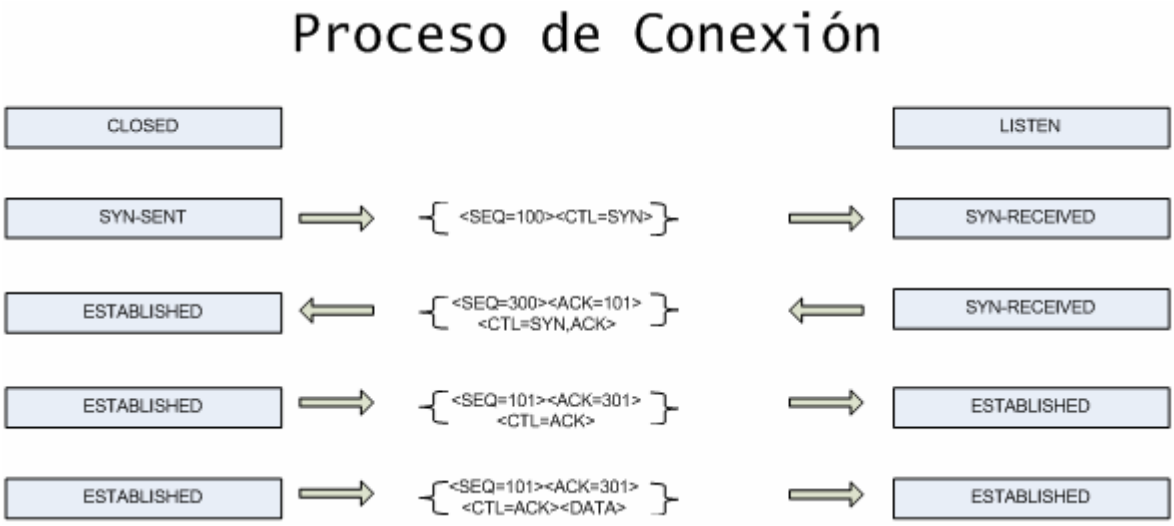


Figura 1.11. Proceso de Conexión TCP

Como se pude observar de la figura superior, por cada secuencia enviada existe un reconocimiento con el número de la secuencia más uno, también se puede observar el tipo de bandera que más relevancia tiene en el encabezado a la hora de establecer la conexión, finalmente el último paso se produce la transmisión de datos, cabe notar que las banderas y secuencias son las mismas que en paso anterior, ya que la comunicación se ha establecido y de lo contrario tendríamos confirmaciones de las confirmaciones.

Por último revisaremos el proceso de desconexión del protocolo TCP una vez que se han transmitido los datos del usuario A al B. De la misma manera que en proceso de conexión nos valdremos de un una ilustración para que se entienda de mejor manera los pasos de desconexión.

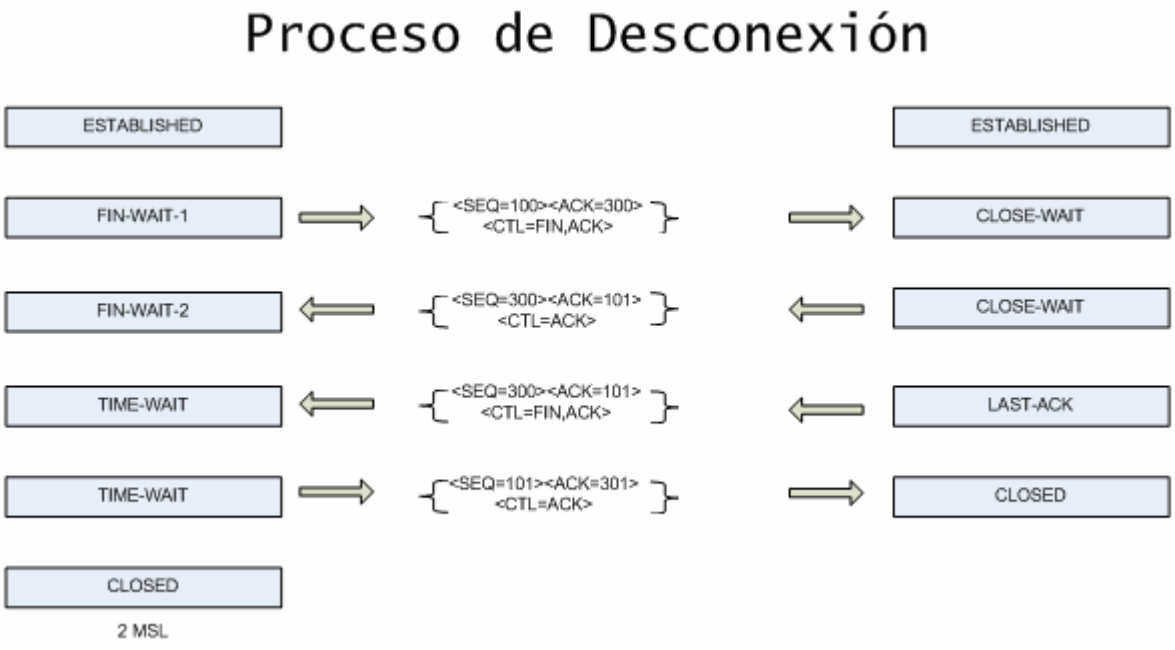


Figura 1.12. Proceso de Desconexión TCP

En la figura se puede apreciar que el proceso de desconexión es un poco más complicado que el de conexión, debido a que se debe estar seguro de que el proceso se ha cerrado, para no tener problemas con las aplicaciones y transferencias de datos; primero se envía una solicitud de FIN, una vez que esta es enviada, quien la envía no volverá a realizar transmisiones hasta que reciba de su contraparte la misma petición, por lo tanto cambia de estado, una vez que el segundo usuario recibe la notificación de terminación de conexión, envía su confirmación y luego procede a enviar su propio mensaje de desconexión, el primer usuario envía la confirmación al recibir FIN y finalmente espera 2 MSL (Maximum Segment Lifetime) que son 2 minutos para estar seguro de que su contraparte no ha enviado más peticiones y termina la comunicación.

1.1.4.3.1.3 Factores de Confiabilidad.

Para que sea considerado como un protocolo confiable, TCP necesita tener facilidades en ciertas áreas, las más importantes son las siguientes:

- Transferencia de Datos Básica
- Confiabilidad
- Control de Flujo
- Multiplexación
- Conexiones

- Seguridad y Precedencia

Transferencia de Datos Básica.- En este aspecto TCP se maneja de tal manera que decide bloquear o permitir datos a su conveniencia, cabe anotar que los datos se transmiten por octetos o grupos de estos.

Confiabilidad.- Se le asigna un número de secuencia a cada octeto transmitido y se requiere de una confirmación positiva ACK desde el TCP receptor.
Si un ACK no es recibido dentro de un tiempo de espera, los datos son inmediatamente retransmitidos; en el receptor los números de secuencia son utilizados para corregir el orden de los segmentos que pudieran ser recibidos en un orden diferente a incorrecto; y , para poder eliminar aquellos segmentos que están duplicados.
Los daños que se pudieran suscitar en la transmisión de los segmentos son manejados mediante una suma de verificación de cada segmento transmitido.

Control de Flujo.- TCP hace que el receptor se convierta en el ente que gobierna la cantidad de datos que envía el transmisor; esto es posible regresando una ventana (Window Size) junto con la confirmación ACK, indicando el rango de números de secuencia aceptables que pueden ser enviados más allá de una recepción exitosa.

Multiplexación.- Para poder permitir que varios procesos accedan a la comunicación del TCP simultáneamente, este protocolo provee un grupo de *puertos* dentro de cada host, estos puertos junto con la dirección IP forman una especie de contenedor. Un par de estos contenedores identifica plenamente a cada conexión, de tal manera que varios contenedores pueden ser usados al mismo tiempo en una misma conexión o en varias conexiones.

Conexiones.- Cuando dos procesos necesitan acceder a sus respectivos TCP’s primero se necesita establecer una comunicación entre ellos, debido a que la comunicación se realiza a través de un sistema de comunicación de Internet que no es confiable, y un host no confiable, un mecanismo de handshake con números de secuencia basados en un sistema de reloj se usa para poder evitar inicialización de conexiones erróneas.

Seguridad y Precedencia.- Los usuarios de este protocolo pueden indicar el nivel de seguridad y la precedencia en la red de los datos en sus comunicaciones, esto se logra a través del uso de unos bits dispuestos en el encabezado TCP.

1.1.4.3.2 IP (Internet Protocol)

1.1.4.3.2.1 Encabezado IP

En la presente parte del documento se podrá ver en detalle los encabezados IP, tanto el perteneciente a la versión cuatro como la versión seis de dicho protocolo, cabe resaltar que la versión seis del protocolo IP aún no entra en funcionamiento, se prevee que esta nueva versión reemplace a la antigua, lo que significa que las actuales direcciones IP están representadas en las nuevas, por esta razón se debe conocer ambas versiones.

A continuación se mostrará el encabezado de IPv4 ilustrado en la siguiente figura.

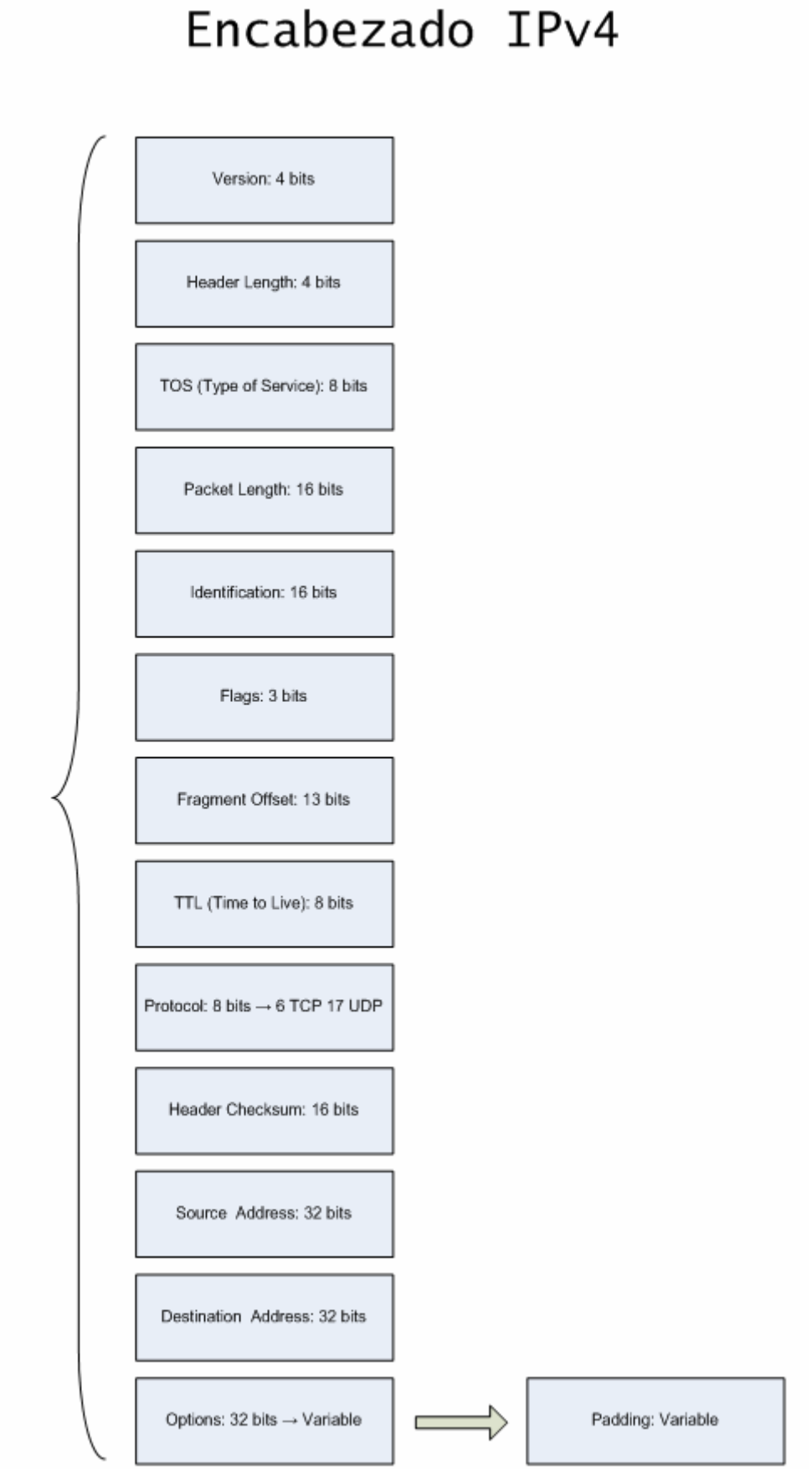


Figura 1.13. Encabezado IPv4

Version, esta es la primera parte del encabezado IP, esta compuesto de 4 bits, este campo nos indica cual es el formato del encabeza de Internet, en este caso nos referimos a la versión 4.

Header Length, este campo nos indica la longitud del encabezado, tiene por tamaño 4 bits; además nos indica el punto en el cual comienzan los datos, debe notarse que el valor mínimo que puede tomar este campo es de 5.

Type of Service, este campo de 8 bits, nos permite tener una idea del nivel de calidad de servicio que deseamos tener, estos parámetros nos sirven al momento de querer enviar datagramas a través de una red en particular y poder indicar el tipo de servicio que se desea al momento de esa transmisión. Algunas redes nos ofrecen servicios de precedencia, lo que significa que al momento de tener datos con una precedencia alta, estos serán despachados con más rapidez a la hora de un tráfico alto a través de la red. La opción de mayor importancia son los tres tipos de negociación que posee este parámetro: baja-demora, alta-confiabilidad y alta-producción.

Este es el momento para mencionar que tal como en TCP este parámetro ha sido modificado varias veces, sobre todo en los bits reservados para usos futuros, una de estas modificaciones y la que más importancia ha tenido es la introducción de los campos ECN tal como en TCP, estos campos sirven de la misma manera que en TCP y se implementaron en los dos últimos bits del campo TOS. Cabe anotar que debido a una serie de cambios en este campo durante los años, no puede garantizar el correcto funcionamiento de estos dos últimos bits, en algunos casos los mismos equipos (routers) se encargarán de poner en cero estos dos bits.

A continuación se mostrará un gráfico de este parámetro indicando el uso de cada bit, además se podrá observar más abajo tablas con los valores que pueden tomar dichos bits.

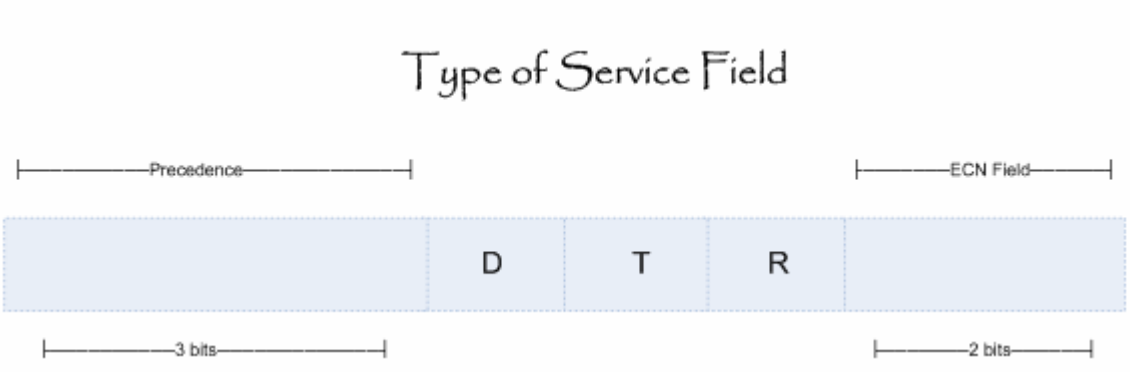


Figura 1.14. Bits del Campo Tipo de Servicio

VALORES DEL CAMPO TOS	
Precedencia	
111	Network Control
110	Internetwork Control
101	CRITIC/ECP
100	Flash Override
011	Flash
010	Immediate
001	Priority
000	Routine
Delay	
0	Normal Delay
1	Low Delay
Throughput	
0	Normal Throughput
1	High Throughput
Reliability	
0	Normal Reliability
1	High Reliability
ECN	
00	Not ECT (Not ECN Capability)
01	ECT (1)
10	ECT (0)
11	CE

Tabla 1.2. Valores del Campo TOS[10]

[10] http://www.networksorcery.com/enp/rfc/rfc791.txt
http://www.networksorcery.com/enp/rfc/rfc3168.txt

Packet Length, este campo esta compuesto de 16 bits, nos indica la longitud del datagrama medido en octetos, esta parámetro nos permite tener una longitud de hasta 65535 octetos, como es de esperarse esta longitud es en realidad impractica para la mayoría de redes existentes, por resta razón todos los host deben estar preparados para recibir 576 octetos, ya sea que lleguen completos o fragmentados, se transmitirán más de 576 octetos únicamente si el host de destino esta en capacidad de recibir dicha cantidad de información.

Esta capacidad de 576 octetos nos da la libertad de poder enviar una cantidad razonable de datos y encabezados, sobre todo si tenemos en cuenta que el típico encabezado de IP es de 20 octetos, más un razonable espacio para encabezados de protocolos superiores, se podrían transmitir un promedio de 512 octetos de datos.

Identification, este es un valor de identificación que le añade el transmisor para poder ayudar al momento del ensamblaje de los fragmentos de los datagramas, es un parámetro de 16 bits.

Flags, como su nombre lo indica no son más que bits, los cuales nos van a ayudar a poder tener control sobre la fragmentación de datos, a continuación les mostraré un poco mejor cuales son sus funciones mediante una sencilla tabla.

CONTROL FLAGS	
Reserved	**Debe ser 0**
DF	**0→ May Fragment; 1→ Don't Fragment**
MF	**0→ Last Fragment; 1→ More Fragments**

Tabla 1.3. Banderas de Control

Fragment Offset, nos indica a que parte del datagrama este fragmento debe ir, es decir nos muestra en caso de que haya fragmentación, cual es el orden y en donde debe ir dicho fragmento para encajar en el datagrama. Este parámetro esta medido unidades de ocho octetos (64 bits), y el primer fragmento deberá tener un offset de cero; este campo es de 13 bits.

Time to Live, o tiempo de vida es un campo de 8 bits, nos indica el tiempo que el datagrama puede circular en el sistema Internet, este parámetro esta relacionado con un segundo, pero cada vez que el datagrama pasa por un equipo debe restarse uno, aún si el proceso toma menos de un segundo, este parámetro se modifica cada vez que se procesa el encabezado; si el TTL llega al valor de cero este datagrama debe ser eliminado, se implementa este tipo de control para evitar que los datos no entregados en forma correcta permanezcan en el sistema y congestionándolo para siempre, además de brindar un tiempo seguro para su entrega.

Protocol, esta parte del protocolo nos permite saber cual es el protocolo superior al que va destinado los datos, este campo esta compuesto de 8 bits.

Header Checksum, este parámetro es la suma de comprobación del encabezado únicamente, como varios parámetros del encabezado IP cambian como el TTL el checksum es recalculado y verificado en cada punto de procesamiento del encabezado.

Source Address, como su nombre lo indica es la dirección de origen de los datos, dicho campo posee 32 bits.

Destination Address, es la dirección de destino a la cual se dirigen los datos, al igual que en la dirección de origen este parámetro cuenta con 32 bits.

Options, puede aparecer o no en un datagrama, este parámetro debe ser implementado por todos los módulos IP (host y gateways), lo que es opcional es la transmisión en uno u otro datagrama más no su implementación.

Este parámetro es variable, puede ser implementado de dos formas diferentes: como un solo octeto de “opción de tipo”; y como varios octetos entre ellos uno de “opción de tipo”, “opción de longitud” y “opción de datos”, el octeto de opción de longitud se cuenta a si mismo como a los dos octetos restantes.

Padding, este es el último parámetro del encabezado IP, es de longitud variable, su función es la de asegurarse que el encabezado IP termine el múltiplos de 32 bits, esto debido a que el campo Options puede tener longitudes distintas, este campo debe ser cero.

Una vez revisado el encabezado de IPv4 podemos pasar a la revisión del encabezado de IPv6, la cual como ya se dijo anteriormente aún no entra en funcionamiento, dicha entrada en funcionamiento se prevee en un futuro muy cercano.

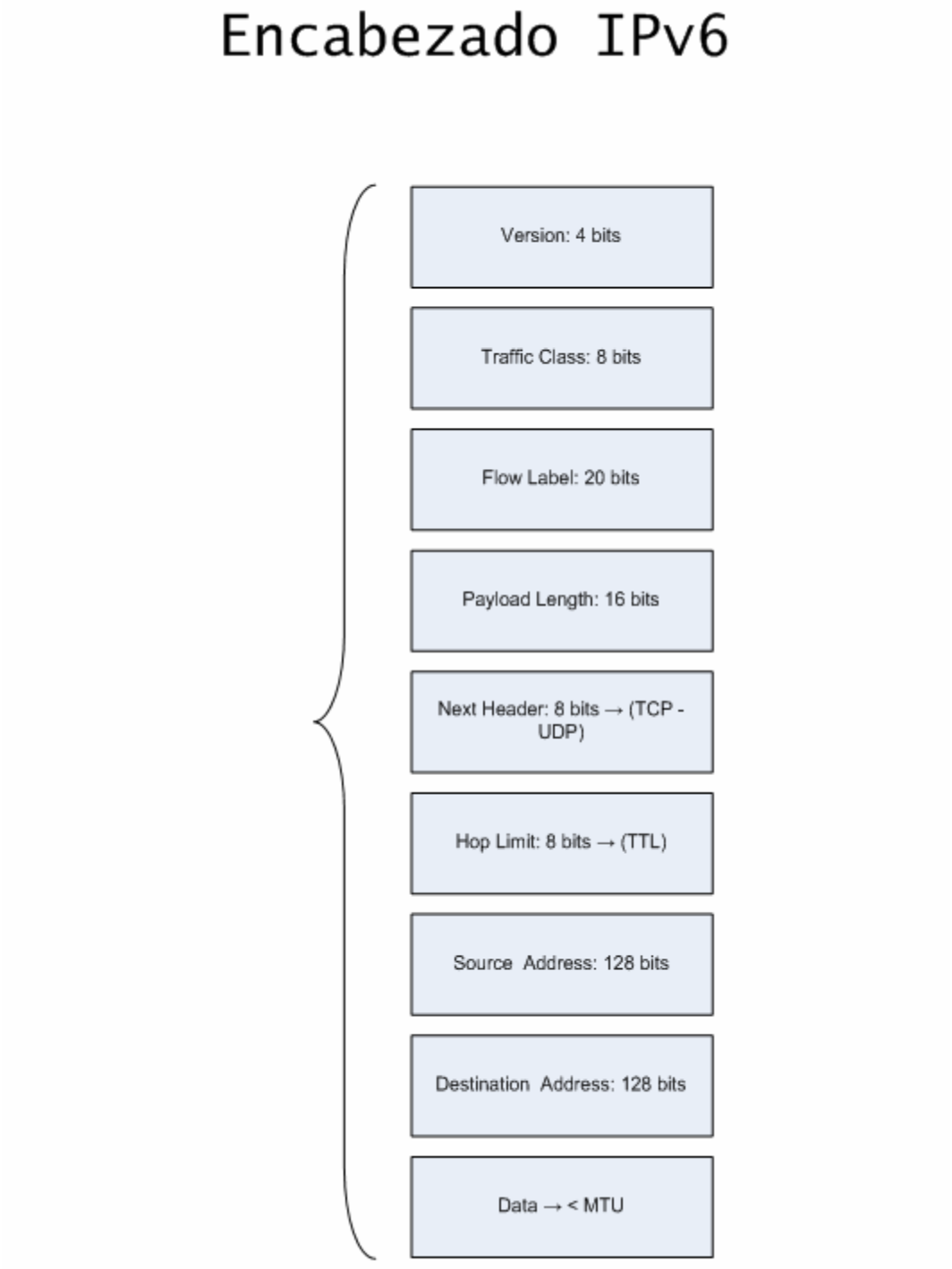


Figura 1.15. Encabezado IPv6

Version, este es el parámetro con el que se inicia el encabezado de IPv6, su longitud es de 4 bits, nos indica el número de la versión del Protocolo de Internet, en este caso es el seis.

Traffic Class, es un parámetro de 8 bits, el cual ha sido destinado para el uso de nodos de origen y routers para identificar y distinguir entre las diferentes clases o prioridades de los paquetes IP.
Para poder garantizar una buena funcionabilidad, este parámetro usará en primera instancia el parámetro TOS de IPv4 que cumple con la misma función, este parámetro ha sido modificado para poder probar por adelantado como se comportará el trafico IP, lo que significa que este campo no es sino una mejora al campo TOS que funciona en la actualidad.

Flow Label, esta parte del encabezado es de 20 bits, este campo será usado como una fuente para poder etiquetar secuencias de paquetes, los cuales requerirán de un manejo especial por parte de los router (aquellos que funcionen con IPv6), estos manejos pueden ser: calidad de servicio no definida, o servicio en tiempo real. Este campo aún esta en estudio, por lo que los nodos que no posean dicha capacidad pondrán valores de cero en todo este campo.

Payload Length, este parámetro contará con 16 bits enteros sin signo, los cuales tendrán la longitud de la carga básica de funcionamiento de IPv6, el resto del paquete seguirá el encabezado en octetos. Este parámetro no cuenta la extensión del encabezado.

Next Header, este parámetro de 8 bits identifica el tipo de encabezado inmediato que sigue al encabezado IP, usa los mismos valores del campo Protocol de IPv4.

Hop Limit, este campo al igual que Payload Length usa bit enteros sin signo pero esta vez 8, los cuales decrementan 1 cada vez que un nodo transmite un paquete. El paquete se descarta si este parámetro llega a decrementarse hasta cero.

Source Address, este parámetro es quizá el parámetro más importante junto con el campo Destination Address, consta ahora con 128 bits en vez de los 32 de IPv4, contiene la dirección de destino de los datos.

Destination Address, este campo tiene 128 bits y contiene la dirección de destino de los datos.

1.1.4.3.2.2 Direcciones IP

En esta parte del presente documento se revisará la forma en la que funcionan las direcciones dentro del Protocolo IP, estas direcciones son en si el alma del Internet, ya que gracias a ellas podemos identificar a las diferentes máquinas o redes que se encuentran asociadas a estas direcciones en la Red Mundial de la Información.

Los 32 bits de las direcciones IP se agrupan en series de 8 bits separados por puntos, y se representan en formato decimal, a esta forma de representación se le conoce como la notación decimal punteada o en inglés “Dotted Decimal Notation”[11]; el mínimo valor de un octeto es de cero y el máximo es de doscientos cincuenta y cinco, cada uno de los bits de estos octetos tiene un peso binario.

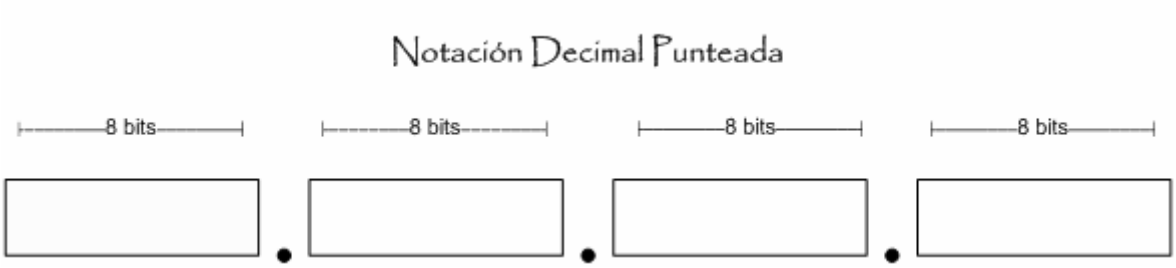


Figura 1.16. Notación Decimal Punteada

Cada dirección tiene implícitamente una parte que identifica a la red y otra parte que se encarga de identificar al host de esta red; de estos cuatro octetos, se utilizan varios de ellos para poder hacer una diferencia entre la red y el host, el número de octetos que se tomen para identificar la red o el host es lo que diferencia a las direcciones IP, existen en la actualidad tres clases de direcciones, en IPv4, estas clases son: A, B y C. Las diferencias entre estas clases se podrán apreciar en el siguiente cuadro.

[11] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm

CLASE	FORMATO	BITS MÁS SIGNIFICATIVOS	RANGO	NÚMERO DE BITS (RED/HOST)
A	N.H.H.H	0	1.0.0.0~126.0.0.0	7/24
B	N.N.H.H	10	128.1.0.0~191.254.0.0	14/16
C	N.N.N.H	110	192.0.1.0~223.255.254.0	22/8

Tabla 1.4. Diferencias ente las Diferentes Clases de Direcciones IP

Otro de los campos que se deben revisar al momento de establecer las direcciones IP es de las subredes, cada red puede ser dividida a su vez en redes más pequeñas llamadas subredes o subnets; el beneficio que posee esta fragmentación, es el de realizar un uso más eficiente de las direcciones IP de una red determinada, me permite gozar de una mayor flexibilidad, y capacidad de contener el tráfico de broadcast.

La forma de poder dividir las redes en subredes es mediante el préstamo de algunos de los bits destinados para la identificación del host y reutilizarlos para que formen parte de un nuevo parámetro llamado campo de subnet, de esta manera se aumenta el número de subredes y por otro lado se reduce el número de host, esto claro en pos de algunos de los beneficios antes mencionados. Este préstamo se aprecia en la siguiente grafica.

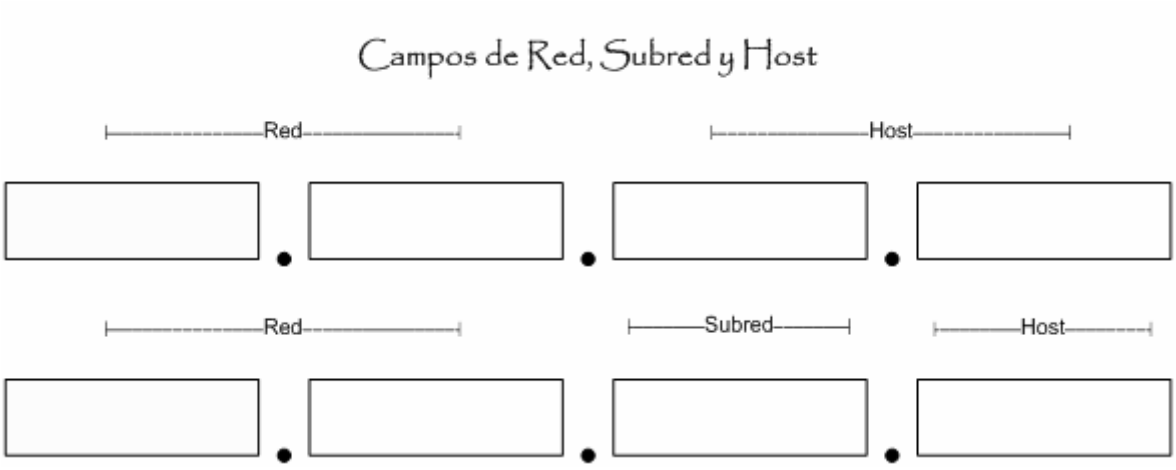


Tabla 1.5. Campos de Red, Subred y Host

Otro de los elementos que nacen con el aparecimiento de la subred es la máscara de subred, la máscara de subred es un campo que me permite conocer cuantos de los bits de

host se tomaron prestados, este campo que acompaña a la dirección IP usa el mismo formato decimal punteado, las diferencias entre este campo y el anterior es que este campo lleva 1's en los bits que representan la red y 0's en los campos que representan al host, estos bits también tienen pesos binarios. La forma correcta en la que se deben tomar los bits del campo de host son de izquierda a derecha y en orden, es decir en la máscara de subred también se notará este orden al momento de representar los bits de red y host. En la siguiente tabla se podrán observar los valores que puede tomar el campo de máscara de subred.

BITS	EQUIVALENTE DECIMAL
1000 0000	128
1100 0000	192
1110 0000	224
1111 0000	240
1111 1000	248
1111 1100	252
1111 1110	254
1111 1111	255

Tabla 1.6. Valores Típicos de la Máscara de Subred

Una vez que se han revisado los conceptos y los valores de la máscara de subred, es preciso revisar otro tema importante, se trata de conocer cuantas subredes y host se obtendrán una vez que se lleve a cabo el proceso de realizar una subred, para ello nos valdremos de unas formulas bastante simples.

$$x + y = Número\_total\_de\_bits$$
$$2^x - 2 = Número\_de\_subredes$$
$$2^y - 2 = Número\_de\_hosts$$
$$x = Número\_de\_bits\_prestados$$
$$x = Número\_de\_bits\_res\tan tes$$

Para poder encontrar las direcciones de las subredes, los routers y hosts realizan operaciones lógicas AND entre la dirección IP y la máscara de subred, el resultado de esta operación nos da como resultado la dirección de la subred en la que estamos trabajando, de esta manera los nodos identifican a la red a la cual se envían los datos.

1.1.4.3.2.3 Modelo de Operación

El protocolo de Internet básicamente realiza dos funciones: Direccionar y Fragmentar

El protocolo de Internet se encarga la transmisión de bloques de datos llamados datagramas desde la fuente hasta su destino, estos son identificados gracias a las direcciones IP tanto de la fuente como del destino que están sujetas a los datagramas mediante los encabezados. La selección de las rutas para la transmisión se denomina routing. El protocolo de Internet también ofrece la opción de fragmentar y reensamblar datagramas extensos, en caso de ser necesario para poder lograr la transmisión de los mismos a través de redes que procesan paquetes pequeños.

El protocolo de Internet no provee facilidades para una comunicación confiable, no existen confirmaciones, ya sean de salto a salto o de extremo a extremo, tampoco posee control sobre errores de datos, ni pedidos de retransmisión o controles de flujo; es decir se encarga de direccional los datos y el resto se lo deja a protocolo de capa superior.

Para poder mejorar el servicio que presta, el protocolo de Internet se vale de cuatro herramientas dentro de su encabezado, las cuales son: Type of Service, Time to Live, Options y Header Checksum. Todas estas funciones se han revisado previamente, por lo que es suficiente citar que dentro de estos los más relevantes son TTL, ya que una vez que este parámetro llegue a cero el datagrama será descartado; otro de los parámetros importantes para mejorar sus funciones es el de checksum que provee una verificación de que la información usada en el procesamiento del datagrama se ha enviado correctamente, lo que significa que los datos en sí pueden tener errores, en caso de presentarse algún error, el datagrama es destruido por el nodo que detecta el mismo.

El proceso de transmisión de los datos se realiza de la siguiente manera: en primera instancia el modulo TCP realiza una llamada al módulo de Internet, al cual le dará el

segmento TCP (incluye el encabezado y los datos) que se convertirá en los datos del datagrama de Internet; además “el módulo TCP le proporcionará la dirección y otros parámetros al encabezado IP”[12], con estos parámetros el protocolo de Internet podrá crear el datagrama y a su vez llamará al modulo de interfase de red para la transmisión del mismo.

La interfase de red crea un encabezado de red local y le añade a este el datagrama, luego procede a la transmisión de los datos; el datagrama llega al gateway que estaba en el encabezado de red local, la interfase de este gateway extrae el datagrama y lo pasa al modulo IP del gateway, este verifica la dirección IP al que esta enviado el paquete y determina si debe enviar los datos en una segunda red, al mismo tiempo el modulo IP determina la dirección de la red local a la que debe pasar la información para que llegue a su destino; después llama al módulo de interfase de red de esta nueva red y le envía el datagrama.

Esta nueva interfase de red vuelve a repetir el proceso de crear un encabezado de red local y le añade el datagrama para enviar los datos al siguiente host de destino.

En el nuevo host la interfase de red extrae el datagrama y se lo entrega al modulo de Internet, este verifica si la información va dirigida a algún protocolo superior dentro del mismo host, si resulta positiva esta conformación le entrega los datos al protocolo superior, en este caso TCP; y, este a su vez le entrega los segmentos a la aplicación destinada.

1.2 DEFINICION DE ISP

Un ISP es la abreviación en inglés de Internet Service Provider, o en español Proveedor de Servicios de Internet, son compañías que se dedican a proveer a personas u otras empresas el acceso al Internet, además de brindar servicios de Web hosting, dominios, e-mail, entre otros. Los ISP’s por lo general ofrecen dos tipos conexiones para acceso al Internet, uno de ellos es por medio de conexiones dial-up o mediante conexiones de banda ancha, también cabe destacar que estas empresas pueden ofrecer diferentes velocidades de acceso, dependiendo del tipo de conexión.

[12] http://www.faqs.org/rfcs/rfc791.html

Dentro de la definición de un ISP se debe tomar en cuenta otros conceptos que nos ayudarán a conocer el funcionamiento del mismo, a continuación vamos a revisar el concepto de última milla.

La última milla es cualquier tipo de tecnología de telecomunicaciones que va desde las empresas de telecomunicaciones hasta un usuario o empresa, recorriendo distancias relativamente pequeñas y dotando comunicación entre ellos. Puesto en otras palabras, la última milla viene a ser la tecnología a nivel de barrios con la que las empresas de telecomunicaciones planean llegar a los usuarios.

La última milla es uno de los desafíos más grandes a nivel tanto tecnológico y económico, ya que se debe combatir problemas técnicos para poder entregar, en nuestro caso una señal de Internet de banda ancha de niveles óptimos; y, por otro lado se debe pelear con los costos que esto implica, debido a los grandes retos que implica la infraestructura de la última milla para un ISP, se ha empezado a usar una nueva tendencia que es la de hacer la últimas milla una unión de varias tecnologías, es decir una última milla mixta, conjugando lo mejor que puede ofrecer una u otra tecnología.

Una vez que se ha revisado lo que es un ISP y la última milla, pasaremos a revisar en forma breve, algunos conceptos legales para la prestación de los servicios de Internet en nuestro país Ecuador.

1.2.1 Base Legal de Prestación de Servicios de Internet

Para poder prestar los servicios de Internet, en nuestro país se debe cumplir con el "Reglamento para la Prestación de Servicios de Valor Agregado"[13], el cual es elaborado por el Consejo Nacional de Telecomunicaciones (CONATEL).

Dicho reglamento encasilla como servicio de valor agregado al servicio de Internet, y además le da en ciertos artículos de esta ley normativas claras para el funcionamiento de un ISP; en esta parte solo revisaremos los artículos que he considerado de mayor relevancia, dejando a discreción del lector la revisión completa de este reglamento.

[13] Revisar Anexo 1

En una primera instancia el reglamento del CONATEL resuelve que los servicios de valor agregado son aquellos que usan servicios finales de telecomunicaciones e incorporan ciertas aplicaciones para transformar la información que ha de ser transmitida.

Para poder instalar, operar y prestar los servicios de valor agregado, en nuestro caso servicios de Internet se debe tener el titulo habilitante, que es un permiso emitido por la Secretaria Nacional de Telecomunicaciones (SENATEL) previa la autorización del CONATEL.

La duración de los títulos habilitantes es de diez años y pueden ser renovados por un periodo igual, lo que significa que todo ISP que labore en el país tiene derecho de funcionamiento de diez años por lo menos.

El área de cobertura para la prestación de los servicios que se le otorga a una empresa es de nivel nacional, pero se puede iniciar los servicios en áreas regionales o locales, lo que nos facilita a entregar los servicios de Internet según la empresa despliegue su infraestructura.

Para poder conseguir nuestro titulo habilitante debemos especificar los siguientes parámetros:

a) “Objeto
b) Descripción técnica del sistema que incluya infraestructura de transmisión, forma de acceso de conexión con las redes existentes.
c) Descripción de los servicios autorizados, duración, alcance y demás características técnicas especificas relativas a la operación de los servicios de valor agregado.
d) Las causales de extinción del permiso.”[14]

El reglamento del CONATEL también estipula que aquellos solicitantes que se dispongan a usar el espectro radioeléctrico deben incluir el titulo habilitante que requieren, ya que estos permisos deben tramitarse al mismo tiempo para la correcta operación en nuestro caso de los ISP.

[14] “Reglamento para la Prestación de Valor Agregado”, CONATEL, art. 9, pág. 2.

Una vez que alguna empresa o persona haya obtenido el titulo habilitante deberá respetar el principio de libre competencia y en caso de tener más de una compañía transparentar su situación económica.

Las empresas que posean los titulo correspondientes tienen derecho a la conexión internacional desde y hacia sus nodos principales, esto lo pueden hacer mediante infraestructura propia o mediante la contratación de servicios portadores; de la misma manera tienen derecho a la conexión entre sus nodos principales y secundarios, una vez más tienen la opción de realizar esto mediante infraestructura propia o mediante la contratación de servicios portadores.

Otro aspecto importante es que las empresas que dan servicios de valor agregado como Internet tiene derecho al acceso a cualquier red publica de telecomunicaciones previa la firma de los contratos de interconexión.

El reglamento establece en forma clara para los proveedores de servicios de Internet, en su artículo 25 sección a) es lo siguiente:

a) "Los permisionarios proveedores de servicios de Internet:
    1. Podrán acceder a sus usuarios a través de servicios portadores y/o finales.
    2. Podrán acceder a sus usuarios mediante el uso de infraestructura propia siempre y cuando obtengan el titulo habilitante para la prestación de servicios portadores y/o finales."[15]

Finalmente uno de los aspectos más importantes para un ISP en nuestro medio es que los usuarios corporativos de acceso a Internet, deberán suscribir el contrato para la respectiva red de acceso con los operadores finales y/o portadores debidamente autorizados, esto por supuesto que el proveedor del servicio de Internet no cuente con los permisos necesarios para poseer una infraestructura propia.

[15] "Reglamento para la Prestación de Valor Agregado", CONATEL, art. 25, pág. 5.

1.3 SITUACIÓN ACTUAL EMPRESARIAL

En esta parte del presente documento nos enfocaremos en la situación de una compañía de proveedora de servicios de Internet que busca expandirse e incluir entre sus clientes a los sectores residenciales; cabe destacar que el presente estudio busca una solución tanto técnica como económica de llegar los clientes residenciales, y que puede ser aplicada a cualquier tipo de ISP, sin embargo debemos tomar como referente a una de estas empresas, la empresa que nos servirá de modelo es New Access S.A., tomaremos como ejemplo y revisaremos la situación de esta empresa debido a sus antecedentes y metas a futuro.

1.3.1 Antecedentes

New Access es una empresa proveedora de servicios de Internet, la cual fue constituida y ha entrado en operaciones desde el año 2002, la empresa presta servicios a la capital del Ecuador, tanto al Distrito Metropolitano de Quito como a sus alrededores.

Figura 1.17. Referencia Geográfica del Distrito Metropolitano de Quito

El Distrito Metropolitano de Quito se encuentra ubicado en plena cordillera de los Andes, haciendo de esta una ciudad peculiarmente angosta, lo que en consecuencia nos deja a sus valles aledaños un tanto separados de la zona urbana.

Desde sus inicios esta compañía se ha especializado en abarcar entre sus clientes a empresas, es decir, sus clientes son en su mayor parte corporativos, este es principalmente el mejor motivo para tomar a New Access como la empresa más prometedora para el desarrollo del presente estudio.

New Access posee su nodo principal en pleno corazón de la ciudad de Quito, aledaños al parque de la Carolina, y posee varios nodos secundarios a lo largo de la ciudad para poder tener una cobertura de la ciudad y sus alrededores.

A principios de operación este ISP poseía una salida internacional por medios satelitales, principalmente por las falencias de conexión a nivel de nuestro país Ecuador; pero actualmente la empresa posee sus salidas internacionales por medio de fibra óptica lo cual mejora la calidad del servicio y a su vez los vuelve más competitivos, es precisamente esta competitividad la que impulsa a New Access a querer diversificar su cartera de clientes, para poder llegar a sectores residenciales.

1.3.2 Objetivo Comercial

New Access nace en primera instancia como un ISP dedicado principalmente a dar servicios de Internet a clientes empresariales, dejando de lado en primeras instancias a los clientes residenciales; pasada la primera etapa de toda empresa, que es la de posicionarse en el mercado, se prevee la expansión de su cartera de clientes.

Como es de conocimiento del lector, el término clientes residenciales es un poco amplio, por lo que debemos especificar un sector en especial al referirnos este tipo de clientes, en nuestro caso de estudio y de la empresa proveedora de servicios de Internet, nos interesa específicamente los conjuntos residenciales y edificios de departamentos, más no a los clientes residenciales fuera de estas zonas habitacionales.

La expansión de la empresa, comprende no solo un crecimiento de clientes, sino la diversificación de los mismo, en este caso se planea la inserción de los clientes residenciales, pero este crecimiento debe ir de la mano con un cambio en la infraestructura que maneja la empresa, en este caso la última milla del ISP debe también acomodarse a este nuevo objetivo comercial de la empresa.

Una vez que se ha decidido por incluir a los clientes residenciales a la cartera de clientes, se deben fijar metas en el campo comercial, ya que este segmento del mercado reacciona de manera distinta que el sector corporativo.

El primer cambio que se debe tener en cuenta a la hora de comparar los clientes corporativos y los clientes residenciales es el costo a pagar por el servicio, ya que un cliente particular seguramente no esta dispuesto a pagar las mismas sumas de dinero que una empresa. Por otro lado el segmento de mayor competencia es el residencial, por lo que los precios que se ofrezcan al consumidor deberán ser iguales o mejores que la competencia; para poder lograr esta meta es necesario que la parte de infraestructura se adapte a estas necesidades.

Parte de la política de la empresa como lo refleja la campaña a nivel comercial de New Access es la de ir de la mano con la tecnología y ofrecer al cliente la mejor solución que se ajuste al cliente, este es un concepto que se desea llevar y aplicar a estos nuevos usuarios; y ya, que parte del éxito al incursionar con los clientes residenciales es la calidad y la versatilidad del servicio, la política de la empresa se ajusta a estos nuevos clientes.

La ventaja de esta política comercial es que le permite a la parte técnica acogerse a varias tecnologías para poder prestar estos nuevos servicios, con el respaldo de un ente administrativo, en pos de un servicio de calidad.

1.3.3 Infraestructura Actual de la Empresa

Como se mencionó en las página anteriores, el ISP que tendremos como referencia es la empresa New Access, parte de los diseños que se presentarán como posibles soluciones se ajustan a la realidad actual de esta empresa, pero cabe destacar que la infraestructura que presenta esta empresa es la más flexible y la que nos brindará las mejores condiciones para la implementación de este tipo de proyectos.

Empezaremos por citar la infraestructura que posee la empresa en sus nodos, principal como secundarios; posteriormente revisaremos sus salidas internacionales.

La infraestructura existente en el nodo principal es de carácter inalámbrico, punto-multipunto y punto-punto, en el nodo principal existen seis zonas de cobertura cada una con una abarcando de 60º, que en conjunto cubren 360º. Este nodo principal se encuentra ubicado en la parte norte de la ciudad de Quito, colindante a la parte norte del parque de La

Carolina. A este nodo principal se enlazan varios clientes mediante la infraestructura punto-multipunto, y mediante la infraestructura punto-punto se enlazan los nodos secundarios. Dentro de este nodo principal se encuentran tanto los routers principales, y los servidores de aplicaciones para el funcionamiento del tráfico y demás servicios asociados con un ISP.

En los nodos secundarios podemos encontrar de igual manera infraestructura inalámbrica tanto punto-punto como punto-multipunto, la primera para enlazarse al nodo principal y en ocasiones a otro nodo secundario y la segunda para comunicación con clientes, los nodos secundarios cumplen la función de repetidores.

New Access posee dos salidas internacionales por medio de fibra óptica, cada una conectada a un portador diferente, esto le permite tener un respaldo en caso de falla de cualquiera de las ellas y además le permite balancear a sus clientes para evitar problemas de saturación del ancho de banda.

Cabe destacar que la empresa trabaja con una red IP, debido principalmente a las facilidades y versatilidad de este tipo de redes y por otro lado respondiendo a la necesidad de la mayoría de clientes que requieren canales libres y transparentes.

A continuación se mostrará una figura de la infraestructura actual de la empresa, de tal manera que se pueda observar los elementos más representativos que se encuentran en este momento al servicio de New Access.

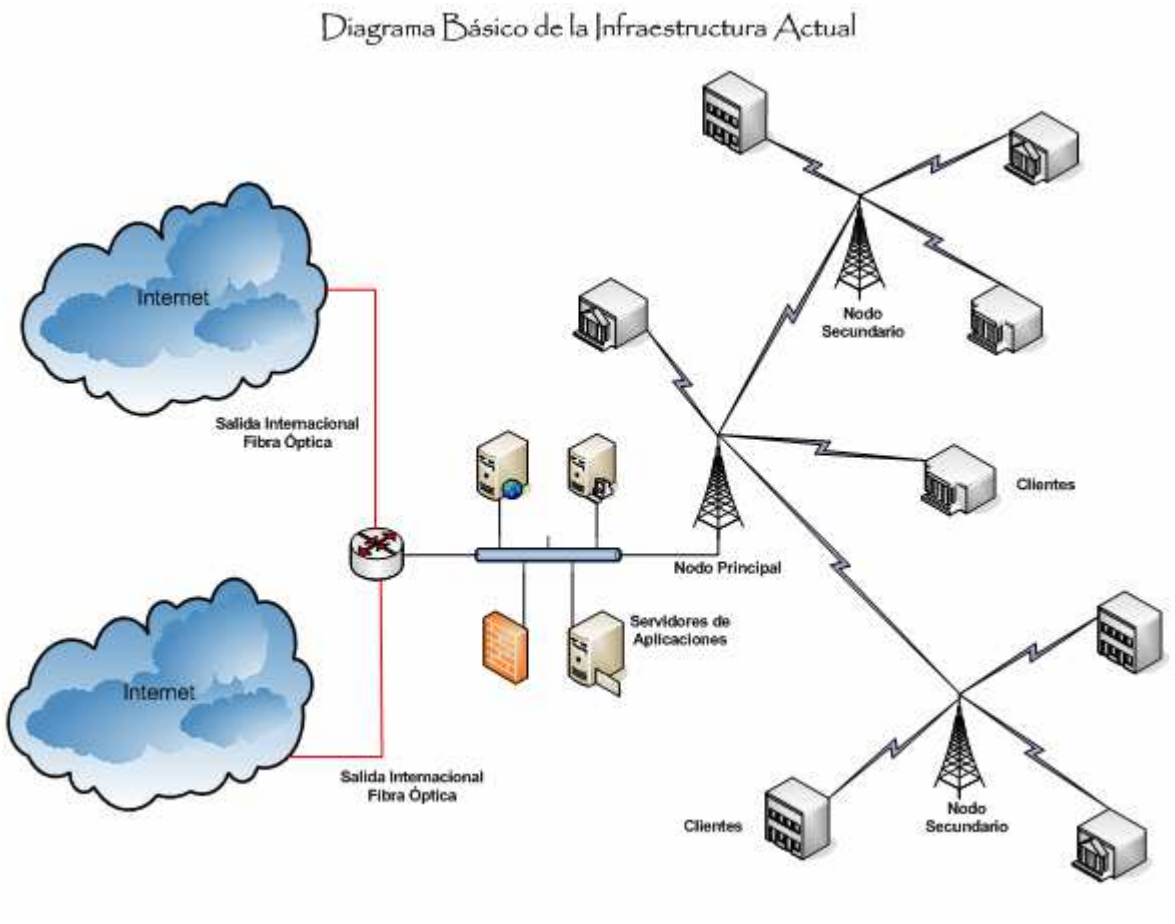


Figura 1.18. Diagrama Básico de la Infraestructura Actual

CAPITULO II

DESCRIPCIÓN DE LAS TECNOLOGIAS DE ACCESO

2.1 ETHERNET

2.1.1 Historia

Los inicios de Ethernet se propiciaron a principios de 1970, en los laboratorios de XEROX, su creador es Robert Metcalfe, quien en ese momento trabajaba en la división de nuevos proyectos, comenzó a desarrollar un esquema de comunicación entre computadoras, con un tráfico moderado y esporádicamente con tráfico elevado. Pero no es hasta 1973 que Metcalfe en una carta a sus jefes hace notar la posible utilidad de su creación.

Originalmente Ethernet fue desarrollado para redes basadas en cables coaxiales, con una tasa de transmisión máxima de 3 Mbps y con CSMA/CD o Carrier Sense Multiple Access Collision Detect, este último un protocolo que permitía que varias máquinas se comunicaran a través de un mismo canal sin necesidad de testigos.

Metcalfe abandona finalmente XEROX en 1979 y decide fundar su propia compañía llamada 3COM, durante un breve periodo de tiempo se dedica a convencer mediante charlas y disertaciones en universidades el potencial del uso de las computadoras personales así como el de su invención, finalmente decide acudir a tres compañías DEX, Intel y XEROX (DIX) para juntarse y promover a Ethernet como un estándar para ser utilizado en las crecientes y nuevas redes de computadoras.

DIX en el año de 1980 desarrolla una Ethernet capaz de comunicarse a velocidades de 10 Mbps y a través de par trenzado, de esta manera nace la Ethernet 1.0, que fue posteriormente estandarizada con el nombre de IEEE 802.3.

En un principio se pensaba que Ethernet no podría satisfacer las necesidades de las redes de comunicaciones, se especulaba que Token Ring era superior teóricamente, pero la realidad era que Ethernet se desempeñaba tan bien que al poco tiempo opacó a su competencia y en el proceso 3COM que comercializaba las tarjetas de interfaz de red o NIC por sus siglas en inglés se convirtió en una de las empresas más grandes del mercado, para satisfacción de su fundador y creador de Ethernet.

2.1.2 Introducción

Ethernet como se mencionó anteriormente fue estandarizada en la IEEE 802.3, el modelo que se llevó a la estandarización fue el Ethernet 1.0, pero a lo largo de los años se han realizado modificaciones y actualizaciones a este estándar, motivado en parte por el gran crecimiento de las redes Ethernet y las velocidades a las que se puede transmitir datos gracias a esta tecnología; en esta parte del documento revisaremos de manera general algunos datos acerca de 802.3 para luego entrar más en detalle.

Uno de las conceptos que vamos a revisar es el de DTE y DCE, conceptos que se aplicarán a lo largo de esta descripción de Ethernet.
DTE, data terminal equipment, o en español equipo terminal de datos; este es un dispositivo que puede ser tanto la fuente como el destino de las tramas de datos.
CDE, data communication equipment, equipo de comunicación de datos; estos son equipos intermedios de la red que reciben y direccionan las tramas a través de la red.

Otro de los términos que se verán a lo largo de este capitulo es el de NIC, este término es la agrupación de las siglas de network interfase card, o como ya se mencionó con anterioridad tarjeta de interfase de red.

Ethernet es una tecnología que permite la comunicación de varias máquinas o dispositivos de red a través de un mismo medio físico, por medio físico nos referimos a los cables y otros dispositivos que nos permiten conectar las computadoras entre sí. Existen

como es de imaginarse una serie de formas de llevar dichas conexiones a cabo, esto se conoce como topologías, y por lo que se ha escrito se puede deducir que existen varias configuraciones de topologías aplicables a Ethernet; pero, por más complejas que sean estas combinaciones podemos decir que son "una combinación de tres conexiones básicas: Punto-Punto, Topología Bus y Topología Estrella."[16]

Para poder clarificar de mejor manera estos tres tipos de conexión, se procederá a ilustrarlas mediante las siguientes gráficas.

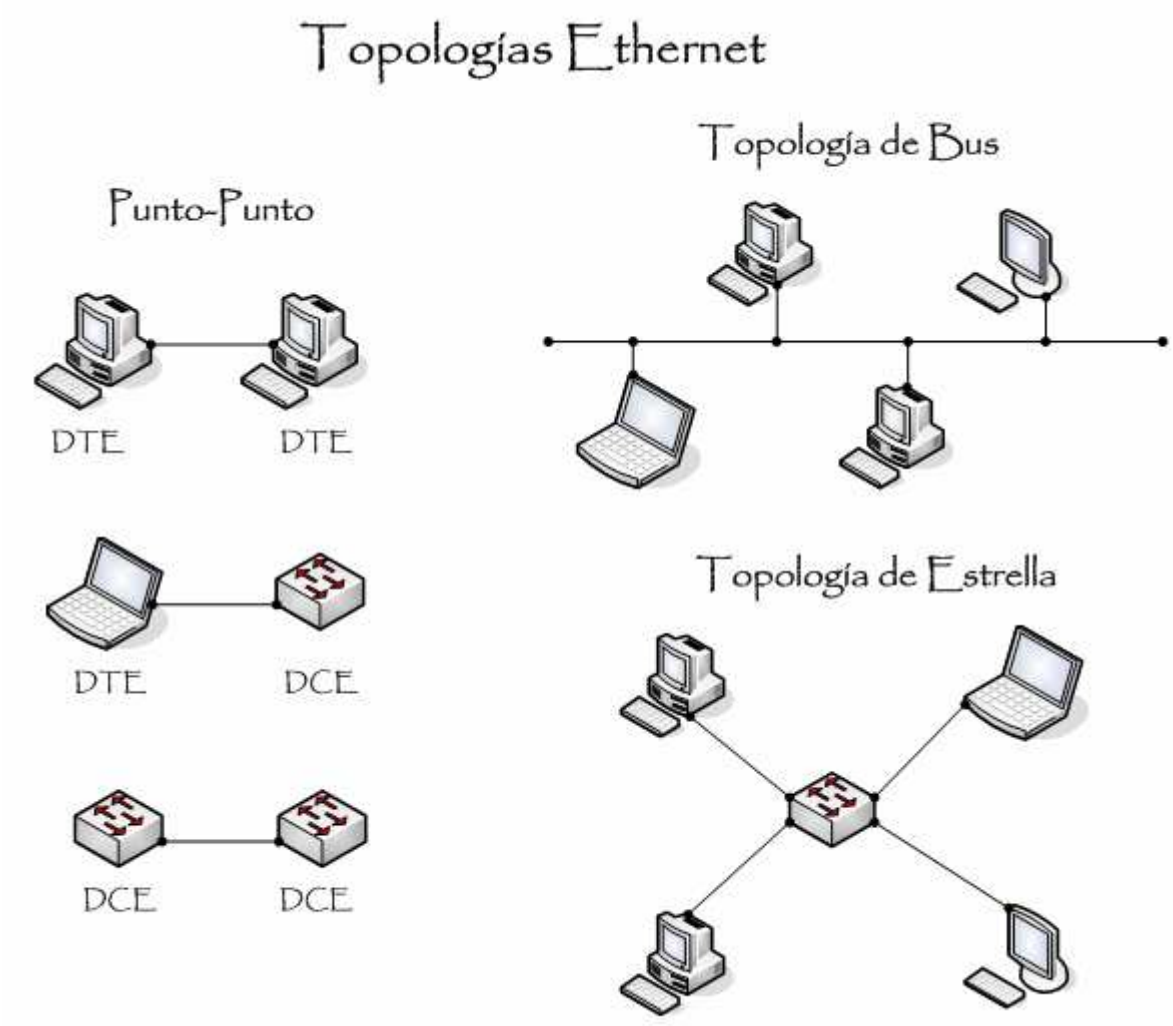


Figura 2.1. Topologías Ethernet

Una vez que Ethernet fue estandarizada en la IEEE 802.3, sus capas fueron diseñadas para poder tener congruencia y funcionamiento con otro modelo conocido como el modelo OSI, es decir posee una capa física y una capa de enlace.

[16] http://www.cisco.com/univercd/cc/td/doc/cisntwk/ito_doc/ethernet.htm

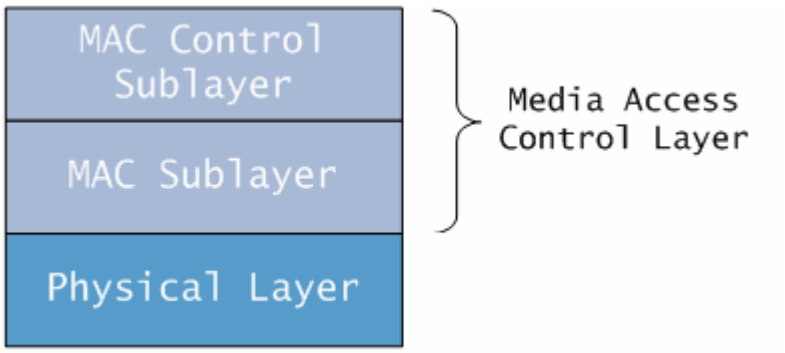


Figura 2.2. Capas Ethernet

Como se puede apreciar en la figura de arriba, 802.3 posee dos capas, la primera la capa de control del medio de acceso y la segunda la capa física, sin embargo la primera se subdivide en dos partes, la subcapa MAC y la subcapa MAC Control que es una capa opcional, ya que en su lugar podría ir otra subcapa denominada LLC que esta bien detallada en la norma IEEE 802.2 o en su lugar una capa superior perteneciente a otro protocolo.

La capa MAC controla el acceso del nodo a la medio físico de la red, el único requerimiento para una comunicación básica entre dos nodos de una red es que ambas capas MAC puedan soportar la misma tasa de transmisión (Si no interviene un protocolo de capa superior); por otro lado la capa física es la que se encarga de especificar parámetros como la tasa de transferencia de datos, la codificación de la señal y el tipo de medio de conexión entre los nodos.

Hay que tener en cuenta que las dos capas de Ethernet, en especial la física, representan la etapa más baja en el proceso de comunicación, siendo de esta manera las capas pueden ser implementadas por las NICs, la capa física sería totalmente implementada agregando el cable y los equipos de interconexión.

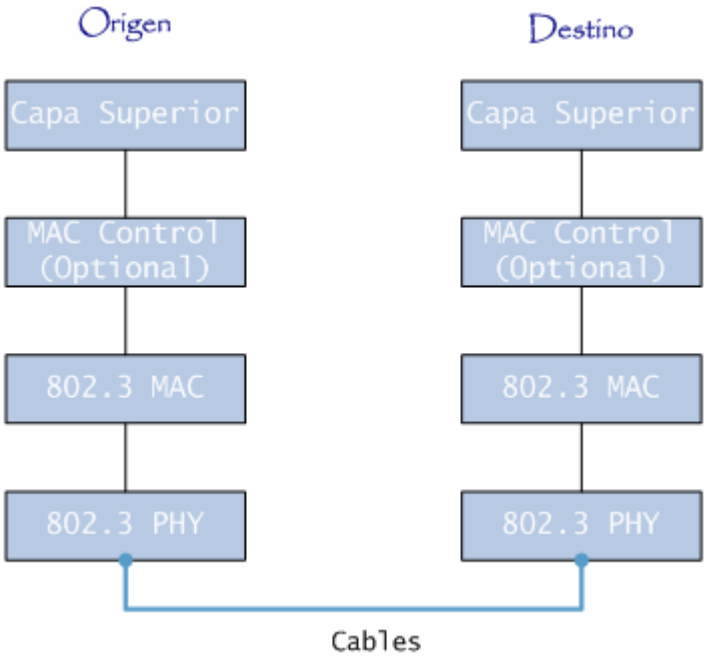
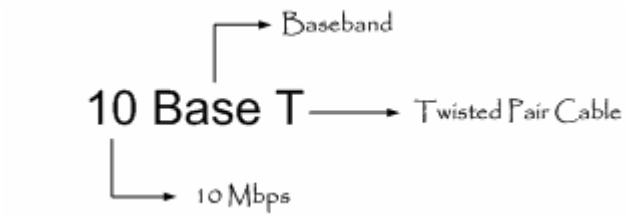


Figura 2.3. Flujo de Información a través de las Capas Ethernet

Para referirnos a las cualidades que posee la capa física se ha llegado a una convención de nombres, la cual consiste en la agrupación de tres términos, los cuales cada uno representa una de las tres cualidades que controla esta capa que son: Tasa de transmisión, el método de transmisión y la codificación del tipo de señal del medio. Se podrá apreciar de mejor manera esta convención con el siguiente ejemplo.



Del ejemplo anterior podemos fácilmente apreciar que nuestro primer término representa la tasa de transferencia en Mbps, el segundo término la codificación de la señal, y por último el método de transmisión, por lo general se apreciará siempre el término Base referente a la modulación banda-base, debido a que las implementaciones Ethernet son hechas de esta manera, en algún momento en los inicios de esta tecnología se podía ver Broad por modulación de banda ancha, lamentablemente no tuvo un buen desempeño por lo que se dejo de fabricar adaptadores Ethernet para este tipo de sistemas.

2.1.3 Capa MAC

La capa MAC le permite a un protocolo de capa superior o MAC client el realizar intercambiar datos entre otras capas superiores de una o varias entidades a la vez.
La subcapa MAC Control le provee servicios adicionales, por ejemplo la de controlar la operación de la subcapa MAC; esta acción puede ser usada para implementar un control de flujo entre los pares MAC client a través del canal.

Las interacciones entre las capas superior e inferior y las subcapas MAC se pueden apreciar de mejor manera en el siguiente gráfico.

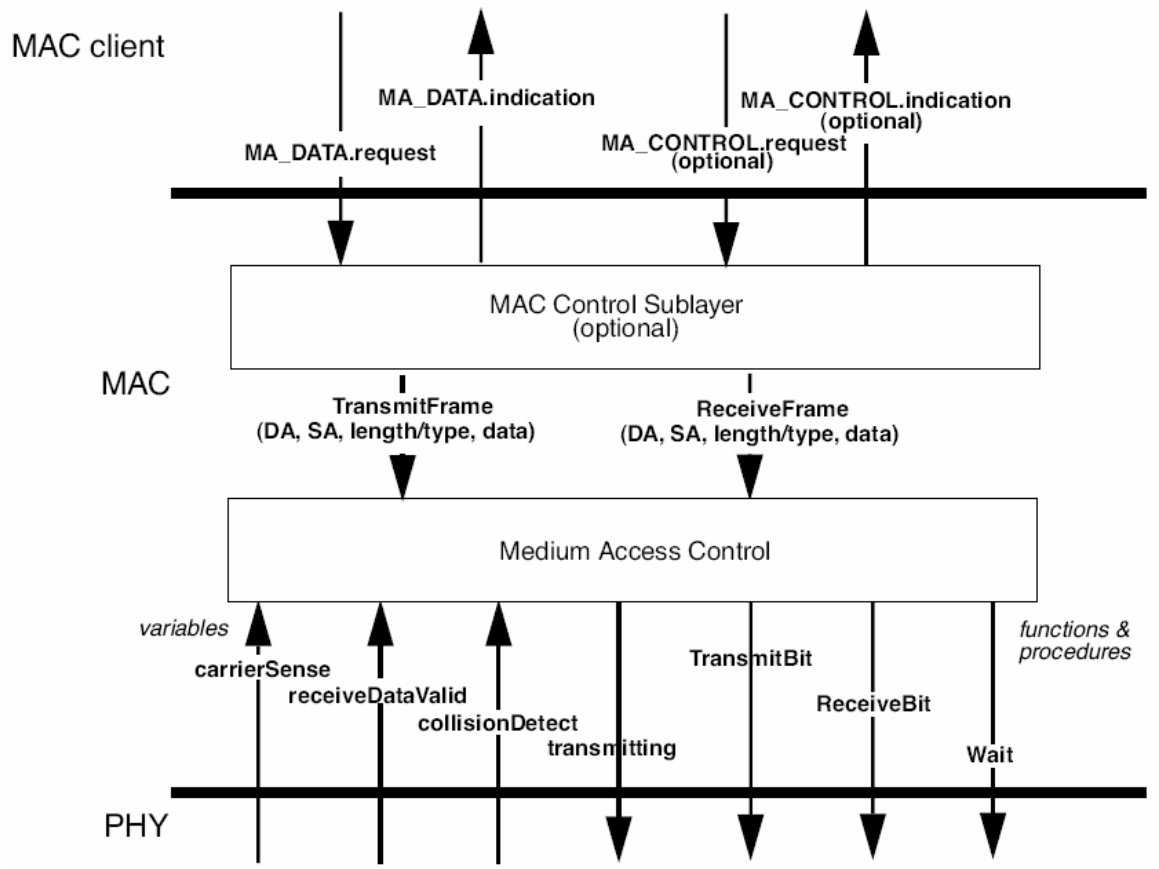


Figura 2.4. Interacción entre las Capas y Subcapas Ethernet[17]

En la figura se puede apreciar fácilmente las interacciones que existen entre la capa MAC y las capa superior o MAC client, estas son: MA_DATA.request, MA_DATA.indicator, MA_CONTROL.request y MA_CONTROL.indicator.

[17] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

MA_DATA.request y MA_DATA.indicator son las interacciones entre la capa MAC y las capas superiores, estas son obligatorias; MA_CONTROL.request, MA_CONTROL.indicator son las interacciones opcionales y serán obligatorias solo cuando la subcapa MAC control sea implementada.

A continuación se podrá revisar las funciones de cada una de las cuatro interacciones que existen entre la capa MAC y su inmediata superior.

- ✓ MA_DATA.request, es una primitiva que define la transferencia de datos desde una capa superior hacia una o varias entidades pares, esta es generada cuando la capa MAC client necesita transferir datos.

- ✓ MA_DATA.indicator, es la primitiva que se encarga de definir la transferencia de datos desde la subcapa MAC (a través de la subcapa MAC control si esta se encuentra implementada) a la entidad o entidades MAC client, esta primitiva se genera cuando un dato arriba a la subcapa MAC y este es destinado a una capa superior.

- ✓ MA_CONTROL.request, esta que es una primitiva optativa se encarga de definir la transferencia del control del comando desde una capa MAC client hacia la subcapa MAC control.

- ✓ MA_CONTROL.indicator, al igual que la primitiva anterior esta es opcional y se encarga de definir la transferencia del control de la subcapa MAC control a la MAC client.

La subcapa MAC realiza las siguientes acciones:

1. Encapsulamiento de datos
    a. Entramado, se encarga de la delimitación y la sincronización de la trama.
    b. Direccionamiento, maneja tanto las direcciones de origen y destino.
    c. Detección de Errores, detección de errores de transmisión de medios físicos.
2. Manejo del Medio de Acceso
    a. Revisión del Medio, evita colisiones.

b. Medidas de Contención, maneja las colisiones.

Además de manejar las acciones antes mencionadas la subcapa MAC debe ser capaz de soportar dos tipos de operación, el uno half duplex y el otro full duplex.

En el modo half duplex las estaciones deben competir por el uso del canal y la forma de pelear por este canal esta definida por los algoritmos DCMA/CD. En este modo la comunicación bidireccional se logra mediante un intercambio rápido de tramas; el modo half duplex se puede conseguir en cualquier medio que soporte la tecnología Ethernet, y es requerido en aquellos medios que son incapaces de soportar tanto transmisiones y recepciones simultaneas sin interferencias.

El modo full duplex es usado solo si las siguientes condiciones se cumplen:

- El medio físico es capaz de soportar simultáneas transmisiones y recepciones sin interferencia.
- Deben haber exactamente dos estaciones en la LAN, esto permite que el medio físico sea tratado como un enlace punto a punto full duplex entre las estaciones. En tal caso no existe una pelea por el acceso al medio físico, por lo que los algoritmos de acceso múltiple como CSMA/CD se vuelven inútiles.
- Ambas estaciones deben ser capaces y deben estar configurados para ser usados en un modo de operación full duplex.

La configuración física más común para la operación full duplex consiste en un switch, con cada uno de sus puertos destinados a la conexión de un solo dispositivo.

2.1.3.1 Formato de la Trama MAC

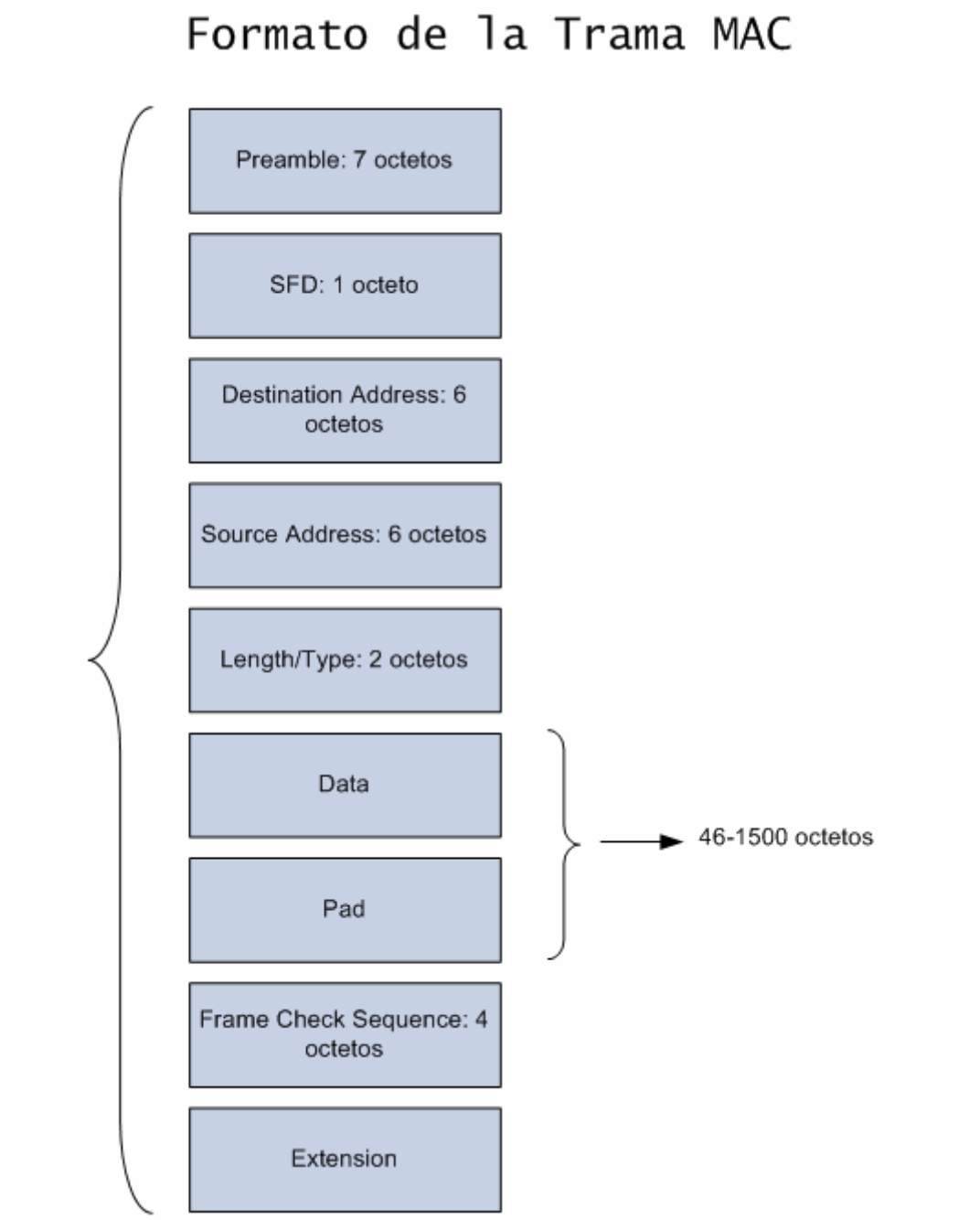


Figura 2.5. Formato de la Trama MAC

Preamble, este parámetro esta constituido por siete octetos, y es usado para permitir al circuito PLS (physical synchronization sublayer) alcanzar el estado de sincronización con el reloj de la trama recibida.

SFD (Start Frame Delimiter), este parámetro esta compuesto por un octeto, y representa la siguiente secuencia 10101011, este parámetro esta inmediatamente después de parámetro preamble y nos indica el inicio de la trama.

Destination Address, este campo nos indica la estación a la cual la trama esta destinada, esta dirección puede ser individual o de multicast, este campo esta compuesto por 6 octetos.

Source Address, este campo al igual que el anterior esta compuesto por 6 octetos, nos indica la estación de la cual la trama fue enviada, este parámetro no es interpretado por la subcapa MAC.

Length/Type, este parámetro de 2 octetos toma uno de dos significados dependiendo de su valor numérico, el primero de los dos octetos es el más relevante.
Si el valor numérico de este campo es menor o igual al valor del campo maxValidFrame entonces este campo nos indica el número de octetos datos de la capa superior contenidos en la trama, es decir actúa como un parámetro de longitud.
Si el valor numérico de este campo es mayor o igual a 1536 en decimal, entonces este campo nos indica la naturaleza del protocolo de capa superior, en este caso cumple la función de un parámetro de tipo. La interpretación de tipo o longitud de este parámetro son mutuamente excluyentes

MAC Client Data, este parámetro también se le conoce como Data, constituido por una secuencia de n octetos, este parámetro al tratarse de los datos de las capas superiores cuenta una total transparencia, ya que cualquier secuencia puede ser enviada a este campo, su única limitación es el número de octetos definido por el estándar que a sido usado, un valor mínimo debe ser usado para el correcto funcionamiento de CSMA/CD, este mínimo es especificado por la implementación a ser usada, pero en caso de no ser necesaria se añadirán bits u octetos.

Pad, este parámetro esta estrechamente relacionado con el anterior, pues para que CSMA/CD funcione de forma adecuada el parámetro Data tiene que tener un mínimo de 46 octetos y un máximo de 1500, si el campo data no es lo suficientemente grande este campo se encargara, ya sea de aumentar bits u octetos hasta tener dicha longitud, este

campo esta inmediatamente después del campo data para poder calcular e implementar en campo siguiente FCS.

Frame Check Sequence, o por su abreviación FCS; este campo esta constituido por 4 octetos, y usa una revisión de redundancia cíclica (o por sus siglas en inglés CRC) tanto en los algoritmos de transmisión y recepción, para la generación de un campo CRC a ser utilizado en este parámetro.
Este valor es computado como una función de los contenidos de source address, destination address, length, data y pad. Su codificación es definida por el siguiente polinomio generador:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Formula 2.1. Polinomio Generador CRC

"Para poder generar la CRC se realizan los siguientes pasos:

a) Los primeros 32 bits de la trama se complementan
b) Los n bits de la trama son considerados los coeficientes del polinomio M(x) de grado n-1 (el primer bit del campo destination address es el coeficiente del término x^{n-1} y el ultimo bit de campo data es el coeficiente del ternito x^0).
c) M(x) es multiplicado por x^{32} y dividido para G(x), produciendo un residuo R(x) de grado ≤ 3.
d) Los coeficientes de R(x) son considerados la secuencia de 32 bits.
e) La secuencia de 32 bits es complementada y el resultado denominado CRC."[18]

Extension, este campo esta a continuación del parámetro FCS, y consiste en una serie de bits de extensión, los cuales pueden ser distinguidos de los bits de datos, la longitud de este campo puede ir desde cero hasta una cantidad limitada por (slotTime-minFrameSize) bits; el contenido de este campo no es calculado dentro de la FCS. Este campo tendrá una extensión diferente de cero cuando se trate de implementaciones half duplex con velocidades de transmisión superiores a 100 Mbps.

[18] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

2.1.3.2 Direcciones MAC

El campo de direcciones MAC de Ethernet debe tener dos direcciones, la primera una dirección de destino y la segunda una dirección de origen, la función de cada una de estas direcciones ya se cito con anterioridad en este mismo documento, sin embargo esta sección se encargara de revisar la presentación de las direcciones.

Las direcciones, tanto la de destino como la de origen deben tener 48 bits de longitud, esto representa los 6 octetos que se propuso originalmente, cabe destacar que si las direcciones poseen menos bits, no serán reconocidos como una dirección valida Ethernet.

El primer bit de la dirección de destino, que representa al bit menos significativo puede ser usado para distinguir a que tipo de dirección representa, una dirección individual o una de grupo, si este bit posee el valor de cero, representa a una dirección individual, mientras que el valor de uno, significa que la dirección representa a un grupo; cabe destacar que una dirección de grupo puede tener como destino, ninguna, más de una o todas las estaciones conectadas a la LAN. En el caso de la dirección de origen, este bit esta reservado y posee un valor de cero.

El segundo bit es usado para distinguir direcciones administradas en forma universal/global o local, si este bit tiene el valor de cero, la administración de esta dirección es universal; y, de poseer el valor de uno la dirección tendrá administración local. Se debe tener en cuenta que al momento de ser una dirección de broadcast este valor también es uno.

La transmisión de estos campos se realiza de tal forma que los bits menos significativos se transmitan primeros.

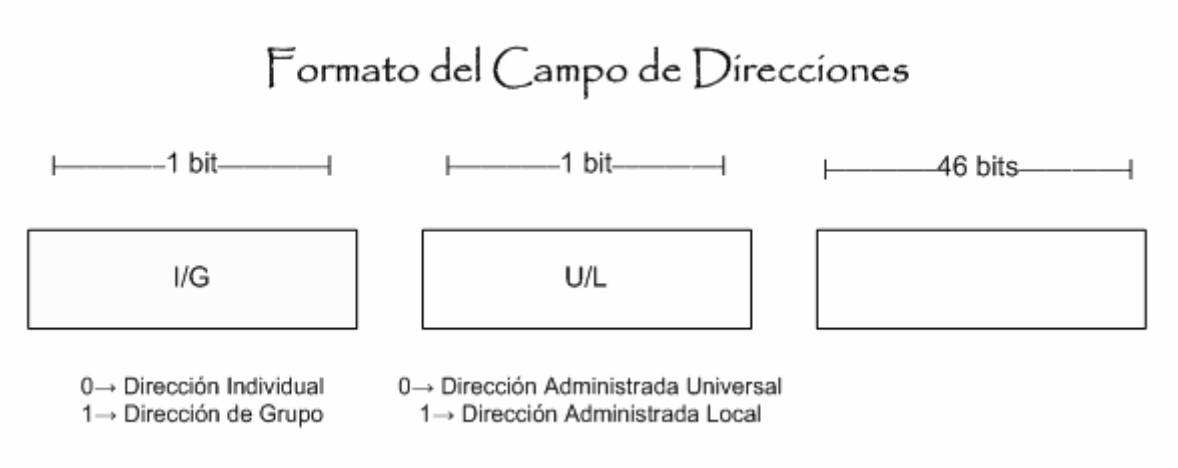


Figura 2.6. Formato del Campo de Direcciones

Como se pudo leer existen dos tipos de direcciones, las direcciones individuales y las de grupo; las direcciones individuales están relacionadas con una estación en particular; las direcciones de grupo están asociadas a múltiples destinos, es decir a una o más estaciones dentro de una red.

Existen a su vez dos tipos de direcciones de grupos, las direcciones multicast groups y las direcciones de broadcast; las primeras están asociadas a convenciones de capas superiores y a estaciones lógicamente asociadas; mientras que las segundas están asociadas a todas las estaciones conectadas dentro de la LAN.

Cuando todos los bits de la dirección de destino son 1’s, esta dirección representa una dirección de broadcast, la cual tiene como destino todas las estaciones activas dentro de una red, este tipo de dirección se usa para llegar a todas las estaciones de una red a la vez, todas las estaciones pueden reconocer una dirección de broadcast, pero no todas pueden generara una.

2.1.4 CSMA/CD

El algoritmo CSMA/CD es capaz de realizar las siguientes funciones:

Para la transmisión de tramas: Acepta datos desde la capa superior y construye la trama; le entrega a la capa física una serie de bits continuos para la transmisión al medio.

Para la recepción de tramas: Recibe una serie de datos desde la capa física; le envía a las capas superiores las tramas ya sean tramas de broadcast o tramas con direcciones directas a la estación local; descarta o pasa al manejador de red todas las tramas que no han sido enviadas hacia la estación local.

En el modo half duplex, retrasa la transmisión de la serie de bits en cualquier momento que el medio físico se encuentre ocupado.

Le añade el valor correcto del campo FCS a las tramas salientes y verifica la correcta alineación de los límites de los octetos.

Revisa las tramas entrantes para descubrir errores de transmisión mediante el campo FCS y verifica los límites de alineación de los octetos.

Retrasa la transmisión de una serie de tramas de bits por un periodo específico de tiempo de trama.

En modo half duplex, termina la transmisión cuando se detecta una colisión.

Así mismo en modo half duplex, se encarga de preparar la retransmisión después de la colisión, hasta que un límite de específico de retransmisión es alcanzado.

Una vez que se ha producido una colisión en el modo half duplex este se encarga de mantener esta colisión hasta que toda la red se encuentre al tanto de dicha acción por medio del envío de un mensaje de jam.

Se encarga de descartar las transmisiones recibidas si estas no tienen la longitud mínima.

CSMA/CD se encarga de adjuntar el preámbulo, SFD, destination address, source address, lenght/type y FCS a todas las tramas, e inserta el campo pad en aquellas tramas que no tiene la longitud mínima para ser transmitidas.

Remueve el preámbulo, SFD, destination address, source address, lenght/type, FCS y pad (en caso de ser necesario) de las tramas recibidas.

En caso de tratarse de una transmisión con velocidades superiores a los 100 Mbps y en modos half duplex, se encarga de añadir los bits de extensión a la primera trama de una ráfaga (o puede ser a la única trama) si esta tiene una longitud menor al SlotTime.

Finalmente se encarga de retirar los bits de extensión de las tramas recibidas en caso de producirse comunicaciones en el modo half duplex y a velocidades mayores a los 100 Mbps.

2.1.4.1 Modo de Operación CSMA/CD

El modo de operación de CSMA/CD esta basado en 7 procesos que son concurrentes, estos procesos son: Frame transmitter, frame receiver, bit transmitter, bit receiver, deference, burst timer y set extending.

Como se menciono, estos procesos tienen la característica de ser repetitivos, por lo tanto la mejor manera de visualizar estos procesos es mediante diagramas de bloque, los cuales serán mostrados a continuación.

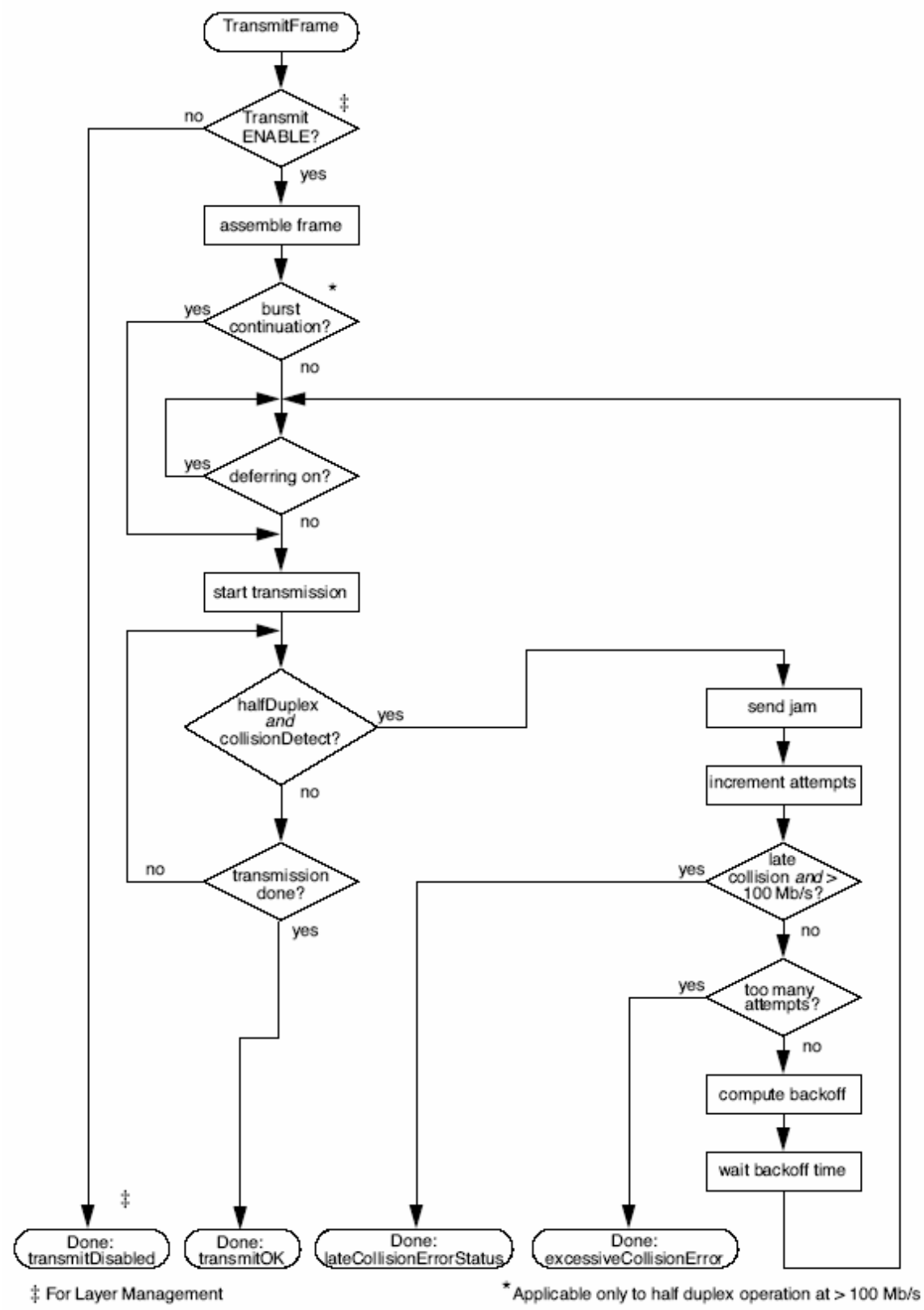


Figura 2.7. Proceso Frame Transmitter[19]

[19] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

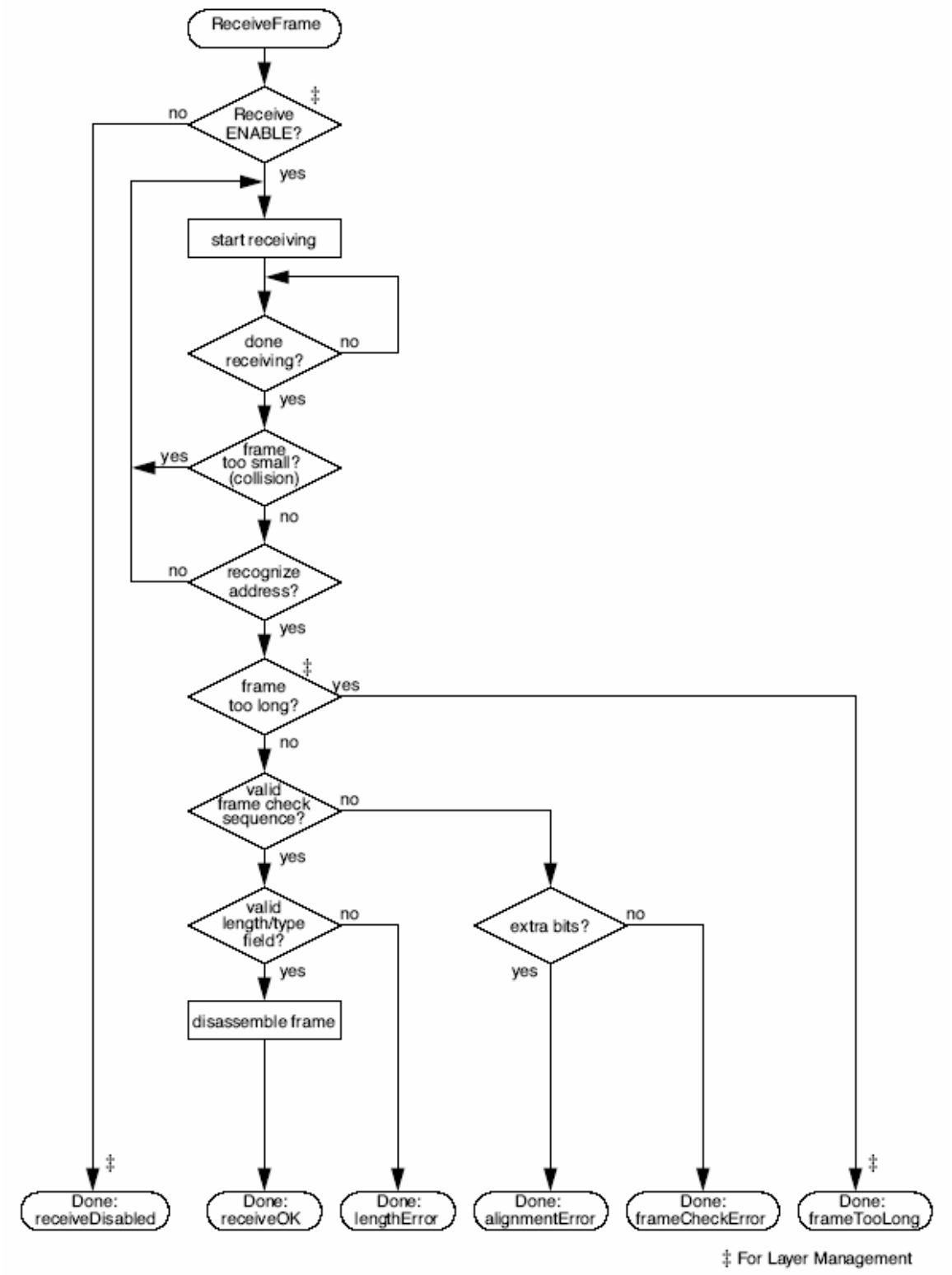


Figura 2.8. Proceso Frame Receiver[20]

[20] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

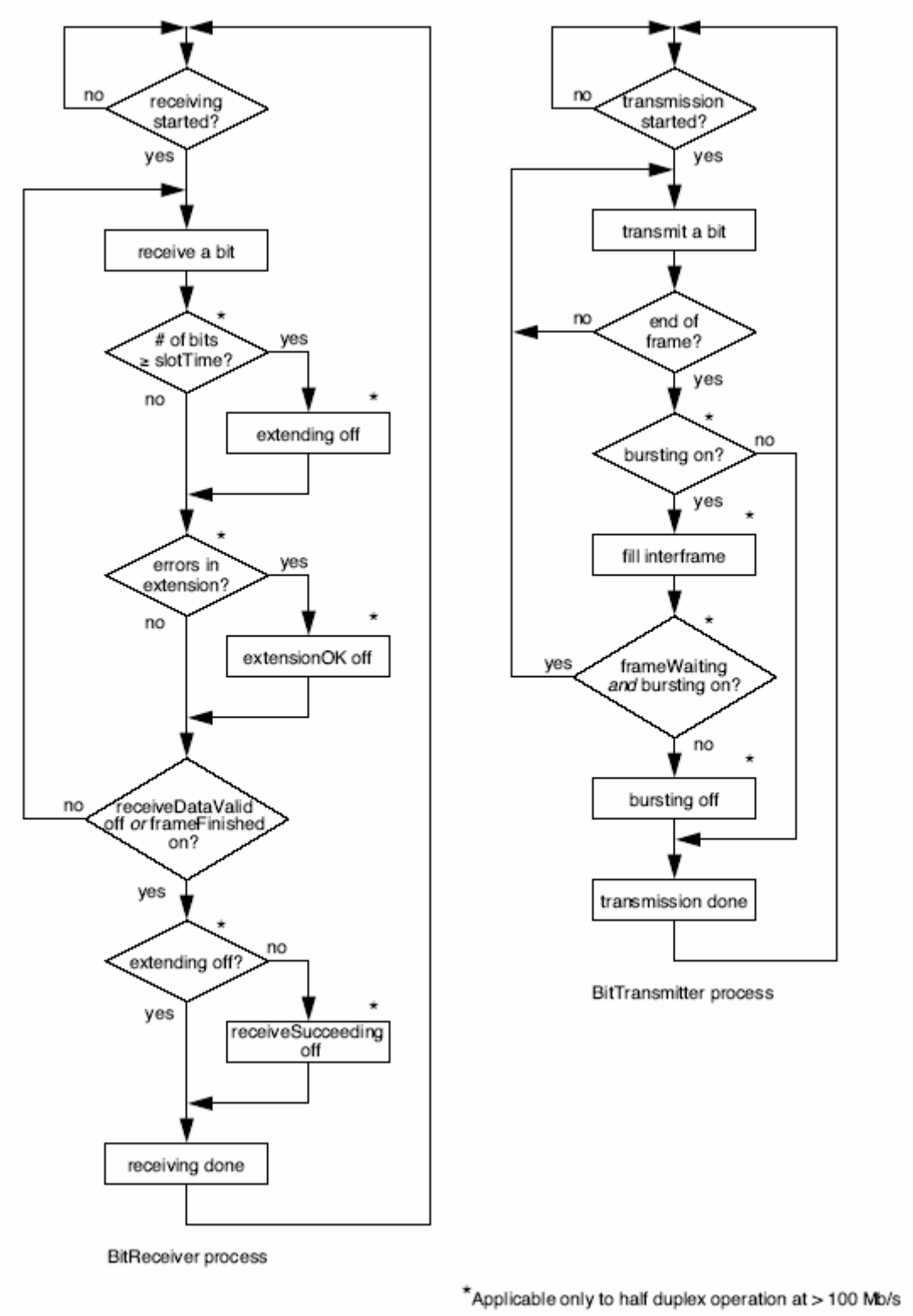


Figura 2.9. Procesos Bit Receiver y Bit Transmitter[21]

[21] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

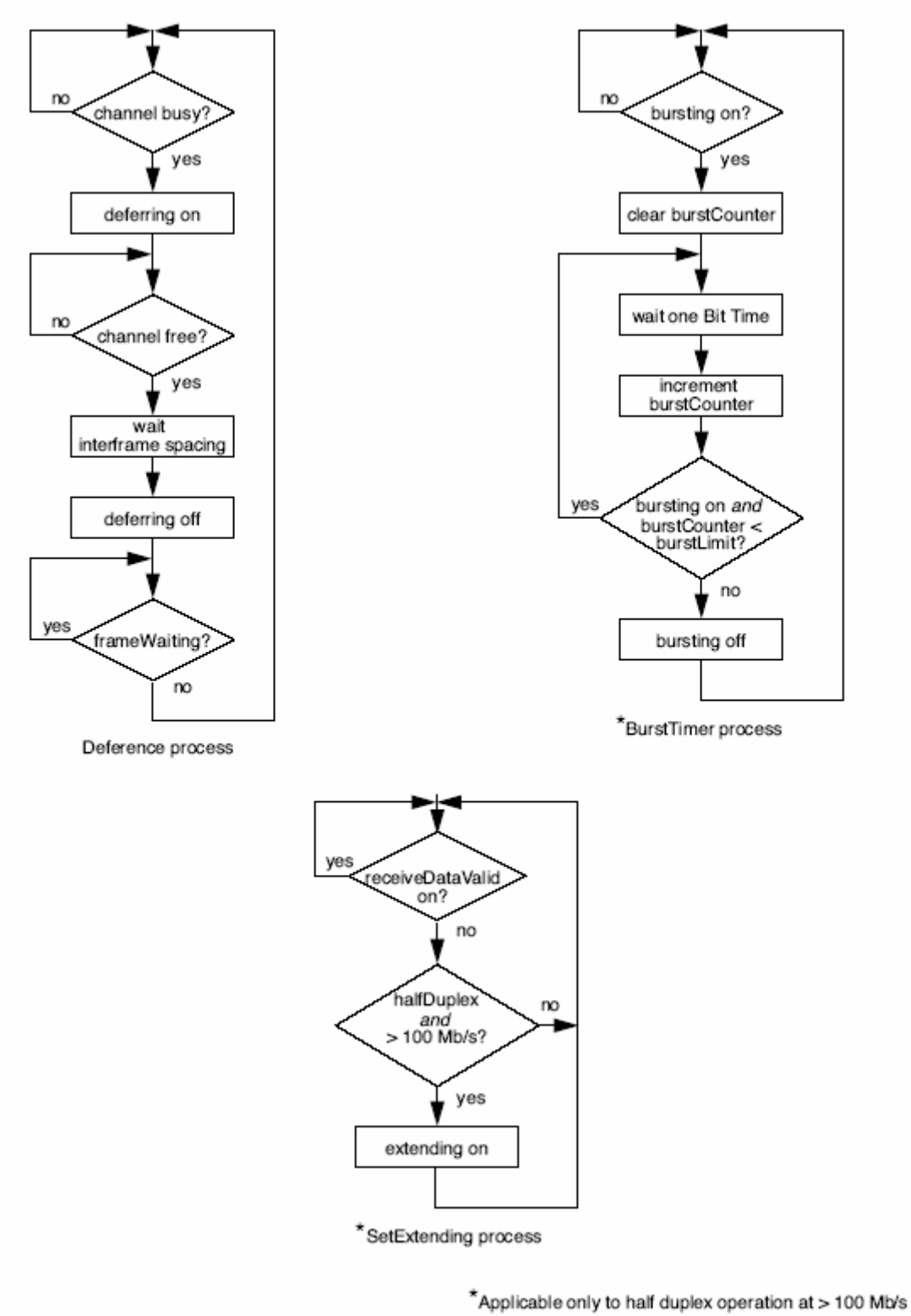


Figura 2.10. Procesos Deference, Burst Timer y Set Extending[22]

[22] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

2.1.5 Capa Física

2.1.5.1 Capa Física para 10 Mbps

2.1.5.1.1 Subcapa PLS (Physical Signaling)

El servicio que provee la subcapa PLS le permite a la subcapa MAC el poder intercambiar bits de datos o PLS data_units, con sus similares en otras estaciones.

Las primitivas asociadas entre las dos subcapas, tanto la MAC como la PLC pueden ser definidas en dos categorías:

- ✓ Primitivas que soportan interacciones MAC punto-punto.
- ✓ Primitivas que poseen significancia local y soporte a las interacciones entre las subcapas.

A su vez estos dos grupos se pueden subdividir de la siguiente manera:

- ✓ Punto-punto
  PLS_DATA.request
  PLS_DATA.indication
- ✓ Entre Subcapas
  PLS_CARRIER.indication
  PLS_SIGNAL.indication
  PLS_DATA_VALID.indication

Las primitivas PLS_DATA soportan la transferencia de datos entre la subcapa MAC y el resto de sus pares dentro de la misma LAN y definidas en el medio de broadcast.
Cabe destacar que el modo half duplex todos los bits transmitidos desde la subcapa MAC serán recibidos en respuesta por la misma unidad.

Las primitivas PLS_CARRIER, PLS_DATA_VALID, y PLS_SIGNAL proveen la información necesaria para que la subcapa MAC pueda realizar las funciones de acceso al medio.

2.1.5.1.2 Interfase AUI (Attachment Unit Interface)

Este parte del documento podremos revisar las funciones que desempeña la interfase AUI, que es usada también para poder conectar tanto a los equipos terminales de datos DTE (Data Terminal Equipment) con un MAU (Media Attachment Unit) que no forma parte del DTE. Esta interfase se usa para poder proveer al DTE de un medio físico ya se coaxial, par transado o fibra manteniendo idéntico el PLS, MAC para cualquiera de estos medios; también le permite separar el DTE del MAU con un cable hasta 50m.

El AUI puede operar en dos modos diferentes, el modo normal y monitoreo; todas las interfases deben soportar el modo normal, mientras que el modo monitoreo es opcional.
Cuando la interfase opera en el modo normal, el AUI esta lógicamente conectado con el MDI (Media Dependent Interface) que es en si el tipo de conector que maneja cada implementación Ethernet. El DTE debe seguir los algoritmos de acceso al medio, los cuales le proveen acceso compatible con el medio de la LAN, para poder enviar los datos por el AUI. El MAU siempre enviara de regreso al DTE todo dato que este reciba por el MDI.

Cuando la interfase ente en el modo monitoreo, el transmisor del MAU esta lógicamente aislado del medio, ya en este modo se convierte en un observador del medio; las funciones de entrada y las de error en la calidad de la señal funcionan sin problema.
Tanto el PLS como el AUI son capaces de soportar tanto al DTE como al MAU en modos de operación half y full duplex; sin embargo el modo full duplex del MAU no soporta el modo monitoreo.

2.1.5.1.2.1 Estructura de la Trama

La trama que es transmitida por la interfase AUI debe tener la siguiente estructura:

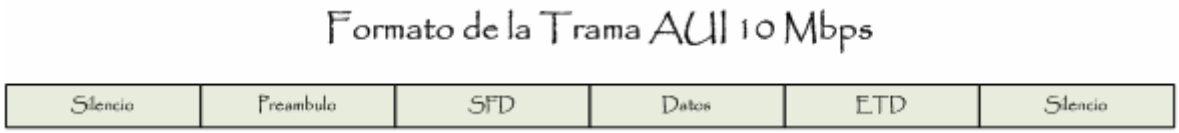


Figura 2.11. Formato de la Trama AUI 10Mbps

2.1.5.1.2.2 Codificación de los Datos

La codificación Manchester es usada para la transmisión de los datos a través de la interfase AUI; la codificación Manchester es un mecanismo de señalización binaria que combina los datos y el reloj en una mezcla de símbolos y bits. Cada símbolo-bit esta dividido en dos niveles, el segundo nivel tiene el nivel inverso del primer nivel, y la transición entre niveles se produce en la mitad de cada símbolo-bit.

A nivel de voltajes se debe considerar las siguientes especificaciones:

- ✓ "Vmax debe ser <1315 mV, Vmin debe ser >450 mV, y Vmax/Vmin debe ser <1.37"[23].
- ✓ "Vdm debe permanecer <1170 mV y 24 ns después de un cruce por cero."[24]

2.1.5.1.3 10BASE-T MAU (Media Attachment Unit)

El MAU tiene las siguientes características:

- ✓ Permite la comunicación entre la subcapa Physical Signaling (PLS) por medio de la interfase Attachment Unit Interface (AUI) hasta el enlace banda base de par trenzado.
- ✓ Soporta tráficos de mensaje a una tase de datos de 10 Mbps.
- ✓ Permite la operación sobre par trenzado desde distancias de 0 a 100 m. sin necesidad de repetidores.
- ✓ Permite que el DTE o un repetidor puedan confirmar la operación del MAU y la disponibilidad del medio.
- ✓ Soporta configuraciones de red usando CSMA/CD como método de acceso con señalización banda base.
- ✓ Permite conexiones entre dos MAU del tipo punto-punto, en una topología de estrella.
- ✓ Permite la incorporación de los MAU dentro de los límites físicos del DTE o repetidor.
- ✓ Permite tener los medios de operación half duplex, full duplex, o ambos.

[23] http://standard.ieee.org/getieee802/download/802.3-2002.pdf
[24] IBID 23

El 10BASE-T MAU es capaz de operar en modo normal únicamente. Cuando el modo normal esta en funcionamiento, las funciones de este son las de servir de conexión directa entre el DTE o un repetidor y el medio.

Los datos desde el DTE o un repetidor son puestos en una de los segmentos de comunicación simplex; y, los datos recibidos en el otro segmento de comunicación simplex son puestos en el DTE o repetidor.

2.1.5.1.3.1 Conectores MDI

Los conectores que usan para enlace entre el segmento de par trenzado debe ser de 8 terminales, conocidos como RJ45. Estos conectores deben ser usados tanto en los paneles del MAU como en el cable de par trenzado.

La siguiente tabla nos mostrara la asignación de cada terminal de los conectores con la señal que se transmitirá por ellos.

TERMINAL	*SEÑAL MDI*
1	TD+
2	TD–
3	RD+
4	No usado en 10BASE-T
5	No usado en 10BASE-T
6	RD–
7	No usado en 10BASE-T
8	No usado en 10BASE-T

Tabla 2.1. Asignación de Señal y Terminal MDI 10 Mbps

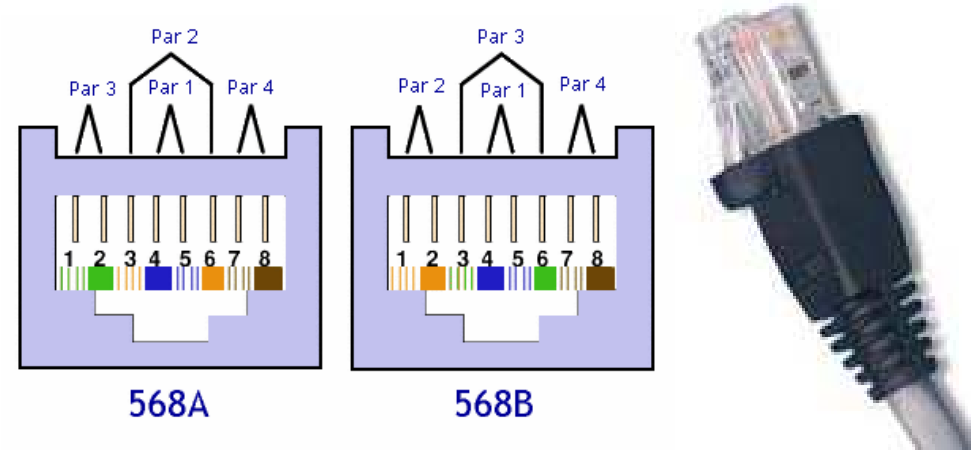


Figura 2.12. Conectores MDI

2.1.5.1.3.2 Parámetros de Transmisión

Para poder encajar con los parámetros definidos en la transmisión de datos usando 10BASE-T se debe usar un cable UTP o STP categoría 5 o superior 24AWG y tener las distancias tanto de cableado horizontal y vertical dentro de los 100 m sin repetidor.

2.1.5.1.4 10BASE-F MAU (Media Attachment Unit)

La MAU usada para 10Base-F posee las siguientes características:

- ✓ Provee los medios para conectar la subcapa PLS a través de la interfase AUI con un segmento de fibra óptica mediante el MDI de fibra.
- ✓ Soporta tráfico de mensajes a tasa de datos de 10 Mbps.
- ✓ Provee una conexión de hasta 1 km. de cable de fibra óptica en 10BASE-FP con una red estrella entre las dos MAUs. Provee una conexión de hasta 2 km. de cable de fibra óptica entre dos repetidores con 10BASE-FB MAUs. Provee una conexión de hasta 2 km. de cable de fibra óptica entre dos 10BASE-FL MAUs. Provee compatibilidad entre FOIRL MAUs y 10BASE-FL MAUs de hasta 1 km. de cable de fibra óptica.
- ✓ Le permite al DTE la posibilidad de verificar el MAU y la disponibilidad del medio.
- ✓ Soporta la configuración del sistema usando CSMA/CD como mecanismo de acceso al medio.

- ✓ Provee de un censado de portadora ininterrumpida durante una colisión.
- ✓ Soporta topologías de estrellas cableadas.
- ✓ Permite la incorporación del MAU dentro de los límites físicos del DTE o un repetidor.

2.1.5.1.4.1 Especificaciones MDI

Dado que el medio es fibra óptica, las propiedades que debe tener se muestran en la siguiente tabla:

Parameter	Units	10BASE-FP	10BASE-FB	10BASE-FL
TRANSMIT OPTICAL PARAMETERS				
Center wavelength				
—min.	nm	800	800	800
—max.	nm	910	910	910
Spectral width (FWHM)	nm	<75	<75	<75
Optical modulation extinction ratio	dB	≤13	≤13	≤13
Optical idle signal amplitude	dBm	≤57	see 15.2.1.10	see 15.2.1.10
Optical transmit pulse rise and fall times				
—max. (data)	ns	10	10	10
—min. (data)	ns	2	0	0
—max. difference (data)	ns	3	3	3
—max. (idle)	ns	N/A	10	25
—min. (idle)	ns	N/A	0	0
—max. difference (idle)	ns	N/A	3	25
Optical transmit pulse				
—overshoot	%	5	25	25
—undershoot	%	5	10	10
Optical transmit pulse edge jitter				
—added, DO circuit to MDI	ns	N/A	N/A	±2
—total at MDI (data)	ns	±1	±2	±4
—total at MDI (idle)	ns	N/A	±2	N/A
Optical transmit pulse				
Duty cycle distortion				
—data	ns	±1	±2.5	±2.5
—idle	ns	N/A	±2.5	±50.0
Optical transmit average power range				
—min.	dBm	–15	–20	–20
—max.	dBm	–11	–12	–12

Tabla 2.2. Parámetros de Fibra Óptica para 10 Mbps[25]

[25] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

RECEIVE OPTICAL PARAMETERS				
Optical receive average power range —min. —max.	 dBm dBm	 –41 –27	 –32.5 –12.0	 –32.5 –12.0
MAU optical receive edge jitter (data) —received at MDI —added, MDI to DI circuit —total at DI circuit (MAU end of AUI)	 ns ns ns	 ±4.5 N/A N/A	 ±2.0 N/A ±6.5	 ±6.5 ±8.5 ±15.0
Optical receive pulse rise and fall times —max. (data) —min. (data) —max. difference (data) —max. (idle) —min. (idle) —max. difference (idle)	 ns ns ns ns ns ns	 18.5 2.0 3.0 N/A N/A N/A	 31.5 0.0 3.0 31.5 0.0 3.0	 31.5 0.0 3.0 41.0 0.0 25.0

Tabla 2.3. Parámetros para Fibra Óptica a 10 Mbps[26]

2.1.5.2 Capa Física para 100 Mbps

2.1.5.2.1 Subcapa RS (Reconciliation Sublayer) e Interfase MII (Media Independent Interfase)

El propósito de esta interfase es la de conectar de manera simple, económica y fácil las subcapas MAC y física a 10 y 100 Mbps; y ente las estaciones de gestión y las entidades físicas a una tasa de transferencia de datos de 10 Mbps o superior.

Esta interfase tiene las siguientes características:

- ✓ Es capas de soportar tasas de transferencia de datos de 10 y 100 Mbps; así como funciones de gestión para capas físicas soportando tasas de datos de 10Mbps o mayores.
- ✓ Los datos y delimitadores estas sincronizados a referencias sincronizadas.
- ✓ Provee caminos de datos de transmisión y recepción de cuatro bits independientes.
- ✓ Usa niveles de señales TTL, compatibles con procesadores digitales CMOS ASIC.
- ✓ Provee una interfase de gestión simple.
- ✓ Es capaz de manejar distancias limitadas de cable blindado.
- ✓ Soporta operaciones full duplex.

[26] IBID 25

El MII puede soportar dos tasas específicas de datos, la de 10 Mbps y la 100 Mbps; las funciones son idénticas en las dos así como la relación entre los tiempos de señalización; la única diferencia entre las dos es la frecuencia del reloj.

2.1.5.2.1.1 Estructura de la Trama MII

Las tramas de datos transmitidas a través de la interfase MII deben tener el siguiente formato.

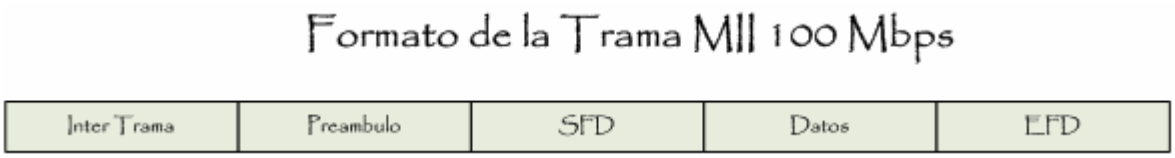


Figura 2.13. Formato de la Trama MII 100Mbps

2.1.5.2.2 Subcapa PCS (Physical Coding Sublayer) y PMA (Physical Medium Attachment)

2.1.5.2.2.1 Subcapa PCS

La interfase PCS es la interfase independiente del medio que provee una interfase entre la subcapa de reconciliación con implementaciones 100BASE-T físicas. Esta subcapa cumple con funciones similares la interfase AUI dando servicios a la MII.

Además de cumplir con todos los servicios de la MII nos ofrece lo siguiente:

- ✓ Codificación y decodificación de los datos MII a grupos de código de cinco bits (4B/5B).
- ✓ Genera indicadores de detección de colisión y censado de portadora.
- ✓ Provee de la serialización de los grupos de código para su transmisión a partir de la existente PMA serial y viceversa.
- ✓ Realiza un mapeo de la transmisión, recepción, censado de portadora y detección de colisión entre la MII y la subcapa PMA.

2.1.5.2.2.2 Subcapa PMA

La subcapa PMA provee un medio independiente mediante el cual la subcapa PCS pueda acceder a varios medios físicos, esta capa se encarga de dar ciertas funciones:

- ✓ Mapea la transmisión y recepción de los bits codificados entre la PMA y PMD.
- ✓ Genera una señal de control indicando la disponibilidad de la subcapa PMD a la PCS, así como sincronización con auto negociación cuando se implementa.
- ✓ En forma opcional, puede generar indicativos de actividad y error en la portadora desde la subcapa PMD.
- ✓ De la misma manera, censa fallas en el canal de recepción y transmite el indicativo Far-End Fault; así como la detección del mismo.
- ✓ Recupera el reloj desde los datos NRZI provistos por el PMD.

2.1.5.2.3 100Base-TX PDM (Physical Medium Dependent)

En esta parte del documento nos centraremos en la revisión de la interfase PDM e incluiremos la MDI para transmisiones banda base sobre par trenzado, este estándar le permite la interacción con un cableado UTP o STP categoría 5 o superior.

2.1.5.2.3.1 Asignación de Contactos para Cables de Par Trenzado

100BASE-TX adopta la misma asignación de de contactos que 10BASE-T, en la siguiente tabla se podrán observar los contactos tanto en el modo normal como cruzado.

CONTACTO	*SEÑAL MDI SIN CRUCE*	*SEÑAL MDI CON CRUCE*
1	Transmit +	Receive +
2	Transmit –	Receive –
3	Receive +	Transmit +
4		
5		
6	Receive –	Transmit –
7		
8		

Tabla 2.4. Asignación de Señal y Terminal MDI 100 Mbps

2.1.5.2.3.2 Características del Sistema de Cableado

El sistema de cableado usado para que soporte 100BASE-TX con canales duplex requiere dos pares de cable categoría 5 balanceado con una impedancia nominal de 100 Ω.

Los componentes del sistema de cableado, es decir cable, pathcords y conectores usados en la implementación deben ser categoría 5, especificados en la norma ANSI/TIA/EIA-568-A.

2.1.5.2.4 100Base-FX PDM

En esta parte del presente documento revisaremos las especificaciones PMD para 100BASE-FX. Las especificaciones para el medio de transmisión son parecidas a 10BASE-F.

2.1.5.2.4.1 Interfase MDI (Medium Dependent Interface)

La interfase dependiente del medio para 100BASE-FX debe tener uno de los siguientes conectores:

- ✓ Conector de interfase de fibra óptica de bajo costo, comúnmente llamado conector duplex SC.
- ✓ Conector de interfase del medio (MIC); cuando este es usado el receptáculo debe ser marcado como “M”.
- ✓ Conector de medio óptico Plug and Socket, comúnmente llamado ST.

La alternativa recomendada es el conector SC.

2.1.5.3 Capa Física para 1000 Mbps

Gigabit Ethernet es una versión extendida de la 802.3 para las familias de capas físicas de 1000 Mbps. Gigabit Ethernet usa la misma interfase de la capa MAC de 802.3, esta vez conectada la capa de interfase independiente del medio Gigabit a través de subcapas como: 1000BASE-LX, 1000BASE-SX, 1000BASE-CX, y 1000BASE-T.

Gigabit Ethernet logra extender la capa MAC de 100 Mbps a 1000 Mbps. La tasa de bit es más rápida y los tiempo de bit más cortos, ambos en proporción al cambio de ancho de banda. En el modo full duplex, tiempo de transmisión de un paquete a sido reducido por un factor de diez; las topologías de 1000 Mbps en su modo de operación full duplex es comparable a las encontradas en 100BASE-T full duplex; en modo half duplex, el tiempo mínimo de transmisión de paquetes ha sido reducido, pero no en un factor de diez. Los promedios de retrasos en los cables son similares a aquellos en 100BASE-T.

2.1.5.3.1 Subcapa RS (Reconciliation Sublayer) e Interfase GMII (Gigabit Media Independent Interfase)

El propósito de esta interfase es la de proveer una conexión simple, barata y fácil entre la subcapas MAC y físicas, y entre las subcapas físicas y las estaciones de gestión.

La interfase GMII posee las siguientes características:

- ✓ Es capaz de soportar operaciones a 1000 Mbps.
- ✓ Los datos y las delimitaciones están sincronizadas mediante las referencias del reloj.
- ✓ Provee de caminos de datos tanto de transmisión y recepción independientes de 8 bits.
- ✓ Provee una interfase de gestión simple.
- ✓ Utiliza niveles de señal compatibles con los procesadores ASIC CMOS y algunos procesadores bipolares
- ✓ Es capaz de operar en modos full duplex.

La implementación de las interfases a sido realizada de la forma chip-to-chip (circuito integrado a circuito integrado) con pistas en circuito impreso. La implementación de tarjeta madre a tarjeta adicional entre dos o más circuitos impresos no se ha implementado.

Esta interfase es usada para proveer independencia del medio de tal manera que un controlador de acceso al medio idéntico pueda ser usado con cualquier tipo de interfase física ya sea cobre o fibra.

2.1.5.3.1.1 Tasa de Operación

El GMII soporta operaciones solo a 1000 Mbps; las operaciones a 10 y 100 Mbps son soportadas por la MII.

Las capas físicas que proveen a GMII deben soportar 1000 Mbps, y pueden soportar tasas de transferencia adicionales usando otra interfase como MII. Las capas físicas deben reportar las tasas de operación a las cuales son capaces de funcionar mediante la interfase de gestión. Las subcapas de Reconciliación que le proveen a GMII deben soportar 1000

Mbps y pueden soportar al igual que las capas físicas tasas de operación adicionales usando otras interfases.

2.1.5.3.1.2 Trama de datos de GMII

La trama de datos transmitida a través de la interfase GMII debe ser transferida según las especificaciones mostradas a continuación.

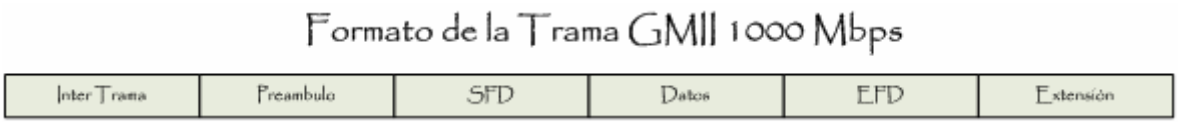


Figura 2.14. Formato de la Trama GMII 1000 Mbps

2.1.5.3.2 Subcapa PCS (Physical Coding Sublayer) y PMA (Physical Medium Attachment) para Familias 1000BASE-X

En esta parte del presente documento podremos conocer tanto la subcapa PCS y PMA que son comunes tanto para las familias con implementaciones de capa física de 1000 Mbps, mejor conocidas como 1000BASE-CX, 1000BASE-LX, y 1000BASE-SX.

1000BASE-CX especifica operaciones sobre medios de cobre, dos pares de cobre de cableado balanceado a 150 Ω; 1000BASE-LX especifica operaciones sobre fibra, un par de fibra usando transmisiones ópticas de longitudes de onda larga; 1000BASE-SX especifica operaciones también sobre fibra, usando un par de fibra óptica con transmisión de longitudes de onda corta.

Esta capa se basa en el uso de codificaciones 8B/10B para canales de fibra, una subcapa PMA compatible con versiones de velocidades mejoradas de chips seriales de 10 bits de la ANSI, y especificaciones ópticas y eléctricas similares.

Los objetivos de la familia 1000BASE-X son los mostrados a continuación:

- ✓ Soportar CSMA/CD.
- ✓ Ser compatible con repetidores 1000 Mbps.
- ✓ Ser capaz de ofrecer Auto-Negociación entre las PMDs a 1000 Mbps.
- ✓ Proveer una tasa de datos de 1000 Mbps a la interfase GMII.

- ✓ Soportar cableados balanceados de cobre de 150 Ω o fibra óptica capaz de cumplir las especificaciones ISO/IEC 11801.
- ✓ Permitir a una red la posibilidad de extenderse hasta 3 km., incluyendo: enlaces de 25 m a 150 Ω balanceado de extremo; redes de un repetidor de 50 de extremo (usando todo cableado de cobre balaceado de 150 Ω); redes de un repetidor de 200 m de extremo (usando fibra); y, enlaces DTE/DTE de 3000 m (usando fibra).
- ✓ Preservar el comportamiento full duplex en los canales PMD.
- ✓ Soportar un BER de 10–12.

2.1.5.3.2.1 Subcapa PCS (Physical Coding Sublayer)

La interfase PCS es la interfase del medio independiente gigabit GMII que provee una interfase uniforme a la subcapa de reconciliación para todas las implementaciones físicas a 1000 Mbps.

La subcapa PCS de 1000BASE-X provee todos los servicios requeridos por GMII, incluyendo:

- ✓ Codificación de los octetos de datos GMII a grupos de código de 10 bits (8B/10B) para comunicación y viceversa con la PMA.
- ✓ Genera indicativos de censado de portadora y detección de colisión para uso en los clientes half duplex.
- ✓ Gestiona procesos de auto negociación e informa a la entidad de gestión mediante el GMII cuando el medio físico esta listo para usarse.

2.1.5.3.2.2 Subcapa PMA (Physical Medium Attachment)

La subcapa PMA provee un medio independiente para el PCS, permitiéndole soportar el uso de un rango de bits seriales orientados al medio. La subcapa PMA para 1000BASE-X realiza las siguientes funciones:

- ✓ Mapeo de la recepción y transmisión de los grupos de código entre el PCS y PMA mediante la interfase de servicio PMA.
- ✓ Realiza la serialización de los grupos de código para la transmisión de la capa inferior PMD, y viceversa.
- ✓ Recupera el reloj desde los datos codificados 8B/10B suministrados por el PMD.

- ✓ Mapea la transmisión y recepción de bits mediante el PMA y PMD mediante la interfase de servicio PMD.
- ✓ Realiza un laso de los datos en la interfase de servicio PMD.

2.1.5.3.2.3 Subcapa PMD (Physical Medium Dependent)

La señalización para la capa física de la familia 1000BASE-X para medios de fibra y cobre es adaptada de la ANSI X3.230 (FCPH), en esta se definen sistemas de señalización a 1062.5 Mbps, sistemas de señalización full duplex para fibra óptica monomodo, multimodo y cableado de cobre balanceado de 150 Ω.

2.1.5.3.2.4 Código de transmisión 8B/10B

La subcapa PCS usa códigos de transmisión para mejorar las características de transmisión de la información a ser transferida a través del enlace; la codificación es definida por el código de transmisión, asegurando que existen las suficientes transiciones presentes en la serie de bits físicos para poder recuperar el reloj en el receptor. Dichas codificaciones también incrementan en gran manera la facilidad de detectar cualquier error de un bit o varios bits que pueden ocurrir mediante la transmisión y recepción de la información.

Adicionalmente, algunos de los grupos de códigos contienen un bit distintivo que ayuda al receptor al momento de lograr la alineación del código de grupo en una ráfaga de bits entrante. El código de transmisión 8B/10B especificado en este estándar posee una gran densidad de transición, es un código de recorrido de longitud limitada, y balanceado en DC; la densidad de transición de los símbolos de 8B/10B varían desde 3 a 8 transiciones por símbolo.

2.1.5.3.3 1000BASE- LX/SX PMD (Physical Medium Dependent)

En esta parte del documento mi estimado lector encontrara las especificaciones para la 1000BASE-SX PMD y 1000BASE-LX PMD (incluyendo la MDI), y el medio de transmisión banda base para fibra multimodo monomodo.

2.1.5.3.3.1 Subcapas PMD y MDI para 1000BASE-SX

Dentro de las especificaciones de la subcapa PMD y la interfase MDI se encuentran los rangos de operación de la fibra óptica, estas se mostrarán en la siguiente tabla:

Fiber type	Modal bandwidth @ 850 nm (min. overfilled launch) (MHz · km)	Minimum range (meters)
62.5 μm MMF	160	2 to 220
62.5 μm MMF	200	2 to 275
50 μm MMF	400	2 to 500
50 μm MMF	500	2 to 550
10 μm SMF	N/A	Not supported

Tabla 2.5. Rango de Operación para 1000BASE-SX[27]

Description	62.5 μm MMF	50 μm MMF	Unit
Transmitter type	Shortwave Laser		
Signaling speed (range)	1.25 ± 100 ppm		GBd
Wavelength (λ, range)	770 to 860		nm
T_{rise}/T_{fall} (max; 20%-80%; λ > 830 nm)	0.26		ns
T_{rise}/T_{fall} (max; 20%-80%; λ ≤ 830 nm)	0.21		ns
RMS spectral width (max)	0.85		nm
Average launch power (max)	See footnote [a]		dBm
Average launch power (min)	–9.5		dBm
Average launch power of OFF transmitter (max)[b]	–30		dBm
Extinction ratio (min)	9		dB
RIN (max)	–117		dB/Hz
Coupled Power Ratio (CPR) (min)[c]	9 < CPR		dB

Tabla 2.6. Características de Transmisión para 1000BASE-SX[28]

[27] http://standard.ieee.org/getieee802/download/802.3-2002.pdf
[28] IBID 27

Description	62.5 μm MMF	50 μm MMF	Unit
Signaling Speed (range)	1.25 ± 100 ppm		GBd
Wavelength (range)	770 to 860		nm
Average receive power (max)	0		dBm
Receive sensitivity	–17		dBm
Return loss (min)	12		dB
Stressed receive sensitivity[a, b]	–12.5	–13.5	dBm
Vertical eye-closure penalty[c]	2.60	2.20	dB
Receive electrical 3 dB upper cutoff frequency (max)	1500		MHz

Tabla 2.7. Características de Recepción para 1000BASE-SX[29]

2.1.5.3.3.2 Subcapas PMD y MDI para 1000BASE-LX

Al igual que para 1000BASE-LX se podrán apreciar las especificaciones del medio físico en las tablas presentadas a continuación:

Fiber type	Modal bandwidth @ 1300 nm (min. overfilled launch) (MHz · km)	Minimum range (meters)
62.5 μm MMF	500	2 to 550
50 μm MMF	400	2 to 550
50 μm MMF	500	2 to 550
10 μm SMF	N/A	2 to 5000

Tabla 2.8. Rango de Operación para 1000BASE-LX[30]

[29] IBID 27
[30] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

Description	62.5 μm MMF	50 μm MMF	10 μm SMF	Unit
Transmitter type	Longwave Laser			
Signaling speed (range)	1.25 ± 100 ppm			GBd
Wavelength (range)	1270 to 1355			nm
T_{rise}/T_{fall} (max, 20-80% response time)	0.26			ns
RMS spectral width (max)	4			nm
Average launch power (max)	–3			dBm
Average launch power (min)	–11.5	–11.5	–11.0	dBm
Average launch power of OFF transmitter (max)	–30			dBm
Extinction ratio (min)	9			dB
RIN (max)	–120			dB/Hz
Coupled Power Ratio (CPR)[a]	28 < CPR< 40	12 < CPR < 20	N/A	dB

Tabla 2.9. Características de Transmisión para 1000BASE-LX[31]

Description	Value	Unit
Signaling speed (range)	1.25 ± 100 ppm	GBd
Wavelength (range)	1270 to 1355	nm
Average receive power (max)	–3	dBm
Receive sensitivity	–19	dBm
Return loss (min)	12	dB
Stressed receive sensitivity[a, b]	–14.4	dBm
Vertical eye-closure penalty[c]	2.60	dB
Receive electrical 3 dB upper cutoff frequency (max)	1500	MHz

Tabla 2.10. Características de Recepción para 1000BASE-LX[32]

2.1.5.3.3.3 Interfase MDI (Medium Dependent Interface)

La capa PMD para 1000BASE-SX y 1000BASE-LX se une al cable de fibra óptica mediante el receptáculo óptico en el MDI. Los receptores ópticos 1000BASE-SX y 1000BASE-LX deben ser SC duplex, y deben cumplir con los siguientes requerimientos:

[31] IBID 30
[32] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

- ✓ Cumplir con las dimensiones y especificaciones de interfase de la IEC 61754-4 [B25] y IEC 61754-4.
- ✓ Deberán cumplir con las especificaciones de la ISO/IEC 11801.
- ✓ Garantizar que la polaridad se mantenga.
- ✓ El lado del receptor del receptáculo de estar localizado a la derecha cuando es visto el puerto óptico del transmisor con los seguros en la superficie de arriba.

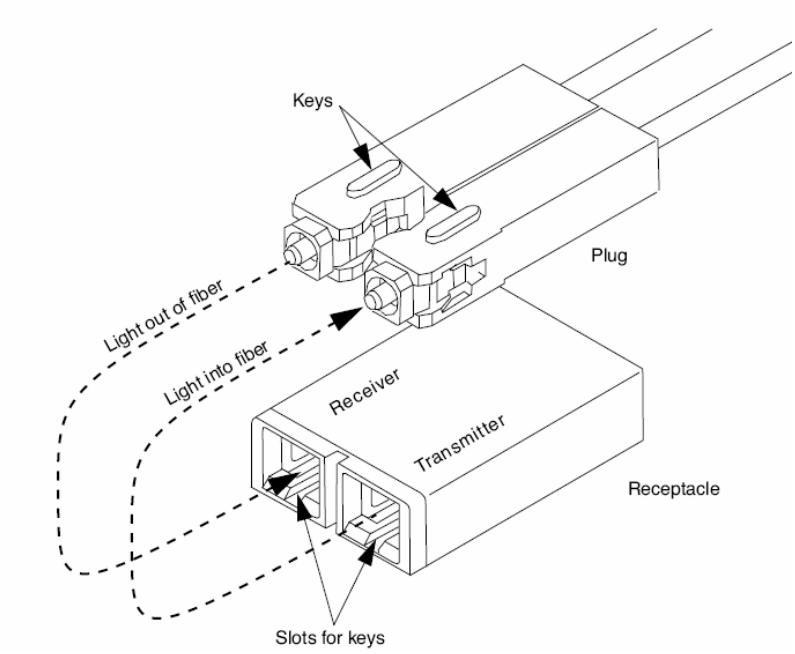


Figura 2.15. Conector MDI de Fibra Óptica[33]

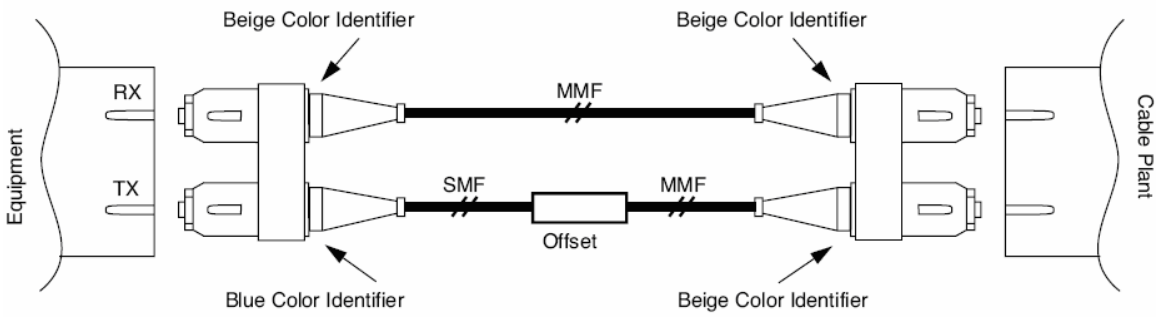


Figura 2.16. Colocación del Patchcord para Fibra Monomodo[34]

[33] http://standard.ieee.org/getieee802/download/802.3-2002.pdf
[34] IBID 33

2.1.5.3.4 Subcapas PCS y PMA para 1000BASE-T

La capa física de 1000BASE-T PHY es una de las familias de Gigabit Ethernet de redes de alta velocidad CSMA/CD. La subcapa PCS, PMA y las especificaciones del medio para transmisiones banda base de 1000BASE-T han sido puesta para aquellos que deseen un desempeño de 1000 Mbps sobre sistemas de cableado categoría 5 de par trenzado. La señalización de 1000BASE-T requiere de 4 pares de cable categoría 5, tal como especifica la norma ISO/IEC 11801:1995, ANSI/EIA/TIA-568-A (1995) y ANSI/TIA/EIA TSB95.

Los objetivos de 1000BASE-T son los que se encuentran especificados a continuación:

- ✓ Soporta CSMA/CD.
- ✓ Cumple con las especificaciones necesarias para la interfase GMII.
- ✓ Es capaz de soportar repetidores a 1000Mbps.
- ✓ Provee de líneas de transmisión que soportan operaciones full y half duplex.
- ✓ Iguala o mejora la operación descrita en la FCC Class A/CISPR.
- ✓ Soporta operaciones sobre 100 m. en cableado categoría 5 balanceado.
- ✓ Posee una tasa de error de bits (BER) menor o igual a 10-10
- ✓ Soporta auto negociación.

2.1.5.3.4.1 Modo de Operación de 1000BASE-T

La capa física de 1000BASE-T emplea transmisión banda base full duplex a través de 4 pares de cableado categoría 5. La tasa de datos de 1000 Mbps se alcanza gracias a la suma de las transmisiones de datos a tasas de 250 Mbps sobre cada par; el uso de híbridos y canceladores habilita la transmisión full duplex, permitiendo que los símbolos sean transmitidos y recibidos en el mismo par al mismo tiempo.

Señalización banda base con una tasa de modulación de 125 Mbaud es usada en cada par; los símbolos transmitidos son seleccionados de una constelación de símbolos de 5 niveles cuadridimensional; cada símbolo cuadridimensional puede ser visto como un grupo de cuatro (An, Bn, Cn, Dn), de un grupo de cinco símbolos de una dimensión, tomados del grupo {2, 1, 0, –1, –2}.

1000BASE-T usa un sistema de señalización continuo; en la ausencia de datos se transmiten símbolos definidos. Estos símbolos pertenecen a un grupo de código en el cual cada símbolo esta restringido al grupo {2, 0, –2} para mejorar la sincronización.
La modulación de amplitud de pulso PAM de cinco niveles (PAM5) es usada en cada par.
La tasa de modulación de 125 MBaud encaja con la tasa del reloj de la interfase GMII de 125 MHz y da como resultado un periodo de símbolo de 8 ns.

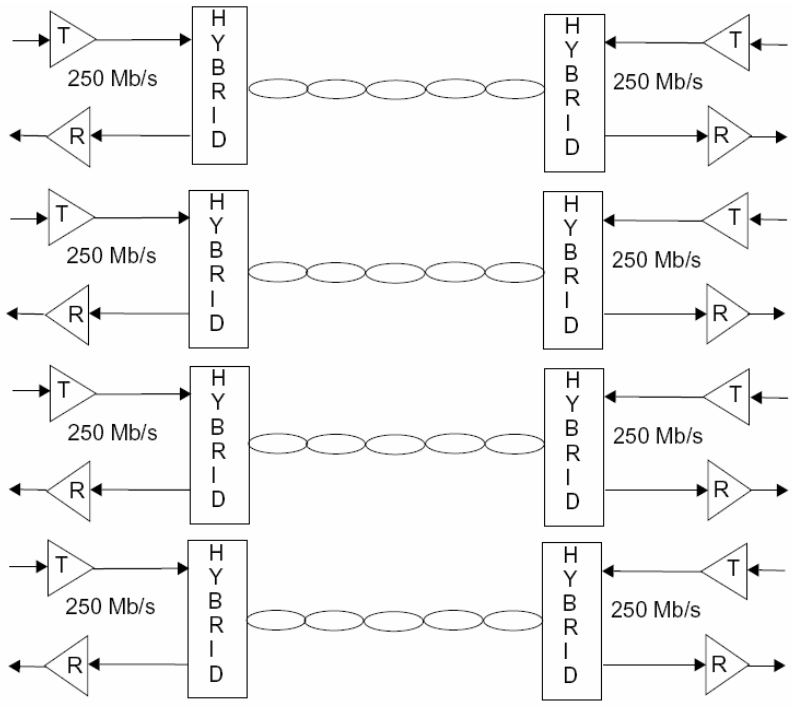


Figura 2.17. Topología 1000BASE-T[35]

2.1.5.3.4.2 Subcapa PCS (Physical Coding Sublayer)

Las funciones realizadas por la subcapa PCS comprende la generación de grupos de códigos continuos para su transmisión sobre cuatro canales y el procesamiento de de los grupos de código recibidos en la capa física remota.

El proceso de convertir bits de datos en grupos de códigos es llamado 4D-PAM5, el cual hace referencia a la técnica de codificación de modulación de amplitud de pulso de cinco niveles de cuatro dimensiones que se usa. Mediante este esquema de codificación, 8 bits son convertidos a una transmisión de cuatro símbolos de cinco números.

[35] http://standard.ieee.org/getieee802/download/802.3-2002.pdf

Entre tramas, una subrutina de grupos de código que usan solo los símbolos {2, 0, –2} se transmiten; a esto se le llama modo idle. La codificación del modo idle toma en cuenta la información de si la capa física esta operando de forma confiable o no y permite que esta información sea transportada a la estación remota. Durante operación normal, el modo idle es seguido por un modo de datos con un delimitador de inicio de trama.

El PCS recibe grupos de código procesados del PMA; el receptor PCS detecta el inicio y fin de las tramas de datos; y, durante la recepción de datos, decodifica grupos de código recibidos en octetos RXD<7:0> que son entregados al GMII. La conversión de grupos de códigos a octetos usa la técnica de decodificación de datos 8B1Q4. La subcapa PCS recibe también detecta errores en las secuencia recibidas y las marca para el GMII.

La subcapa PCS tiene una función de censado de portadora, una función de presencia de colisión y una interfase de gestión.

2.1.5.3.4.3 Subcapa PMA (Physical Medium Attachment)

La subcapa PMA enlaza los mensajes de esta subcapa al medio físico, además provee la gestión del canal y funciones de control; esta subcapa provee comunicaciones full duplex a 125 MBaud a través de cuatro pares de cableado balanceado hasta 100m de longitud.

El control de la capa física comienza siguiendo el proceso de auto negociación y provee las funciones de inicio necesarias para las operaciones 1000BASE-T; determina si la capa física opera en estado normal, habilitando la transmisión de datos sobre el enlace, o si la capa física envía grupos de código especiales, es decir opera en modo idle.

2.1.5.3.4.4 Señalización

La señalización 1000BASE-T es realizada por la subcapa PCS generando secuencias de grupos de códigos que la subcapa PMA transmite sobre cada par. El esquema de señalización debe cumplir con los siguientes objetivos:

- ✓ Mapeo de código de símbolo FEC para datos.

- ✓ Mapeo algorítmico y mapeo inverso desde el octeto de datos a un cuarteto de símbolos de cinco y viceversa.
- ✓ Símbolos no correlacionados en la ráfaga de símbolos transmitidos.
- ✓ No correlación entre ráfagas de símbolos viajando en ambas direcciones en ninguna combinación de pares.
- ✓ No correlación entre ráfagas de símbolos en los pares BI_DA, BI_DB, BI_DC, y BI_DD.
- ✓ El modo Idle usa una subsecuencia de grupos de código, en donde cada símbolo esta restringido al grupo {2, 0, –2} para facilitar la sincronización, inicio y reentradas.
- ✓ La habilidad de determinar de forma rápida o instantánea si una ráfaga de símbolos representa datos, idle o extensión de portadora.
- ✓ Delimitadores robustos para delimitadores de inicio de ráfaga (SSD), delimitadores de fin de ráfaga (ESD), y demás señales de control.
- ✓ Debe poseer la habilidad de señalar los diferentes estados del receptor local a la terminal remota, para indicar que el receptor local no opera de forma confiable y necesita un reingreso.
- ✓ La habilidad de detectar y corregir intercambio de pares e inesperadas conexiones cruzadas.
- ✓ Habilidad de detector y corregir las polaridades incorrectas en los conectores.
- ✓ Debe poder corregir automáticamente las variaciones en los retrasos a través de los pares.

Esta capa física opera en dos modalidades, el modo normal y el modo de entrenamiento; en el primero el PCS genera grupos de código que representan datos, control o idle para ser transmitidos por el PMA; en el Segundo modo el PCS se configura para generar solo grupos de código idle para ser transmitidos de nuevo por el PMA, el cual habilita el receptor en el otro extremo para “entrenar” hasta que esta listo para regresar al modo normal.

2.1.5.3.4.5 Características del Sistema de Cableado

El sistema de cableado usado para soportar 1000BASE-T requiere de cableado balanceado categoría 5 de cuatro pares con una impedancia nominal de 100 Ω.

Los componentes del sistema de cableado, es decir cables, conectores y patchcord usados para proveer el segmento de enlace debe ser también categoría 5 y regirse a la norma ANSI/TIA/EIA-568-A e ISO/IEC 11801. Además de los siguientes requisitos:

- ✓ 1000BASE-T usa una topología estrella con un sistema de cableado categoría 5 para el enlace entre las entidades.
- ✓ 1000BASE-T es una aplicación clase D de la ISO/IEC.
- ✓ El ancho del espectro de la señal PMD transmitida es aproximadamente de 80 MHz.
- ✓ El uso de blindaje esta fuera de la literatura de este estándar.

2.1.5.3.4.6 Conectores MDI

Conectores de ocho terminales llamados RJ45 deben ser usados como el mecanismo de interfase del cable. Este tipo de conector debe ser usado en el cable como en las terminales.

Figura 2.18. Conector MDI para 1000Mbps

En la siguiente tabla se mostrara el contacto y la señal MDI correspondiente a este tanto para conexiones directas como cruzadas.

CONTACTO	*MDI*	*MDI-X*
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Tabla 2.11. Asignación de Señal y Terminal MDI 1000Mbps

2.2 xDSL

2.2.1 Historia

Para comenzar con esta breve reseña histórica primero revisaremos el significado de DSL (Digital Subscriber Line) que en español es Línea de Subscriptor Digital, este nombre tiene sentido si tomamos en cuenta que la tecnología que mencionamos se fundamenta en las redes de telefonía existentes.

La historia de la tecnología denominada xDSL empieza a finales de la década de los 80’s, más específicamente en el año de 1988 en los laboratorios Bell, comenzó como un trabajo de uno de sus ingenieros al tratar de enviar señales digitales sobre una línea telefónica utilizando en ancho de banda desperdiciado en dicho cable.

Como es de imaginarse el éxito de dicho proyecto no tuvo la acogida de las empresas de telefonía fija de la época, ya que para ese entonces les resultaba mucho más rentable que una persona adquiriera una segunda línea telefónica, y un modem para comunicarse con las nuevas redes de datos; por esta razón la comercialización de la tecnología xDSL se vería retardada por algunos años.

El propósito inicial de la tecnología DSL fue la de llevar el denominado video bajo demanda o VOD por sus siglas en inglés a las viviendas, y de esta manera permitir que las empresas de telefonía amparadas por recientes reformas de libre competencia, pudieran brindar servicio a la par de las empresas de televisión por cable.

Desafortunadamente los pronósticos del video bajo demanda no fueron acertados y la tecnología xDSL termino dando un giro algo inesperado; debido a que las empresas de

cable empezaron a ofrecer conexiones de banda ancha a sus clientes para conexiones en empresas y domicilios ansiosos por tener acceso al Internet, de esta manera la tecnología en un principio olvidada por las empresas de telefonía fija ahora empezaba a tomar fuerza para brindar conexiones a redes de alta velocidad.

Una vez que DSL entra al mercado en la década de los 90's se desarrollaron varios tipos de variaciones de esta tecnología, la primera en desarrollarse fue la denominada ADSL (Asymmetric Digital Subscriber Line) o Línea de Subscriptor Digital Asimétrica en la cual el ancho de banda de bajada es mayor al ancho de banda de subida, lo cual tiene sentido si consideramos que el propósito original de esta tecnología era la de llevar VOD a sus clientes, afortunadamente esta tecnología se adapta perfectamente al tráfico de Internet que presentan los usuarios residenciales, ya que es por lo general mayor la información que se descarga que la que se envía, por esta razón ADSL fue la primera variación de DSL que se desarrollo.

Con el tiempo aparecieron otras variaciones de DSL como RADSL, SDSL, HDSL, SHDSL, VDSL, cada una con ventajas y mejoras a lo largo de los años, es por esta gran diversidad que se denominó a esta tecnología con el nombre de xDSL.

2.2.2 Introducción

La tecnología xDSL (Digital Subscriber Line) es una nueva tecnología de módems, que permite usar el viejo tendido telefónico de par trenzado usado por las compañías de telefonía fija, para poder transmitir datos a altas velocidades o permitir acceso de banda ancha hacia el Internet o la conexión a redes de datos.

Como se puede notar xDSL en realidad hace referencia a los módems y no a las líneas de abonados, esto se debe a que para poder tener acceso a esta tecnología se instalan solo módems y no el tendido de cobre, debido a que se usa el tendido telefónico ya existente.

Antes de la llegada de DSL las compañías telefónicas empezaron a usar módems analógicos para poder transmitir datos, estos módems analógicos realizaban la conversión de los datos en pulsos de tonos los cuales eran transmitidos a través del cableado de cobre, la capacidad de estos primeros módems eran relativamente baja, ya que las velocidades de transmisión que alcanzaban eran de apenas unos miles bits por segundo; estos dispositivos

se ajustaban a la teoría de Shanon, la cual establece la capacidad del canal en base al ancho de banda y la señal a ruido en la transmisión.

$$C = Bw * \log_2(1 + \frac{S}{N})$$

Formula 2.2. Fórmula de la Capacidad del Canal de Shanon

Es decir que en base a esta formula, un fabricante promedio podía llegar a tener 24 o 30 dB de señal a ruido y con anchos de banda utilizables de 400 Hz. las velocidades bordeaban los 24 Kbps el los 90's.

Con el pasar de los años la modulación y las técnicas de corrección de errores se fueron mejorando y evolucionando hasta que se llegó a alcanzar velocidades de 56.6 Kbps, esta velocidad se convertiría en la barrera práctica a la hora de establecer las velocidades de conexión de los módems analógicos, esta barrera nace de las limitaciones del núcleo de la red telefónica y no de la línea de abonado, es decir que las velocidades no mejoraron por falta de capacidad en las cables de cobre, sino de las limitaciones en los dispositivos de conexión y transporte de datos.

De esta manera es que se empieza a buscar un método por el cual se pueda utilizar el ancho de banda desperdiciado en los pares tranzados de cobre, se empieza a desarrollar la tecnología xDSL, la cual para poder funcionar necesita tener elementos DSL en ambos extremos de la conexión, es decir uno en el abonado y otro en la oficina central, en otras palabras DSL es una tecnología de módems digitales, los cuales me permiten transmitir datos a altas velocidades, mejor conocidas como conexiones de banda ancha.

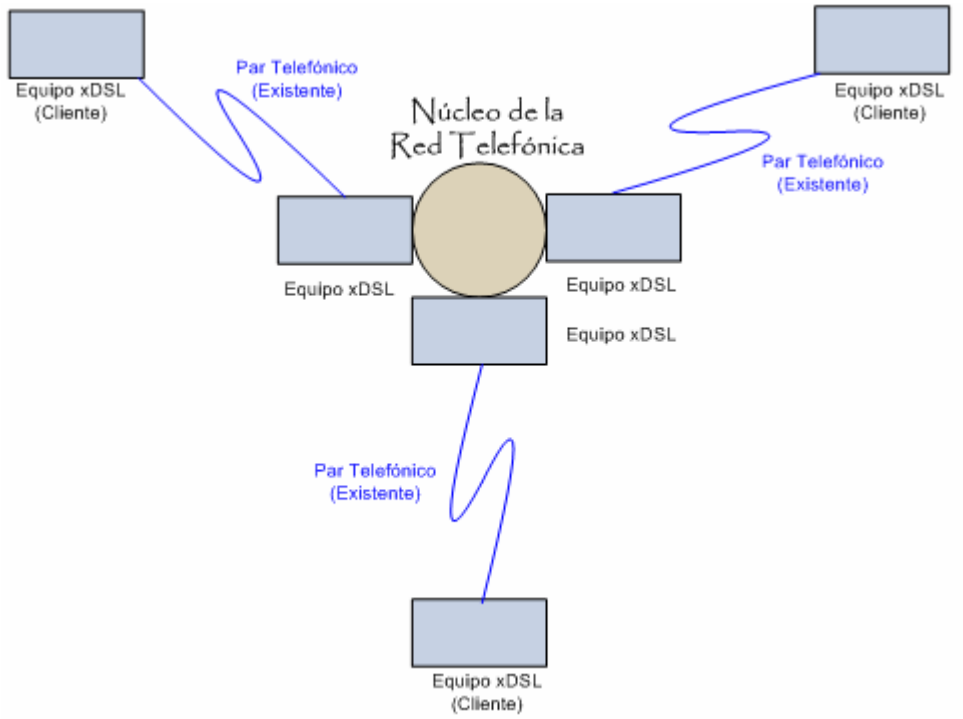


Figura 2.19. Esquema General de una Implementación xDSL

xDSL permite la transmisión full duplex a 128 Kbps a distancias de 6 Km. a través del cableado telefónico, permitiendo en forma simultanea el uso de los servicios de telefonía tradicionales como es la transmisión analógica de voz; estas características de desempeño varían según la técnica y la distancia que se empleen.

Como se mencionó anteriormente se debe tener equipos DSL en ambos extremos de la conexión para poder levantar el servicio, el uno es el CPE (Customer Premise Equipment) o equipo correspondiente al cliente y el CO (Central Office) u oficina central; el par tranzado de cobre se denomina “Local Loop” y dependiendo de la longitud del lazo se verán afectadas la calidad del servicio y las tasas transferencia.

La tecnología DSL sufrió varios cambios para poder adaptarse a los diferentes mercados que existen en la actualidad, las variaciones que se llevaron a cabo son principalmente las que afectan a las velocidades de transmisión, estos nuevos tipos de DSL se agruparon y tomaron el nombre de xDSL, de entre estos varios tipos de DSL’s el más difundido es ADSL, el cual se adapta al mercado residencial que busca conexiones de banda ancha al Internet; debido a esta característica será la rama de la tecnología xDSL que se procederá a estudiar con más detenimiento, cabe destacar que los parámetros revisados para ADSL se adaptan al resto de la tecnología xDSL, ya que mayormente las diferencias están en las velocidades de conexión que cada una me ofrece.

2.2.3 ADSL

2.2.3.1 Definición

ADSL tal como se citó previamente es la abreviación en inglés de Asymmetric Digital Subscriber Line o en español Línea de Subscritor Digital Asimétrica, esta es una rama de la familia tecnológica xDSL.

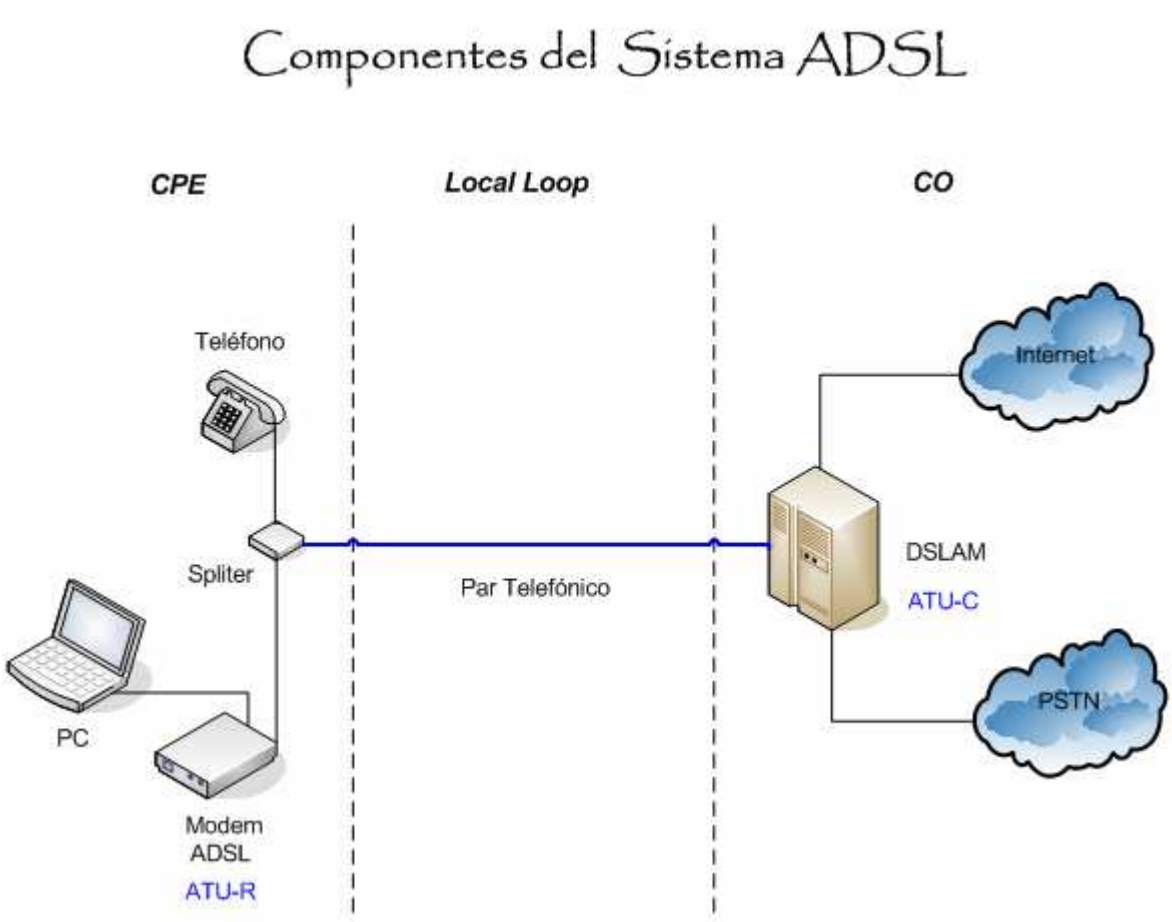


Figura 2.20. Componentes del Sistema ADSL

2.2.3.2 Capacidad de Transporte

Los sistemas ADSL pueden soportar hasta siete canales de transmisión de datos simultáneamente, cuatro canales independientes simplex para downstream (AS0, AS1, AS2, AS3) y tres canales duplex (LS0, LS1, LS2).

Todos los canales deben ser capaces de funcionar a tasas de transferencia de múltiplos de 32 Kbps, pero deben además permitir tasas de transferencia de 1.544 Mbps para poder interactuar con otras tasas de transferencia de diferentes sistemas.

Las tasas de transferencias máximas de un sistema ADSL dependen de las características del local loop en el cual se despliegue este sistema, estas velocidades se establecen durante los procesos de iniciación.

ADSL debe soportar el funcionamiento de dos tipos de transmisión, STM (Synchronous Transfer Mode) y ATM (Asynchronous Transfer Mode), si se desea usar una u otra, estas deben estar configuradas en ambos extremos de la conexión, es decir en el ATU-C (ADSL Transceiver Unit at the CO) y ATU-R (ADSL Transceiver Unit at the Remote Terminal).

Cada uno de los dispositivos que formen parte del sistema ADSL deben estar en capacidad de transportar una referencia de tiempo de red o NTR (Network Timing Reference) para su sincronización.

2.2.3.2.1 Transporte de Datos en STM

Los sistemas que deseen transportar datos en el modo STM deben soportar los canales AS0 y LS0, el resto de los canales de datos son opcionales, el canal AS0 deberá soportar tasas de transferencia de múltiplos de 32 Kbps desde 32 Kbps hasta 6.144 Mbps, LS0 debe soportar transferencias de datos a partir de 16 Kbps, a partir de los 32 kbps la tasa de transferencia se incrementara en múltiplos de 32 Kbps hasta llegar a los 640 Kbps; los canales opcionales también deben soportar múltiplos de 32 Kbps y tasas de transferencia fuera de estos múltiplos es opcional.

Bearer channel	Lowest Required Integer Multiple	Largest Required Integer Multiple	Corresponding Highest Required Data Rate (kbit/s)
AS0	1	192	6144
AS1	1	144	4608
AS2	1	96	3072
AS3	1	48	1536
LS0	1	20	640
LS1	1	20	640
LS2	1	20	640

Tabla 2.12. Tabla de los Múltiplos de 32 Kbps Requeridos para STM[36]

[36] Recomendación G.992.1, International Telecomunication Union, Pág. 15.

2.2.3.2.2 Transporte de datos en ATM

Los sistemas ADSL que usen transporte de datos mediante ATM deberán utilizar los canales con múltiplos de 32 Kbps, en los de downstream hasta 6.144 Mbps y en hasta 640 Kbps en upstream, cuando el modo ATM este seleccionado el canal AS0 debe servir solo en dirección downstream y LS0 para upstream.

Los canales AS1 y LS1 son opcionales a la hora de establecer transporte ATM, los canales AS2, AS3 y LS2 no son soportados en el modo ATM.

2.2.3.3 Características Funcionales de ATU-C

2.2.3.3.1 Network Timing Reference

Para que un sistema ADSL pueda tener referencia de tiempo, el transporte de ADSL lleva consigo un marcador de tiempo de 8 Khz. como NTR, este marcador de tiempo es usado para reproducción de video y sonido en el decodificador (convertidor D/A) para ciertas aplicaciones.

El ATU-C debe generar un referencia de tiempo local de 8 Khz. dividiendo el reloj por un integrador apropiado, por lo general el reloj interno en equipos ADSL es de 2.208 Mhz. en cuyo caso el integrador es de 276; para poder transmitir este NTR entre supertramas se usan cuatro bits, del ntr3 al ntr0.

2.2.3.3.2 Trama de Downstream

Para el ATU-C y en forma especifica para la trama de downstream se encuentran definidos dos tipos de entramados: full overhead y reduced overhead, cada uno de estos dos tipos tiene dos versiones, por lo que en total tenemos cuatro tipos de entramados posibles que se pueden encontrar para transmisiones desde el CO, se les identifica desde el 0 al 3; en la siguiente tabla se puede observar la definición de cada uno de los tipos de tramas del ATU-C.

ESTRUCTURA DE TRAMA	DESCRIPCIÓN
0	Trama Full Overhead con temporización bit a modem asincrónica (mecanismo de control de sincronización habilitado)
1	Trama Full Overhead con temporización bit a modem sincrónica (mecanismo de control de sincronización deshabilitado)
2	Trama Reduce Overhead con separación de byte rápido y sincronizado, usando los buffers de rápida e intercalada latencia respectivamente
3	Trama Reduce Overhead con unión de byte rápido y sincronizado, usando los buffers de rápida e intercalada latencia respectivamente

Tabla 2.13. Descripción de los Tipo de Tramas del ATU-C para Downstream[37]

Durante la inicialización el ATU-C deberá indicar cual es el número de trama más alto que soporta, teniendo en cuenta que debe soportar todos los números de trama inferiores a este; por otro lado, si el ATU-R indica un número de trama inferior al del ATU-C, este deberá adaptarse al número de trama indicada por el ATU-R.

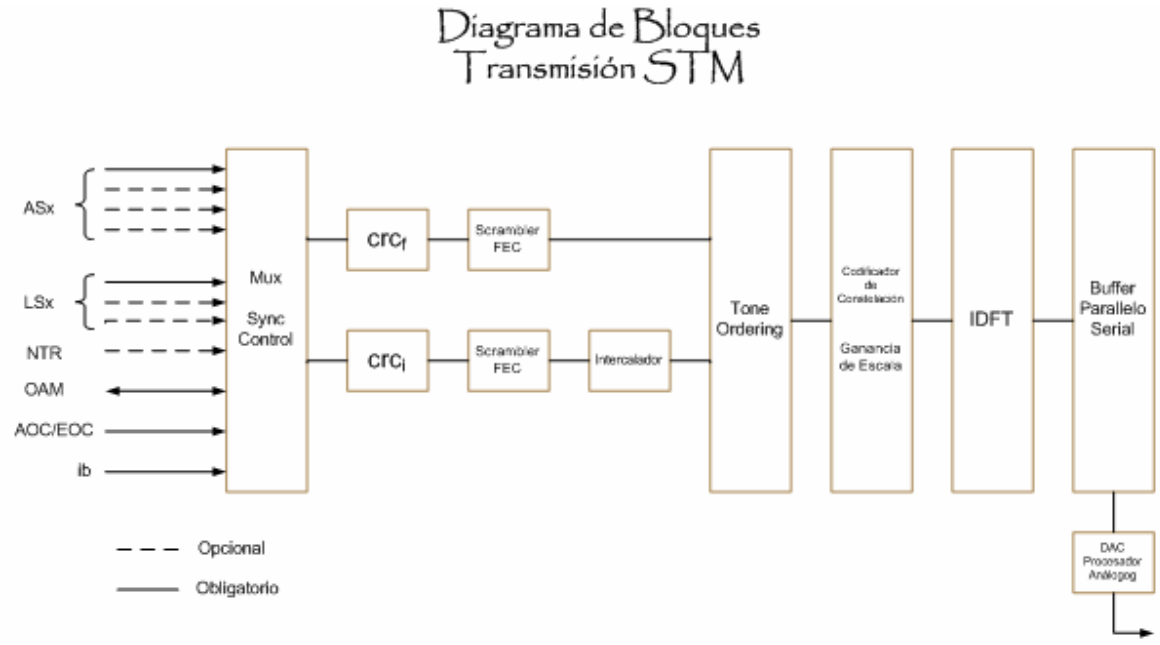


Figura 2.21. Diagrama de Bloques para Transmisión STM

[37] Recomendación G.992.1, International Telecomunication Union, Pág. 25.

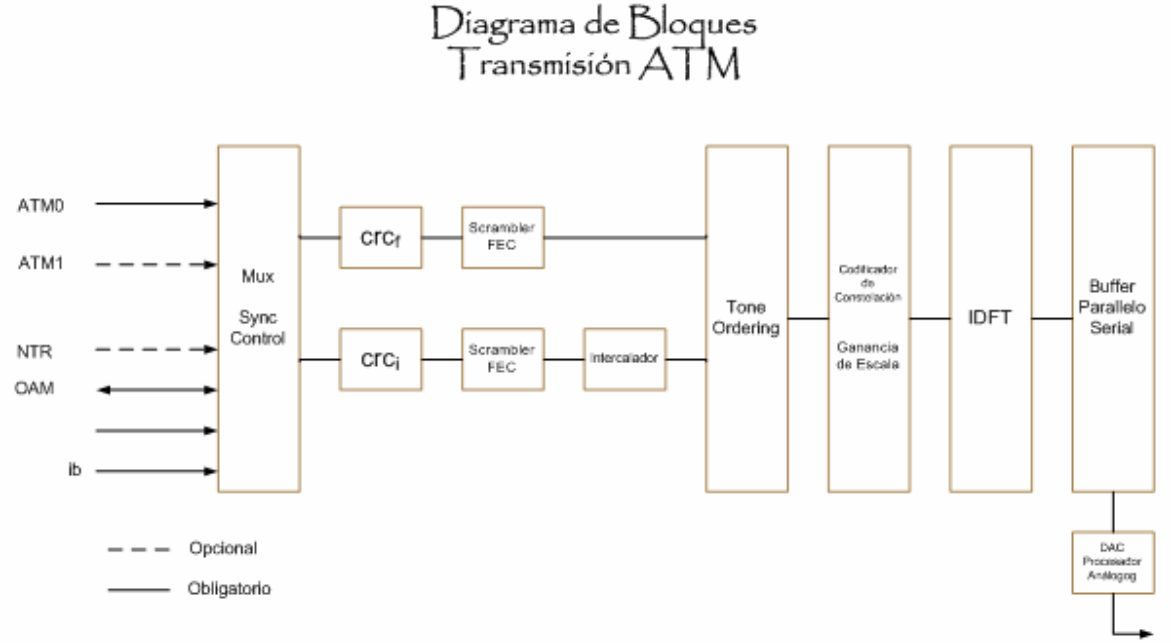


Figura 2.22. Diagrama de Bloques para Transmisión ATM

Los canales de datos tanto los obligatorios como los opcionales deben sincronizarse una tasa de trama DMT de 4 Khz., y multiplexada en buffers de datos separados, el rápido y el intercalado. Los pasos de CRC (cyclic redundancy check), scrambling y codificación FEC (Forward Error Correction) deberán ser aplicadas a cada uno de los contenidos de los buffers en forma separada. Las dos cadenas de datos deben ser ordenadas en tono y combinadas en símbolos de datos los cuales son entregados al codificador de constelación. Después de la codificación, los datos deben ser modulados para producir una señal análoga para su correspondiente transmisión a través del loop local.

Los bits de identificación de nivel de trama no deben ser insertados en los símbolos de datos de la estructura de trama o supertrama; La limites de la trama DMT son definidos por el prefijo cíclico que inserta el modulador, por otro lado los limites de la supertrama son definidos por el símbolo de sincronización, el cual es insertado por el modulador y no lleva información del usuario.

En cada trama hay datos que han sido transformados y nueva información añadida para preservar los datos, por lo que se ha procedido a poner puntos de referencia en donde se puede describir los datos de las tramas, estos puntos de referencia son A, B, y C.

A (Trama de Datos Multiplexada).- “En este punto encontramos los datos multiplexados y sincronizados después del CRC, estos datos al salir del multiplexor deben tener una tasa de transferencia de 4000 Baud/s.”[38]

B (Trama de Datos de Salida del FEC).- “Esta parte nos muestra la trama de datos a la salida del codificador FEC, estos datos tienen una tasa de símbolos DMT.”[39]

C (Trama de Datos de Entrada del Codificador de Constelación).- “En este tramo encontramos los datos de la trama que son presentados al codificador de constelación.”[40]

2.2.3.3.2.1 Supertrama

ADSL usa además de las tramas revisadas anteriormente una unión de varias tramas para crear la denominada supertrama, cada una de estas supertramas lleva 68 tramas de datos, estas están identificadas por números que van desde el 0 hasta el 67, estas supertramas están moduladas en símbolos DMT, seguidas por símbolos de sincronización que no llevan datos ni de usuario o encabezados, estos símbolos de sincronización son introducidos por el modulador para establecer los limites de la supertrama.

La tasa de transferencia de los símbolos DMT es de 4000 baud/s., pero para poder realizar la inserción de los símbolos de sincronización se debe acelerar esta tasa de transferencia hasta los 4058.823 baud/s.

En cada una de las tramas de esta supertrama encontraremos datos tanto del buffer de multiplexación rápida e intercalada, el tamaño de los datos de cada buffer depende de la cantidad de canales de datos que maneje el equipo ADSL, ya que si hay más canales de datos podría existir más datos en uno u otro buffer.

[38] Recomendación G.992.1, International Telecomunication Union, Pág. 26.
[39] IBID 38
[40] IBID 38

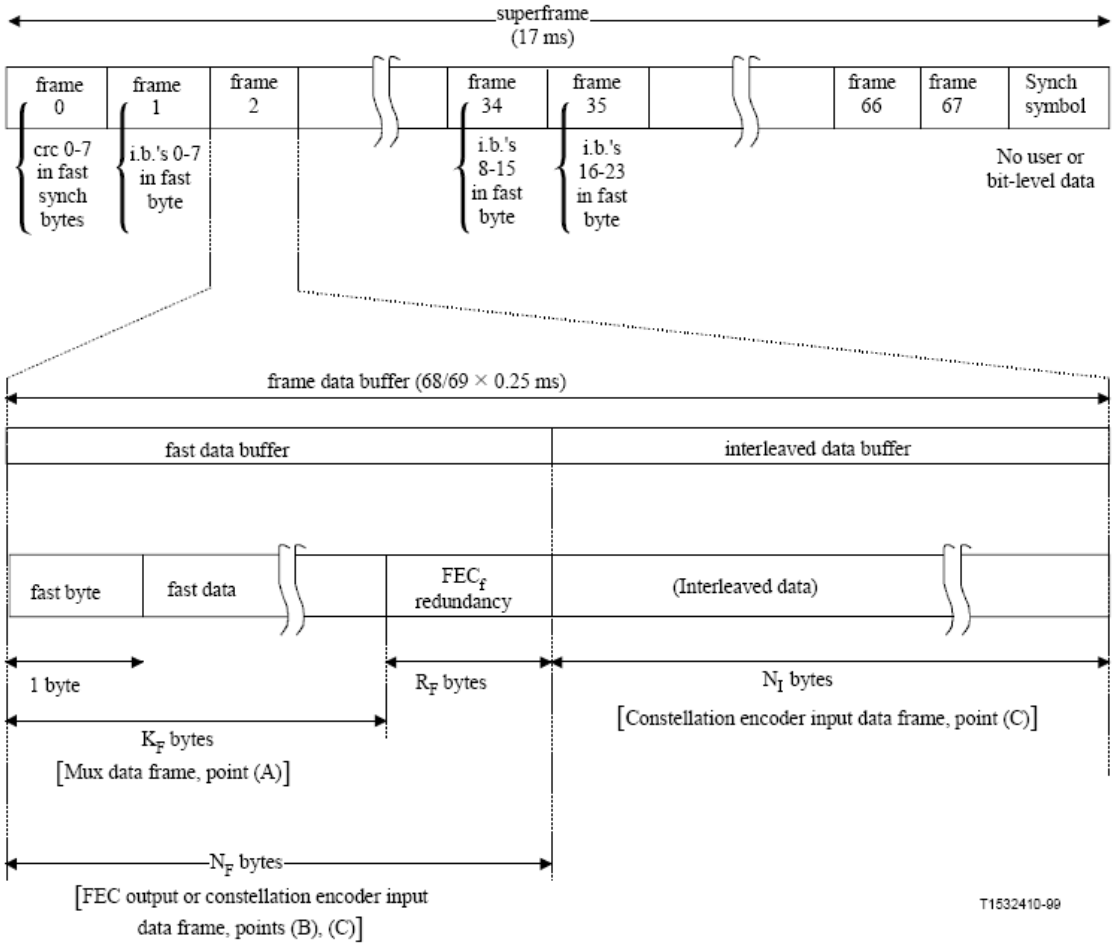


Figura 2.23. Estructura de la Supertrama ATU-C[41]

En cada una de las supertramas ADSL se deben reservar ocho bits de CRC (crc0-crc7) entre los datos del buffer rápido, además de estos ocho bits, se deben reservar 24 bits indicadores (ib0-ib23) para funciones de operación, administración y mantenimiento (OAM).

Estos bits se incluyen en el caso de los CRC en el byte de sincronización de los datos del buffer rápido, o mejor conocido como “fast byte” de la primera trama o trama 0; los bits indicadores restantes se ubican en las tramas 1, 34 y 35. El fast byte en otras tramas se asigna a parejas de tramas pares/impares que pasen por el buffer de datos rápidos.

Para cualquier otra trama que no sea la 0 o la 34, el bit 0 del fast byte tanto de la trama par como en la trama impar siguiente debe ser establecido como “0”, esto indica que estas tramas llevan información para el control de la sincronización.

[41] Recomendación G.992.1, International Telecomunication Union, Pág. 27.

Cuando no se requiere enviar mensajes de sincronización, CRC o bits indicadores, los fast bytes de las tramas contienen bits que indican que no hay acción de sincronización; en estos casos se puede utilizar este fast byte para enviar mensajes de operación para los canales de datos (EOC).

Para indicar que se envían mensajes de operación para los canales de datos, en las tramas que no sean la 0 o 34, el bit 0 del fast byte de las tramas par y su pareja impar deben establecerse como “1”.

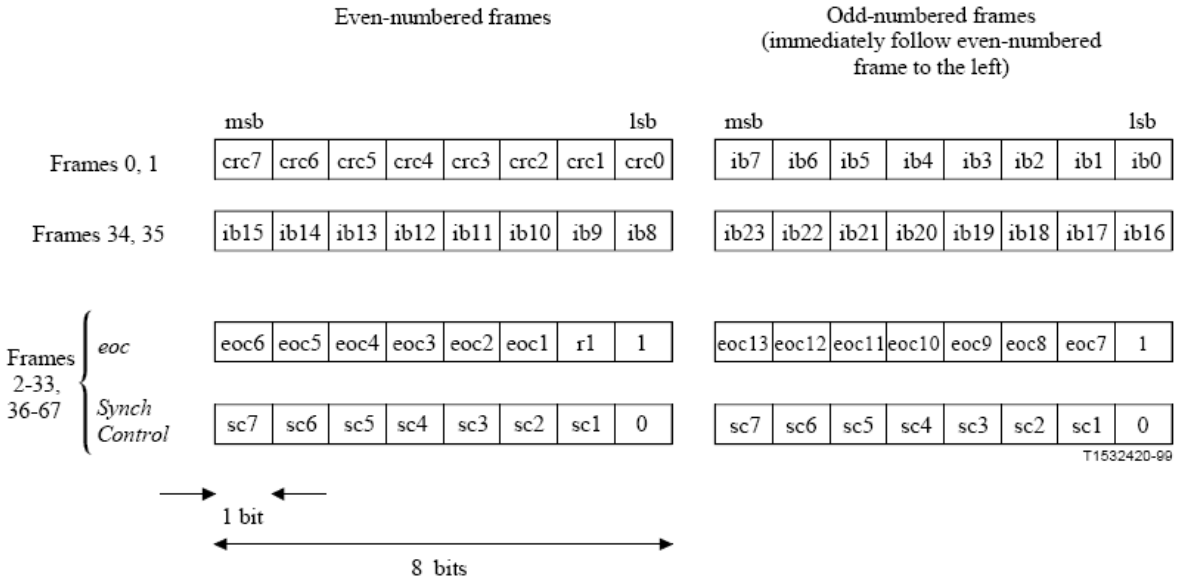


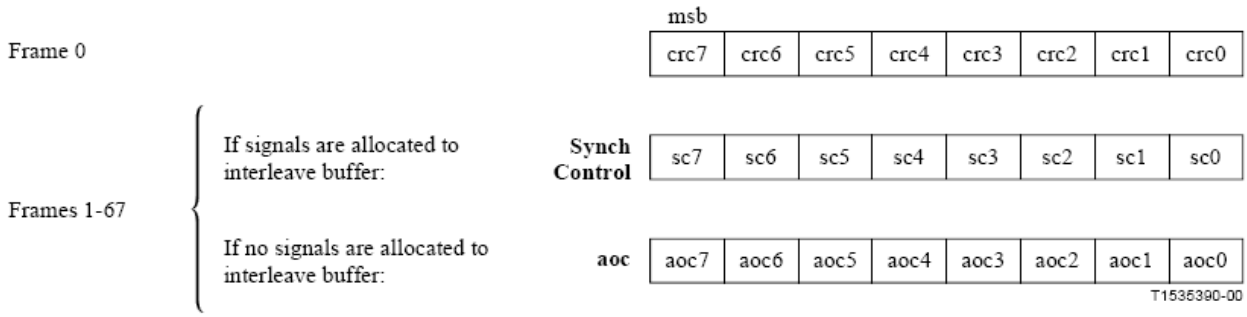
Figura 2.24. Formato del Fast Byte de la Supertrama[42]

El byte de sincronización de los datos el buffer de intercalado, mejor conocido como “sync byte”, es el encargado de llevar los bits CRC de la supertrama anterior hasta la trama 0; en todas las demás tramas de la 1 a la 67, el sync byte debe ser usado para el control de la sincronización de los canales de datos que pasan por el buffer de intercalado, o para llevar el encabezado de control de canal ADSL (AOC).

Cuando se trabaja en el modo de full overhead, y existen datos que pasen por el buffer de intercalado los datos de AOC deben ser transportados por el byte LEX, y el sync byte es el encargado de determinar cuando este byte LEX llevara los datos AOC o cuando lleva

[42] Recomendación G.992.1, International Telecomunication Union, Pág. 28.

bytes de datos provenientes del canal de datos; por otro lado si no hay datos provenientes del buffer de intercalado, el sync byte debe llevar los datos AOC directamente.



NOTE – The names "fast byte" and "sync byte" are abbreviations for, and are used interchangeably with, "fast synchronization byte" and "interleaved synchronization byte", respectively.

Figura 2.25. Formato del Byte de Sincronización Intercalado ATU-C[43]

2.2.3.3.2.2 Estructura de la Trama con Full Overhead

Cada trama de datos debe ser codificada en símbolos DMT, cada una de las tramas esta compuesta por datos de buffer rápido e intercalado, y de la misma manera que en las revisiones de anteriores esta estructura de la trama cambia según en punto de referencia se encuentre la trama, el punto A, B, o C; los bytes que salen del buffer de datos rápidos deben ser sincronizados primero en el codificador de constelación, seguidos por los bytes del buffer de intercalado, los bits son sincronizados desde el bit menos significativo en primer lugar.

Cada uno de los canales de dato debe ser asignado a ambos buffers, es decir al rápido o al de intercalado, donde se obtienen pares de bytes de cada canal.

2.2.3.3.2.3 Estructura de la Trama con Reduced Overhead

En las tramas Full Overhead se pueden apreciar encabezados que permiten la sincronización de los canales de datos tanto los ASx como los LSx, pero cuando estas funciones no son necesarias, se trabaja con las denominadas tramas con reduced overhead, cabe destacar que se tienen todas las funciones de las tramas con full overhead pero sin los espacios en el encabezado para los bits de sincronización.

En las tramas con reduced overhead existen dos modos de transmitir los datos, la primera con funciones simultaneas de los buffers de datos rápido e intercalado, y por otro

[43] Recomendación G.992.1, International Telecomunication Union, Pág. 29.

lado la transmisión de dato solo por uno de los dos buffers, es decir solo con el buffer de datos rápido o intercalado.

En el primer modo de operación, el modo de funcionamiento es exactamente igual al de la trama con full overhead, pero sin necesidad de llevar los bits de sincronización para los datos del buffer de intercalado y para los datos del buffer rápido, en vez de llevar información de sincronización, la leyenda de no acción de sincronización.

En la otra maño, cuando se usa solo uno de los buffers, ya sea el fast byte o el sync byte serán los únicos que llevaran la información del encabezado, el funcionamiento de las tramas 0, 1, 34, y 35 no cambian con respecto al uso que se le daba en las tramas con full overhead; en el resto de tramas, los bits para sincronización llevaran o los datos de AOC o mensajes de no acción de sincronización.

2.2.3.3.3 CRC

Una vez que los dato pasan a través de los buffers de datos, tanto el rápido como el intercalado, los datos pasan al bloque de CRC (Cyclic Redundancy Check), uno por cada salida de los buffers, de esta forma se integran los bits crc a la supertrama.

Los bits crc responden al siguiente polinomio generador:

$$crc(D) = c_0 D^7 + c_1 D^6 + ... + c_6 D + c_7$$

Formula 2.3. Polinomio Generador del CRC para ATU-C[44]

En donde D es el operador delay; como se menciono anteriormente estos bits son llevados por los fast o sync bytes de la trama 0 de cada buffer.

2.2.3.3.4 Scrambler

Una vez que tenemos las cadenas de datos binarios a la salida de los buffers de datos, debemos pasarlos en forma separada por los bloques de reordenamiento, teniendo en cuanta que los bits menos significativos son los que ingresaran primeros; el reordenamiento de estas cadenas de datos se realizan de acuerdo al siguiente algoritmo:

[44] Recomendación G.992.1, International Telecomunication Union, Pág. 32.

$$d'_n = d_n \oplus d'_{n-18} \oplus d'_{n-23}$$

Formula 2.4. Algoritmo del Reorganizador ATU-C[45]

Donde d_n es el dato enésimo de salida del buffer de datos rápido o intercalado, mientras que *d'n* corresponde a la enésima salida del scrambler.

Esta reorganización se aplica a las cadenas de datos sin sincronización ya sea de trama o de símbolo, de la misma manera independiente se realiza la de-reorganización.

2.2.3.3.5 Forward Error Correction

Los equipos ADSL, especialmente aquellos que pertenecen al ATU-C deben ser capaces de soportar en sus transmisiones de downstream la codificación RS FEC (Reed Solomon Forward Error Correction).

Con una tasa de 4000 tramas de datos por segundo y 255 bytes por trama de datos, la tasa de transmisión es de aproximadamente 8 Mbps; pero en el canal de datos AS0 se puede de forma opcional, mediante la inclusión de dos palabras de código en una sola trama de datos FEC alcanzar tasas de transmisión de 16 Mbps.

2.2.3.3.6 Tone Ordering

Una señal DMT en el dominio del tiempo posee una gran relación pico a promedio, lo que significa que su amplitud de distribución es casi Gaussiana, por lo que gran cantidad de datos pueden ser añadidos por el convertidor digital a análogo.

Errores ocasionados por los ordenamientos en tonos son más propensos en los tonos que pueden transmitir una mayor cantidad de bits, pero estos errores pueden ser fácilmente solucionados mediante por la codificación FEC si los tonos con mayor cantidad de datos son asignados a los provenientes del buffer de intercalado.

La cantidad de bits y ganancia de cada tono debe ser calculada por el ATU-R, estos valores son almacenados en una tabla la cual debe ser transmitida al ATU-C.

[45] Recomendación G.992.1, International Telecomunication Union, Pág. 37.

Primero se deben reservar ocho por el número de bytes de una trama bits del buffer de datos rápidos para los tonos con el menor número de bits asignados; luego ocho por el número de bytes del buffer de intercalado bits para el resto de tonos.

Luego se codifican los tonos con el número de bits asignados a cada tono, en algunos casos los tonos tendrán bits de los dos buffers.

A continuación se presentara un ejemplo con 6 tonos DMT y 1 byte por trama por cada buffer.

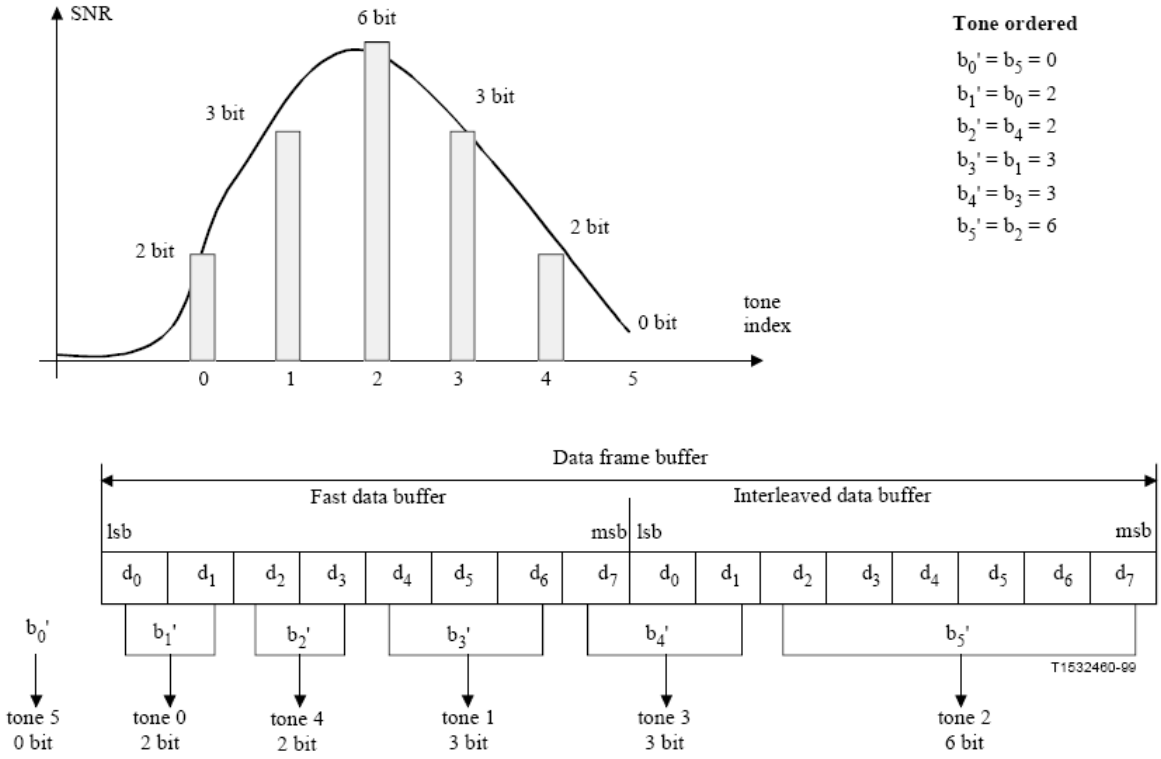


Figura 2.26. Ejemplo del Ordenamiento en Tonos

2.2.3.3.7 Codificador de Constelación

Los equipos ADSL tienen la opción de implementar un bloque de procesamiento de código de Trellis de 16 estados y 4 dimensiones de forma opcional para mejorar el desempeño; por otro lado se debe usar un codificador de constelaciones algorítmico para construir las constelaciones con un número de bits máximo entre 8 y 15 incluidos.

A continuación se podrá revisar el codificador de constelaciones funcionando en su modo básico, dejando el bloque de mejoramiento para futuros estudios.

2.2.3.3.7.1 Extracción de Bits

Los bits de datos de la trama del buffer deben ser extraídos de acuerdo a la tabla de reordenamiento usada para el reordenamiento de tonos (b_i), comenzando por el menos significativo; el número de bits por tono puede tomar cualquier valor entero no negativo dentro de los valores de 8 a 15 y mayores que 1. Para un tono dado, los bits se extraen de la trama de datos y pasan a formar parte de una palabra binaria $\{v_{b-1}, v_{b-2},\ldots, v_1, v_0\}$, por lo tanto el primer bit en ser extraído debe ser v_0, el menos significativo.

2.2.3.3.7.2 Funcionamiento del Codificador de Constelación

Una vez que se tiene la palabra binaria, formada por los bits extraídos de la trama de datos, procedemos a formar constelaciones basados en los bits b de las palabras binarias, en el caso de valores de b pares se forman las constelaciones tomando como coordenadas X,Y a los bits v_{b-1}, v_{b-2}, etc., en el caso de valores b impares se debe formar las parejas de coordenadas X,Y de entre cinco bits de la palabra binaria, se debe tener en cuenta que cada punto tiene una representación complementaria a partir de valores de b impares mayores a 3.

A continuación un ejemplo de la constelación para b = 2, 3, 4, y 5.

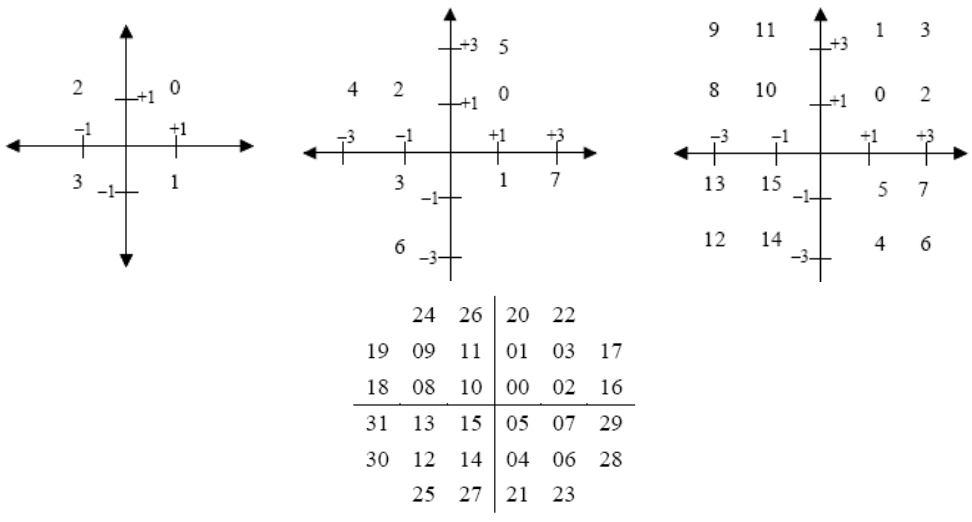


Figura 2.27. Representación de Constelaciones para Valores de b = 2, 3, 4 y 5.

2.2.3.3.8 Ganancia de Escala

La ganancia de escala es un factor por el cual se multiplican los puntos de coordenadas X,Y de la constelación formada, los valores de g_i son de 0 y entre 0.19 hasta 1.33, esta ganancia de escala es implementada una vez que se ha realizado una solicitud por parte del ATU-R.

La ganancia de escala no puede ser aplicada al momento de transmitir los símbolos de sincronización.

2.2.3.3.9 Modulación

2.2.3.3.9.1 Subportadoras

El espaciamiento de frecuencias entre subportadoras Δf es de 4.3125 Khz. Tal como se reviso anteriormente, el número máximo de portadoras a ser usadas en sistemas ADSL es de tan solo 255, a frecuencias nΔf (n = 1 hasta 255).

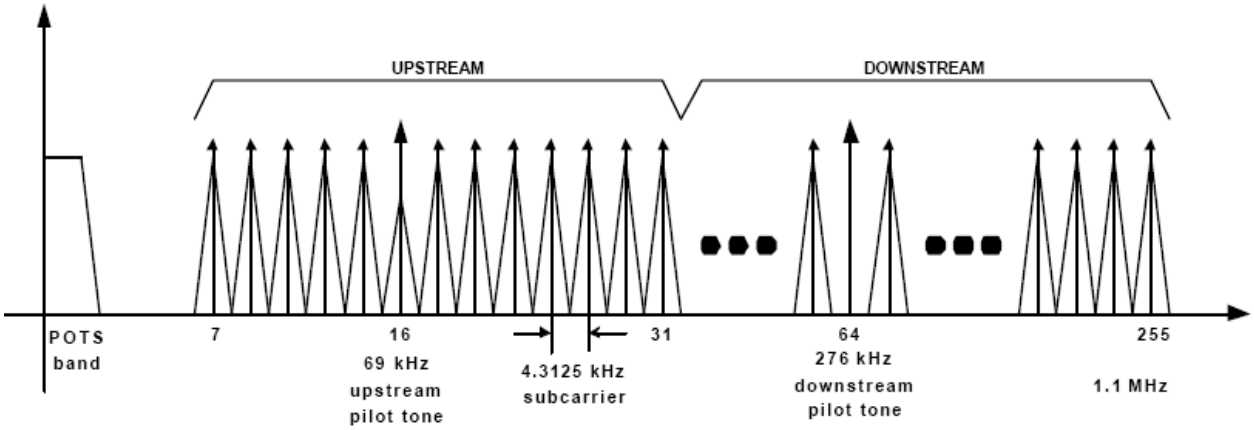


Figura 2.28. Distribución de las Subportadoras ADSL

El limite más bajo de n es limitado por la duplexión y el tipo de servicio que se escoja, por ejemplo en funcionamiento sobre POTS este limite depende del filtro splitter que se use, en otras palabras depende del fabricante; por otro lado la portadora más alta a ser utilizada se establece en la estimación de canal.

La frecuencia de Nyquist (n = 256) no debe ser utilizada para transportar datos, ya que su uso esta destinado para futuras aplicaciones; sin embargo los equipos deben ser capaces de generarla en forma practica.

2.2.3.3.9.2 Modulación por la Transformada de Fourier Discreta Inversa (IDFT)

La modulación mediante la transformada establece la relación entre 512 valores reales x_n y Z_i:

$$x_n = \sum_{i=0}^{511} \exp\left(\frac{j\pi ni}{256}\right) Z_i; n = 0,...,511$$

Formula 2.5. Transformada Inversa Rápida de Fourier para Modulación en ATU-C[46]

Tanto el codificador de constelación como la ganancia de escala generan solo 255 valores complejos de Z_i; por lo tanto para poder tener valores reales de x_n, a los 255 valores de entrada se les incrementa otros valores para que el vector Z tengan simetría Hermitiana, es decir:

$$Z_i = conj(Z'_{512-i}); i = 257,...,511$$

Formula 2.6. Formula para la Obtención de Valores Reales de x_n[47]

Cabe destacar que los valores de entrada son los 255 valores complejos más una componente de DC con valor de cero y un valor real si se usa la componente de Nyquist.

2.2.3.3.10 Prefijo Cíclico

Las últimás 32 muestras de salida del bloque IDFT, es decir de la salida 480 a la 511, deben ser extraídas y puestas al principio del siguiente bloque de 512 muestras a modo de prefijo y enviadas al DAC en secuencia.

2.2.3.3.11 Rango Dinámico de Transmisión

Los niveles de ruido así como los de distorsión de cada portadora, se miden mediante una prueba de Relación de Poder de Multi Tono o MTPR por sus siglas en inglés.

En cada portadora el nivel de MTPR no debe ser menor a (3N+20) dB, en donde N es el tamaño de la constelación en bits que usa cada portadora; teniendo en cuenta que el mínimo valor de N es de 6 ninguna portadora debe tener un menos de 38 dB de MTPR.

[46] Recomendación G.992.1, International Telecomunication Union, Pág. 51.
[47] Recomendación G.992.1, International Telecomunication Union, Pág. 52.

2.2.3.4 Características Funcionales de ATU-R

Para empezar a detallar las funciones del ATU-R primero debemos destacar que las funciones de transporte y canales revisados previamente y aplicables al ATU-C son las mismas que cumplen los equipos correspondientes al ATU-R.

2.2.3.4.1 Network Timing Reference

En caso de que el ATU-C indica el uso de los bits indicadores del 20 al 23 para la transmisión del cambio del offset de fase, el ATU-R debe entregar una señal de 8 Khz. A la interfase de capa superior, ya sea la ATM o STM.

2.2.3.4.2 Trama de Upstream

La trama de la señal de upstream (transmisión del ATU-R) es muy similar a la trama de downstream (transmisión del ATU-C), con algunas excepciones las cuales se presentan a continuación:

- No existen los canales ASx y por lo tanto no se usan los bytes de sincronización.
- Existen máximo tres canales, por lo que existen solo tres parejas de bytes tanto del buffer de datos rápido como intercalado.
- Los parámetros de la codificación FEC y la profundidad de intercalado varían.
- Cuatro de los bits de los sync como fast bytes quedan sin ser utilizados.
- Los bits indicadores del NTR no se usan en la dirección de upstream, por el contrario el ATU-R debe ser capaz de reconstruir las señales del NTR enviadas por el ATU-C.

Están definidas dos tipos de tramas, la primera denominada full overhead y la segunda reduced overhead; cada una de estas tramas posee dos versiones, lo que nos deja con un total de cuatro tramas, y nos referiremos a ellas como estructuras de tramas 0, 1, 2 y 3.

El uso de una u otra estructura de trama dependerá del tipo de configuración que posea el equipo, ya sea STM o ATM. Las funciones de la trama ATU-R es muy similar a las de la trama ATU-C, con la excepción de que solo tenemos tres canales full duplex sincronizados a una tasa de símbolo ADSL DMT de 4 Khz. Y multiplexados en dos buffers separados, el de intercalado y rápido.

2.2.3.4.2.1 Supertrama

La estructura de la supertrama de transmisión ATU-R es idéntica a la estructura de la ATU-C; ATU-R debe soportar los mismos bits indicadores que la supertrama de downstream, con la excepción de que los bits ib20 al ib23 no deben trasportar NTR en la dirección de upstream, en su lugar deben estar configurados en “1”.

Dos chequeos de redundancia cíclica se generan para los datos tanto del buffer de datos rápido como para el de intercalado en cada supertrama. Los bits crc son transportados en el fast byte de la trama 0 y en el sync byte de la trama 0 en el buffer de intercalado.

2.2.3.4.2.2 Estructura de la Trama con Full Overhead

Cada trama de datos debe ser codificada en símbolos DMT, cada trama esta compuesta por datos de los buffers de intercalado y rápido, la trama tiene diferentes aspectos dependiendo de en punto de control se encuentre, estos son A, B o C; los datos provenientes del buffer de datos rápido deben sincronizarse primero en el codificador de constelación, seguidos por los bytes del buffer de datos intercalados, tal como en el equipo del CO los bits menos significativos deben ir primero.

2.2.3.4.2.3 Estructura de la Trama con Reduced Overhead

En la estructura de la trama con Full Overhead se puede encontrar los encabezados que contienen los bits de sincronización de los tres canales LSx, pero cuando no se necesita esta sincronización debido a que no se tienen los canales opcionales en funcionamiento, se usa la trama con reduced overhead, esta trama contiene todas las funciones que la trama full overhead, excepto el control de sincronización.

2.2.3.4.3 Scrambler

Las salidas de las tramas de datos de los buffers de datos rápido e intercalado deben ser reorganizadas en forma separada usando los mismos algoritmos que en las señales de downstream.

2.2.3.4.4 Forward Error Correction

Los datos de upstream deben soportar codificaciones Reed Solomon y su intercalamiento debe ser realizado mediante los mismos algoritmos para los datos de

downstream; tanto el encabezado FEC, el número de símbolos por palabra de código y la profundidad de intercalado son especificadas por el ATU-C al momento de la iniciación.

2.2.3.4.5 Tone Ordering

Los algoritmos de ordenamiento de tonos deben ser los mismos usados para los datos de downstream.

2.2.3.4.6 Codificador de Constelación (Codificación Trellis)

Para mejorar el desempeño del sistema se puede usar un bloque de procesamiento de Wei de 16 estados y 4 dimensiones con código de Trellis de forma opcional. Un codificador de constelación algorítmico debe ser usado para la construcción de la constelación con un máximo número de bits entre 8 y 15 inclusive. El algoritmo de codificación debe ser el mismo que se usa en los datos de downstream.

2.2.3.4.7 Codificador de Constelación (Sin Codificación)

Un codificador algorítmico de codificación debe ser usado para la construcción de la constelación con un máximo número de bits entre 8 y 15 inclusive; el algoritmo de codificación debe coincidir con el usado en para los datos de downstream; el codificador de constelación no debe usar codificación Trellis en esta opción.

2.2.3.4.8 Ganancia de Escala

Para la transmisión de símbolos de datos se debe aplicar la ganancia de escala g_i como un pedido del ATU-C; los valores permitidos de g_i son cero y de 0.19 hasta 1.33 correspondientes a -14.5 dB hasta +2.5 dB.

2.2.3.4.9 Modulación

2.2.3.4.9.1 Subportadoras

El espaciamiento de frecuencias Δf, entre las portadoras debe ser de 4.3125 Khz.; el análisis del canal nos permite el uso de máximo 31 portadoras o subportadoras a frecuencias de nΔf, el rango de n dependerá del servicio que se desee brindar; cabe destacar que el mínimo n esta limitado por el splitter y el máximo por la estimación del canal y no mayor a 31, las frecuencias de corte están a discreción del fabricante.

La portadora a la frecuencia de Nyquist no debe ser utilizada para transmisión de datos, pero los equipos deben ser capaces de implementarla, esta portadora y sus usos están reservados para futuros usos.

2.2.3.4.9.2 Modulación por la Transformada de Fourier Discreta Inversa

La modulación mediante la transformada establece la relación entre 64 valores reales x_n y Z_i.

$$x_n = \sum_{i=0}^{63} \exp\left(\frac{j\pi ni}{32}\right) Z_i$$

Formula 2.7. Transformada Inversa Rápida de Fourier para Modulación en ATU-R[48]

El codificador y la ganancia de escala generan solo 31 valores complejos de Z_i (se debe tomar en cuenta que los valores son cero en la componente de DC como valor real más el valor complejo). Para poder generar los valores reales de x_n, a estos datos se les debe aumentar otros valores para que el vector Z posea simetría Hermitiana, estos nuevos valores responden a la siguiente formula:

$$Z_i = conj[Z_{64-i}]; i = 33,...,63$$

Formula 2.8. Formula para la Obtención de Valores Reales de x_n[49]

2.2.3.4.10 Prefijo Cíclico

Las últimas 4 muestras de salida del bloque IDFT, es decir de la salida 60 a la 63, deben ser extraídas y puestas al principio del siguiente bloque de 64 muestras a modo de prefijo y enviadas al DAC en secuencia.

2.2.3.4.11 Rango Dinámico de Transmisión

Los niveles de señal a ruido y la relación de distorsión de cada portadora, se mide mediante la prueba de Relación de Poder de Multi Tono o MTPR.

Sobre la banda de frecuencia de transmisión, los valores del MTPR en cualquier portadora no deben ser menores a (3N+20) dB, siendo N el tamaño de la constelación en

[48] Recomendación G.992.1, International Telecomunication Union, Anexo A, Pág. 128.
[49] Recomendación G.992.1, International Telecomunication Union, Anexo A, Pág. 129.

bits a ser usado en una portadora, es decir que debe ser de 38 dB si se tiene en cuenta que el valor mínimo de N en cualquier portadora es de 6.

2.2.3.5 Operaciones EOC (Embedded Operations Channel) y Mantenimiento

El EOC es una componente del encabezado del sistema ADSL el cual provee comunicación entre las entidades de gestión tanto en el ATU-C como el ATU-R.

2.2.3.5.1 EOC Transparente

El EOC debe soportar en forma obligatoria el envío de mensajes autónomos, se encarga de proveer el canal de comunicación entre las entidades de gestión de los equipos del CO y CPE, este canal esta definido tanto para direcciones upstream y downstream mediante la transmisión de los mensajes autónomos.

Estos mensajes autónomos pueden transmitirse desde el ATU-C o ATU-R, y se transforman en canales trasparentes de datos que pueden ser insertados en cualquier momento, inclusive sin requerimientos de tasas de inserción entre mensajes.

Este EOC transparente carece de un control de flujo, se entiende que el mismo es implementado por un protocolo de capa superior en caso de ser necesario.

2.2.3.5.2 Requerimientos EOC

Los servicios del EOC deben ser usados para mantenimientos en servicio o mantenimientos fuera de servicio, monitoreo del desempeño ADSL e información de status del ATU-R.

2.2.3.5.2.1 Protocolo y Organización del EOC

El EOC le permite al ATU-C (en funciones de master) solicitar comandos, mientras que al ATU-R (en funciones de slave) responder comandos; es el ATU-C el encargado de establecer la tasa de transmisión en el enlace, se debe tener en cuenta que solo un mensaje EOC puede ser enviado en dirección upstream por cada mensaje recibido, a excepción del mensaje denominado “dying gasp” cuya inserción por parte del ATU-R se realiza en cuanto las condiciones necesarias se completan.

2.2.3.5.2.2 Estructura del Mensaje EOC

El mensaje EOC esta compuesto por trece bits los cuales forman parte de cinco campos, estos bits y campos están resumidos en la tabla mostrada a continuación:

CAMPO	BIT(S)	DESCRIPCIÓN	NOTA
1	1,2	Campo de Dirección	Se pueden tener cuatro direcciones "00" Dirección ATU-R "11" Dirección ATU-C
2	3	"0" Datos, "1" Código de Operación	Datos usados para lectura/escritura o cuando un mensaje de datos es enviado
3	4	Campo de Paridad de Byte, "1" Impar, "0" Par	Indicación de Orden de Byte para transmisión multi byte
4	5	Campo de Mensaje Autónomo: ATU-C: ✓ "1" Comandos de ATU-C a ATU-R ✓ "0" Transferencias Autónomas ATU-R: ✓ "1" Para Responder los Comandos ATU-C ✓ "0" Transferencias Autónomas	Al poner "0" en el ATU-R se envía el mensaje de dying gasp o transferencias de datos autónomas
5	6-13	Campo de Información	Pueden ser uno de los 58 códigos de operación u 8 bits de datos

Tabla 2.14. Campos de Mensaje EOC

2.2.3.5.2.3 Protocolo EOC

El protocolo EOC opera según el modo de comandos repetitivos y respuesta, el ATU-C actúa como master en la comunicación y propone los mensajes de comando, mientras que el ATU-R actúa como slave y responde los mensajes propuestos por el ATU-C. Tres mensajes idénticos y debidamente direccionados consecutivos deben ser recibidos antes de iniciar una acción, esto tanto para el ATU-C y ATU-R.

Únicamente un comando y tres o menos mensajes, bajo el control del ATU-C deberán ser reconocidos cada vez; solo cuando no se tengan mensajes reconocidos, el ATU-C podrá enviar un mensaje diferente de los mensajes previamente enviados, este nuevo mensaje dará como resultado un mensaje reconocido, el ATU-C puede solo responder el mensaje previamente enviado, una vez que todos los mensajes reconocidos sean idénticos.

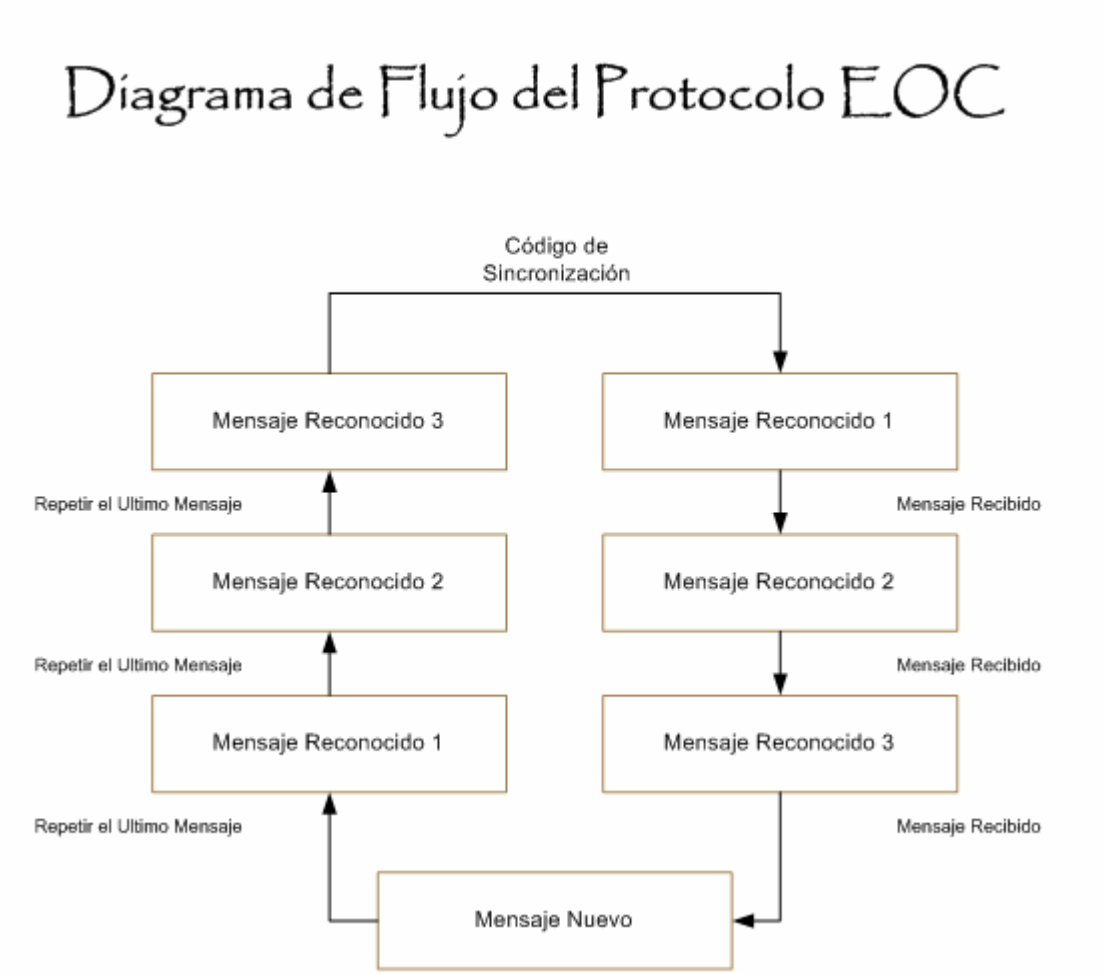


Figura 2.29. Diagrama de Flujo del Protocolo EOC

2.2.3.6 Iniciación

2.2.3.6.1 Introducción

Para poder establecer una conexión entre los equipos ADSL se requiere en primer plano una iniciación entre ellos; el proceso a cumplirse se puede fácilmente revisar en el siguiente gráfico.

Figura 2.30. Diagrama de los Procesos de Iniciación[50]

Para poder separar las señales tanto de upstream como de downstream cada fabricante tiene dos formas de realizar esta opción, la primera es FDM (Frecuency Division Multiplexing) o mediante la cancelación de eco mediante sobre posición de espectros.

Si en algún momento durante la iniciación se detecta una falla, es decir un error, timeouts, o un malfuncionamiento, ya sea el ATU-C o ATU-R envía mensajes mediante los cuales se procede a un reseteo de los equipos.

2.2.3.6.2 Entrenamiento del Transceptor ATU-C

La sincronización del entrenamiento mutuo comienza con el envío de la señal R-REVERB1, y esta se mantiene durante el entrenamiento, ya que los transceptores cuentan el número de símbolos desde ese punto.

Las señales QUIET son definidas por un voltaje de salida del DAC de cero.

[50] Recomendación G.992.1, International Telecomunication Union, Pág. 86.

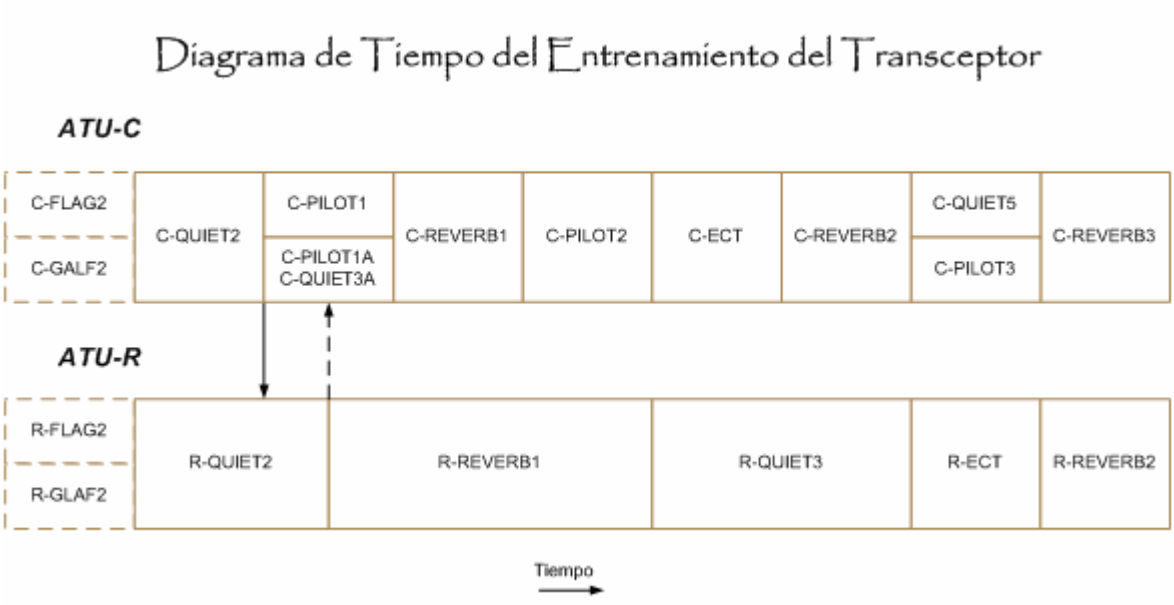


Figura 2.31. Diagrama de Tiempos del Entrenamiento del Transceptor[51]

C-QUIET2.-

C-QUIET2 empieza al terminar ya sea C-FLAG2 o C-GALF2; la duración mínima de esta señal es de 128 símbolos, mientras que la máxima duración es de 2048 símbolos; el siguiente estado al que puede pasar el ATU-C depende de los parámetros de la negociación.

C-PILOT1.-

C-PILOT1, durante esta señal el equipo en el CO debe medir el poder agregado a la señal de upstream recibida, esto de un grupo de portadoras transmitidas durante la señal R-REVERB1, y a su vez calcular la densidad espectral de poder de downstream.

Una vez que hayan pasado 16 símbolos desde la detección del primer símbolo de R-REVERB1 el ATU-C debe iniciar un contador, el cual establece la sincronización de la siguiente transición entre los estados de los dos equipos.

Después de 512 símbolos el ATU-C debe dar la señal de C-REVERB1; ya que la duración mínima del C-PILOT es de 512 símbolos, cabe destacar que en algunos casos se excede este mínimo debido al retraso de propagación y el concebido tiempo en la detección

[51] Recomendación G.992.1, International Telecomunication Union, Pág. 91.

de la señal en el ATU-R y su respuesta que es R-REVERB1, el C-PILOT1 puede durar hasta 4436 símbolos.

C-PILOT1A.-

Es la misma señal transmitida como C-PILOT1, la duración de esta es de hasta 4000 símbolos, su duración exacta depende de R-QUIET2.

Una vez que han pasado 16 símbolos después de la detección del primer símbolo de R-REVERB1 el ATU-C debe iniciar un contador y debe proceder a C-QUIET3A. La señal C-QUIET3A sigue a C-PILOT1A.

C-QUIET3A.-

Dentro de los 512 a 516 símbolos después de la detección del primer símbolo de R-REVERB1, el ATU-C debe ir a C-REVERB1; la duración mínima de C-QUIET3A es de 512 a 516 (496) símbolos, mientras que el máximo es de 516; La duración total de C-QUIET3A y C-PILOT1A es de 516 mínimo, pero se puede exceder esto hasta los 4436 símbolos debido a la propagación de la señal y el tiempo que se demora el ATU-R el detectar C-PILOT1A y responder con R-REVERB1.

C-REVERB1.-

Es la señal que le permite al receptor ATU-C y ATU-R ajustar su control de ganancia automática (AGC) a un nivel apropiado. La patente de los datos que usa C-REVERB1 debe ser la secuencia pseudo aleatoria de downstream usada en la modulación del ATU-C y repetida aquí por conveniencia.

$$d_n = 1; n = 1,...,9$$
$$d_n = d_{n-4} \oplus d_{n-9}; n = 10,...,512$$

Formula 2.9. Secuencia Pseudo Aleatoria de Downstream[52]

La primera pareja de datos se usa para transmitir la portadora de DC que es cero, mientras que el resto de parejas se usa para transmitir los pares que definen los puntos X,Y, cabe mencionar que el periodo es de solo 511 bits, por lo que el dato 512 debe ser igual al dato 1, los datos 1 al 9 deben reiniciarse para cada símbolo.

[52] Recomendación G.992.1, International Telecomunication Union, Pág. 92.

La duración de C-REVERB1 es de 512 símbolos repetitivos sin prefijo cíclico.

Power Cut-Back.-

La densidad espectral de potencia nominal transmitida por C-REVERB1 es de -40 dBm/Hz.

C-PILOT2.-

Esta señal es la misma que C-PILOT1, su duración es de 3072 símbolos; La señal C-ECT sigue a C-PILOT2.

C-ECT.-

Esta señal es definida por cada fabricante, se usa para entrenar a su sistema de cancelador de eco en el ATU-C para implementaciones de espectros sobrepuestos; los fabricantes que usen FDM tienen libertad absoluta de definir esta señal, sin embargo debe estar restringida a 512 símbolos.

El receptor ATU-R podría ignorar esta señal, la señal C-REVERB2 sigue a C-ECT.

C-REVERB2.-

C-REVERB2 permite que el receptor ATU-R realice sincronización y entrene cualquier ecualizador en el receptor; esta señal es la misma que C-REVERB1, y su duración es de 1536 símbolos repetitivos sin prefijos cíclicos, el estado que sigue a C-REVERB2 depende de los parámetros de negociación.

C-QUIET5.-

La duración de esta señal es de 512 símbolos, C-REVERB3 sigue a C-QUIET5.

C-PILOT3.-

La duración es de 512 símbolos y es la misma señal que C-PILOT1; C-REVERB3 sigue a C-PILOT3.

C-REVERB3.-

Esta es una segunda señal de entrenamiento, la cual permita al receptor ATU-R realizar o mantener sincronización, así como el entrenamiento de cualquier ecualizador; C-

REVERB3 es la misma C-REVERB2; la duración de esta señal es de 1024 símbolos repetitivos sin prefijos cíclicos; este es el último segmento del entrenamiento del transceptor, C-SEGUE1 le sigue inmediatamente.

2.2.3.6.3 Entrenamiento del Transceptor ATU-R

R-QUIET2.-

R-QUIET2 comienza al término de R-FLAG o R-GALF2, la duración mínima de esta señal es de 128 símbolos DMT después de la detección de C-PILOT1/1A; el ATU-R avanza a la señal R-REVERB1 solo después de que a detectado cualquier parte de C-PILOT1/1A, necesaria para una detección confiable; la máxima duración de R-QUIET2 es de 8000 símbolos.

El tiempo de lazo esta definido como el esclavo de la señal recibida de un reloj ADC, y enlazando los relojes locales del DAC y ADC juntos, la sincronización de lazo debe siempre realizarse en el ATU-R.

El tiempo de lazo debe ser preciso durante el periodo que comienza con la señal R-QUIET2 y termina antes de los últimos 512 símbolos de R-REVERB1; un ATU-C podría querer entrenar su ecualizador durante los últimos 512 símbolos de R-REVERB1, este entrenamiento requiere suficientes estabilidad en las muestras del reloj en el transmisor ATU-R.

Una vez que la sincronización del lazo es precisa en el ATU-R, este debe volver a revisar el tiempo de lazo después de un cierto periodo durante los 512 símbolos después de la aparición de C-PILOT; esto se aplica a C-QUIET5, C-QUIET3 y a C-ECT.

R-REVERB1.-

Esta señal le permite al ATU-C realizar las siguientes acciones:

- ✓ Medir la potencia del ancho de banda de subida para poder ajustar el nivel de potencia transmitida por el ATU-C.
- ✓ Ajustar su control de potencia de recepción.
- ✓ Sincronizar su receptor y entrenar su ecualizador.

La patente de datos del R-REVERB1 es la secuencia pseudo aleatoria de upstream usada en la modulación del ATU-R y repetida en este punto por conveniencia.

$$d_n = 1; n = 1,...,6$$
$$d_n = d_{n-5} \oplus d_{n-6}; n = 7,...,64$$

Formula 2.10. Secuencia Pseudo Aleatoria de Upstream[53]

Donde la primera pareja de datos es usada para la transmisión de la componente de DC cuyo valor es de cero, mientras que los siguientes pares son usados para definir las componentes X.Y; el periodo es de solo 63 bits, por lo que el dato 64 debe ser igual al dato 1; los datos del 1 al 6 deben ser re iniciados para cada símbolo de R-REVERB1.

La densidad espectral de potencia nominal transmitida por R-REVERB1 y todas las señales subsiguientes de upstream es de -38 dBm/Hz.

R-REVERB1 es una señal periódica sin prefijos cíclicos, la cual es transmitida consecutivamente por 4096 símbolos; los primeros 512 símbolos coinciden con las señales C-QUIET3 o C-PILOT1 en tiempo, los segundos 512 símbolos coinciden con C-REVERB1, y los restantes 3072 símbolos coinciden con C-PILOT2; la señal R-QUIET3 le sigue inmediatamente a R-REVERB1.

R-QUIET3.-

La duración de esta señal es de 2048 símbolos, de los cuales los primeros 512 símbolos coinciden con C-ECT en tiempo, los siguientes 1536 símbolos coinciden con C-REVERB2; el símbolo final de R-QUIET3 puede ser acortado por cualquier número de muestras para acomodar la alineación de la trama de transmisión a recepción.

R-ECT le sigue en forma inmediata a R-QUIET3.

R-ECT.-

Esta señal es similar a C-ECT, ya que esta definida por cada constructor para el entrenamiento del cancelador de eco en el ATU-R, la duración de esta señal esta confinada a 512 símbolos DMT; R-REVERB2 le sigue a R-ECT.

R-REVERB2.-

La señal R-REVERB2 es la misma que R-REVERB1, puede ser usada por el ATU-C para realizar recuperaciones de reloj y entrenamiento de ecualizadores de recepción; la

[53] Recomendación G.992.1, International Telecomunication Union, Anexo A, Pág. 133

duración de esta señal debe estar entre 1024 y 1056 símbolos; esta es el último segmento del entrenamiento del receptor.

Una vez terminada esta señal el ATU-R comienza con el análisis del canal y comienza a transmitir R-SEGUE1.

2.2.3.6.4 Análisis del Canal ATU-C

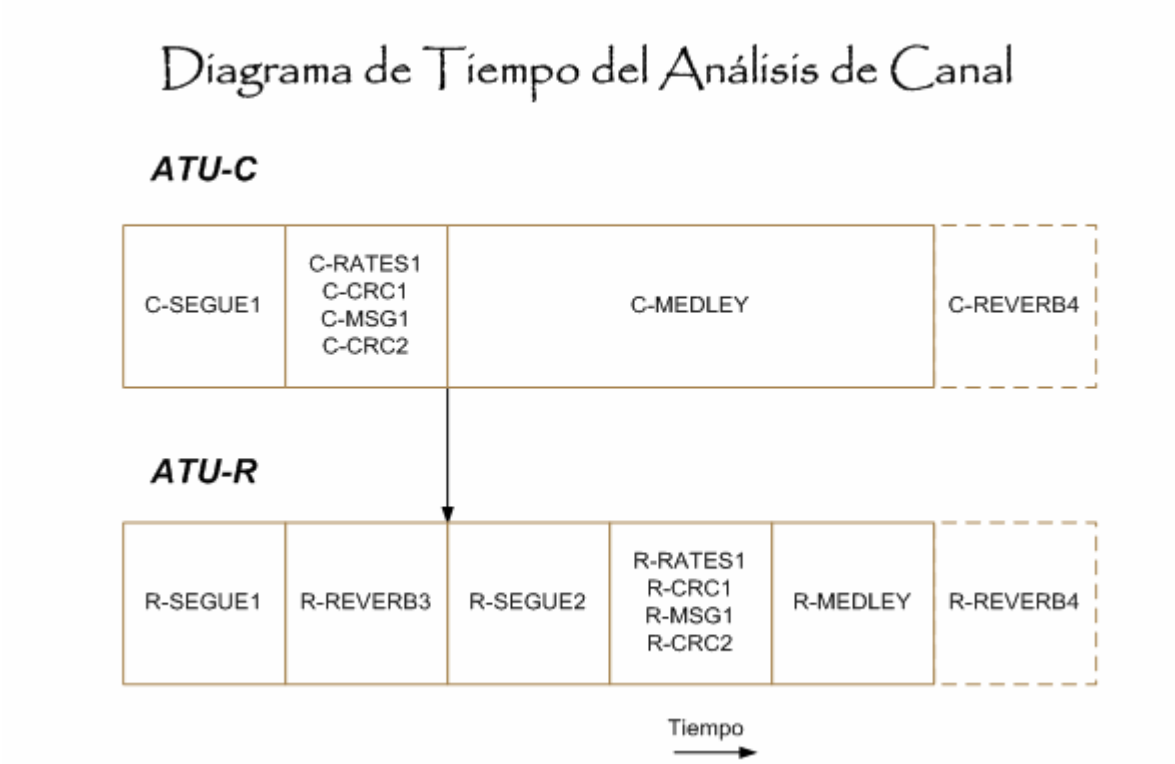


Figura 2.32. Diagrama de Tiempo del Análisis del Canal[54]

Durante el análisis del canal, la sincronización entre el ATU-C y ATU-R puede verse interrumpida durante R-REVERB3 debido a su duración infinita; si durante el análisis del canal, cualquier CRC check sum indica un error en cualquier dato de control, se activará un reset mediante C-SILENT1.

C-SEGUE1.-

Excepto por el tomo piloto, C-SEGUE1 debe ser generado desde un tono por tono reverso de 180 grados en fase de C-REVERB1; la duración de C-SEGUE1 es de 10 periodos de símbolos repetitivos; Siguiendo a C-SEGUE1, el ATU-C entra a C-RATES1.

[54] Recomendación G.992.1, International Telecomunication Union, Pág. 95.

C-RATES1.-

Esta es la primera señal del ATU-C en llevar un prefijo cíclico; el propósito de este es la de transmitir cuatro opciones para tasas de datos y formatos al ATU-R, cada una de estas opciones consta de tres campos:

B_F.- Lista el número de bits en el buffer de datos rápido para cada canal ASx, LSx, LS0 (upstream), LS1 (upstream), y LS2 (upstream), debido a esto B_F tiene un total de 80 bits; los primeros 8 bits de B_F especifican el número de bytes en AS0, los segundos 8 de AS1, etc., cada bit se transmite desde el menos significativo.

B_I.- En igual forma lista el número de bytes en el buffer de datos intercalados; para poder soportar tasas de datos mayores a 8 Mbps, el campo B_I es de 8 bits.

{RS_F, RS_I, S, I, FS(LS2)}.- Es un grupo de diez bytes, de un byte por cada campo. El campo RS_F lleva el número de bytes de paridad por símbolo en el buffer rápido de downstream, $0 \leq RS_F \leq 63$. RS_I contiene el número de bytes de paridad por símbolo en el buffer de intercalado de downstream, $0 \leq RS_F \leq 63$. El campo S lleva el número de símbolos por palabra de código en downstream, $0 \leq S \leq 63$. El campo I contiene los bits menos significativos de la profundidad intercalado de downstream en código de palabras, $0 \leq I \leq 128$. El campo FS(LS2) es un campo con ocho ceros. Los restantes cinco campos son los mismos pero para upstream.

Las cuatro opciones son transmitidas en orden de preferencia decreciente; C-RATES1 es precedido por un prefijo de cuatro bytes (01010101 01010101 01010101 01010101).

	PREFIJO	OPCIÓN 1			OPCIÓN 2			OPCIÓN 3			OPCIÓN 4		
		B_F	B_I	RRSI	B_F	B_I	RRSI	B_F	B_I	RRSI	B_F	B_I	RRSI
Número de Bytes	4	10	10	10	10	10	10	10	10	10	10	10	10

Tabla 2.15. Resumen de C-RATES1

Solo un bit de información es transmitido por cada símbolo de C-RATES1, un bit “0” es codificado en un símbolo de C-REVERB1 y un bit “1” es codificado en un símbolo de C-SEGUE1; dado que existen un total de 992 bits de información de C-RATES1, la duración de C-RATES1 es de 992 símbolos; se transmite el bit menos significativo primero, empezando por el prefijo; a continuación de C-RATES viene C-CRC1.

C-CRC1.-

C-CRC1 es un chequeo de redundancia cíclica para la detección de errores en la recepción de C-RATES1 en el ATU-R, este campo es generado con los bits de C-RATES1, dando como resultado 16 bits que son transmitidos en 16 periodos de símbolo. Una vez transmitido C-CRC1 se procede a entrar al estado C-MSG1.

C-MSG1.-

Esta señal transmite un mensaje de 48 bits al ATU-R; este mensaje incluye la identificación del fabricante, niveles de potencia usados por el ATU-C, opciones del código de Trellis, opciones del cancelador de eco, etc.
El mensaje *m* esta definido de la siguiente manera:

$$m = \{m_{47}, m_{46}, ..., m_1, m_0\}$$

Formula 2.11. Definición del Mensaje de C-MSG1

Al momento de la transmisión se realiza por el menos significativo, se utilizan 48 periodos de símbolo para la transmisión de este mensaje.

M_I	PARÁMETROS
47-44	Margen mínimo requerido de SNR en la inicialización (0-15 dB)
43-18	Reservados para futuros usos (deben ser “0”)
17	Opción del Codificación de Trellis (“0” Sin, “1” Con código de Trellis)
16	Opción de sobre posicionamiento de espectro (“0” Sin, “1” Con cancelación de eco)
15	Sin uso (debe ser “1”)
14-12	Reservados para usos futuros (deben ser “0”)
11	NTR (“1” Indica que ATU-C usara los bits indicadores ib23-ib20)
10,9	Modo de trama
8-6	Densidad espectral de potencia transmitida durante la iniciación
5,4	Reservados (deben ser “0”)
3-0	Número de bits máximo por portadora soportada

Tabla 2.16. Descripción de los Bits de C-MSG1

M_8	M_7	M_6	DENSIDAD ESPECTRAL DE POTENCIA (DBM/HZ)
1	1	1	-40
1	1	0	-42
1	0	1	-44
1	0	0	-46
0	1	1	-48
0	1	0	-50
0	0	1	-52

Tabla 2.17. Descripción de los Bits m_8, m_7, m_6 del C-MSG1[55]

C-CRC2.-

Es una señal para realizar un chequeo cíclico de redundancia para la detección de errores en la recepción del C-MSG1 en el ATU-R, esta definido de la misma manera que C-CRC1, una vez concluido este estado pasamos a C-MEDLEY.

C-MEDLEY.-

C-MEDLEY es una señal pseudo aleatoria de ancho de banda usada para estimación en el ATU-R de la SNR de downstream; los datos transmitidos se derivan de la secuencia pseudo aleatoria usada en C-REVERB1, pero a diferencia de la usada anteriormente, esta usa un prefijo cíclico y la secuencia de datos continua desde un símbolo al siguiente, cabe destacar que no se reinician los datos del 1 al 9; ya que se tiene 512 bits por símbolo, el vector de portadora cambia de un periodo de símbolo a otro; C-MEDLEY se transmite para 16384 periodos de símbolo.

Una vez que se finaliza el C-MEDLEY se pasa al estado C-REVERB4.

2.2.3.6.5 Análisis del Canal ATU-R

Durante el proceso del análisis del canal existen dos situaciones en las cuales el ATU-R se resetea a si mismo, esto se produce cuando la señal R-SILENT0, que es desplegada en respuesta a un timeout y un error de recepción en los datos de control; los timeout pueden suscitarse cuando el tiempo del mensaje R-REVERB3 excede el limite de 4000 símbolos; y la manera en la que un error se produzca es cuando cualquier C-CRC indique fallas en los datos enviados.

[55] Recomendación G.992.1, International Telecomunication Union, Pág. 98

R-SEGUE1.-

Esta señal es generada de un tono por tono reverso con fase de 180 grados a partir de R-REVERB1; la duración de esta señal es de 10 símbolos periódicos. Una vez terminado este estado se prosigue con la señal R-REVERB3.

R-REVERB3.-

R-REVERB3 es similar a la señal R-REVERB1, con la diferencia de que R-REVERB3 es la primera señal del ATU-R con un prefijo cíclico para cada símbolo; la duración de la señal no esta definida, pero su máximo es de 4000 símbolos; si C-CRC2 no es detectada durante la duración de R-REVERB3, el ATU-R debe indicar timeout y proceder a resetearse mediante R-SILENT0. Después de la detección de C-RATES1 hasta C-CRC2, el equipo debe continuar enviando la señal R-REVERB3 durante 20 símbolos adicionales antes de pasar a R-SEGUE2.

R-SEGUE2.-

R-SEGUE2 es similar a R-SEGUE1, con la diferencia de que posee un prefijo cíclico; una vez que se ha terminado la duración de esta señal se pasa a entrar en el estado R-RATES1.

R-RATES1.-

Al igual que C-RATES1 su propósito es el mismo, pero para el canal de upstream, se puede apreciar las diferencias en la siguiente tabla de resumen:

	PREFIJO	OPCIÓN 1			OPCIÓN 2			OPCIÓN 3			OPCIÓN 4		
		B_F	B_I	RRSI	B_F	B_I	RRSI	B_F	B_I	RRSI	B_F	B_I	RRSI
Número de Bytes	4	3	3	5	3	3	5	3	3	5	3	3	5

Tabla 2.18. Resumen de R-RATES1

B_F.- Lista el número de bytes del buffer de datos rápido para LS0, LS1, LS2, en ese orden, posee un total de 24 bits; los primeros 8 bits especifican en número de bits para LS0, y así hasta LS2, en cada byte se transmite primero el bit menos significativo primero.

B_I.- En forma similar lista el número de bytes en buffer de intercalado.

{RS_F, RS_I, S, I, FS(LS2)}.- Es un grupo de cinco bytes; RS_F es el número de bits de paridad por símbolo en el buffer rápido en dirección upstream; RS_I es el número de bits de paridad por símbolo en el buffer de intercalado en dirección upstream; S es el número de símbolos por palabra de código en upstream; I es el número de profundidad de upstream en palabras de código para el buffer de intercalado; finalmente, FS(LS2) es un campo de 8 ceros.

Las cuatro opciones se transmiten en orden de preferencia decreciente; para este sistema ATU-C tiene el control de las tasas de datos, por lo que R-RATES1 es una copia de los parámetros necesarios de C-RATES1.

Tan solo un bit de datos de R-RATES1 por periodo de símbolo es transmitido; un bit "0" es codificado en un símbolo de R-REVERB1 y un "1" en un símbolo de R-SEGUE1; debido a que hay un total de 384 bits de información, la longitud de R-RATES1 es de 384 símbolos; el orden de transmisión es el mismo que el mostrado en la tabla anterior, con el bit menos significativo primero, de tal manera que el bit menos significativo de la opción 1 se transmite como el 33er símbolo luego del prefijo. Después de R-RATES1 le sigue R-CRC1.

R-CRC1.-

Es un chequeo de redundancia cíclica destinado para la detección de errores de recepción de R-RATES1 en el ATU-C, posee las mismás características de C-CRC1, y los 16 bits son transmitidos comenzando con c_0 en 16 periodos de símbolo usando el mismo método que R-RATES1; una vez terminada esta señal se procede con el estado R-MSG1.

R-MSG1.-

Esta señal transmite un mensaje de 48 bits al ATU-C, este mensaje lleva información sobre la identificación del fabricante, opciones de código de Trellis, opciones del cancelador de eco, etc.; este mensaje esta definido por:

$$m = \{m_{47}, m_{46}, ..., m_1, m_0\}$$

Formula 2.12. Definición del Mensaje de R-MSG1

Siendo m_0 el bit menos significativo, primero en ser transmitido; se tiene un total de 48 periodos de símbolos; una vez que se ha transmitido R-MSG1 se procede a enviar R-CRC2.

M_I	PARÁMETROS
47-18	Reservados para futuros usos (deben ser “0”)
17	Opción del Codificación de Trellis (“0” Sin, “1” Con código de Trellis)
16	Opción de sobre posicionamiento de espectro (“0” Sin, “1” Con cancelación de eco)
15	Sin uso (debe ser “1”)
14	Soporte de de tasas de bits altas (S=1/2)
13	Soporte de latencia dual de downstream
12	Soporte de latencia dual de upstream
11	NTR
10,9	Modo de trama
8-4	Reservados para futuros usos (deben ser “0”)
3-0	Número de bits máximo por portadora soportada

Tabla 2.19. Descripción de los Bits de R-MSG1

R-CRC2.-

Es un chequeo de redundancia cíclico para detección de errores en la recepción de R-MSG1 en el ATU-C, posee la misma estructura que las demás CRC, se transmiten 16 periodos de símbolo para los 16 bits de información, una vez que se termina esta señal se procede con R-MEDLEY.

R-MEDLEY.-

Es una señal pseudo aleatoria de banda ancha usada para la estimación de la SNR en upstream, en el ATU-C, los datos transmitidos se derivan de la secuencia pseudo aleatoria definida para R-REVERB1, pero a diferencia de esta R-MEDLEY posee un prefijo cíclico y la secuencia de datos continua desde un símbolo al siguiente, sin reiniciar los bits de datos del 0 al 6; debido a que la secuencia es de 63 bits y la señal de 64, el vector de portadora cambia de un periodo de símbolo al siguiente.

R-MEDLEY es transmitido en 16384 periodos de símbolos, siguiendo a esta señal encontramos a R-REVERB4.

R-REVERB4.-

Esta señal es la misma que R-REVERB3, la duración de la señal es de 128 símbolos; esta señal es el ultimo paso en el análisis del canal, inmediatamente después le sigue R-SEGUE3.

2.2.3.6.6 Intercambio ATU-C

Durante el intercambio, existen dos eventos los cuales causaran que el ATU-C se resetee mediante C-SILENT1, la primera es por timeout o por errores de detección provocados por los CRC; durante la parte interactiva se producirá un timeout cuando el tiempo en C-REVERB4 exceda los 6000 símbolos, o cuando C-REVERB-RA o C-REVERB5 excedan los 4000 símbolos.

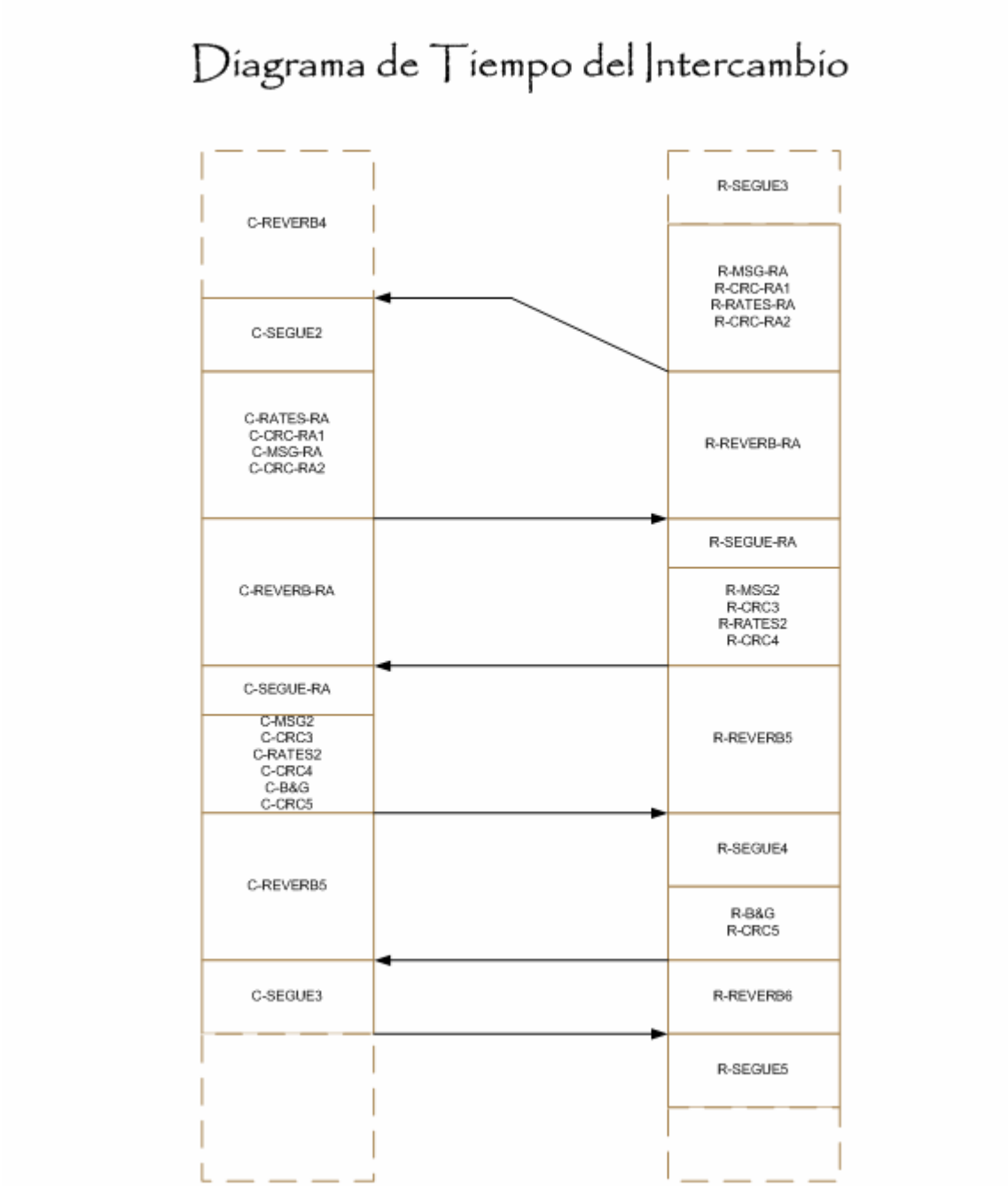


Figura 2.33. Diagrama de Tiempo del Intercambio[56]

C-REVERB4.-

Esta señal es parecida a C-REVERB2, a diferencia del prefijo cíclico en cada símbolo, y su duración máxima de 6000 símbolos, cabe destacar que una vez que empieza esta señal su permanencia en el proceso de intercambio continua aya que su duración no esta fijada.

[56] Recomendación G.992.1, International Telecomunication Union, Pág. 103.

Si el ATU-C no detecta R-CRC-RA2 dentro de los 6000 símbolos, deberá entrar en timeout y resetearse mediante C-SILENT1; después de la detección de R-SEGUE3 hasta R-CRC-RA2, el equipo deberá transmitir C-REVERB4 por 80 símbolos más antes de proseguir con C-SEGUE2.

C-SEGUE2.-

Esta señal es la misma que C-SEGUE1, la diferencia esta en el prefijo cíclico, su duración es de 10 periodos de símbolo, una vez concluido C-SEGUE2 procedemos con C-RATES-RA para empezar el segundo intercambio de tasas.

C-RATES-RA.-

C-RATES-RA es usada para enviar cuatro nuevas opciones para configuraciones de transporte, tanto para upstream como downstream; el contenido de C-RATES-RA no esta restringido por los mensajes previos.

Estas opciones en general serán más cercanas a las tasas de bits óptimas por canal que aquellas en C-RATES1, y deben estar basadas en la información de canal recibida mediante R-MSG-RA.

El formato de esta señal es el mismo que C-RATES1, con la excepción de que los cuatro bytes de prefijo no son transmitidos, y la señal es transmitida 8 símbolos por símbolo, como en C-MSG2; la duración de esta nueva señal es de 120 símbolos.

El campo {RS_F, RS_I, S, I, FS(LS2)} en esta ocasión deberá tener una sintaxis un poco más grande (en relación a C-RATES1), ya que es un conjunto de 10 bytes.

RS_F contiene el número de bits de paridad por símbolo en el buffer rápido de downstream; RS_I contiene los números de bits de paridad por símbolo en el buffer de intercalado de downstream, en los 5 bits menos significativos, en el bit 7 lleva el número de bytes de payload en el canal AS0 de downstream; S contiene el número de símbolos de downstream por código de palabra, en los 5 bits menos significativos, sin embargo los bits del 5 al 0 deben esta codificados con “0” para indicar S=1/2, finalmente los dos bits más significativos indican la profundidad de intercalado de downstream en palabras de código; I contiene los 8 bits menos significativos de la profundidad de intercalado de downstream

en palabras de código; finalmente el campo FS(LS2) lleva 8 bits con el valor de "0". Los mismos campos existen pero para upstream, un byte cada uno.

Estas cuatro opciones son transmitidas en orden decreciente de preferencia, se puede observar el resumen de esta señal en la siguiente tabla:

	PREFIJO	OPCIÓN 1			OPCIÓN 2			OPCIÓN 3			OPCIÓN 4		
		B_F	B_I	RRSI	B_F	B_I	RRSI	B_F	B_I	RRSI	B_F	B_I	RRSI
Número de Bytes	4	3	3	5	3	3	5	3	3	5	3	3	5

Tabla 2.20. Resumen de C-RATES-RA

	BITS							
Campo	7	6	5	4	3	2	1	0
RS_F	0	0	MSB		(Valores de RS_F)			LSB
RS_I	B_8	0	MSB		(Valores de RS_I)			LSB
S	I_9	I_8	MSB		(Valores de S)			LSB
I	I_7	I_6	I_5	I_4	I_3	I_2	I_1	I_0
FS(LS2)	{00000000}							

Tabla 2.21. Valores del Campo RRSI de C-RATES-RA[57]

C-CRC-RA1.-

Este es un chequeo de redundancia cíclica para la detección de errores provenientes de la recepción de C-RATES-RA en el ATU-R, su relación con C-RATES-RA es la misma que C-CRC3 con C-MSG2, sus 16 bits deben ser transmitidos en dos símbolos; una vez que C-CRC-RA1 se termina, se procede con la señal C-MSG-RA.

C-MSG-RA.-

Tiene el mismo formato mostrado en C-MSG1, la tabla mostrada a continuación es un resumen de los bits de este campo, los 48 bits son transmitidos en 6 símbolos.

M_I	PARÁMETROS
47-44	Nuevo margen mínimo de ruido requerido a la inicialización para downstream ATU-R
43-38	Margen mínimo de ruido requerido en steady state para downstream ATU-R (-32 a +31 dB)
37-32	Máximo margen de ruido requerido a la inicialización y en steady state para downstream ATU-R
31-0	Reservado para futuros usos (deben ser "0")

Tabla 2.22. Distribución de los Bits de C-MSG-RA

[57] Recomendación G.992.1, International Telecomunication Union, Pág. 105.

Le sigue a C-MSG-RA la señal C-CRC-RA2.

C-CRC-RA2.-

Es un chequeo de redundancia cíclico para detectar errores en la recepción de C-MSG-RA en el ATU-R, su relación con C-MSG-RA es el mismo que C-CRC3 con C-MSG2, sus 16 bits deben ser transmitidos en 2 símbolos; después de C-CRC-RA2, se pasa a la señal C-REVERB-RA.

C-REVERB-RA.-

Esta señal es la misma que C-REVERB4, sin embargo si el ATU-C no detecta la señal R-SEGUE-RA dentro de 4000 símbolos deberá entrar en timeout y resetearse mediante C-SILENT1; después de la detección de R-CRC4, el equipo debe continuar transmitiendo C-REVERB-RA durante al menos 80 símbolos más antes de cambiar al estado C-SEGUE-RA.

C-SEGUE-RA.-

Esta señal es la misma que C-SEGUE2, le sigue a esta la señal C-MSG2.

C-MSG2.-

Esta señal transmite un mensaje de 32 bits al ATU-R; este mensaje lleva información acerca del número total de bits por símbolo soportados, la estimación de la atenuación en lazo de upstream, y el margen de desempeño con la opción de tasa seleccionada; el mensaje esta definido por:

$$m = \{m_{31}, m_{30}, ..., m_1, m_0\}$$

Formula 2.13. Definición del Mensaje de C-MSG2

El bit m_0 es el primero en transmitirse, la asignación de los bits del mensaje se muestran en la siguiente tabla:

M_I	PARÁMETROS
31-26	Atenuación de lazo promedio estimada
25-21	Reservados para futuros usos (deben ser “0”)
20-16	Margen de desempeño con opción de tasa seleccionada
15-9	Reservados para futuros usos (deben ser “0”)
8-0	Número total de bits soportados

Tabla 2.23. Distribución de los Bits de C-MSG2

Un total de 4 periodos de símbolo son usados para comunicar los 32 bits del mensaje, con 8 bits transmitidos en cada símbolo; dos bits son codificados en portadoras con números $n_{1C\text{-}MSG2}$ hasta $n_{1C\text{-}MSG2+3}$ usando una constelación definida previamente, los bits menos significativos son transmitidos en el primer símbolo de C-MSG2.

C-CRC3.-

Es un chequeo de redundancia cíclico para la detección de errores en la recepción de C-MSG2 en el ATU-R; posee las mismas definiciones que C-CRC1, y sus 16 bits deben ser transmitidos en 2 periodos de símbolos; Una vez que se termina la señal C-CRC3 se pasa a C-RATES2.

C-RATES2.-

Esta es la respuesta a R-RATES-RA, combina la opción seleccionada de downstream con la se upstream, transmite la decisión final de las tasas que serán usadas en ambas direcciones.

El ATU-C no debe cambiar la opción de downstream de aquella seleccionada en R-RATES2.

La longitud de C-RATES2 es de 8 bits, y en caso de que ninguna de las opciones requeridas durante C-RATES1 o C-RATES-RA pueden ser implementadas, el ATU-C regresa a C-SILENT1 para realizar un re entrenamiento; un periodo de símbolo es usado para transmitir 8 bits; después de esta señal empieza C-CRC4.

DOWNSTREAM/UPSTREAM	PATRÓN DE BITS (MSB PRIMERO)
Opción 1/Opción 1	00010001
Opción 1/Opción 2	00010010
Opción 1/Opción 3	00010100
Opción 1/Opción 4	00011000
Opción 2/Opción 1	00100001
Opción 2/Opción 2	00100010
Opción 2/Opción 3	00100100
Opción 2/Opción 4	00101000
Opción 3/Opción 1	01000001
Opción 3/Opción 2	01000010
Opción 3/Opción 3	01000100
Opción 3/Opción 4	01001000
Opción 4/Opción 1	10000001
Opción 4/Opción 2	10000010
Opción 4/Opción 3	10000100
Opción 4/Opción 4	10001000
Todas Fallan	00000000

Tabla 2.24. Patrón de los Bits de C-RATES2[58]

C-CRC4.-

Es un chequeo de redundancia cíclico para detectar errores en la recepción de C-RATES2 en el ATU-R, esta relación es la misma que la que posee C-CRC3 con C-MSG2; los 16 bits deben ser transmitidos en 2 símbolos; después de esta señal entramos a C-B&G.

C-B&G.-

C-B&G debe ser usado para la transmisión al ATU-R de los bits de ganancia e información g_i y b_i respectivamente, que van a ser usados en las portadoras de upstream, el factor de ganancia es parecido al usado por la portadora durante las transmisiones de R-MEDLEY.

Tal como se ha especificado en anteriores ocasiones, las componentes de DC y portadoras de Nyquist llevan los valores de cero, esto se transmite a los bits b_0, g_0, b_{32}, g_{32} que llevan el valor de cero.

Cada valor b_i debe ser representado como un entero sin signo de 4 bits, los valores que puede tomar van de cero hasta el máximo número de bits que el ATU-R puede modular en cada portadora, este valor consta en R-MSG1.

[58] Recomendación G.992.1, International Telecomunication Union, Pág. 108.

Cada valor de g_i debe ser representado con una cantidad de punto fijo sin signo de 12 bits, este valor debe instruir a su correspondiente b_i que incremente el poder un poco más que el transmitido durante R-MEDLEY.

En las portadoras que no transmiten datos los valores de b_i y g_i deben ser cero, pero si una portadora no transmite datos, pero puede realizar esta acción más adelante, los valores de b_i deben ser cero, pero g_i debe tener valores entre 0.19 y 1.33 (000.001100000 hasta 001.010101011).

La información de C-B&G debe ser mapeada en un mensaje de 496 bits o 62 bytes definido por:

$$m = \{m_{496}, m_{495}, ..., m_1, m_0\} = \{g_{31}, b_{31}, ..., g_1, b_1\}$$

Formula 2.14.- Definición del Mensaje de C-B&G

Los bits más significativos están en los valores de m más altos, pero su transmisión comienza con m_0; el mensaje debe ser transmitido en 62 símbolos.

Una vez que se termina la señal C-B&G pasamos a C-CRC5.

C-CRC5.-

Es un chequeo de redundancia cíclico de detección de errores en la recepción de C-B&G en el ATU-R, tiene la misma relación con esta señal que C-CRC3 con C-MSG2; sus 16 bits deben ser transmitidos en 2 símbolos; después de esta señal se procede con C-REVERB5.

C-REVERB5.-

Esta señal es la misma que C-REVERB4, la diferencia estriba en el tiempo de duración de 4000 símbolos; la duración de C-REVERB5 depende del estado de ATU-R y la capacidad de procesamiento del ATU-C; se debe transmitir el C-REVERB5 hasta que ha recibido el chequeo, un establecimiento del transmisor ATU-C, y los bits y ganancias de downstream en R-B&G.

Si los bits, ganancias, el chequeo y su establecimiento no se han suscitado dentro de los 4000 símbolos el equipo debe entrar en timeout y resetearse mediante C-SILENT1; se debe pasar al estado C-SEGUE3 tan pronto como este preparado según las condiciones especificadas en R-B&G.

C-SEGUE3.-

Esta señal es usada para notificar al ATU-R que el ATU-C esta apunto de entrar al estado de señal de steady state C-SHOWTIME; la señal C-SEGUE3 es la misma que C-SEGUE2, su duración es de 10 periodos de símbolos; una terminado este estado el ATU-C ha terminado su iniciación y debe entrar el estado C-SHOWTIME.

2.2.3.6.7 Intercambio ATU-R

Durante el intercambio, existen dos posibilidades en las cuales el ATU-R debe resetearse a si mismo, estos son timeouts y errores de detección producidos por los CRC, ambas activan la señal R-SILENT0; este intercambio es parte sincronización entre equipos y parte interacción; durante la parte interacción un timeout debe ocurrir cuando el tiempo en ciertos estados excede los 4000 símbolos.

R-SEGUE3.-

La señal R-SEGUE3 es la misma que R-SEGUE2; la duración de la señal es de 10 periodos de símbolo; después de esta señal se pasa a R-MSG-RA para empezar la segunda tasa de intercambios.

R-MSG-RA.-

Esta señal comparte las mismas características que R-MSG2, con la diferencia de que esta señal posee 80 bits.

M_I	PARÁMETROS
79-56	Reservados para futuros usos (debe ser “0”)
55-49	Número de byte de encabezado RS (R)
48-40	Número de bytes de payload RS (K)
39-32	Número de tonos portadores de datos (ncloaded)
31-25	Atenuación de lazo promedio estimada
24-21	Ganancia de código (0-7.5 dB)
20-16	Margen de desempeño con opción de tasa seleccionada
15-14	Reservados para futuros usos (deben ser “0”)
13-12	Profundidad de Intercalado máxima
11-0	Número total de bits por símbolo DMT

Tabla 2.25. Distribución de los Bits R-MSG-RA

BIT 13	BIT 12	D_{MAX}
0	0	64 (Obligatoria)
0	1	128 (Opcional)
1	0	256 (Opcional)
1	1	512 (Opcional)

Tabla 2.26. Valores del Campo Profundidad de Intercalado Máxima R-MSG-RA[59]

R-CRC-RA1.-

Es un chequeo de redundancia cíclico para la detección de errores en la recepción de R-MSG-RA; la relación de esta señal es la misma entre R-CRC3 con R-MSG2; después de esta señal el equipo pasa a R-RATES-RA.

R-RATES-RA.-

R-RATES-RA es la respuesta a C-RATES1 basada en los resultados del análisis del canal de downstream y muestra similaridades con la señal R-RATES2; en vez de listar B_F y B_I, el equipo realiza una de las siguientes acciones:

- Envía de regreso solo el número de opción de la tasa de datos más alta que puede ser soportada, basada en la medición de SNR del canal de downstream.
- Indica que no se realizaron selecciones de opción, pero se harán luego, basados en la información de C-RATES-RA.
- Indica que ninguna de las opciones pedidas durante C-RATES1 pueden ser implementadas.

Como en R-RATES2, 4 bits son usados para el número de opción; un total de 8 bits son usados en R-RATES-RA; u periodo de símbolo es usado para la transmisión de 8 bits; una vez terminada esta señal se procede a R-CRC-RA2.

El formato de R-RATES-RA es el mismo que R-RATES2, con la excepción de la patente de bit usada para indicar “No selección de opción”.

[59] Recomendación G.992.1, International Telecomunication Union, Pág. 111.

DOWNSTREAM	PATENTE DE BIT R-RATES-RA (MSB PRIMERO)
Opción 1	00010001
Opción 2	00100010
Opción 3	01000100
Opción 4	10001000
“No Selección de Opción”	00000001
“Todas la Opciones Fallaron”	00000000

Tabla 2.27. Patente de Bits R-RATES-RA

R-CRC-RA2.-

Es un chequeo de redundancia cíclico para detección de errores en la recepción de R-RATES-RA; su relación con esta señal es la misma que posee R-CRC3 con R-MSG2; una vez que pasa esta señal se procede con R-REVERB-RA.

R-REVERB-RA.-

Es la misma señal que R-REVERB3; la duración de esta señal depende del estado de las señales en el ATU-C y el capacidad de proceso del ATU-R, sin embargo tiene una duración de 4000 símbolos; el ATU-R debe transmitir R-REVERB-RA hasta haber recibo y revisado la fiabilidad de los bits y ganancia de upstream que contiene C-RATES-RA; después de haber recibido C-CRC-RA2, debe continuar transmitiendo R-REVERB-RA durante otros 64 símbolos, después pasar a R-SEGUE-RA.

Si no se ha producido una detección exitosa de las señales de control dentro de los 4000 símbolos, el ATU-R debe entrar en timeout y resetearse mediante R-SILENT0.

R-SEGUE-RA.-

Esta señal es la misma que R-SEGUE4; una vez pasada esta señal sigue R-MSG2.

R-MSG2.-

R-MSG2 transmite señal de mensaje de 32 bits al ATU-C; este mensaje incluye el número total de bits por símbolos soportados, la atenuación estimada de laso de downstream y el margen de desempeño con la selección de tasa de opción; el mensaje esta definido por:

$$m = \{m_{31}, m_{30}, ..., m_1, m_0\}$$

Formula 2.15. Definición del Mensaje de R-MSG2

El bit m_0 es el primero en ser transmitido; el resto de los componentes del mensaje están descritos en la siguiente tabla:

M_I	PARÁMETROS
31-25	Atenuación de lazo promedio estimada
24-21	Reservados para futuros usos (deben ser “0”)
20-16	Margen de desempeño con opción de tasa selecciona
15-12	Reservados para futuros usos (Deben ser “0”)
11-0	Número total de bits soportados

Tabla 2.28. Distribución de los Bits R-MSG2

Un total de 4 periodos de símbolos son usados para comunicar los 32 bits del mensaje, con 8 bits transmitidos por cada símbolo; dos bits son codificados en el número de una portadora desde $n_{1R\text{-}MSG2}$ hasta $n_{1R\text{-}MSG2+3}$ usando una constelación 4QAM; los mismo dos bits son codificados en al misma manera en un grupo de portadoras de respaldo, desde $n_{2R\text{-}MSG2}$ hasta $n_{2R\text{-}MSG2+3}$.

Los bits menos significativos del mensaje son transmitidos en el primer símbolo de R-MSG2, con los dos bits menos significativos de cada byte codificado en las portadoras $n_{1R\text{-}MSG2}$ y $n_{2R\text{-}MSG2}$.

Una vez que se pasa la señal R-MSG2, le sigue R-CRC3.

R-CRC3.-

Es un chequeo de redundancia cíclico para la detección de errores en la recepción de R-MSG2 en el ATU-C; los bits son transmitidos en 2 periodos de símbolo, una vez que termina la señal R-CRC3 le sigue R-RATES2.

R-RATES2.-

Esta es la respuesta a C-RAYES-RA basada en los resultados del análisis de canal de downstream; en vez de listar B_F y B_I como C-RATES1, el equipo envía de regreso solo un número de opción de tasa de datos seleccionado que puede soportar, basado en mediciones del SNR del canal de downstream.

Como en C-RATES2, 4 bits son usados para la opción de número; un total de 8 bits son usados para R-RATES2.

Si ninguna de las opciones requeridas durante C-RATES1 puede ser implementada, el ATU-R envía el mensaje R-SILENT0 para un re entrenamiento; un periodo de símbolo es usado para la transmisión de 8 bits; después de la transmisión de esta señal, le sigue R-CRC4.

DOWNSTREAM	PATENTE DE BIT R-RATES-RA (MSB PRIMERO)
Opción 1	00010001
Opción 2	00100010
Opción 3	01000100
Opción 4	10001000
“Todas la Opciones Fallaron”	00000000

Tabla 2.29.- Patente de Bits R-RATES2[60]

R-CRC4.-

Es un chequeo de redundancia cíclico para la detección de errores en la recepción de R-RATES2 en el ATU-C; su relación con R-RATES2 es similar a la que tiene R-CRC3 con R-MSG2; le sigue la señal R-REVERB5.

R-REVERB5.-

Es la misma señal de R-REVERB3; la duración de esta señal depende del estado de las señales en el ATU-C y la capacidad de proceso del ATU-R, pero posee un máximo de tiempo de 4000 símbolos; el ATU-R debe transmitir R-REVERB5 hasta que haya recibido y revisado la fiabilidad de los bits y ganancias de upstream contenidas en C-B&G; después de que el equipo haya recibido C-CRC5, debe continuar transmitiendo la señal R-REVERB5 durante otros 64 símbolos, y después debe entrar a R-SEGUE4.

En caso de que no logre una detección de las señales de control dentro de los 4000 símbolos, debe entrar en timeout y resetearse mediante R-SILENT0.

R-SEGUE4.-

El propósito de esta señal es la de notificar al ATU-C que el ATU-R esta apunto de entrar en R-B&G; R-SEGUE4 es la misma que R-SEGUE3; la duración de esta señal es de 10 periodos de símbolos.

[60] Recomendación G.992.1, International Telecomunication Union, Pág. 112.

R-B&G.-

R-B&G debe ser usado para la transmisión al ATU-C de los bits de ganancia e información g_i y b_i respectivamente, que van a ser usados en las portadoras de downstream, el factor de ganancia es parecido al usado por la portadora durante las transmisiones de C-MEDLEY.

Tal como se ha especificado en anteriores ocasiones, las componentes de DC y portadoras de Nyquist llevan los valores de cero, esto se transmite a los bits b_0, g_0, b_{256}, g_{256} que llevan el valor de cero.

Cada valor b_i debe ser representado como un entero sin signo de 4 bits, los valores que puede tomar van de cero hasta el máximo número de bits que el ATU-R puede modular en cada portadora, este valor consta en C-MSG1.

Cada valor de g_i debe ser representado con una cantidad de punto fijo sin signo de 12 bits, este valor debe instruir a su correspondiente b_i que incremente el poder un poco más que el transmitido durante R-MEDLEY.

En las portadoras que no transmiten datos los valores de b_i y g_i deben ser cero, pero si una portadora no transmite datos, pero puede realizar esta acción más adelante, los valores de b_i deben ser cero, pero g_i debe tener valores entre 0.19 y 1.33 (000.001100000 hasta 001.010101011).

La información de R-B&G debe ser mapeada en un mensaje de 4080 bits o 510 bytes definidos por:

$$m = \{m_{4079}, m_{4078}, ..., m_1, m_0\} = \{g_{255}, b_{255}, ..., g_1, b_1\}$$

Formula 2.16. Definición del Mensaje de R-B&G

Los bits más significativos están en los valores de m más altos, pero su transmisión comienza con m_0; el mensaje debe ser transmitido en 510 símbolos. Una vez que se termina la señal R-B&G pasamos a R-CRC5.

R-CRC5.-

Es un chequeo de redundancia cíclico para la detección de errores en la recepción de R-B&G en el ATU-C; su relación con R-B&G es similar a la que tiene R-CRC3 con R-MSG2; le sigue la señal R-REVERB6.

R-REVERB6.-

Es la misma señal de R-REVERB3; la duración de esta señal depende del estado de las señales en el ATU-C y la capacidad de proceso del ATU-R, pero posee un máximo de tiempo de 4000 símbolos; el ATU-R debe transmitir R-REVERB6 hasta que haya recibido todos los 10 símbolos C-SEGUE3; después debe pasar a R-SEGUE5; si no ha podido detectar C-SEGUE3 dentro de los 4000 símbolos, debe entrar en timeout y resetearse mediante R-SILENT0.

R-SEGUE5.-

El propósito de esta señal es la de notificar al ATU-C que el ATU-R esta apunto de entrar al estado de señalización steady state R-SHOWTIME; R-SEGUE5 es la misma que R-SEGUE3; la duración de esta señal es de 10 periodos de símbolos.

Una vez que a pasado esta señal el ATU-R ha terminado su inicialización y debe pasar al estado R-SHOWTIME.

2.2.3.6.8 Detalles de la Sincronización Durante la Iniciación

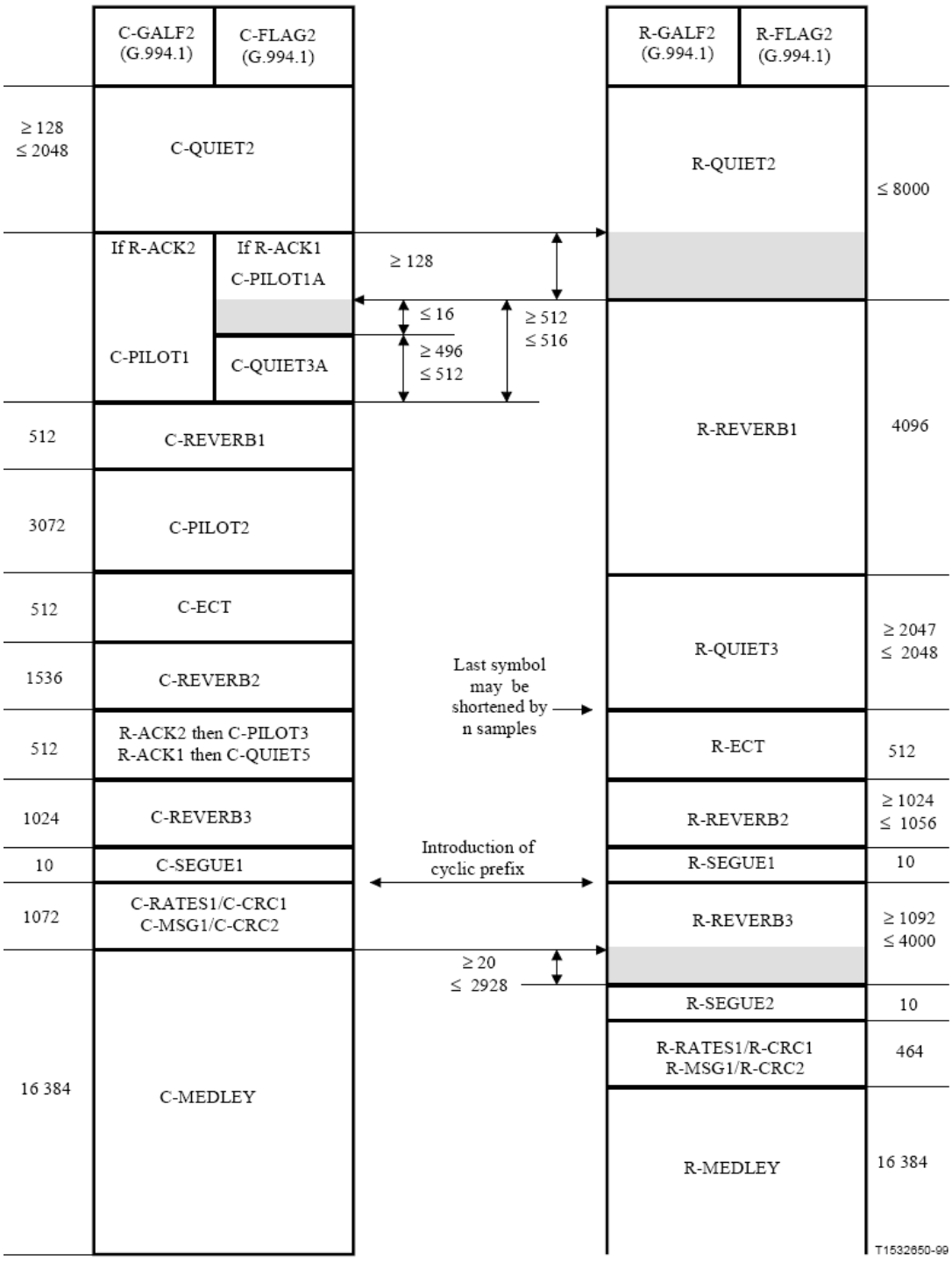


Figura 2.34. Diagrama de Tiempos de Iniciación (Parte I)[61]

[61] Recomendación G.992.1, International Telecomunication Union, Pág. 117.

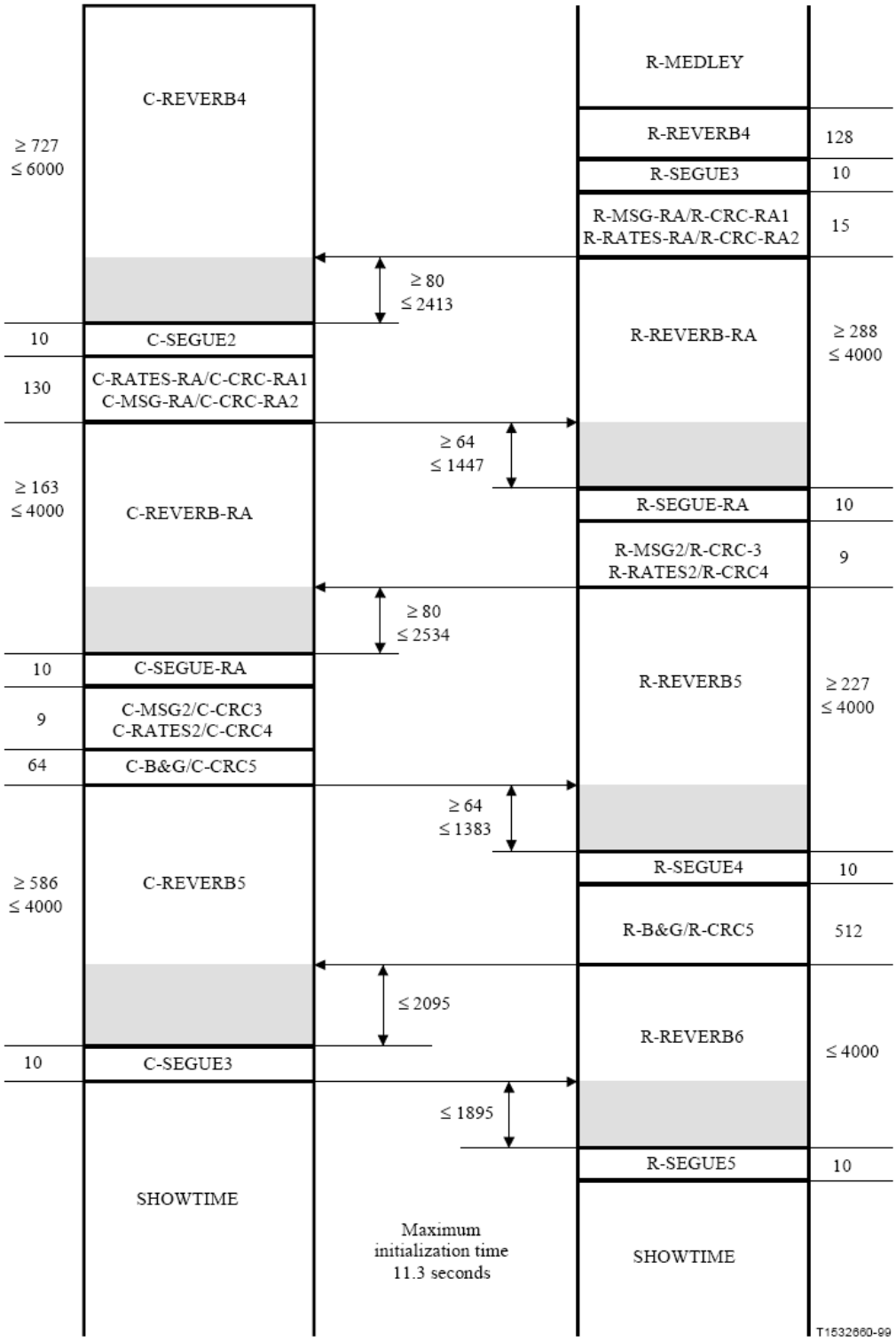


Figura 2.35. Diagrama de Tiempos de Iniciación (Parte II)[62]

[62] Recomendación G.992.1, International Telecomunication Union, Pág. 118.

2.2.3.7 Adaptación en Línea y Reconfiguración del AOC

2.2.3.7.1 EL Canal de Control de Encabezado ADSL (AOC)

Los datos del AOC son llevados como bytes del encabezado en la estructura de la trama; la multiplexión de estos bytes en la trama dependen de la estructura de la trama usada y la los canales de datos y su ubicación en los buffers rápido y de intercalado.

2.2.3.7.1.1 Encabezado de Mensaje AOC

El tipo y longitud de un mensaje AOC esta definido por un encabezado de byte de longitud. El canal AOC envía una patente de bits, todos ceros como iniciación y un mensaje valido siempre comienza con un byte no cero.

ENCABEZADO	LONGITUD DEL MENSAJE (BYTES)	INTERPRETACIÓN
00001111	Indefinido	Mensaje de Reconfiguración
1100xxxx	Indefinido	Mensaje Especifico del Fabricante
11110000	1	Mensaje de Incapaz de Realizar (Byte de Encabezado)
11111100	13	Mensaje de Petición de Intercambio de Bit Extendido
11111111	9	Mensaje de Petición de Intercambio de Bit
11111111	3	Mensaje de Reconocimiento de Intercambio de Bit

Tabla 2.30. Encabezados del Mensaje AOC

Los valores de los bytes del encabezado están dados en forma binaria, los MSB a la izquierda, y representados por aoc7 al aoc0, los cuales son llevados en el encabezado; todos los demás bytes del mensaje de AOC deben ser mapeados de acuerdo a esta misma convención.

2.2.3.7.1.2 Protocolo AOC

Todos los mensajes AOC deben ser transmitidos cinco veces consecutivas para seguridad; al menos 20 patentes de AOC deben ser insertadas entre dos grupos consecutivos de cinco mensajes iguales.

Un equipo que reciba un mensaje AOC debe tomar acciones solo si ha recibido tres mensajes idénticos en un periodo de tiempo de cinco veces ese mensaje en particular; cuando un equipo recibe un mensaje que no reconoce no debe realizar ninguna acción.

2.2.3.7.2 Adaptación en Línea Intercambio de Bit

El intercambio de bit le permite a un sistema ADSL cambiar el número de bits asignados a una portadora, o cambiar la energía de transmisión de una subportadora sin interrumpir el flujo de datos.

Ambos equipos pueden empezar el intercambio de bit; el proceso de intercambio en los canales de upstream y downstream son independientes y toman lugar en forma simultánea.

En el protocolo de intercambio de bit el receptor es el ATU-x que esta recibiendo los datos, el transmite un mensaje de petición de intercambio de bit y recibe un mensaje de confirmación de intercambio de bit; el transmisor es el que transmite los datos, recibe el mensaje de petición de intercambio de bit y transmite el mensaje de confirmación de intercambio de bit.

Debe existir un máximo de una confirmación de petición de intercambio de bit de downstream en cualquier momento; y debe haber un máximo de una confirmación de intercambio de bit de upstream en cualquier momento.

2.2.3.7.2.1 Canal de Intercambio de Bit

El proceso de intercambio de bit usa el canal AOC, todos los mensajes deben repetirse cinco veces consecutivas en este canal.

2.2.3.7.2.2 Conteo de Supertrama

Los transceptores coordinan el intercambio de bits de la siguiente manera:

- ✓ Los transmisores ATU-C y ATU-R deben hincar sus contadores inmediatamente después de transmitir C-SEGUE3 y R-SEGUE5 respectivamente, estos marcan el paso de la iniciación la operación de steady state.
- ✓ El conteo de supertrama empieza con la primera supertrama al inicio del Showtime siendo al supertrama 0.
- ✓ Cada trasmisor debe incrementar su contador después de enviar cada supertrama ADSL.
- ✓ Correspondientemente cada receptor debe iniciar su contador inmediatamente después de haber recibido C-SEGUE3 o R-SEGUE5 respectivamente, e ir incrementándolo después de recibir cada supertrama.

- ✓ El conteo de supertrama es realizado hasta 256.

La sincronización de los contadores de las supertramas de los transmisores y receptores es mantenida usando en símbolo de sincronización de la estructura de la trama ADSL; cualquier forma de reinicio que requiera una transición desde la inicialización hasta el steady state debe reiniciar el conteo de supertramas.

2.2.3.7.2.3 Petición de Intercambio de Bit

El receptor debe iniciar un intercambio de bit enviando un pedido de intercambio de bit al transmisor mediante el canal de AOC, este pedido le indica al transmisor cual subportadora debe ser modificada.

El formato del pedido se muestra en la siguiente tabla:

ENCABEZADO DEL MENSAJE	CAMPOS 1-4 DEL MENSAJE	
11111111 (8 bits)	Comandos (8 bits)	Índice de Sub Canal (8 bits)

Tabla 2.31. Formato del Mensaje de Petición de Intercambio de Bit

El encabezado del mensaje debe ser de ocho “1’s” binarios; el campo 1-4 del mensaje consiste de un comando de ocho bits seguido por un índice de sub canal de ocho bits; el índice de sub canal se cuenta desde las frecuencia más bajas a las altas, con la frecuencia más baja de portadora como el número cero, la subportadora cero no se usa.

VALOR	INTERPRETACIÓN
00000000	Sin Acción
00000001	Incrementar el Número de bits correspondientes en uno
00000010	Decrementar el Número de bits correspondientes en uno
00000011	Incrementar la potencia de transmisión en 1 dB
00000100	Incrementar la potencia de transmisión en 2 dB
00000101	Incrementar la potencia de transmisión en 3 dB
00000110	Reducir la potencia de transmisión en 1 dB
00000111	Reducir la potencia de transmisión en 2 dB
00001xxx	Reservado para comandos a discreción del fabricante

Tabla 2.32. Comandos de la Petición de Intercambio de Bit[63]

El mensaje de petición de intercambio de bit debe ser transmitido cinco veces consecutivas; ara evitar la divergencia de g_i entre los equipos después de varios

[63] Recomendación G.992.1, International Telecomunication Union, Pág. 121.

intercambios de bit, para una actualización de g_i de Δ dB, el nuevo valor de g_i esta definido mediante la siguiente formula:

$$g_i' = (1/512) \times round(512 \times g_i \times 10\exp(\Delta/20))$$

Formula 2.17. Cálculo de g_i Después de Varios Intercambios de Bit[64]

2.2.3.7.2.4 Pedido de Intercambio de Bit Extendido

Cualquier adaptación en línea puede ser codificada en una petición de intercambio de bit extendida; sin embargo debido a que una portadora con un solo bit no es permitida, una petición de intercambio de bit extendida que contiene seis campos debe ser usada cuando se decremente el número de bits de una portadora de 2 a 0, o cuando se incrementen los números de bits de 0 a 2.

El formato de esta petición es similar al formato de la petición de intercambio de bit, pero el número de mensajes de campo se incrementa a seis, y un encabezado de mensaje diferente es usado.

ENCABEZADO DEL MENSAJE	CAMPOS 1-6 DEL MENSAJE	
11111100 (8 bits)	Comandos (8 bits)	Índice de Sub Canal (8 bits)

Tabla 2.33. Formato del Mensaje de Petición de Intercambio de Bit Extendido

El receptor debe iniciar un intercambio de bit extendido enviando un mensaje de intercambio de bit extendido al transmisor; este pedido le indica al transmisor cual portadora debe ser modificada.

El receptor debe usar dos campos de mensaje idénticos para pedir un incremento o decremento de 0 a 2 o de 2 a 0 bits respectivamente en una portadora; esta petición debe ser transmitida cinco veces consecutivas.

2.2.3.7.2.5 Confirmación de Intercambio de Bit

Dentro de 400 ms. Después de haber recibido el mensaje de petición de intercambio de bit, el transmisor debe enviar un mensaje de confirmación de intercambio de bit, el cual contiene lo siguiente:

Un encabezado del mensaje de confirmación de intercambio de bit “11111111”

[64] Recomendación G.992.1, International Telecomunication Union, Pág. 121.

Un campo de mensaje, el cual consiste de un comando de confirmación de ocho bits, seguido por un número de contador de supertrama de ocho bits; el comando de confirmación debe estar codificado por “11111111”, mientras que el número de contador indica donde el intercambio de bit se realiza. Este número de contador debe ser al menos 47 mayor que el número de contador cuando el pedido fue recibido.

Esta confirmación debe ser transmitida cinco veces consecutivas.

ENCABEZADO DEL MENSAJE	COMANDO DE CONFIRMACIÓN	NÚMERO DE CONTADOR DE SUPERTRAMA
11111111 (8 bits)	11111111 (8 bits)	(8 bits)

Tabla 2.34. Formato de Confirmación de Intercambio de Bit

2.2.3.7.2.6 Receptor - Intercambio de Bit

El receptor debe iniciar un timeout de 500 ± 20 ms. desde el momento que envía un mensaje de petición de intercambio de bit. Cuando ninguna confirmación ha sido recibida en este intervalo de timeout, el receptor debe reenviar dicho mensaje y reiniciar el timeout.

Solo cuando una confirmación ha sido recibida dentro de este intervalo de timeout debe el receptor prepararse para un intercambio de bit en el tiempo especificado en el mensaje de confirmación.

Sin embargo después de un número de reenvios, el receptor debe tomar acciones de recuperación para asegurar el intercambio de bit, dichas acciones están a discreción de cada fabricante.

El receptor debe esperar hasta que el contador de supertrama sea igual al valor especificado en el mensaje de confirmación; entonces, desde la trama 0 del la siguiente supertrama ADSL el receptor debe:

- ✓ Cambiar la asignación de bit de la portadora correspondiente y realizar un reordenamiento de tonos basados en la nueva asignación de bit de la portadora.
- ✓ Actualizar los parámetros de recepción aplicables a la portadora correspondiente, para contabilizar un cambio en la energía de transmisión.

2.2.3.7.2.7 Transmisor – Intercambio de Bit

Después de la transmisión de la confirmación de bit, el transmisor debe esperar hasta que el contador de supertrama sea igual al valor especificado en la confirmación de intercambio de bit; entonces comenzando con la trama 0 de la siguiente supertrama ADSL, el transmisor debe:

- ✓ Cambiar la asignación de bit de la portadora correspondiente, y realizar un reordenamiento de tonos basados en la nueva asignación de bit de portadora.
- ✓ Cambiar la energía de transmisión en la portadora correspondiente por el factor deseado.

Si el transmisor recibe un nuevo mensaje de petición de intercambio de bit durante la espera, debe inmediatamente detener la espera y actualizar el contador de supertrama para el intercambio de bit acordado en el nuevo mensaje; el transmisor debe reiniciar el proceso para el nuevo mensaje de petición de intercambio de bit, asumiendo que el nuevo mensaje es igual al previo.

2.2.4 Otras Tecnologías xDSL

Una vez que se ha revisado más de cerca la tecnología ADSL, revisaremos de forma muy breve algunas de las otras familias de xDSL existentes.

Cabe mencionar que las diferencias entre una y otra tecnología son mayormente las velocidades que ofrece, sin embargo en algunos casos se vera que existen diferencias más grandes.

2.2.4.1 Splitterless Asymmetric Digital Subscriber Line

Es una variación de la tecnología ADSL, se le conoce bajo el nombre de g.lite y su mayor diferencia es la falta de un splitter para la separación de los servicios POTS y la transmisión de datos.

Mediante esta tecnología se puede usar al mismo tiempo los servicios de voz y la transmisión de datos bajo un mismo par de cobre; posee las mismas características que las

revisadas en ADSL, pero en este caso las tasas de datos son diferentes, con 1.536 Mbps para downstream y 512 Kbps para upstream.

En esta ocasión el sistema g.lite corre sobre dos canales simplex, el uno para downstream y el otro para upstream, cabe destacar que al igual que ADSL, se puede usar para la transmisión de voz y servicios ISDN al mismo tiempo con completa compatibilidad.

Esta rama de la tecnología xDSL soporta solamente transmisión de datos ATM, esto por supuesto no afecta el desempeño ni la confiabilidad; el uso del fast retraining es obligatorio, debido a la falta de splitter, ya que se producen variaciones en el local loop que pueden causar perdidas de comunicación; finalmente el uso de la estructura de trama se ve limitada a la 3, esto se realiza cuando el ATU-R especifica el uso de esta estructura de trama con el uso del buffer de datos intercalados.

2.2.4.2 High Bit Rate Digital Subscriber Line

Mejor conocido como HDSL, esta tecnología corre sobre dos pares de cobre y aplica la misma técnica de cancelación de eco usada por los sistemas ADSL, desafortunadamente HDSL no permite el uso de forma simultánea de servicios POTS y datos.

Una de las desventajas de este sistema es el uso de no un par sino dos, para la transmisión de datos, debido a esto la presente tecnología no ha tenido la acogida que otras ramas xDSL tal como SDSL.

Existen tres formas de llevar a cabo la implementación HDSL:

- ✓ Usando 2 o 3 pares de cobre el paralelo, con tasas de transmisión de 784 Kbps cada uno.
- ✓ Usando tasas de bit incrementadas a 1,168 Mbps sobre 2 pares de cobre en paralelo.
- ✓ Usando un solo par con tasas de bit aun más incrementadas hasta los 2.320 Mbps.

El código de línea usado para estas implementaciones puede ser 2B1Q o CAP, sin embargo solo una de estas se puede usar al a vez, por lo general para tasas de bit de 2.048 Mbps se usa 2B1Q, mientras que para 1,544 Mbps sobre dos pares se usa CAP.

2.2.4.3 Single Pair High Speed Digital Subscriber Line

Se le conoce por sus siglas en ingles SHDSL, esta rama de la tecnología xDSL esta diseñada para operaciones duplex en un solo para de cobre, sin embargo soporta transmisiones sobre dos pares de cobre juntos de diferentes características.

Las tasas de transmisión a las cuales los transceptores pueden operar van desde los 192 Kbps hasta los 2.312 Mbps con pasos de 8 Kbps a la vez; estos equipos a su vez son espectralmente compatibles con las demás gamas de equipos xDSL, lo cual le asegura su compatibilidad en el mercado.

Sin embargo no es capaz de soportar el uso de splitters para poder permitir la coexistencia de servicios de voz o ISDN.

2.2.4.4 Very High Data Rate Digital Subscriber Line

Esta es la tecnología xDSL que permite las tasas de transferencia más altas, en si misma establece nuevos adelantos con respecto al resto de las tecnologías xDSL, pero a un costo que para algunos usuarios la vuelve poco practica, las distancias a las cuales funciona.

Las tasas de transferencia máximas están alrededor de los 52 Mbps, y puede funcionar tanto en modos simétricos de transferencia de datos como asimétricos; las distancia de funcionamiento de VDSL son mucho más cortas de los 6 Km. que establece ADSL, para poder apreciar de mejor manera esta reducción de longitud se presentara una tabla con las distancia promedio para los servicios xDSL.

XDSL	SIMÉTRICO/ ASIMÉTRICO	DISTANCIA DEL LOCAL LOOP (KM.)	DOWNSTREAM (MBPS)	UPSTREAM (MBPS)
SDSL	S	3	1,544	1.544
HDSL	S	4	1,544	1,544
ADSL	A	6	6	0.640
ADSL g.lite	A	6	1.5	0.512
VDSL	A	1	26	3
VDSL	A	0.3	52	6
VDSL	S	1	13	13
VDSL	S	0.3	26	26

Tabla 2.35. Distancias y Velocidades Típicas xDSL

Al igual que ADSL esta tecnología usa splitter para separar los servicios de POTS y datos, haciéndola más atractiva a los posibles usuarios de VDSL.

2.2.4.5 Symmetric Digital Subscriber Line

Mejor conocida como SDSL es una tecnología bien explotada por las empresas, ya que como su nombre lo indica nos permite la transmisión de datos en forma simétrica, particularmente importante para empresas debido a que se realizan transferencia y se comparten archivos de forma frecuente.

Esta tecnología nace para solucionar el problema de las líneas dedicadas T1 o E1, las cuales causan interferencias suficientes para dejar inservibles los pares adyacentes a estos en una PSTN.

SDSL permite velocidades de 1.544 Mbps o 2.048 Mbps a distancia de 6 Km., esto la convierte en el principal contrincante de HDSL, sin embargo esta tecnología ha tenido gran aceptación debido a que esta diseñada para funcionar sobre un solo para de cobre a diferencia de HDSL, pero al igual que esta no se puede tener coexistencia de transmisiones de voz y datos en el mismo par.

Esta tecnología xDSL usa esquemas de modulación 2B1Q, el cual no produce interferencia en los pares adyacentes, factor que permite de su uso, una ventaja para el usuario.

2.3 WiFi

2.3.1 Descripción General

2.3.1.1 Componentes

La arquitectura 802.11 posee varios componentes que interactúan entre si para poder brindar una movilidad a las estaciones (STA) dentro de la red inalámbrica; el conjunto de servicios básicos (BSS) es el bloque básico de la red LAN inalámbrica, dentro del área de cobertura de esta BSS podemos encontrar estaciones que se disponen a entablar comunicación entre ella, pero cuando una de estas estaciones sale de esta área de cobertura no podrá se capaz de mantener la comunicación con el resto de las estaciones.

Una subclase de BSS denominada BSS independiente es el componente más simple de la red LAN inalámbrica 802.11, esta consiste de solamente dos estaciones, estas estaciones se comunican directamente, este tipo de operación se denomina red Ad Hoc.

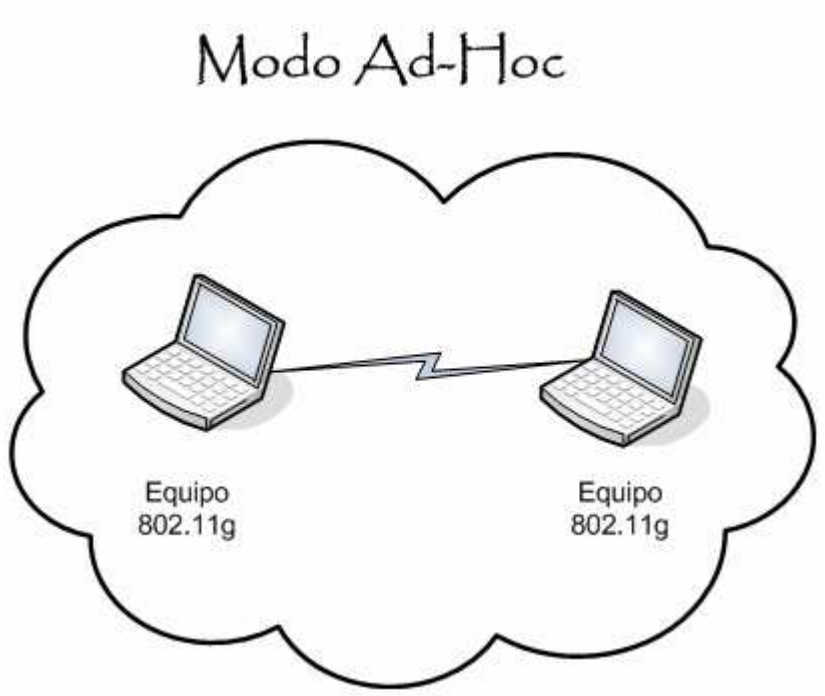


Figura 2.36. Red Ad Hoc

La asociación entre estaciones y BSS es dinámica, para convertirse en parte de la infraestructura BSS, una STA debe asociarse primero, el proceso de asociación es dinámico e implica el uso de un servicio de sistema de distribución (DSS).

Las limitaciones físicas que posee 802.11 determinan la distancia de una conexión, para algunos casos esta distancia es suficiente, pero en otros casos se necesita incrementar el área de cobertura.

Una BSS puede formar parte de una red extendida, la cual esta basada en una unión de múltiples BSS, el medio para poder lograr esta unión es el sistema de distribución (DS).

802.11 separa el medio inalámbrico (WM) de el medio del sistema de distribución (DSM) de una forma lógica, cada medio lógico se usa para un propósito diferente.

El sistema de distribución permite que la tecnología WiFi soporte dispositivos móviles, médiate los servicios lógicos, para manejar direcciones de mapeo de destino y la integración de múltiples BSS.

Un punto de acceso (AP) es una estación que provee acceso a los servicios del sistema de distribución además de actuar como una estación. Los datos se mueven entre los BSS y el DS a través de un AP, cabe destacar que un punto de acceso también es una estación, y por lo tanto es una entidad direccionable, las direcciones usadas por un AP para la comunicación médiate un medio inalámbrico y un medio del sistema de distribución no son necesariamente las mismas.

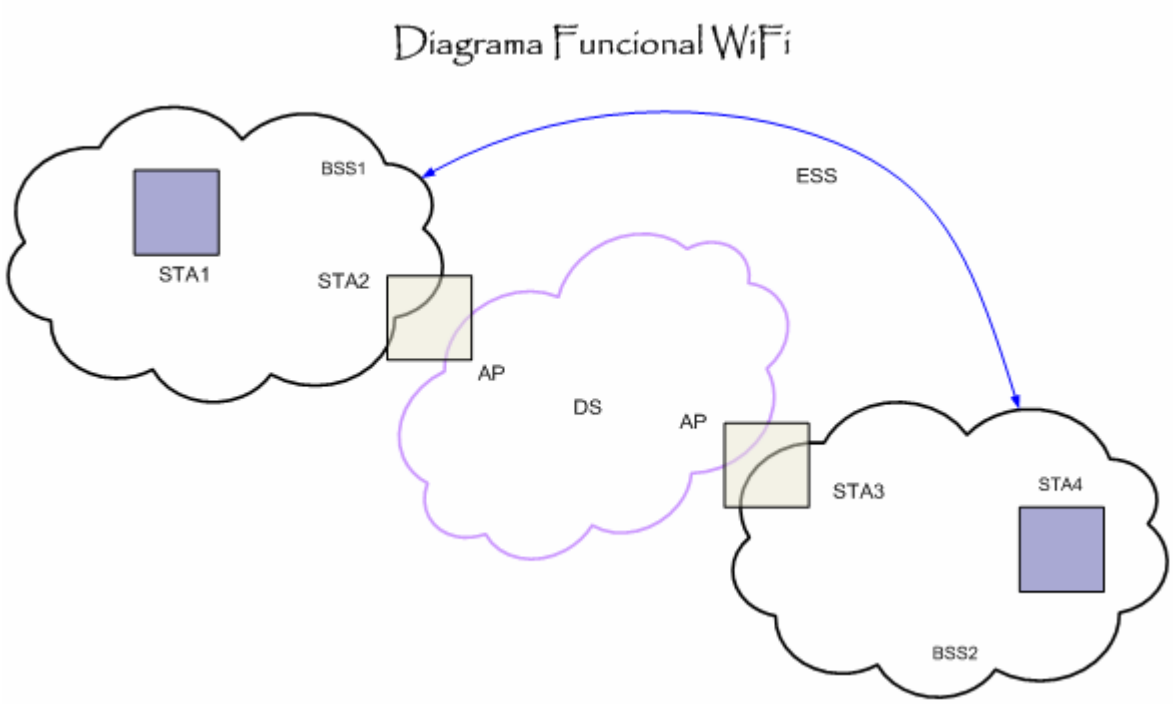


Figura 2.37. Diagrama Funcional WiFi

El conjunto de servicio extendido o ESS por sus siglas en ingles es una red de cobertura larga, DS y BSS pueden crear una red WiFi de tamaño y complejidad arbitraria, para poder trabajar de forma eficiente, la ESS aparece ante la subcapa LLC igual que una red independiente BSS (IBSS), esto permite que cualquier estación dentro de la ESS se pueda comunicar y que las estaciones móviles se desplacen de una BSS a otra el forma transparente para la subcapa LLC.

Una vez que se ha establecido el concepto de una ESS, se debe tener en cuenta que se pueden tener varias posibles situaciones dentro de una ESS:

- Las BSS pueden estar parcialmente sobrepuestas.
- Las BSS pueden estar físicamente separadas, ya que en forma lógica no existe ningún límite de distancia entre estas.
- Las BBS pueden estar físicamente colocadas en una misma posición.
- Una o varias redes IBSS o ESS pueden estar físicamente presentes en el mismo espacio como una o varias redes ESS.

La RSNA (Robust Security Network Association) define un número de aplicaciones para mejorar la autenticación y la privacidad equivalente cableada (WEP), entre estas podemos mencionar: mejoras en el mecanismo de autenticación de estaciones; algoritmos de gestión de llave; establecimiento de llave criptografiada; un mecanismo de encapsulación de datos mejorada (CTR) con protocolo de autenticación de mensaje y un protocolo de integridad de llave temporal (TKIP) opcional.

El RSNA se apoya en dos componentes externos a la arquitectura 802.11, estos son el PAE (Port Access Entity) que esta presente en todas las estaciones y el AS (Authentication Server) que viene en todo AP.

La capa física de una red inalámbrica no provee un área de cobertura bien definida, las características de propagación son dinámicas e impredecibles.

Para poder establecer una integración entre la arquitectura WiFi y las redes LAN cableadas, se debe usar un último componente lógico denominado portal, a través de este

portal una unidad de datos de una red diferente accede al DS de la red 802.11. Es posible para un dispositivo tener ambas funciones a la vez, la de AP y portal.

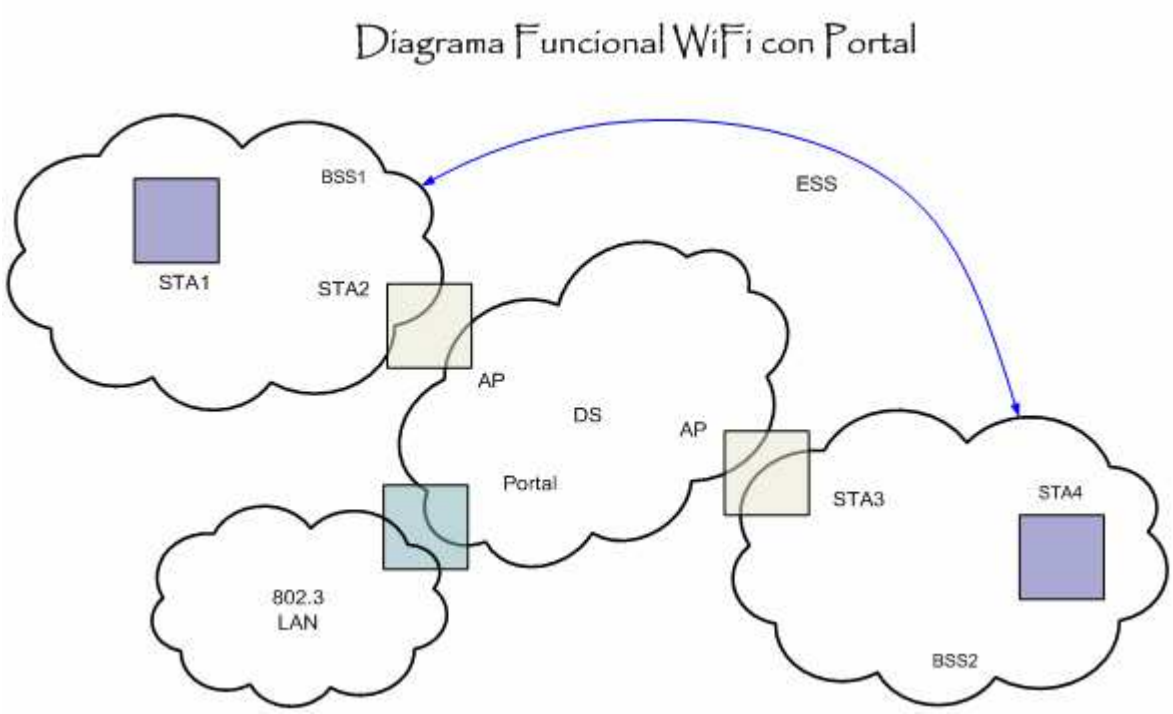


Figura 2.38. Diagrama Funcional WiFi con Portal

2.3.1.2 Interfases de Servicio Lógicas

El DS dentro de una red 802.11 pude ser implementada desde una red diferente, por lo que se revisaran los servicios que el DS puede soportar, tenemos dos categorías de servicios, los cuales son usados por la subcapa MAC:

- Servicios de Estación (SS)
- Servicios de Sistema de Distribución (DSS)

El conjunto de los servicios soportados por una red WiFi son:

- ✓ Autenticación
- ✓ Asociación
- ✓ De autenticación
- ✓ Disociación
- ✓ Distribución

- ✓ Integración
- ✓ Confidencialidad
- ✓ Reasociación
- ✓ Entrega MSDU (Unidad de Datos de Servicio MAC)

Este conjunto de servicios se reparte en dos grupos, el primer grupo que forman parte de cada estación y los que forman parte de los DS.

2.3.1.2.1 Servicio de Estación

El servicio que provee una estación es conocido como servicio de estación (SS), este se encuentra en cada estación incluyendo los puntos de acceso, estos servicios son usados por las entidades de la subcapa MAC.

- ➢ Autenticación
- ➢ De autenticación
- ➢ Confidencialidad
- ➢ Entrega MSDU

2.3.1.2.2 Servicio de Sistema de Distribución

Este servicio es provisto por el sistema de distribución, generalmente es usado para cruzar los limites lógicos de espacio de dirección y medios.

- ➢ Asociación
- ➢ Disociación
- ➢ Distribución
- ➢ Integración
- ➢ Reasociación

2.3.1.2.3 Múltiples Espacios de Dirección Lógicos

Las redes 802.11 usan el espacio de dirección de 48 bits usado por las familias 802, por lo que las direcciones WiFi son compatibles con el espacio de dirección usado por las redes LAN Ethernet.

Esto implica que en muchas instancias las direcciones MAC Ethernet y las direcciones MAC WiFi son las mismas.

WiFi también permite que el espacio de direcciones lógicas pueda ser diferente, esta habilidad para manejar varios medios lógicos y espacios de dirección sea la llave para poder tener una independencia a la hora de la implementación del DS.

2.3.1.3 Revisión de Servicios

Existen nueve servicios especificados, seis de los cuales están diseñados para soportar entrega MSDU entre las estaciones, los restantes se usan para control de acceso y confidencialidad.

Cada servicio esta soportado por uno o varios tipos de trama MAC, algunos por los mensajes de gestión y otros por los mensajes de datos MAC. La subcapa MAC usa tres tipos de mensajes, los cuales son datos, gestión y control.

2.3.1.3.1 Distribución de Mensajes dentro de un Sistema de Distribución.

2.3.1.3.1.1 Distribución

Es el primer servicio usado por las estaciones WiFi, este servicio es invocado por cada mensaje de datos hacia o desde una estación operando en una ESS, este se envía mediante DSS.

En una red ESS, en caso de tener varios BSS y se envía un mensaje de datos de una estación en un BSS hacia otra estación en otro BSS, el mensaje pasa de la estación al AP, el cual le entrega el mensaje al servicio de distribución del DS, el cual se encarga de llevar el mensaje a través del DS hasta su destino, en este caso el AP en el segundo BSS, y de aquí se entrega a la estación de destino.

Si un mensaje fuera enviado dentro de un mismo BSS, el servicio de distribución se encarga de establecer que el AP de destino es el mismo que el de origen.

2.3.1.3.1.2 Integración

Si el servicio de distribución determina que el destino que se desea alcanzar es parte de una red LAN integrada, los puntos de salida del DS pasan a ser un portal en vez de un AP.

Los mensajes que son distribuidos a un portal causan que el DS invoque la función de integración (después del servicio de distribución). Esta función es responsable de realizar las acciones necesarias para entregar el mensaje desde el DSM hasta el medio LAN, la integración es una DSS.

Por otra parte los mensajes enviados desde una LAN integrada, a través del DS, hasta una estación, invocaran la función de integración antes de que el mensaje sea distribuido por el servicio de distribución.

2.3.1.3.2 Servicios que Soportan el Servicio de Distribución

El propósito principal de la subcapa MAC es la de transferir MSDU entre las entidades de la subcapa MAC, la información requerida para que el servicio de distribución opere es provista por los servicios de asociación; antes de que un mensaje de datos pueda ser manejado por el servicio de distribución, la estación debe estar asociada.

2.3.1.3.2.1 Tipos de Movilidad

Los tres tipos más importantes de transiciones describen la movilidad de las estaciones dentro de la red son:

1) No Transición.- En este tipo de transición se deben distinguir dos subtipos:

Estático.- Sin movimiento

Movimiento Local.- Movimiento dentro del rango físico de la comunicación entre estaciones, en una misma área de servicio básico.

2) Transición BSS.- Este tipo esta definido como el movimiento de una estación desde un BSS dentro de una ESS hacia otro BSS dentro del mismo ESS.

3) Transición ESS.- Se define como el movimiento de una estación desde un BSS de un ESS hasta un BSS perteneciente a un ESS diferente, este caso se produce únicamente si se consideran que la estación esta en movimiento; la conexión con las capas superiores en este caso no es segura, por lo que la desconexión del servicio ocurre.

2.3.1.3.2.2 Asociación

Para entregar un mensaje a través del DS, el servicio de distribución necesita conocer cual AP acceder para la estación dada; esta información se le da al DS mediante el concepto de asociación.

La asociación es necesaria pero no suficiente para poder garantizar la movilidad de transición BSS; la asociación es suficiente para la movilidad sin transición, la asociación es un DSS.

Antes de que una estación pueda enviar un mensaje de datos mediante un AP, debe primero estar asociado con el AP; el acto de asociación invoca el servicio de asociación, el cual provee la estación para el mapeo de AP para el DS; el DS usa esta información para poder completar el servicio de distribución de mensaje.

Dentro de una red de seguridad robusta (RSN), el proceso de la transmisión de datos es un poco diferente; en un RSNA el puerto 802.11 determina en que momento permitirá el paso de datos a través del enlace WiFi; un puerto 802.11 mapea una asociación, este puerto consiste en realidad de dos puertos, uno controlado y otro sin control, el puerto controlado esta bloqueado para trafico de datos en general entre estaciones, hasta que los procesos de autenticación sean completados por el puerto sin control; una vez realizado este paso se habilita la protección de datos para evitar accesos no autorizados, el puerto controlado se abre para dejar pasar estos datos protegidos.

En cualquier instante, una estación puede asociarse a solo un AP a la vez, esto asegura que el DS pueda determinar cual AP esta sirviendo a una determinada STA, una vez que la asociación esta completa, una estación puede hacer uso del DS para comunicarse; la asociación siempre es iniciada por la estación móvil y no por el AP.

Un AP puede asociarse con varias estaciones a la vez; una estación aprende que AP's están presentes y después solicita establecer una asociación mediante la invocación al servicio de asociación.

2.3.1.3.2.3 Reasociación

La asociación es suficiente para entregas de mensajes sin transición entre estaciones WiFi; funciones adicionales se necesitan para soportar transiciones BSS; estas funciones adicionales son provistas por el servicio de reasociación, la reasociación es un DSS.

El servicio de reasociación es invocado para mover una asociación existente con un AP hacia otro; esto mantiene al DS informado del mapeo actual entre el AP y la STA mientras esta se mueve desde un BSS hacia otro dentro de una misma ESS; reasociación también habilita cambios en los atributos de asociación, de una asociación establecida mientras la estación permanece asociada con el mismo AP; le reasociación debe ser iniciada por la estación móvil.

No se proveen facilidades para mover una RSNA durante la reasociación, sin embargo una RSNA antigua se borra y una nueva se construirá.

2.3.1.3.2.4 Disociación

El servicio de disociación es invocado en cualquier momentos que una asociación existente sea terminada; la disociación es un DSS.

En un ESS, este servicio le indica al DS que evite la información de asociación existente, por lo que los intentos de enviar mensajes a través del DS a una estación desasociada se imposible.

El servicio de disociación puede ser invocada por cualquier elemento asociado, la disociación es una notificación y no un pedido; esta no puede ser rehusada por cualquier elemento en asociación.

Los AP’s pueden necesitar desasociar estaciones para permitir que el AP sea removido de una red ya sea por mantenimiento u otras razones.

Las estaciones deben intentar desasociarse en cualquier momento que desee abandonar la red; sin embargo, el protocolo MAC no depende de la invocación de las estaciones al servicio de disociación.

2.3.1.3.3 Control de Acceso y Servicios de Confidencialidad

Dos servicios son necesarios para las redes 802.11 puedan tener equivalentes funcionales a los inherentes de las redes cableadas; el diseño de redes LAN asume los atributos físicos del cable, en particular los diseños de redes LAN cableadas asumen la naturaleza del medio físico cerrado y controlado del cable, pero en redes 802.11 la naturaleza del medio físico abierto viola esas suposiciones.

Dos servicios son provistos para poder brindar funcionalidades a la par de las suposiciones de redes LAN cableadas, estas son autenticación y confidencialidad; la autenticación es usada en vez de la conexión física del medio cableado; confidencialidad de datos es usada para brindar los aspectos de confidencialidad de medios cableados cerrados.

En una red inalámbrica que no soporte RSNA, dos servicios: autenticación y confidencialidad son definidos; la autenticación se usa en vez de la conexión física al medio cableado; la encriptación WEP fue definida para proveer los aspectos de confidencialidad cercanos a los de medios cableados.

Una RSNA usa el servicio de autenticación junto con TKIP y CCMP para proveer el control de acceso; la entidad de gestión de estación (SME) provee el manejo de llave mediante una trama EAPOL-Key; la confidencialidad e integridad de los datos, se proveen mediante la gestión de llave RNS con TKIP y CCMP.

2.3.1.3.3.1 Autenticación

La autenticación 802.11 opera a nivel de enlace entre las estaciones, WiFi no provee autenticaciones entre usuarios o de extremo a extremo.

WiFi intenta controlar el acceso a redes LAN mediante el servicio de autenticación; la autenticación es un SS; este servicio puede ser usado por todas las estaciones para establecer sus identidades a otras estaciones con las cuales pretende comunicarse, ya sea para redes ESS o IBSS. Si un nivel mutuo de aceptación de autenticación no ha sido establecido entre dos estaciones, la asociación no será establecida.

Se han definido dos métodos de autenticación: Autenticación de sistema abierto y autenticación de llave compartida; la autenticación de sistema abierto admite cualquier estación al DS; mientras que la autenticación de llave compartida se basa en WEP para demostrar conocimiento de una llave de encriptación WEP; cabe destacar que el mecanismo de autenticación WiFi permite también nuevos métodos de autenticación.

Una RSNA también soporta autenticación basada en las normas IEEE 802.1X, o llaves pre-compartidas (PSKs); la autenticación 802.1X utiliza un EAP (Extensible Authentication Protocol) para autenticar estaciones y AS entre ellos.

En una RSNA, tanto los autenticadotes como los suplicantes intercambian información de protocolo mediante el puerto sin control, debido a que el puerto controlado esta bloqueado para tráfico en general, hasta que los procesos de autenticación se hayan completado de forma exitosa por el puerto sin control.

El algoritmo de autenticación de sistema abierto se usa tanto en BSS como en IBSS RSNAs, sin embargo, debido a que la autenticación de sistema abierto es opcional en una RSNA IBSS, RSNA deshabilita el uso de la autenticación por llave compartida.

Una estación puede autenticarse con varias estaciones en cualquier instante.

2.3.1.3.3.2 Pre-Autenticación

Debido a que el proceso de autenticación puede ocupar mucho tiempo, dependiendo del protocolo de autenticación que se use, el servicio de autenticación puede ser invocado de forma independiente al servicio de asociación.

La pre-autenticación se realiza de forma típica por una estación, mientras esta asociado con un AP, con el cual esta previamente autenticado; cabe destacar que las redes WiFi no requieren que las estaciones se pre-autentiquen con los AP's; sin embargo la autenticación es requerida antes que se produzca una asociación.

Si la autenticación se deja para el momento de la reasociación, esto puede impactar la velocidad a la cual una estación se puede reasociar entre AP's, limitando el desempeño en transiciones BSS; el uso de la pre-autenticación lleva al servicio de autenticación por encima del tiempo critico del proceso de reasociación.

2.3.1.3.3.3 De Autenticación

El servicio de de autenticación es invocado cuando una autenticación de llave compartida o sistema abierto existente desee ser terminada, la de autenticación es un SS.

En un ESS, ya que el proceso de autenticación es un requisito para la asociación, el acto de una de autenticación debe llevar a que la estación se desasocie, el servicio de de autenticación puede ser invocado por cualquier elemento autenticado; la de autenticación no es un pedido, es una notificación, la cual no puede ser rehusada por algún elemento; cuando un AP envía una notificación de de autenticación a una estación asociada, la asociación debe también terminar.

En un ESS RSN, la autenticación por sistema abierto es requisito; mientras que la de autenticación resulta en la terminación de cualquier asociación por parte de la estación de autenticada, también deshabilita el puerto controlado de la estación y elimina cualquier asociación de seguridad establecida, ya sea individual o grupal; la notificación de de autenticación es provista mediante la capa MAC.

En una IBSS RNS, la autenticación por sistema abierto es opcional, pero una de las estaciones debe reconocer las tramas de de autenticación; la de autenticación provoca la terminación de las asociaciones de seguridad y deshabilita el puerto controlado.

2.3.1.3.3.4 Confidencialidad

En una red cableada, solamente aquellas estaciones conectadas físicamente por el cable pueden enviar o recibir trafico LAN; con un medio inalámbrico compartido, esto no sucede.

Todas las estaciones WiFi pueden recibir todo el tráfico que este en su rango y pueden transmitir hacia cualquier otra estación en rango, por lo que cualquier enlace inalámbrico sin confidencialidad hacia una red cableada existente puede representar una seria brecha de seguridad de dicha LAN cableada.

Para poder brindar la seguridad de una red inalámbrica al nivel de una LAN cableada, WiFi ofrece la habilidad de proteger el contenido de los mensajes; esta funcionalidad se ve implementada por el servicio de confidencialidad; confidencialidad es un SS.

WiFi provee tres tipos de algoritmos de criptografía para proteger el tráfico de datos: WEP, TKIP y CCMP; WEP y TKIP están basados en el algoritmo RC4[65], mientras que CCMP esta basado en el estándar de encriptación avanzado (AES); se le proporciona un método a las estaciones mediante el cual puede seleccionar el algoritmo a ser usado para una asociación.

El estado de confidencialidad inicial de las estaciones WiFi es transparente; si el servicio de confidencialidad no es invocado, todos los mensajes deben ser enviados sin protección, si esta política no es aceptada por el transmisor, no deberá enviar tramas de datos; y en caso de que esta política no sea aceptada por el receptor, deberá descartar cualquier trama de datos recibida.

Las tramas de datos sin protección recibidas en la estación configurada para confidencialidad obligatoria, tal como las tramas de datos protegidas usando una llave no valida en la estación de recepción, son descartadas sin una indicación al LLC; estas tramas son reconocidas por el medio inalámbrico para evitar desperdiciar ancho de banda en el WM por reenvios.

[65] RC4 es un algoritmo de propiedad de RSA Security Inc.

2.3.1.3.3.5 Gestión de Llave

La confidencialidad mejorada, autenticación de datos, y mecanismos de protección reejecutados, requieren llaves de criptografía renovadas. Para poder proveer estas llaves renovadas, nos valemos de dos protocolos llamados: 4-Way Handshake y Group Key Handshake.

2.3.1.3.3.6 Autenticidad de Origen de Datos

El mecanismo de autenticidad de origen de datos, le permite a una estación que recibe una trama de datos el poder determinar cual estación transmitió el MPDU; esta opción es requerida en una RSNA para prevenir que una estación sea enmascarada como otra estación, este mecanismo es provisto a las estaciones mediante el CCMP o TKIP.

El mecanismo de autenticidad de origen de datos es aplicable únicamente para tramas de datos unicast; los protocolos no garantizan la autenticidad del origen de datos de tramas broadcast o multicast, debido a que no se puede lograr mediante llaves simétricas, el costo computacional de usar llaves públicas es demasiado elevado.

2.3.1.3.3.7 Detección de Reejecución

El mecanismo de detección de reejecución define el medio mediante el cual, una estación que recibe una trama de datos de otra estación, puede detectar si la trama de datos es una retransmisión no autorizada; este mecanismo esta disponible para las estaciones que usen CCMP o TKIP.

2.3.1.4 Relación entre Servicios

Una estación posee dos variables de estado con cada estación con la que se comunica directamente mediante el medio inalámbrico de ser necesarios:

- ✓ Autenticación.- Los valores son de autenticado y autenticado.
- ✓ Asociación.- Los valores son desasociado y asociado.

Estas dos variables crean tres estados locales para cada estación remota:

Estado 1.- Estado de arranque inicial, de autenticado, desasociado.

Estado 2.- Autenticado, no asociado.

Estado 3.- Autenticado y asociado.

Las relaciones entre estos estados se pueden apreciar mejor en la siguiente gráfica:

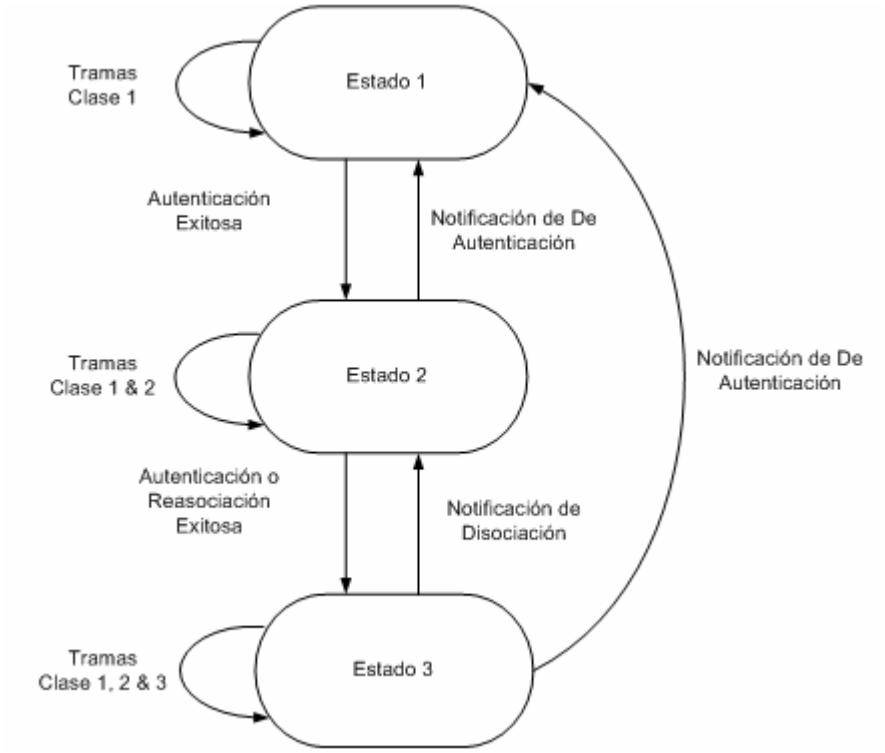


Figura 2.39. Relaciones entre las Variables de Estado y Servicios

El estado existente entre las estaciones de origen y destino determinan el tipo de trama que puede ser intercambiada entre este par de estaciones; los tipos de tramas permitidas están agrupadas en clases, las cuales corresponden a un estado en particular de las estaciones.

En el estado 1, solo las tramas clase 1 son permitidas, en el estado 2, las clases de tramas 2 y 1 son permitidas, y en el estado 3 todas las tramas son permitidas, es decir las clases 1, 2 y 3.

2.3.1.4.1 Tramas Clase 1

Tramas de control:

- Request to Send (RTS).

- Clear to Send (CTS).
- Acknowledgment (ACK).
- Contention - Free (CF) - End + ACK.
- CF – End.

Tramas de Gestión:

- Probe Request/Respond.
- Beacon.
- Autenticación: La autenticación exitosa permite a la estación intercambiar las tramas clase 2; la autenticación fallida deja a la estación en el estado 1; la STA debe autenticarse de nuevo previo el envío de tramas clase 2.
- De autenticación: La notificación de de autenticación cuando la estación esta en el estado 2 o 3 le obliga a pasar al estado 1, la STA debe llegar a estar autenticada de nuevo para poder enviar las tramas clase 2.
- Announcement Traffic Indication Message (ATIM).

Tramas de Datos:

- Datos: tramas de datos con bits de control de trama (FC) “To DS” y “From DS” ambos falsos.

2.3.1.4.2 Tramas Clase 2

Tramas de Gestión:

- Association Request/Response: Una asociación exitosa permite el uso de tramas clase 3, una asociación fallida deja a la estación en el estado 2.
- Reassociation Request/Response: Una reasociación exitosa permite tramas clase 3, por el contrario una reasociación fallida deja a la estación en el estado 2, las tramas de reasociación deben solamente ser enviadas si la estación origen esta asociada con el mismo ESS.
- Disassociation: La notificación de disociación cuando se encuentra en un estado 3 cambia el estado de la STA al 2, esta estación de be asociarse de nuevo para poder utilizar el DS.

Si la estación A recibe una trama clase 2 con una dirección de unicast en el campo de dirección, de la estación B, la cual no esta autenticada con la estación A, esta debe enviar trama de de autenticación a la estación B.

2.3.1.4.3 Trama Clase 3

Tramas de Datos:

- Subtipos de Datos: Tramas de datos permitidas; es decir, “To DS” o “From DS” de los bis FC deben ser seteados en verdaderos para utilizar el DSS.

Tramas de Gestión:

- De autenticación: la notificación de de autenticación en un estado 3 implica disociación también, cambiando el estado de la STA de 3 a 1, la estación debe autenticarse de nuevo previa nueva asociación.

Tramas de Control:

- PS-Poll.

Si una estación A recibe una trama clase 3 con una dirección de unicast en el campo de dirección desde la STA B, la cual esta autenticada pero no asociada con la estación A, la STA A debe enviar un trama de disociación a la estación B.

Si la estación A recibe una trama clase 3 con una dirección de unicast en el campo de dirección desde la estación B, la cual no esta autenticada con la STA A, la estación A debe enviar una trama de de autenticación a la STA B.

2.3.1.5 Diferencias entre Redes de Área Local ESS e IBSS

Como se pudo apreciar en páginas anteriores una IBSS es usada para soportar redes tipo ad hoc; en una red IBSS, una estación se comunica directamente con otra o varias estaciones.

Una IBSS consiste de estaciones directamente conectadas, por definición existe una sola BSS, por lo que al no existir un DS físico, no puede haber un portal, y por consiguiente redes LAN cableadas o DSS no están soportadas.

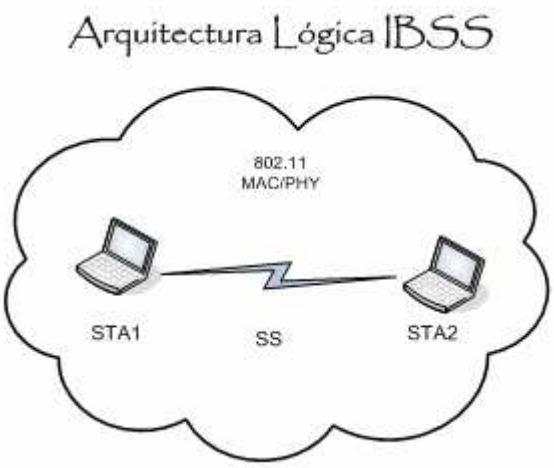


Figura 2.40. Arquitectura lógica IBSS

En la figura mostrada, solo se tiene un mínimo de dos estaciones, una IBSS puede tener un número arbitrario de miembros, dentro de una IBSS solo se permiten las tramas clase 1 y 2, debido a la falta de DS; los servicios aplicados a una IBSS son los SS.

En una IBSS, cada estación debe reforzar sus propias políticas de seguridad; en una ESS, un AP puede reforzar una política de seguridad uniforme a través de todas las estaciones.

2.3.1.6 Contenidos de la Información de Mensaje que Soportan los Servicios

Cada servicio esta soportado por uno o más mensajes WiFi.

2.3.1.6.1 Datos

Para una estación que desea enviar datos a otra, debe enviar un mensaje de datos, como se muestra a continuación:

Mensajes de Datos

- Tipo de Mensaje: Datos.
- Subtipo de Mensaje: Datos.
- Ítems de Información: Dirección de origen del mensaje, dirección de destino del mensaje, identificación de BSS.
- Dirección del Mensaje: Desde estación a estación.

2.3.1.6.2 Asociación

Para una estación que desea asociarse, el servicio de asociación produce el siguiente mensaje:

Pedido de Asociación

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: Pedido de Asociación.
- Ítems de Información: Dirección de la estación que inicia la asociación, dirección del AP con el cual la estación se asociara, identificación del ESS.
- Dirección del Mensaje: Desde estación a AP.

Respuesta de Asociación

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: Respuesta de Asociación.
- Ítems de Información: Resultado del pedido de asociación, este es un item con valores de “exitoso” y “fallido”; si la asociación es exitosa, la respuesta debe incluir el identificador de asociación (AID).
- Dirección del Mensaje: Desde AP a estación.

2.3.1.6.3 Reasociación

Para una estación intentando reasociarse, el servicio de reasociación desencadena el siguiente mensaje:

Petición de Reasociación

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: Petición de reasociación.
- Ítems de Información: Dirección de la estación que inicia la reasociación, dirección del AP con el cual la estación se reasociara, identificación de ESS.
- Dirección del Mensaje: Desde estación al AP con el cual se desea reasociarse.

Respuesta de Reasociación

- Tipo de Mensaje: Gestión.

- Subtipo de Mensaje: Respuesta de Reasociación.
- Ítems de Información: Resultado del pedido de reasociación, este ítem lleva valores de “exitoso” y “fallido”; si la reasociación es exitosa, la respuesta debe incluir el AID.
- Dirección del Mensaje: Desde AP a estación.

2.3.1.6.4 Disociación

Para una estación que desea terminar una asociación activa, el servicio de disociación produce el siguiente mensaje:

Disociación

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: Disociación.
- Ítems de Información: Dirección de la estación que esta siendo desasociada, esta debe ser la dirección de broadcast en el caso de una disociación de un AP con todas las estaciones; la dirección del AP con el cual la estación esta asociada actualmente.
- Dirección del Mensaje: Desde estación a estación.

2.3.1.6.5 Confidencialidad

Para una estación que desea invocar un algoritmo de confidencialidad, el servicio de confidencialidad selecciona el algoritmo de confidencialidad y configura el bit de la trama protegida en forma adecuada.

2.3.1.6.6 Autenticación

Para una estación que desea autenticarse con otra, usando la autenticación de sistema abierto o de llave compartida, el servicio de autenticación produce una o más tramas de gestión de autenticación a ser intercambiadas, la secuencia exacta de las tramas y sus contenidos dependen del esquema de autenticación invocado; para ambos esquemas de autenticación, el algoritmo de autenticación es identificado dentro del cuerpo de la trama de gestión.

En un ambiente IBSS, ambas estaciones pueden ser la estación que inicia la autenticación STA1, mientras que en un ambiente ESS, la STA1 es la estación móvil y la STA2 es el AP.

Autenticación (Primera Trama de Secuencia)

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: Autenticación.
- Ítems de Información: Identificación del algoritmo de autenticación, aserción de la identidad de la estación, número de secuencia de la transacción de autenticación, información dependiente del algoritmo de autenticación.
- Dirección del Mensaje: La primera trama en la secuencia de transacción es siempre de STA1 a STA2.

La primera trama en la secuencia de autenticación debe estar siempre sin encriptación.

Autenticación (Trama de Secuencia Intermedia)

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: Autenticación.
- Ítems de Información: Identificación del algoritmo de autenticación, número de secuencia de la transacción de autenticación, información dependiente del algoritmo de autenticación.
- Dirección del Mensaje: Número de secuencia de transacción par: desde STA2 a STA1; número de secuencia de transacción impar: desde STA1 a STA2.

Autenticación (Trama de Secuencia Final)

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: Autenticación.
- Ítems de Información: Identificación del algoritmo de autenticación, número de secuencia de la transacción de autenticación, información dependiente del algoritmo de autenticación, el resultado de la petición de autenticación, este item lleva el valor de “exitoso” y “fallido”.
- Dirección del Mensaje: Desde STA2 a STA1.

2.3.1.6.7 De Autenticación

Una estación que desea invalidar la autenticación actual que fue establecida usando la autenticación de sistema abierto o llave compartida, envía el siguiente mensaje:

De Autenticación

- Tipo de Mensaje: Gestión.
- Subtipo de Mensaje: De Autenticación.
- Ítems de Información: Dirección de la estación que esta siendo de autenticada, dirección de la estación con la cual esta autenticada; esta debe ser la dirección de broadcast en caso de que una estación desee de autenticar todas las estaciones autenticadas.
- Dirección del Mensaje: Desde estación a estación.

2.3.1.7 Modelo de Referencia

Para el mejor entendimiento de la tecnología WiFi, se separa a la misma en dos partes, la capa de enlace o MAC y la capa Física, estas capas tienen una estrecha relación con el modelo OSI, lo que significa que le permite acoplarse en las capas superiores con cualquier tipo de tecnología basada en este modelo referencial.

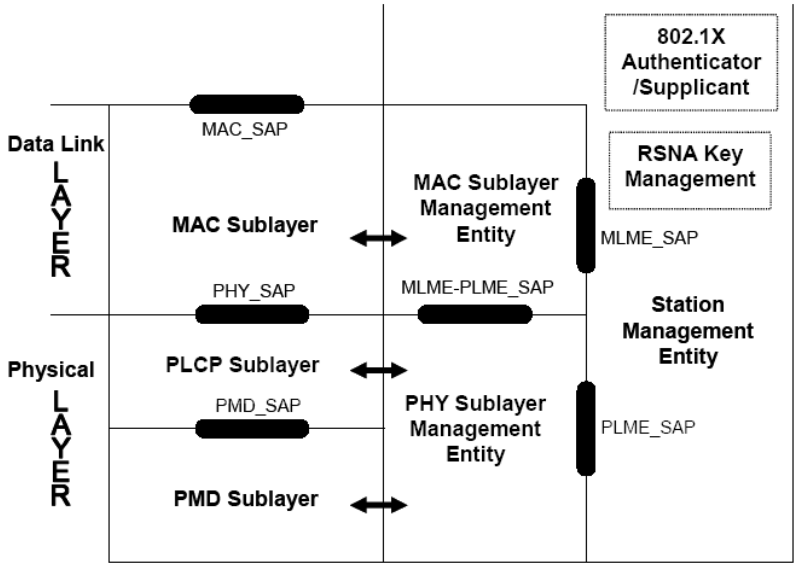


Figura 2.41. Modelo de Referencia de la Tecnología WiFi[66]

[66] IEEE 802.11i, Institute of Electrical and Electronics Engineers, Pág. 13.

2.3.1.8 802.11 y 802.1X

Una RSNA se basa en 802.1X para proveer los servicios de autenticación y usa el esquema de gestión de llave 802.11; el mecanismo de control de acceso 802.1X se aplica a la asociación entre una estación y un AP; y, a la relación entre estaciones IBSS y parejas de estaciones; la entidad de gestión de estación (SME) de un AP hace el papel de autenticador, y opcionalmente de aplicante y papeles de servidor de autenticación (AS).

En una ESS, el SME de una estación no AP realiza el papel de aplicante; en una IBSS, el SME de una estación realiza los papeles de autenticador y aplicante, además de tomar el papel de AS.

2.3.1.8.1 802.11 usando 802.1X

WiFi depende de 802.1X para controlar el flujo de MSDU entre el DS y las estaciones mediante el modelo de puertos controlado/sin control de 802.1X.

Las tramas de autenticación de 802.1X son transmitidas mediante las tramas de datos WiFi a través del puerto sin control; el puerto controlado esta bloqueado para el tráfico general de datos entre dos estaciones, hasta que el proceso de autenticación se haya completado de forma exitosa en el puerto sin control.

Es responsabilidad tanto del autenticador como del aplicante la implementación del bloqueo de puertos; cada asociación entre un par de estaciones crea un par único de puertos 802.1X, cada autenticación se lleva acabo en esos dos puertos.

2.3.1.8.2 Revisión del Modelo Funcional de Infraestructura

Vamos a partir de dos casos en particular, el primero cuando se usa un AS y un PSK.

2.3.1.8.2.1 Operaciones AKM (Authentication and Key Management) con AS

Las siguientes operaciones AKM son llevadas a cabo al usar un AS 802.1X:

- Previo al uso de 802.1X, WiFi asume que el autenticador y el AS han establecido un canal seguro; las credenciales de autenticación deben ser distribuidas al aplicante y AS previa la asociación.

- Una estación descubre la política de seguridad de un AP mediante el monitoreo pasivo de las tramas Beacon, o mediante una prueba; si se usa la autenticación 802.1X, el proceso de autenticación EAP inicia cuando el autenticador del AP envía el EAP-Request o el aplicante de la estación envía el mensaje EAPOL-Start. Las tramas de autenticación EAP pasan entre el aplicante y el AS mediante los puertos sin control del autenticador y aplicante.
- El aplicante y AS se autentican entre ellos y generan un PMK (Pairwise Máster Key), el PMK es enviado desde el AS al autenticador mediante un canal seguro.

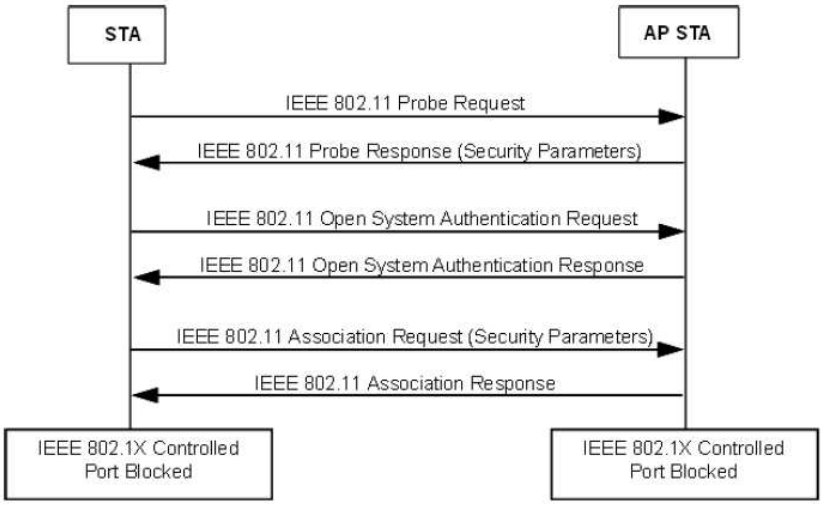


Figura 2.42. Proceso de Establecimiento de Asociación 802.11[67]

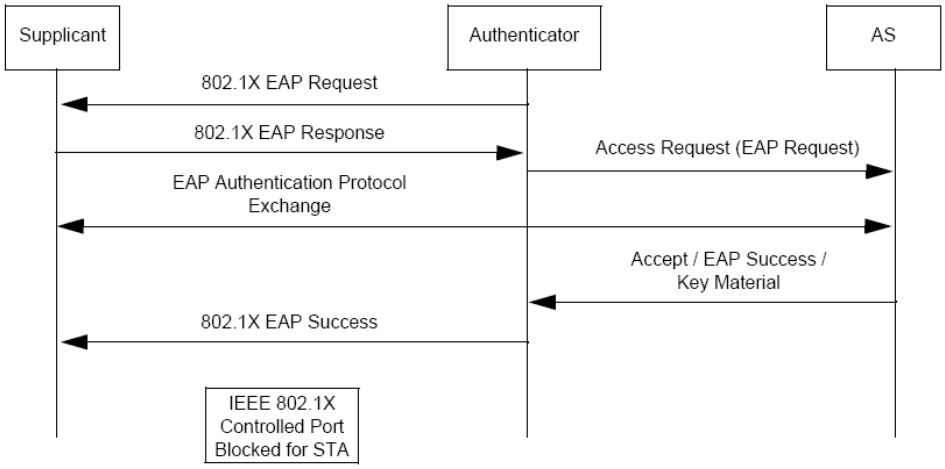


Figura 2.43. Autenticación EAP 802.1X[68]

[67] IEEE 802.11i, Institute of Electrical and Electronics Engineers, Pág. 15.
[68] IBID 67

El autenticador inicia el 4-Way Handshake con tramas EAPOL-Key par poder cumplir con las siguientes tareas:

- Confirma que las parejas mantengan el PMK
- Confirma que el PMK este activo
- Entrega una llave transitoria de pareja (PTK) al PMK
- Instala la encriptación de pareja y la llave de integridad a 802.11
- Transporta la llave temporal de grupo (GTK) y el número de secuencia GTK desde el autenticador al aplicante y los instala en la estación, en caso de no estar instalado en el AP también realiza esta acción.
- Confirma la selección de tipo de cifrado.

Una vez que se completa el 4-Way Handshake, el autenticador y el aplicante se han autenticado uno con otro, por lo que los puertos controlados 802.1X se desbloquean y permiten tráfico de datos en general.

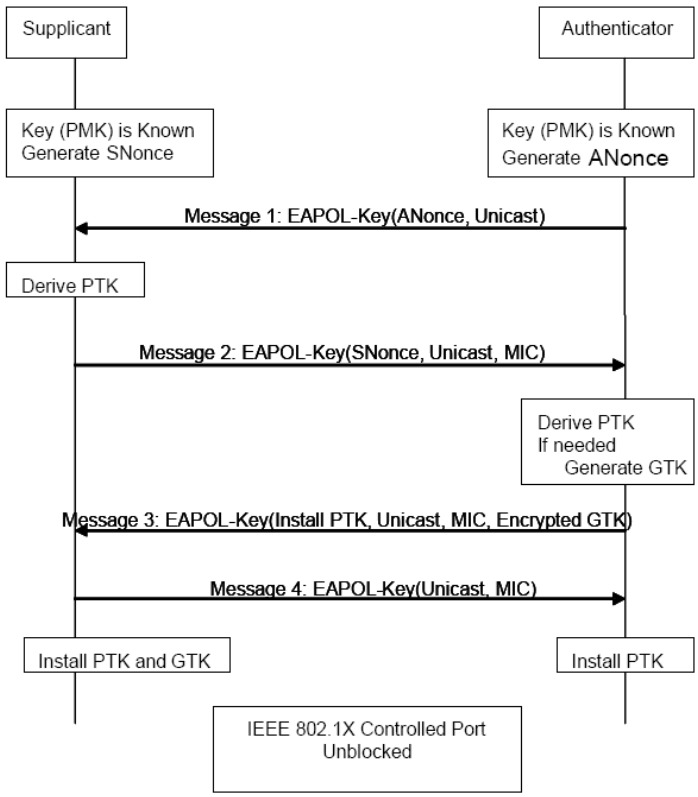


Figura 2.44. Proceso de Establecimiento de Llaves de Grupo y Pareja[69]

[69] IEEE 802.11i, Institute of Electrical and Electronics Engineers, Pág. 16.

Si el autenticador cambia después el GTK, envía esta nueva llave y su número de secuencia al aplicante usando el Group Key Handshake, para que el aplicante pueda seguir recibiendo mensajes de broadcast/multicast y opcionalmente, transmitir y recibir tramas unicast; las tramas EAPOL-Key son usadas para llevar a cabo estos intercambios.

2.3.1.8.2.2 Operaciones con PSK

Las siguientes operaciones AKM se llevan a cabo cuando el PMK es un PSK:

- Una estación descubre la política de seguridad de un AP mediante el monitoreo pasivo de las tramas Beacon o mediante pruebas; una estación se asocia con un AP y negocia una política de seguridad; el PMK es el PSK.
- El 4-Way Handshake con tramas EAPOL-Key es usado tal como el la autenticación 802.1X, cuando un AS esta presente.
- El GTK y su número de secuencia son enviados desde el autenticador al aplicante de igual manera que cuando se tiene un AS.

2.3.2 Definición de Servicios MAC

2.3.2.1 Servicio de Datos Asincrónico

Este servicio provee parejas de entidades LLC con la habilidad de intercambiar unidades de datos de servicios MAC (MSDU); para soportar este servicio, la capa MAC local usa los servicios de nivel físico para transportar un MSDU hasta una entidad MAC, donde será entregada a su correspondiente par LLC.

Tal transporte MSDU asincrónico es realizado según el mejor esfuerzo, por lo que no hay garantías de que el MSDU sea entregado de forma exitosa; el transporte broadcast y multicast es parte del servicio de datos asincrónicos provisto por la capa MAC.

Debido a las características del medio inalámbrico, las MSDU de broadcast y multicast pueden experimentar una calidad de servicio baja, comparada con las MSDU de unicast.

Todas las estaciones deben soportar el servicio de datos asincrónicos, debido a que algunas funciones de la capa MAC pueden reordenar algunas MSDU, existen dos clases de

servicios dentro del servicio de datos asincrónico, seleccionando la clase de servicio, cada entidad LLC controla si una entidad MAC puede o no reordenar las MSDU.

2.3.2.2 Servicios de Seguridad

Los servicios de seguridad en 802.11 son provistos por el servicio de autenticación y los mecanismos WEP, TKIP y CCMP, el servicio de confidencialidad ofrecido por la implementación WEP, TKIP y CCMP es la encriptación de las MSDU; WEP, TKIP y CCMP son servicios lógicos en la capa MAC, mientras que las implementaciones de los servicios WEP, TKIP y CCMP son transparentes para el LLC y otras capas superiores a la MAC.

Los servicios de seguridad provistos por WEP, TKIP y CCMP son los siguientes:

- ✓ Confidencialidad
- ✓ Autenticación
- ✓ Control de acceso en conjunción con gestión de capa.

Los servicios de seguridad de la subcapa MAC provistos por WEP, TKIP y CCMP, se basa en información de ninguna entidad de sistema o gestión de capa 2; las entidades de gestión comunican información a WEP mediante un grupo de atributos MIB. Las entidades de gestión comunican información a TKIP y CCMP a través de interfases de un grupo de entidades de gestión de subcapa MAC (MLME) y atributos MIB.

2.3.2.3 Ordenamiento MSDU

Los servicios provistos por la subcapa MAC permiten, y en ciertos casos pueden requerir, el reordenamiento de MSDU, MAC no reordena de forma intencional los MSDU, con excepción de que sea necesaria la mejora de probabilidad de las entregas exitosas basadas en el modo operación de la estación de recepción designada.

El efecto de este reordenamiento para un grupo de MSDU recibidos en la interfase de servicio MAC de una estación única, es el cambio en el orden de entrega de los MSDU de broadcast y multicast, relativo al MSDU directo, originado desde una dirección de estación de origen única.

Si un protocolo de capa superior usando el servicio de datos asincrónicos no puede tolerar este posible reordenamiento, la clase de servicio opcional de ordenamiento estricto debería ser usado. Los MSDU's transferidos entre cualquier par de estaciones usando la clase de servicio de ordenamiento estricto no están sujetas al ordenamiento relativo que es posible al usar la clase de servicio de multicast reordenable, sin embargo el deseo de recibir MSDU's enviados usando la clase de servicio de ordenamiento estricto en una estación termina en el uso simultaneo de las facilidades de gestión de potencia MAC de la estación.

2.3.3 Formatos de Trama

Todas las estaciones deben ser capaces de construir tramas para la transmisión y decodificar tramas en la recepción.

2.3.3.1 Formatos de Trama MAC

Cada trama consiste de los siguientes componentes básicos:

- Un encabezado MAC, comprende el control de trama, duración, dirección y la información de control de secuencia.
- Un cuerpo de trama de longitud variable, el cual contiene la información especifica para el tipo de trama.
- Una secuencia de chequeo de trama (FCS), que contiene un código de redundancia cíclica de 32 bits (CRC).

2.3.3.1.1 Formato de Trama General

Los formatos de trama MAC comprenden un conjunto de campos que ocurren en un orden fijo en todas las tramas.

Los campos Dirección 2, Dirección 3, Control de Secuencia, Dirección 4 y Cuerpo de Trama están solo presentes en ciertos tipos de tramas.

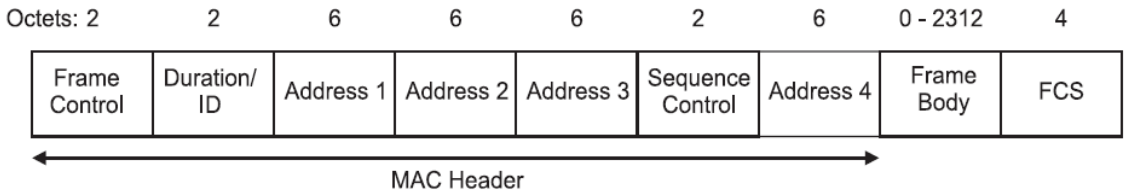


Figura 2.45. Formato de Trama MAC

2.3.3.1.2 Campos de Trama

2.3.3.1.2.1 Frame Control

El campo de control de trama consiste de los siguiente sub campos: Protocol Version, Type, Subtype, To DS, From DS, More Fragmentes, Retry, Power Managment, More Data, Protected Frame; y, Order.

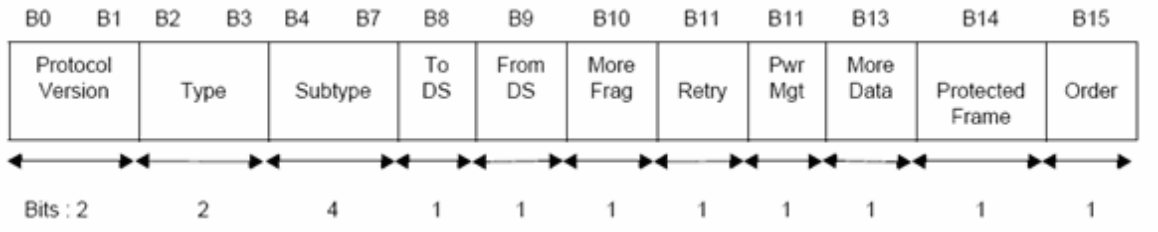


Figura 2.46. Campo de Control de Trama

Protocol Version.- Este campo tiene una longitud de 2 bits, para este estándar su valor es de 0. Todos los demás valores están reservados para futuros usos, un dispositivo que reciba una versión superior a la que puede soportar, descartara la trama sin indicar a la estación de origen o al LLC.

Type y Subtype.- El campo type es de 2 bits de longitud, mientras que el subtype de 4; entre ambos campos identifican la función de la trama; existen tres tipos de tramas: control, datos y gestión. Cada tipo de tramas tiene varios subtipos.

To DS.- Este es un campo de 1 bit, tiene el valor de “1” en tramas de tipo de datos destinadas al DS; esto incluye todas las tramas de tipo de datos enviadas por estaciones asociadas con un AP; este campo es “0” para todas las demás tramas.

From DS.- Al igual que el campo anterior este posee una longitud de 1 bit, tiene el valor de “1” para las tramas de tipo de datos que existen en el DS, y el valor de “0” para el resto de tramas.

More Fragments.- Este parámetro posee una longitud de 1 bit, cuando toma el valor de “1”, los MSDU tienen otro fragmento a continuación, toma el valor de “0” para otro tipo de tramas.

Retry.- Este parámetro toma el valor de “1” cuando la trama ya sea de datos o gestión es una retransmisión de una trama anterior, para cualquier otro tipo toma valores de “0”, este parámetro sirve como indicativo para ayudar a eliminar tramas duplicadas, su longitud es de 1 bit.

Power Management.- Este campo nos ayuda a establecer el modo de manejo de potencia de una estación, este campo se mantiene invariable durante el intercambio de tramas de una estación durante una secuencia definida; el valor indica el modo en el cual la estación estará después de una secuencia de intercambio de tramas exitosa.

Un valor de “1” indica que la estación estará en modo de ahorro de energía; el valor de “0” indica que la STA estará en modo activo, este campo siempre tendrá el valor de “0” cuando las tramas son transmitidas desde un AP.

More Data.- Al igual que los anteriores este campo tiene una longitud de 1 bit, este campo es usado para indicar a una estación en modo de ahorro de energía que más MSDU o MMPDU están en el buffer del AP para esta STA. El valor de “1” indica que al menos una MSDU o MMPDU están el buffer.

En transmisiones broadcast/multicast desde un AP, este campo toma el valor de “1”, para indicar que aun quedan MSDU o MMPDU a ser transmitidos, este campo toma el valor de “0”, para todas las demás tramas y en caso de que existan transmisiones broadcast/multicast desde cualquier estación que no sea AP.

Protected Frame.- Este campo toma valores de “1” cuando la información contenida en el campo Frame Body haya sido procesado por un algoritmo de encapsulación

criptográfica; este campo toma valores de 1 solo cuando se trata de tramas de datos y tramas de gestión, subtipo autenticación; el valor de “0”, es tomado por este campo en todas las demás tramas. Cuando el campo protected frame tiene el valor de “1” en la trama de datos, el campo Frame Body queda protegido utilizando el algoritmote encapsulación criptográfica; solamente WEP puede usar dicho algoritmo para las tramas de gestión de subtipo autenticación.

Order.- Este es el ultimo sub campo del campo Frame Control, y tiene una longitud de 1 bit, toma el valor de “1” en cualquier trama de tipo dato que contiene MSDU, o fragmentos del mismo, los cuales están siendo transmitidos usando la clase de servicio de orden estricto; toma el valor de “0” para el resto de tramas.

2.3.3.1.2.2 Duration/ID

Este es un campo con una longitud de 16 bits, este campo posee los siguientes contenidos:

En tramas de tipo control, con subtipo Power Save (PS)-Poll, este campo contiene la identificación de asociación (AID) de la estación que transmite la trama en los 14 bits menos significativos, y en los 2 más significativos lleva los valores de “1”; el AID tiene un rango de 1 a 2007.

En las demás tramas, este campo contiene un valor de duración; para las tramas transmitidas durante el contention-free period (CFP), este campo tiene el valor de 32768.

En el caso de que este campo tenga valores menores 32768, el valor de duración es usado para actualizar el vector de ubicaron de red (NAV).

2.3.3.1.2.3 Address

Existen cuatro campo de direcciones en el formato de trama MAC, estos campos son usados para indicar el BSSID, estos cuatro campos de direcciones son la dirección de origen, dirección de destino, dirección de la estación de transmisión y la dirección de la estación de recepción.

El uso de estas cuatro direcciones para cada tipo de trama se indica mediante las siglas BSSID, DA, SA, RA, y TA, cabe destacar que ciertos tipos de tramas no contienen algunos de los campos de direcciones.

Una dirección de subcapa MAC puede ser una de las siguientes dos:

Dirección Individual.- Una dirección asociada con una estación en particular de la red.

Dirección de Grupo.- Una dirección de multi-destino, asociada a una o más estaciones en una red dada. A su vez este tipo de dirección puede tener dos clases:

- Dirección Multicast-group.- Es una dirección asociada por una convención de nivel superior con un grupo de estaciones relacionadas lógicamente.
- Dirección de Broadcast.- Una dirección de multitas distinguida que siempre denota a todo un grupo de estaciones dentro de una red dada; cuando todos los campos de la dirección de destino tienen el valor de 1, se interpreta a esta como una dirección de broadcast; el grupo esta definido, por todas las estaciones activas dentro del medio de comunicación; todas las estaciones pueden reconocer una dirección de broadcast, aunque no estén en capacidad de generar una.

2.3.3.1.2.3.1 Campo BSSID

Este campo tiene una longitud de 48 bits, con el mismo formato que una dirección MAC, identifica de forma única a cada BSS, el valor de este campo en una BSS infraestructura es la dirección MAC en uso por la estación el en AP de la BSS.

El valor de este campo en una IBSS es una dirección MAC administrada localmente formada por 46 bits escogidos de forma aleatoria, mientras que los restantes dos bits toman el valor de 0 para el bit individual/grupal y 1 para el bit universal/local; este mecanismo tiene una alta probabilidad de seleccionar una BSSID única.

Cuado se tiene todos “1”, se indica la dirección de broadcast BSSID, esta puede ser solamente usada en el campo BSSID de las tramas de gestión de subtipo probe request.

2.3.3.1.2.3.2 Campo Destination Address (DA)

Este campo contiene una dirección MAC ya sea individual o de grupo que identifica la entidad o entidades MAC destinadas a ser el recipiente final de las MSDU o fragmentos de estos que viene en el campo frame body.

2.3.3.1.2.3.3 Campo Source Address (SA)

Contiene una dirección MAC individual que identifica a la entidad MAC desde la cual la transmisión de MSDU o fragmentos contenidos en el frame body se iniciaron, el bit individual/grupal siempre se transmitirá como “0” en la dirección de origen.

2.3.3.1.2.3.4 Campo Receiver Address (RA)

Este campo contiene una dirección MAC ya sea individual o grupal que identifica la estación o estaciones destinadas a ser el recipiente inmediato en el medio inalámbrico, de la información del frame body.

2.3.3.1.2.3.5 Campo Transmitter Address (TA)

El campo TA contiene la dirección MAC individual que identifica a la estación que ha transmitido, al medio inalámbrico las MPDU del frame body; el bit individual/grupal siempre se transmite como “0” en la dirección de transmisor.

2.3.3.1.2.4 Sequence Control

Este es un campo de 16 bits de longitud y consiste de dos sub campos, el primero Sequence Number y Fragment Number, a estos se le puede apreciar de mejor manera en la siguiente grafica.

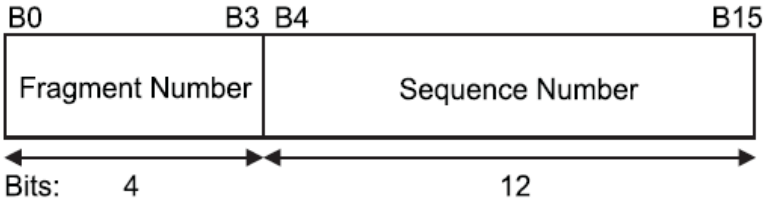


Figura 2.47. Campo Sequence Control

Sequence Number.- Tiene una longitud de 12 bits, nos indica el número de secuencia de un MSDU o MMPDU, debido a que a cada MSDU o MMPDU se le asigna un número de secuencia al ser transmitido, estos números de secuencia son asignados de un contador de modulo 4096, empezando desde 0 e incrementándose de a 1 por cada MSDU o MMPDU, cada fragmento de un MSDU o MMPDU contiene el número de secuencia asignado; el número de secuencia permanece constante en todas las retransmisiones de una MSDU, MMPDU o fragmentos.

Fragment Number.- Este sub campo tiene una longitud de 4 bits, e indica el número de cada fragmento de un MSDU o MMPDU; el número de fragmento tiene el valor de 0 en el primer o único fragmento, y se incrementa en uno por cada fragmento sucesivo; el número del fragmento permanece constante en todas las retransmisiones del fragmento.

2.3.3.1.2.5 Frame Body

Este es un campo de longitud variable, contiene la información específicamente para tipos de trama y subtipos; el tamaño mínimo de este campo es de cero octetos, mientras que el máximo esta definido por la longitud máxima de MSDU+ICV+IV

2.3.3.1.2.6 FCS

El campo FCS tiene 32 bits los cuales contienen un CRC de 32 bits; este campo es calculado a partir de todos los campos del encabezado MAC y el campo frame body, nos referiremos a estos como campos de calculo.

El FCS se calcula usando el siguiente polinomio generador estándar de grado 32:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Formula 2.18. Polinomio Generador Estándar FCS

El FCS es el complemento a 1 de la suma en modulo 2 de estos dos campos:

- El residuo de $x^k \times \left(x^{31} + x^{30} + x^{29} + ... + x^2 + x + 1\right)$ divido en modulo 2 para *G(x)*, donde k es el número de bits de los campos de calculo.
- El residuo después de la multiplicación de los contenidos de los campos de cálculo (tomados como polinomios) por x^{32} y dividido para *G(x)*.

El campo FCS es transmitido con el coeficiente del término de mayor orden.

2.3.3.2 Formato de Tipos de Tramas Individuales

2.3.3.2.1 Tramas de Control

Existen varias tramas de control, cada una con diferentes campos, sin embargo todas las tramas poseen un campo en general es el Frame Control, a continuación se presenta la descripción de este campo para las tramas de control.

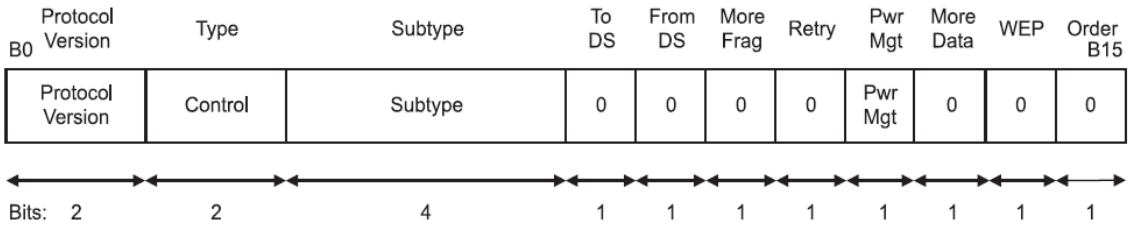


Figura 2.48. Descripción del Campo Frame Control para Tramas de Control

Debido a la gran cantidad de tramas de control, no se verán con detalle, tan solo una descripción de los campos que poseen las mismas.

Trama Request To Send (RTS).-

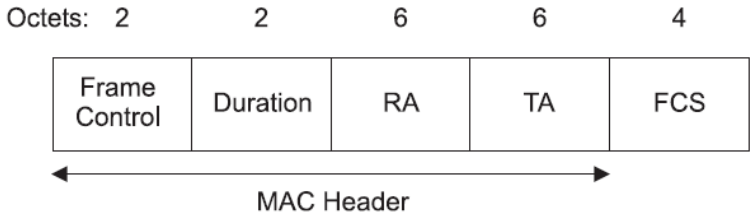


Figura 2.49. Campos de la Trama RTS

Trama Clear To Send (CTS).-

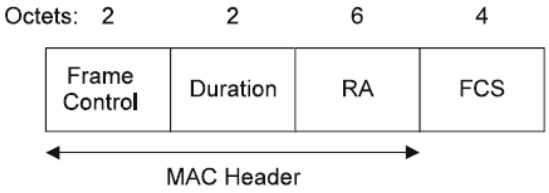


Figura 2.50. Campos de la Trama CTS

Trama Acknowledgment (ACK).-

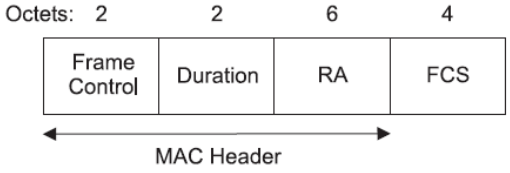


Figura 2.51. Campos de la Trama ACK

Trama Power-Save Poll (PS-Poll).-

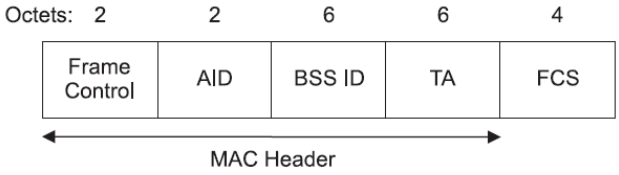


Figura 2.52. Campos de la Trama PS-Poll

Trama CF-End.-

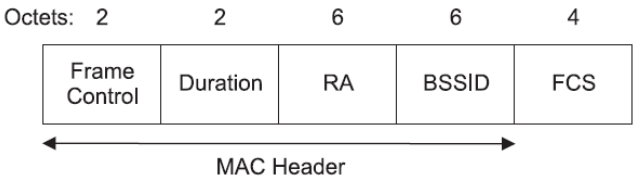


Figura 2.53. Campos de la Trama CF-End

Trama CF-End + CF-Ack.-

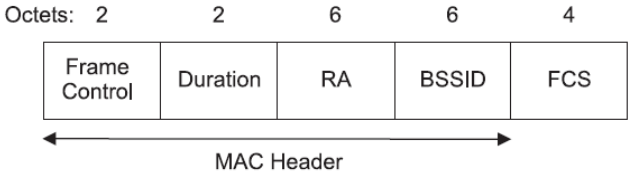


Figura 2.54. Campos de la Trama CF-End + CF-Ack

2.3.3.2.2 Tramas de Datos

El formato de las tramas de datos es independiente de los subtipos, se puede apreciar el formato de las tramas de datos en la siguiente grafica.

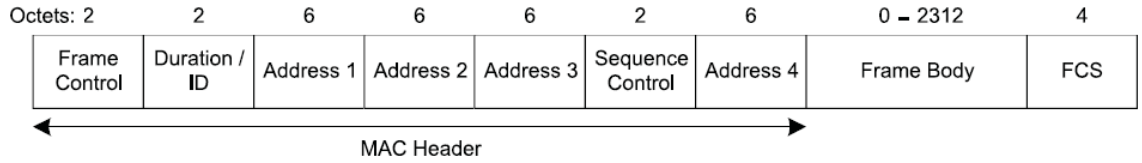


Figura 2.55. Formato de las Tramas de Datos

El contenido de los campos de direcciones es dependiente de los valores que se presenten en los campos To DS y From DS; cabe mencionar que en algunos casos, puede que los campos de direcciones no lleven ninguna dirección y por lo tanto sean omitidos; el campo address 1 lleva siempre direcciones de recepción y address 2 direcciones de transmisión.

TO DS	FROM DS	ADDRESS 1	ADDRESS 2	ADDRESS 3	ADDRESS 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Tabla 2.36. Contenidos de los Campos de Direcciones[70]

Una estación usa el contenido address 1 para realizar comparaciones de direcciones para tomar decisiones de recepción; en casos donde el campo contenga direcciones grupales, el BSSID es validado para asegurar que el multicast o broadcast se origina en el mismo BSS. Las estaciones usan el address 2 para dirigir el ACK si es necesario; el DA es el destino del MSDU en el campo frame body; el SA es la dirección de la entidad MAC que inicia el MSDU; RA es la dirección de la estación contenida en el AP en el sistema de distribución inalámbrico, que es el siguiente recipiente de la trama inmediato; TA es la dirección de la estación contenida en el AP en el sistema de distribución inalámbrica que esta transmitiendo la trama.

BSSID en las tramas de datos esta determinada de la siguiente manera:

- Si la estación en un AP o esta asociada con un AP, la BSSID es la dirección en uso actual por la estación contenida en el AP.
- Si la estación es un miembro de una IBSS, la BSSID es la BSSID de la IBSS.

[70] IEEE 802.11, Institute of Electrical and Electronics Engineers, Pág. 44.

Con todas las tramas de tipo datos, en un CFP, el campo de duración tiene el valor de 32768, mientras que con todas las tramas tipo datos transmitidas durante el periodo de contención, el campo de duración se rige por las siguientes reglas:

- Si el campo address 1 contiene un grupo de direcciones, el valor de duración es de 0
- Si el bit More Fragments tiene el valor de 0, y el campo address 1 tiene una dirección individual, el valor del campo duration tiene el tiempo en microsegundos que se requieren para transmitir una trama ACK, más un intervalo SIFS.
- Si el bit de More Fragments tiene un valor de 1, y el campo address 1 lleva una dirección individual, el valor del campo duration lleva el tiempo en microsegundos que se necesitan para transmitir el siguiente fragmento de esta trama de datos, más dos tramas de ACK y tres intervalos de SIFS.

2.3.3.2.3 Tramas de Gestión

Al igual que el caso de las tramas de datos, las de gestión son independientes del subtipo de trama, se puede ver el formato de la trama de gestión en la siguiente grafica:

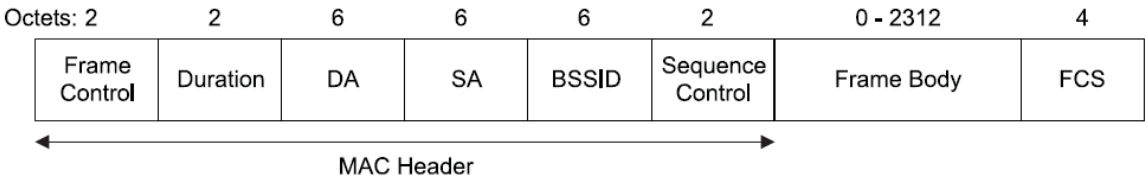


Figura 2.56. Formato de la Tramas de Gestión.

Una estación usa el contenido del campo address 1 para realizar una correspondencia de direcciones con las direcciones de recepción; en el caso en que este campo tenga un grupo de direcciones y el tipo de tramas diferente a Beacon, el BSSID también es validado para asegurarse de que el broadcast o multicast este dentro del mismo BSS; si es de tipo Beacon, se usan otras reglas de correspondencia.

El BSSID en las tramas de gestión se determina de la siguiente manera:

- Si la estación es un AP o esta asociada a un AP, el BSSID es la dirección que se encuentre en uso por la estación contenida en el AP.
- Si la estación es un miembro de algún IBSS, el BSSID es el BSSID del IBSS.

- En tramas de gestión de subtipo Probe Request, el BSSID es ambos, un BSSID específico o el BSSID de broadcast.

El DA es el destino de la trama; SA es la dirección de la estación que transmite la trama.

En todas las tramas que pasan en un CPF, el campo Duration tiene el valor de 32768, mientras que en las tramas de gestión que pasen durante el periodo de contención, el campo de duración se rige mediante las siguientes reglas:

- Si el campo DA contiene un grupo de direcciones, el valor de Duration es de 0.
- Si el bit More Fragments es 0 y el campo DA contiene una dirección individual, el valor del campo de duración es el tiempo en microsegundos requerido para la transmisión de la trama ACK, más un intervalo SIFS.
- Si el bit More Fragments tiene el valor de 1 y el campo DA lleva consigo una dirección individual, el campo de duración lleva el tiempo en microsegundos requerido para la transmisión del siguiente fragmento, más dos tramas ACK y tres intervalos SIFS.

El campo frame body consiste en campos fijos y elementos de información para cada subtipo de trama de gestión, todos estos elementos y campos son obligatorios a menos que se especifique lo contrario. Estos campos y elementos debe aparecer en las tramas en un orden específico, en caso de que no se entienda algún campo de las tramas, este se ignora y en caso de tener valores reservados, simplemente no aparece en las tramas.

2.3.3.3 Componentes del Frame Body de Gestión

Dentro de las tramas de gestión, los componentes del frame body obligatorios de longitud fija, son definidos como campos fijos, mientras que los obligatorios de longitud variable y todos los componentes del frame body opcionales están definidos como elementos de información.

2.3.3.3.1 Campos Fijos

Debido a la extensión de estos campos, se dejara a discreción del lector la investigación más detenida de estos campos, por el momento se listaran dichos campos:

Authentication Algorithm Number

- Authentication Transaction Sequence Number
- Beacon Interval
- Capability Information
- Current AP Address
- Listen Interval
- Reason Code
- Association ID
- Status Code
- Timestamp

2.3.3.3.2 Elementos de Información

Estos elementos están definidos de tal forma que posean un formato general, el cual consiste de un octeto para el campo Element ID, un octeto para el campo Length, y un campo de longitud variable especifica de cada elemento para el campo Information.

El campo Length especifica el número de octetos que tendrá el campo Information.

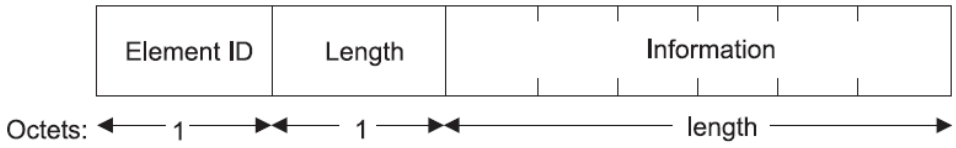


Figura 2.57. Formato de los Elementos de Información.

Una vez que se conoce el formato de los elementos de información, se mostraran cuales son los dichos elementos con la ayuda de la siguiente tabla:

ELEMENTO DE INFORMACIÓN	ELEMENT ID
SSID	0
Supported rates	1
FH Parameter Set	2
DS Parameter Set	3
CF Parameter Set	4
TIM	5
IBSS Parameter Set	6
Reserved	7-15
Challenge text	16
Reserved (Challenge text extension)	17-31
Reserved	32-42
Reserved	43-47
RSN	48
Reserved	49-255

Tabla 2.37. Elementos de Información

2.3.4 Seguridad

2.3.4.1 Framework

En esta parte del documento revisaremos dos clases de algoritmos de seguridad para las redes WiFi:

- ✓ Algoritmos creados para usar una RSNA, denominados algoritmos RSNA
- ✓ Algoritmos Pre-RSNA

2.3.4.1.1 Métodos de Seguridad

En la seguridad Pre-RSNA se tiene los siguientes algoritmos:

- WEP
- Autenticación de entidad 802.11

Mientras que en la seguridad RSNA se usan los siguientes algoritmos:

- TKIP
- CCMP
- Procedimientos de establecimiento y terminación RSNA, incluyendo autenticación 802.1X
- Procedimiento de manejo de llave

2.3.4.2 Métodos de Seguridad Pre-RSNA

Excepto por la autenticación de sistema abierto, todos los mecanismos de seguridad Pre-RSNA han descontinuados debido a que han fallado en cumplir con sus metas de seguridad; nuevas implementaciones deben soportar métodos Pre-RSNA solo como ayuda para la migración a métodos RSNA.

2.3.4.2.1 Wired Equivalent Privacy (WEP)

WEP-40 fue definido como un método para proteger la confidencialidad del intercambio de datos usando una llave de 40 bits, entre usuarios autorizados de una red inalámbrica; la implementación WEP es opcional; los mismos algoritmos han sido utilizados ampliamente con llaves de 104 bits en vez de 40 bits en implementaciones de campo, se le conoce como WEP-104.

2.3.4.2.1.1 Formato MPDU WEP

El algoritmo WEP encripta el frame body de la siguiente manera:

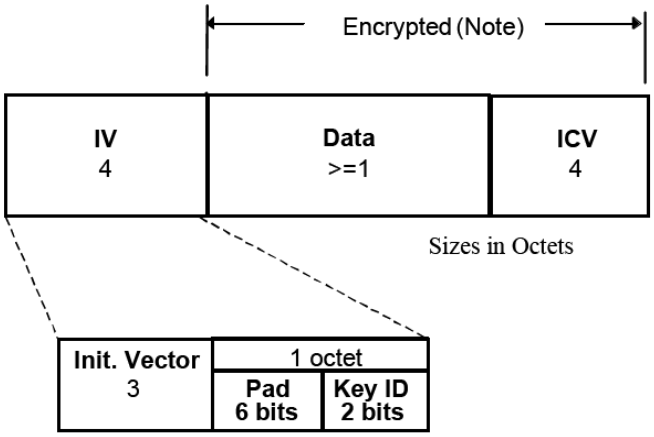


Figura 2.58. Construcción del MPDU WEP Extendido

El campo ICV WEP debe tener 32 bits de longitud, el frame body extendido debe empezar con el campo IV de 32 bits; este campo debe contener tres sub campos: el primero de 3 octetos que contiene el vector de inicialización (IV), el segundo de 2 bits llamado Key ID, y el tercero de 6 bits llamado Pad.

El sub campo Key ID contiene uno de los cuatro posibles valores de una llave secreta usada para desencriptar el frame body; cuando las llaves key-mapping se usan, el valor de Key ID se ignora.

El contenido del sub campo Pad debe ser 0; mientras que el sub campo Key ID ocupa los 2 bits más significativos del ultimo octeto en el campo IV, y Pad los 6 bits menos significativos.

2.3.4.2.1.2 Estados WEP

WEP usa solamente llaves de encriptación, no realiza autenticación; WEP usa dos tipos de llaves de encriptación: llaves key-mapping y llaves fijas.

Una llave key-mapping en una llave sin nombre correspondiente a distintos pares de direcciones de transmisión y recepción; se debe usar estas llaves si se configura pares de direcciones; se debe usar estas llaves key-mapping para poder encriptar y desencriptar las MPDU transmitidas por las direcciones, pese a la presencia de otras llaves, al optar por este tipo de llaves el valor del sub campo Key ID debe ser 0 e ignorado en la recepción.

El otro tipo de llave que se puede usar para encriptar y desencriptar los MPDU, es la llave fija, el sub campo Key ID lleva los valores de 0, 1, 2 o 3; estos valores sirven para que el receptor obtenga la llave fija apropiada; todas las implementaciones WEP deben soportar las llaves fijas.

2.3.4.2.1.3 Encapsulación MPDU WEP

WEP debe realizar tres transformaciones al texto de entrada MPDU para alcanzar la encapsulación WEP, se computa la ICV con el texto de entrada y se les añade después de los datos MPDU; WEP encripta los datos de texto de entrada MPDU y el ICV usando RC4 junto con la semilla. WEP codifica el IV y el identificador de llave en el campo IV, poniéndolo al principio del campo encripted data.

El ICV debe ser computado y colocado al principio de los datos de texto de entrada previa encriptación, pero la codificación IV puede realizarse en cualquier orden, según la conveniencia de la implementación.

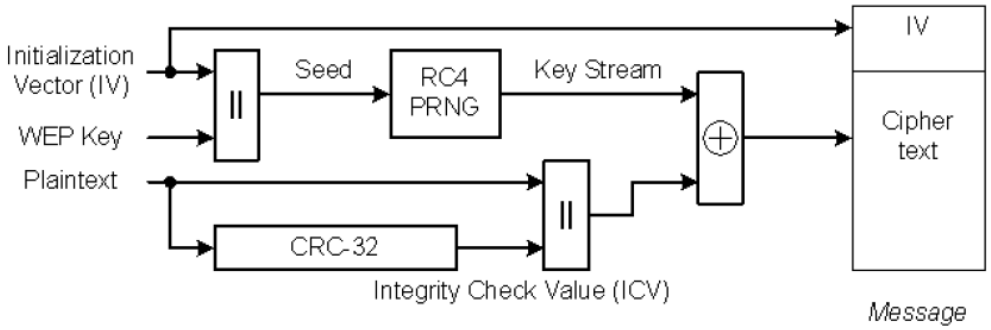


Figura 2.59. Diagrama de bloques del Encapsulamiento WEP

2.3.4.2.1.4 Desencapsulamiento MPDU WEP

WEP debe realizar tres transformaciones al MPDU WEP para poder lograr el desencapsulamiento de la carga; WEP extrae el IV y el identificador de llave de los MPDU recibidos; si una llave tipo key-mapping esta presente, esta debe ser usada como la llave WEP, de lo contrario, el identificador de llave se extrae del sub campo Key ID del campo WEP IV, de esta manera se identifica la llave fija a ser usada.

WEP usa la semilla construida para desencriptar el campo de datos de la MPDU WEP, esto produce los datos de texto de entrada y un ICV; finalmente WEP recalcula el ICV y compara bit a bit con el ICV desencriptado a partir del MPDU; si los dos son idénticos, WEP retira el IV e ICV del MPDU, y se lo acepta como valido; en caso de tener alguna diferencia en un bit, WEP genera un indicador de error al gestionador MAC.

Si debido a incapacidades de desencriptación las MPDU de un MSDU no deben pasar al LLC.

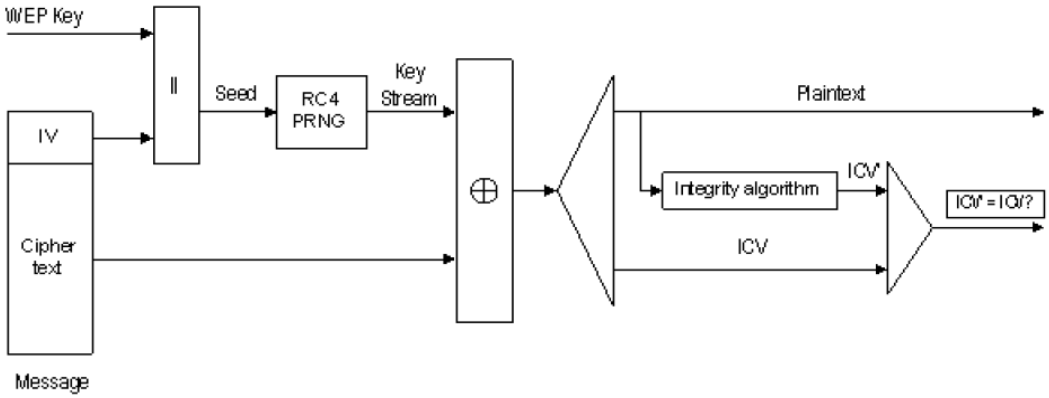


Figura 2.60. Diagrama de Bloques del Desencapsulamiento WEP

2.3.4.2.2 Autenticación Pre-RSNA

En una ESS, una estación no AP y un AP deben completar un intercambio de autenticación 802.11 previa su asociación, este intercambio es opcional en una red IBSS.

Todas las tramas de gestión de subtipo autenticación deben ser unicast, debido a que la autenticación WiFi se realiza entre parejas de estaciones, la autenticación broadcast/unicast no esta permitida; estas tramas son de aviso y pueden ser enviadas como una trama con direcciones grupales.

La autenticación de llave compartida ha sido descontinuada y no debe ser implementada excepto para aquellos casos en los que se requiera compatibilidad con dispositivos previos a la utilización de RSNA.

2.3.4.2.2.1 Autenticación de Sistema Abierto

La autenticación de sistema abierto es un algoritmo de autenticación nulo; cualquier estación pidiendo por autenticación de sistema abierto debe ser autenticada si la estación recipiente tiene una autenticación de sistema abierto. Una estación puede negarse a autenticarse con otra estación que solicite autenticación. La autenticación de sistema abierto es el algoritmo de autenticación predefinido para equipos previos a la utilización de RSNA.

La autenticación de sistema abierto utiliza una secuencia de transacción de dos mensajes; el primer mensaje confirma la identidad y pide autenticación; el segundo

mensaje devuelve el resultado de la autenticación; si el resultado es exitoso, las estaciones deben declararse mutuamente autenticadas.

2.3.4.2.2.1.1 Primera Trama de la Autenticación de Sistema Abierto

Tipo de Mensaje: Gestión.
Subtipo de Mensaje: Autenticación.
Ítems de Información: Identificador de algoritmo de autenticación = “Open System”; confirmación de identidad de la estación; número de secuencia de transacción de autenticación = 1; información dependiente del algoritmo de autenticación (ninguno).
Dirección del Mensaje: De estación que pide la autenticación a la estación que responde.

2.3.4.2.2.1.2 Trama Final de la Autenticación de Sistema Abierto

Tipo de Mensaje: Gestión.
Subtipo de Mensaje: Autenticación.
Ítems de Información: Identificador de algoritmo de autenticación = “Open System”; número de secuencia de transacción de autenticación = 2; información dependiente de algoritmo de autenticación (ninguno); el resultado de al petición de autenticación.
Dirección del Mensaje: de la estación que responde a la estación que pide la autenticación.

2.3.4.2.2.2 Autenticación de Llave Compartida

La autenticación de llave compartida busca la autenticación de estaciones, tanto de las que son miembros de aquellas que comparten una llave secreta como de aquellas que no.
La autenticación de llave compartida puede ser usada si y solo si WEP a sido seleccionada.

Este mecanismo usa una entrega de llave compartida a las estaciones participantes, mediante un canal seguro que es independiente de 802.11; esta llave compartida esta colocada en una MIB de atributo solo escritura en un intento de mantener el valor de la llave interno a la estación.

2.3.4.2.2.2.1 Primera Trama de la Autenticación de Llave Compartida

Tipo de Mensaje: Gestión.
Subtipo de Mensaje: Autenticación.

Ítems de Información: Confirmación de la identidad de estación; identificación de algoritmote autenticación = “Shared Key”; número de secuencia de transacción de autenticación = 1; información dependiente de algoritmo de autenticación (ninguno).
Dirección del Mensaje: Desde la estación pidiendo al autenticaron a la estación que responde.

2.3.4.2.2.2.2 Segunda Trama de la Autenticación de Llave Compartida

Antes de enviar la segunda trama en la secuencia de autenticación, la estación que responde debe usar WEP para generar una cadena de octetos para ser usados como el texto de prueba de autenticación.

Tipo de Mensaje: Gestión.
Subtipo de Mensaje: Autenticación.
Ítems de Información: Identificación de algoritmo de autenticación = “Shared Key”; número de secuencia de transacción de autenticación = 2; información dependiente de algoritmo de autenticación = el resultado de la autenticación; el codigo resultante de la petición de autenticación.

Si el código de estado no es “exitoso”, esta debe ser la ultima trama de la secuencia; y el contenido del campo texto reprueba no esta especificado. Si el código de estado es “exitoso”, los siguientes ítems de información adicional deben tener contenidos validos:

Información dependiente de algoritmo de autenticación = el texto de prueba.

Este resultado de la autenticación debe tener una longitud de 128 octetos, deben estar llenos de octetos generados por el PRNG WEP; el valor exacto del campo de prueba no es importante, pero dicho valor no debe ser estático.

2.3.4.2.2.2.3 Tercera Trama de la Autenticación de Llave Compartida

La estación que pide la autenticación debe copiar el texto de prueba de la segunda trama en la tercera; la tercera trama debe ser transmitida después de la encapsulación WEP usando la llave compartida.

Tipo de Mensaje: Gestión.
Subtipo de Mensaje: Autenticación.
Ítems de Información: Identificación de algoritmo de autenticación = “Shared Key”; número de secuencia de transacción de autenticación = 3; información dependiente de algoritmo de autenticación = el texto de prueba de la segunda trama.
Dirección del Mensaje: De la estación que pide la autenticación a la estación que responde.

2.3.4.2.2.2.4 Trama Final de la Autenticación de Lave Compartida

La estación que responde debe realizar el desencapsulamiento WEP de la tercera trama; si la revisión del ICV WEP resulta exitosa, esta estación debe comparar el contenido desencriptado del texto de prueba con el enviado en la segunda trama; si resultan ser los mismos, entonces esta estación responde con un código de estado exitoso en la trama final; en caso de que el ICV o el texto de prueba fallen, la estación que responde debe enviar un código de estado fallido en la trama final.

Tipo de Mensaje: Gestión.
Subtipo de Mensaje: Autenticación.
Ítems de Información: Identificador de algoritmo de autenticación = “Shared Key”; número de secuencia de transacción de autenticación = 4; información dependiente de algoritmo de autenticación = el resultado de la autenticación; el código resultante de la petición de autenticación.
Dirección del Mensaje: De la estación de respuesta hacia la estación que pode la autenticación.

2.3.4.3 Protocolos de Confidencialidad de Datos RSNA

Vamos a revisar dos protocolos de integridad y confidencialidad: TKIP y CCMP; cabe destacarse que la implementación de CCMP es obligatoria en aquellos equipos que posean RSNA; mientras que TKIP es opcional, pero debe correr bajo WEP, para que los equipos que únicamente soportan WEP sean capaces de actualizarse.

2.3.4.3.1 Temporal Key Integrity Protocol (TKIP)

TKIP es una mejora al sistema de cifrado del protocolo WEP bajo el hardware pre-RSNA; entre las modificaciones que presenta TKIP a WEP están las siguientes:

- El transmisor calcula un código de integridad de mensaje (MIC) de criptografía con llave en el MSDU de las direcciones de origen y destino, la prioridad MSDU y los datos de entrada MSDU. TKIP anexa el MIC calculado a los datos MSDU previa la fragmentación en MPDU; el receptor verifica el MOC después de la desencripción, chequeo de ICV y de fragmentación de los MPDU en MSDU y procede a descartar cualquier MSDU recibido con un MIC inválido. En otras palabras TKIP brinda la protección necesaria contra los ataques exteriores.
- Debido a las limitaciones de diseño del MIC, aun es posible para una terminal ajena comprometer la integridad de los mensajes, por los que TKIP también implementa contramedidas; estas contramedidas comprometen la probabilidad ataque y la cantidad de información que se puede interceptar mediante una llave.
- TKIP usa un contador de secuencia TKIP (TSC) de pares MPDU, para las secuencias de MPDU que envía; el receptor desecha los MPDU recibidos fuera de orden sin incremento en los números de secuencia; ofreciendo protección contra las reejecuciones; estos TSC son codificados como una IV WEP e IV extendidos.
- TKIP usa una función mixta de criptografía para combinar la llave temporal, la dirección de transmisión (TA) y el TSC en la semilla WEP; el receptor recupera la TCS de una MPDU recibida y utiliza la función mixta para calcular la misma semilla WEP necesaria para desencriptar la MPDU; esta función de llave mixta esta diseñada para no sufrir daño de ataques débiles de llave contra la llave WEP.

2.3.4.3.1.1 Encapsulación TKIP

Como se menciono anteriormente, TKIP mejora WEP, esto incluye la encapsulación, entre las mejoras podemos encontrar las siguientes:

- En calculo del MIC TKIP protege a los campos de datos MSDU, SA, DA y prioridad; el calculo del MIC se realiza sobre la concatenación ordenada de SA, DA, prioridad y datos MSDU; luego se anexa a los datos MSDU; TKIP descarta cualquier rastro de MIC previa su anexión.
- En caso de ser necesario 802.11 fragmenta los MSDU en uno o más MPDU, por lo que TKIP le asigna un valor TSC incrementado consecutivamente a cada MPDU,

tomando en cuenta que todas las MPDU generadas a partir de un mismo MSDU tengan el mismo valor de IV extendido.

- Para cada MPDU, el protocolo TKIP usa la función mixta de llave para calcular la semilla WEP.
- TKIP representa la semilla WEP como una IV WEP y llave RC4, pasándola con cada MPDU hasta WEP para la generación del ICV, y la encripción del texto de entrada MPDU, ya sea con todo o parte del MIC; WEP usa la semilla como la llave fija WEP, identificada por un identificador de llave asociado con la llave temporal.

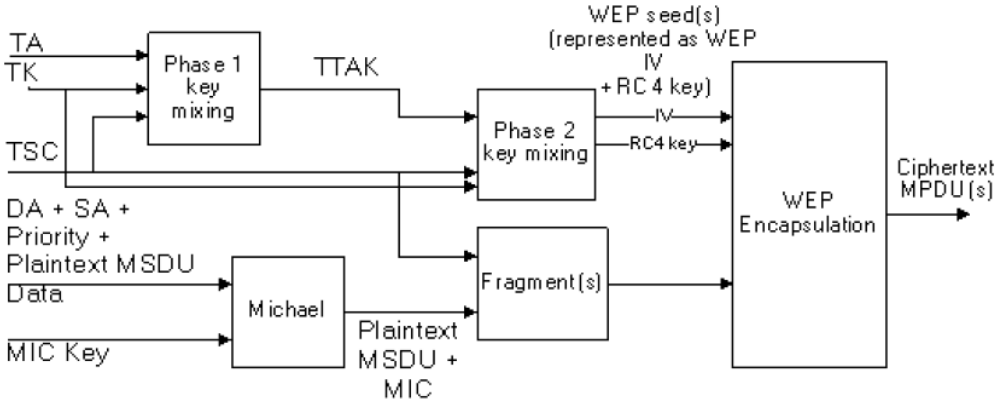


Figura 2.61. Diagrama de Bloques de la Encapsulación TKIP

2.3.4.3.1.2 Desencapsulamiento TKIP

Las mejoras al desencapsulamiento WEP son las siguientes:

- Antes de realizar la desencapsulación de una MPDU recibida, TKIP extrae el número de secuencia TSC y el identificador de llave del IV WEP y el IV extendido, se descarta los MPDU que violen las reglas de secuencia, caso contrario usa la función mixta para construir la semilla WEP.
- TKIP representa la semilla como una IV WEP y llave RC4, la pasa junto al MPDU hasta WEP para la desencapsulación.
- Si WEP indica una revisión exitosa del ICV, la implementación reensambla el MPDU en un MSDU; si la de fragmentación MSDU tiene éxito, el receptor verifica el MIC, en caso de falla en la de fragmentación se descarta el MSDU.
- El paso de verificación MIC recalcula el MIC a partir de la SA, DA, Priority y datos MSDU (sin el MIC); calcula el MIC resultante y lo compara bit a bit con el MIC recibido.

- Si el MIC recibido y el local son idénticos, la verificación es exitosa, y el TKIP debe entregar el MSDU a la capa superior, si difieren, la verificación falla y el receptor debe descartar el MSDU y debe tomar las correspondientes contramedidas.

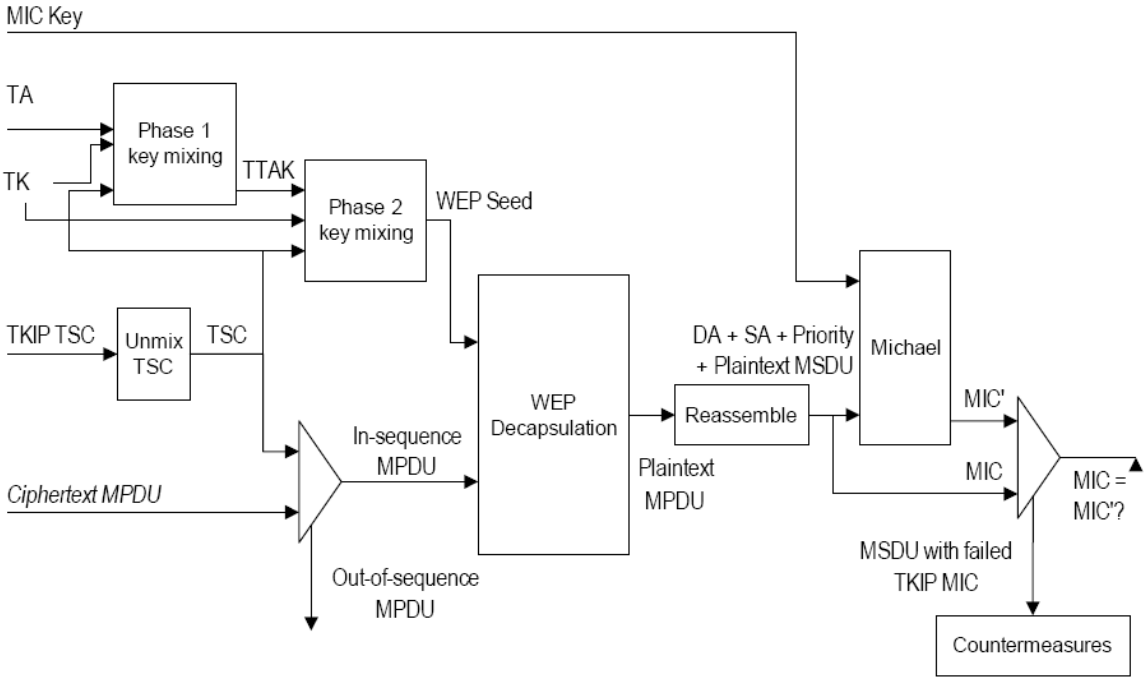


Figura 2.62. Diagrama de Bloques de la Desencapsulación TKIP

2.3.4.3.1.3 Formatos MPDU TKIP

TKIP vuelve a usar el formato MPDU WEP pre-RSNA, pero extiende el MPDU en 4 octetos para acomodar la extensión del IV WEP, al cual se le denomina IV extendido, además extiende el formato MSDU en 8 octetos para acomodar el nuevo campo MIC, quedando el IV extendido inmediatamente después del IV WEP y antes de los datos encriptados; por otro lado el MIC es anexado a los datos MSDU, formado parte de los datos encriptados.

Una vez que el MIC es anexado a los datos MSDU, estos octetos son considerados parte de los mismos a al hora de la de fragmentación.

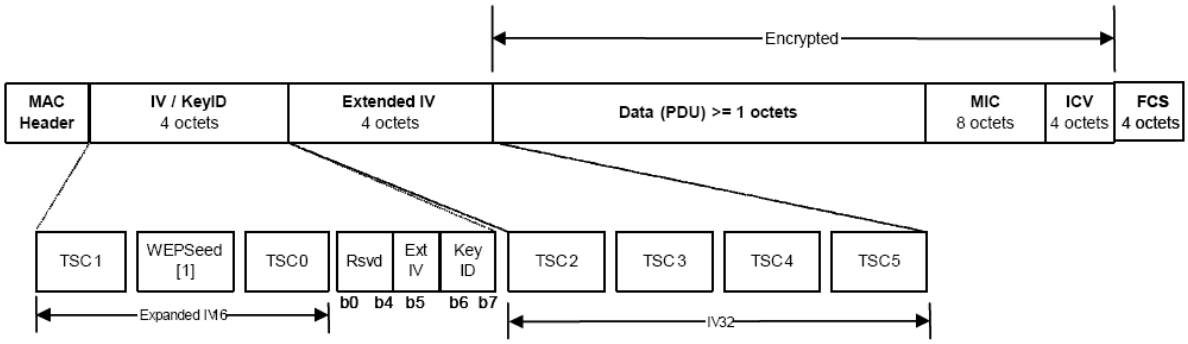


Figura 2.63. Formato de la MPDU TKIP

El bit ExtIV del campo Key ID indica la presencia o no del IV extendido, si este bit tiene el valor de “0”, solo la IV WEP es transmitida y si es “1” se transmite tanto la IV WEP como la IV extendida; en equipos con capacidad TKIP este bit siempre debe ser “1”, a menos que se use solo WEP.

TSC5 es el octeto más significativo, los octetos TSC0 y TSC1 forman el número de secuencia IV y son usados en el mezclador de llave de fase 2 TKIP; los octetos TSC2 al TSC5 son usados en el hashing de llave de fase 1 TKIP, estos octetos están en el IV extendido.

2.3.4.3.2 Protocolo CTR con CBC-MAC (CCMP)

El protocolo CCMP es obligatorio para los equipos que cumplan con la implementación RSN.

CCMP esta basado en el algoritmo de encriptación AES, específicamente en CCM, este combina CTR para la confidencialidad y CBC-MAC para la autenticación e integridad; CCM protege la integridad tanto de los datos como parte del encabezado del MPDU.

CCM para WiFi es un modo genérico que puede ser usado con cualquier algoritmo de encriptación orientado para bloqueo, este tiene dos parámetros M y L, CCMP usa valores de 8 y 2 para M y L respectivamente.

CCM requiere de llaves temporales nuevas para cada sesión y un valor único actual para cada trama protegida por una llave temporal, para lograr tal acometida nos valemos de un

número de paquete (PN) de 48 bits, en caso de usar el mismo PN para una misma llave todas las seguridades se invalidan.

2.3.4.3.2.1 Formato MPDU CCMP

CCMP expande el MPDU en 16 octetos, repartiéndose 8 para el encabezado CCMP y 8 para el campo MIC.

Dentro del encabezado CCMP encontramos varios campos, de los más importantes es el campo PN de 48 bits y representado por un arreglo de 6 octetos, PN5 es el octeto más significativo; otro punto fuerte que debe ser notado es que no se usa en campo ICV WEP.

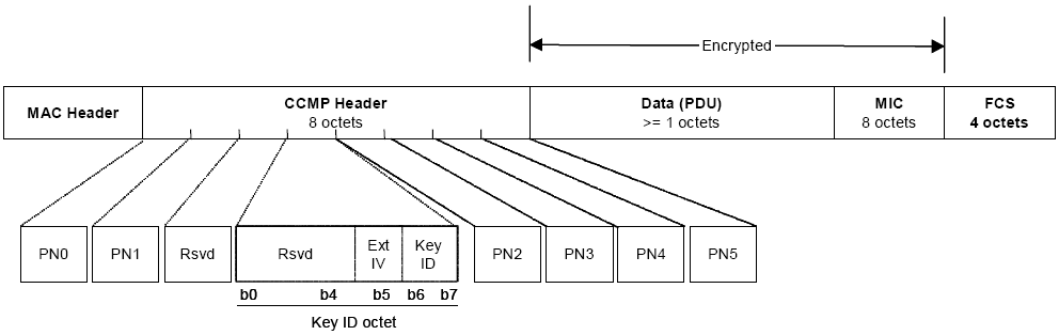


Figura 2.64. Formato de la MPDU CCMP Extendido[71]

Dentro de este formato se debe tener en cuenta que los bit reservados deben tomar valores de “0” y en el proceso de recepción son ignorados.

2.3.4.3.2.2 Encapsulamiento CCMP

CCMP encripta la carga del texto de entrada MPDU y lo encapsula, siguiendo los pasos descritos a continuación:

[71] IEEE 802.11i, Institute of Electrical and Electronics Engineers, Pág. 58.

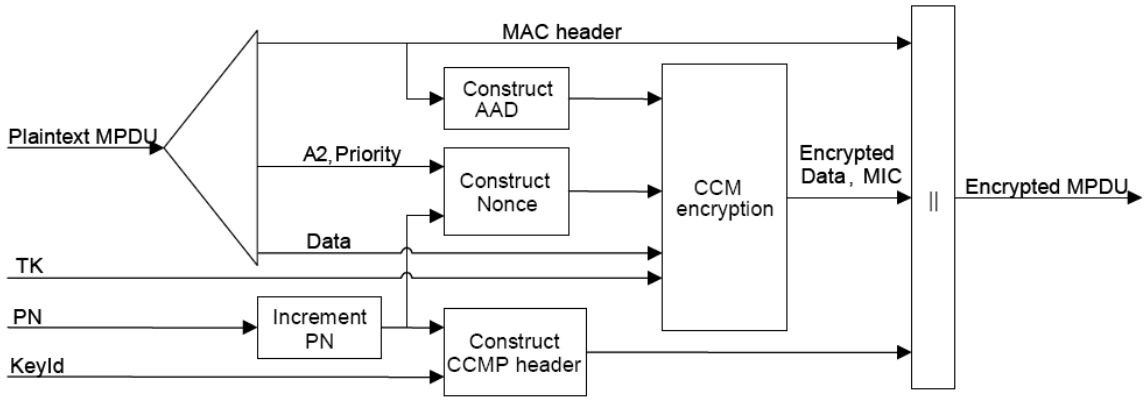


Figura 2.65. Diagrama de Bloques del Encapsulamiento CCMP

Incrementa el PN, para obtener un PN nuevo para cada MPDU, de tal forma que no se repita un PN para una misma llave temporal; se debe tener en cuenta que las MPDU retransmitidas no son modificadas en la retransmisión.

Usa los campos del encabezado MPDU para construir los datos de autenticación adicionales (AAD) para el CCM; el algoritmo CCM provee la protección de integridad para los campos que forman esta AAD; aquellos datos que pueden cambiar durante una retransmisión son enmascarados con ceros al momento del cálculo del AAD.

Construye el bloque actual CCM a partir de PN, A2 y el campo de prioridad, siendo A2 la dirección MPDU 2.

Coloca el PN y el identificador de llave en los ocho octetos del encabezado.

Usa la llave temporal, AAD, Nonce, y los datos MPDU del texto cifrado y MIC, a este proceso se le conoce como el proceso de origen del CCM.

A partir del encabezado MPDU, encabezado CCMP, datos encriptados y MIC se genera el MPDU encriptado.

2.3.4.3.2.3 Desencapsulamiento CCMP

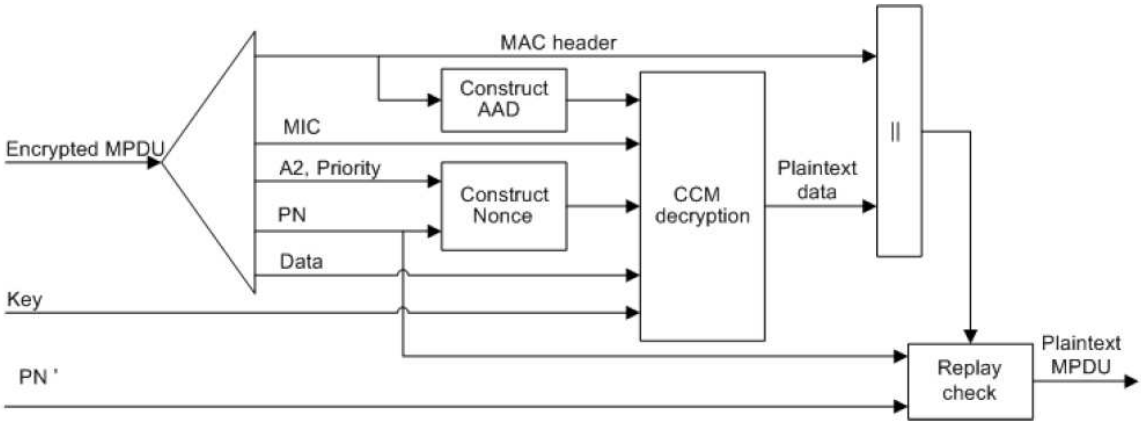


Figura 2.66. Diagrama de Bloques del Desencapsulamiento CCMP

El CCMP de encarga de la desencriptación de la carga del texto cifrado MPDU y lo desencapsulamiento del texto de entrada mediante los siguientes procesos:

El MPDU encriptado es pareado para poder llevar a cabo la construcción del AAD y los valores Nonce.

Se forma el AAD a partir del encabezado MPDU del MPDU encriptado.

El valor Nonce se construye de los valores de los campos A2, PN, y Priority.

El MIC se extrae para ser usado en el chequeo de integridad de CCM.

El receptor CCM procesa la llave temporal, AAD, Nonce, MIC, y los datos del texto cifrado MPDU para recuperar el texto de entrada MPDU, así como para revisar la integridad tanto del AAD como de los datos del texto de entrada.

Tanto el encabezado MPDU como los datos del texto de entrada provenientes de los procesos del receptor CCM se concatenan para formar el texto de entrada MPDU.

El proceso de desencriptación previene la retransmisión del MPDU mediante la validación del PN en los MPDU, esto implica verificar que dicho valor sea mayor al conteo de retransmisiones por sesión.

2.3.4.4 Distribución de Llaves

2.3.4.4.1 4 Way Handshake

La RSNA usa varios protocolos para poder completar el proceso de autenticación 802.1X, uno de ellos es el denominado 4 Way Handshake, a continuación se vera como fluye la información al usar este protocolo.

Mensaje 1.- Autenticador → Aplicante
Mensaje 2.- Aplicante → Autenticador
Mensaje 3.- Autenticador → Aplicante
Mensaje 4.- Aplicante → Autenticador

2.3.4.4.1.1 Mensaje 1

El mensaje 1, al igual que los demás mensajes de este protocolo, usa las tramas EAPOL-Key, por lo que se especificarán los valores que toman los campos de este tipo de tramas, en cada mensaje.

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap)
- Key Type = 1 (Pairwise)
- Install = 0
- Key Ack = 1
- Key MIC = 0
- Secure = 0
- Error = 0
- Request = 0
- Encrypted Key Data = 0
- Reserved = 0

Key Length = Cipher suite specific
Key Replay Counter = n
Key Nonce = ANonce
EAPOL-Key IV = 0

Key RCS = 0
Key MIC = 0
Key Data Length = 22
Key Data = PMKID

El autenticador envía el mensaje 1 al aplicante al final de una autenticación exitosa 802.1X; en la recepción, el aplicante determina si el contador de retransmisión de llave es menor o igual al valor local, el aplicante descarta el mensaje, en caso contrario se realizan las siguientes acciones: Se genera un nuevo valor de SNonce, se deriva el PTK y construye el mensaje 2.

2.3.4.4.1.2 Mensaje 2

Los valores para el mensaje 2 se muestran a continuación:

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap) “El mismo usado en el mensaje 1”
- Key Type = 1 (Pairwise) “El mismo usado en el mensaje 1”
- Install = 0
- Key Ack = 0
- Key MIC = 1
- Secure = 0 “El mismo usado en el mensaje 1”
- Error = 0 “El mismo usado en el mensaje 1”
- Request = 0 “El mismo usado en el mensaje 1”
- Encrypted Key Data = 0
- Reserved = 0

Key Length = 0
Key Replay Counter = n
Key Nonce = SNonce
EAPOL-Key IV = 0
Key RCS = 0
Key MIC = MIC

Key Data Length = La longitud en octetos incluyendo el elemento de información RSN
Key Data = Incluyendo el elemento de información RSN

En esta ocasión el aplicante le envía este mensaje 2 al autenticador; una vez recibido, el autenticador revisa que el contador de retransmisión de llave corresponda con el mensaje 1, si no es el caso, este mensaje se descarta, caso contrario se realizan las siguientes acciones: Deriva el PTK, verifica el MIC del mensaje 2; en caso de que no concuerde el MIC recalculado con el que envía el aplicante, se descarta el mensaje, si el MIC es valido se procede a revisar el elemento de información RSN, comparándolo bit a bit con el del mensaje de petición de asociación o reasociación; si no son iguales se procede con la disociación, en caso de coincidir se construye el mensaje 3.

2.3.4.4.1.3 Mensaje 3

Los valores del mensaje 3 se muestran a continuación:

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap) “El mismo usado en el mensaje 1”
- Key Type = 1 (Pairwise) “El mismo usado en el mensaje 1”
- Install = 0/1 (0 si el AP no soporta mapeo de llaves, o si la estación tiene el bit NoPairwise activado)
- Key Ack = 1
- Key MIC = 1
- Secure = 1 (llaves instaladas)
- Error = 0 “El mismo usado en el mensaje 1”
- Request = 0 “El mismo usado en el mensaje 1”
- Encrypted Key Data = 1
- Reserved = 0

Key Length = Cipher suite specific
Key Replay Counter = n + 1
Key Nonce = ANonce “El mismo usado en el mensaje 1”
EAPOL-Key IV = 0 (Version 2) o Aleatorio (Version 1)

Key RCS = Número de secuencia inicial que la estación de autenticación usara en las MPDU protegidas por el GTK.
Key MIC = MIC
Key Data Length = La longitud en octetos incluyendo el elemento de información RSN y GTK
Key Data = El elemento de información RSN de la trama de respuesta del AP y en forma opcional un segundo elemento de información RSN que es la asignación del cifrado del pareo del autenticador, en caso de que se haya negociado un grupo de cifrado, el GTK encapsulado y el identificador de llave de GTK.

En la recepción de este mensaje el aplicante descarta de manera silenciosa el mensaje si el campo de conteo de retransmisión de llave posee valores que ya han sido usados o si el valor de ANonce en el mensaje 3 difiere del valor en el mensaje 1.

Además de realizar la acción antes citada, el aplicante realiza las siguientes acciones: verifica el elemento de información RSN, y en caso de no ser idéntico al de la trama de respuesta, la estación se desasocia, si un segundo elemento de información RSN viene en el mensaje, el aplicante debe utilizar este cifrado de pareado o de autenticarse, si al información del elemento es correcta, se verifica el MIC del mensaje 3.

Si el MIC recalculado no concuerda con el MIC que el autenticador incluye en la trama, el aplicante debe descartar el mensaje 3, caso contrario, el aplicante actualiza el ultimo valor del contador de retransmisión de llave, construye el mensaje 4, lo envía al autenticador; y, configura la capa MAC para enviar y recibir MPDU protegidas de unicast de clase 3 mediante el PTK.

2.3.4.4.1.4 Mensaje 4

Los valores usados en este mensaje se pueden observar a continuación:

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap) “El mismo usado en el mensaje 1”

- Key Type = 1 (Pairwise) “El mismo usado en el mensaje 1”
- Install = 0
- Key Ack = 0 (Este es el ultimo mensaje)
- Key MIC = 1
- Secure = 1
- Error = 0
- Request = 0
- Encrypted Key Data = 0
- Reserved = 0

Key Length = 0

Key Replay Counter = n + 1

Key Nonce = 0

EAPOL-Key IV = 0

Key RCS = 0

Key MIC = MIC

Key Data Length = 0

Key Data = No se necesita.

Este mensaje se envía desde el aplicante al autenticador, por lo que al recibirlo, el autenticador verifica que el contador de retransmisión de llave, sea uno de los que pueden ser usados por este protocolo, si no lo es descarta el mensaje, caso contrario revisa el MIC; si el recalculado con el enviado el enviado por el aplicante no concuerdan se descarta el mensaje, si es valido se procede a configurar el PTK de la capa MAC; y se actualiza el contador de retransmisión de llave, para que use un valor nuevo en caso de que una nueva llave sea necesaria.

2.3.4.4.2 Group Key Handshake

Un autenticador se vale de este handshake para poder enviar el GTK al aplicante, este intercambio se debe iniciar cuando el aplicante esta desasociado o de autenticado, este proceso se realiza de la siguiente manera:

Mensaje 1.- Autenticador → Aplicante

Mensaje 2.- Aplicante → Autenticador

En caso de necesitarse este handshake como el 4 Way handshake, se debe realizar primero el intercambio 4 Way handshake.

2.3.4.4.2.1 Mensaje 1

Al igual que el proceso anterior se usan las tramas EAPOL-Key, por lo que los valores de esta trama se mostraran para ambos mensajes.

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap)
- Key Type = 0 (Group/STAKey)
- Install = 0
- Key Ack = 1
- Key MIC = 1
- Secure = 1
- Error = 0
- Request = 0
- Encrypted Key Data = 1
- Reserved = 0

Key Length = 0
Key Replay Counter = n + 2
Key Nonce = 0
EAPOL-Key IV = 0 (Version 2) o Aleatorio (Version 1)
Key RCS = El ultimo número de secuencia transmitido por el GTK
Key MIC = MIC
Key Data Length = Cipher suite specific
Key Data = Encriptado, el GTK encapsulado y el identificador de llave de GTK.

El autenticador le envía el mensaje 1 al aplicante, este en la recepción se encarga de verificar que el valor del contador de retransmisión de llave no haya sido enviado anteriormente, este valor debe ser mayor al de cualquier otra trama recibida a lo largo de esta sesión.

Verifica que el MIC sea valido, en este caso verifica que no exista errores de integridad de los datos, configura el GTK temporal de la capa MAC y por último responde este mensaje con el mensaje 2 y aumenta el contador de retransmisión.

2.3.4.4.2.2 Mensaje 2

Los valores del mensaje 2 se muestran a continuación:

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap) “El mismo que en el mensaje 1”
- Key Type = 0 (Group/STAKey) “El mismo que en el mensaje 1”
- Install = 0
- Key Ack = 0
- Key MIC = 1
- Secure = 1
- Error = 0
- Request = 0
- Encrypted Key Data = 0
- Reserved = 0

Key Length = 0
Key Replay Counter = n + 2 “El mismo que en el mensaje 1”
Key Nonce = 0
EAPOL-Key IV = 0
Key RCS = 0
Key MIC = MIC
Key Data Length = 0
Key Data = No se requiere.

El autenticador al momento de la recepción verifica que el valor del contador de retransmisión de llave sea igual a uno de los valores usados por el Group Key Handshake y que el MIC sea valido.

2.3.4.4.3 STAKey Handshake

Este proceso se realiza en caso de que una estación necesite establecer una asociación de seguridad STAKey (STAKeySA) con otra estación conectada a un mismo AP, dicha solicitud se realiza a través del AP; pero la inicia la estación.

El flujo de este intercambio se muestra a continuación:

STAKey Request.- Estación de Inicio → Autenticador
Mensaje 1.- Autenticador → Estación Par
Mensaje 2.- Estación Par → Autenticador
Mensaje 1.- Autenticador → Estación de Inicio
Mensaje 2.- Estación de Inicio → Autenticador

2.3.4.4.3.1 Mensaje STAKey Request

Tal como se ha revisado con anterioridad este proceso de handshake utiliza las tramas EAPOL-Key, por lo que se procederá a mostrar los valores que toman estos campos a través de los varios mensajes.

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap)
- Key Type = 0 (Group/STAKey)
- Install = 0
- Key Ack = 0
- Key MIC = 1
- Secure = 1
- Error = 0
- Request = 1
- Encrypted Key Data = 0
- Reserved = 0

Key Length = 0
Key Replay Counter = El contador de retransmisión de petición en la estación de inicio
Key Nonce = 0
EAPOL-Key IV = 0
Key RCS = 0
Key MIC = MIC
Key Data Length = La longitud en octetos del campo de datos de llave
Key Data = La dirección MAC de pareja.

Una estación envía el mensaje STAKey Request a un AP con la dirección MAC de la estación par; el AP al momento de la recepción verifica que el valor del contador de retransmisión de llave sea igual o mayor que la copia local del contador; luego verifica que el MIC sea valido y configura el contador de retransmisión de llave local para la estación de inicio con el valor recibido.

2.3.4.4.3.2 Mensaje 1

Para este mensaje, los valores de la trama son los siguientes:

Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap)
- Key Type = 0 (Group/STAKey)
- Install = 1
- Key Ack = 1
- Key MIC = 1
- Secure = 1
- Error = 0
- Request = 0
- Encrypted Key Data = 1
- Reserved = 0

Key Length = Cipher suite specific
Key Replay Counter = n + 3 (Asumiendo que este sigue al Group Key Handshake entre la estación par y el AP)

Key Nonce = 0
EAPOL-Key IV = 0 (Version 2) o Aleatoria (Version 1)
Key RCS = 0
Key MIC = MIC
Key Data Length = La longitud en octetos del campo de datos de llave
Key Data = La dirección MAC del iniciador encriptada y STAKey.

Una vez que el AP recibió el mensaje de petición STAKey, se envía el mensaje 1 a la estación par identificada en el mensaje de petición, dicha estación verifica que el valor del contador de retransmisión de llave no sea ningún valor usado previamente, procede luego a validar el MIC y establece el valor del contador de retransmisiones de llave local con el valor recibido; la estación par configura el SATKey para comunicarse directamente con la estación de inicio, y envía el mensaje 2 al AP.

2.3.4.4.3.3 Mensaje 2

Los valores que se envían en el mensaje 2 se muestran a continuación:
Description Type = N
Key Information:

- Key Description Version = 1 (RC4) o 2 (NIST AES Key wrap)
- Key Type = 0 (Group/STAKey)
- Install = 0
- Key Ack = 0
- Key MIC = 1
- Secure = 1
- Error = 0
- Request = 0
- Encrypted Key Data = 0
- Reserved = 0

Key Length = 0
Key Replay Counter = n + 3 (igual que en el mensaje 1)
Key Nonce = 0
EAPOL-Key IV = 0
Key RCS = 0

Key MIC = MIC
Key Data Length = La longitud en octetos del campo de datos de llave
Key Data = La dirección MAC del iniciador.

El mensaje 2 es un mensaje de reconocimiento al mensaje 1, una vez que se recibe el mensaje 2, el AP verifica que el contador de retransmisiones de llave tenga el mismo valor enviado en el mensaje 1, valida el MIC e incrementa su valor del contador para la estación par, finalmente el AP envía el mensaje 1 a la estación de inicio.

2.3.4.4.3.4 Mensaje 1 y 2 para la Estación de Inicio

Después de los intercambios entre el AP y la estación par, comienza el mismo intercambio, pero ahora entre el AP y la estación de inicio, los mensajes son iguales con ciertas diferencias que se muestran a continuación:

El valor del contador de retransmisión de llave, las direcciones son ahora entre el AP y la estación de inicio.

La encapsulación de datos de llave MAC de las estaciones están invertidas.

En caso de que el intercambio falle, el AP se comunicara con la estación par para borrar la dirección de origen del STAKey.

2.3.5 Descripción Funcional de la Subcapa MAC

A continuación podremos observar un poco más de cerca el funcionamiento de la subcapa MAC, así como los servicios que nos aporta. Comenzaremos con mostrar una grafica en la que se ve las partes que conforman la subcapa MAC:

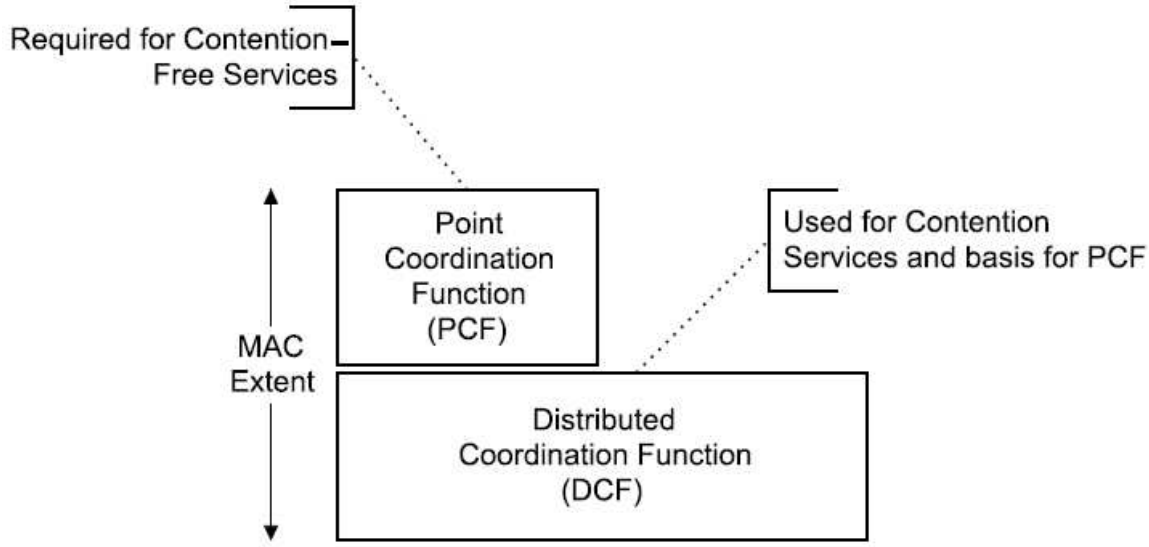


Figura 2.67. Arquitectura MAC[72]

De la figura se puede reconocer fácilmente 2 componentes de la subcapa MAC, la primera es la Función de Coordinación Distribuida (DCF), que viene a ser el método de acceso fundamental WiFi, se le conoce también como CSMA/CA o Acceso Múltiple de Censado de Portadora con Prevención de Colisión.

Lo que implica que cualquier estación que desee transmitir información al medio primero debe censar el medio para verificar que este libre, o esperar, además debe conocer cual es la duración de la información que se transmite, para no interrumpir las transmisiones.

La segunda componente de la subcapa MAC es la Función de Punto de Coordinación, que es un método de acceso opcional para las configuraciones de red de tipo infraestructura; este método de acceso controla que estación tiene el derecho de transmitir.

Tanto el DCF como el PCF deben coexistir de tal forma que permita la operación de ambos en un mismo BSS, de forma alternada con un periodo de contención libre seguido por un periodo de contención.

[72] IEEE 802.11, Institute of Electrical and Electronics Engineers, Pág. 70.

Otra de las funciones que provee la subcapa MAC es la fragmentación y de fragmentación, lo que lleva a la partición y ensamble de las MSDU o MMPDU en tramas de nivel MAC más pequeñas llamadas MPDU.

2.3.5.1 DCF

El protocolo de acceso al medio básico de WiFi es el DCF, que permite compartir el medio en forma automática mediante el uso de CSMA/CA, este protocolo esta diseñado para reducir las colisiones al momento del acceso al medio.

El cesando del medio se debe realizar mediante mecanismos tanto físicos como virtuales.

El mecanismo virtual de censado de portadora, se realiza mediante la distribución de información reservada que anuncian el uso independiente del medio, esto se logra gracias al intercambio de las tramas RTS (Request To Send) y CTS (Clear To Send), las cuales contienen el campo Duration/ID, que tiene como dato el tiempo que permanecerá ocupado el canal, para la transmisión de las tramas de datos.

Si la estación que envía el RTS no detecta la CTS, dicha estación puede repetir el proceso de manera más rápida.

Cabe destacar que este mecanismo virtual debe ser detectado por todas las estaciones, y a diferentes tasas de datos, ya que cada estación puede estar transmitiendo a diferentes tasas de datos.

2.3.5.1.1 Mecanismo de Censado de Portadora

Como ya se menciono con anterioridad, se debe usar dos mecanismos de censado de portadora, uno virtual y otro físico, si uno de estos nos indica que el medio esta ocupado, se establecerá que el medio esta ocupado, caso contrario se determina que esta inactivo.

El mecanismo virtual se conoce como NAV o vector de distribución de red, el cual mantiene las predicciones del tráfico futuro, basado en la información proveniente de las tramas CTS y RTS.

El mecanismo de censado de portadora combina el estado NAV y el estado del transmisor de la estación con censado físico, para determinar si el estado del medio es ocupado o inactivo, el estado NAV se puede representar mediante un contador que puede contar desde cero hasta una tasa uniforme, si es cero el medio esta inactivo, caso contrario esta ocupado.

2.3.5.1.2 Confirmaciones de Nivel MAC

Al momento de la recepción de algunas tramas, la estación de recepción debe responder una confirmación, que generalmente es una trama ACK.

En algunos casos la falta de esta trama de confirmación le indica a la estación de inicio que se ha producido un error; puede suceder que el mensaje fue recibido correctamente, pero el mensaje de confirmación se perdió, este error es irreconocible para la estación de inicio si se trata de un primer intercambio de tramas.

2.3.5.1.3 Espaciamiento de Intertrama (IFS)

Al espaciamiento entre tramas se le ha denominado IFS, se han definido cuatro tipos de IFS para definir varios niveles de acceso al medio.

SIFS (short interframe space), es el menor espacio entre tramas, se usa para separar tramas de un mismo intercambio.

PIFS (PCF interframe space), este espaciamiento se usa cuando una estación opera en el modo PCF, y le permite ganar prioridad de acceso al medio al inicio del CFP.

DIFS (DCF interframe space), se usa cuando una estación opera en el modo DCF, una estación no debe transmitir durante este periodo hasta determinar que el medio esta inactivo.

EIFS (extended interframe space), este espaciamiento se usa para poder determinar que se produjo errores en la transmisión y empezar la retransmisión.

2.3.5.1.4 Tiempo de Retiro Aleatorio

Una vez que se ha determinado que el canal esta inactivo, una estación antes de proceder a la transmisión de datos debe esperar un tiempo determinado, este es el tiempo de retiro aleatorio, que se conforma de un número aleatorio y un periodo de tiempo de terminado por los componentes físicos; este periodo de tiempo ayuda a reducir considerablemente las colisiones entre múltiples estaciones intentando tener acceso al medio.

Este número aleatorio toma valores entre cero y CW, este CW es un valor que corresponde a la potencia de 2 menos 1, es decir, valores de 7, 15, 31, 63, 127, 255; si se produce un error en la transmisión, se incrementa este valor hasta llegar al máximo, y permanece en dicho valor hasta que se produzca un transmisión exitosa, es decir al recibir una trama ACK en respuesta a la trama enviada.

2.3.5.1.5 Procedimiento de Acceso DCF

El método de acceso para DCF es CSMA/CA, y es el mismo con algunas variaciones para PCF, a continuación veremos como se realiza dicho proceso.

Una estación que desea transmitir un MPDU pendiente bajo el modo de operación DCF, primero debe determinar si el medio esta ocupado o inactivo, en caso de estar inactivo, se procede al intercambio de la primera trama después de un periodo de contención libre, seguido por un periodo de retiro aleatorio, este periodo se incrementara hasta un limite y permanecerá así hasta que se produzca un intercambio efectivo.

2.3.5.1.5.1 Procedimiento de Retiro

Este procedimiento entra en funcionamiento cuando se requiere de la transmisión de tramas y el medio se encuentra ocupado, o cuando una estación se da cuenta de una transmisión fallida.

Primero se calcula el tiempo de retiro en forma aleatoria, todas las ranuras de tiempo de retiro se producen después de un periodo mayor al DIFS, ya que los mecanismos de

censado de portadora establecen que el medio esta inactivo; o después de un EIFS, una vez que se determina que el medio esta inactivo.

Una estación usa el mecanismo de censado de portadora para determinar si el medio tiene actividad durante la ranura de tiempo de retiro, si no hay actividad, se debe decrementar el tiempo de retiro en un periodo de tiempo.

Si el medio esta ocupado, el procedimiento de retiro debe ser suspendido, se debe tener un periodo de inactividad de duración similar aun DIFS o EIFS para reactivar el procedimiento, la transmisión debe iniciar en el momento que el temporizador de retiro llegue a cero.

Como resultado de este procedimiento, cuando varias estaciones empiecen el retiro aleatorio, la estación con el tiempo de retiro más pequeño usando la función aleatoria, gana el acceso al canal.

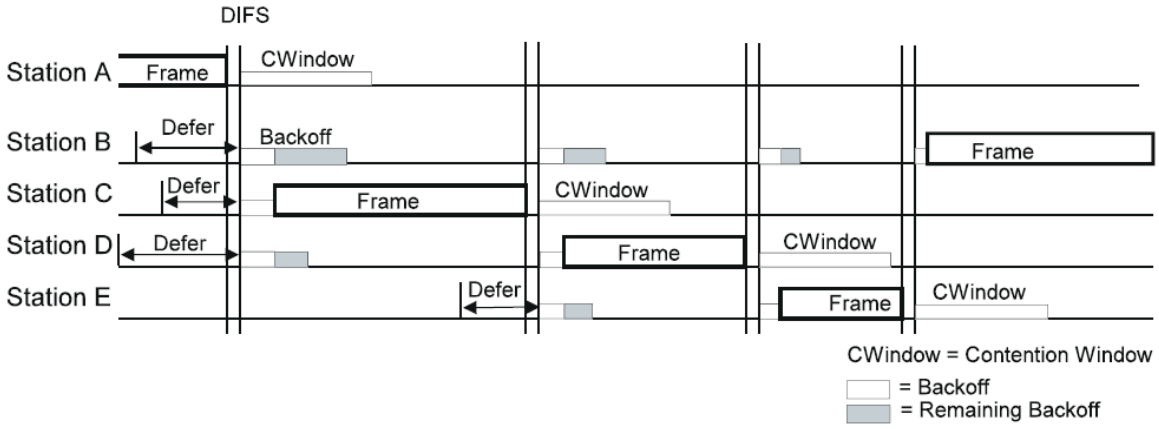


Figura 2.68. Procedimiento de Retiro[73]

2.3.5.1.5.2 Procedimientos de Recuperación y Límites de Retransmisión

La recuperación de errores es la responsabilidad de la estación que inicia el intercambio de tramas, estos errores se producen por colisiones durante el intercambio de las tramas RTS y CTS.

[73] IEEE 802.11, Institute of Electrical and Electronics Engineers, Pág. 78.

La recuperación de errores se debe realizar mediante la retransmisión de las tramas que la estación de inicio cree que tienen fallas, la retransmisión debe continuar hasta tener una transmisión exitosa o se alcance un limite relevante, hasta que ocurra uno u otro evento se debe tener un conteo de retransmisiones cortas y largas para cada MSDU o MMPDU, estos se resetean o incrementan de forma independiente.

En caso de fallar la transmisión de un RTS el contador de retransmisiones cortas se incrementa, ya sea para el MSDU o MMPDU, hasta su limite; cuando esto sucede este contador de resetea y se incrementa el contador de retransmisión largo, esto continua hasta alcanzar el limite del contador de retransmisión largo, en cuyo caso los intentos de retransmisión cesan.

2.3.5.1.6 Procedimiento de Confirmación

Una vez que se ha recibido con éxito una trama que requiere de confirmación, el AP genera una trama ACK, y es transmitida a la estación que no es AP, siempre y cuando se responda a una trama unicast que requiera una confirmación; esta trama ACK se debe transmitir después del periodo SIFS, sin importar el estado del canal.

La estación de origen debe esperar un cierto tiempo para recibir la trama ACK antes de determinar que la transmisión del MPDU ha fallado.

En caso de que se produzca la recepción de la trama ACK dentro del timeout de ACK, se puede proceder con el proceso de intercambio de las tramas, caso contrario se deben iniciar los procedimientos de retiro.

2.3.5.2 PCF

El segundo componente de la subcapa MAC la PCF, es la encargada de proveer la transferencia de tramas de contención libre; el punto de coordinación (PC) debe estar en el AP.

Para el AP es una opción convertirse en el PC, sin embargo todas las estaciones obedecen de forma inherente las reglas de acceso PCF debido a que este esta basado en el DCF, enviando el NAV al principio de cada CFP (periodo de contención libre).

Si se decide utilizar el PCF todas las estaciones deben funcionar en presencia de una BSS con un PC en funcionamiento, y por lo tanto debe ser capaz de recibir las tramas enviadas bajo el control PCF.

De igual manera las estaciones que deciden responder las tramas CF-Poll del PC se denominan estaciones PC-Pollables y no usan el intercambio RTS/CTS.

Un PC puede realizar retiro para las retransmisiones de una trama que no necesite de confirmación al estar en modo CFP, el PC puede retransmitir una trama que no necesite de confirmación después del periodo PIFS.

El modo PCF se construyo por encima del DCF basado en el protocolo CSMA/CA.

2.3.5.2.1 Estructura CFP y Temporización

El PCF controla la transferencia de tramas durante un CFP, cada CFP debe alternarse con un CP (periodo de contención); cada CFP debe comenzar con una trama Beacon que contiene el elemento DTIM (Mensaje de Indicación de Trafico Entregado), los CFP deben ocurrir a una tasa de repetición definida, sincronizada con el intervalo de faro.

El coordinador de puntos genera el CFP a una tasa de repetición de contención libre, la cual se define como un número de intervalos DTIM.

2.3.5.2.2 Procedimiento de Acceso PCF

El protocolo de transferencia de contención libre esta basado en un esquema de petición de datos (poll) controlado por un PC desde un AP en la BSS.

El PC obtiene el control del medio al inicia del CFP e intenta mantener el control de todo el CFP, esperando un periodo de tiempo más pequeño entre transmisiones que las estaciones usando el procedimiento de acceso DCF.

2.3.5.2.2.1 Acceso Fundamental

Al principio de cada CFP, el PC debe censar el medio, cuando este inactivo, se debe enviar una trama Beacon que llevara el CF Parameter SET y un DTIM.

Después de la trama faro inicial, el PC debe esperar al menos un periodo SIFS, luego transmitir una de las siguientes tramas: Trama de Datos, Trama CF-Poll, Trama CF-Poll + Datos o una trama CF-End.

Si no hay CFP, no existe traffico en el buffer y no hay petición de datos para el PC, por lo que se debe enviar la trama CF-End inmediatamente después de la trama Beacon.

Las estaciones que reciban tramas libres de errores del PC deben responder después de un periodo SIFS, en caso de que la estación sea no pollable debe responder una trama de confirmación.

2.3.5.2.3 Procedimiento de Transferencia PCF

Las tramas transferidas bajo el PCF típicamente son tramas alternadas enviadas desde y hacia el AP/PC; durante el CFP, el orden de las transmisiones y la estación permitida para la transmisión de tramas al PC en cualquier momento, es controlado por el PC.

Una estación que maneja su parte física mediante FH (Salto de Frecuencia), pierde el control del canal en el limite del tiempo de permanencia, por lo que se requiere que la transmisión del MPDU y su confirmación sean transmitidas antes del limite del tiempo de permanencia; en caso de que no se disponga del tiempo necesario, la transmisión debe ser diferida y transmitirse una trama nula.

2.3.5.3 Fragmentación

La subcapa MAC puede fragmentar y reensamblar directamente MSDU y MMPDU, los mecanismos de fragmentación y de fragmentación permiten la retransmisión de fragmentos.

La longitud de un fragmento MPDU debe ser un número igual de octetos para todos los fragmentos excepto el ultimo, que debe ser más pequeño; la longitud de un fragmento MPDU debe ser siempre de un número par de octetos, excepto el ultimo que puede tener una longitud par o impar de octetos.

La longitud de los fragmentos nuca debe ser mayor al umbral de fragmentación, a menos que WEP sea invocado por el MPDU, en caso de que este activo WEP, el MPDU debe expandirse en el IV e ICV, que corresponderá a un fragmento mayor al umbral de fragmentación.

Una vez que se generan los fragmentos por primera vez, antes de un proceso WEP, tanto su longitud como el cuerpo de la trama deben permanecer fijos desde su envió hasta su recepción, se debe tener en cuenta que una estación debe estar en capacidad de recibir fragmentos de cualquier longitud.

Si un fragmento necesita ser retransmitido, tanto su longitud como el contenido del cuerpo de la trama deben permanecer fijo durante el periodo de vida del MSDU o MMPDU en dicha estación, una vez que se transmite el fragmento, su longitud o contenido no puede variar para acomodarse al tiempo de permanencia. Cada fragmento tiene un campo de control de secuencia, compuesto por un número de secuencia y de fragmento; cuando una estación desea transmitir un MSDU o MMPDU el número de secuencia debe permanecer igual para todos los fragmentos del mismo MSDU o MMPDU. Los fragmentos deben ser enviados desde el número de fragmento más bajo al más alto, el número de fragmento empieza en cero. El campo de control de trama posee un bit denominado More Fragments Bit, que debe ser cero en caso de indicar que se trata del último o el único fragmento del MSDU o MMPDU.

La estación de inicio debe mantener un contador de transmisión MSDU para cada MSDU que se desee transmitir, este contador tiene el tiempo máximo permitido para transmitir un MSDU, dicho contador se inicia al intentar transmitir el primer fragmento, en caso de que el contador exceda el valor de tiempo de vida, los fragmentos restantes se descartan en la estación de origen u no se realizan intentos por completar la transmisión.

2.3.5.4 De Fragmentación

Cada fragmento contiene la información que permite el reensamblado completo del MSDU o MMPDU, el encabezado de cada fragmento contiene la siguiente información que es usada en la estación de destino: Frame type; address of the sender; destination address; sequence control, el cual permite que la estación de destino revise si los fragmentos entrantes pertenecen a un mismo MSDU o MMPDU, y la secuencia en la que los fragmentos deben ser armados; more fragments indicator, el cual informa si el fragmento entrante es el ultimo al tener en cero este valor.

La estación de recepción reconstruye los datos según el orden del número de fragmento que viene en el campo sequence control, en caso de que a los fragmentos se les haya aplicado WEP, se deben primero desencriptar los datos antes de reensamblar los datos, si la estación aun no recibe el fragmento con el bit more fragments en cero, continua ensamblando el MSDU o MMPDU, hasta el instante en que lo recibe.

Todas las estaciones deben soportar al menos la recepción de fragmentos de tres MSDU o MMPDU, se debe tener en cuenta que recibir más de tres fragmentos, implica que el número de tramas descartadas aumentara drásticamente.

La estación de destino debe tener contadores de tiempo de vida para los fragmentos recibidos, en caso de recibir más de tres fragmentos diferentes se debe implementar más contadores, al igual que en la estación de origen, si los fragmentos de un MSDU son recibidos fuera del tiempo de vida, todos los fragmentos del mismo MSDU son descartados, y en caso de tratarse de un MSDU o MMPDU directo los fragmentos se confirman y luego se descartan.

Para poder ensamblar los MPDU de forma correcta, se deben descartar todos los fragmentos duplicados, y en caso de tratarse de MSDU directos se deben conformar y luego descartar.

2.3.5.5 Soporte de Multi Tasas

Para algunas implementaciones de capa física, es posible soportar varias tasas de transferencia de datos, las cuales permiten realizar un cambio dinámico de tasa con el objetivo de mejorar el desempeño.

Todas las tramas de control que inicien un intercambio de trama deben ser transmitidas a una de las tasas de transferencia básicas de una BSS, a menos que el mecanismo de protección de estaciones transmisoras este habilitado, y la trama de control sea una trama del mecanismo de protección; en cuyo caso, la trama de control debe ser transmitida a la tasa de transferencia acordada según las reglas para la transmisión de tramas de protección y sus tasas.

Los MPDU de datos y/o gestión con unicast en la dirección 1 deben ser enviadas a cualquier tasa de datos soportada que seleccione el mecanismo de cambio, ninguna estación debe transmitir una trama unicast a tasas que el receptor no pueda soportar.

Bajo ninguna circunstancia una estación debe iniciar la transmisión de tramas de datos o gestión, a tasas de datos mayores a las máximas tasas de operación.

2.3.5.6 Operaciones entre Dominio Regulatorios

Una estación que haya sido habilitada para funcionar entre dominios regulatorios debe pasar a un escaneo pasivo cuando ha perdido la conectividad con su ESS; este escaneo pasivo se realiza únicamente con las capacidades de recepción de la estación.

Dicha estación deberá permanecer en su escaneo pasivo hasta que detecte un canal valido, mediante el cual detectara la trama WiFi, de esta trama, y específicamente del Beacon, extraerá el código de país, la potencia máxima de transmisión, los canales a ser usados; una vez que ha extraído esta información se dispone a enviar una trama Probe Request a un AP y de la respuesta de esta trama extraerá la información que le haga falta, y procederá a configurar su capa física para operar en el dominio regulatorio en el que se encuentra.

2.3.5.7 Mecanismo de Protección

El propósito del mecanismo de protección es el de asegurar que una estación no transmita un MPDU de datos o un MMPDU con un preámbulo o encabezado ERP OFDM a menos que intente una actualización del NAV de estaciones NonERP receptoras.

Las estaciones ERP deben usar el mecanismo de protección para los MPDU ERP OFDM del tipo datos o un MMPDU cuando el campo USE_PROTECTION del elemento de información ERP esta en “1”.

Las tramas del mecanismo de protección deben ser enviadas usando una de las tasas de transferencia obligatorias de 802.11b o 802.11; de tal manera que todas las estaciones sepan la duración del intercambio aun si no soportan las señales ERP OFDM.

Cuando se use las opciones ERP PBSS o DSSS OFDM para 802.11g, no se necesitan usar los mecanismos de protección.

En caso de que una BSS este compuesta únicamente de estaciones ERP, pero con conocimiento de que los vecinos de una BSS co-canal tienen trafico NonERP; el AP puede optar por usar los mecanismos de protección, para proteger el trafico de la BSS de interferencias.

2.3.6 Entidad de Gestión de Subcapa MAC

2.3.6.1 Sincronización

Se debe tener en cuenta que todas las estaciones dentro de un mismo BSS deben estar sincronizadas, a un solo reloj común, esto se logra mediante una función de sincronización de tiempo (TSF), la cual mantiene los temporizadores de todas las estaciones sincronizadas; todas las estaciones deben mantener un temporizador TSF local.

2.3.6.1.1 TSF para Redes Tipo Infraestructura

En una red tipo infraestructura, el AP debe ser el temporizador maestro, y por consiguiente debe realizar la TSF; el AP debe iniciar su temporizador TSF

independientemente de cualquier otro inicio de AP, en un esfuerzo por minimizar la sincronización de los temporizadores TSF de varios APs.

El AP debe periódicamente transmitir tramas especiales llamadas faros o beacons, que contienen una copia de su temporizador TSF para sincronizar las otras estaciones del BSS; una estación receptora debe siempre aceptar la información de temporización de los faros enviada por el AP que sirve al BSS.

Si el temporizador TSF de una estación es diferente al dato del tiempo proveniente del faro, la estación receptora debe configurar su temporizador local para recibir el dato del tiempo recibido.

2.3.6.1.2 TSF para una BSS Independiente

El TSF en una IBSS debe ser implementada mediante un algoritmo de distribución que debe ser realizado por todos los miembros de la BSS; cada estación en la BSS debe transmitir faros; cada estación dentro de la IBSS debe adoptar el dato del tiempo recibido de cualquier faro o probar la respuesta que tiene un valor TSF posterior a su mismo temporizador TSF.

2.3.6.2 Gestión de Potencia

2.3.6.2.1 Gestión de Potencia en Redes Tipo Infraestructura

Las estaciones que cambian de modo de gestión de potencia deben informar al AP, mediante los bits de gestión de potencia en campo de control de trama.

El AP no puede transmitir de forma arbitraria MSDU a las estaciones que se encuentran en el modo de ahorro de potencia (PS), en cambio debe poner los datos en buffer y transmitirlos solamente en periodos de tiempo designados.

Las estaciones que tienen datos en buffer dentro del AP se encuentran identificadas en un mapa de información de trafico (TIM), el cual debe ser incluido como un elemento en los faros generados por el AP; una estación debe determinar que tiene MSDU en buffer luego de recibir e interpretar un TIM.

Si se tiene una BSS operando bajo el modo DCF, o durante el periodo de contención del modo PCF, una estación que ha determinado que tiene una MSDU en el AP, y funciona en el modo PS debe transmitir una trama PS-Poll al AP, este le contesta con el MSDU que tenia en el buffer inmediatamente, o le confirma la trama y le envía los datos más adelante.

Si el TIM indica que el MSDU que se encontraba en el buffer es enviado durante el periodo de contención libre (CFP), una estación pollable que opera en el modo PS no debe enviar la trama PS-Poll, sino que debe mantenerse activo hasta que el MSDU sea recibido .

Si cualquier estación de un BSS funciona en modo PS, el AP debe tener en buffer los MSDU de broadcast o multicast y entregarlos a todas las estaciones inmediatamente después de la siguiente trama Beacon que contenga una transmisión de TIM de entrega (DTIM).

Una estación debe mantenerse en su modo de gestión de potencia hasta que le informe al AP de dicho cambio, esto se realiza mediante un intercambio de tramas; el modo de gestión de potencio no debe cambiar durante ninguna secuencia de intercambio de trama.

2.3.6.2.1.1 Modos de Gestión de Potencia de una Estación

Una estación puede estar en cualquiera de estos dos estados: Despierto, que es un estado de potencia completa; y, dormido, en el cual la estación no puede transmitir o recibir y consume poca potencia.

La forma en la que las estaciones transitan entre los dos estados de potencia debe ser determinada por el modo de gestión de potencia de la estación.

Modo Activo (AM)	La estación puede recibir tramas en cualquier momento; en el modo activo, una estación debe estar en el modo despierto. Una estación que se encuentra en la lista de polling de un PCF debe estar en modo activo durante la duración del CFP.
Ahorro de Potencia (PS)	La estación escucha los faros seleccionados y envía las tramas PS-Poll al AP si el TIM indica que existe un MSDU en buffer para la estación. En modo PS, una estación debe estar en el estado dormido y debe entrar el en estado despierto para recibir los faros seleccionados, para recibir transmisiones broadcast y multicast seguidas por ciertos tipos de faros, para recibir y esperar respuestas para transmitir tramas PS-Poll, o para recibir transmisiones de contención libre de MSDU en el buffer.

Tabla 2.38. Modos de Gestión de Potencia

Una vez que se una estación ha iniciado el intercambio de tramas para informarle al AP que va ha realizar el cambio de estado, el bit de gestión de potencia del campo de control de trama indica el estado que tomara la estación.

2.3.6.2.2 Gestión de Potencia en una IBSS

Para el caso de IBSS se tiene un punto de vista similar al caso infraestructura, en el cual las estaciones se encuentran sincronizadas, los MSDU de multicast y aquellos MSDU que deben ser transmitidos a estaciones con ahorro de potencia, son primeramente anunciados durante un periodo en el que todas las estaciones están activas; el anuncio es realizado mediante un mensaje de información de trafico ad hoc (ATIM); una estación en el modo PS debe escuchar estos anuncios para determinar si necesita seguir en estado activo.

Cuando un MSDU esta por ser transmitido a una estación que se encuentra en el modo PS, la estación de transmisión primero transmite una trama ATIM durante la ventana ATIM, en la cual todas las estaciones incluyendo las inactivas están despiertas. Esta ventana ATIM es un periodo de tiempo determinado en el cual solo los faros y tramas

ATIM pueden ser transmitidas, las transmisiones ATIM suelen ser aleatorias, después de que un faro sea transmitida o recibida por la estación.

Los ATIM directos deben ser confirmados; en caso de no ser confirmado, la estación debe ejecutar los procedimientos de retiro para la retransmisión del ATIM, los ATIM de multicast no deben ser confirmados.

Si una estación recibe una trama ATIM directa, debe confirmarla y permanecer activa durante todo el intervalo de faro esperando por el anuncio de recepción del MSDU; si no recibe el ATIM debe entrar al modo dormir para el final de la ventana ATIM. Las transmisiones del anuncio de MSDU mediante el ATIM es aleatoria después de la ventana de ATIM.

Es posible que el ATIM pueda ser recibido por más de una estación, y que una estación que reciba un ATIM pueda recibir más de un MSDU desde la estación de transmisión; las tramas ATIM únicamente son direccionadas para las estaciones de destino de un MSDU.

Después de un intervalo ATIM; solo aquellos MSDU directos que han sido exitosamente anunciados con un ATIM de confirmación; y, MSDU de broadcast/ multicast que han sido anunciados con un ATIM, deben transmitidos a estaciones en modo PS; las transmisiones de estas tramas deben realizarse usando el procedimiento de acceso DCF normal.

La estimación del estado de ahorro de potencia de otra estación puede basarse en la información de gestión de potencia transmitida por aquella estación, así como por el historial de intentos fallidos de transmisión; el uso de RTS/CTS en una IBSS puede reducir el número de transmisiones a la estación que esta en modo PS; si un RTS es enviado y un CTS no es recibido, la estación transmisora puede asumir que la estación de destino esta en modo PS.

2.3.7 Capa Física

Hay diferentes medios físicos que han sido definidos como parte del estándar 802.11, cada medio físico consiste de dos funciones de protocolo:

- Una función de convergencia de capa física, la cual adapta las habilidades del sistema de medio físico dependiente (PMD) al servicio de la capa física. Esta función esta soportada por el procedimiento de convergencia de capa física (PLCP), el cual define el método de mapeo de las MPDU a un formato de tramas adecuado para enviar y transmitir datos e información de gestión, entre dos o más estaciones usando el sistema PMD de asociación.
- Un sistema PMD, cuya función define las características y métodos de transmisión y recepción de datos mediante el medio inalámbrico entre dos o más estaciones.

Cada subcapa PMD puede requerir la definición de un único PLCP; si la subcapa PMD ya provee servicios físicos definidos, la función de convergencia de capa física puede ser nula.

2.3.8 Capa Física OFDM para Bandas de 5 GHz (802.11a)

2.3.8.1 Introducción

En esta parte del presente documento revisaremos a profundidad la capa física OFDM (Multiplexación por División de Frecuencias Ortogonales) para las frecuencias de 5 GHz, o mejor conocida como 802.11a; esta capa física opera en las bandas UNII, es decir de 5.15-5.25, 5.25-5.35, 5.470-5.725 y 5.725-5.825.

Con la llegada del sistema OFDM, las tasas de transferencia aumentan, teniendo ahora 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, que son una mejora a las tasas de transferencia originales de 802.11, las cuales eran solo de 1 o 2 Mbps, bajo sistemas Spread Spectrum.

Cabe destacarse que las tasas de transferencia de 6, 12 y 24 Mbps son obligatorias, y que el sistema trabaja con 52 subportadoras las cuales son moduladas usando BPSK, QPSK, QAM, o 64QAM; y que la codificación FEC se usa con tasas de código de 1/2, 2/3, o 3/4.

Tal como se reviso anteriormente para las capas físicas en general, esta capa física posee dos funciones de protocolo:

Una función de convergencia de capa física, la cual adapta las capacidades del sistema PMD al servicio de capa física. Esta función esta soportada por la PLCP, la cual define el método de mapeo de las PSDU a un formato apto para el envió y recepción de datos e información de gestión entre dos o más estaciones usando el sistema PMD de asociación.
Un sistema PMD cuya función define las características y métodos de transmisión y recepción de datos mediante el medio inalámbrico entre dos o más estaciones, cada una usando el sistema OFDM.

2.3.8.1.1 Funciones de Capa Física OFDM

La arquitectura de la capa física OFDM en la banda de 5 GHz, se ajusta al modelo referencial mostrado en secciones anteriores; esta capa física contiene tres entidades funcionales: la función PMD, la función de convergencia de capa física y la función de gestión de capa.

2.3.8.1.1.1 Subcapa PLCP

Para poder tener una capa MAC que pueda operar con un mínimo de dependencia con las diferentes capas físicas, se define la subcapa de convergencia de capa física; esta función simplifica la interfase de servicio de capa física a los servios MAC.

2.3.8.1.1.2 Subcapa PMD

La subcapa PMD provee un medio para poder enviar y recibir datos entre dos o más estaciones, específicamente para sistemas OFDM en 5 GHz.

2.3.8.1.1.3 Entidad de Gestión de Capa Física (PLME)

La PLME realiza la gestión de las funciones locales de capa física, en conjunto con la entidad de gestión de capa MAC.

2.3.8.2 Subcapa PLCP OFDM

Como se menciono en párrafos anteriores, una de las tres entidades que forman la capa física 802.11a es la subcapa PLCP, la cual se encarga de realizar el procedimiento de

convergencia por el cual un PSDU (Unidad de Datos de Servicio PLCP)se convierte en una PPDU (Unidad de Datos de Protocolo PLCP) y viceversa.

Durante la transmisión, el PSDU debe ser provisto de un preámbulo PLCP y un encabezado para poder crear un PPDU, mientras que en el receptor, el preámbulo PLCP y encabezado es procesado para ayudar en la desmodulación y entrega del PSDU.

2.3.8.2.1 Formato de Trama PLCP

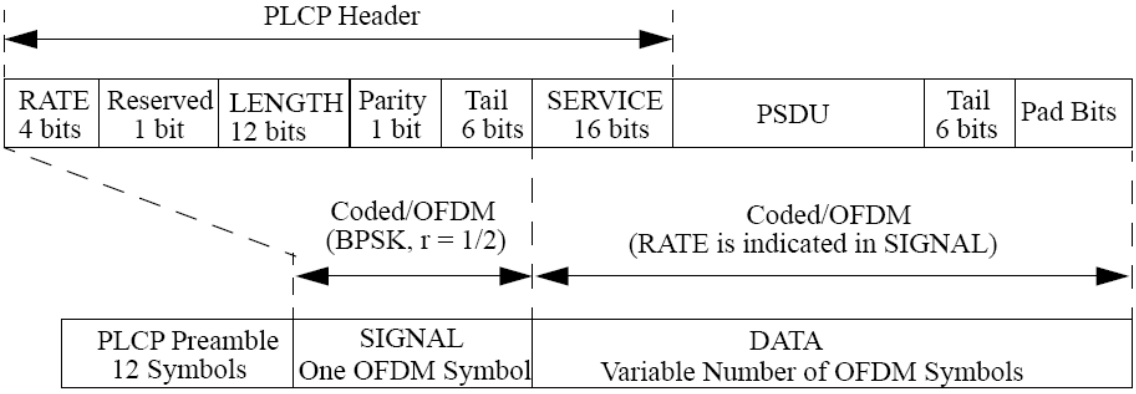


Figura 2.69. Formato de Trama PPDU[74]

En la figura se puede apreciar el formato PPDU incluyendo el preámbulo PLCP, el encabezado PLCP OFDM, PSDU, y los bits de cola y camino; el encabezado contiene los campos: LENGTH, RATE, una bit de reserva, un bit de paridad par y el campo SERVICE.

En términos de modulación, los campos LENGTH, RATE, los bits de reserva y paridad constituyen un solo símbolo separado OFDM, llamado SIGNAL, el cual es transmitido en una combinación de modulación BPSK y tasa 1/2.

El campo SERVICE, junto con el PSDU y los bits de cola y camino se denominan DATA, que es transmitido como vario símbolos OFDM; los bits de cola de SIGNAL, habilitan la codificación de los campos RATE y LENGTH, estos campos son requeridos para decodificar la parte DATA del paquete.

[74] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 7.

Además el mecanismo de revisión de canal libre (CCA), puede ser aumentado, mediante la predicción de la duración del paquete a partir de los campos RATE y LENGTH, aun si la tasa de transferencia no es soportada por la estación.

2.3.8.2.1.1 Proceso de Codificación PPDU

El proceso de codificación se compone por varios pasos, los cuales se muestran a continuación:

Se produce el campo de preámbulo PLCP, compuesto por 10 repeticiones de una secuencia de entrenamiento corta y dos repeticiones de una secuencia de entrenamiento largo, precedido por un intervalo de guardia (GI).

Se produce el campo de encabezado PLCP, a partir de los campos RATE, LENGTH y SERVICE; los dos primeros campos son codificados mediante un código convolucional de tasa R=1/2, y mapeado en un solo símbolo OFDM codificado BPSK, al cual se le llama símbolo SIGNAL; para facilitar el reconocimiento de los campos RATE y LENGTH, se insertan unos 6 bits de cola de valor “0” al encabezado.

A partir del campo RATE se calcula el número de bits de datos por símbolo OFDM, la tasa de codificación, el número de bits por cada subportadora OFDM y el número de bits codificados por símbolo.

Se le anexa al PSDU el campo SERVICE, extendiendo el campo con al menos 6 bits de valor “0” al final, y todo constituye la parte denominada DATA del paquete.

Se inicia el reordenamiento con una semilla sin ceros pseudo aleatoria, generando la secuencia de reordenamiento y realizando una función XOR con la cadena extendida de bits de datos.

Se reemplaza los 6 bits reordenados de valor “0” que siguen a los datos, con 6 bits sin reordenar de valor cero.

Codificar la cadena de datos extendida y reordenada con un código convolucional R=1/2, se omiten algunas partes de la cadena de salida codificada para alcanzar la tasa de codificación deseada.

Dividir la cadena de bits codificados en grupos de bits capaces de entrar un símbolo OFDM, en cada grupo realizar un reordenamiento de los bits de acuerdo a la regla de correspondencia de la tasa deseada.

Dividir el código resultante y la cadena de datos reordenados en grupos de bits capaces de entrar en un símbolo OFDM, por cada grupo de bit, convertir el grupo de bit en un número complejo de acuerdo a las tablas codificación de modulación.

Divida la cadena de números complejos en grupos de 48 números complejos, cada grupo debe ser asociado con un símbolo OFDM; en cada grupo, los números complejos serán numerados del 0 al 47 y procesados subsecuentemente en subportadoras OFDM numeradas desde el -26 al -22, -20 al -8, -6 al -1, 1 al 6, 8 al 20, y del 22 al 26; las subportadoras -21, -7, 7 y 21 se saltan y más tarde serán usadas para insertar subportadoras piloto, la subportadora 0, es omitida y se le da un valor de cero.

Cuatro subportadoras son insertadas como pilotos en las posiciones -21, -7, 7 y 21; el número total de subportadoras es 52.

Por cada grupo de subportadoras de -26 a 26, se convierte las subportadoras al dominio del tiempo usando la transformada inversa de Fourier; dependiendo de la forma de onda de la transformada de Fourier se genera una extensión circular de si misma que forma el GI, y trunca la forma de onda resultante a un símbolo OFDM único, mediante la aplicación del ventaneo del dominio del tiempo.

Se anexan los símbolos OFDM uno tras otro, iniciando después del símbolo SIGNAL describiendo tanto el campo RATE y LENGTH.

Reconvertir la forma de onda banda base compleja resultante, a una radio frecuencia dependiendo de la frecuencia central del canal deseado y transmitir.

2.3.8.2.1.2 Parámetros de Tasa Dependientes

Los parámetros de modulación dependientes en la tasa de datos usada, se muestran en la siguiente tabla:

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Tabla 2.39. Parámetros de Tasa Dependientes[75]

2.3.8.2.2 Preámbulo PLCP

El campo de preámbulo PLCP es usado para sincronización; consiste de 10 símbolos cortos y 2 símbolos largos, como se muestra en la figura:

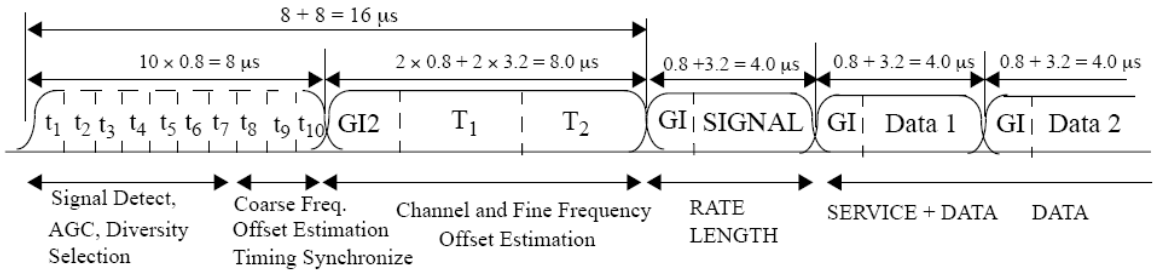


Figura 2.70. Estructura de Entrenamiento OFDM[76]

Donde t1 a t10 denotan los símbolos de entrenamiento cortos, y T1 y T2 los símbolos de entrenamiento largo; al preámbulo le siguen el campo SIGNAL y DATA, el tiempo total

[75] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 9.
[76] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 10.

de la longitud de entrenamiento es de 16 μs. Las líneas punteadas denotan las repeticiones debido a la periodicidad de la transformada inversa de Fourier.

2.3.8.2.3 Campo Señal (SIGNAL)

SIGNAL contiene los campos RATE y LENGTH, el primero contiene la información acerca del tipo de modulación y las tasas de codificación a ser usada en el resto del paquete.

La tasa de transferencia es de 6 Mbps, y los datos de SIGNAL no deben estar reordenados.

SIGNAL tiene 24 bits, los cuatro primeros, de 0 al 3 deben codificar el campo RATE, el bit 4 esta reservado, los bits 5 al 16 codifican el campo LENGTH, se transmiten primero los bits LSB.

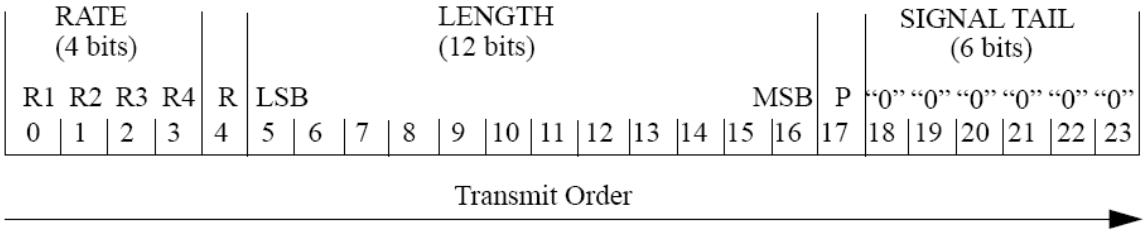


Figura 2.71. Asignación de los Bits de SIGNAL[77]

Los bits correspondientes al campo RATE deben tener los siguientes valores:

Rate (Mbits/s)	R1–R4
6	1101
9	1111
12	0101
18	0111
24	1001
36	1011
48	0001
54	0011

Tabla 2.40. Bits del Campo RATE[78]

[77] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 14.
[78] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 14.

El campo LENGTH debe ser un entero sin signo que indica el número de octetos en el PSDU que la capa MAC esta pidiendo que la capa física transmita.

Mientras que el bit 4 esta reservado, el bit 17 debe ser un bit de paridad par para los bits del 0 al 16; los bits del 18 al 23 forman el SIGNAL TAIL, estos deben ser cero.

2.3.8.2.4 Campo de Datos (DATA)

El campo DATA contiene los campos SERVICE, el PSDU y los bits de cola junto con los bits de camino.

El campo SERVICE tiene 16 bits, el bit 0 debe ser transmitido en primer lugar, los bits 0 al 6 tienen el valor de cero y se usan para sincronizar el re ordenador en la recepción, mientras que los restantes nueve bits del 7 al 15 están reservados y también tienen el valor de cero.

Los bits de cola deben ser seis y deben tener el valor de “0”, son necesarios para poder regresar al codificador convolucional a su estado cero. Mientras que los bits de camino se añaden para que el número de bits de DATA sea un número de bits codificados por símbolo.

2.3.8.2.4.1 Modulación de Subportadora

Las subportadoras OFDM deben ser moduladas mediante el uso de modulaciones BPSK, QPSK, QAM, o 64QAM, dependiendo de la tasa requerida; los datos de entrada seriales binarios reordenados y codificados, deben ser divididos en grupos de números de bits por símbolo, ya sea 1, 2, 4, o 6; para luego ser convertidos en números complejos que representan los puntos de las constelaciones de las modulaciones antes mencionadas.

Las valores de salida se denominan d, y están constituidos por la multiplicación entre el valor resultante (I=jQ) por un factor de normalización K_{MOD}.

Este factor de modulación depende del modo de modulación base, se debe tener en cuenta que tipo de modulación puede ser diferente al que se tiene en el inicio y al final de la transmisión, debido al cambio de las señales SIGNAL a DATA; el propósito del factor es mantener el mismo nivel de potencia para todas las modulaciones.

Modulation	K_{MOD}
BPSK	1
QPSK	$1/\sqrt{2}$
16-QAM	$1/\sqrt{10}$
64-QAM	$1/\sqrt{42}$

Tabla 2.41. Factor de Normalización y Tipo de Modulación.[79]

2.3.8.2.4.2 Modulación OFDM

La cadena de números complejos provenientes del las modulaciones BPSK, QPSK, QAM o 64QAM, se agrupan en grupos de 48 números complejos, dejando las subportadoras piloto libre así como la componente de DC.

Los valores de las subportadoras piloto son añadidos después con tres valores consecutivos de 1 y uno de -1; dejando el valor de la componente de DC con el valor de cero para no ser usada.

Una vez que se han colocado todos los valores en cada subportadora, se puede apreciar la ubicación de las frecuencias de subportadoras en el siguiente gráfico.

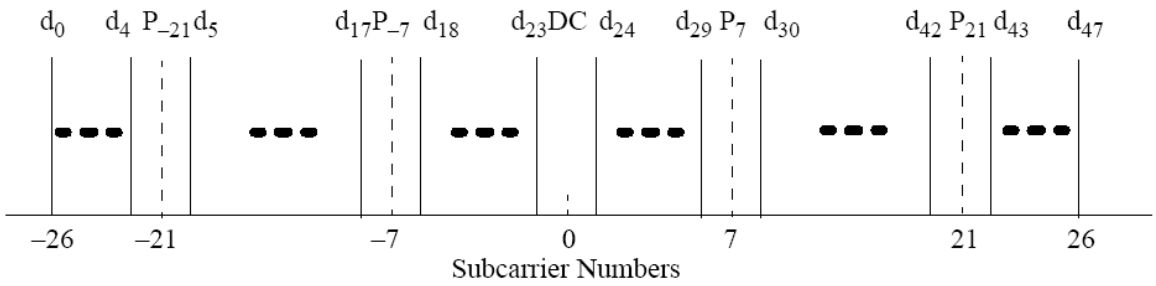


Figura 2.72. Ubicación de las Frecuencia de Subportadora

[79] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 19.

2.3.8.2.5 Revisión de Canal Libre (CCA)

La PLCP debe estar en capacidad de realizar una CCA y reportar el resultado de la misma a la capa MAC, es decir que el mecanismo CCA debe detectar si el medio esta ocupado.

2.3.8.2.6 Especificaciones de Operación PMD

A continuación se mostrara el diagrama de bloques que describe la capa física del sistema OFDM de forma general, los bloques corresponden a uno o varios de los procesos que se han listado con anterioridad.

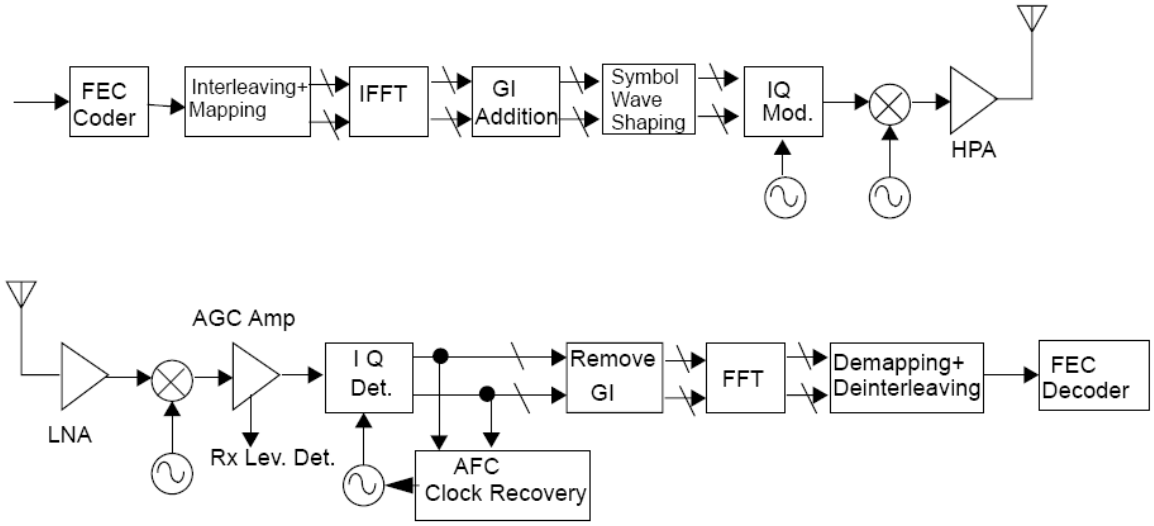


Figura 2.73. Diagrama de Bloques del Transmisor y Receptor OFDM[80]

Para poder complementar la revisión del sistema OFDM para las bandas de 5 GHz, se presentan a continuación, algunos de los valores específicos para el funcionamiento de 802.11a.

[80] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 24.

INFORMACIÓN DE LA TASA DE DATOS	6, 9, 12, 18, 24, 36, 48 Y 54 MBPS (6, 12 Y 24 MBPS SON OBLIGATORIAS)
Modulación	BPSK OFDM QPSK OFDM 16-QAM OFDM 64-QAM OFDM
Código de Error de Corrección	K = 7
Número de Subportadoras	52
Tasa de Código	1/2, 2/3, 3/4
Ancho de Banda Ocupado	16.6 MHz

Tabla 2.42. Principales Parámetros de 802.11a[81]

Una vez que se ha revisado algunos de los aspectos básicos en el funcionamiento de los sistemas OFDM, podemos ver en detalle varios aspectos relacionados con la transmisión de RF.

2.3.8.2.6.1 Frecuencias de Canal de Operación

La capa física OFDM debe operar en la banda de 5 GHz, debido a que el uso del espectro depende de cada organismo regional, se decidió por usar una parte de esta banda que se conoce como la banda UNII de 5 GHz, la cual es de libre uso en la mayoría de los países.

Las frecuencias centrales de canal son definidas en múltiplos de 5 MHz por encima de los 5 GHz; las relaciones entre las frecuencias y los números del canal se pueden establecer mediante la siguiente ecuación:

$$Frecuencia = 5000 + 5 \times n_{ch}[MHz]$$
$$n = 0,1,...,200$$

Formula 2.19. Relación entre la Frecuencia Central de Canal y el Número de Canal

Una vez que se tiene las diferentes frecuencias centrales debidamente numeradas e identificadas, se puede listar aquellas que están disponibles para el uso en equipos WiFi.

[81] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 24.

BANDA (GHZ)	NÚMEROS DE CANAL DE OPERACIÓN	FRECUENCIAS CENTRALES DE CANAL (MHZ)
U-NII Banda Baja (5.15-5.25)	36	5180
	40	5200
	44	5220
	48	5240
U-NII Banda Media (5.25-5.35)	52	5260
	56	5280
	60	5300
	64	5320
(5.47-5.725)	100	5500
	104	5520
	108	5540
	112	5560
	116	5580
	120	5600
	124	5620
	128	5640
	132	5660
	136	5680
	140	5700

Tabla 2.43. Tabla de los Números de Canal Central Validos

Cabe destacar que solo se esta listando la frecuencia central del canal y no se han colocado las subportadoras, tal como se reviso, en la frecuencia central no se usara subportadora.

En una topología de red de múltiples celdas, que se encuentren adyacentes y/o sobre puestas, pueden funcionar simultáneamente usando diferentes canales.

En el siguiente gráfico se puede apreciar el espectro frecuencia de los canales entre las frecuencias de 5180 a 5320 MHz, para los otros 11 canales restantes se tiene un espectro semejante.

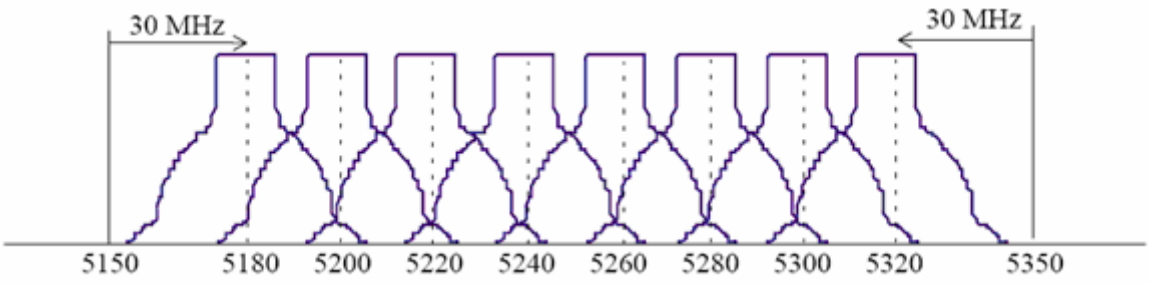


Figura 2.74. Espectro de Frecuencia de los Canales para 802.11a

2.3.8.2.7 Especificaciones de Transmisión PMD

2.3.8.2.7.1 Niveles de Potencia de Transmisión

Dentro de las especificaciones de transmisión, nos corresponde revisar los niveles de potencia de transmisión para cada una de las bandas en las cuales se encuentran los diferentes canales.

Banda de Frecuencia (GHz)	Máxima Potencia de Salida con Antenas de hasta 6 dBi de Ganancia (mW)	EIRP
5.15-5.25	40 (2.5 mW/MHz)	200 mW
5.25-5.35	200 (12.5 mW/MHz)	200 mW
5.470-5.725	_____	1 W
5.725-5.825	800 (50 mW/MHz)	_____

Tabla 2.44. Niveles de Potencia de Transmisión.[82]

2.3.8.2.7.2 Máscara de Espectro de Transmisión

La densidad espectral de la señal transmitida, debe estar dentro de la máscara de espectro de transmisión propuesta por este estándar, lo que significa que todos los equipos con certificación WiFi que permitan el estándar 802.11a deben ajustarse a la máscara de espectro propuesta a continuación:

[82] IEEE 802.11h, Institute of Electrical and Electronics Engineers, Pág. 53.

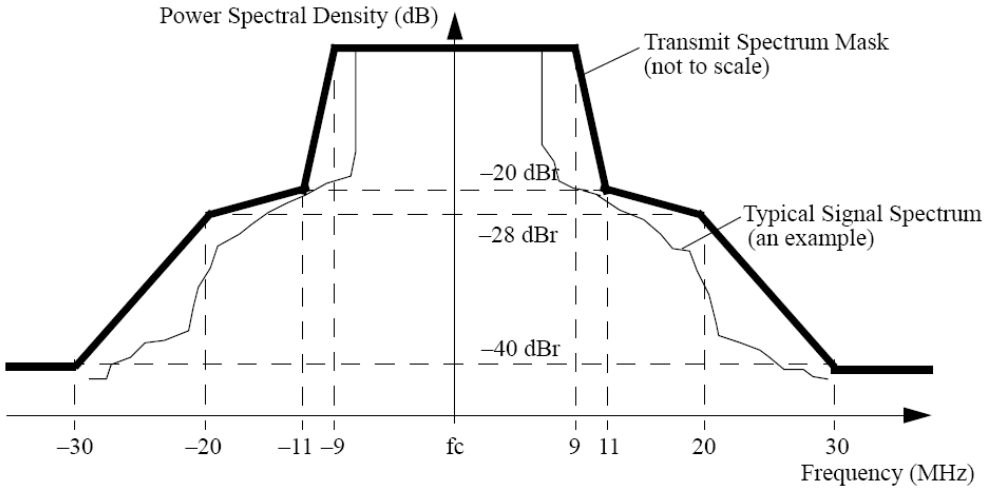


Figura 2.75. Máscara de Espectro de Transmisión.[83]

2.3.8.2.8 Especificaciones de Recepción PMD

2.3.8.2.8.1 Nivel de Sensibilidad de Entrada

En cada receptor se debe tener un nivel de sensibilidad mínimo al momento de la recepción, para nuestro caso, se tiene un nivel de sensibilidad para las diferentes tasas de transferencia; este nivel se puede ver en la siguiente tabla.

Tasa de Datos (Mbps)	Sensibilidad Mínima (dBm)
6	-82
9	-81
12	-79
18	-77
24	-74
36	-70
48	-66
52	-65

Tabla 2.45. Sensibilidad Mínima

2.3.8.2.8.2 Nivel de Entrada Máximo del Receptor

En el receptor se debe tener un nivel de entrada máxima de -30 dBm., este nivel de señal se mide en la antena, para cualquier modulación banda base.

[83] IEEE 802.11a, Institute of Electrical and Electronics Engineers, Pág. 29.

2.3.8.3 Subcapa PMD OFDM

La subcapa PMD OFDM acepta las primitivas de servicio de la subcapa PLCP y provee los medios reales por los que los datos son transmitidos o recibidos desde el medio inalámbrico.

Las funciones combinadas tanto de las primitivas y parámetros de la subcapa PMD OFDM de las funciones recibidas, resultan en una cadena de datos, información de sincronización, y parámetros asociados de la señal recibida, son entregados a la subcapa PLCP; un sistema parecido se aplica a la transmisión de datos.

2.3.8.3.1 Revisión de las Interacciones

Las primitivas asociadas con la subcapa PLCP de 802.11a están dentro de dos grupos básicos:

- Primitivas de servicio que soportan interacciones extremo a extremo PLCP.
- Primitivas de servicio que poseen significancia local y soportan interacciones entre subcapas.

2.3.9 Capa Física de Alta Velocidad de Secuencia Directa de Espectro Ensanchado para Bandas de 2.4 GHz (802.11b)

2.3.9.1 Introducción

En un principio, los primeros equipos WiFi que salieron al mercado, trabajaban en la banda de 2.4 GHz, utilizando FHSS (Frecuency Hopping Spread Spectrum) o DSSS (Direct Sequence Spread Spectrum), estos equipos no estaban sujetos a ninguna norma posterior, ya sea 802.11a, 802.11b, o 802.11g; simplemente se trataba de equipos WiFi 802.11.

Estos equipos fueron los primeros en salir al mercado, pero solo podían soportar tasas de transferencia de 1Mbps hasta 2 Mbps, en poco tiempo, se vieron obsoletos ya que las tasas de transferencia eran relativamente bajas y se buscaba mejorarlas, primero mediante la salida de 802.11a, que trabajaba en la banda de 5 Ghz, y luego con la salida de 802.11b;

esta última tenia por meta mejorar la existente capa física DSSS, dotándola de mejores tasas de transferencia, de hasta 11 Mbps.

Para poder incrementar las velocidades de la capa física DSSS, se incluyeron una serie de nuevas opciones y características que mejoran dicho desempeño, uno de ellos es el de remplazar la modulación CCK con una codificación convolucional binaria de paquetes, así como la mejora del throughput en las tasas de transferencia más altas, mediante el uso de un preámbulo PLCP más pequeño.

Esta nueva capa física se denomina capa física de alta tasa de transferencia DSSS o HR/DSSS, y esta compuesta por dos funciones protocolo:

Una función de convergencia de capa física, la cual adapta las capacidades del sistema de medio físico dependiente (PMD) al servicio de capa física; esta función esta soportada por el PLCP, el cual define el método de mapeo de los MPDU a formatos de trama aptos para la transmisión y recepción de datos entre dos o más estaciones usando el sistema de asociación PMD.

Un sistema PMD, cuya función es la de definir las características y el método de transmisión y recepción de datos a través del medio inalámbrico entre dos o más estaciones, las cuales usen el sistema de capa física de altas tasas de transferencia.

2.3.9.1.1 Funciones de Capa Física de Altas Tasas de Transferencia

La capa física de altas tasas de transferencia (HR) contiene tres entidades funcionales: la función PMD, la función de convergencia de capa física, y la función de gestión de capa.

La subcapa PLCP, esta definida para poder permitir que la capa MAC opere con la mínima dependencia de la subcapa PMD, esta función simplifica la interfase de servicios de capa física para los servicios MAC.

La subcapa PMD provee los medios y métodos de transmisión y recepción de datos a través del medio inalámbrico entre dos o más estaciones, las cuales usan el sistema HR.

Por su parte la entidad de gestión de capa física, realiza el manejo de las funciones físicas locales en conjunto con la entidad de gestión MAC.

2.3.9.2 La Subcapa PLCP HR

Esta subcapa se encarga de proveer los procedimientos de convergencia para las tasas de transferencia de alta velocidad (2, 5.5 y 11 Mbps), en las cuales los PSDU se convierten en PPDU; los PSDU son añadidos a un preámbulo PLCP y encabezado para crear el PPDU; se tiene dos preámbulos, uno obligatorio que es largo, que opera con las especificaciones DSSS de 1 y 2 Mbps y un preámbulo corto.

Este preámbulo corto es opcional y esta destinado para cuando se requiera de un máximo throughput, en este modo no existe interoperabilidad con equipos antiguo, por lo que 802.11b no esta destinada a funcionar con equipos fuera de esta norma.

2.3.9.2.1 Formato PPDU

Como se menciono anteriormente se tienen a disposición dos diferentes preámbulos, uno largo y obligatorio y otro corto y opcional.

2.3.9.2.1.1 Formato PPDU PLCP Largo

El formato PPDU largo, tiene como componentes el preámbulo PLCP HR, el encabezado PLCP HR, y el PSDU.

El preámbulo PLCP consiste de los siguientes campos: sincronización (SYNC), y el delimitador de inicio de trama (SFD); el encabezado por su parte contiene los siguientes campos: señalización (SIGNAL), servicio (SERVICE), longitud (LENGTH), y el CCITT CRC-16.

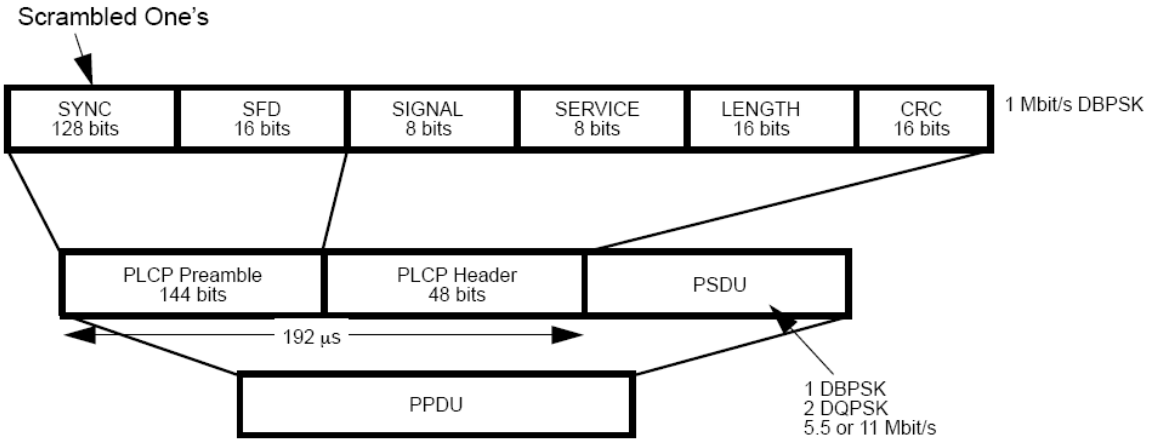


Figura 2.76. Formato PPDU PLCP Largo[84]

2.3.9.2.1.2 Formato PPDU PLCP Corto

El preámbulo PLCP corto junto con su encabezado es opcional para HR/DSSS. Estos se usan para minimizar el throughput de la red. Para 802.11g el soporte de este tipo de preámbulo es obligatorio.

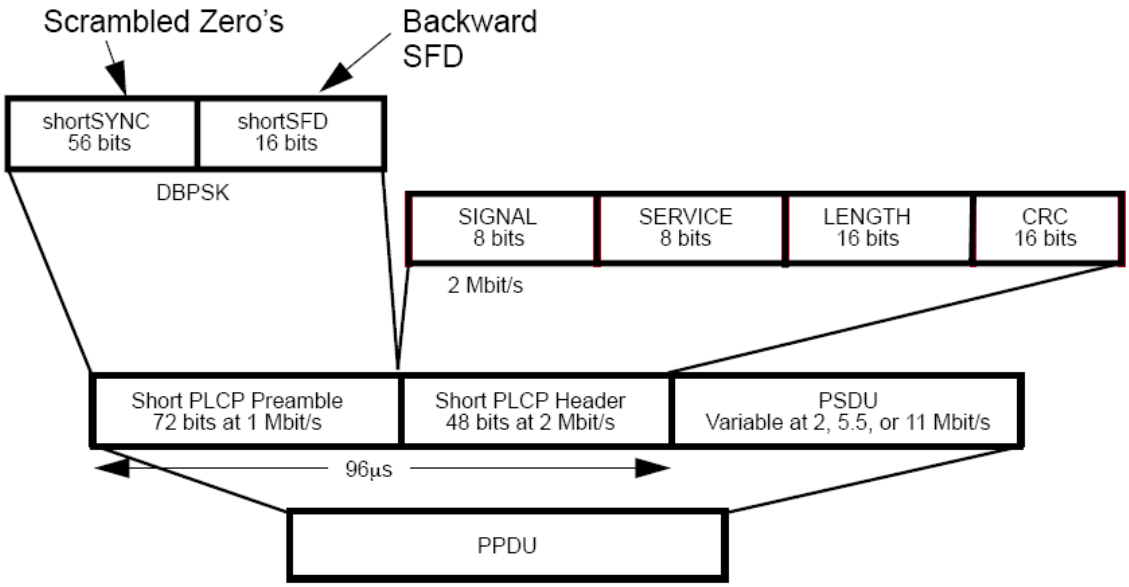


Figura 2.77. Formato PPDU PLCP Corto[85]

El preámbulo PLCP corto usa código de ensanchamiento Barrer a 1 Mbps con modulación DBPSK, mientras que el encabezado PLCP corto usa el código de

[84] IEEE 802.11b, Institute of Electrical and Electronics Engineers, Pág. 13.
[85] IEEE 802.11b, Institute of Electrical and Electronics Engineers, Pág. 14.

ensanchamiento Barrer a 2 Mbps con modulación DQPSK; el PSDU se transmite a 2, 5.5 o 11 Mbps.

2.3.9.2.2 Definiciones de los Campos PPDU PLCP

2.3.9.2.2.1 Campo SYNC PLCP Largo

Este campo tiene una longitud de 128 bits, en los cuales se encuentran ordenados de forma aleatoria bits con el valor “1”, este campo sirve para que el receptor pueda realizar las operaciones de sincronización necesarias; los primeros valores de este campo deben ser (1101100), el receptor debe ser capaz de sincronizar un campo SYNC sin valores cero en el estado inicial.

2.3.9.2.2.2 Campo SFD Largo

El SFD indica el inicio de los parámetros de capa física dependiente dentro del preámbulo; tiene 16 bits los cuales deben tener los siguientes valores (1111 0011 1010 0000), el bit de la derecha se transmite primero.

2.3.9.2.2.3 Campo SIGNAL PLCP Largo

Este campo le indica a la capa física cual va ha ser la modulación utilizada en la transmisión y recepción de los PSDU, posee 8 bits; la tasa de transferencia de datos debe ser igual al valor este campo multiplicado por 100 Kbps; estos valores representan 1, 2, 5.5 y 11 Mbps.

2.3.9.2.2.4 Campo SERVICE PLCP Largo

Este campo tiene 8 bits, tres de estos bits han sido seleccionados para soportar la extensión de la tasa de transferencia alta, el bit 7 se usa para suplir el campo LENGTH; el bit 3 se usa para indicar el método de modulación, “0” CCK y “1” PBCC; finalmente el bit 2 se usa para indicar que los símbolos del reloj y la frecuencia de transmisión se derivan del mismo oscilador; el resto de los bits desde b0 a b6 están reservados tienen el valor de cero.

2.3.9.2.2.5 Campo LENGTH PLCP Largo

Este campo tiene 16 bits, y representa un entero sin signo que indica el número en microsegundos que se requiere para la transmisión del PSDU.

2.3.9.2.2.6 Campo CRC PLCP

Los campos SIGNAL, SERVICE y LENGTH, deben ser protegidos con una secuencia de chequeo de trama (FCS); este campo realiza esta función mediante el complemento a uno del residuo generado mediante la división de modulo 2 de los campos PLCP protegidos para el polinomio:

$$G(x) = x^{16} + x^{12} + x^5 + 1$$

Formula 2.20. Polinomio Generador del Campo CRC PLCP Largo

2.3.9.2.2.7 Cambio de Tasa de modulación y Modulación de Datos PLCP Largos

Tanto el preámbulo como el encabezado PLCP largo deben ser transmitidos mediante una modulación DBPSK de 1 Mbps; los campos SIGNAL y SERVICE en conjunto deben indicar la modulación a ser usada para la transmisión del PSDU; tanto el transmisor como receptor deben iniciar el tipo de modulación indicada en estos dos campos con el primer octeto del PSDU.

2.3.9.2.2.8 Campo SYNC PLCP Corto

Este campo consiste de 56 bits, en los cuales se encuentran ceros en orden indistinto; este campo le permite al receptor y transmisor tener el tiempo necesario para realizar las operaciones de sincronización; el estado inicial o semilla debe ser (0011011).

2.3.9.2.2.9 Campo SFD PLCP Corto

El campo SFD corto debe tener 16 bits y consiste de los siguientes bits: 0000 0101 1100 1111; el bit de la derecha es el primero en ser transmitido, y los equipos que no soporten esta opción no deben detectar este campo.

2.3.9.2.2.10 Campo SIGNAL PLCP Corto

Este campo le indica a la capa física la tasa de datos que debe ser usada para la transmisión y recepción del PSDU, este campo tiene 8 bits, el número que se envíe en este campo multiplicado por 100 Kbps es la tasa buscada.

2.3.9.2.2.11 Campo SERVICE PLCP Corto

Este campo es el mismo descrito para el encabezado largo.

2.3.9.2.2.12 Campo LENGTH PLCP Corto

Este campo es el mismo definido anteriormente para el encabezado largo.

2.3.9.2.2.13 Campo CRC Corto

Este campo protege a los campos SIGNAL, SERVICE y LENGTH; realizando las mismas funciones que el campo CRC para el encabezado largo.

2.3.9.2.2.14 Cambio de Tasa de Modulación y Modulación de Datos PLCP Cortos

El preámbulo PLCP debe ser transmitido usando la modulación DBPSK a 1 Mbps; el encabezado PLCP corto debe ser transmitido a 2 Mbps; los campos SIGNAL y SERVICE combinados me indican cual debe ser el tipo de modulación que se debe usar para la transmisión del PSDU.

Tanto el transmisor como receptor deben iniciar la modulación y tasa indicada por estos dos campos con el primer octeto del PSDU.

2.3.9.3 Subcapa PMD de Altas Tasas de Transferencia

Esta subcapa acepta las primitivas de servicio de la subcapa PLCP y provee los medios por los cuales los datos son transmitidos o recibidos a través del medio.

Las funciones combinadas, tanto de las primitivas como parámetros de la subcapa PMD, para la función de recepción resultan en una cadena de datos, información de sincronización y parámetros de señales recibidas asociadas, los cuales son entregados a la subcapa PLCP; una funcionalidad similar se presenta para la transmisión de datos.

2.3.9.3.1 Revisión de las Interacciones

Las primitivas asociadas con la subcapa PLCP a la PMD de altas tasas de transferencia están predispuestas en dos categorías:

- ✓ Primitivas de servicio que soportan interacciones PLCP de par a par.
- ✓ Primitivas de servicio que tienen significancia local y que soportan interacciones entre capas.

2.3.9.3.2 Especificaciones de Operación PMD

2.3.9.3.2.1 Rango de frecuencias de Operación

La capa física de 802.11b opera en el rango de frecuencias de 2.4 a 2.4835 GHz, dicho rango se encuentra en funcionamiento en América, Europa y Japón; o, puede trabajar en el rango de 2.471 a 2.497 para el Japón.

En la siguiente tabla se podrá apreciar las frecuencias de canal central y el número de dicho canal.

CHNL_ID	Frecuencia (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2562
12	2467
13	2472
14	2484

Tabla 2.46. Número del Canal de Operación 802.11b

En una topología de red de múltiples celdas, las celdas adyacentes o sobre puestas pueden operar simultáneamente usando diferentes canales, sin interferencia si las

distancias entre las frecuencias centrales es de al menos 25 MHz, el canal 14 solo se usa en Japón.

802.11b posee cuatro diferentes tipos del modulaciones y tasas de datos, las básicas basadas en modulación DBPSK a 1 Mbps, las tasas de datos mejoradas basadas en modulación DQPSK a 2 Mbps; y finalmente dos tipos de modulaciones adicionales: esquema de modulación CCK para 5.5 y 11 Mbps, y un opcional esquema PBCC para una posible mejora del desempeño.

Los canales de operación se pueden escoger según dos tipos de operación, una con canales separados para evitar la interferencia, y otro con canales sobre puestos con una separación de canal de 10 MHz entre las frecuencias centrales para evitar la mayor parte de interferencia.

Set	Número de Canales	Números de Canal HR/DSSS
1	3	1, 6, 11
2	6	1, 3, 5, 7, 9, 11

Tabla 2.47. Canales de Operación 802.11b en América[86]

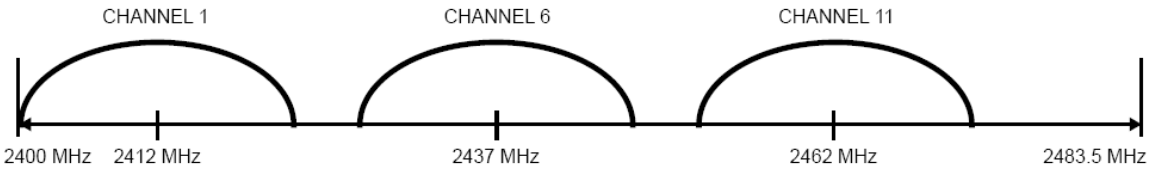


Figura 2.78. Canales Separados 802.11b en América

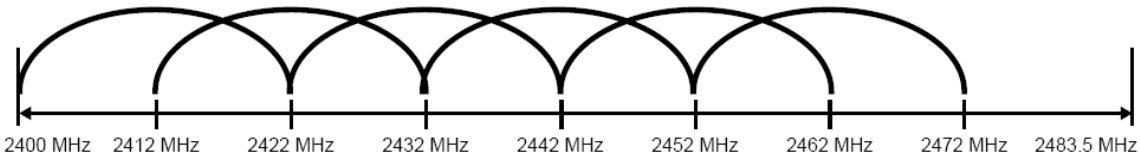


Figura 2.79. Canales con Sobre Posición 802.11b en América

[86] IEEE 802.11b, Institute of Electrical and Electronics Engineers, Pág. 49.

Set	Número de Canales	Números de Canal HR/DSSS
1	3	1, 7, 13
2	7	1, 3, 5, 7, 9, 11, 13

Tabla 2.48. Canales de Operación 802.11b en Europa[87]

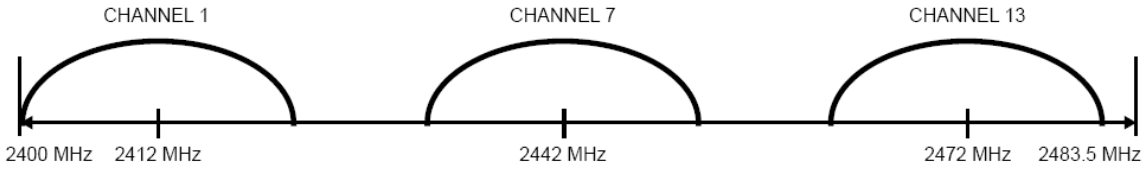


Figura 2.80. Canales Separados 802.11b en Europa

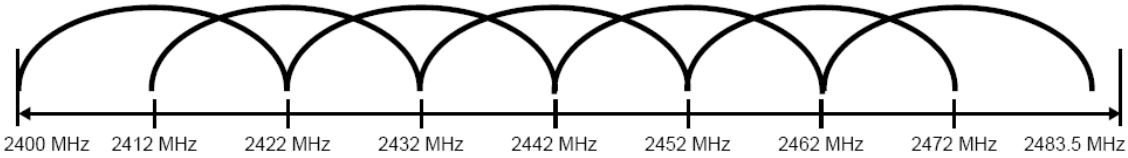


Figura 2.81. Canales con Sobre Posición 802.11b en Europa

2.3.9.3.3 Especificaciones de Transmisión PMD

2.3.9.3.3.1 Niveles de Potencia de Transmisión

Los niveles de potencia que pueden irradiar los dispositivos WiFi que trabajen bajo la norma 802.11b, dependerán del área geográfica en los cuales se encuentren, ósea, dependerá de si se encuentran los dispositivos en América, Europa o Japón, los valores máximos de radiación se encuentran en la siguiente tabla:

Potencia de Salida Máxima	Ubicación Geográfica
1000 mW	USA
100 mW (EIRP)	Europa
10 mW/MHz	Japón

Tabla 2.49. Niveles de Potencia de Transmisión[88]

[87] IBID 86
[88] IEEE 802.11b, Institute of Electrical and Electronics Engineers, Pág. 52.

2.3.9.3.3.2 Máscara de Espectro de Transmisión

El espectro de transmisión de los equipos 802.11b se deben ajustar a la máscara de espectro de transmisión, por lo tanto cualquier equipo WiFi que desee trabajar bajo esta norma se debe acoger a la siguiente máscara:

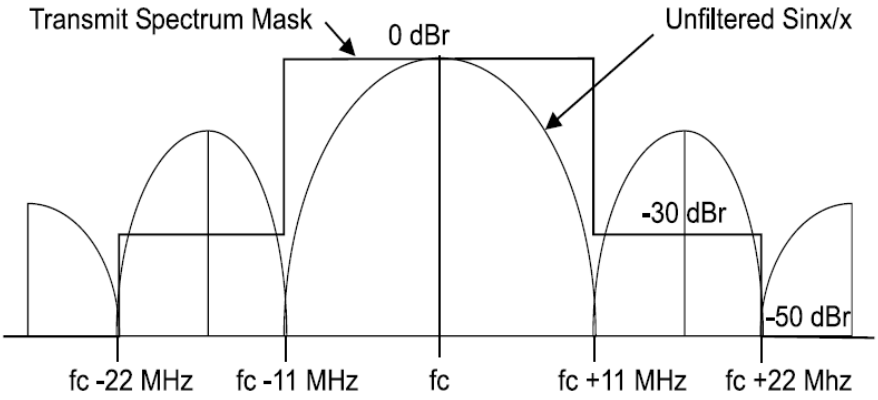


Figura 2.82. Máscara de Espectro de Transmisión[89]

2.3.9.3.4 Especificaciones de Recepción PMD

El nivel de sensibilidad de entrada mínima para los equipos debe ser menor o igual que -76 dBm, por otra parte la relación de error de trama (FER) debe ser menor a 8×10^{-2} en una transmisión a 11 Mbps con modulación CCK.

En cambio el nivel máximo de señal de entrada debe ser de -10 dBm, esto medido en la antena.

2.3.10 Capa Física de Tasas de Transferencia Extendidas de Secuencia Directa de Espectro Ensanchado para Bandas de 2.4 GHz (802.11g)

2.3.10.1 Introducción

La capa física de tasas de transferencia extendidas (ERP), mejor conocida como 802.11g, esta construida sobre las tasas de datos de 1 y 2 Mbps para DSSS, y las tasas de datos de 1, 2, 5.5, y 11 Mbps de 802.11b; 802.11g trae consigo tasas de datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, de las cuales las tasas de 1, 2, 5.5, 11, 6, 12 y 24 Mbps son obligatorias.

[89] IEEE 802.11b, Institute of Electrical and Electronics Engineers, Pág. 53.

Dos modulaciones ERP PBCC opcionales están definidas, con tasas de datos de 22 y 33 Mbps, y un último modo de modulación conocido como DSSS OFDM se incorpora con tasas de datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

2.3.10.1.1 Modos de Operación

Los sistemas 802.11g implementan todos los modos obligatorios para las capas físicas DSSS y HR/DSSS, además posee la capacidad de decodificar todos los mensajes de las capas físicas anteriormente mencionadas.

Los sistemas ERP tiene la capacidad de detectar los preámbulos ERP y los preámbulos 802.11b en caso de que se requiera de un asesoramiento de canal libre, ya que no se requieren de mecanismos de protección en estos casos.

Una BSS ERP es capaz de operar en cualquier combinación de los modos disponibles 802.11g y en modos NonERP, y en caso de estar activadas las opciones necesarias se puede permitir combinaciones entre estas.

Los modos de operación de los sistemas ERP se pueden resumir de la siguiente manera:

ERP-DSSS/CCK.-

La capa física utiliza las habilidades de 802.11b con las siguientes excepciones:

- ✓ El uso del encabezado PPDU PLCP corto es obligatorio.
- ✓ El CCA posee un mecanismo que detecta todos los símbolos de sincronización obligatorios para 802.11g.
- ✓ El máximo nivel de señal de entrada es de -20 dBm.
- ✓ El uso de una misma referencia de oscilación es obligatoria para la frecuencia de reloj de símbolo y la frecuencia central de transmisión.

ERP-OFDM.-

La capa física utiliza las habilidades básicas de 802.11a con las siguientes excepciones:

- ✓ El plan de frecuencia tiene concordancia con 802.11b.

- ✓ El CCA tiene un mecanismo que detecta todos los símbolos obligatorios para 802.11g.
- ✓ La precisión en la frecuencia es de ± 25 PPM.
- ✓ El máximo nivel de señal de entrada es de -20 dBm.
- ✓ La ranura de tiempo es de 20 μs a menos que la BSS este compuesta solamente de estaciones ERP, en cuyo caso se aumentan 9 μs.
- ✓ El periodo de SIFI es de 10 μs de acuerdo con 802.11b.

ERP-PBCC.- (Opcional)

Este es un esquema de modulación de una sola portadora que codifica la carga de datos usando un código convolucional binarios de paquete de 256 estados; este es una extensión de la modulación PBCC usada en 802.11b; en este modo están definidas dos tasas de datos, 22 y 33 Mbps.

DSSS-OFDM.- (Opcional)

Esta es una modulación hibrida que combina un preámbulo y encabezado DSSS con una transmisión OFDM; el modo DSSS-OFDM posee tasas de datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

En caso de que se use el modo opcional DSSS-OFDM, las tasas soportadas por este modo son las mismas que por el modo ERP-OFDM.

Las modulaciones disponibles para 802.11g son de alto desempeño ya que deben coexistir en un medio compartido, esta coexistencia se logra mediante la inclusión de un censado de portadora virtual, protocolos CSMA/CD-CA y fragmentación de MSDU.

2.3.10.1.2 Descripción

La capa física de tasas de transferencia extendida consiste de las siguientes funciones protocolo:

Una función de convergencia de capa física, la cual adapta las capacidades del sistema de medio físico dependiente a los servicios físicos disponibles; esta función esta soportada por la PLCP, la cual define un método para el mapeo de los MSDU en formato de trama

adecuado para enviar y recibir datos e información de gestión entre dos o más estaciones usando el sistema de asociación PMD.

Un sistema PMD, cuya función define las características y el método de transmisión y recepción de datos a través del medio inalámbrico entre dos o más estaciones, cada una usando ERP.

2.3.10.1.3 Funciones de Capa física de Tasas de Transferencia Extendidas

Los sistemas ERP contienen tres entidades funcionales: la función PMD, la función de convergencia de capa física (PLCP) y la función de gestión de capa.

Los servicios ERP son provistos a la capa MAC mediante las primitivas de servicio de capa física; la interoperabilidad se logra mediante los mecanismo de censado de portadora y el mecanismo de protección; este le permite a las estaciones NonERP que conozcan el trafico ERP aunque no lo puedan de modular para poder considerarlo en el trafico del medio.

2.3.10.2 Subcapa PLCP de Tasas de Transferencia Extendidas

El protocolo de convergencia especifica como los PSDU son convertidos en PPDU y viceversa, los PPDU son formados a partir de la anexión de un PSDU a un preámbulo y encabezado PLCP de tasa extendida.

2.3.10.2.1 Formato PPDU

Una estación 802.11g debe soportar tres diferentes tipos de formatos de preámbulos y encabezados; el primero es el preámbulo y encabezado largos, el cual permite interoperabilidad con las estaciones 802.11b si usan las tasas de datos de 1, 2, 5.5 y 11 Mbps; la modulación opcional DSSS-OFDM con todas sus tasas y la modulación opcional ERP-PBCC con todas sus tasas.

El segundo es el preámbulo y encabezado cortos, este soporta tasas de 2, 5.5, y 11 Mbps así como DSSS-OFDM y ERP-PBCC.

El tercero es el preámbulo y encabezado ERP-OFDM, el cual tiene dos formatos PPDU opcionales, para poder soportar las tasas de modulación DSSS-OFDM opcionales.

2.3.10.2.1.1 Formato PPDU de Preámbulo Largo

Este formato es el mismo usado en 802.11b, con algunas diferencias, lo que significa que es apto para se usado en los modos de 1, 2, 5.5 y 11 Mbps, y es compatible con BSS usando este modo, para poder acomodar los modos opcionales como ERP, el preámbulo PPDU largo solo difiere en lo siguiente:

Usa un bit del campo SERVICE para indicar cuando el modo opcional ERP-PBCC esta siendo usado.

Usa dos bits adicionales del campo SERVICE para resolver la ambigüedad entre los modos de 22 y 33 Mbps.

Se establecen tres tasas opcionales adicionales las cuales están definidas en el campo SIGNAL, que son 22 Mbps ERP-PBCC, 33 Mbps ERP-PBCC y todas las tasas DSSS-OFDM.

Debido a que el cambio se produce en el campo SERVICE, se mostraran estos cambios reflejados en la nueva disposición de los bits de este campo; en donde los bits reservados tienen el valor de cero.

b0	b1	b2	b3	b4	b5	b6	b7
Reserved	Reserved	Locked Clock Bit 0 = not locked 1 = locked	Modulation Selection 0 = Not ERP-PBCC 1 = ERP-PBCC	Reserved	Length Extension Bit (ERP-PBCC)	Length Extension Bit (ERP-PBCC)	Length Extension Bit

Tabla 2.50. Definición de los Bits del Campos SERVICE[90]

De donde los bits b3, b5 y b6 han dejado de ser reservados para cumplir con las funciones antes detalladas.

[90] IEEE 802.11g, Institute of Electrical and Electronics Engineers, Pág. 19.

2.3.10.2.1.2Formato PPDU de Preámbulo Corto

Este preámbulo PPDU corto es el mismo que se usa para 802.11b, pero para este caso su implementación es obligatoria, por lo que es adecuado para los modos de 2, 5.5 y 11 Mbps.

2.3.10.2.1.3Formato PPDU ERP-OFDM

Tanto el formato, preámbulo y encabezados para el PPDU PLCP ERP-OFDM son los mismo que se uso en 802.11a.

2.3.10.2.1.4Formato PPDU de Preámbulo Largo DSSS-OFDM

Ambos, el encabezado y preámbulo largo y corto que fueron descritos anteriormente son nuevamente usados en DSSS-OFDM.

Para todas las tasas DSSS-OFDM y modos de preámbulos, el campo SIGNAL, debe tener el valor para 3 Mbps, este valor es un valor inicial para asegurar compatibilidad con las BSS y asegurarse que las estaciones NonERP lean el campo y estimen este uso del medio.

El PSDU esta anexado a un preámbulo y encabezado PLCP; el preámbulo PLCP es el mismo descrito para 802.11b, mientras que el encabezado es similar al descrito anteriormente para preámbulos largos PPDU y el formato PSDU es idéntico al revisado para 802.11a.

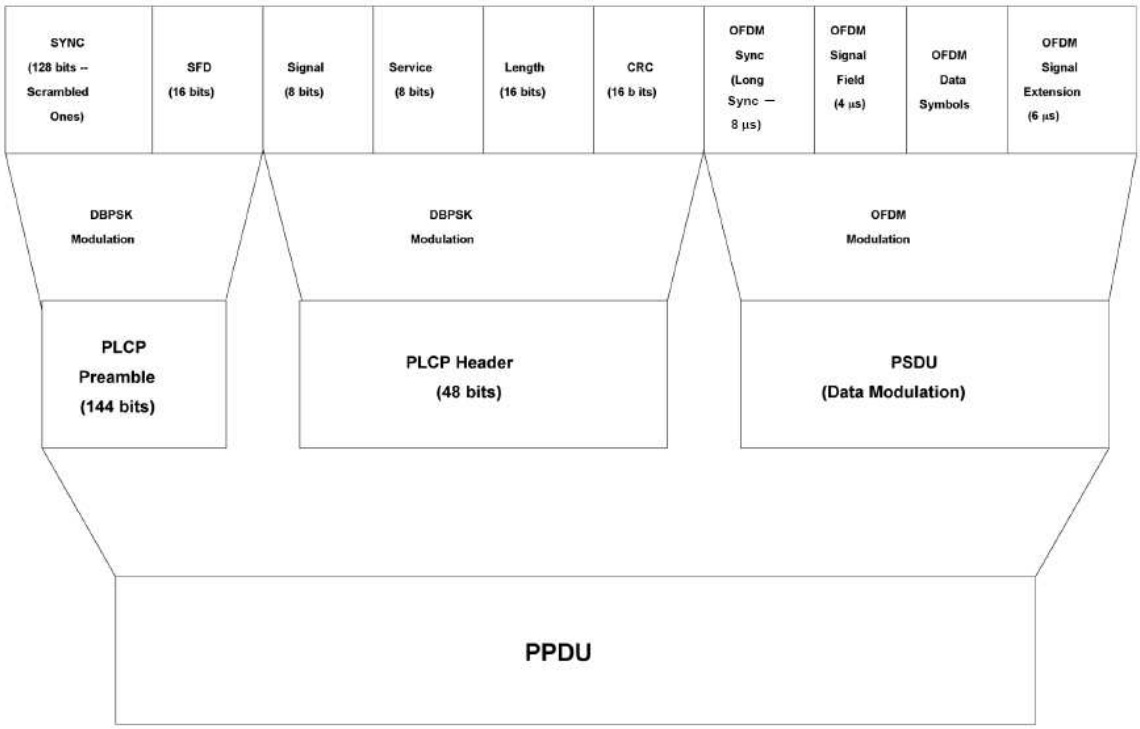


Figura 2.83. Formato PPDU de Preámbulo Largo para DSSS-OFDM[91]

2.3.10.2.1.5Formato PPDU PLCP DSSS-OFDM Corto

En este caso se usa el formato de preámbulo corto PLCP que describió anteriormente, el cual ayuda a maximizar el throughput del sistema.

De la misma manera que en el caso anterior el preámbulo es el mismo que el usado para 802.11b, el encabezado es igual al descrito previamente para 802.11g y el PSDU tiene remembranza con el PSDU de 802.11a.

[91] IEEE 802.11g, Institute of Electrical and Electronics Engineers, Pág. 22.

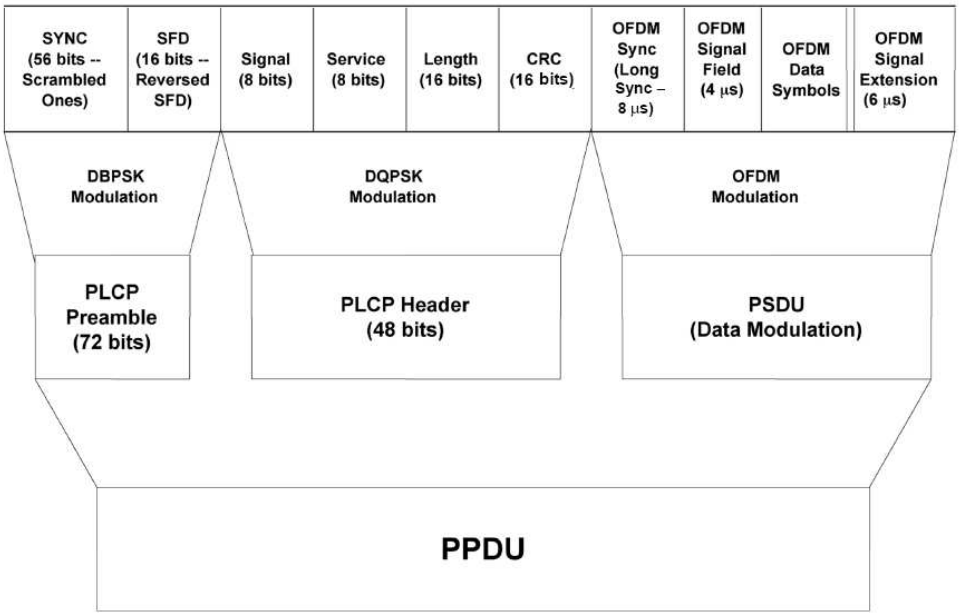


Figura 2.84. Formato PPDU de Preámbulo Corto para DSSS-OFDM[92]

2.3.10.2.2 Cambio de Tasa y Modulación de Datos PLCP

2.3.10.2.2.1 Formatos de Preámbulos Cortos y Largos

El preámbulo corto y largo y el encabezado largo se transmiten a 1 Mbps y una modulación DBPSK; el encabezado PLCP corto se debe transmitir a 2 Mbps.

Para la transmisión del PSDU existen 4 formatos de modulación que son obligatorios: 1 y 2 Mbps ERP-DSSS; 5.5 y 11 Mbps ERP-CCK.

De igual manera para la transmisión del PSDU existen 4 formatos de modulación opcionales; todos están basados en una codificación convolucional binaria de paquete (PBCC), a 5.5, 11, 22, 33 Mbps; las dos primeras tasas son las mismas descritas para 802.11b así como su máscara espectral.

2.3.10.2.2.2 Formatos ERP-PBCC a 22 y 33 Mbps

Estos dos formatos se encuentran codificados mediante un codificador convolucional binario de paquete, el cual tiene 126 estados y una tasa de 2/3.

[92] IEEE 802.11g, Institute of Electrical and Electronics Engineers, Pág. 23.

La forma en la que este formato alcanza las velocidades de 33 Mbps para la sección de datos es usando un reloj de 16.5 MHz, fuera de este cambio la modulación es la misma que para 22 Mbps.

2.3.10.2.2.3Formatos ERP-OFDM

La modulación y tasas de transferencia son las mismas que las estudiadas en 802.11a.

2.3.10.2.2.4Formato PLCP DSSS-OFDM Corto y Largo

Las tasas del PSDU son varias debido a que este se compone de cuatro partes principales: una secuencia de entrenamiento larga, un campo signal, los símbolos de datos y un campo de extensión signal.

El primer componente se transmite de la misma manera que la secuencia en 802.11a; el campo signal se transmite a 6 Mbps con modulación OFDM, mientras que los datos se transmiten con modulación OFDM a 6, 9, 12, 18, 24, 36, 48 o 54 Mbps, al igual que con 802.11a; finalmente el campo de extensión signal es un periodo de tiempo de no transmisión (6 μs).

2.3.10.3 Especificaciones Operacionales PMD ERP

La capa física de los sistemas ERP deben atenerse a las especificaciones que rigen para la banda de 2.4 GHz.

Es decir que las frecuencias de canal de operación son las mismas que las revisadas para 802.11b, así como los números de canal. De la misma manera los niveles de potencia de transmisión deben atenerse a la norma antes mencionada.

2.3.10.4 Especificaciones de Operación ERP

Para los equipos que se ajustan a los sistemas ERP, se tiene ciertas especificaciones de funcionamiento propias, diferentes a las revisadas en algún modelo de capa física anterior.

Uno de ellos es el nivel de entrada máxima, el cual esta alrededor de los -20 dBm medido en los conectores de la antena, para todas las tasas de transferencia de datos soportadas por los sistemas ERP.

La máscara espectral de transmisión para 802.11g esta compuesta en realidad por dos máscaras, la primera para modos ERP-OFDM y otra para ERP-DSSS.

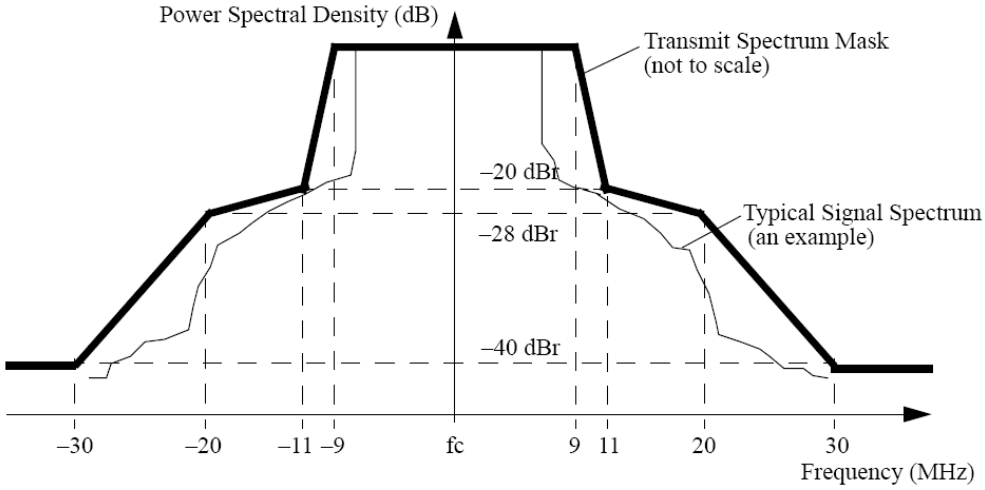


Figura 2.85. Máscara Espectral de Transmisión para los Modos ERP-OFDM

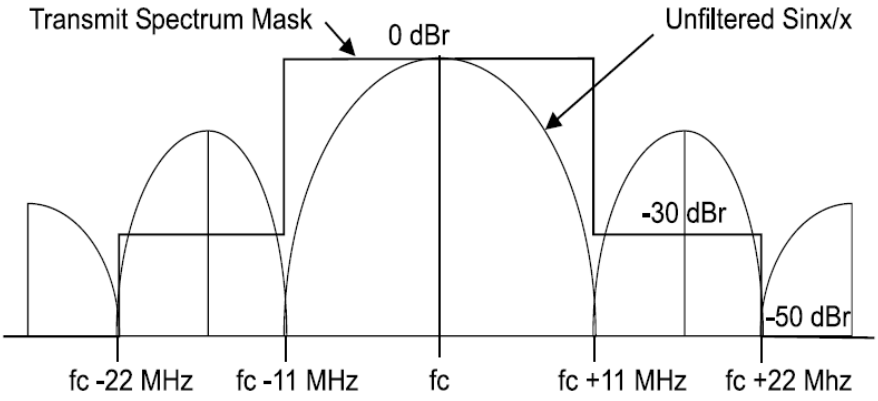


Figura 2.86. Máscara Espectral de Transmisión para los Modos ERP-DSSS

2.3.10.5 Especificaciones de Operación ERP-PBCC

Tal como se reviso con anterioridad, los sistemas 802.11g poseen varios modos de funcionamiento, en algunos las especificaciones de operación han sido las mismas que las revisadas para otros estándares, pero en otros casos dichas especificaciones son únicas, en este caso revisaremos las especificaciones de operación para los modos ERP-PBCC.

Los niveles de sensibilidad de entrada mínimos en el receptor son de -76 dBm par el modo de 22 Mbps, y de -74 dBm para el modo de 33 Mbps.

2.3.10.6 Subcapa PMD de Tasa de Transferencia Extendida

La subcapa ERP acepta las primitivas de servicio de la subcapa PLCP y provee de los medios por los cuales los datos son transmitidos o recibidos por el medio; las funciones combinadas tanto de las primitivas de la subcapa PMD de tasa de transferencia extendida y los parámetros de la función de recepción, resulta en una cadena de datos, información de sincronización y parámetros de la señal recibida asociada son entregados a la subcapa PLCP; una funcionalidad similar es provista para la transmisión de datos.

2.3.10.6.1 Revisión de la Interacciones

Las primitivas asociadas con la subcapa PLCP para el ERP están dispuestas en dos categorías principales:

- ✓ Primitivas de servicio que soportan interacciones PLCP de par a par.
- ✓ Primitivas de servicio que tienen significancia local y soportan interacciones entre capas.

2.4 WiMAX

2.4.1 Introducción

Esta tecnología nace gracias a la necesidad del desarrollo e implementación de redes de banda ancha al rededor del mundo; debido a que el despliegue de redes cableadas es costoso en tiempo y recursos, WiMAX nace como solución ideal, ya que ofrece un acceso inalámbrico de banda ancha, capaz de complementar las redes cableadas existentes con una fiabilidad y desempeño similar.

2.4.1.1 Bandas de Frecuencia

Como ya se mencionó, esta tecnología al igual que WiFi es inalámbrica, pero su alcance es mayor por lo que las aplicaciones dependen del espectro que se decida usar; en este caso tenemos varias bandas de frecuencias en las cuales se ha definido que WiMAX funcione.

2.4.1.1.1 Bandas Licenciadas de 10 a 66 GHz

Dentro de las bandas de 10 a 66 GHz, teniendo en cuenta que se requiere de línea de vista (LOS), se puede tener tasas de datos de 120 Mbps, lo cual las vuelven excelentes para los servicios con accesos punto multipunto (PMP), es decir que los usuarios de esta tecnología dentro de esta banda de frecuencias serian pequeñas oficinas (SOHO) o aplicaciones para empresas grandes.

2.4.1.1.2 Frecuencias por Debajo de los 11 GHz

Si se tiene frecuencias por debajo de los 11 GHz, no se necesita línea de vista (NLOS) y existe multipath, lo que permite entregar los servicios y las funcionalidades ofrecidas por esta tecnología en lugares con poca o ninguna línea de vista.

2.4.1.1.3 Frecuencias por Debajo de los 11 GHz sin Licencia

Las capacidades de WiMAX dentro de estas bandas sin licencia, especialmente para las bandas de 5 a 6 GHz son las mismas que para las bandas licenciadas por debajo de los 11 GHz, sin embargo se debe tener en cuenta que si opera dentro de estas bandas, se aumentara la interferencia y existirán problemas de coexistencia, especialmente si debido a

normas locales se debe tener limitaciones de potencia mayores a las previstas dentro del funcionamiento normal de los equipos.

Para estas frecuencias, la capa física y MAC se ven mejoradas con mecanismos de selección dinámica de frecuencias, para detectar y evitar las interferencias.

2.4.1.2 Modelo Referencial

La tecnología WiMAX esta compuesta de dos capas, la primera la capa MAC y la capa física, las cuales se adaptan al modelo de referencia OSI.

La capa MAC esta compuesta de tres subcapas, la primera es la subcapa de convergencia de servicios específicos (CS), la cual se encarga de realizar cualquier transformación o mapeo de los datos de red externos, recibidos por el punto de acceso de servicio CS, en unidades de datos de servicio MAC recibidos a su vez por la subcapa de parte común MAC (CPS).

La segunda subcapa denominada MAC CPS provee las funciones de núcleo MAC de acceso al sistema, ubicación de ancho de banda, establecimiento de conexión y mantenimiento de la misma; recibe los datos de varios CS, por medio de la MAC SAP.

La calidad de servicio (QoS) se aplica a la transmisión y el manejo de los datos en la capa física.

La capa MAC contiene una subcapa de seguridad separada, la cual provee los servicios de autenticación, intercambio de llave compartida y encriptación.

Los datos, el control de la capa física y las estadísticas son transferidos entre la MAC PCS y la capa física mediante el punto de acceso de servicio de capa física (PHY SAP).

Por su parte la capa física incluye una serie de especificaciones, cada una varia según el rango de frecuencia de operación y las aplicaciones que tenga que soportar.

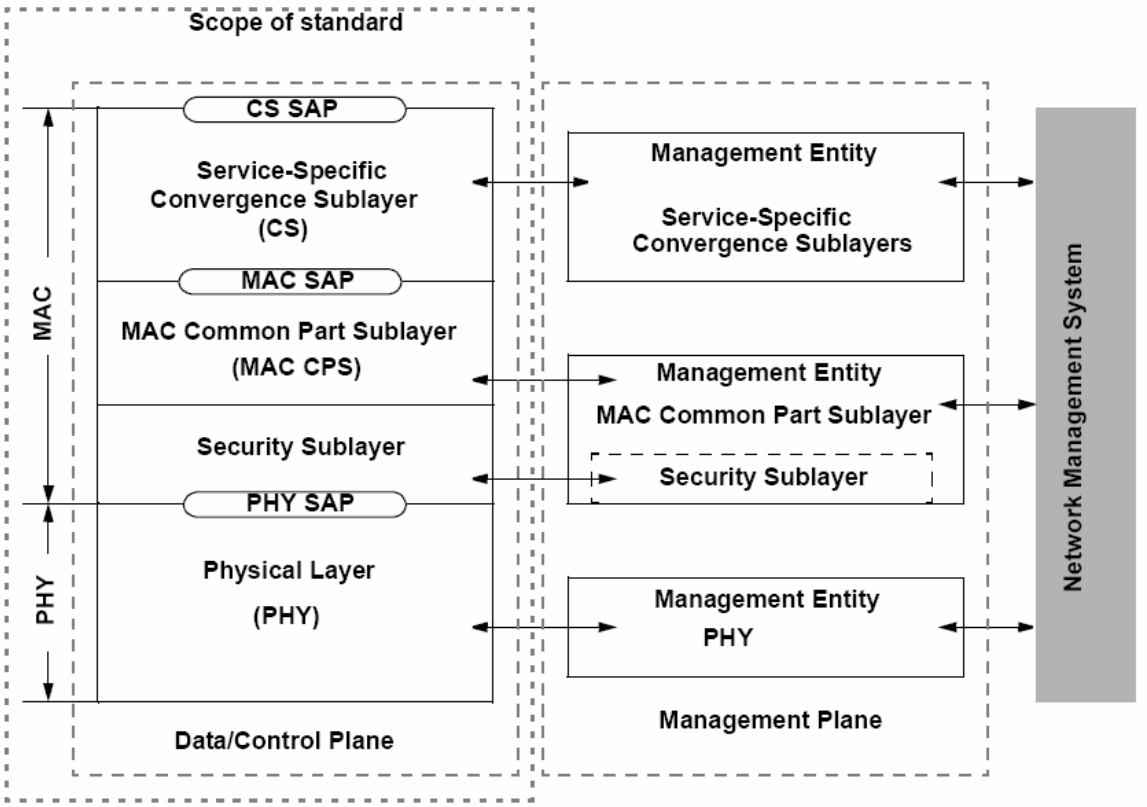


Figura 2.87. Esquema del Modelo de Referencia WiMAX[93]

2.4.2 CS de Servicios Específicos

La subcapa de convergencia de servicios específicos se encuentra encima de la subcapa MAC CPS, y utiliza los servicios provistos por dicha capa.

Las funciones que desempeña esta subcapa son los siguientes:

- Acepta las unidades de datos de protocolo (PDU) de capa superior, de la capa inmediatamente superior.
- Realiza la clasificación de los PDU de capa superior.
- Procesa los PDU en caso de ser necesario según su clasificación.
- Entrega los PDU CS al punto de acceso de servicio MAC apropiado.
- Recibe los PDU CS de la entidad par.

Se encuentran definidas dos especificaciones para la subcapa de convergencia, una subcapa de convergencia ATM y una subcapa de convergencia de paquete.

[93] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 3.

2.4.2.1 CS ATM

Esta subcapa es una interfase lógica que se encarga de la asociación de diferentes servicios ATM con el punto de acceso de servicio CPS MAC.

La CS ATM acepta las celdas ATM de las capas superiores ATM, realiza una clasificación y en caso de ser provisto realiza una supresión del encabezado, para después entregar los PDU CS a la SAP MAC más apropiada.

2.4.2.1.1 Definición de Servicio CS

La subcapa de convergencia ATM esta específicamente diseñada para soportar la convergencia de los PDU generados por el protocolo de capa ATM de una red ATM.

2.4.2.1.2 Plano Datos y Control

2.4.2.1.2.1 Formatos PDU

Las unidades de datos de protocolo (PDU) CS ATM deben consistir de un encabezado PDU CS ATM, y una carga PDU CS ATM; esta carga debe ser la misma que la carga de una celda ATM.

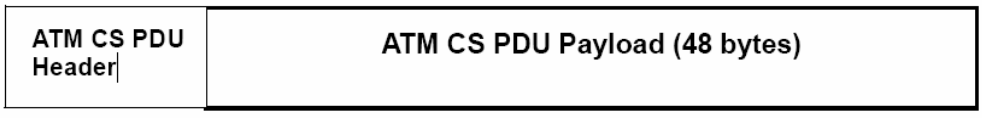


Figura 2.88. Formato PDU CS ATM

2.4.2.1.2.2 Clasificación

Una conexión ATM, la cual esta definida de forma única por un par de valores, el identificador de camino virtual (VPI) y el identificador de canal virtual (VCI), correspondientes al canal virtual (VC) o el camino virtual (VP).

En el modo VP conmutado, todos los VCI dentro de un VPI de entrada son automáticamente procesados en un VPI de salida; en el modo VC conmutado, los valores de entrada VPI/VCI son procesados individualmente en valores VPI/VCI de salida.

De esta manera al realizar la supresión del encabezado (PHS), la CS ATM diferencie dos tipos de coerciones y realice la supresión correspondiente.

Un clasificador es un conjunto de criterios que se aplican a cada celda ATM que entra en la subcapa de convergencia ATM; el clasificador consiste de algunos criterios como el VPI, VCI y una referencia para un identificador de conexión (CID).

Si una celda ATM coincide con los criterios de selección especificados, pasa al SAP MAC para ser entregado al identificador de conexión por el CID.

2.4.2.1.2.2.1 Modo VP Conmutado

Para el modo VP conmutado, el campo VPI constituido por 20 bits, es procesado en un CID de 16 bits, este procesamiento se realiza en la conexión MAC que haya sido establecida; debido a que los parámetros QoS y categoría de servicio se determinan al establecer la conexión, el procesamiento garantiza el correcto manejo del trafico por parte de la capa MAC

2.4.2.1.2.2.2 Modo VC Conmutado

Para el modo VC conmutado, los campos VPI y VCI, en total 52 bits son procesados en un CID de 16 bits por la conexión MAC establecida; ya que el QoS y la categoría de servicio se determinan al establecer la conexión, este procesamiento garantiza el correcto manejo del tráfico por parte del MAC.

Se debe tener en cuenta que todas las combinaciones VPI/VCI no pueden ser soportadas simultáneamente por este modo.

2.4.2.1.2.3 PHS

Al realizar la supresión del encabezado, una parte repetitiva de la carga del encabezado de las unidades de datos de servicio del CS es suprimida por la entidad transmisora y restablecida por la entidad receptora.

Para guardar mayor ancho de banda, las celdas ATM que compartan el mismo CID pueden ser empacadas y transportadas por una PDU de CPS MAC.

Cuando se apaga el PHS ninguna parte del encabezado de celda ATM debe ser suprimido. Si el PHS esta o no activado, se puede observar en el mensaje de petición de adición de servicio dinámico (DSA-REQ), en la creación de la conexión, al igual que los VPI o VPI/VCI.

2.4.2.1.2.3.1 PHS para las Conexiones ATM VP Conmutadas

En el modo VP conmutado, el VPI se procesa en un CID, esto permite que se descarte el remanente del encabezado de celda ATM, a excepción del VCI, el indicador de tipo de carga (PTI) y la prioridad de pérdida de celda (CLP), los cuales son encapsulados en un encabezado PDU CS.

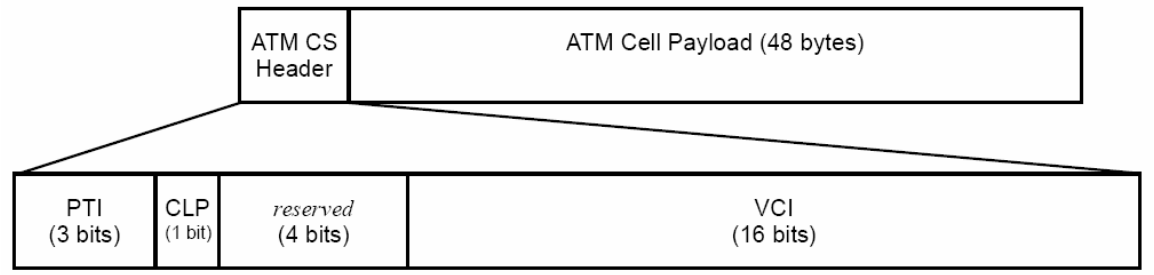


Figura 2.89. Formato PDU CS para Conexiones ATM VP Conmutadas[94]

2.4.2.1.2.3.2 PHS para las Conexiones ATM VC Conmutadas

En el modo VC conmutado, las combinaciones VPI/VCI son procesadas en un CID, esto permite dispensar de los remanentes del encabezado de celda ATM, con la excepción del PTI y CLP; estos campos son encapsulados en un encabezado PDU CS.

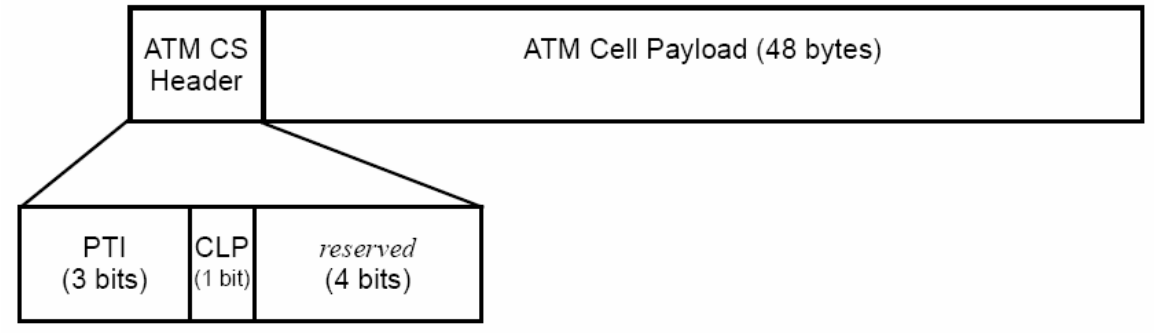


Figura 2.90. Formato PDU CS para Conexiones ATM VC Conmutadas[95]

[94] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 19.
[95] IBID 94

2.4.2.2 CS de Paquete

La subcapa de convergencia de paquete, se encuentra encima de la subcapa de parte común MAC; la CS realiza las siguientes funciones:

- ✓ Clasificación del PDU de protocolo de capa superior en una conexión apropiada.
- ✓ Supresión de la información del encabezado, esta función en opcional.
- ✓ Entrega de los resultantes PDU CS a la SAP MAC asociada con el flujo de servicio para transporte con la SAP MAC par.
- ✓ Recepción de la PDU CS de su par SAP MAC.
- ✓ Reconstrucción de cualquier información de encabezado suprimido, es opcional.

La CS es la responsable de entregar los SDU MAC al punto de acceso de servicio MAC; por otro lado la capa MAC es la responsable de la entrega de los SDU MAC entre los pares SAP MAC, según el QoS, fragmentación, concatenación y otras funciones de transporte asociadas a características de flujo de servicio de una conexión en particular.

La CS es responsable también por la recepción del SDU MAC de su par SAP MAC y entregarlo a la entidad de capa superior.

La subcapa de convergencia de paquete es usada para trasportar todo tipo de datos de protocolos basados en paquetes, tal como Internet Protocol (IP), Point-to-Point Protocol (PPP); y, Ethernet.

2.4.2.2.1 Formato SDU MAC

Una vez que se ha clasificado y asociado los PDU de capa superior con un tipo de conexión MAC, estos deben ser encapsulados en un formato SDU MAC, el cual esta compuesto de un campo denominado índice de supresión de carga de encabezado (PHSI), el cual debe estar presente cunado se ha aplicado algún PHS, y el PDU.

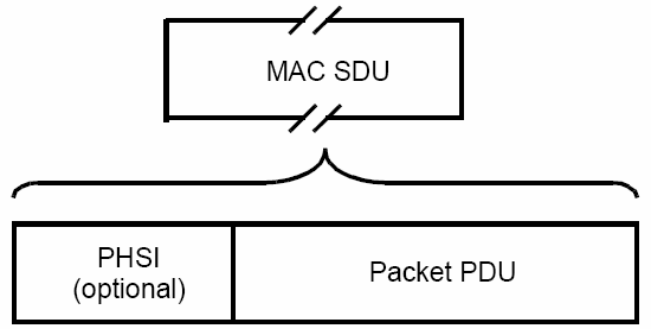


Figura 2.91. Formato SDU MAC

2.4.2.2.2 Clasificación

La clasificaron es el proceso por el cual un SDU MAC es procesado en una conexión en particular para la transmisión entre pares MAC. Dicho proceso asocia un SDU MAC con una conexión, la cual también crea una asociación con las características de flujo de servicio de la conexión; este proceso facilita la entrega de los SDU MAC ateniéndose a las características QoS.

El clasificador es un criterio de selección aplicado a cada paquete entrante a la red WiMAX; este consiste en criterios de selección de paquetes de protocolo específicos, un clasificador de prioridad, y una referencia para un CID; si el paquete concuerda con el criterio, pasa al SAP para ser entregado según la conexión definida por el CID.

Las características de flujo de servicio de la conexión provee el QoS para el paquete.

Varios clasificadores pueden referirse al mismo flujo de servicio; la prioridad de clasificador es usada para ordenar la aplicación de clasificación para paquetes; un orden explicito es necesario ya que algunas patentes usadas por los clasificadores pueden coincidir, se establecen clasificadores de bajada en las estaciones base y clasificadores de subida en las estaciones de subscriptor.

2.4.2.2.3 PHS

En la PHS, una parte repetitiva del encabezado de la capa superior es suprimida en el SDU MAC por la entidad transmisora y restablecida por la entidad receptora, la implementación de PHS es opcional.

El transmisor usa clasificadores para hacer un mapa de los paquetes en el flujo de servicio, el clasificador realiza un mapa único de paquete para su regla PHS asociada; el receptor usa el CID y el índice PHS (PHSI) para restaurar el campo PHS (PHSF).

Una vez que un PHSF ha sido asociado a un PHSI, no debe ser cambiado; cambiar el valor del PHSF de un flujo de servicio, representa establecer una nueva regla PHS, remover la anterior del flujo de servicio y colocar la nueva; en caso de eliminar un clasificador, cualquier regla PHS asociada debe ser eliminada también.

Toda estación base debe asignar todos los valores PHSI como todos los valores CID; tanto el transmisor como receptor deben especificar el PHSF y el tamaño PHS (PHSS), esto permite a los encabezados pre configurados o no incluidos en esta tecnología establecer el cache de entrada.

2.4.2.2.3.1 Operación PHS

La estación de subscriptor (SS) realiza sus reglas de clasificación; si una regla concuerda el resultado debe ser un flujo de servicio de subida, CID, y una regla PHS. La regla PHS provee los PHSF, PHSI, PHSM (máscara PHS), PHSS y PHSV (PHS valido), si el PHSV esta seteado o no esta presente, la SS debe comparar los bytes del encabezado con los bytes en el PHSF que deben suprimirse según la PHSM, si concuerdan, la SS debe suprimir todos los bytes en el PHSF de subida excepto los bytes enmascarados por la PHSM; luego la SS debe fijar el PDU con el PHSI y formar la SDU MAC, pasándolo al SAP MAC para su transporte de subida.

La capa MAC de la estación base (BS) debe determinar el CID asociado mediante la revisión del encabezado MAC genérico; la capa MAC de BS envía el PDU al SAP MAC

asociado con ese CID; la CS de paquete receptora usa el CID y el PHSI para encontrar el PHSF, PHSM y PHSS; la BS reensambla el paquete y procesa el paquete en forma normal.

Este proceso se repite para las operaciones en downlink, intercambiando las operaciones de la BS y SS.

2.4.2.2.4 Parte Específica Ethernet 802.3

Los PDUs Ethernet son procesados en un SDU MAC, se debe tener en cuenta que puede pasar el PDU tal como viene o puede tener supresión en el encabezado.

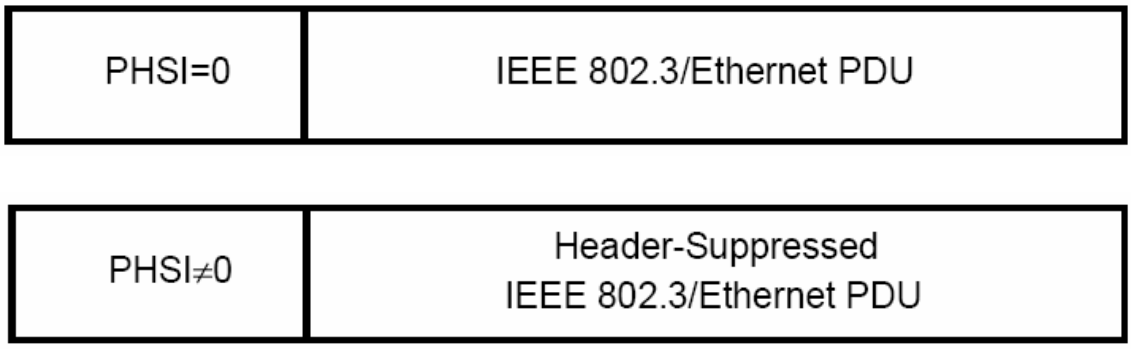


Figura 2.92.- Formato PDU CS Ethernet con y sin Supresión de Encabezado[96]

Dentro de los clasificadores CS de Ethernet encontramos los siguientes parámetros: dirección MAC de origen y destino y el tipo Ethernet.

2.4.2.2.5 Parte Especifica VLAN 802.1Q

Tal como se reviso para Ethernet, los PDUs DS VLAN deben tener el siguiente formato, ya se con supresión de encabezado o no.

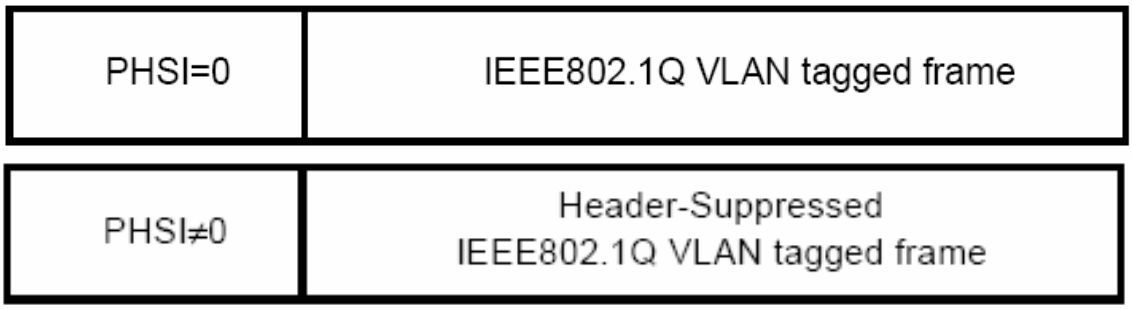


Figura 2.93. Formato PDU CS VLAN con y sin Supresión de Encabezado[97]

[96] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 27.

Dentro de los clasificadores CS los siguientes parámetros son de importancia: Las direcciones de origen y destino MAC, y el tipo Ethernet.

2.4.2.2.6 Parte Específica IP

El formato de los PDU CS IP con o sin supresión de encabezado debe tener el siguiente formato:

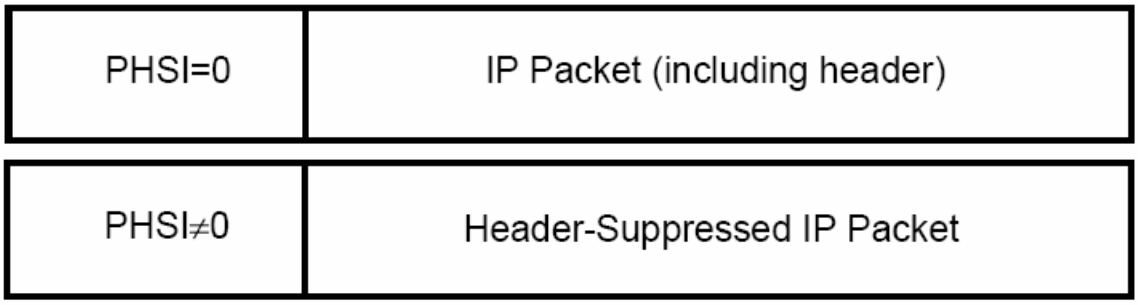


Figura 2.94. Formato PDU CS IP con y sin Supresión de Encabezado[98]

Los parámetros más importantes de los clasificadores IP son los campos del encabezado IP y protocolo de transporte.

2.4.3 Subcapa de Parte Común MAC

Una red que utilice un medio compartido como lo es el medio inalámbrico debe tener un mecanismo eficiente para poder compartir dicho medio; redes inalámbricas punto-multipunto de dos vías y redes con topología de malla, son dos ejemplos de eficiencia al compartir el medio inalámbrico.

2.4.3.1 PMP (Punto-Multipunto)

El enlace de bajada, es decir de la estación base al usuario, opera sobre las bases de los sistemas PMP; el enlace inalámbrico WiMAX opera con una estación base central y antenas sectoriales, capaces de manejar varios sectores independientes simultáneamente.

En un canal dado y un sector de antena, todas las estaciones reciben la misma transmisión o partes de esta; la BS es el único transmisor operando en esta dirección, de tal manera que transmite sin tener que coordinar con las otras estaciones, excepto por la

[97] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 28.
[98] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 29.

duplexión por división de tiempo (TDD), el cual divide el tiempo en periodos de transmisión de downlink y uplink.

El downlink es generalmente broadcast; en casos en el que el mapa de downlink no especifique que porción de la trama de downlink le corresponde a determinada estación, todas las estaciones capaces de escuchar lo harán, estas estaciones revisaran el CID y retendrán solo los PDU que les pertenezcan.

Las estaciones de subscriptor comparten el enlace de subida a la BS basados en los principios de la demanda; dependiendo de la clase de servicio utilizado, la SS puede tener derechos continuos de transmisión, o el derecho a la transmisión puede ser otorgado por la BS luego de recibir una petición del usuario.

Además de mensajes a direcciones únicas, se pueden enviar mensajes en conexiones multicast, como broadcast a todas las estaciones.

Dentro de un sector, los usuarios se atienen al protocolo de transmisión que controla las contenciones entre los usuarios, y permite que el servicio sea confeccionado según el retraso y requerimientos de ancho de banda según la aplicación de cada usuario; esto se logra cuatro diferentes tipos de mecanismos de planificación de uplink.

Esto se logra usando polling, procedimientos de contención, y otorgando anchos de banda no solicitados.

El uso del polling simplifica las operaciones de acceso y garantiza que las aplicaciones reciban servicio de una forma determinística si es necesario; en general las aplicaciones de datos toleran los retardos, pero las aplicaciones de tiempo real como voz o video requieren de un servicio con bases más uniformes y algunas veces con un control estricto de planificación.

La capa MAC esta orientada a conexión, con el propósito de tener varios niveles de QoS y procesar servicios para las SS. Flujos de servicio pueden ser provistos cuando una SS se instala en el sistema; después de que una SS se haya registrado, conexiones son

asociadas con estos flujos de servicio, de forma adicional se pueden establecer nuevas conexiones cuando el servicio de un usuario necesite cambiar.

Una conexión define tanto el procedimiento entre procesos convergentes entre pares que utilizan la capa MAC y el flujo de servicio; el flujo de servio define los parámetros de QoS para los PDUs que están siendo intercambiados en la conexión.

El concepto de un flujo de servicio en una conexión es esencial para la operación del protocolo MAC; los flujos de servicio proveen un mecanismo de gestión del QoS para uplink y downlink; particularmente, los flujos de servicio son fundamentales para el proceso de asignación de ancho de banda; una estación de subscriptor solicita ancho de banda de uplink en una conexión entre pares básica. El ancho de banda se asigna por la BS a una SS como una suma de asignaciones en respuesta a las peticiones de conexión entre pares desde la SS.

Las conexiones una vez que se establecen pueden requerir de un mantenimiento activo; los requerimientos del mantenimiento pueden variar dependiendo del tipo de servicio conectado.

Una conexión puede ser terminada; generalmente ocurre cuando cambia el servicio de usuario establecido; esta finalización de conexión es solicitada por la SS o la BS.

2.4.3.2 Malla

La principal diferencia entre un PMP y modo de malla opcional es que en el modo PMP, solo existe tráfico entre la BS y las SS, mientras que en malla, el tráfico puede pasar entre otras SS y directamente entre SS. Dependiendo del algoritmo protocolar usado, esto puede realizarse sobre igualdad, mediante una planificación distribuida, o basándonos en la superioridad de la malla BS, lo cual resulta en una planificación centralizada; o finalmente mediante una combinación de ambas.

Dentro de una red de malla, un sistema que tiene conexión directa a los servicios principales fuera de la red, se denomina estación base de malla; todos los demás sistemas de una red malla son las SS de malla; en general, los sistemas de una red malla son denominados nodos; dentro del contexto de una malla, las conexiones de uplink y

downlink se definen como el tráfico en la dirección de la BS de malla y el tráfico saliente de la BS de malla respectivamente.

Se deben definir tres términos importantes en un sistema de malla, estos son el vecino, vecindario y vecindario extendido; las estaciones con las cuales un nodo tiene lasos directos son llamados vecinos, los vecinos de un nodo forman un vecindario, los vecinos de un nodo se consideran que están a un salto de distancia del nodo, y finalmente un vecindario extendido contiene a los vecinos del vecindario.

En un sistema de malla ni la BS de malla puede transmitir sin haberlo coordinado con los otros nodos; usando una planificación distribuida, todos los nodos incluyendo la BS de malla deben coordinar sus transmisiones dentro de un vecindario de dos saltos, y deben transmitir sus agendas a todos sus vecinos; de forma opcional la planificación puede ser establecida por una petición y otorgamientos no coordinados entre dos nodos.

Los nodos deben asegurarse de que las transmisiones resultantes no causen colisiones con el tráfico de datos y control dentro de la agenda de cualquier otro nodo dentro del vecindario de dos saltos de distancia; este mecanismo es el mismo para uplink y downlink.

Usando una planificación centralizada, los recursos son otorgados de una forma más centralizada, la estación base de malla recolectara las peticiones de recursos de todas las estaciones dentro de un determinado rango de salto; determinara la cantidad de recursos otorgados para cada enlace en la red, para uplink y downlink, y las comunicara a todas las estaciones dentro de un rango de saltos; los mensajes de otorgación no contienen toda la planificación, cada nodo lo calculara usando el algoritmo de predicción y los parámetros dados.

Todas las comunicaciones están dentro del contexto de un enlace, el cual se establece entre dos nodos; un enlace será usado para las transmisiones de datos entre los dos nodos.

El QoS se provee mediante mensajes enviados a través del enlace, no se asocian ni servicios o QoS a un enlace, pero casa mensaje unicast tiene parámetros de servicio en el encabezado.

2.4.3.3 Plano de Datos y Control

2.4.3.3.1 Direcciones y Conexiones

2.4.3.3.1.1 PMP

Cada SS tiene una dirección MAC universal de 48 bits, similar a la usada en Ethernet y WiFi.

Las conexiones son identificadas por un CID de 16 bits; al inicializar una estación de subscriptor, dos pares de conexiones de gestión se establecen entre la SS y la BS, un tercer par de conexiones de gestión puede generarse de forma opcional, lo que permite tres niveles de QoS para el manejo de trafico entre la BS y la SS.

El uso de un CID de 16 bits permite un total de conexiones de 64 Kbps en cada canal de uplink y downlink.

2.4.3.3.1.2 Malla

Todo nodo debe tener una dirección MAC universal de 48 bits.

Un nodo una vez que ha sido autorizado por la red recibe un identificador de nodo de 16 bits, este identifica al nodo durante operaciones normales, este identificador de nodo se transfiere en el sub encabezado de malla, siguiendo al encabezado MAC genérico, tanto en mensajes de unicast como multicast.

Para poder direcciones los nodos dentro del vecindario local, un identificador de enlace de 8 bits debe ser usado, cada nodo debe asignar un ID a cada enlace que establece con sus vecinos, este ID de enlace se transmite como parte del CID en el encabezado genérico MAC en un mensaje de unicast. Este identificados de enlace se usa para distribuir la planificación entre los nodos.

2.4.3.3.2 Formatos PDU MAC

El formato de un PDU MAC consiste de tres campos, el primero es en encabezado MAC genérico de longitud fija, luego una carga PDU MAC, que de estar presente puede ser ceros, sub encabezados y ceros, o más SDUs MAC y/o fragmentos de los mismos; esta carga es de longitud variable, lo que le permite a la capa MAC tener varios tipos de tráficos de capas superiores sin necesidad de conocer los formatos o patrones de bits de aquellos mensajes; y finalmente tiene un campo CRC que es opcional y obligatorio para ciertas capas físicas.

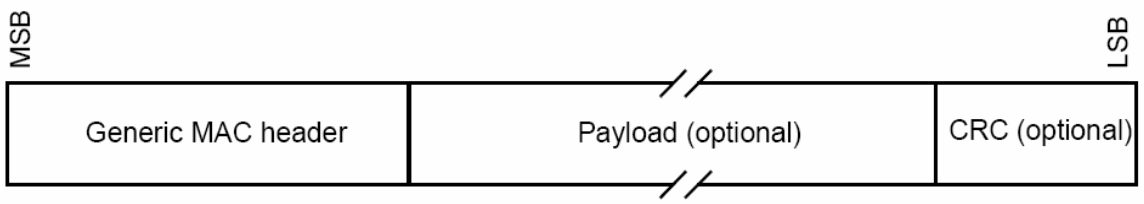


Figura 2.95. Formato PDU MAC[99]

2.4.3.3.2.1 Formatos de Encabezados MAC

Existen dos tipos de formatos de encabezados MAC, el primero es un formato genérico, el cual encabeza todos los PDU MAC de gestión o datos; el segundo es un encabezado para el pedido de ancho de banda, en caso de necesitarse ancho de banda adicional.

Todos los encabezados tienen encripción, desde el primer byte del encabezado.

Para poder distinguir el un encabezado del otro, nos valemos del campo Tipo de Encabezado (HT), en caso de ser cero es un encabezado genérico; a continuación se mostrara los dos encabezados.

[99] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 35.

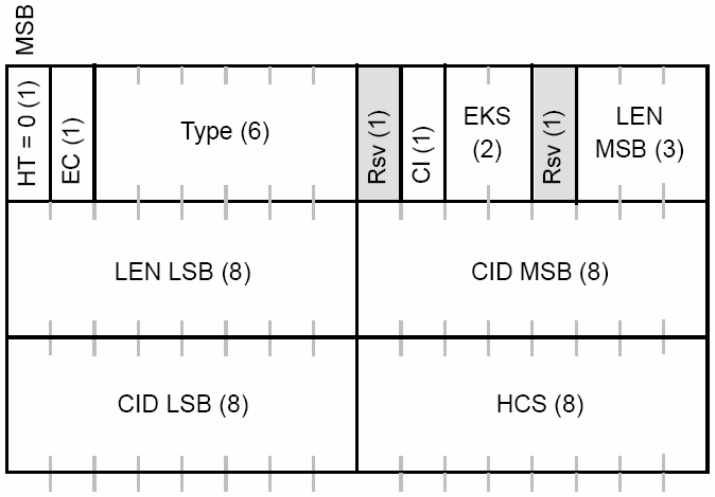


Figura 2.96. Formato de Encabezado Genérico MAC[100]

Name	Length (bits)	Description
CI	1	CRC Indicator 1 = CRC is included in the PDU by appending it to the PDU Payload after encryption, if any 0 = No CRC is included
CID	16	Connection identifier
EC	1	Encryption Control 0 = Payload is not encrypted 1 = Payload is encrypted
EKS	2	Encryption Key Sequence The index of the Traffic Encryption Key (TEK) and Initialization Vector used to encrypt the payload. This field is only meaningful if the EC field is set to 1.
HCS	8	Header Check Sequence An 8-bit field used to detect errors in the header. The transmitter shall calculate the HCS value for the first five bytes of the cell header, and insert the result into the HCS field (the last byte of the MAC header). It shall be the remainder of the division (Modulo 2) by the generator polynomial $g(D = D^8 + D^2 + D + 1$ of the polynomial D^8 multiplied by the content of the header excluding the HCS field. (Example: [HT EC Type]=0x80, BR=0xAAAA, CID=0x0F0F; HCS should then be set to 0xD5).
HT	1	Header Type. Shall be set to zero.
LEN	11	Length. The length in bytes of the MAC PDU including the MAC header and the CRC if present.
Type	6	This field indicates the subheaders and special payload types present in the message payload.

Tabla 2.51. Campos del Encabezado Genérico MAC

[100] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 36.

Type bit	Value
#5 most significant bit (MSB)	Mesh subheader 1 = present, 0 = absent
#4	ARQ Feedback Payload 1 = present, 0 = absent
#3	Extended Type Indicates whether the present Packing or Fragmentation Subheaders, is Extended 1 = Extended 0 = not Extended. Applicable to connections where ARQ is not enabled
#2	Fragmentation subheader 1 = present, 0 = absent
#1	Packing subheader 1 = present, 0 = absent
#0 least significant bit (LSB)	Downlink: FAST-FEEDBACK Allocation subheader Uplink: Grant Management subheader 1 = present, 0 = absent

Tabla 2.52. Descripción del Campo Type

Por otro lado en encabezado de petición de ancho de banda, consiste de una petición de ancho de banda y no debe contener carga.

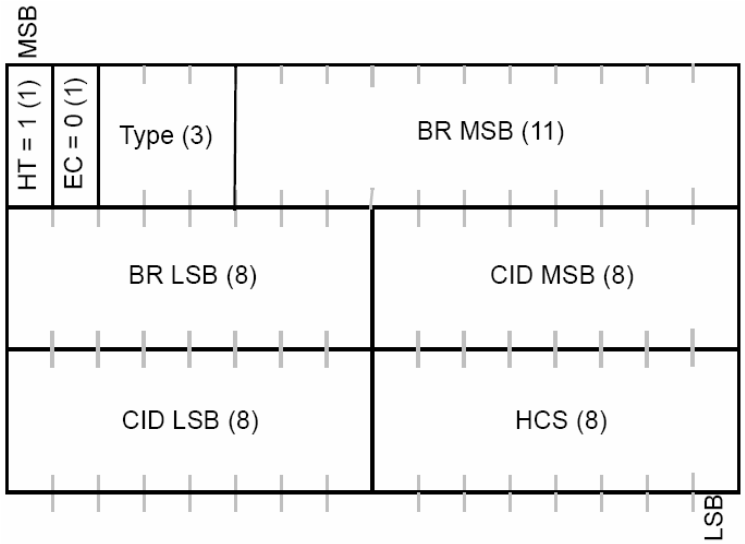


Figura 2.97. Formato del Encabezado de Petición de Ancho de Banda[101]

La petición de ancho de banda debe tener las siguientes propiedades:

- La longitud del encabezado debe ser de 6 bytes siempre.
- El campo EC debe estar en cero, indicando no encripción.
- El CID debe indicar la conexión por la cual el ancho de banda de uplink se requiere.

[101] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 37.

- El campo BR debe indicar el número de bytes pedidos.
- Los tipos permitidos de ancho de banda pedido son 000 para incremento y 001 para agregado.

Si una estación de subscriptor recibe una petición de incremento de ancho de banda debe descartar el PDU.

Name	Length (bits)	Description
BR	19	Bandwidth Request The number of bytes of uplink bandwidth requested by the SS. The bandwidth request is for the CID. The request shall not include any PHY overhead.
CID	16	Connection identifier
EC	1	Always set to zero
HCS	8	Header Check Sequence Same usage as HCS entry in Table 5
HT	1	Header Type = 1
Type	3	Indicates the type of bandwidth request header

Tabla 2.53. Campos del Encabezado de Petición de Ancho de Banda

2.4.3.3.2.2 Sub-Encabezados MAC y Cargas Especiales

Existen cinco tipos de sub encabezados; cuatro de ellos sub encabezados de pares PDU: Malla, fragmentación, FAST-FEEDBACK_Allocation y Gran Gestión; estos van después del encabezado genérico, en caso de tener sub encabezados de fragmentación y de gran gestión, este ultimo ira primero, en caso de tener un sub encabezado de malla, este va primero que cualquier otro y el encabezado FAST-FEEDBACK_Allocation va al ultimo.

Finalmente el último sub encabezado es el de pares SDU, y es el sub encabezado de empaquetado; los sub encabezados de empaquetado y fragmentación son excluyentes, pero en caso de estar los dos se debe dar prioridad al que se encuentre primero.

2.4.3.3.2.3 Mensajes de Gestión MAC

Existe un grupo de mensajes de gestión MAC, estos mensajes deben ser transportados en la carga del PDU MAC; todos los mensajes deben empezar con un campo de tipo de mensaje de gestión y contener más campos.

Los mensajes que viajes a través de las conexiones básicas, de broadcast y de rango inicial no deben ser fragmentados o empaquetados, mientras que los mensajes bajo conexiones primarias pueden ser fragmentados o empaquetados.

Para las capas físicas SCa, OFDM y OFDMA, los mensajes transmitidos bajo las cuatro conexiones antes mencionadas, deben usar CRC.

Figura 2.98. Formato de los Mensajes de Gestión MAC[102]

2.4.3.3.3 Construcción y Transmisión de PDU MAC

2.4.3.3.3.1 Convenciones

Los datos son transmitidos de acuerdo a las siguientes reglas:

- Los campos de los mensajes MAC y campos de tiempo, longitud y valores (TLV), se transmiten como una secuencia de sus dígitos binarios, comenzando con el bit más significativo.
- Campos específicos como SDU o fragmentos correspondientes son transmitidos en el mismo orden de bytes a como son recibidos de las capas superiores.
- Campos especificados como cadenas son transmitidas en el orden de símbolos de la cadena.

2.4.3.3.3.2 Concatenación

Múltiples PDU MAC pueden ser concatenados en una sola transmisión, tanto para uplink como downlink; debido a que cada PDU MAC esta identificado por un CID único, la entidad MAC de recepción es capaz de presentar el SDU MAC al SAP MAC adecuado. Los mensajes MAC, datos, peticiones de ancho de banda pueden ser concatenados en una misma Transmisión.

[102] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 43.

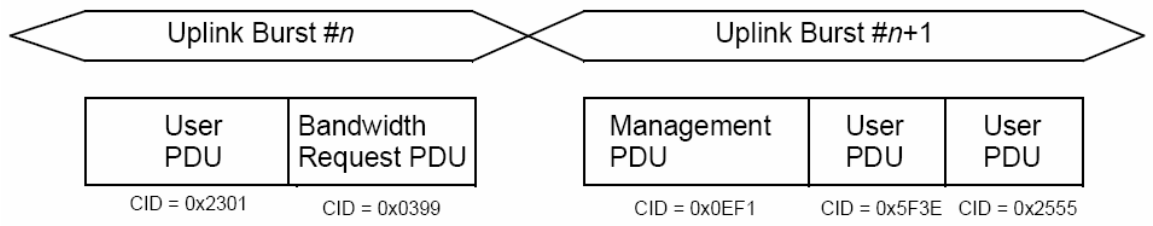


Figura 2.99. Ejemplo de la Concatenación PDU MAC[103]

2.4.3.3.3.3 Fragmentación

La fragmentación es el proceso en el cual un SDU MAC se divide para su transmisión en varios PDU; este proceso se realiza para permitir un uso eficiente del ancho de banda disponible relativo a los requerimientos de QoS de un flujo de servicio de una conexión.

Las características de fragmentación como las de reensamble son obligatorias para los equipos bajo la norma WiMAX.

La autoridad de realizar fragmentación al tráfico de una conexión se establece cuando la conexión se crea por el SAP MAC, dicha fragmentación puede iniciarse por la BS o la SS según estemos en downlink o uplink.

Durante las conexiones que no tengan activada la petición de repetición automática (ARQ), se usa un número de secuencia otorgado a cada fragmento, de manera que se pueda determinar si se han perdido paquetes intermedios, en caso de una perdida, la entidad de recepción descartara los PDU MAC hasta tener un nuevo fragmento inicial o un PDU sin fragmentación.

Para conexiones con ARQ activado, los fragmentos se forman para cada conexión concatenando un grupo de bloques ARQ con números de secuencia adyacentes; el valor de número de secuencia de bloque (BSN) del sub encabezado de fragmentación es el BSN para el primer bloque ARQ que aparece en el segmento.

[103] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 123.

2.4.3.3.3.4 Empaquetado

Si el empaquetado es activado en una conexión, la capa MAC puede empaquetar varios SDU MAC en un solo PDU MAC; del lado del transmisor se tiene la total discreción de realizar o no el empaquetamiento, sin embargo la capacidad de realizar el desempaquetamiento es obligatoria.

Se realizan empaquetamientos para SDU de longitudes fijas y variables, y de la misma manera se realizan diferentes procesos cuando se activa o no el ARQ.

2.4.3.3.3.5 Calculo del CRC

Un flujo de servicio puede necesitar de un chequeo de redundancia cíclica (CRC) para cada PDU MAC de datos llevado por ese flujo de servicio, de ser este el caso, un CRC igual a los definidos para la tecnología Ethernet es añadido a la carga del PDU.

Este CRC cubrirá al encabezado genérico MAC y la carga; este debe ser calculado después de la encriptación.

2.4.3.3.3.6 Encriptación PDU MAC

Cuando se transmite un PDU por una conexión que tiene una asociación de seguridad (SA), el transmisor debe realizar una encriptación y autenticación de datos de la carga PDU tal como lo especifica el SA; y el receptor debe realizar la desencripción y la autenticación.

El encabezado genérico MAC no se encripta debido a que este lleva la información de encripción necesaria para su desencripción.

La información de encriptación tiene un periodo de vida, en especial el número de secuencia de llave, el cual es periódicamente renovado, la BS tiene nueceros de secuencia de llave independientes para cada conexión y va realizando el incremento de este campo.

Al comparar el número de secuencia de llave del PDU recibo con el que se supone se a el correcto, tanto la SS o la BS puede establecer fácilmente una perdida de sincronización,

para que se pueda tener un servicio ininterrumpido, las estaciones deben tener a la mano los dos últimos números de las secuencias de llave, además del presente.

Todo PDU que se reciba bajo una conexión SA que no este encriptado debe ser descartado.

2.4.3.3.3.7 Padding

En caso de que el espacio entre las ráfagas de datos sea al menos del tamaño del encabezado, este espacio debe ser inicializado, de manera que tengamos un PDU MAC de espacio no usado, en este caso el CID debe tener el valor denominado CID de padding; los valores de tipo y demás llevaran los valores de cero y se le tomara como un PDU normal.

2.4.3.3.4 Servicios de Planificación

Los servicios de planificación representan los mecanismos que posee la capa MAC para la planificación de datos al momento de su transporte en una conexión.

Existen cuatro servicios: servicio de otorgación sin solicitud (UGS), servicio de polling en tiempo real (rtPS), servicio de polling sin tiempo real (nrtPS), y el mejor esfuerzo (BE).

El UGS esta diseñado para tramas de datos de tiempo real las cuales consistan en paquetes de datos de tamaño fijo en intervalos periódicos, tales como T1/E1, VoIP sin supresión de silencio; los QoS que se aplican al mismo son tasa de trafico sostenido máximo, latencia máxima, tolerancia al jitter, política de petición/transmisión.

El rtPS, nos presta servicio para tramas de datos en tiempo real, las cuales posean paquetes de datos de tamaño variable a intervalos periódicos, como video MPEG; por otro lado los parámetros QoS usados son tasa de trafico reservada mínima, tasa de trafico sostenido máximo, latencia máxima y política de petición/transmisión.

En tercer lugar nrtPS, nos permite manejar tramas de datos tolerantes a retrasos que tienen paquetes de datos de tamaño variable, estos requieren una tasa de datos mínima, como FTP; los parámetros QoS utilizados en este servicio son tasa de trafico reservada

mínima, tasa de trafico sostenida máxima, prioridad de trafico y política de petición/transmisión.

Finalmente el servicio BE, nos permite lidiar con tramas de datos las cuales no requieren un mínimo de servicio, por otro lado se manejan según la disposición de espacio, en este caso los parámetros QoS requeridos son tasa de tráfico sostenida máxima, prioridad de tráfico y política de petición/transmisión.

2.4.3.3.4.1 Planificación de Transmisión Sin Parámetros

Este tipo de planificaciones seleccionan los datos para las transmisiones en una ubicación de ancho de banda y trama en particular y se realiza mediante downlink o uplink según sea la BS o la SS respectivamente; además de cualquier otro factor que el planificador considere pertinente se deben tener en cuenta los siguientes para cada flujo de servicio:

- ✓ Los servicios de planificación especificados por el flujo de servicio.
- ✓ Los valores asignados a los parámetros QoS del flujo de servicio.
- ✓ La disponibilidad de datos para la transmisión.
- ✓ La capacidad del ancho de banda otorgado.

2.4.3.3.4.2 Planificación Petición/Otorgamiento de Uplink

Esta planificación la realiza la estación base con el intento de proveer a las SS de ancho de banda de uplink para transmisiones o la posibilidad de petición de ancho de banda; si se tiene un servicio planificado y sus QoS, una BS puede anticipar las latencias necesarias y desempeño del trafico de uplink y por ende puede anticipar los tiempos, otorgamientos o polling.

Scheduling type	PiggyBack Request	Bandwidth stealing	Polling
UGS	Not allowed	Not allowed	PM bit is used to request a unicast poll for bandwidth needs of non-UGS connections.
rtPS	Allowed	Allowed	Scheduling only allows unicast polling.
nrtPS	Allowed	Allowed	Scheduling may restrict a service flow to unicast polling via the transmission/request policy; otherwise all forms of polling are allowed.
BE	Allowed	Allowed	All forms of polling allowed.

Tabla 2.54. Servicios de Planificación y Reglas de Uso

2.4.3.3.4.2.1 UGS

Tal como se cito anteriormente, este servicio no sirve para aplicaciones en tiempo real con intervalos periódicos y tamaño de fijo de trama de datos; la BS debe proveer elementos de información de ráfaga de otorgación de datos a la SS en intervalos periódicos basados en el flujo de servicio de tasa de trafico sostenida máxima.

El tamaño de estos otorgamientos deben ser lo suficiente para mantener los datos de longitud fija asociados con el flujo de servicio, pero puede ser mayor según lo decida la BS.

Para que este servicio funcione de forma adecuada, la política de petición/transmisión debe ser tal que la SS esta prohibida de usar cualquier oportunidad de petición de contención para esta conexión; los elementos de información de servicio de llave son el trafico sostenido máximo, latencia máxima, tolerancia al jitter y política de petición/transmisión; en caso de estar presente, los parámetros de la tasa de tráfico reservado mínimo deben ser los mismos parámetros de la tasa de trafico sostenida.

El sub encabezado de gestión de otorgación es usado para pasar la información de estado de la SS a la BS, sin importar el estado del flujo de servicio UGS; el bit más significativo del campo gestión de otorgación es el indicador slip (SI), la SS debe activar esta bandera una vez que detecta que el flujo de servicio ha excedido su profundidad de cola de transmisión, una vez que la SS detecta que la cola de transmisión de flujo de servicio esta sin saturaciones, debe desactivar el SI.

Esta bandera le permite a la BS tener un compensación por adelantado de condiciones tales como la perdida de ruta o desajustes en la tasa de reloj, mediante el despacho de otorgaciones adicionales; el bit poll-me (PM) puede ser usado para pedir ser tomado en cuenta en el polling para una diferente conexión UGS.

La BS no debe colocar más ancho de banda que el indicado por el parámetro tasa de trafico sostenida máxima del grupo de parámetros del QoS; excepto en los caso en el que la bandera SI este activada; en caso de que suceda esto, la BS debe aumentar un 1% adicional de ancho de banda para compensar desajusten en la tasa de transmisión.

2.4.3.3.4.2.2 rtPS

Este servicio se usa para poder soportar aplicaciones en tiempo real con paquetes de datos de tamaños variables, tal como la transmisión de videos; este servicio ofrece oportunidades de petición unicast, periódicas y en tiempo real, las cuales encajan con las necesidades en tiempo real de los flujos y permiten que la SS especifique el tamaño de las otorgaciones deseadas. Este servicio requiere de más peticiones que el UGS, pero tamaños de otorgaciones variables para optimizar la eficiencia de transporte de datos.

La BS debe proveer oportunidades de petición unicast periódicamente; para que el servicio funcione correctamente, las características la política de petición/transmisión deben ser tales que la SS esta prohibida de usar cualquier oportunidad de petición de contención para dicha conexión.

La BS puede encargar oportunidades de petición de unicast como se menciono anteriormente, aún si existen peticiones previas sin cumplirse; por ende la SS usa loa las oportunidades de petición de unicast para poder obtener oportunidades de transmisión de uplink.

2.4.3.3.4.2.3 nrtPS

Este servicio ofrece polls unicast, las cuales aseguran que el flujo de servicio reciba las oportunidades de petición aun en congestión de la red; la BS típicamente entrega los CID nrtPS en intervalos de un segundo o menos.

La BS debe proveer oportunidades de petición de unicast continuamente; para que este servicio funcione correctamente, los parámetros de la política de petición/transmisión deben ser tales que la SS sea capaz de usar la oportunidades de petición de contención; esto tiene como resultado que la SS utilice las oportunidades de petición tanto como las oportunidades de petición de unicast y tipos de ráfagas de otorgaciones de datos sin solicitud.

2.4.3.3.4.2.4 Servicio BE

El servicio BE tiene como propósito el proveer un servicio eficiente para trafico de características del mejor esfuerzo; para que este servicio funcione correctamente, los parámetros de la política de petición/transmisión deben ser tales que la SS sea capaz de usar las oportunidades de petición de contención; esto da como resultado que la SS use las oportunidades de petición de contención tanto como las oportunidades de petición de unicast y los tipos ráfagas de otorgación de datos sin solicitud.

2.4.3.3.5 Colocación de Ancho de Banda y Mecanismos de Petición

En cada entrada y consiguiente inicialización de una SS a la red, se le asigna uno de tres CID dedicados, con el propósito de enviar y recibir mensajes de control. Dichos pares de conexiones son usados para permitir niveles QoS diferenciados para diferentes conexiones que llevan el tráfico de gestión MAC.

Incremento o decremento de los requerimientos de ancho de banda son necesarios para todos los servicio excepto para UGS; las necesidades de las incompresibles conexiones UGS no cambian durante la conexión; mientras que los requerimiento de las conexiones UGS compresibles varían según el trafico, tales como T1 con canalización.

Los servicios de acceso múltiple asignado por demanda (DAMA) han dado suficientes recursos para las asignaciones basadas en demanda, según las necesidades aumentan.

Cuando una SS necesita pedir ancho de banda a una conexión con servicio planificado BE, envía un mensaje para la BS el cual contiene los requerimientos inmediatos de la conexión DAMA; el QoS para la conexión fue determinado al momento del establecimiento de la conexión y es revisado por la BS.

Para que una SS pueda pedir ancho de banda de uplink a la BS existen varios mecanismos, los cuales se revisaran a continuación.

2.4.3.3.5.1 Petición

Este mecanismo hace referencia al proceso en el cual la SS le indica a la BS que necesita ancho de banda de uplink; esta petición puede venir de un encabezado de petición de ancho de banda o un pedido piggyback, la implementación del pedido piggyback es opcional.

Debido a que los perfiles de ráfaga de uplink pueden cambiar dinámicamente, todos los pedidos de ancho de banda deben estar hechos en términos del número de bits necesarios para transportar el encabezado MAC y su carga, pero no la carga de la capa física.
Los pedidos de ancho de banda pueden ser de incremento o decremento, cuando la BS recibe uno de incremento, debe aumentar la cantidad de ancho de banda pedido a la percepción actual de necesidad de ancho de banda de la conexión.

Cuando la BS recibe un pedido de ancho de banda agregado, este debe reemplazar su percepción de la necesidad de ancho de banda de la conexión con la cantidad de ancho de banda requerido.

La naturaleza auto correctiva del protocolo petición/otorgación requiere que la SS deba usar periódicamente las peticiones de ancho de banda agregadas; el periodo puede estar en función del QoS de un servicio y de la calidad del enlace.

Debido a las posibilidades de colisión, las peticiones de ancho de banda transmitidas en los elementos de información de petición de broadcast o multicast deben ser peticiones agregadas.

2.4.3.3.5.2 Otorgamientos

Para una SS, las peticiones de ancho de banda hacen referencia a conexiones individuales mientras que los otorgamientos de ancho de banda son direccionados a los CID básicos de las estaciones de subscriptor, no a CID individuales.

Debido a que es no determinístico la decisión por cual un pedido se cumple, cuando la SS recibe una oportunidad de transmisión más pequeña que la desperada, no se dan explicaciones. En todos los casos, basados en la última información recibida de la BS y el estado de la petición, la SS puede decidir entre retirarse y realizar una petición otra vez o descartar el SDU.

Una SS puede usar los elementos de información de petición que son transmitidos en dirección al grupo de polling de multicast del cual es miembro, o dirigida a su CID básico.

En todos lo casos, el perfil de ráfaga de elemento de información de petición es usada, aun si la BS es capaz de recibir la SS con un perfil de ráfaga más eficiente.

En un elemento de información de otorgación de datos dirigido a su CID básico, la SS puede realizar peticiones de ancho de banda para cualquiera de sus conexiones.

2.4.3.3.5.3 Polling

El polling es el proceso por el cual la estación base distribuye ancho de banda para las estaciones de subscriptor, con el único propósito de realiza peticiones de ancho de banda.

Estas distribuciones pueden ser para SS individuales o a grupos de SS; dichas distribuciones a grupos de conexiones y/o SS es en realidad la definición de elementos de información de petición de ancho de banda.
Cuando se realiza polling de unicast, a esta única estación se le da un ancho de banda suficiente para que responda con una petición de ancho de banda en caso de necesitarlo, a estaciones con UGS no se le da polling de unicast a menos que en sus transmisiones el bit PM este activado.

Cuando no se tenga ancho de banda suficiente para realizar un polling individual a un número de SS inactivas se realiza un polling de multicast o broadcast, esto se hace mediante el CID, para salvaguardar el ancho de banda solo las estaciones que lo necesiten responderán utilizando un algoritmo de contención para evitar colisiones.

2.4.3.3.5.4 Peticiones de Ancho de Banda Enfocadas en Contenciones para MAN Inalámbricas OFDM

La capa física MAN inalámbrica OFDM soporta dos mecanismos de petición de ancho de banda basados en contenciones; uno de los mecanismos es obligatorio y le permite a la estación enviar un encabezado de petición de ancho de banda durante la petición Region-Full, y en mecanismo opcional le permite enviar una transmisión de contención enfocada durante la petición Region-Focused.

La transmisión consiste de un código de contención modulado enviado mediante un canal de contención que posee cuatro portadoras.

2.4.3.3.5.5 Peticiones de Ancho de Banda CDMA basados en Contenciones para MAN Inalámbricas OFDMA

La capa física MAN inalámbrica OFDMA suporta dos mecanismos de petición de ancho de banda basados en contenciones, los cuales son obligatorios.

Las estaciones deben enviar un encabezado de petición de ancho de banda o usar el mecanismo basado en CDMA.

La estación selecciona uno de los códigos permitidos para realizar la petición de ancho de banda, por otra parte la estación base le asignara cierto uplink pero en vez de enviar un CID básico, le envía un CID de broadcast junto con un elemento de información de asignación CDMA, el cual le especifica la región de transmisión y el código usado por la SS.

Una vez que la estación determina que la asignación le pertenece, envía el PDU MAC de petición de ancho de banda y/o los datos, la estación no debe enviar este PDU de petición si la BS le indica esto a través del elemento de información de asignación CDMA.

2.4.3.3.5.6 Soporte Opcional de la Topología de Malla

Los sistemas inalámbricos HUMAN tienen la posibilidad de soportar la topología de malla, y a diferencia de los sistemas PMP, no existe una diferencia clara entre las tramas de uplink y downlink.

Debido a que los nodos en la topología malla se comunican entre ellos, la conexión entre ellos se realiza a través de las estaciones de subscriptor, por lo que las comunicaciones en todos los enlaces debe ser controlado por un algoritmo centralizado, planificando de una forma distribuida dentro del vecindario extendido de un nodo, o una combinación de los dos.

2.4.3.3.6 Soporte de Capa MAC de las Diferentes Capas Físicas

2.4.3.3.6.1 Duplexión por División de Frecuencia (FDD)

En un sistema FDD, los canales de uplink y downlink están colocados en diferentes frecuencias, de tal manera que los datos de downlink pueden ser transmitidos en ráfagas.

Se usa tramas de longitud fija tanto para el uplink y downlink, de tal forma que se facilite el uso de diferentes tipos de modulación; un beneficio es que se pueden tener estaciones operando en modos full y half duplex.

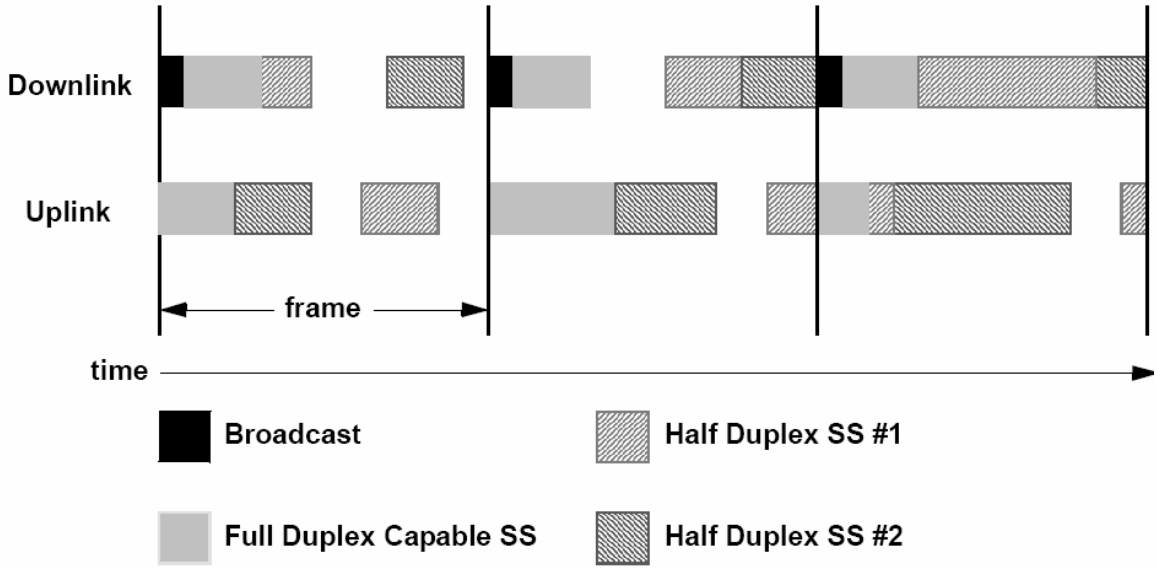


Figura 2.100. Ejemplo de una Asignación de Ancho de Banda de Ráfaga FDD.[104]

2.4.3.3.6.2 Duplexión por División de Tiempo (TDD)

Para los sistemas TDD, las transmisiones de uplink y downlink se realizan en diferentes momentos, bajo una misma frecuencia; las tramas TDD poseen una duración fija, y contienen una sub trama de uplink y downlink.

[104] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 152.

La trama se divide en una serie de ranuras físicas (PS), lo que facilita la repartición del ancho de banda.

La división entre el uplink y el downlink es un parámetro del sistema y es controlado por las capas de nivel superior.

2.4.3.3.6.3 DL-MAP

Los mensajes DL-MAP define el uso de los intervalos de downlink para una capa física en modo ráfaga.

2.4.3.3.6.4 UL-MAP

El UL-MAP define el uso del uplink en términos del offset de la ráfaga relacionada con el tiempo de inicio de la asignación.

2.4.3.3.6.5 Servicios MAC para Sistemas de Antenas Adaptativas

Los sistemas de antenas adaptativas usan más de una antena, esto les permite mejorar la capacidad del sistema así como el rango de la mismo, mediante el ajuste de la patente de la antena y concentrando su radiación para cada subscriptor individual.

La eficiencia espectral puede ser mejorada, otro aspecto que puede mejorarse es la ganancia SNR mediante la combinación de múltiples señales y dirigir esta ganancia a usuarios en particular.

Por el lado de uplink, las transmisiones de ráfaga no necesariamente mejoran el rango del sistema, sino que mejora la capacidad del mismo.

Los mecanismos definidos por la capa MAC permiten el uso en forma opcional de ASS, lo que significa que permiten el uso de arreglos adaptativos y al mismo tiempo mantienen compatibilidad con las estaciones de subscriptor que no permitan dicho mecanismo.

Cabe destacar que para la implementación de este tipo de sistemas se debe contar con las BS que sean compatibles con los arreglos adaptativos y con las SS con o sin capacidad ASS, esto se logra ya que las tramas no ASS tienen reservados campos para datos ASS, las estaciones que no sean compatibles simplemente ignoran estos campos.

2.4.3.3.7 Acciones de Contención

La BS controla la asignación de los canales de uplink a través de los mensajes UL-MAC y determina las mini ranuras que pueden colisionar.

El método de contención en caso de colisiones se basa en un retiro exponencial binario truncado, ubicando la ventana de retiro inicial de la SS con el valor de la ventana de retiro máxima de la BS.

Cuando una SS tiene información que enviar y quiere entrar al proceso de contención, envía su ventana de retiro interna, la estación selecciona un número al azar dentro de su ventana de retiro, el cual indica el número de transmisiones de contención que debe esperar para empezar a transmitir.

Una vez que ha esperado, antes de iniciar la transmisión espera la recepción un IE de tipo ráfaga de otorgación de datos, una vez que la SS la recibe, las acciones de contención terminan.

En caso de que se termine el número de veces que la SS debe diferir su transmisión y no haya recibido la IE después de esperar cierto tiempo, la SS debe aumentar la ventana de retiro en un factor de 2 y repetir el proceso.

En caso de que se alcance el máximo valor de la ventana de retiro se debe descartar el PDU.

2.4.3.3.8 Ingreso a la Red e Inicialización

Todos los sistemas WiMAX deben ser capaces de aplicar ciertos procedimientos antes de poder dar ingreso e inicializar un nuevo SS o nodo a su red, los procedimientos que se

describen serán únicamente para modos de operación PMP, los procesos para redes en modo malla se describirán más adelante.

Las fases que se debe pasar para ingresar e inicializarse son los siguientes:

- Escanear canales de downlink y establecer sincronización con la BS
- Obtener los parámetros de transmisión, mediante el mensaje de descripción de canal de uplink (UCD)
- Realizar ajustes
- Negociar habilidades básicas
- Autorizar la SS y realizar el intercambio de llave
- Registrarse
- Establecer la conectividad IP
- Establecer la hora del día
- Transferir los parámetros de operación
- Configurar las conexiones

La implementación de las siguientes fases es opcional a menos que se especifique que se trata de una SS gestionadas: Establecer la conectividad IP, establecer la hora del día y transferir los parámetros de operación.

Debemos tener en cuenta que cada SS tiene cierta información de identificación que proviene del fabricante: dirección MAC universal de 48 bits, y un certificado digital X.509 que evita se produzca clonaciones de estaciones.

2.4.3.3.8.1 Escaneo y Sincronización con el Downlink

En inicializaciones o después de perdidas de señal, la SS debe adquirir un canal de downlink.

La estación debe tener una memoria de almacenamiento no volátil en la cual almacenara los parámetros de operación, y debe primero intentar adquirir el canal de downlink que aparezca en esta memoria; en caso de falla debe escanear continuamente la frecuencia de downlink hasta encontrar una señal valida de downlink.

Una vez que los elementos de la capa física han adquirido sincronización, la capa MAC debe intentar adquirir los parámetros de control de downlink y posteriormente de uplink.

2.4.3.3.8.2 Obtener los Parámetros de Downlink

La capa MAC debe buscar los mensaje de gestión de capa MAC DL-MAP; la estación adquiere sincronización de capa MAC una vez que ha recibido al menos un mensaje DL-MAP.

La capa MAC se mantendrá sincronizada mientras reciba mensajes DL-MAP y DCD (descriptor del canal de downlink) en su canal. Si no se reciben estos mensajes en un determinado periodo de tiempo, la estación debe intentar reestablecer la sincronización.

2.4.3.3.8.3 Obtener Parámetros de Uplink

Después de la sincronización, para poder obtener los parámetros de uplink se debe esperar por el mensaje UCD (descriptor de canal de uplink), este es transmitido de forma periódica por la BS en todos los canales activos de uplink, teniendo una dirección de broadcast MAC como destino.

Si no logra encontrar un canal de uplink después de un tiempo, la estación debe volver a buscar otro canal de downlink.

De los parámetros de descripción de canal se puede determinar si el canal de uplink se puede usar, en caso de no poder ser usado, se debe volver a buscar otro canal de downlink; pero si se determina que se puede usar este canal, al SS debe extraer los parámetros de uplink del UCD; luego se espera por el siguiente DL-MAP y se extrae el periodo de sincronización.

Finalmente la SS debe esperar por un mapa de asignación de ancho de banda y debe transmitir según las especificaciones del mismo.

Si se deja de recibir mensajes UL-MAP en un determinado tiempo, la SS debe dejar de usar el canal y buscar un nuevo canal de downlink.

2.4.3.3.8.4 Ajuste Inicial y Ajustes Automáticos

El ajuste es el proceso de adquisición del offset de tiempo correcto y ajustes de potencia tales como que las transmisiones de la estación estén alineadas con un símbolo que marque el inicio de los límites de una mini ranura en las capas físicas SC y SCa, o alineadas con la trama de recepción de la BS para las capas físicas OFDM y OFDMA; otro ajuste es el recibir dentro de los umbrales de recepción apropiados.

Los retrasos de tiempo a través de la capa física deben ser constantes, cualquier variación en los delays debe ser tomado en cuenta en tiempo de guarda de uplink de capa física.

Para las capas físicas SC, SCa y OFDM, la SS debe enviar un mensaje RNG-REQ, el cual es enviado en un intervalo de ajuste inicial, y en caso de la capa física OFDMA, se debe enviar el código CDMA en el canal de uplink; en caso de no haber respuesta se reenvía el mensaje con mayor potencia, y cuando se reciba un mensaje con su dirección MAC la SS debe considerar la recepción del RNG-RSP como un éxito.

2.4.3.3.8.5 Calibración de los Parámetros de Ajuste

El ajuste de los parámetros locales en una SS como resultado de la recepción de un RNG-RSP es considerado como una implementación dependiente con las siguientes restricciones:

- Todos los parámetros deben estar dentro del rango aprobado en todo momento.
- Los ajusten en potencia deben iniciar a partir del valor inicial seleccionado al momento del ajuste inicial a menos existan parámetros de potencia validos en la memoria no volátil, de ser así se usara este valor.
- Los ajustes en potencia deben ser tanto en incremento como decremento según la cantidad que especifique el mensaje RNG-RSP.
- En caso de que durante la inicialización el nivel de potencia sea haya incrementado hasta si máximo y no se tenga respuesta de la BS se debe regresar al mínimo.

Cuando se recibe un RNG-RSP, la estación no debe transmitir hasta que las señales de radio frecuencia hayan sido ajustadas según los parámetros del RNG-RSP y se hayan estabilizado.

2.4.3.3.8.6 Negociar Habilidades Básicas

Inmediatamente después de haber terminado los procesos de ajuste, la SS le informa a la estación base sus habilidades básicas mediante la transmisión de un mensaje SBC-REQ, con las capacidades activadas.

La estación base responde con un mensaje SBC-RSP, en el cual todas las habilidades en común con de la BS y SS están activadas.

2.4.3.3.8.7 Autorización SS e Intercambio de Llave

La SS y la BS realizan la autorización e intercambio de llave según el protocolo PKM, este protocolo se revisara más adelante.

2.4.3.3.8.8 Registrarse

Este proceso es por el cual se que permite que una SS el ingreso a la red y una estación de subscriptor gestionada recibe su CID de gestión secundaria, y se vuelve de hecho gestionable.

Para registrarse con una BS, la SS debe enviar un mensaje REG-REQ a la estación base; la BS debe responder con un mensaje REG-RSP, mientras que para una SS que ha indicado ser una estación gestionada, el mensaje REG-RSP debe incluir el CID de gestión secundario.

Sin tener el REG-RSP, una SS no puede enviar tráfico a la red. La BS al recibir el REG-REQ de una SS gestionada, debe esperar por un TFTP-CPLT.

La SS puede incluir la versión de IP en uno de los parámetros del REG-REQ para indicar que versión de IP soporta en la conexión de gestión secundaria; si se incluye la versión de IP en la REG-REQ, la BS debe incluir la versión de IP en el REG-RSP para

indicarle a la SS cual es la versión de IP que debe usar en la conexión de gestión secundaria.

La BS debe indicar el uso de una de las versiones IP que maneja la SS; en caso de que no se incluya este parámetro en la REG-REQ, se debe concluir que solo se maneja IPv4, por lo que la falta de este parámetro en REG-RSP le indica a la SS que use IPv4 en la conexión de gestión secundaria.

2.4.3.3.8.9 Establecer Conectividad IP

Una vez terminado el registro, la SS debe invocar los mecanismos DHCP para poder obtener una dirección IP así como cualquier otro parámetro necesario para establecer una conectividad IP; en caso de que la estación tenga un archivo de configuración, la respuesta del DHCP debe contener el nombre del archivo que tienen los parámetros de configuración.

El establecimiento de la conectividad IP debe ser realizada sobre la conexión de gestión secundaria de la SS.

2.4.3.3.8.10 Establecer la Hora del Día

Las SS y la BS necesitan tener la fecha y hora actual; esto es un requerimiento para eventos de acceso temporizado para realizar extracciones por parte del sistema de gestión; este no necesita de autenticaciones y necesita ser preciso solo al segundo más cercano.

El protocolo mediante el cual la hora del día es extraída es el usado en la RFC 868[105], el cual se usa también en los protocolos TCP y UDP; tanto la petición como la respuesta se deben transferir usando UDP; el tiempo extraído del servido debe ser combinado con el offset de tiempo recibido de la respuesta DHCP para crear la hora local, este proceso se debe realizar sobre la conexión de gestión secundaria de la SS.

Cabe destacar que esta operación no es necesaria para un registro exitoso, sin embargo es necesaria para operaciones sobre la marcha, la adquisición de la hora del día es una

[105] RFC 868, Time Protocol, Mayo de 1983.

implementación dependiente, pero no se deben realizar más de tres peticiones en ningún periodo de cinco minutos.

2.4.3.3.8.11 Transferencia de Parámetros de Operación

Después de una sesión DHCP exitosa, la estación debe descargar el archivo de configuración de SS usando TFTP sobre la conexión de gestión secundaria de la SS.

El servidor de archivo de configuración TFTP se especifica en el campo “siaddr” de la respuesta DHCP.

Tanto los parámetros de los campos requeridos en la respuesta DHCP y el archivo de configuración son requerimientos mínimos para la interoperabilidad.

Una vez que se ha descargado el archivo de configuración, la SS debe notificar a la BS mediante la transmisión de un mensaje TFTP-CPLT bajo la conexión de gestión primaria; la transmisión debe continuar hasta que se reciba el TFTP-RSP de la BS, o cuando la SS termina la retransmisión por expiración de retransmisión.

2.4.3.3.8.12 Ingreso a la Red y Sincronización en el Modo Malla

La inicialización de un nodo y sus procesos de ingreso a la red en el modo malla son diferentes a los que se encuentran en el modo PMP.

Todo el proceso puede ser dividido en las siguientes etapas:

- ✓ Escanear redes activas y establecer sincronización áspera con la red.
- ✓ Obtener los parámetros de la red, mediante los mensajes MSH-NCFG.
- ✓ Abrir un canal de patrocinador.
- ✓ Autorización de Nodo.
- ✓ Realizar registro.
- ✓ Establecer conectividad IP.
- ✓ Establecer la hora del día.
- ✓ Transferir parámetros de operación.

Cada nodo contiene una dirección MAC universal de 48 bits, asignada por el fabricante, el cual se usa para identificar el nodo durante la inicialización y autenticación con un nodo vecino.

2.4.3.3.8.12.1 Escaneo y Sincronización Áspera de la Red

Durante la sincronización o después de la perdida de señal, el nodo debe escanear mensajes MSH-NCFG, para adquirir la sincronización con la red, el nodo extrae los parámetros de tiempo del mensaje.

El nodo debe tener una memoria no volátil en la cual debe guardar los parámetros de operación, debe intentar recobrar sincronización usando los parámetros de esta memoria, si falla debe escanear posibles canales dentro de la banda de operación hasta encontrar una.

Una vez que el nodo se ha sincronizado con la red, se debe adquirir los parámetros de la red y realizar una lista de sus vecinos.

2.4.3.3.8.12.2 Obtener los Parámetros de la Red

El nodo debe seguir recibiendo los mensajes MSH-NCFG hasta que reciba del mismo nodo dos mensajes y reciba un MSH-NCFG: Network Descriptor con un ID de operación que coincida con el suyo, y debe al mismo tiempo construir una lista de sus vecinos.

De la lista de vecinos selecciona uno que tenga un ID lógico de red, una vez que el nodo candidato ha seleccionado a su nodo patrocinador, lo usa para obtener las habilidades básicas y realizar el proceso de autorización, para lo cual el nodo candidato le pide al nodo patrocinador que abra un canal de patrocinador para un intercambio de mensajes más efectivo.

2.4.3.3.8.12.3 Abrir un Canal de Patrocinador

El nodo candidato envía un mensaje MSH-NENT: NetEntryRequest al nodo patrocinador para que abra el canal; si lo rechaza se reintenta y en caso de no tener éxito se termina el patrocinio.

Si se acepta el mensaje, el nodo patrocinador responde con un mensaje MSH-NENT: NetEntryAck y abre el canal; pudiendo ser usado inmediatamente después de recibir el mensaje de aceptación, una vez que sucede esto, el nodo candidato se convierte en un nodo patrocinador.

Una vez que el canal se ha establecido se realiza el intercambio de mensajes y al terminar el nodo candidato termina el proceso mediante el mensaje MSH-NENT: NetEntryClose y lo confirma mediante el MSH-NCFG: NetEntryAck.

2.4.3.3.8.12.4 Negociar las Habilidades Básicas

En el modo de operación de malla una vez que se ha establecido el enlace lógico, se negocia las habilidades básicas tal como en el modo PMP, el nodo actúa como la SS.

2.4.3.3.8.12.5 Autorización de Nodo

Se debe realizar los procesos de seguridad PMK al igual que para modos PMP, siendo el nodo candidato la SS, el nodo patrocinador debe dirigir la información hasta en nodo autorizador, este autoriza o no si el nodo puede unirse a la red.

2.4.3.3.8.12.6 Registro de Nodo

El registro es el proceso mediante el cual se le asigna al nodo su ID de nodo; el nodo patrocinador debe canalizar la información al nodo registrador y se produce el registro.

2.4.3.3.8.12.7 Establecer la Conectividad IP

El nodo debe adquirir su dirección IP usando DHCP; este proceso se realiza mediante el canal de patrocinador.

2.4.3.3.8.12.8 Establecimiento de la Hora del Día

El nodo en una red tipo malla obtiene la hora del día usando el protocolo definido en la RFC 868; los mensajes deben ser llevados mediante UDP en el canal de patrocinador.

2.4.3.3.8.12.9 Transferencia de los Parámetros de Operación

Una vez que se obtiene la dirección IP, el nodo debe descargar un archivo de parámetros usando TFTP.

2.4.3.3.8.12.10 Estableciendo Enlaces con los Vecinos

Después de entrar a la red, un nodo puede establecer enlaces con otros nodos además de su patrocinador, mediante el siguiente procedimiento:

a) El nodo A envía un reto: HMAC {Operator Share Secret, frame number, Node ID of node A, Node ID of node B}; el operator shared secret es una llave privada obtenida por el proveedor, el frame number es el ultimo número de trama recibido del nodo B.

b) El nodo B después de la recepción, calcula el mismo valor del ítem a) y compara, si no coinciden, envía un rechazo, si coinciden, el nodo acepta el enlace y responde con un reto HMAC {Operator Shared Secret, frame number, Node ID of node B, Node ID of node A}, además selecciona de forma aleatoria un ID de enlace sin usar, que de ahora en adelante deberá indicar el enlace entre el nodo B y A.

c) El nodo A después de la recepción, calcula el mismo valor del ítem b) y compara, si el valor no coincide envía un rechazo, si coincide, el nodo A envía una aceptación; además selecciona de forma aleatoria un ID de enlace, que identificara el enlace entre el nodo A y B.

2.4.3.3.9 QoS (Calidad de Servicio)

2.4.3.3.9.1 Teoría de Operación

Entre los requerimientos para QoS se pueden tener los siguientes:

- Una configuración y función de registro para pre configuración de flujos de servicio QoS basados en SS y parámetros de tráfico.
- Una función de señalización para establecimientos dinámicos de flujos de servicio QoS habilitados y parámetros de tráfico.
- Utilización del planificador MAC y parámetros de trafico QoS para flujos de servicio uplink.
- Utilización de parámetros de trafico QoS para flujos de servicio downlink.
- Agrupamiento de las propiedades de flujo de servicio en clases de servicios etiquetadas, de tal manera que las entidades de capa superior y aplicaciones externas puedan pedir flujos de servicio con parámetros QoS deseados en una manera conciente general.

El mecanismo principal para proveer QoS es la asociación de paquetes atravesando la interfase MAC en un flujo de servicio identificado por un CID; un flujo de servicio es un flujo unidireccional de paquetes que son provistos por un QoS en particular; la SS y BS proveen este QoS de acuerdo al grupo de parámetros QoS definidos por el flujo de servicio.

El propósito general de las características QoS es la de definir orden de transmisión y planificación sobre la interfase aire; sin embargo estas características necesitan funcionar con mecanismos fuera de la interfase para poder garantizar un QoS de extremo a extremo.

Existen flujos de servicio para uplink y downlink sin haber sido activados para el transporte de datos, todos los flujos de servicio tienen un SFID de 32 bits y un CID de 16 bits.

2.4.3.3.9.2 Flujos de Servicio

Un flujo de servicio es un servicio de transporte MAC que provee transporte unidireccional de paquetes ya sea paquetes de uplink desde la SS o paquetes de downlink desde la BS.

Un flujo de servicio esta caracterizado por un grupo de parámetros QoS como latencia, jitter, seguros de throughput; para estandarizar las operaciones entre la SS y BS, estos atributos incluyen detalles de cómo la SS pide asignación de ancho de banda de uplink y el comportamiento esperado del planificador de uplink de la BS.

Un flujo de servicio esta caracterizado parcialmente por los siguientes atributos:

ID de flujo de servicio: una SFID se asigna a cada flujo de servicio existente, la SFID sirve como el identificador principal del flujo de servicio en la red, un flujo de servicio tiene al menos un SFID y una dirección asociada.

CID: asociado a un SFID que existe solo cuando la conexión posee un flujo de servicio activo o admitido.

ProvisionedQoSParamSet: Un grupo de parámetros QoS provisto por medio de capa superior.

AdmittedQoSParamSet: Define un grupo de parámetros QoS para los cuales la BS esta reservando recursos, el mayor recurso es ancho de banda, pero también puede ser memoria o recursos de tiempo necesarios para activar el flujo.

ActiveQoSParamSet: Define un grupo de parámetros QoS que indican el servicio que esta proveyendo actualmente el flujo de servicio, solo un flujo de servicio activo puede enviar paquetes.

Modulo de Autorización: Una función lógica dentro de la BS que aprueba o niega cada cambio relacionado con los parámetros QoS y clasificadores asociados con un flujo de servicio, tal como un sobre que limita los posibles valores de AdmittedQoSParamSet y ActiveQoSParamSet.

El ActiveQoSParamSet es un subgrupo del AdmittedQoSParamSet, el cual es un subgrupo del sobre autorizado.

En el modelo de autorización dinámica este sobre es determinado por el modulo de autorización (AuthorizedQoSParamSet); en el modulo de autorización provisto, este sobre se determina por el ProvisionedQoSParamSet.

Es útil pensar en tres tipos de flujo de servicio:

- Provisto: Este flujo de servicio es conocido vía aprovisionamiento, como el sistema de gestión de red; los parámetros AdmittedQoSParamSet y ActiveQoSParamSet son nulos.
- Admitido: Este tipo de flujo de servicio tiene recursos reservados por la BS para sus AdmittedQoSParamSet, pero estos parámetros son nulos, ya que el flujo de servicio admitido puede haber sido provisto por otro mecanismo.
- Activo: Este flujo de servicio tiene recursos comprometidos por la BS para sus ActiveQoSParamSet, es decir que esta activamente enviando comparaciones, las cuales contienen otorgaciones sin solicitud para un flujo de servicio UGS; sus parámetros no son nulos.

2.4.3.3.9.3 Modelo Objeto

Los objetos más importantes de la arquitectura están representados por rectángulos con nombre, cada objeto tiene un número de atributos, los nombres de los atributos que lo identifiquen de forma única están subrayados, los atributos opcionales están entre llaves.

Las relaciones entre el número de objetos esta marcada en cada extremo de la línea de asociación entre objetos; el flujo de servicio es el concepto central del protocolo MAC; este esta identificado por un SFID de 32 bits, y los flujos de servicio pueden estar en ambas direcciones uplink y downlink; los flujos de servicio admitidos y activos están relacionados con en CID de 16 bits.

Los datos salientes de usuario son admitidos a la SAP MAC por un proceso CS para transmisiones sobre la interfase MAC.

La información entregada por la SAP MAC incluye el CID que identifica la conexión a través de la cual la información se entrega; el flujo de servicio para la conexión esta relacionada con la conexión MAC mediante el CID.

La clase de servicio es un objeto opcional que puede ser implementado en la BS; esta tiene un conjunto de parámetros QoS particulares, contienen una referencia como una macro que selecciona todos los parámetros QoS de la clase de servicio, los grupos de parámetros QoS del flujo de servicio pueden aumentar o incluso anular las configuraciones de los parámetros QoS de la clase de servicio, siempre que posean autorización de la BS.

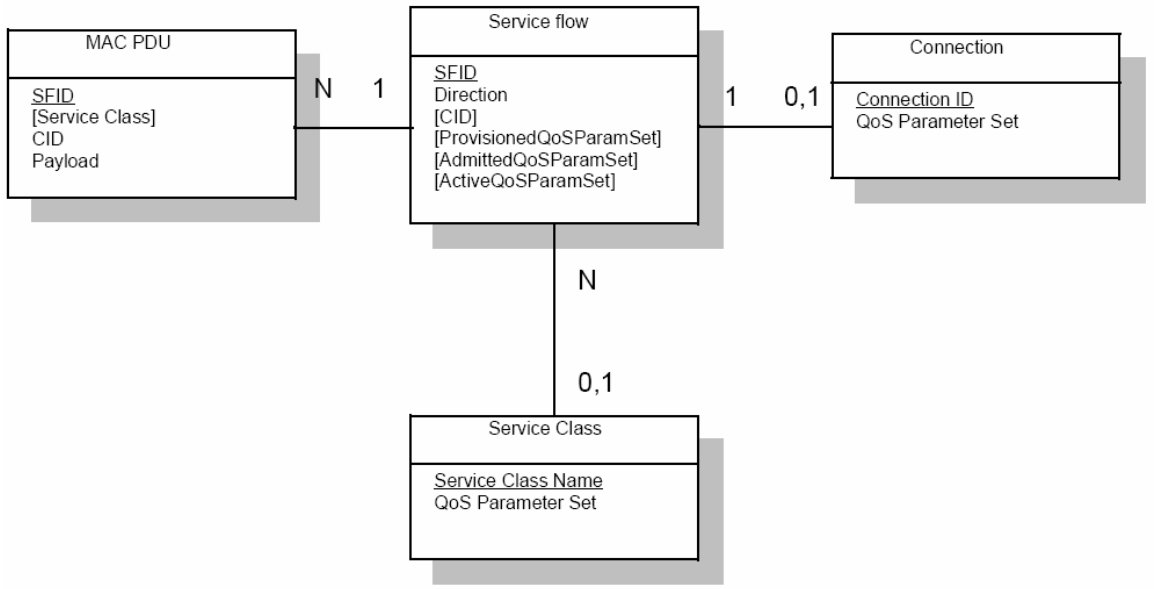


Figura 2.101. Teoría de Operación del Modelo Objeto[106]

[106] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 221.

2.4.3.3.9.4 Clases de Servicios

La clase de servicios cumple las siguientes funciones:

- Le permite al operador, en caso de que lo desee, mover la carga de la configurar los flujos de servicio desde el servidor de telecomunicaciones a la BS. El operador provee a las SS de un nombre de clase de servicio; la implementación del nombre lo realiza la BS, esto permite que el operador pueda cambiar la implementación de cierto servicio para adaptarse a circunstancias locales sin cambiar los servicios de la SS.
- Permite a los protocolos de capa superior crear un flujo de servicio mediante su nombre de clase de servicio.

Todo flujo de servicio debe tener su conjunto de parámetros QoS especificados de cualquiera de estas tres formas:

Mediante la inclusión explicita de todos los parámetros de tráfico.

Mediante la referencia indirecta a un conjunto de parámetros de tráfico al especificar un nombre de clase de servicio.
Mediante la especificación de un nombre de clase de servicio junto con parámetros de modificación.

El nombre de la clase de servicios se expande a su conjunto de parámetros definidos en el momento que la BS admite el flujo de servicios.

Cuando un nombre de clase de servicio se entrega en una petición de activación o admisión, es posible que el conjunto de parámetros QoS resultante pueda cambiar de activación en activación.

2.4.3.3.9.5 Autorización

Cada cambio en los parámetros QoS del flujo de servicio debe estar aprobados por un modulo de autorización, dichos cambios incluyen peticiones de admisión de decisiones de control y peticiones de activación de flujo de servicio; peticiones de reducción tomando en

cuenta los recursos para ser admitidos o activados son también revisados por el modulo de autorización.

En el modelo de autorización estática, el modulo de autorización almacena los estatus de aprovisionamiento de todos los flujos de servicio pospuestos; las peticiones de activación y admisión para estos flujos de servicio provistos deben ser permitidos, mientras que el grupo de parámetros de QoS admitidos sean un subgrupo de los parámetros QoS provistos, así como que el grupo de parámetros QoS activos sean un subgrupo de los parámetros QoS admitidos. Peticiones para cambiar los parámetros QoS provistos deben ser rechazadas, como los pedidos para crear nuevos flujos de servicio dinámicos. Esto define un sistema estático donde todos los posibles servicios están definidos en la configuración inicial de cada SS.

En el modelo de autorización dinámica, el modulo de autorización también se comunica a través de una interfase separada a un servidor de políticas independiente, este servidor de políticas puede proveer el modulo de autorización con noticias avanzadas de peticiones de admisión y activación, y especifica la debida acción de autorización a ser tomada ante las solicitudes. Las peticiones de admisión y activación de la SS son revisadas por el modulo de autorización para asegurarse de que el ActiveQoSParamSet que esta siendo solicitado sea un subgrupo del grupo provisto por el servidor de políticas; los pedidos que son señalados por adelantado por el servidor de políticas externo son permitidas, pero aquellas que no son preseñaladas por este servidor externo pueden resultar en una petición en tiempo real al servidor o pueden ser rechazadas.

Previa la configuración de conexión inicial, la BS debe extraer el grupo QoS provistos para una SS; este es entregado al modulo de autorización dentro de la BS; la BS debe ser capaz de tomar el grupo de parámetros QoS provistos y usar esta información para autorizar flujos dinámicos que son un subgrupo del grupo de parámetros QoS provistos, la BS debería implementar mecanismos para redefinir este proceso de aprobación automática.

2.4.3.3.9.6 Tipos de Flujos de Servicio

Se tienen tres tipos de flujos de servicio:

Flujos de Servicio Provistos.- Un flujo de servicio puede ser provisto pero no activado inmediatamente; esta es la descripción de cualquier flujo de servicio que contiene un atributo que provee pero difiere activación y admisión. La red asigna un SFID para este tipo de flujo de servicio, la BS puede requerir de igual manera un modulo de política previa la admisión.

Flujos de Servicio Admitidos.- Este protocolo soporta un modelo de activación de dos fases que es muy usado para aplicaciones de telefonía; en este modelo de activación de dos fases los recursos para una llamada son inicialmente admitidos, y una vez que la negociación de extremo a extremo se ha completado, los recursos son activadas, este modelo sirve para los siguientes propósitos:

- Conservar recursos de la red hasta que una completa conexión de extremo a extremo se establezca.
- Realizar revisiones de políticas y controles de admisión sobre los recursos tan rápido como sea posible, y en particular antes de informar al extremo de la conexión un pedido de conexión.
- Prevenir potenciales escenarios de robo de servicio.

Flujos de Servicio Activos.- Un flujo de servicio que tiene un ActiveQoSParamSet no nulo se conoce como un flujo de servicio activo, este pide y se le asigna ancho de banda para transportar paquetes de datos.

Un flujo de servicio puede ser provisto e inmediatamente activado, o un flujo de servicio puede ser creado dinámicamente e inmediatamente activado; es este caso la activación de dos fases es omitida y el flujo de servicio esta disponible para un uso inmediato sobre autorización.

2.4.3.3.9.7 Creación del Flujo de Servicio

Existe la creación del flujo de servicio en forma dinámica, el cual puede ser iniciado tanto de la BS como de la SS, a continuación se presentarán los dos casos.

Creación del flujo de servicio dinámico con iniciación de la SS es una habilidad opcional para WiMAX, la SS envía una petición de adición de servicio dinámico (DSA-

REQ) la cual incluye una referencia del flujo de servicio y un grupo de parámetros QoS, la BS responde con una DSA-RSP indicando la aceptación o rechazo, y la SS responde con un DSA-ACK.

En la creación del flujo de servicio dinámico iniciado por la BS se envía primero un DSA-REQ que contiene un SFID para cada uno de los flujos de servicio de uplink y downlink, posiblemente su CID asociado, y un grupo de parámetros QoS de admisión o activación; la SS responde con un DSA-RSP indicando la aceptación o rechazo, y finalmente la estación base envía un DSA-ACK.

2.4.3.3.9.8 Modificación y Eliminación del Flujo de Servicio Dinámico

Tanto los flujos de servicio dinámicos como los provistos se modifican mediante el mensaje de cambio de servicio dinámico (DSC), el cual puede cambiar los parámetros QoS activos y admitidos del flujo.

Un intercambio exitoso DSC cambia los parámetros QoS del flujo de servicio, reemplazando ambos grupos de parámetros, los activos y los admitidos; si el mensaje contiene solo parámetros admitidos, los activos son nulos y el flujo se desactiva; si el mensaje no contiene parámetros, ambos son nulos y el flujo deja de ser admitido; cuando el mensaje contiene ambos parámetros, se realiza la admisión, si es exitosa y el resto de verificaciones de los parámetros activos están correctas se reemplaza estos datos y pasan a ser el nuevo grupo de parámetros admitidos y activados para el flujo de servicio; en caso de alguna falla los parámetros del flujo no cambian.

2.4.3.3.9.9 Gestión del Flujo de Servicio

Los flujos de servicio pueden ser creados, cambiados o eliminados tal como se vio anteriormente, esto se logra mediante una serie de mensajes de gestión MAC, más específicamente los siguientes mensajes: DSA, DSC y DSD.

El mensaje DSA crea un nuevo flujo de servicio, el DSC cambia un flujo ya existente y DSD elimina un flujo de servicio existente.

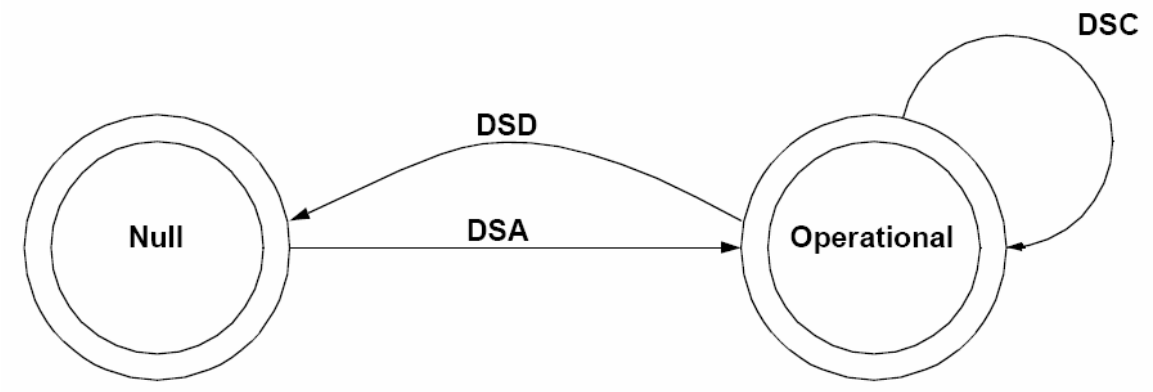


Figura 2.102. Diagrama de Estados del Flujo de Servicio Dinámico[107]

El estado nulo implica que no existe un flujo de servicio que tenga un SFID o ID de transacción que concuerde con el que lleva el mensaje; una vez que un flujo de servicio existente recibe un mensaje DSx, este cambia a otro estado, pero se mantiene en operación.

Debido a que existen muchos flujos de servicio en operación, los mensajes solo surten efecto sobre aquellos flujos en los que coincide el SFID especificado.
Cada secuencia de mensaje DSx es una transacción única con un identificador de transacción único; las transacciones DSA/DSC consisten de una secuencia petición/respuesta/confirmación; la transacción DSD consiste de una secuencia petición/respuesta.

2.4.3.3.10 Selección de Frecuencia Dinámica para Operaciones sin Licencia

La selección de frecuencia dinámica (DFS) es obligatoria para operaciones sin licencia, es decir en bandas de frecuencia abiertas; los sistemas deberían detectar y evitar a usuarios primarios; el uso de un algoritmo de selección de canal es requerido, lo que resulta en un esparcimiento uniforme de canal a lo largo de un mínimo número de canales.

Los procedimientos de este DFS son los siguientes:

- ✓ Revisar canales para usuarios primarios.
- ✓ Descontinuar operaciones después de detectar usuarios primarios.
- ✓ Detectar usuarios primarios.
- ✓ Planificar una revisión de canales.
- ✓ Petición y reporte de mediciones.

[107] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 227.

- ✓ Selección y publicación de un nuevo canal.

2.4.3.3.10.1Revisar Canales para Usuarios Primarios

Una estación base o de subscriptor no debe usar un canal que se sabe contiene usuarios primarios o no ha sido revisado recientemente por presencias de usuarios primarios.

Una BS debe revisar la presencia de usuarios primarios por lo menos en el periodo de prueba de inicio antes de operar en un canal nuevo, si este no ha sido revisado en la ultima revisión valida; o en un periodo de prueba de inicio antes de operar en un canal nuevo si el canal fue previamente identificado como portador de un usuario primario; y en el periodo de prueba de operación mientras se opera sobre un canal, estas pruebas se realizan en periodos de inactividad o operaciones normales.

Una SS puede operar en un nuevo canal sin seguir los procedimientos de prueba de inicio anteriormente mencionados si la SS se cambia de canal como resultado de un anuncio de cambio de canal desde la BS; o si la SS se inicializándose con una BS que no esta publicada, usando el anuncio de cambio de canal de que esta cambiándose a un nuevo canal.

2.4.3.3.10.2Descontinuar Operaciones después de Detectar Usuarios Primarios

Si una BS o SS están operando en un canal y detectan usuarios primarios, los que pueden causar interferencia, deben descontinuar cualquiera de las siguientes transmisiones:

- ➢ PDUs MAC que llevan datos dentro del periodo de operación de datos.
- ➢ PDUs MAC que llevan mensajes de gestión MAC dentro del periodo de operación de gestión.

2.4.3.3.10.3 Detectando Usuarios Primarios

Cada BS o SS debe usar un método de detección de usuarios primarios operando en un canal, el cual cumpla con los requerimientos regulatorios, este método se implementara según el fabricante.

2.4.3.3.10.4 Planificación para Revisión de Canales

Una BS puede medir uno o más canales por si mismo y pedir a cualquier SS que mida uno o más canales por su cuenta, ya sea en un periodo de inactividad o de operación normal.

La BS que pide a las SS que realicen una medición no deben transmitir PDU MAC a cualquier SS durante el intervalo de medición; si el canal medido es el canal de operación, la BS no debe planificar ninguna transmisión de uplink desde las SS durante el periodo de medición.

2.4.3.3.10.5 Pidiendo y Reportando Mediciones

La SS debe para canal medido llevar un listado de la siguiente información:

- Número de trama de la trama durante la cual la primera medición se llevo a cabo.
- Tiempo acumulado de medición.
- Existencia de un usuario primario en el canal.
- Si una MAN sin licencia de alta velocidad inalámbrica usando el mismo sistema de capa física fue detectada sobre el canal de medición.
- Si transmisiones desconocidas fueron detectadas sobre el canal.

La BS puede pedir un reporte de mediciones mediante el envío de un mensaje REP-REQ; la SS después de recibir dicho mensaje debe responder con un mensaje REP-RSP y reiniciar sus contadores de medición para cada canal reportado.

En caso de que una SS detecte un usuario primario en el canal de operación de esta, debe cesar la transmisión de datos y enviar lo más pronto posible un reporte no solicitado REP-RSP, la BS proveerá de oportunidades para la transmisión de estos reportes no solicitados, de la misma manera la SS realizara reportes no solicitados donde no se haya detectado interferencia de usuarios primarios sobre el umbral.

2.4.3.3.10.6 Seleccionando y Publicando un Nuevo Canal

Una BS puede usar una variedad de información, incluyendo la información adquirida durante la inicialización SS y la información recolectada por las mediciones realizadas por

la BS y SS, para escoger un canal, si la BS decide moverse a un nuevo canal, un canal que sea soportado por todas las SS en el sector debe ser seleccionado.

Una BS debe informar a sus estaciones asociadas el nuevo canal a ser usado, y los perfiles de ráfagas de uplink definidos para el antiguo canal son validas para el nuevo.

2.4.3.3.11 Soporte MAC para H-ARQ (Petición de Repetición Automática Hibrida)

El esquema de petición de repetición automática hibrida es una parte opcional de la capa MAC, H-ARQ puede ser soportado solamente por capas físicas OFDMA; las terminales pares H-ARQ y los parámetros de asociación deben ser especificados y negociados durante los procedimientos de inicialización, una ráfaga no puede tener una mezcla de tráfico H-ARQ y no H-ARQ.

Uno o más PDU MAC pueden concatenarse y para formar un paquete H-ARQ se añade un CRC a la ráfaga de la capa física.

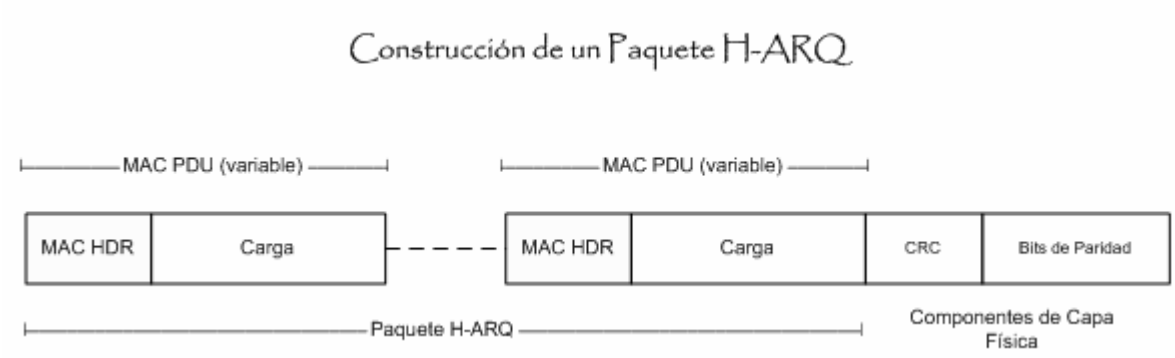


Figura 2.103. Construcción de un Paquete Codificado H-ARQ[108]

Cada paquete H-ARQ es codificado de acuerdo a las especificaciones de capa física, y cuatro sub paquetes son generados de la codificación resultante; un identificador de sub paquete (SPID) se usa para distinguir los cuatro sub paquetes.

En caso de comunicaciones downlink, una BS puede enviar uno de los sub paquetes en una transmisión de ráfaga; debido a la redundancia entre los paquetes, la SS puede decodificar correctamente el paquete codificado original aun antes de recibir todos los cuatro sub paquetes.

[108] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 267.

Si logra decodificar el paquete codificado original, la SS envía un ACK a la BS, la cual detiene el envío de los sub paquetes adicionales; caso contrario la SS envía una NAK, lo que causa que la BS transmita uno de los sub paquetes de los cuatro, esto continua hasta que la SS decodifica de forma exitosa el paquete codificado.

La regla de transmisión de los sub paquetes es la siguiente:

- En la primera transmisión la BS debe enviar el sub paquete marcado “00”.
- La BS puede enviar uno de los paquetes marcados “00”, “01”, “10” o “11” en cualquier orden.
- La BS puede enviar más de una copia de cualquier sub paquete, y puede omitir cualquier sub paquete excepto el sub paquete “00”.

El esquema H-ARQ soporta múltiples canales H-ARQ por cada conexión, cada una de las cuales puede tener una transacción de paquete codificado pendiente; el número de canales en uso esta determinado por la BS; estos canales H-ARQ están diferenciados por un identificador de canal H-ARQ (ACID); este ACID para cualquier sub paquete puede ser identificado de forma única por la información de control llevada en los MAPs.

H-ARQ puede ser usado para mitigar el efecto canal y fluctuaciones de interferencia; H-ARQ provee mejora en el desempeño debido a una ganancia SNR y diversidad de tiempo alcanzada mediante la combinación de previos paquetes codificados erróneamente, paquetes retransmitidos y ganancia de codificación adicional mediante redundancia incremental.

2.4.4 Subcapa de Seguridad

La subcapa de seguridad provee a los subscriptores de una privacidad a lo largo de la red inalámbrica de banda ancha, mediante conexiones encriptadas entre la SS y BS.

Además, esta capa provee de operadores con fuertes protecciones contra robo de servicios; la BS refuerza la encriptación de los flujos de servicio asociados a lo largo de la red; la parte de privacidad emplea un protocolo de gestión de llave cliente/servidor de autenticación en el cual la BS como el servidor controlan la distribución del material de llave al SS cliente; adicionalmente los mecanismos básicos de privacidad se han reforzado

incorporando una autenticación SS basada en certificados digitales a su protocolo de gestión de llave.

Si durante la negociación de las capacidades, la SS especifica que no soporta la seguridad 802.16, los pasos de autorización e intercambio de llave deben ser omitidos; la BS si así lo determina, debe considerar la SS autenticada, caso contrario no debe prestarle servicio.

2.4.4.1 Arquitectura

Esta subcapa MAC tiene dos componentes:

- Un protocolo de encapsulación para paquetes de datos encriptados a lo largo de la red de acceso de inalámbrica de banda ancha fija; este protocolo define un grupo de conjuntos criptográficos; y, las reglas para aplicar estos algoritmos a la carga PDU MAC.
- Un protocolo de gestión de llave (PKM) que provee la distribución segura de los datos de llave desde la BS a la SS; a través de este protocolo, la SS y BS sincronizan datos de llave.

2.4.4.1.1 Encriptación de Paquetes de Datos

Los servicios de encriptación están definidos como un grupo de capacidades dentro de la subcapa de seguridad MAC, la información para la encriptación se encuentra en el encabezado MAC de formato general.

La encriptación se aplica siempre a la carga PDU MAC, sin embargo el encabezado genérico no se encripta.

2.4.4.1.2 Protocolo de Gestión de Llave

Una SS usa el protocolo PKM para obtener autorización y trafico de material de llave desde la BS, y para soportar re autorizaciones periódicas y renovación de llave.

Este protocolo usa certificados digitales X.509, algoritmos de encriptación de llave pública RSA y algoritmos de encriptación fuertes para realizar intercambio de llave entre la SS y BS.

El protocolo PKM se atiene al modelo cliente/servidor, en donde la SS o cliente solicita material, y la BS o servidor responde las solicitudes, asegurando que cada cliente reciba solamente el material de llave para el cual está autorizado.

PKM usa criptografía de llave pública para establecer un secreto compartido (AK) entre la SS y BS; este secreto es usado para asegurar los siguientes intercambios PKM de tráfico de encriptación de llave.

La BS autentica un cliente SS durante el intercambio de autorización inicial; cada SS lleva un certificado X.509 único provisto por el fabricante, este certificado contiene la llave pública del SS y su dirección MAC

Cuando se solicite un AK, una SS presenta su certificado digital a la BS, esta lo verifica y utiliza la llave publica para encriptar un AK, este es enviado de regreso a la SS.

La BS asocia una identidad autenticada de SS a un subscriptor pago y hereda los servicios de datos que el subscriptor esta autorizado a acceder; una vez que la BS autentica a la SS esta queda protegida de ataques empleando SS clonados, gracias al certificado X.509.

2.4.4.1.3 Asociaciones de Seguridad

Una asociación de seguridad (SA) es un conjunto de informaciones de seguridad que una BS y uno o más de sus clientes comparten para poder tener comunicaciones seguras a lo largo de la red WiMAX; tres tipos de SA están definidos: primarias, estáticas y dinámicas.

Cada SS gestionable establece una asociación de seguridad primaria durante el proceso de inicialización; las SA estáticas están provistas dentro de la BS y las SA dinámicas se establecen y eliminan en respuesta al inicio y finalización de flujos de servicio específicos. Tanto los SA dinámicos como estáticos pueden ser compartidos por varias SS.

Las asociaciones de seguridad se identifican mediante un SAID, cada SS gestionable debe establecer una SA primaria exclusiva con su BS; el SAID de cualquier SA primaria de SS debe ser igual al CID básico de esa SS.

El material de llave de SA tiene un tiempo de vida limitado, cuando la BS entrega este material también provee en tiempo de vida restante, cada SS debe encargarse de solicitar un nuevo material de llave, el material antiguo debe expirar antes de recibir el nuevo.

2.4.4.1.4 Asociación de Conexiones con Asociaciones de Seguridad

Se deben seguir las siguientes reglas para poder asociar las conexiones con SAs:

- Todas las conexiones de transporte deben ser asociadas con un SA existente.
- Conexiones de transporte multicast pueden ser asignadas a cualquier SA estático o dinámico.
- La conexión de gestión secundaria debe ser asociada a un SA primario.
- Las conexiones básicas y de gestión primaria no deben ser asociadas a ningún SA.

2.4.4.1.5 Conjunto Criptográfico

Un conjunto criptográfico es un conjunto de métodos para encriptación de datos, autenticación de datos e intercambio de llave de encriptación de trafico (TEK) de una SS.

2.4.4.2 Protocolo PKM

2.4.4.2.1 Autorización SS y Revisión del Intercambio AK

La autorización SS consta de los siguientes procesos:

- La BS autentica una identidad de SS cliente.
- La BS provee a la SS autenticada un AK, del cual una llave de encriptación de llave (KEK) y llaves de autenticación de mensaje son entregadas.
- La BS provee a la SS autenticada la SAID y propiedades de SA estáticas y primarias, de las cuales esta autorizada a obtener la información de llave.

Una vez que se logra la autorización inicial, la SS buscara periódicamente reautorizaciones con la BS; la SS inicia la autorización enviando un mensaje de información de autenticación que contiene el certificado X.509.

Después de este mensaje de información la SS envía un mensaje de petición de autorización para obtener un AK, este mensaje consta de los siguientes puntos:

- ✓ Un certificado X.509.
- ✓ Una descripción de los algoritmos criptográficos que la SS solicitante soporta.
- ✓ El CID básico de la SS, este es el primer CID estático que la BS asigna a un SS durante ajuste inicial.

En respuesta a este mensaje de solicitud la BS responde con un mensaje de respuesta de autorización que contiene los siguientes elementos:

- ➢ Un AK encriptado con la llave publica de la SS.
- ➢ Un número de secuencia de llave de cuatro bits, usado para distinguir entre generaciones sucesivas de AKs.
- ➢ Un tiempo de vida de llave.
- ➢ Los SAID y propiedades de la primaria y ninguna o más SA estáticas de las cuales la SS esta autorizada a obtener la información de llave.

La BS luego de recibir el mensaje de solicitud de autenticación debe determinar los servicios básicos unicast que le permitirá a la SS, así como los servicios provisionales estáticos adicionales la SS ha solicitado, cabe destacar que ciertos servicios protegidos dependen de los parámetros criptográficos que soporten la SS y BS.

La re autenticación es idéntica a la autorización con la excepción de que la SS no envía el mensaje de información de autenticación.

2.4.4.2.2 Revisión del Intercambio TEK

2.4.4.2.2.1 Revisión del Intercambio TEK para Topologías PMP

Una vez autorizada, la SS inicia un TEK para cada SAID especificada, cada TEK esta encargado del manejo del material de llave asociado a cada SAID, cada TEK envía periódicamente a la BS un mensaje de solicitud de llave, pidiendo una nuevo material de llave.

El TEK esta encriptado usando la KEK derivada del AK.

EL TEK continua activo mientras se produzcan los siguientes eventos:

- ✓ La SS tenga un AK valido
- ✓ La BS continúe proveyendo a la SS de nuevo material de llave durante los ciclos de renovación de llave.

El mecanismo de autorización detiene todo TEK si la SS recibe un mensaje de rechazo de autorización durante el periodo de reautorización; y varios TEK pueden iniciarse o detenerse durante el periodo de reautorización si las autorizaciones SAID estáticas de SS cambian.

2.4.4.2.2.2 Revisión del Intercambio TEK para Modos Malla

Después de la autorización, un nodo inicia un TEK por cada SAID con su nodo vecino, cada TEK es responsable por el material de llave cada nodo es responsable por mantener los TEK entre el y sus nodos vecinos con los que haya iniciado intercambios TEK y su correspondiente renovación.

El nodo vecino responde la petición de llave con un mensaje de respuesta de llave que lleva el material de llave activo de la BS.

El TEK en la respuesta de llave esta encriptado usando la llave publica de nodo del atributo de certificado SS.

La respuesta de llave también lleva consigo el tiempo de vida restante de cada material llave, para poder planificar la petición de un nuevo material de llave.

2.4.4.2.3 Selección de Capacidades de Seguridad

Como parte del intercambio de autorización, la SS le provee a la BS la lista de todos los conjuntos criptográficos que soporta, la BS por su parte selecciona solo un de ellos para utilizarlo con pedido de SA primario de la SS.

La BS debe rechazar la autorización si determina que ningún conjunto criptográfico es satisfactorio.

En caso de que la BS le indique al SS un conjunto criptográfico que no pueda soportar, este no debe iniciar el intercambio TEK para las SA estáticas que no soporte.

2.4.4.2.4 Maquinaria de Autorización

Esta maquinaria de autorización consiste de seis estados y ocho eventos distintos que pueden desencadenar la transición de estados.

Los estados son los siguientes: Start, Authorize Wait, Authorized, Reauthorize Wait, Authorize Reject Wait y Silent.

2.4.4.2.5 Maquinaria TEK

La maquinaria TEK consiste de seis estados y nueve eventos que pueden activar la transición de estados.

Los seis estados de la maquinaria TEK son: Start, Operational Wait, Operational Reauthorize Wait, Operational, Rekey Wait y Rekey Reauthorize Wait.

En varios estados tienen material de llave valido y por lo tanto tráfico encriptado puede pasar por ellos. La maquinaria de autorización inicia una maquinaria TEK para cada SAID autorizado.

2.4.4.3 Creación y Asociación de las SA Dinámicas

Las asociaciones de seguridad dinámicas son SA que una BS establece y elimina de forma dinámica en respuesta a la habilitación y deshabilitación de flujos de servicio específicos. Las SS aprenden la asignación de un flujo de servicio de privacidad con la SA asignada dinámicamente de ese flujo a través del intercambio de mensajes DSx.

La creación de las SA dinámicas se realiza cuando la BS envía un mensaje de adición SA; mientras que la SS una vez recibido el mensaje debe iniciar la maquinaria TEK para cada SA que conste en el mensaje.

La asignación dinámica SA se produce una vez que se ha creado un nuevo flujo de servicio, y la SS solicite un SA existente para ser utilizado mediante el envío del SAID del

SA en un mensaje DSA-REQ o DSC-REQ; la BS revisa la autorización de la SS y contesta.

Con las creaciones de servicio dinámico iniciadas por la BS, una BS puede también asignar un nuevo flujo de servicio a un SA existente que soporte un SS en particular; el SAID de la SA debe ser comunicado a la SS a través de un mensaje.

2.4.4.4 Uso de Llave

2.4.4.4.1 Uso de Llave de BS

La BS es responsable por mantener la información de llave para todas las asociaciones de seguridad.

2.4.4.4.1.1 Tiempo de Vida de la Llave AK

Una vez que la SS termina con la negociación de las capacidades básicas, debe iniciar un intercambio de autorización con su BS; la recepción de un mensaje de petición de autorización inicia la activación de un nuevo AK, el cual la BS envía a la SS solicitante; este AK debe permanecer activo hasta que expira de acuerdo con su tiempo de vida, que es un parámetro que los configura la BS.

Este tiempo de vida debe ser reportado por la BS de la forma más precisa que le sea posible en el mensaje de respuesta de autorización.

Si una SS no consigue su reautorización antes de la expiración de su AK, la BS no debe retener AK activos para la SS y debe considerar la SS desautorizada, debe retirar de sus tablas de llave todos los TEK asociados con una SA primaria de SS desautorizada.

2.4.4.4.1.2 Periodo de Transición AK sobre el Lado de la BS

La BS siempre debe estar preparada para enviar un AK a una SS que lo solicite; la BS debe ser capaz de soportar dos AK activos simultáneamente para cada SS cliente, la BS tiene dos AK activos durante un periodo de transición AK, estos dos AK poseen tiempos de vida sobrepuestos.

Una vez que la BS recibe el mensaje de solicitud de autorización se inicia el periodo de transición AK y debe activar un AK para la SS, pero en respuesta a este mensaje debe activar un segundo AK el cual le hará llegar a la SS mediante el mensaje de respuesta de autorización, este nuevo AK tiene un tiempo de vida mayor al primero.

La BS debe considerar al tiempo de vida del primer AK más el segundo como el tiempo de vida AK para esa SS, una vez que termine el tiempo de vida de la llave más antigua termina el periodo de transición; y activa la petición de un nuevo AK.

2.4.4.4.1.3 Uso del AK por la BS

La BS debe usar el material de llave del AK de la SS para las siguientes tareas:

- ✓ Verificar HMAC (Código de Autenticación de Mensaje Cortado) en el mensaje de solicitud de llave recibido de la SS.
- ✓ Calcular el HMAC escrito en la petición de llave, rechazo de llave, mensaje enviados de TEK inválidos a la SS.
- ✓ Encriptando el TEK en mensaje de respuesta de llave que envía a la SS.

2.4.4.4.1.4 Tiempo de Vida TEK

La BS debe mantener dos grupos de TEK activos por SAID, lo cuales corresponden a dos generaciones sucesivas de material de llave. Dos generaciones de TEK deben tener tiempos de vida sobrepuestos, los cuales son determinados por los parámetros de configuración del sistema de BS, el TEK más nuevo debe tener un tiempo de vida mayor al primero, cada TEK se vuelve activo a la mitad del tiempo de vida del siguiente y expira a la mitad del tiempo de vida del nuevo.

El tiempo de vida debe ser tan preciso como le se posible enviar a la BS mediante el mensaje de respuesta de solicitud de llave.

2.4.4.4.1.5 Uso del TEK por la BS

La transición de la BS entre dos TEK activos difiere de acuerdo a si el TEK se usa para tráfico de uplink o downlink, para cada SAID, la BS debe realizar la transición siguiendo las siguientes reglas:

- ✓ En el momento de la expiración del antiguo TEK, la BS debe inmediatamente usar el nuevo TEK para encriptación.
- ✓ El periodo de transición de uplink comienza desde el momento que la BS envía el nuevo TEK en un mensaje de repuesta de llave y termina una vez que el TEK más antiguo expira.

La BS debe iniciar la transición a una llave de encriptación de downlink sin importar si el cliente SS ha adquirido una copia de dicho TEK.

La BS usa dos TEK activos de acuerdo a las siguientes reglas:

- ✓ La BS debe usar el más antiguo de los dos TEK activos para encriptar el tráfico de downlink.
- ✓ La BS debe ser capaz de desencriptar el tráfico de uplink ya sea que use el nuevo o el antiguo TEK.

2.4.4.4.2 Uso de Llave de SS

La SS es responsable de mantener la autorización con su BS y mantener un AK activo, y estar preparada para usar sus AK obtenidos.

2.4.4.4.2.1 Reautorización SS

Los AK tienen periodos de vida limitados y deben ser renovados periódicamente, una SS renueva sus AK mediante el envió de una petición de autorización a la BS.

La maquinaria de autorización de la SS planifica el inicio de la reautorización antes de que su AK expire.

La BS por su parte debe llevar la cuenta de sus AK y desactivar la llave una vez que ha expirado.

2.4.4.4.2.2 Uso del AK por la SS

La SS debe ser capaz de usar los AK para autenticar la respuesta de llave, rechazo de llave y mensajes de rechazo TEK, la SS debe ser capaz de desencriptar un TEK en un

mensaje de respuesta de llave con el KEK derivado de cualquiera de sus AK; la SS debe usar número de secuencia de llave AK acompañante para determinar cual grupo de los materiales de llave usar.

2.4.4.4.2.3 Uso del TEK por la SS

Una SS debe ser capaz de mantener dos grupos sucesivos de material de llave de tráfico por cada SAID autorizado.

La SS debe solicitar un nuevo TEK antes de que el periodo de vida del TEK que usa llegue a su fin.

La SS debe realizar las siguientes acciones por casa SAID autorizado:

- Debe usar el más nuevo de sus TEK para encriptar el tráfico de uplink.
- Debe ser capaz de desencriptar el tráfico de downlink encriptado con cualquiera de los TEK.

2.4.4.4.2.4 Uso TEK en el Modo Malla

Por cada SAID, el vecino debe iniciar la transición entre TEK activos de acuerdo a las siguientes reglas:

- ✓ Al momento de la expiración del TEK antiguo, el vecino debe inmediatamente usar el nuevo TEK para realizar las encriptaciones.
- ✓ El vecino que genera el TEK debe usar el más antiguo de los TEK para encriptar el tráfico hacia el nodo que inicia el intercambio TEK.
- ✓ El vecino que genera el TEK debe ser capaz de desencriptar el tráfico de cada nodo usando cualquiera de los TEK, ya sea el nuevo o antiguo.

Por cada de sus SAID, el nodo iniciador debe realizar las siguientes acciones:

- Debe usar el más nuevo de los TEK para realizar la encriptación del tráfico hacia sus vecinos con los que ha iniciado un intercambio TEK.
- Debe ser capaz de desencriptar el tráfico desde su vecino usando cualquiera de los TEK.

2.4.4.4.2.5 Uso de Nodo del Operador de Secreto Compartido en el Modo Malla

Cada nodo debe ser capaz de mantener dos operadores de secreto compartido (AK) activos; el nodo debe usar estos para calcular un HMAC para la petición de llave y mensajes de solicitud de llave cuando se realiza el intercambio TEK con sus vecinos.

2.4.4.5 Métodos Criptográficos

En esta parte del presente documento se especifican los algoritmos criptográficos y tamaños de llave usados por el protocolo PKM.

2.4.4.5.1 Métodos de Encriptación de Datos

2.4.4.5.1.1 Encriptación de Datos con DES (Data Encryption Standard) en Modo CBC (Cipher Block Chaining)

Si el identificador de algoritmo de encriptación en el grupo criptográfico indica el valor 0x01, los datos sobre la conexión asociada debe usar el modo CBC del algoritmo estándar de encriptación de datos para encriptar la carga del PDU MAC.

El CBC debe calcularse mediante operaciones XOR entre los parámetros de información de llave TEK y el DL-MAP para el downlink y operaciones XOR entre los parámetros de información de llave TEK y los del UL-MAP.

2.4.4.5.1.2 Encriptación de Datos con AES (Advanced Encryption Standard) en el Modo CCM

Si identificador de algoritmo de encriptación de datos en los grupos criptográficos de un SA tiene el valor 0x02, los datos sobre las conexiones asociadas con esa SA usan el modo CCM del algoritmo estándar de encriptación avanzada.

2.4.4.5.2 Encriptación de Llave Pública de AK

Los AK en los mensajes de solicitud de autorización deben ser encriptados con una llave publica RSA[109], usando la llave publica de la SS, el protocolo usa en número 65537 como su exponente publico y un modulo de longitud de 1024 bits.

[109] El algoritmo de llave publica RSA toma su nombre de las iniciales de sus diseñadores: Rivest, Shamir y Adleman.

2.4.4.5.3 Firmas Digitales

El protocolo PKM emplea algoritmos de firmas RSA con SHA-1 (FIPS 186-2)[110] para los dos tipos de certificados que maneja.

Como con las llaves de encriptación RSA, la capa de privacidad usa 65537 como exponente publico para sus operaciones de firmas, la autoridad de certificación del fabricante debe emplear llaves de firmas de longitud de al menos 1024 bits y menores a 2048.

2.4.4.6 Perfil de Certificación

2.4.4.6.1 Formato del Certificado

Revisaremos en detalle el formato que tiene el certificado digital X.509 mediante la siguiente tabla:

[110] FIPS (Estándar de Procesamiento de Información Federal) 186-2 es un mecanismo de generación de formas digitales con llaves de encriptación públicas y privadas, estas firmas se reducen mediante el SHA-1 (Algoritmo de Corte de Seguridad).

Campos X.509 v3	Descripción
tbs.Certificate.version	Indica la versión del certificado X.509. Siempre debe ser v3 (valor de 2).
tbs.Certificate.serialNumber	Entero único que el fabricante CA asigna al certificado.
tbs.Certificate.signature	Identificador de Objeto (OID) y parámetros opcionales que definen el algoritmo usados para firmar el certificado. Este campo debe contener el mismo identificador de algoritmo que el campo signatureAlgortihm.
tbs.Certificate.issuer	Nombre distintivo del CA que fabrica el certificado.
tbs.Certificate.validity	Especifica cuando el certificado se vuelve activo y cuando expira.
tbs.Certificate.subject	Nombre distintivo que identifica la entidad cuya llave pública esta certificada en el campo subjectPublicKeyInfo.
tbs.Certificate.subjectPublicKeyInfo	Campo que contiene el material de llave público y el identificador del algoritmo con el cual la llave es usada.
tbs.Certificate.issuerUniqueID	Campo opcional que permite re usar los nombres de fabricante con el tiempo.
tbs.Certificate.subjectUniqueID	Campo opcional que permite re usar los nombres de objeto con el tiempo.
tbs.Certificate.extensions	Los datos de extensión.
signatureAlgorithm	OID y parámetros opcionales que definen el algoritmo usado para firmar el certificado.
signatureValue	Firma digital calculada sobre el ASN.1 DER codificado en tbsCertificate.

Tabla 2.55. Formato del Certificado X.509

2.4.4.6.2 Almacenamiento de Certificación SS y Gestión en la SS

Los certificados de las SS que fueron entregados por el fabricante deben almacenarse en una memoria permanente de una sola escritura; las SS que tengan su par de llaves RSA privadas/publicas instaladas por el fabricante deben tener también certificados SS del fabricante.

Las SS que confíen en algoritmos internos para generar su par de llaves RSA deben soportar un mecanismo para instalar un certificado de fabricante SS una vez que se generen las llaves.

2.4.4.6.3 Proceso de Certificación y Gestión en la BS

PKM utiliza certificados digitales para permitir a la BS que verifique los lazos ente una identidad de SS y su llave publica; la BS realiza esto mediante la validación del camino de certificación o cadena del certificado de la SS.

Validar la cadena significa verificar el certificado de la autoridad de certificación (CA) del fabricante.

2.4.5 Capa Física

2.4.5.1 Especificaciones de Capa Física para Sistemas WirelessMAN-SC

2.4.5.1.1 Introducción

La capa física para redes MAN inalámbricas con una sola portadora esta diseñada para operar en la banda de frecuencias de 10 a 66 GHz, además de poseer una gran flexibilidad para poder brindar una optimización en el planeamiento de celdas, costos servicios y capacidad.

Para poder lograr flexibilidad en el uso del espectro, se utilizan las configuraciones TDD y FDD, ambas usan un formato de transmisión de ráfaga, las cuales soportan perfiles de ráfagas adaptativas, en los cuales varios parámetros como esquemas de modulación y codificación pueden ajustarse a cada SS bajo un modo trama por trama; el modo FDD soporta funcionamientos tanto full duplex y half duplex.

La capa física para uplink esta basada en la combinación de TDMA y DAMA, en general el canal de uplink esta dividido en un número de ranuras de tiempo, los usos de los mismos están controlados por la capa MAC de la BS y pueden variar para un mejor rendimiento.

El canal de downlink es TDM, con la información para cada SS multiplexada en una sola trama de datos y recibida por todas las SS dentro del mismo sector; para soportar estaciones FDD half duplex, se tiene también TDMA para downlink.

Los bits de datos de la subcapa de convergencia de transmisión son aleatorios, poseen codificación FEC y están asignados a un modulación QPSK o 16QAM y en caso de soportarlo 65QAM.

La capa física de uplink esta basada en transmisiones TDMA, cada ráfaga esta diseñada para llevar PDU MAC de longitud variable.

2.4.5.1.2 Entramado

Esta capa física posee una trama con dos sub tramas, una de uplink y otra de downlink; la sub trama de downlink comienza con la información necesaria para la sincronización de trama y control.

En el caso TDD, la sub trama de downlink va primero, seguida por la de uplink; por otro lado en FDD, las transmisiones de uplink ocurren al mismo tiempo que la trama de downlink.

Cada SS debe intentar recibir todas las porciones del downlink excepto por aquellas ráfagas cuyo perfil no sea implementado por la SS o sea menos robusto que el perfil de operación.

Las estaciones half duplex no deben intentar escuchar las porciones del downlink que coinciden con su transmisión de uplink.

2.4.5.1.3 Técnicas de Duplexión y Codificación de Parámetros de Tipos de Capa Física

Esta capa física soporta ambos métodos de duplexión FDD y TDD; los valores de los parámetros de los tipos de capa física se muestran en la siguiente tabla:

Tipo de Capa Física	Valor
TDD	**0**
FDD	**1**

Tabla 2.56. Parámetros de Tipos de Capa Física

2.4.5.1.3.1 Operación FDD

Bajo el modo de operación FDD, los canales de uplink y downlink están diferentes frecuencias, la capacidad de downlink de transmitir en ráfagas facilita el uso de diferentes tipos de modulación y permite que el sistema soporte simultáneamente SS full y half duplex.

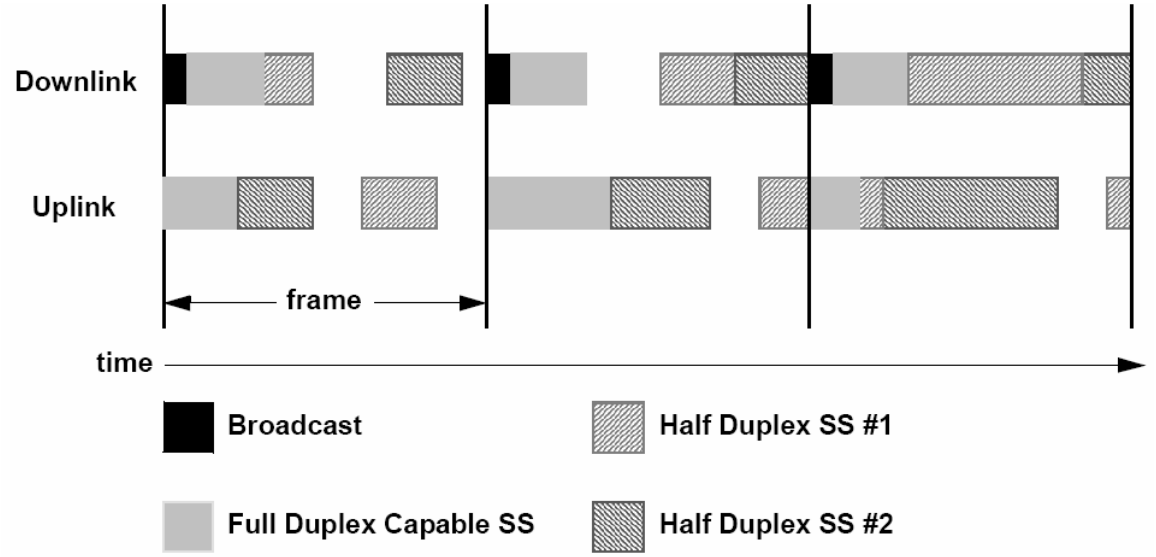


Figura 2.104. Ubicación de Ancho de Banda FDD[111]

2.4.5.1.3.2 Operación TDD

En el caso TDD, las transmisiones de uplink y downlink comparten la misma frecuencia pero están separadas en el tiempo; una trama TDD también tiene una duración fija y contienen una sub trama de uplink y downlink, el entramado TDD es adaptativo ya que la capacidad del enlace distribuida para downlink versus uplink puede variar.

[111] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 308.

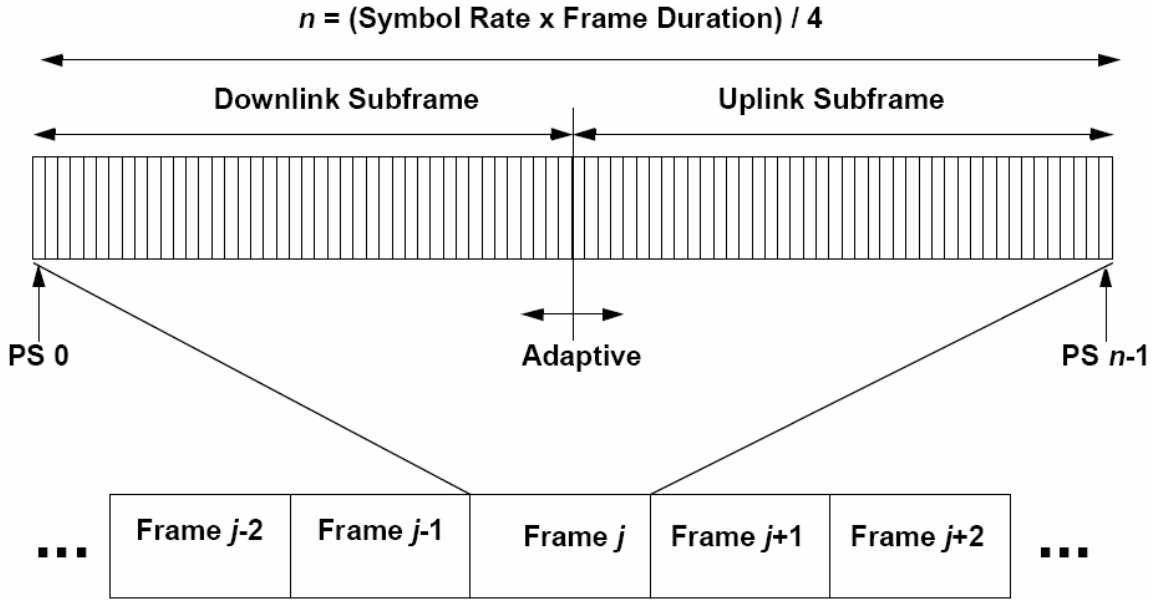


Figura 2.105. Estructura de la Trama TDD[112]

2.4.5.1.4 Capa Física de Downlink

El ancho de banda disponible en la dirección de downlink esta definida con un mecanismo de ajuste de una ranura física (PS); mientras que el ancho de banda de uplink esta definido por un mecanismo de ajuste de una mini ranura, donde una mini ranura es:

$$2^m PS, m = 0,...,7$$

Formula 2.21. Definición de una Mini Ranura

La tasa de símbolo se selecciona de tal forma que se pueda obtener un número entero de PS en cada trama.

2.4.5.1.4.1 Sub Trama de Downlink

La estructura de la sub trama de downlink para TDD esta compuesta de un preámbulo de inicio de trama, seguido por una sección de control de trama, que contiene los DL-MAP y UL-MAP; le siguen las porciones TDM que llevan datos, estas están organizadas en ráfagas con diferentes perfiles y niveles de robustez.

[112] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 309.

Las ráfagas se transmiten en orden decreciente de robustez; en tiempo de guarda separa las sub tramas de uplink y downlink. Cada estación recibe y decodifica la información de control de downlink y mira los encabezados MAC que indican los datos para esa estación.

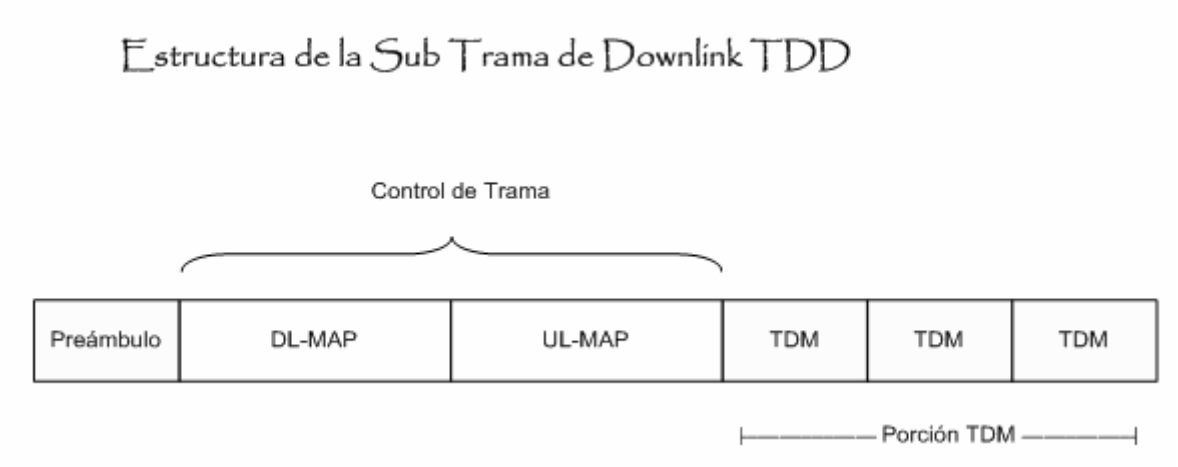


Figura 2.106. Estructura de la Sub Trama de Downlink TDD

En el caso FDD, la estructura de la sub trama de downlink comienza con un preámbulo de inicio de trama seguido por un sección de control de trama, a esta le sigue una porción TDM la que se organiza en ráfagas transmitidas en orden decreciente de robustez; en esta sección TDM los datos pueden corresponder a las siguientes estaciones:

- ✓ SS full duplex.
- ✓ SS half duplex planificadas para transmitir más tarde en la trama que reciben.
- ✓ SS half duplex no planificadas para transmitir en esta trama.

Después de la porción TDM le sigue una porción TDMA, usada para transmitir datos de cualquier estación half duplex programada para transmitir más temprano en la trama que reciben; esto le permite a la estación recibir su información sin decodificar toda la trama.

En la parte TDMA cada ráfaga comienza con un preámbulo para re sincronizar la fase; las porciones de esta sub trama no necesitan estar en orden; además la sección de control lleva asignaciones para las ráfagas TDM y TDMA.

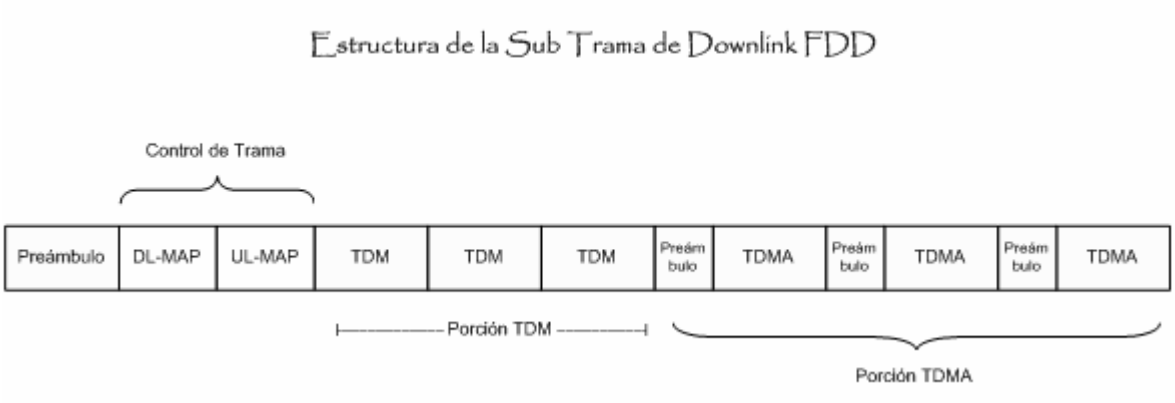


Figura 2.107. Estructura de la Sub Trama de Downlink FDD

La sección de control no debe estar encriptada, contiene los mensajes DL-MAP, UL-MAP, y de forma adicional se puede intercalar los mensajes DCD y UCD.

Los preámbulos tanto pata TDM y TDMA se deben realizar siempre con codificación de símbolo QPSK.

2.4.5.1.4.2 Subcapa PMD de Downlink

La presente capa física para downlink se puede apreciar en el siguiente diagrama de bloques:

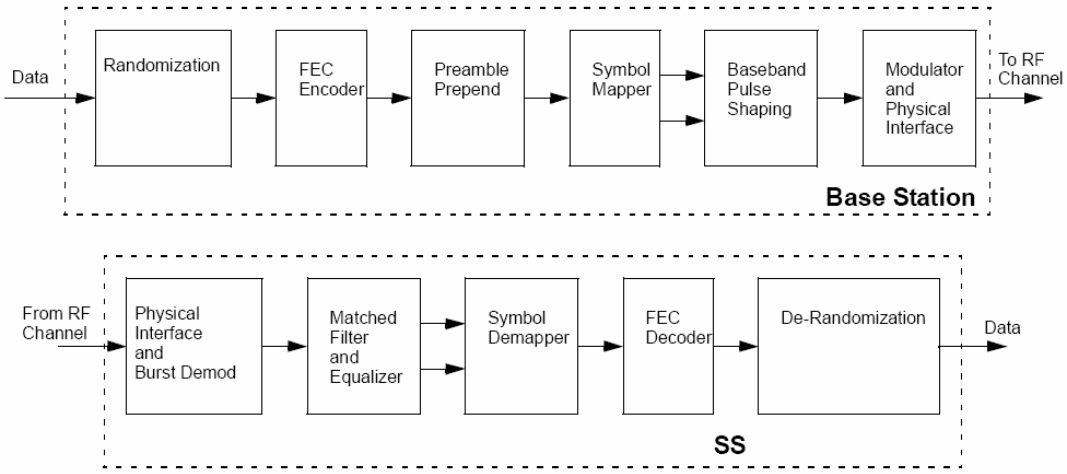


Figura 2.108. Diagrama de Bloques de la Subcapa PMD de Downlink[113]

El proceso de reordenamiento aleatorio se realiza para minimizar la transmisión de una portadora no modulada y para asegurar la recuperación del reloj, los datos se reordenan

[113] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 319.

mediante una suma de modulo 2 entre los datos y la salida de un generador de secuencia binaria pseudo aleatoria (PRBS), que en este caso responde al siguiente polinomio generador:

$$c(x) = x^{15} + x^{14} + 1$$

Formula 2.22. Polinomio Generador PRBS[114]

Una vez se pasa por el reordenamiento se procede a la codificación FEC, en donde se pueden tener cuatro tipos de codificación a escoger, dos obligatorias y dos opcionales:

TIPO DE CÓDIGO	CÓDIGO SALIENTE	CODIFICACIÓN INTERNA
1	Reed-Solomon sobre Campo Galois (GF) 256	Ninguna
2	Reed-Solomon sobre (GF) 256	(24,16) Código convolucional de bloque (modulación QPSK)
3 (Opcional)	Reed-Solomon sobre (GF) 256	(9,8) Código de chequeo de paridad
4 (Opcional)	BTC	_____

Tabla 2.57. Tipos de Codificaciones FEC

Por otra parte la modulación que se usa en WiMAX es una modulación multi nivel, ya que la modulación puede ser escogida por el equipo según la calidad del enlace de radio frecuencia, si las condiciones son buenas se puede escoger un esquema de modulación más complejo para maximizar el throughput teniendo una transferencia de datos confiable, si empeora el enlace se puede pasar a una codificación menos compleja y permitir una transferencia de datos más confiable.

La BS puede soportar obligatoriamente modulaciones QPSK y 16QAM, mientras que opcionalmente soporta 64QAM. En caso de que se realicen estos cambios de modulación se debe tener en cuenta que se realizaran ajusten en la potencia transmitida también, esto se logra ya sea manteniendo la potencia de los picos o la potencia promedio de las señales.

2.4.5.1.5 Capa Física de Uplink

2.4.5.1.5.1 Sub Trama de Uplink

La estructura de la sub trama de uplink que usa la SS para comunicarse con la BS posee tres clases de ráfagas:

[114] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 320.

- Las ráfagas que se transmiten en oportunidades de contención reservadas en el ajuste inicial.
- Ráfagas que son transmitidas en oportunidades de contención definidas por intervalos de petición reservados para respuestas en polls multicast o broadcast.
- Las ráfagas que son transmitidas en intervalos definidos por elementos de información de otorgación de datos específicamente colocados para SS individuales.

Estos tres tipos de ráfagas pueden ocurrir en cualquier orden y cantidad dentro de la trama, según lo indique el planificador de uplink de la BS.

Entre las diferentes ráfagas existen brechas para poder distinguir las ráfagas y para poder sincronizarse con las SS.

Cada ráfaga comienza con un preámbulo, el cual puede ser de 16 o 32 símbolos, el primer preámbulo esta compuesto de 8 símbolos que se repiten y 16 símbolos que se repiten para el segundo; los preámbulos son secuencias de auto correlación cero de amplitud constante, al igual que los preámbulos de downlink.

El UL-MAP lleva la información de al duración de las mini ranuras, tiempo de inicio, el CID y demás información al igual que el DL-MAP para downlink.

2.4.5.1.5.2 Subcapa PMD de Uplink

Los procesos que se llevan a cabo en esta subcapa se pueden visualizar en el siguiente diagrama de bloques:

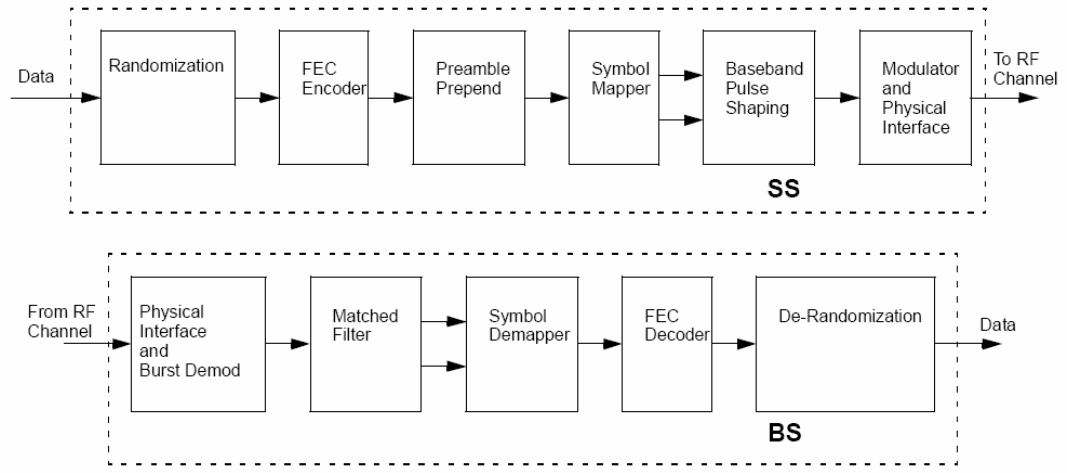


Figura 2.109. Diagrama de Bloques de la Subcapa PMD de Uplink[115]

El proceso de reorganización aleatoria se debe implementar con las mismas bases que para el canal de downlink y con el mismo polinomio generador; y esta misma consideración se debe tomar para la codificación FEC.

La modulación usada para el canal de uplink debe ser variable y según lo especifique la BS, por lo que las modulaciones QPSK y 16QAM deben ser obligatorias y 64QAM opcional; en caso de sucederse cambios en la modulación, las reglas de potencia son iguales a las establecidas para downlink.

2.4.5.1.6 Tasas de Baudios y Anchos de Banda de Canal

Existe una gran cantidad de espectro para los equipos que trabajan en las bandas de 10 a 66 GHz para modos de operación PMP; sin embargo dependiendo de las regiones en las que se encuentren existirán limitaciones de anchos de banda de canal.

Todos los sistemas deben tener una forma de pulso de coseno levantado con un factor de 0.25, y sus tasas de baudios deben adaptarse para tener ranuras físicas con números enteros por trama.

[115] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 340.

Channel size (MHz)	Symbol rate (MBd)	Bit rate (Mb/s) QPSK	Bit rate (Mb/s) 16-QAM	Bit rate (Mb/s) 64-QAM	Recommended Frame Duration (ms)	Number of PSs/frame
20	16	32	64	96	1	4000
25	20	40	80	120	1	5000
28	22.4	44.8	89.6	134.4	1	5600

Tabla 2.58. Tasas de Baudio y Tamaños de Canal para un Factor de Roll-Off de 0.25[116]

2.4.5.1.7 Control del Subsistema de Radio

El demodulador de downlink por lo general se encarga de suministrar un reloj de referencia externo, gracias a los símbolos de reloj en la trama de downlink, este reloj nos sirve para cuando el reloj se encuentra ocupado en otros procesos.

Para poder tener una coexistencia entre los diferentes dispositivos, las frecuencias centrales RF transmitidas ya sean de la BS como de la SS deben tener una precisión mayor a ± 10E-6 y las frecuencias de portadora deben tener una precisión de ± 8E-6.

El algoritmo para el control de la potencia debe ser implementado a conveniencia del fabricante, sin embargo debe ser capaz de soportar las calibraciones iniciales y los procedimientos de ajuste durante el funcionamiento.

2.4.5.2 Especificaciones de Capa Física para Sistemas WirelessMAN SCa

2.4.5.2.1 Introducción

La capa física WirelessMAN SCa esta basada sobre la tecnología de una sola portadora y para operaciones sin línea de vista (NLOS), es decir que funciona en la banda de frecuencias menores a 11 GHz.

Para las bandas de frecuencia que no requieren de licencias, los anchos de banda de los canales permitidos deben estar limitados según anchos de banda regulados, mediante la división para potencias de 2 pero no menores a 1.25 MHz.

Los elementos que posee esta capa física en algunos casos son similares a los definidos para WirelessMAN SC, más características propias, estos se muestran a continuación:

[116] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 343.

- Definiciones TDD y FDD.
- El canal uplink es TDMA.
- El canal downlink es TDM o TDMA.
- Codificación FEC y modulación adaptativa de bloque para uplink y downlink.
- Estructura de Trama que mejora la ecualización y desempeño de estimación de canal para NLOS y ambientes con retardos esparcidos extendidos.
- Ranuras físicas con adaptación en tamaños de ráfaga.
- Modulación FEC concatenada usando Reed-Solomon y modulación de código de Trellis con reordenamiento opcional.
- Opciones adicionales BTC.
- No soporte FEC al usar ARQ para control de errores.
- Opción de diversidad de transmisión de codificación de tiempo de espaciamiento (STC).
- Modos robustos para operaciones con CINR bajos.
- Configuración de parámetros y mensajes entre capas que facilitan implementaciones de sistemas de antenas adaptativas.

2.4.5.2.2 Proceso de Transmisión

Para esta capa física WiMAX, el proceso de transmisión es el mismo tanto para uplink como para downlink, los procesos que sigue la información para su transmisión están identificados en el siguiente diagrama de bloques.

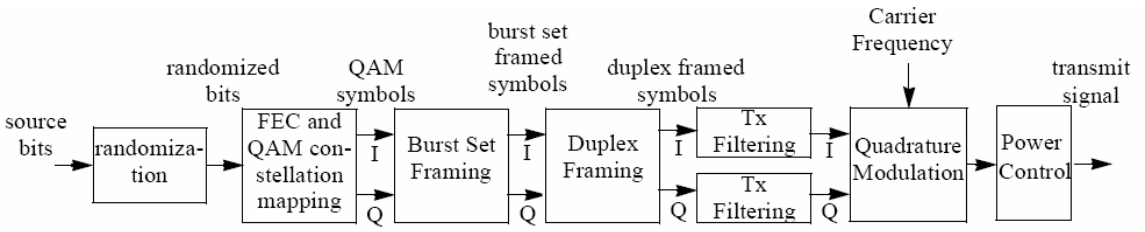


Figura 2.110. Diagrama de Bloques del Proceso de Transmisión WirelessMAN SCa[117]

[117] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 356.

El proceso de la reorganización aleatoria se realiza de la misma manera que para la capa física SC, es decir mediante la suma de modulo 2 y la misma ecuación del polinomio generador.

La modulación FEC concatenada es una concatenación serial entre el código externo Reed-Solomon y una modulación de código de Trellis, entre los dos de forma opcional podemos tener un reordenamiento de bytes opcional.

La modulación de código de Trellis tiene una tasa de 1/2, pero puede llegar a soportar tasas de 2/3, 3/4, 5/6, y 7/8 mediante la reutilización de las salidas de la modulación 1/2.

Se puede no utilizar la modulación FEC, para QPSK esta característica es obligatoria, pero para el resto de modulaciones BPSK, 16QAM, 64QAM y 256QAM es opcional.

Las modulaciones que puede soportar esta nueva capa física para operaciones NLOS son las siguientes:

Modulación	Soporte (M = obligatorio, O = opcional)	
	UL	DL
Spread BPSK	M	M
BPSK	M	M
QPSK	M	M
16 QAM	M	M
64 QAM	M	M
256 QAM	O	O

Tabla 2.59. Modulaciones Soportadas por WirelessMAN SCa

2.4.5.2.2.1 Trama de Conjunto de Ráfagas

Los datos tanto de uplink como downlink deben estar formateadas en tramas de conjuntos de ráfagas, para downlink se debe soportar una o más tramas de conjuntos de ráfagas TDM y para uplink tramas de conjuntos de ráfagas TDMA.

2.4.5.2.2.1.1 Palabra Única

La longitud de la palabra única se representa con la letra U, esta debe ser al menos tan larga como la totalidad el retraso esparcido de canal que se pretende.

Las palabras únicas (UW) se derivan de las secuencias Frank-Zadoff y poseen propiedades de auto correlación cero de amplitud constante; para WiMAX, U puede tomar los valores de 16 y 64, mientras que para los anchos de banda mayores a 20 MHz la longitud U debe ser de 256.

Las secuencias de palabra única para esta capa física son símbolos provenientes de las modulaciones QPSK, 8PSK y 16PSK respectivamente con las longitudes soportadas.

2.4.5.2.2.1.2 Formato del Conjunto de Ráfaga Estándar

El formato de las tramas estándar para un conjunto de ráfagas contiene tres campos: el preámbulo de conjunto de ráfaga, una o más ráfagas con pilotos y un intervalo de resguardo de retraso esparcido de receptor (RxDS).

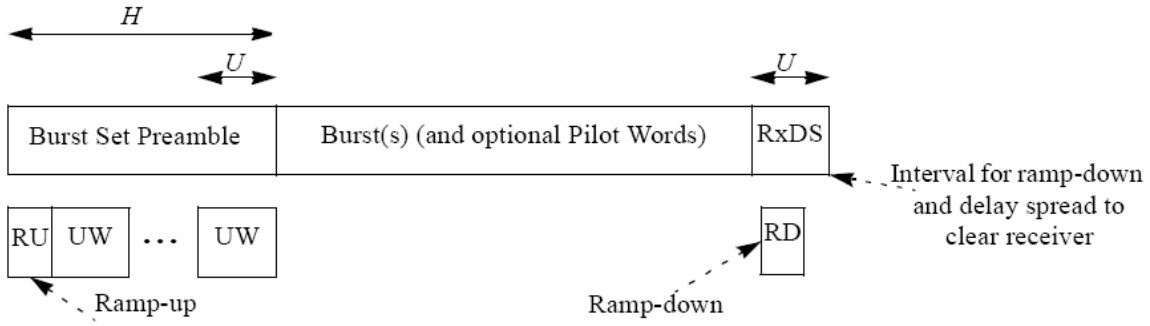


Figura 2.111. Formato de la Trama Estándar de Conjunto de Ráfaga[118]

El preámbulo de esta trama consiste en una región de inicio y el cuerpo del preámbulo; el perfil de ráfaga o el elemento de información para uplink o downlink respectivamente indican la duración del campo de inicio (Rr), el número de UW (m) y U.

[118] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 380.

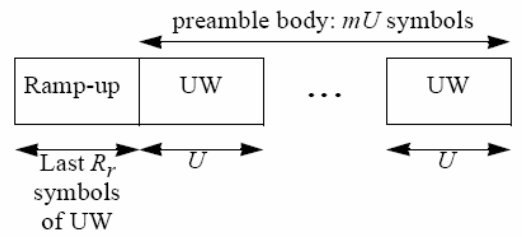


Figura 2.112. Formato del Preámbulo de Conjunto de Ráfaga[119]

La ráfaga de downlink puede contener ráfagas TDM moduladas adaptativamente según el destinatario, las ráfagas están en orden decreciente según su robustez; la única excepción la carga nula de relleno, que debe ir siempre al final. Una ráfaga de uplink contiene una sola ráfaga.

La carga nula se usa cuando la carga de datos no es suficiente para llenar la trama, esta habilidad de poner y desechar la carga nula debe ser obligatoria para los equipos WiMAX que trabajen en esta capa física.

Finalmente el campo RxDS es un periodo de tranquilidad en donde el transmisor finaliza y el receptor recoge los símbolos con retraso esparcido al final del conjunto de ráfaga, este campo se suma a la brecha entre tramas y debe ser de al menos la longitud de una palabra única.

2.4.5.2.2.2 FDD

En FDD los canales de uplink y downlink trabajan en diferentes frecuencia, algunas SS pueden trabajar después de ser configuradas apropiadamente no solo recibiendo ráfagas de downlink y uplink sino trabajando en downlink continuamente.

El sistema FDD con downlink TDM es capaz de soportar varios conjuntos de ráfagas dentro de una sub trama de forma obligatoria, pero no debe ocupar todo el tiempo destinado para downlink.

Toda sub trama de downlink debe comenzar con un preámbulo, seguido de un encabezado de control de trama y la carga que puede contener mensajes además de datos; finalmente lleva el campo RxDS.

[119] IBID 118

Por otro lado la sub trama de uplink debe contener las siguientes categorías de ráfagas:

- Petición de Ajuste Inicial, transmitidas en las ranuras de contención reservadas para este propósito.
- Peticiones de Ancho de Banda que son transmitidas en ranuras de contención reservadas para polls de multicast o broadcast para necesidades de ancho de banda.
- Otorgaciones de ancho de banda que son específicamente colocadas para SS individuales.

Las ráfagas de uplink TDMA, deben tener un preámbulo de conjunto de ráfaga, una ráfaga y un RxDS; una brecha separa las transmisiones de varias SS en uso del canal.

2.4.5.2.2.3 TDD

TDD utiliza una misma frecuencia para llevar las transmisiones uplink y downlink, otorgando intervalos de tiempo a cada una.

Se utiliza una trama compartida, la sub trama de downlink ya primero seguida de la sub trama de uplink, el tamaño de esta trama compartida es constante, sin embargo los tamaños de las sub tramas pueden variar. Los equipos deben ser capaces de acomodar más de un conjunto de ráfagas TDM.

2.4.5.2.2.4 Forma del Pulso Banda Base

Las señales en fase y cuadratura que salen del modulador de símbolos deben ser filtradas por un filtro de coseno levantado, el factor de roll-off debe ser de 0.25, pero de forma opcional se puede soportar factores de 0.15 y 0.18.

2.4.5.2.3 Requerimientos del Sistema

Para esta capa física WiMAX se deben tener en cuenta algunos requerimientos para que el sistema tenga un apropiado funcionamiento, entre ellos es la precisión en la frecuencia del canal, que para una SS debe ser ± 15E-6 y para la BS de ± 8E-6.

Las SNR de las señales transmitidas deben tener no menos de 40 dB, medido en el conector de la antena, mientras que los periodos de finalización e inicio deben tener una tolerancia de 5 μs.

La potencia máxima de entrada de la señal para la BS debe ser de -40 dBm y debe tolerar señales de 0 dBm sin daño en los circuitos; mientras que para una SS el nivel de potencia máxima es de -20 dBm y debe tolerar señales de 0 dBm sin daño en los circuitos.

2.4.5.3 Especificaciones de Capa Física para Sistemas WirelessMAN OFDM

2.4.5.3.1 Introducción

La capa física WirelessMAN OFDM esta basada en la modulación OFDM y diseñada para operaciones NLOS en las bandas de frecuencia menores a los 11GHz.

El uso de un prefijo cíclico (CP) las muestras que se requieren para poder realizar la FFT en el receptor, pueden ser tomadas de cualquier lugar a lo largo del símbolo extendido, esto provee inmunidad al multipath así como tolerancia para los errores de sincronización de símbolo.

Al momento de la inicialización la SS debe buscar todos los posibles valores de prefijo cíclico hasta que encuentre el que usa la BS, la SS debe usar este CP en el uplink; si la BS cambia dicho CP todas las estaciones deberán re sincronizarse con la BS.

Un símbolo OFDM esta hecho de subportadoras, el número de subportadoras determinan el tamaño de la FFT usada, existen tres tipos de subportadoras:

- ✓ Subportadoras de datos.
- ✓ Subportadoras piloto.
- ✓ Subportadoras nulas, no hay transmisión, se usa para bandas de guarda, subportadoras sin uso y la subportadora de DC.

Las subportadoras sin uso existen solo para la sub canalización de las transmisiones de uplink y se implementan solo si la BS puede soportarlas.

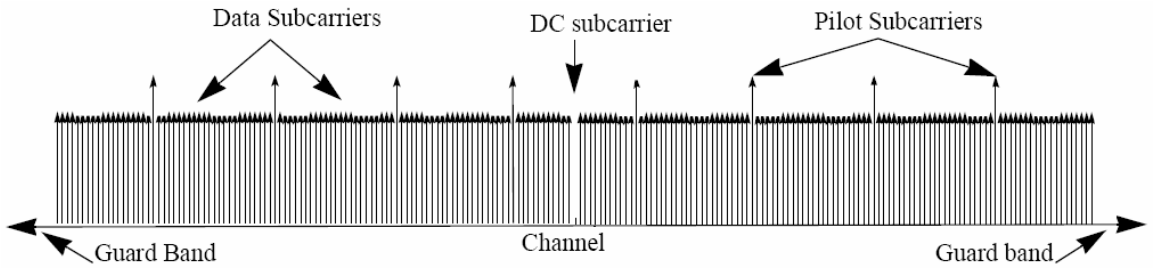


Figura 2.113. Descripción de Frecuencias OFDM[120]

2.4.5.3.2 Codificación de Canal

La codificación de canal esta compuesta de tres pasos: reordenamiento aleatorio, codificación FEC y reordenamiento, y se deben aplicar en este orden para la transmisión.

2.4.5.3.2.1 Reordenamiento Aleatorio

El reordenamiento aleatorio se realiza en cada ráfaga de datos ya sean de uplink o downlink; en caso de que la cantidad de datos a se transmitidos no encaje en la cantidad de datos colocados se debe aumentar solo unos a final del bloque de transmisión.

El registro de cambio debe ser inicializado para cada nueva colocación; el polinomio generador de la secuencia binaria pseudo aleatoria responde a la siguiente ecuación:

$$P(x) = 1 + x^{14} + x^{15}$$

Formula 2.23. Ecuación del Polinomio Generador PRBS[121]

Los preámbulos no deben ser reorganizados de forma aleatoria. A la salida de este polinomio se le realiza operaciones XOR con los bits de cada ráfaga para lograr la información aleatoria.

2.4.5.3.2.2 FEC

La codificación FEC consiste en la concatenación de un código externo Reed-Solomon y un código convolucional interno, tanto para uplink como downlink, de forma opcional se puede soportar turbo códigos de bloque y turbo códigos convolucionales.

[120] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 428.
[121] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 431.

El código concatenado Reed-Solomon-código convolucional (RS-CC), tiene como parámetros para su parte Reed-Solomon N=255, K=239, T=8, que corresponden al número de bits de salida, bits de entrada y bits que pueden ser corregidos respectivamente.

Cada bloque Reed-Solomon es codificado por el codificador convolucional, el cual tiene una tasa de 1/2; pero para soportar tasas de 2/3, 3/4 y 5/6 se debe usar el principio de reutilización de bits.

En la siguiente tabla se pueden apreciar las tasas de código para las diferentes modulaciones:

Modulation	Uncoded block size (bytes)	Coded block size (bytes)	Overall coding rate	RS code	CC code rate
BPSK	12	24	1/2	(12,12,0)	1/2
QPSK	24	48	1/2	(32,24,4)	2/3
QPSK	36	48	3/4	(40,36,2)	5/6
16-QAM	48	96	1/2	(64,48,8)	2/3
16-QAM	72	96	3/4	(80,72,4)	5/6
64-QAM	96	144	2/3	(108,96,6)	3/4
64-QAM	108	144	3/4	(120,108,6)	5/6

Tabla 2.60. Codificación de Canal por Modulación[122]

2.4.5.3.2.3 Reordenamiento

Todos los bits de datos deben ser reorganizados por un bloque de reordenamiento cuyo tamaño de bloque corresponde al número de bits codificados por sub canal por símbolo OFDM.

El reordenamiento esta definido por dos permutaciones, la primera asegura que los bits codificados adyacentes son asignados en subportadoras no adyacentes; la segunda permutación asegura que los bits codificados adyacentes sean asignados en bits más o menos significativos de la constelación.

[122] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 434.

2.4.5.3.2.4 Modulación

La modulación de datos se realiza mediante asignadotes de constelación, se utilizan las modulaciones BPSK, QPSK, 16QAM y 64QAM, aunque esta última es opcional para los equipos que trabajan en las bandas de frecuencia sin licencia.

Los datos salidos de la modulación de constelación serán moduladas en subportadoras de datos.

En la modulación del piloto se debe primero generar una secuencia pseudo aleatoria con el mismo método definido anteriormente, pero con secuencias de inicio especificas y diferentes para uplink y downlink, estos valores resultantes son modulados en símbolos OFDM.

2.4.5.3.2.5 Estructura del Preámbulo y Modulación

Todos los preámbulos están estructurados como uno o dos símbolos OFDM, los símbolos OFDM están definidos por los valores de los componentes de las subportadoras; cada símbolo OFDM contiene un prefijo cíclico cuya longitud es la misma para los CP de los símbolos OFDM de datos.

El primer preámbulo en el PDU de capa física de downlink y el preámbulo del ajuste inicial, consisten de dos símbolos OFDM consecutivos, el primer símbolo lleva el CP y le siguen cuatro repeticiones de un fragmento de 64 muestras, mientras que el segundo tiene el CP seguido de dos fragmentos de 128 muestras.

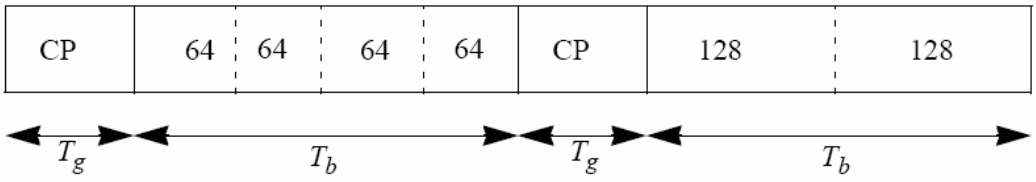


Figura 2.114. Estructura del Preámbulo Largo OFDM[123]

Para uplink solo se usa el preámbulo compuesto de un símbolo OFDM, este contiene el CP seguido de dos fragmentos de 128 muestras, este es el preámbulo corto.

[123] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 447.

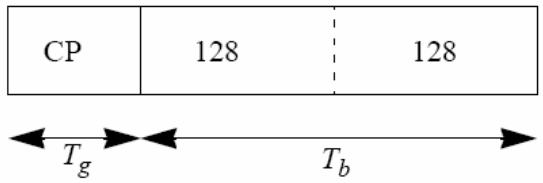


Figura 2.115. Estructura del Preámbulo Corto OFDM[124]

2.4.5.3.3 Estructura de la Trama

2.4.5.3.3.1 PMP

Para las bandas licenciadas los métodos de duplexión deben ser FDD o TDD, en FDD se puede tener transmisiones half duplex; mientras que en bandas sin licencia el método debe ser TDD.

La capa física OFDM soporta transmisiones basadas en tramas, es decir que la trama consiste en una sub trama de uplink y otra de downlink; la sub trama de downlink consiste de un solo PDU de capa física; la sub trama de uplink consiste de intervalos de contención planificados para el ajuste inicial, peticiones de ancho de banda y uno o múltiples PDU de capa física de uplink, cada uno transmitido desde un SS diferente.

Un PDU de capa física de downlink esta compuesto de un preámbulo largo, le sigue una ráfaga de encabezado de control de trama (FCH) de longitud de un símbolo OFDM usando BPSK 1/2, finalmente una o varias ráfagas de downlink.

En caso de existir DL-MAP este debe ir después del FCH. Las ráfagas ya sean de uplink o downlink llevar mensajes MAC, es decir PDUs MAC

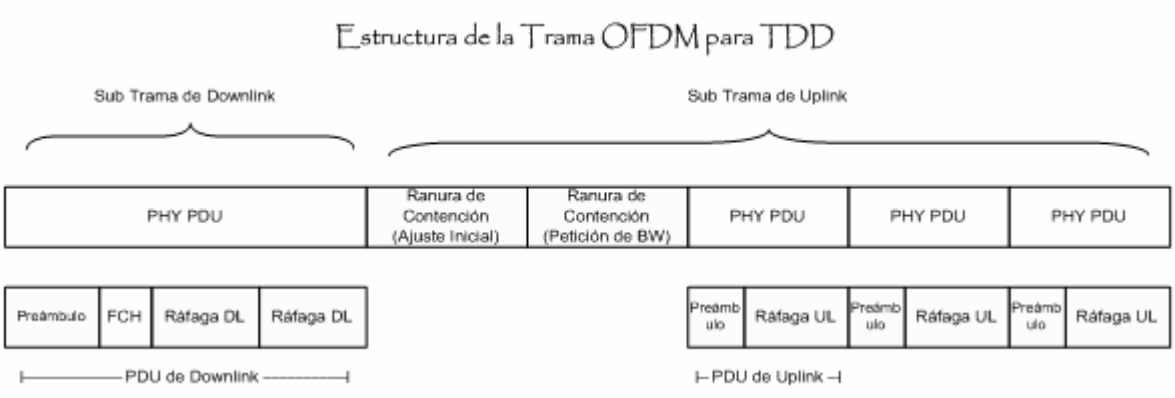


Figura 2.116. Estructura de la Trama OFDM para TDD

[124] IBID 123

Para los sistemas TDD y FDD half duplex, primero se debe enviar las tramas de downlink seguidas de las tramas de uplink teniendo en cuanta las brechas de separación entre tramas y las de retrasos. Las tramas de uplink y downlink son similares a las antes vistas.

2.4.5.3.4 Mecanismos de Control

2.4.5.3.4.1 Sincronización

Para TDD y FDD se recomienda que todas las BS estén sincronizadas a una señal de reloj común; en caso de que se pierda dicha señal, cada BS puede continuar operando y debe re sincronizarse de forma automática cuando la señal se recupere.

La referencia de sincronización puede ser de 1 pulso por segundo o una señal de 10 MHZ, estas señales serán provistas mediante receptores GPS.

2.4.5.3.4.2 Ajustes

Existen dos tipos de ajustes, un ajuste inicial y los ajustes periódicos; los ajustes iniciales se llevan a cabo durante dos fases de operación durante el proceso de registro y cuando se pierde la sincronización, el otro ajuste se lleva a cabo periódicamente.

El ajuste inicial usa el intervalo basado en contención de ajuste inicial, con un preámbulo largo y el ajuste periódico usa las ráfagas de uplink regulares.

El proceso de ajuste es de naturaleza cíclica, en donde parámetros iniciales de tiempo y potencia se usan al principio, seguidos por ciclos donde se calculan o recalculan los parámetros que están siendo usados hasta que los parámetros concuerden con los criterios de aceptación del nuevo subscriptor.

2.4.5.3.4.3 Petición de Ancho de Banda

Existen dos tipos de regiones de petición en una trama, el primero es la petición de región completa, y la petición de región especifica.

Se usa la petición de región completa cuando la sub canalización no esta activada, cada oportunidad de transmisión debe consistir de un preámbulo corto y un símbolo OFDM usando el perfil de ráfaga más robusto.

Cuando al sub canalización esta activada, la transmisión de una SS debe contener un preámbulo de sub canalización correspondiente a la oportunidad de transmisión escogida, seguida de símbolos OFDM usando el perfil de ráfaga más robusto.

En una petición de región especifica, la estación debe enviar un código corto en la oportunidad de transmisión, esta consiste de cuatro subportadoras por dos símbolos OFDM.

2.4.5.3.4.4 Control de Potencia

En esta capa física se necesita de un algoritmo de control de potencia, para en canal de uplink tanto para la calibración inicial como para los ajustes periódicos; el propósito es el de llevar la densidad de potencia recibida de un subscriptor a un nivel deseado.

La estación base debe ser capaz de proveer un medida de potencia precisa de las señales de ráfaga recibidas, este valor puede ser comparado con una señal de referencia y el error puede ser enviado a la capa MAC para realizar los ajustes necesarios.

2.4.5.3.5 Requerimientos de Transmisión

El control del nivel de transmisión debe ser capaz de soportar variaciones mínimas de 30 dB y si la SS soporta sub canalización el control de la potencia debe soportar 50 dB.

Para las bandas que requieren licencias, los anchos de banda de canal deben estar limitados a los anchos de banda regulados divididos para potencias de 2 y redondeados a múltiplos de 250 KHz mientras no sean menores de 1.25 MHz.

2.4.5.3.6 Requerimientos del Receptor

Una vez que se realiza la codificación FEC el BER no debe ser mayor a los 10E-6, en transmisiones con mensajes normales.

La señal de entrada máxima en el receptor debe ser de -30 dBm, sin embargo debe ser capaz de soportar 0 dBm sin daño.

2.4.5.4 Especificaciones de Capa Física para Sistemas WirelessMAN OFDMA

2.4.5.4.1 Introducción

Los equipos de capa física WirelessMAN OFDMA basados en la modulación OFDM, están diseñados para operaciones NLOS para las bandas de frecuencia inferiores a los 11 GHz.

Para estas bandas que requieren de licencias, los anchos de banda de canal permitidos deben estar limitados por los anchos de banda regulados divididos para cualquier potencia de 2 mientras que no sea menor a 1 MHz.

2.4.5.4.2 Definiciones OFDMA

2.4.5.4.2.1 Ranuras y Región de Datos

Una ranura en la capa física OFDMA requiere tanto de tiempo y dimensión sub canal, es la unidad de ubicación de datos más pequeña posible.

La región de datos en OFDMA es una ubicación de dos dimensiones de un grupo de sub canales continuos en un grupo de símbolos OFDMA continuos.

2.4.5.4.2.2 Segmento

Un segmento es una subdivisión del grupo de sub canales OFDMA disponibles.

2.4.5.4.2.3 Zona de Permutación

Es un número de símbolos OFDMA continuos, en el uplink o downlink que usan la misma formula de permutación, las sub tramas de uplink o downlink pueden contener más de una zona de permutación.

2.4.5.4.2.4 Asignación de Datos OFDMA

Los datos de la capa MAC deben ser asignados a una región de datos OFDMA para downlink y uplink usando los algoritmos siguientes:

Downlink.-

- ✓ Segmentar los datos en bloques para que quepan en una ranura OFDMA.
- ✓ Cada ranura debe ocupar uno o más sub canales en el eje de sub canales y dos símbolos OFDMA en eje del tiempo, se debe realizar la asignación de las ranuras de tal manera que la ranura numerada más baja ocupe el sub canal numerado más bajo en el símbolo OFDMA numerado más bajo.
- ✓ Continuar con la asignación de tal forma que el índice de los símbolos OFDMA se incremente, cuando el tope de la región de datos se alcance, se debe continuar con la asignación desde el símbolo OFDMA numerado más bajo en el siguiente sub canal.

Uplink.-

- ✓ Segmentar los datos en bloques de tamaño que quepan en una ranura OFDMA.
- ✓ Cada ranura debe ocupar uno o más sub canales en el eje de sub canales y tres símbolos OFDMA en el eje del tiempo, la asignación de ranuras debe ser tal que la ranura numerada más baja ocupe el sub canal numerado más bajo en el símbolo OFDMA numerado más bajo.
- ✓ Continuar la asignación de tal manera que el índice de símbolo OFDMA se incremente, cuando el tope de la zona de uplink se alcance, se debe continuar con la asignación desde el símbolo OFDMA numerado más pequeño en el siguiente sub canal.

2.4.5.4.3 Estructura de la Trama

2.4.5.4.3.1 Modos de Duplexión

En las bandas con licencia, los métodos de duplexión deben ser FDD o TDD, en el caso de estaciones de subscriptor FDD se pueden tener half duplex FDD.

2.4.5.4.3.2 Estructura de la Trama PMP

Al momento de la implementación de un sistema TDD, la estructura de la trama se construye de las transmisiones de la BS y la SS. Cada trama en las transmisiones de downlink comienzan con en preámbulo seguido por un periodo de transmisión downlink y un periodo de transmisión de uplink, en cada trama, se deben insertar brechas en el uplink y downlink y al final de cada trama.

Las ubicaciones de sub canal en el downlink pueden ser realizadas de las siguientes maneras: uso parcial de sub canales (PUSC), donde algunos de los sub canales son para el transmisor; uso total de sub canales (FUSC), donde todos los sub canales se usan para el transmisor.

Los dos primeros sub canales transmitidos en el primer símbolo de datos de downlink se le conoce como FCH (encabezado de control de trama), este se usa QPSK con tasa 1/2 con cuatro repeticiones en una zona PUSC.

La trama OFDMA puede incluir múltiples zonas, las transiciones entre zonas se indica en el DL-MAP.

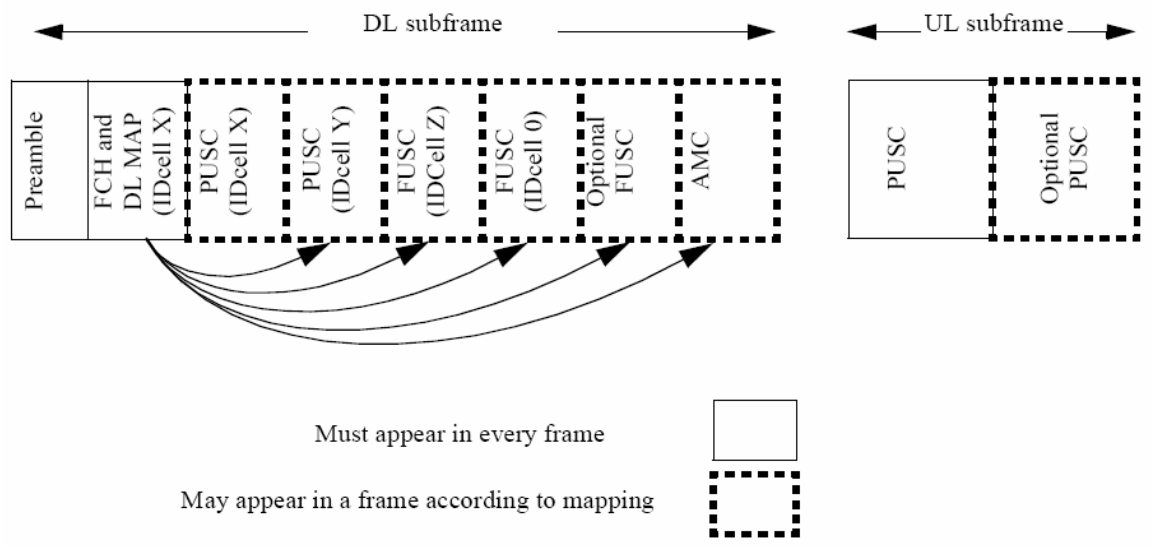


Figura 2.117. Trama OFDMA con Múltiples Zonas[125]

2.4.5.4.3.3 Prefijo de Trama de Downlink

Este prefijo es una estructura de datos transmitida al principio de cada trama y contiene información relacionada con la trama actual y esta asignada al FCH.

2.4.5.4.3.4 Ubicación de Sub Canales para FCH y Numeración de Sub Canal Lógico

En PUSC, cualquier segmento usado debe tener al menos 12 sub canales, las cuatro ranuras en la parte de downlink del segmento contiene el FCH; estas ranuras contiene 48

[125] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 501.

bits modulados con QPSK de tasa 1/2 y repetición de código cuatro; los conjuntos de sub canales asignados para los segmentos 0, 1 y 2 son los sub canales 0-11, 20-31 y 40-51.

Para que la SS entienda estos sub canales como un solo bloque se renumeran desde el sub canal menor hasta el mayor empezando con el valor de cero para el primer sub canal.

2.4.5.4.3.5 Ubicaciones de transmisiones de Uplink

Las ubicaciones para transmisiones de uplink de usuario es un número de sub canales sobre un número de símbolos OFDMA; el número de símbolos debe ser igual a 3N, donde N es un entero positivo.

La estructura de ubicaciones básica es un sub canal para una duración de 3 veces la duración de símbolo OFDMA, las ubicaciones más grandes son repeticiones de la estructura básica.

La estructura de trama usada para uplink incluye una ubicación para el ajuste inicial y una ubicación para transmisión de datos.

2.4.5.4.4 Ubicación de Subportadoras OFDMA

Para OFDMA la frecuencia de subportadora se puede obtener de la siguiente formula:

$$Fs = floor\left(\frac{8}{7}\frac{BW}{8000}\right)8000$$

Formula 2.24. Frecuencias de Subportadora OFDMA[126]

De estas subportadoras se extraen tonos de guarda y obtenemos las subportadora usadas, tanto para uplink y downlink, estas subportadoras usadas son asignadas para subportadoras pilotos y de datos.

Para FUSC, en downlink, los tonos pilotos están ubicados primero, las subportadoras de datos que restan están divididas en sub canales que son usados exclusivamente para datos. Para PUSC en downlink o uplink, el conjunto de subportadoras usadas son divididas en sub canales, y luego las subportadoras piloto son ubicadas dentro de cada sub canal.

[126] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 551.

En FUSC existe una subportadora piloto común, pero en PUSC cada sub canal contiene su propio conjunto de subportadoras piloto.

2.4.5.4.4.1 Downlink

El downlink puede estar dividido en una estructura de tres segmentos e incluye un preámbulo el cual comienza la transmisión. El preámbulo es el primer símbolo de la transmisión downlink, el cual esta modulado BPSK con un código pseudo ruido especifico.

La estructura de símbolo PUSC esta compuesta de subportadoras pilotos, de datos y cero, el símbolo es primero dividido en clusters básicos y las portadoras cero son ubicadas, las portadoras piloto y de datos se ubican dentro de cada cluster.

Parámetro	Valor	Comentarios
Número de Subportadoras de DC	1	Index 1024
Número de Subportadoras de Guarda (Izquierda)	184	
Número de Subportadoras de Guarda (Derecha)	183	
Número de Subportadoras Usadas	1681	Número de todas las subportadoras usadas en un símbolo, incluyendo todos los posibles pilotos y la portadora de DC.
Número de Subportadoras por Cluster	14	
Número de Clusters	120	
Número de Subportadoras de Datos en cada Símbolo por Sub canal	4	
Número de Sub canales	60	

Tabla 2.61. Ubicación de Portadoras de Downlink OFDMA PUSC

Por otro lado la estructura de símbolo para FUSC están construidas de subportadoras piloto, datos y cero, en el símbolo se ubica primero los pilotos y las subportadoras cero y las subportadoras restantes se usan para las subportadoras de datos.

Parámetro	Valor	Comentarios
Número de Subportadoras de DC	1	Index 1024
Número de Subportadoras de Guarda (Izquierda)	173	
Número de Subportadoras de Guarda (Derecha)	172	
Número de Subportadoras Usadas	1703	Número de todas las subportadoras usadas en un símbolo, incluyendo todos los posibles pilotos y la portadora de DC.
Número de Subportadoras de Datos	1536	
Número de Subportadoras de datos por Sub canal	48	
Número de Sub canales	32	

Tabla 2.62. Ubicación de Portadoras de Downlink OFDMA FUSC

Cada sub canal esta compuesto de 48 subportadoras.

2.4.5.4.4.2 Uplink

El uplink al igual que el downlink soporta hasta tres segmentos; el uplink soporta 70 sub canales cada uno con 48 portadoras de datos como bloque mínimo de procesamiento.

Parámetros	Valor
Número de Subportadoras de DC	1
N_{used}	1681
Subportadoras de Guardia: Izquierda, derecha	184, 183
Número de Sub canales	70
Número de Subportadoras	48
Número de Viga	420
Vigas por Sub canal	6

Tabla 2.63. Ubicación de Subportadoras de Uplink OFDMA

2.4.5.4.5 Ajustes OFDMA

Cuando se utiliza la capa física WirelessMAN OFDMA, la capa MAC debe definir un canal de ajuste, este esta compuesto de uno o más grupos de seis sub canales adyacentes, donde los grupos son definidos desde el primer sub canal, o de forma opcional puede estar compuesto de ocho sub canales.

Para realizar una transmisión de ajuste, cada usuario escoge aleatoriamente un código de ajuste de un grupo de códigos binarios previamente definidos, estos códigos se modulan según la modulación BPSK sobre las subportadoras en el canal de ajuste, se ubica un bit por subportadora.

2.4.5.4.5.1 Transmisiones de Ajuste Inicial

Las transmisiones de ajuste inicial deben ser usadas por cualquier SS que desee sincronizarse al canal del sistema por primera vez, esta transmisión debe realizarse durante dos símbolos consecutivos, el mismo código de ajuste se transmite sobre el canal de ajuste durante cada símbolo, sin discontinuidades en la fase.

2.4.5.4.5.2 Ajustes Periódicos y Transmisiones de Petición de Ancho de Banda

Las transmisiones de ajuste periódico son enviadas periódicamente por el sistema de ajuste periódico, las peticiones de ancho de banda son para pedir lugares de uplink a la BS. Se debe tener en cuenta que estas transmisiones se realizan cuando la SS ya esta sincronizada al sistema.

Para realizar estas transmisiones, la SS puede optar por una de las siguientes formas:

- ✓ Modular un código de ajuste sobre el sub canal de ajuste por un periodo de un símbolo OFDMA, los sub canales de ajuste son asignados dinámicamente por la capa MAC.
- ✓ Modular tres códigos de ajuste consecutivos sobre el sub canal de ajuste por un periodo de tres símbolos OFDMA.

2.4.5.4.5.3 Códigos de Ajuste

Los códigos binarios son códigos pseudo ruido producidos por la secuencia binaria pseudo aleatoria, la cual implementa el siguiente polinomio generador:

$$P(x) = 1 + x^1 + x^4 + x^7 + x^{15}$$

Formula 2.25. Polinomio Generador PRBS de Código de Ajuste[127]

De donde el semilla de generación es 0, 0, 1, 0, 1, 0, 1, 1, s0, s1, s2, s3, s4, s5, s6; donde s0 a s6 son los bits de identificación de la celda de uplink.

2.4.5.4.6 Codificación de Canal

El proceso de codificación de canal incluye los procesos de reordenamiento aleatorio, codificación FEC, reordenamiento de bit y modulación.

Cuando el código de repetición es usado, la asignación al momento de la transmisión debe incluir siempre un número par de sub canales adyacentes.

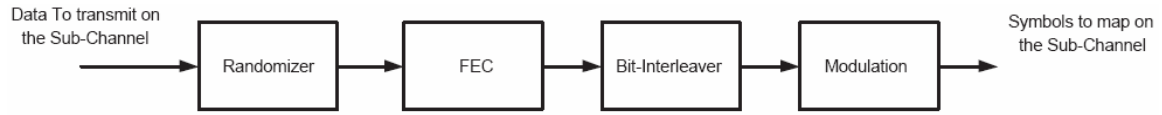


Figura 2.118. Proceso de Codificación de Canal Regular OFDMA[128]

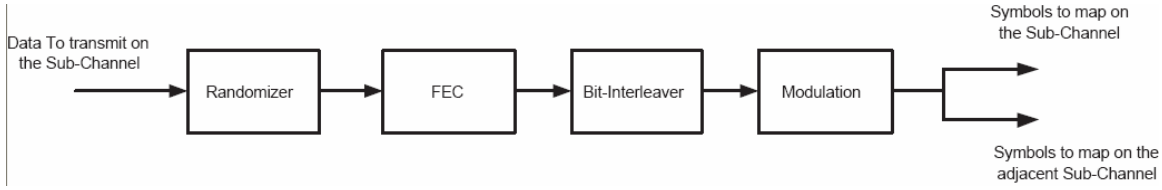


Figura 2.119. Proceso de Codificación de Canal con Repetición de Código OFDMA[129]

2.4.5.4.6.1 Reordenamiento Aleatorio

El reordenamiento aleatorio se realiza a los datos transmitidos tanto para uplink como downlink, este se realiza en cada bloque FEC, si la cantidad de datos no encaja perfectamente con la cantidad de datos asignados, se debe colocar un padding de solo unos al final del bloque de transmisión.

El generador de la secuencia binaria pseudo aleatoria es la misma que se ha revisado con anterioridad para las demás capas física WiMAX.

---

[127] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 578.
[128] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 588.
[129] IBID 128

2.4.5.4.6.2 Codificación

El tamaño del bloque de codificación depende del número de sub canales asignados y la modulación especificada para la transmisión.

Se debe realizar la concatenación de un número de sub canales para poder realizar bloques de codificación más largos donde sea posible, con la única limitante de que no pasar el bloque más largo bajo la misma tasa de codificación.

Modulación	Tasa
QPSK	1/2
QPSK	3/4
16 QAM	1/2
16 QAM	3/4
64 QAM	1/2
64 QAM	2/3
64 QAM	3/4

Tabla 2.64. Modulaciones y Tasas Soportadas por WirelessMAN OFDMA

La codificación convolucional que soporta esta capa física es la misma que se ha definido con anterioridad, es decir tiene una tasa 1/2 pero mediante la reutilización de bits se pueden lograr tasas de 2/3, 3/4, y 5/6.

2.4.5.4.6.3 Reordenamiento de Bit

Todos los bits de datos deben ser reordenados por un bloque de reordenamiento, este proceso se realiza mediante dos permutaciones, la primera asegura que bits codificados adyacentes sean asignados sobre subportadoras no adyacentes; y, la segunda permutación nos asegura que los bits codificados adyacentes sean asignados alternadamente sobre bits más o menos significativos de la constelación.

2.4.5.4.6.4 Modulación

Antes de proceder con la modulación de esta capa física, debemos detenernos para revisar la generación de la secuencia *wk* que es la secuencia que entra al modulador de constelación.

La secuencia se genera mediante un generador PRBS a ser usado de ahora en adelante mediante el siguiente polinomio generador:

$$P(x) = x^{11} + x^{9} + 1$$

Formula 2.26. Polinomio Generador de la Secuencia *wk*

Después del reordenamiento de bit, los bits de datos entran serialmente al modulador de constelación, las modulaciones QPSK y 16QAM son obligatorias mientras que 64QAM es opcional.

2.4.5.4.7 Mecanismos de Control

2.4.5.4.7.1 Sincronización

Para TDD y FDD, se recomienda que todas las BS estén sincronizadas a una sola referencia de tiempo, en caso de que se pierda dicha señal, las BS continuaran operando y se re sincronizaran al recuperar la señal, la señal de sincronización puede ser provista por un pulso por segundo o una señal de referencia de 10 MHz, las cuales se obtienen de un receptor GPS.

Las SS deben adquirir y ajustar sus temporizadores de tal manera que los símbolos OFDMA de uplink estén sincronizados con la BS.

2.4.5.4.7.2 Ajuste

Este proceso se realiza durante dos fases de operación: la registración y la sincronización.
Durante el registro, una nueva estación se registra usando el canal de acceso aleatorio, si es exitoso, pasa al proceso de ajuste bajo el control de la BS, este proceso es cíclico, y consiste en el envió de parámetros hasta que la estación acepte los criterios propuestos.

Durante un nuevo registro se debe realizar el mismo proceso.

2.4.5.4.7.3 Control de Potencia

El algoritmo de control de potencia debe ser capaz de soportar variaciones de 30 dB/s.

2.4.5.4.8 Requerimientos de Transmisión

2.4.5.4.8.1 Control de Nivel de Potencia de Transmisión

El transmisor debe ser capaz de soportar un control de nivel de potencia de 45 dB y para bandas sin licencia de 30 dB.

2.4.5.4.8.2 Error de Constelación para el Transmisor

Tipo de Ráfaga	Error de Constelación Relativo (dB)
QPSK-1/2	16.4
QPSK-3/4	18.2
16 QAM-1/2	23.4
16 QAM-3/4	25.2
64 QAM-2/3	29.7
64 QAM-3/4	31.4

Tabla 2.65. Error de Constelación Permitido[130]

2.4.5.4.9 Requerimientos de Receptor

2.4.5.4.9.1 Sensibilidad de Recepción

En el receptor WiMAX debemos tener un BER de 10E-6 o menor para que cumpla con los requerimientos deseados, esto se mide en el conector de la antena.

2.4.5.4.9.2 Señal de Entrada Máxima de Receptor

La señal de recepción máxima debe ser de -30dBm y debe tolerar 0 dBm sin daño en sus componentes.

[130] IEEE 802.16, Institute of Electrical and Electronics Engineers, Pág. 626.

CAPITULO III

DISEÑO DE LA RED

3.1 DISEÑO PARA EDIFICIOS

3.1.1 Descripción del Edificio

En el presente capitulo nos enfocaremos en los diseños base que nos permitirán realizar el análisis de desempeño de la red así como los elementos necesarios, los cuales serán tomados en cuenta al momento del análisis económico.

Debido a la gran variedad de ambientes habitacionales, es preciso limitar los ambientes en los cuales se trabajará, es decir que si bien es cierto nos referiremos a un edificio de departamentos, debemos especificar tanto los pisos como el numero de departamentos por cada piso.

3.1.1.1 Descripción Física

En la presente sección especificaremos las dimensiones físicas más importantes que tendrán los edificios que usaremos como referencia para los diseños de última milla con las tecnologías Ethernet, xDSL y WiFi.

Comenzaremos por citar el número de pisos que posee nuestro edificio, el cual será de 5 pisos más una planta baja, esta cantidad de pisos se adapta a la realidad habitacional de nuestro país, en el cual los constructores emprenden edificios de departamentos entre 5 a 8 niveles incluyendo la planta baja.

Otro punto a tomar en consideración es la cantidad de departamentos por cada piso, en nuestro caso nos hemos decidido por tomar un departamento por cada piso, es decir que

hablamos de 5 o 6 departamentos por cada edificio; este número de departamentos por edificio se explicará más adelante.

Finalmente luego de un estudio de planos y visitas a edificios dentro de los límites urbanos de la ciudad, se ha determinado que la altura entre pisos es de 3 metros y los departamentos cuentan con áreas de construcción de unos 120 metros cuadrados.

3.1.1.2 Descripción Humana

En este punto del presente capitulo revisaremos aspectos concernientes a la cantidad de habitantes del edificio y su justificación.

Se había mencionado que cada piso contará con un solo departamento, lo cual limita nuestro edificio a tener entre 5 o 6 familias, este límite de familias es fundamental a la hora de planificar la incursión o no de un proyecto de dotación de servicios de Internet.

Debido a circunstancias sociológicas, al tener un gran número de familias por edificio se vuelve más difícil llegar a un consenso al momento de tomar una decisión sobre uno u otro proveedor de servicios de Internet, en nuestro caso se busca entregar servicio a todas las familias o a casi todas, es decir tomar la posición del proveedor incumbente o el único dentro del edificio.

Estos obstáculos de carácter humano nos obliga a enfocarnos en un número de familias menor, sin embargo esto no implica que se pueda realizar implementaciones en edificios más grandes, la diferencia es que el número de familias cliente muy probablemente se acerque a los número estimados en nuestro edificio referencial.

3.1.2 Requerimientos Básicos

Un ISP que desee entrar al mercado residencial, debe tener en cuenta ciertas pautas a la hora de brindar sus servicios dentro de un edificio de departamentos, entre ellas están las siguientes:

- ✓ Seguridad de la red.
- ✓ Privacidad entre los usuarios
- ✓ Transparencia de la tecnología.

La seguridad en la red es un parámetro que debe ser tomado en cuenta, especialmente al trabajar con las tecnologías inalámbricas como WiFi, ya que su naturaleza las vuelve más propensas a brechas en la seguridad; por otro lado las tecnologías cableadas no presentan mayor problema a la hora de la seguridad.

El parámetro de la privacidad entre usuarios es un tema que debe ser tomado con la mayor delicadeza por parte del ISP, ya que no se debe tener un ambiente en el cual la privacidad de los usuarios se vea comprometida, especialmente al trabajar con diseños híbridos de ultima milla, los cuales debido a las diferencias de las tecnologías pueden dejar expuestos a los clientes.

Finalmente, la transparencia de la tecnología para con el usuario es un parámetro que debe ser tomado en cuenta al momento de sopesar la eficiencia de las tecnologías, ya que no se desea tener problemas con el cliente debido a falta de familiaridad o simplicidad de una u otra opción.

3.1.3 Diseño Ethernet

Tal como se mencionó anteriormente, los diseños en los cuales la tecnología Ethernet esté presente son diseños híbridos de última milla, es decir que desde el ISP saldremos mediante una WLAN usando radios de última milla y el último tramo hasta el cliente se realizará utilizando Ethernet y valiéndonos de las normas de cableado de la ANSI/TIA/EIA 568B.

Dentro del diseño Ethernet debemos distinguir dos partes esenciales, la primera tiene relación con los elementos pasivos de la red, como son el cableado y sus componentes, y como segunda parte los elementos activos de la red que son los equipos de conexión.

3.1.3.1 Primer Tramo

En la primera parte de la última milla, debido a la característica del presente estudio de enfocarnos en ambientes residenciales y su dispersión dentro de un ambiente metropolitano, la mejor solución tanto tecnológica como económica es utilizar enlaces de radio desde el ISP hasta los predios de las unidades habitacionales, dichos enlaces se realizan con equipos de última milla basándonos en sistemas punto multipunto o PMP, debido a que estos equipos deben soportar un ambiente altamente congestionado y de

interferencias, se ha decido por utilizar equipos de espectro ensanchado, cuya naturaleza le permite soportar altos niveles de interferencia y garantizar la seguridad de la información.

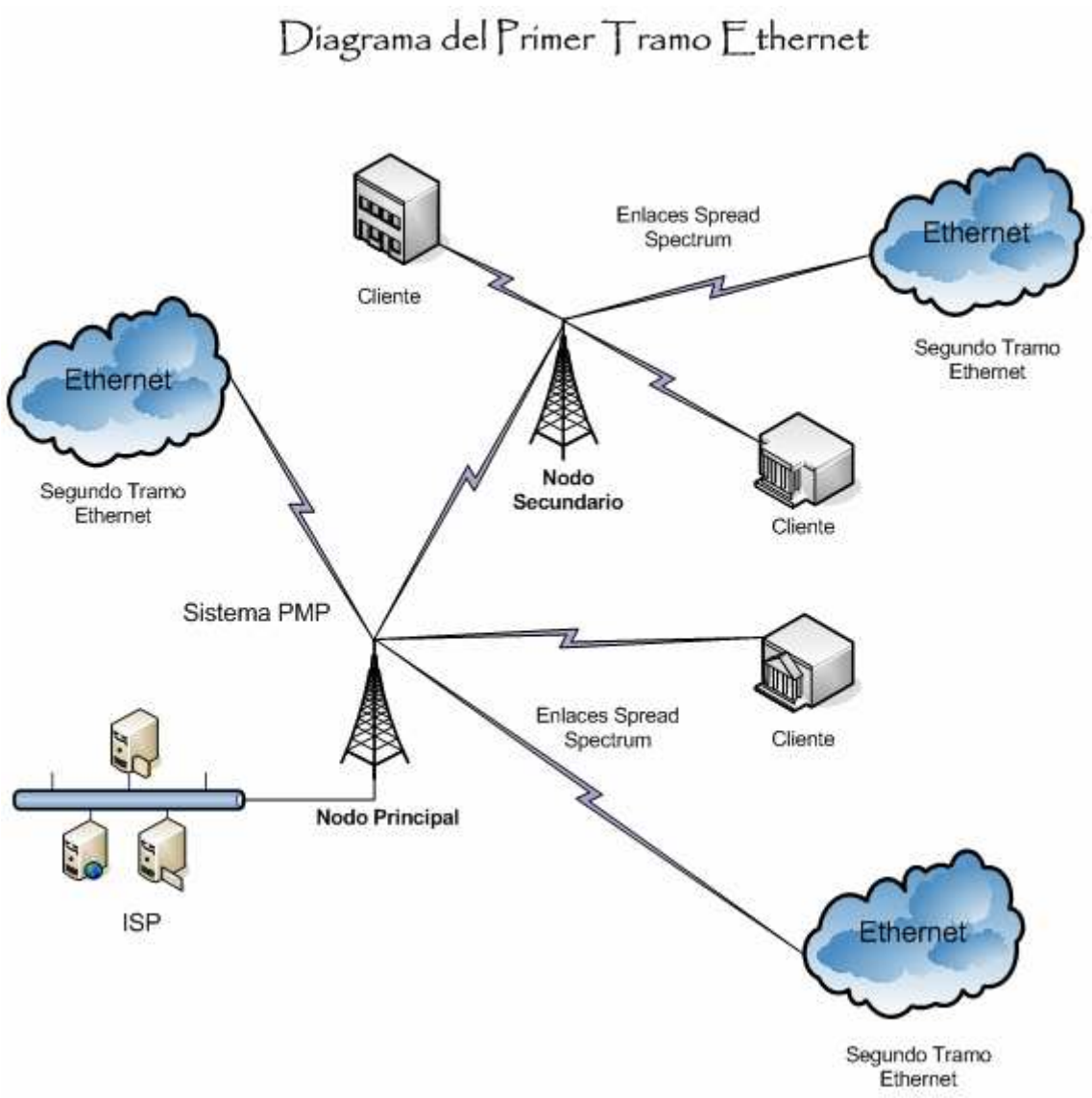


Figura 3.1 . Diagrama del Primer Tramo Ethernet

Dentro de este esquema se puede apreciar claramente que los enlaces inalámbricos llegan a las inmediaciones de las zonas residenciales, a partir de estas se continua mediante la tecnología Ethernet, ya sea basándonos en cobre o fibra óptica detallado más adelante.

En sistema de radio que se usa responde al esquema punto multipunto, y podemos encontrar nodos secundarios, clientes empresariales fuera de nuestro estudio y los clientes residenciales.

Estos enlaces se realizan con equipos de espectro ensanchado, usando espectro ensanchado de secuencia directa o DSSS; las bandas de frecuencia a ser usadas corresponden a 5.8 GHz o 900 MHz ya que son bandas libres y sin licencia dentro de nuestro territorio.

3.1.3.2 Segundo Tramo

Una vez que el primer tramo se ha completado podemos pasar al planeamiento del segundo tramo, este consiste en la implementación de un sistema Ethernet, es decir que debemos diseñar una red basada en la tecnología Ethernet y para ellos debemos usar las normas de cableado ANSI/TIA/EIA 568B.

En el planeamiento de este diseño se debe considerar los elementos activos y los pasivos, dentro de los pasivos nos referimos al cableado y todos sus componentes, mientras que en la parte activa nos encargaremos de los equipos que completaran nuestra infraestructura.

La parte pasiva de nuestro diseño se realiza de acuerdo a las nuevas normativas de cableado estructurado, en las cuales se puede optar por construir solo un MDF o cuarto de equipos central sin pasar por los HC o cuartos de distribución horizontal, dando como resultado que solo se tenga un cableado vertical.

Esta forma de planificar en diseño del cableado estructurado se facilita mediante los nuevos usos de los cables de par trenzado CAT. 5e y 6, así como de la fibra óptica, es decir son capaces de soportar Gigabit Ethernet.

La consideración más importante para tomar esta decisión en el cableado estructurado es que la privacidad, ya que cada departamento tendrá un tramo de fibra o par trenzado directo hasta el MDF, evitando que la información de uno u otro cliente sea enviada mediante un medio compartido dentro de las inmediaciones.

Es preciso mencionar que la administración de los anchos de banda de los clientes se realizará en este tramo, al tener un cableado centralizado se garantiza que se pueda gestionar los anchos de banda de forma independiente para cada cliente, ya que no debemos pasar por equipos o tramos compartidos.

Debido a que las distancias tanto verticales como horizontales para nuestro edificio tipo están dentro de los 90 m., y sobre cables de par trenzado tanto en categorías 5e como 6 se logran tener velocidades de 1000 Mbps se ha decido no usar fibra óptica sino cable categoría 5e.

El uso de par trenzado mejorará los tiempos de instalación sobre una instalación de fibra óptica, sin mencionar que no es necesario invertir en capacitaciones de personal en caso de no tener personal familiarizado con la instalación de fibra óptica.

Sin embargo, el uso de fibra óptica debe ser tomado en cuenta como solución en caso de tener distancias mayores a los 90 m. como única solución, ya que no se puede afrontar una configuración de cableado diferente, la fibra óptica recomendada es 62.5/125 µm. con conectores SC.

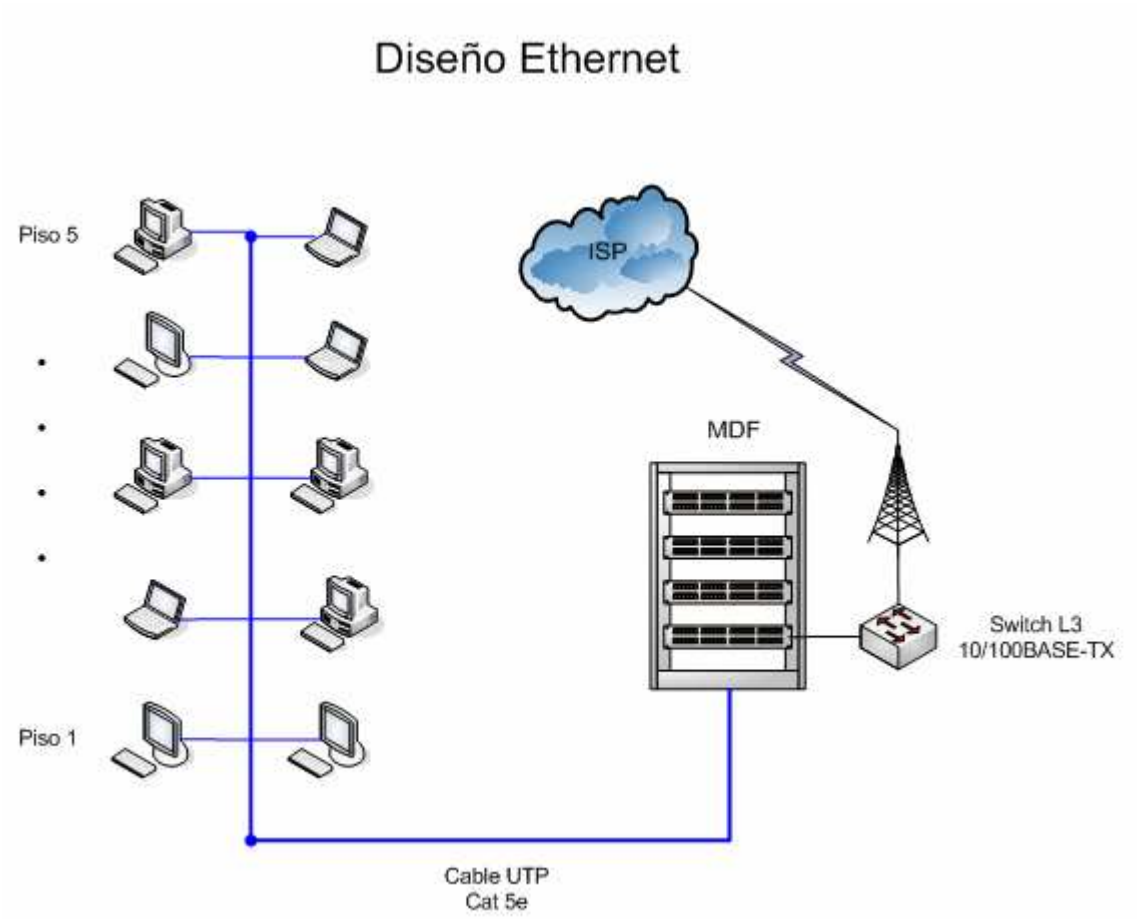


Figura 3.2 . Diseño Ethernet para Edificios

La parte activa de nuestro tramo Ethernet se verá caracterizada por un equipo de altas prestaciones, en nuestro caso es un switch de capa 3, administrable, y capaz de brindar QoS.

Este equipo nos permitirá gracias a poseer prestaciones de capa 3 la omisión de un router y transparencia al momento de la asignación de las direcciones IP del cliente, ya que se deben entregar a los mismos direcciones validas en caso de que deseen correr aplicaciones que así lo necesiten.

Gracias a las características de administración nos es factible separar cada una de las interfases en VLAN's independientes, que junto a la disposición del cableado asegura la privacidad de cada cliente como la seguridad.

Finalmente la característica de soportar parámetros de QoS y en especial uno de estos que es brindar limitaciones de ancho de banda, completa los requerimientos necesarios para ofrecer a cada cliente la flexibilidad y seguridad que necesita.

Cabe destacar que el diseño mostrado no tiene como fin el de dotar de una red LAN al edificio sino de ser parte del medio de acceso a los servicios de Internet que ofrece un ISP.

Debido a que el switch de capa 3 es uno de los parámetros más importantes dentro de nuestro diseño, y su funcionamiento determina gran parte del éxito de esta tecnología sobre el resto de opciones, se llevaron a cabo algunas pruebas con un switch de marca Huawey y modelo S3928P.

3.1.4 Diseño xDSL

Para el diseño en edificios donde se use la tecnología xDSL al igual que para Ethernet se presentan últimas millas híbridas, es decir que desde el ISP saldremos mediante una WLAN usando radios de última milla y el último tramo hasta el cliente se realizará utilizando equipos xDSL, compuestos por DSLAM y módems, además de utilizar las instalaciones de planta interna del edificio.

Dentro del diseño xDSL debemos tomar en cuenta cual de las distintas variantes en la tecnología deseamos usar, en nuestro caso la tecnología ADSL es la que responde a las necesidades planteadas.

3.1.4.1 Primer Tramo

En la primera parte de la última milla, debido a la característica del presente estudio de enfocarnos en ambientes residenciales y su dispersión dentro de un ambiente metropolitano, la mejor solución tanto tecnológica como económica es utilizar enlaces de radio desde el ISP hasta los predios de las unidades habitacionales, ya que las necesidades son similares a las vistas en Ethernet, este tramo es similar al previamente tratado.

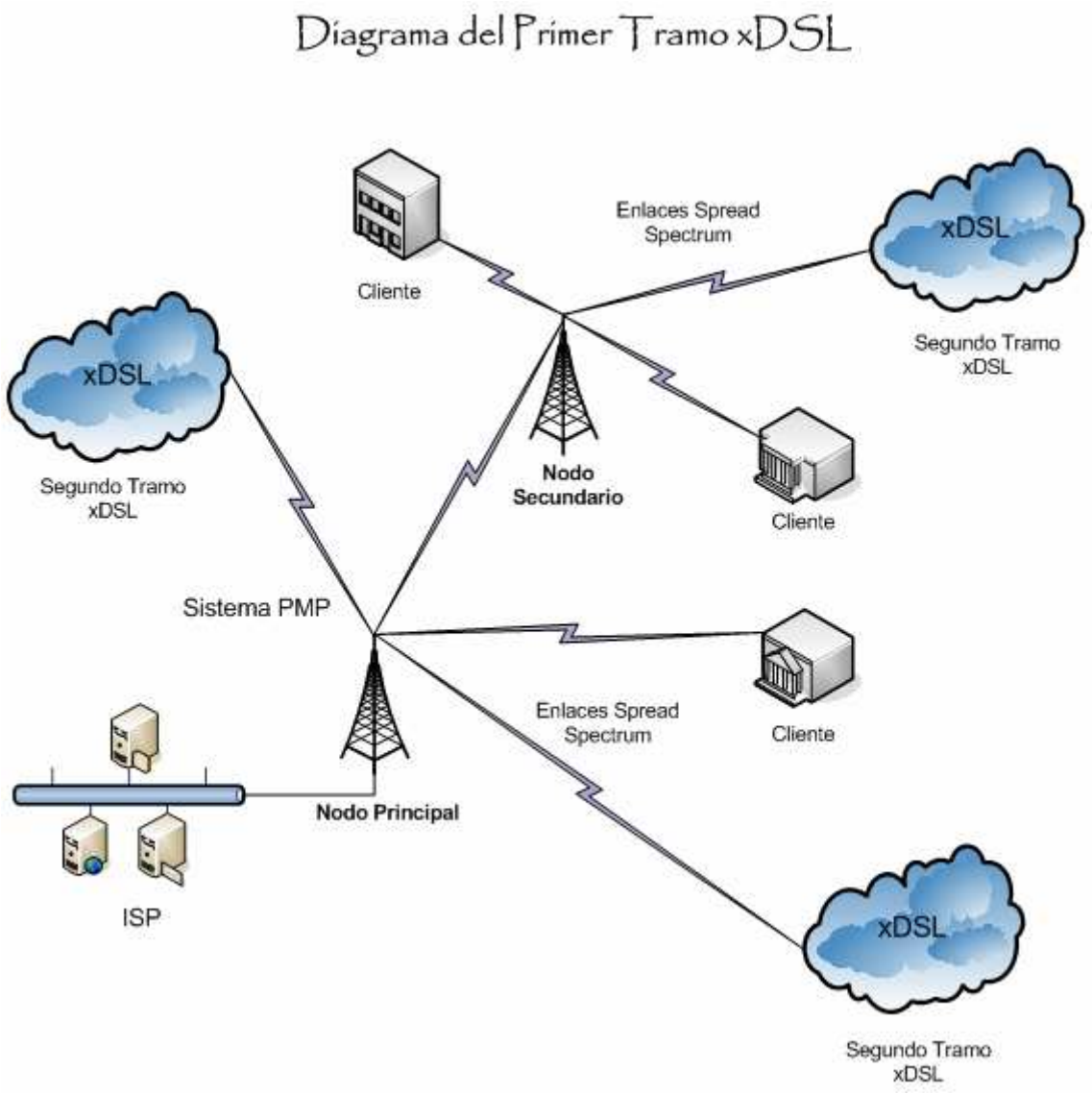


Figura 3.3 . Diagrama del Primer Tramo xDSL

Dentro de este esquema se puede apreciar claramente que los enlaces inalámbricos llegan a las inmediaciones de las zonas residenciales, a partir de estas se continúa mediante la tecnología ADSL, o se puede tener una convergencia de tecnologías.

3.1.4.2 Segundo Tramo

El segundo tramo consiste en la implementación de un sistema ADSL, es decir que debemos diseñar una red basada en la tecnología ADSL, valiéndonos de las instalaciones de planta interna propiedad del edificio.

Debido a que en este caso los elementos pasivos esta conformados por los pares telefónicos y el armario de distribución, solo se requiere de pequeñas modificaciones a las mismas para poder tener conectividad entre equipos sobre la infraestructura existente.

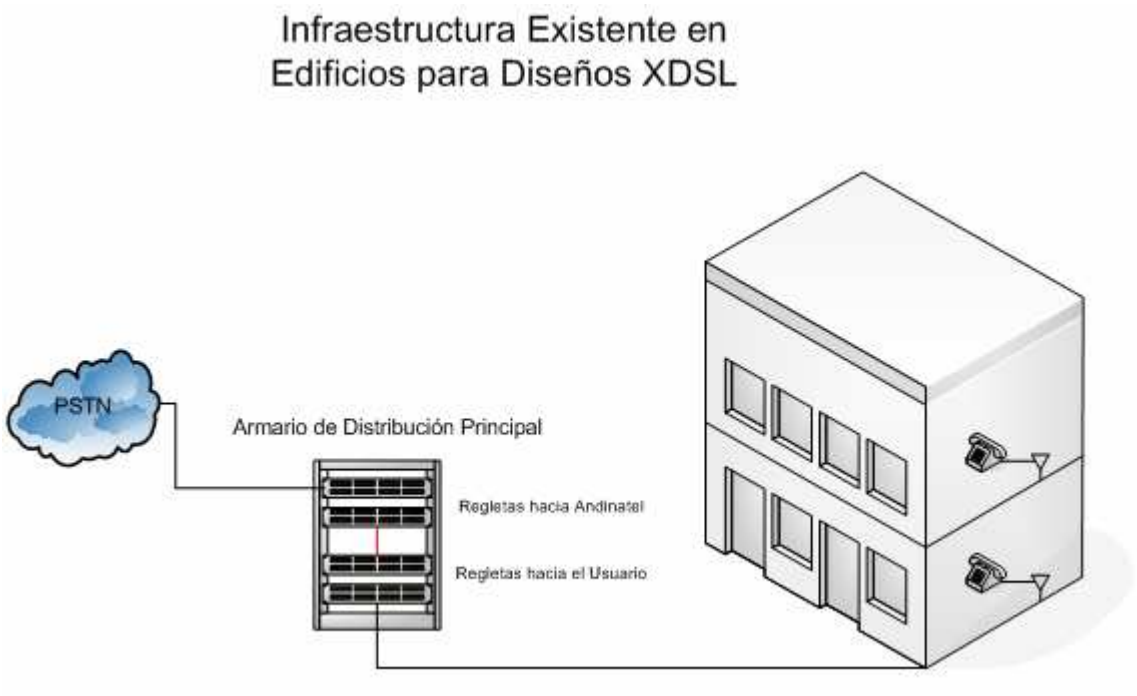


Figura 3.4. Infraestructura Existente en Edificios para Diseños xDSL

La infraestructura que posee todo edificio en planta interna es el cableado telefónico a cada uno de los departamentos mediante multipar telefónico, generalmente categoría 3, los cuales parten del armario de distribución principal.

En el armario de distribución principal se diferencian dos grupos de regletas telefónicas, las que se dirigen en dirección del usuario y las que se dirigen en dirección al operador telefónico y su red PSTN, que en nuestro caso es Andinatel.

Como primer paso se debe montar un segundo armario, el cual nos servirá para montar los equipos ADSL y un nuevo grupo de regletas telefónicas, estas regletas servirán como un ‘espejo’ de las regletas existentes en el armario de distribución; dicho montaje nos ayuda para separar a los clientes que deseen tomar el servicio de aquellos que no lo deseen o ya tengan un servicio xDSL en funcionamiento.

Al separar los clientes garantizamos un seguimiento de nuestros clientes para poder determinar fallas, ya sea de parte de los equipos o del servicio telefónico; no intervenimos de manera invasiva en el armario principal evitando posibles confrontaciones con el operador de servicio telefónico; no interrumpimos el servicio telefónico a usuarios ajenos; y, las reparaciones se facilitan.

La creación del armario espejo nos permitirá manejar fallas previstas o no y en caso de suspensión del servicio por parte de algún cliente, el regreso a la infraestructura inicial se logra en pocos minutos.

Dentro de este armario espejo se deben tener tomas eléctricas y ventilaciones necesarias ya albergarán equipos ADSL, en nuestro caso la unidad terminal ADSL central o ATU-C mejor conocida como DSLAM.

Las distancias entre los equipos centrales y los equipos de usuario o módems son de hasta 6 Km., distancia que nos permite cubrir con facilidad nuestro edificio base e inclusive edificios más altos. Finalmente en el extremo del usuario se debe instalar un splitter el cual se encargará de separar las señales de los equipos ADSL de las señales telefónicas.

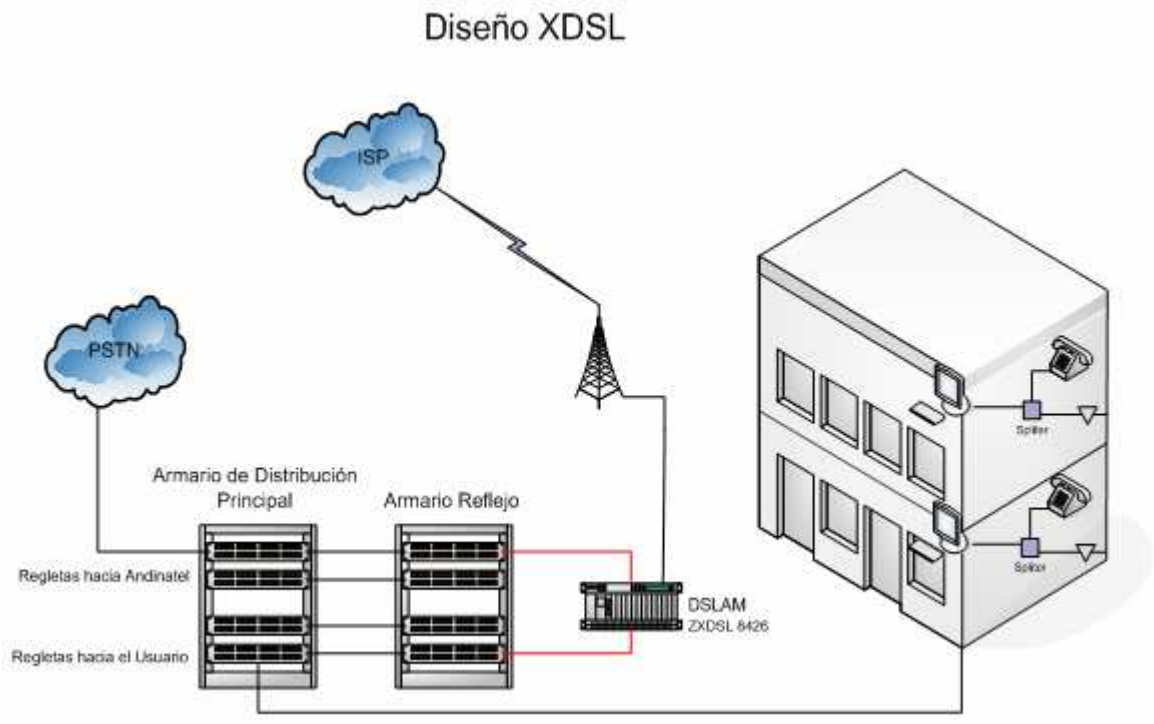


Figura 3.5. Diseño xDSL para Edificios

La parte activa en nuestro diseño xDSL esta compuesta de los equipos centrales y de usuario, es decir el DSLAM y los módems, las características que estos equipos deben tener son descritas a continuación: deben cumplir con las normas g.dmt y g.lite, deben ser capaces de soportar trafico IP, tener características de capa 3 o superiores y brindar QoS.

Las normas g.dmt y g.lite describen el modo de operación para ADSL y SADSL, de las cuales nos interesa el modo de funcionamiento con o sin un splitter, esta característica nos permitirá resolver problemas relacionados con sistemas de alarmas o redes de telefónicas internas en las cuales el uso del splitter puede causar interferencia.

Generalmente los equipos xDSL están construidos bajo características de operación ATM, en nuestro caso no es relevante este medio de transmisión sino que pueda operar bajo premisas IP, esto además le brinda al cliente transparencia.

Al ser equipos de capa 3 o superior no permite simplificar el número de equipos necesarios, ya que el uso de un router no es necesario y se puede separar a cada usuario en VLAN´s independientes por puerto, asegurando la privacidad de los usuarios.

Finalmente la característica de soportar parámetros de QoS y en especial brindar limitaciones de tráfico, completa los requerimientos necesarios para ofrecer a cada cliente la flexibilidad y seguridad.

El equipo que se ha tomado en cuenta para el diseño xDSL para equipos de terminales centrales es el ZXDSL 8426 de la marca ZTE, nos ofrece una gran flexibilidad, expansión y administración; mientras que para los usuarios, su complemento el ZXDSL 831 A, un modem con características avanzadas.

3.1.5 Diseño WiFi

Al igual que para Ethernet o xDSL, los diseños WiFi son diseños híbridos de última milla, es decir que desde el ISP saldremos mediante una WLAN usando radios de última milla y el último tramo hasta el cliente se realizará utilizando WiFi.

Para este diseño es necesario además de tener equipamiento WiFi para el segundo tramo, usar ciertas normativas de cableado para poder desplegar de manera eficiente nuestra red WiFi.

3.1.5.1 Primer Tramo

Este tramo inicial en el diseño WiFi es similar al ya presentado para las otras dos tecnologías, la consideración más importante para el sistema PMP es que su operación no presente interferencia con los puntos de acceso, es decir buscar puntos de acceso que no utilicen la misma banda de frecuencias.

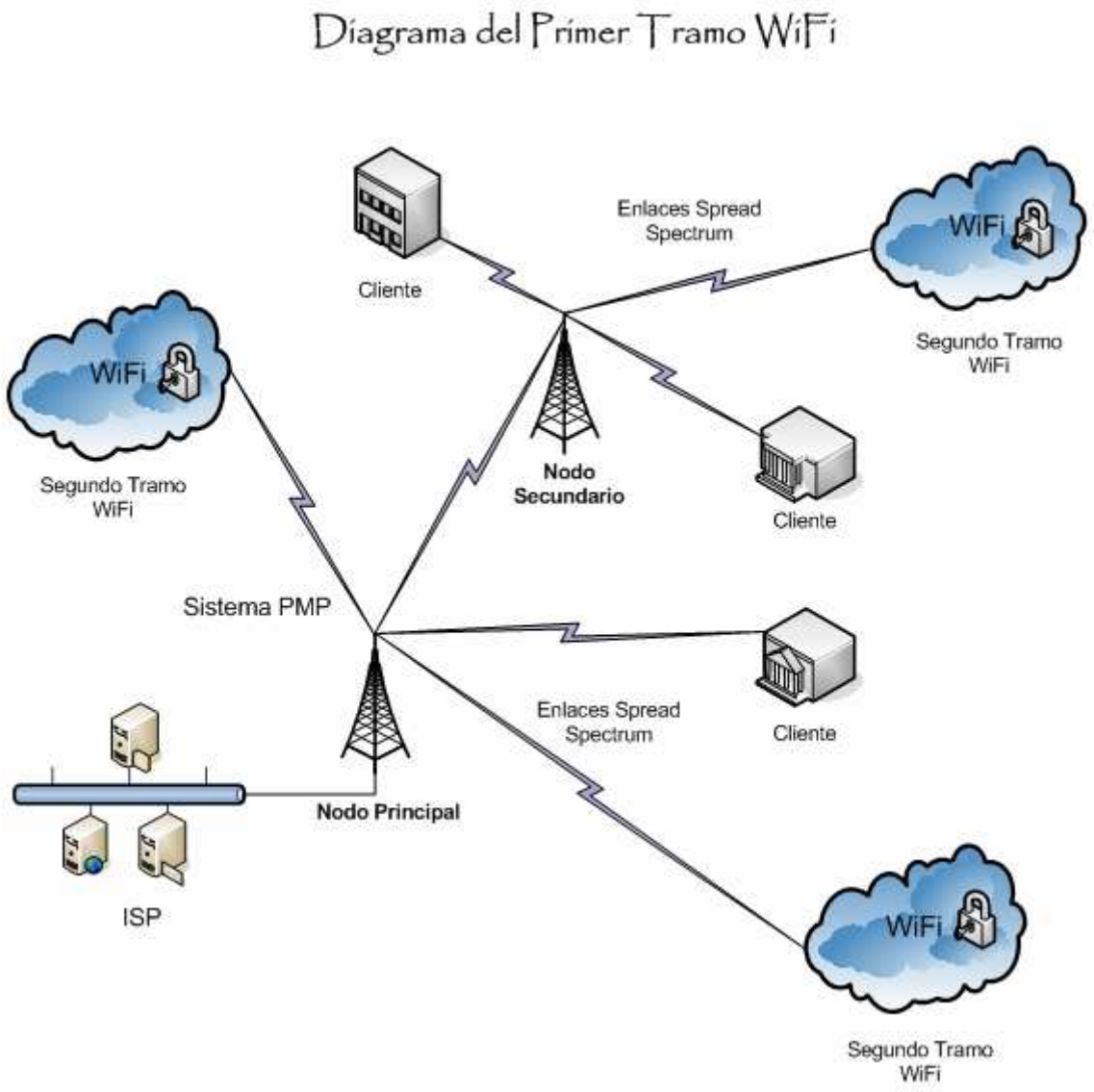


Figura 3.6. Diagrama del Primer Tramo WiFi

Dentro de este esquema se puede apreciar claramente que los enlaces inalámbricos llegan a las inmediaciones de las zonas residenciales, a partir de estas se continúa mediante la tecnología WiFi; cabe destacar que toda las redes WiFi deben tener seguridades por llave, caso contrario pasarían a ser un hotspot público.

Estos enlaces se realizan con equipos de espectro ensanchado, usando espectro ensanchado de secuencia directa o DSSS; las bandas de frecuencia a ser usadas corresponden a 5.8 GHz o 900 MHz ya que son bandas libres y sin licencia dentro de nuestro territorio.

3.1.5.2 Segundo Tramo

Una vez que el primer tramo se ha completado podemos pasar al planeamiento de la red WiFi, en primera instancia nos preocuparemos por el estándar soportado por los equipos 802.11, podemos escoger tanto equipos con normas a, b o g, sin embargo para evitar problemas con los radios de última milla la norma 802.11a que trabaja en frecuencias de 5 GHz debe ser descartada, gracias a mejoras en velocidad y compatibilidad la norma que mejores características presenta es la 802.11g, permitiendo velocidades de conexión de hasta 54 Mbps y compatibilidad con equipos 802.11b, sin tomar en cuenta que al trabajar en la banda de 2 GHz no existe problema con los equipos PMP.

Los equipos WiFi tienen un rango de acción de hasta 100 metros considerando espacios sin obstáculos, en una implementación real dicha área de cobertura se verá limitada dependiendo de la geografía y características de la zona propuesta.

Debido a que las redes WiFi fueron creadas como una extensión a las redes 802.3 o Ethernet, es de suponerse que sus interfaces cableadas sean Ethernet, lo que implica que se deben tomar en consideración algunos aspectos como las normas del cableado al igual que para las redes Ethernet antes revisadas.

La parte pasiva de nuestro diseño se realiza de acuerdo a las normas de cableado estructurado, se debe instalar par trenzado categoría 5e para poder tener la oportunidad de utilizar equipos que soporten potencia sobre Ethernet o PoE; se debe optar por construir solo un MDF.

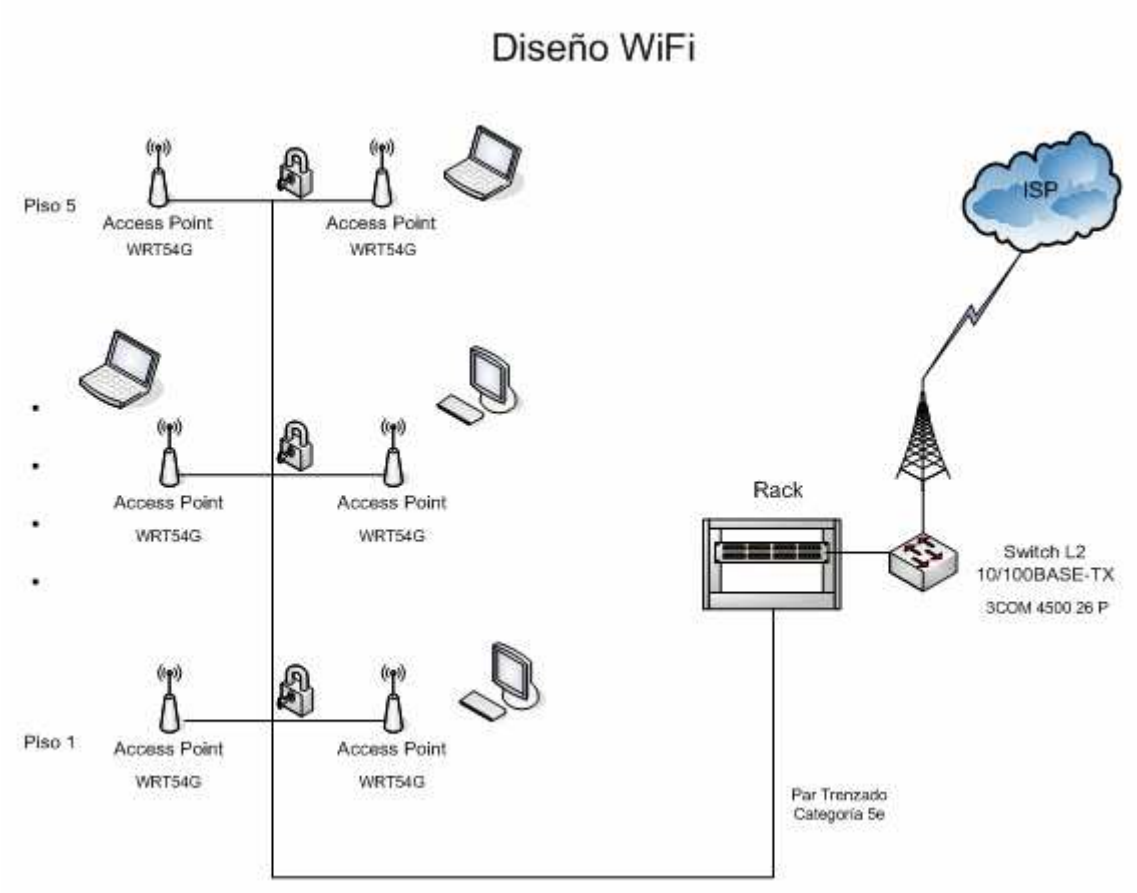


Figura 3.7. Diseño WiFi para Edificios

La parte activa de nuestro tramo WiFi esta compuesto por elementos tanto 802.3 como 802.11g, dentro de los elementos tendremos un switch de administrable capaz de soportar VLAN's, y los equipos inalámbricos deben ser todos access point de capa 3 al menos y que presten QoS a los clientes tanto en la parte inalámbrica como cableada y lo mas importante brindar acceso protegido WiFi o WPA como requerimiento mínimo de seguridad.

Juntos, el switch como los access point me permitirán reunir las características de seguridad, privacidad y transparencia para los clientes.

El switch seleccionado debe estar en capacidad de reemplazar el uso de un router permitiendo transparencia a la hora de la asignación de las direcciones IP; su capacidad de ser administrable me permite asignar a los equipos de un piso a una misma VLAN; mientras que su soporte QoS junto con el de los access point restringirán el trafico circulante por los equipos inalámbricos.

La selección de los equipos inalámbricos debe ser muy estricta, ya que el dejar una brecha en la seguridad pone en riesgo no solo al cliente sino que deja expuesto al ISP; la característica más relevante de los equipos WiFi debe ser su seguridad, deben ser capaces de brindar seguridades WPA, en vista que las seguridades WEP fueran declaradas obsoletas, este factor se vuelve el mas importante dentro de la implementación WiFi debido a que no se desea tener una red de acceso publico.

Los access point que se usaran deben ser capaces de realizar funciones de capa 3 para poder llevar un estricto control de usuarios y se complemente con las funciones brindadas por el switch principal; finalmente su capacidad de brindar QoS en la parte cableada restringirá el trafico que salga de estos equipos.

Los equipos WiFi que se usaran son de la marca Linksys, específicamente el modelo WRT54G, que cumple con todas las características inicialmente propuestas; mientras que el switch será de la marca 3COM de la familia 4500 26 P.

3.1.5.2.1 Diseño de la Cobertura

Una vez que se han decidido los equipos que entraran en funcionamiento, se debe considerar un aspecto importante dentro del diseño de una red inalámbrica, este es el diseño de la cobertura.

Como se menciono anteriormente los equipos WiFi funcionan en un rango de 100 metros sin obstáculos, pero al entrar en ambientes con paredes el área de cobertura de los equipos disminuye, esto significa que para cubrir cierta área se requieran mas de un equipo, esto impacta severamente en la cantidad de recursos que se debe usar para poder brindar una red inalámbrica.

Los equipos 802.11g trabajan con un nivel de hasta -75 dBm, cualquier señal más baja será tomada como interferencia y se perderá la conexión, por lo que se deben tener niveles de señal superiores a este para que exista una cobertura.

Para poder tener calcular de manera más eficiente la cantidad de equipos que se requerirán, utilizaremos un programa que nos ayuda con el planeamiento de las áreas de cobertura, este programa es Ekahau.

Ekahau es una combinación de un site survey con una herramienta de planeación, su funcionamiento es simple, se debe ingresar un mapa del área que se desea dotar de servicio, se realiza un survey inicial, es decir se debe instalar un equipo WiFi y mediante el survey el programa advertirá la propagación real del medio ambiente, finalmente nos muestra un los mejores sitios y la cobertura que tendrá.

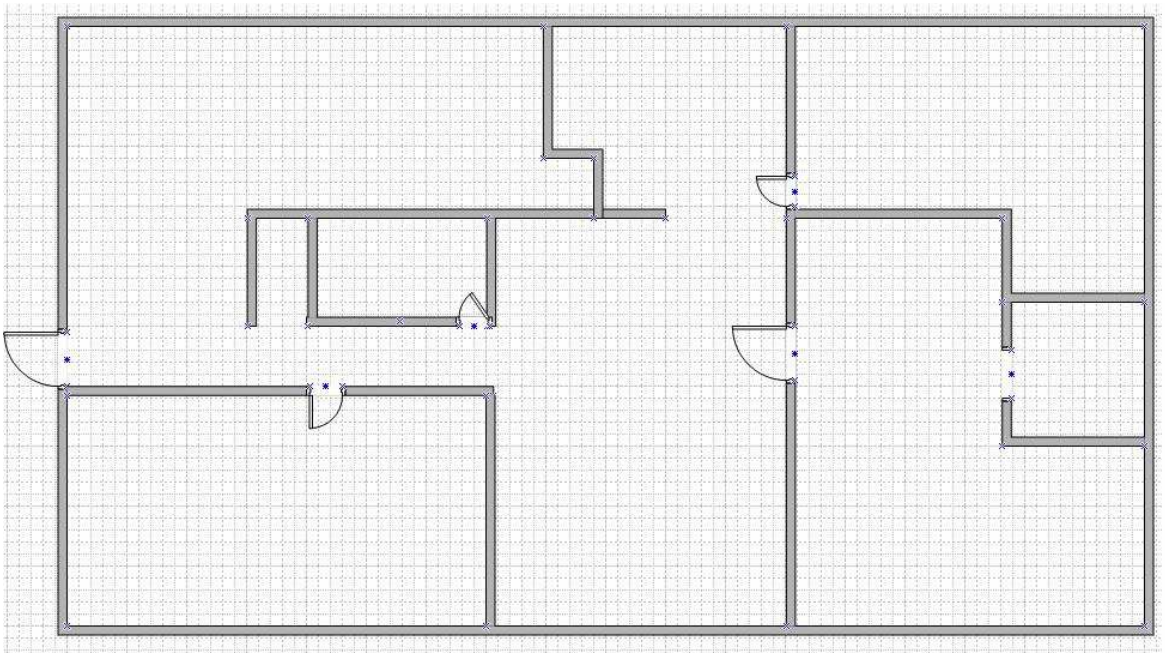


Figura 3.8. Plano de un Piso del Edificio Base

La figura anterior nos muestra el plano de un piso, el cual será insertado al programa de planificación, una vez insertado se realiza el survey, nosotros mientras nos movemos marcamos la trayectoria sobre el mapa, el programa nos muestra el nivel de señal una vez terminado el survey.

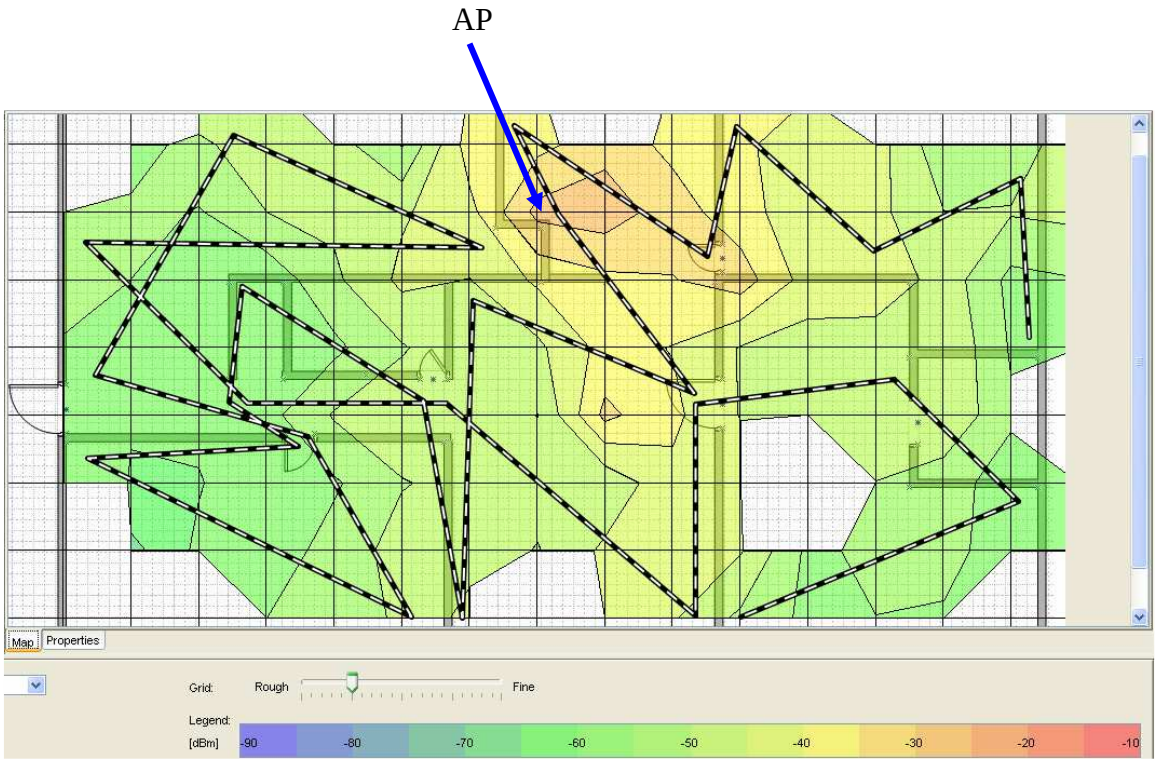


Figura 3.9. Niveles de Señal Obtenidos del Survey

En la figura anterior se puede observar los caminos ingresados con líneas blancas y negras y los niveles de señal sobre el plano con diferentes colores, próxima a la ubicación del access point se obtuvo mayor cantidad de señal, según la escala en las esquinas inferiores se tiene coberturas malas y posibles áreas sin cobertura.

Una vez que se tiene los patrones de radiación, el programa nos ofrece la posibilidad de mostrarnos los mejores lugares para ubicar los puntos de acceso y si se necesitan más de uno.

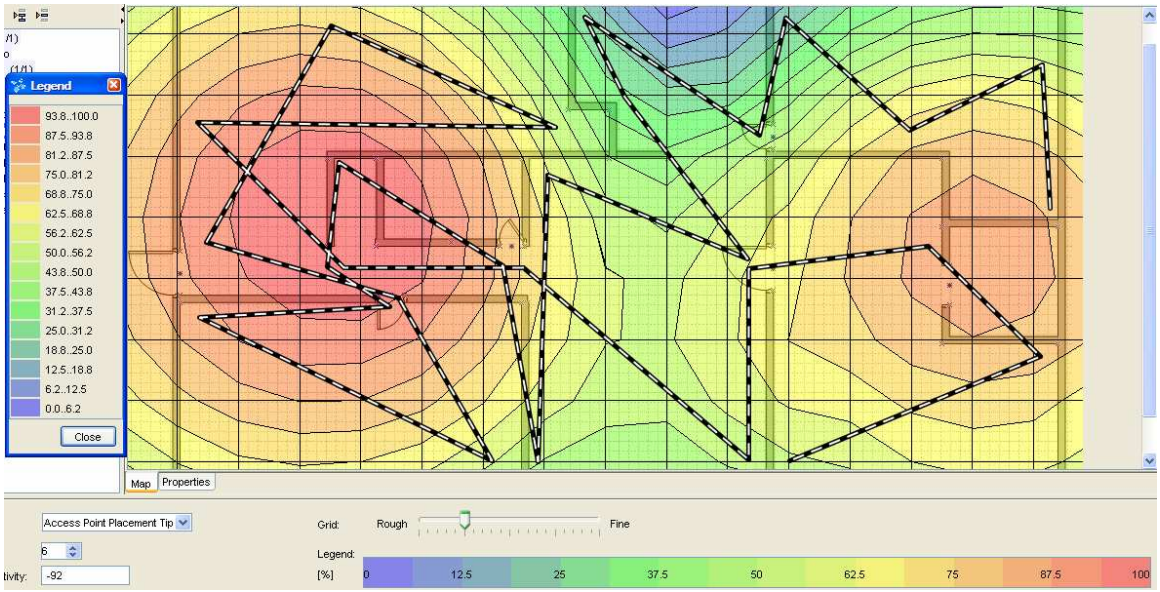


Figura 3.10. Ayuda de Ubicación de Puntos de Acceso

Basado en la cobertura obtenida, el programa nos muestra la mejor ubicación para los access point y el nivel de cobertura en porcentaje, nos muestra dos access point en los extremos del plano y el nivel de cobertura mejora en todas las zonas, de lo que se puede determinar que se necesitaran dos puntos de acceso por cada piso de nuestro edificio base.

3.2 DISEÑO PARA CONJUNTOS HABITACIONALES

3.2.1 Descripción del Conjunto Habitacional

Siguiendo con los diseños base para clientes residenciales, el segundo ambiente en ser estudiado es el conjunto habitacional, los conjuntos habitacionales probaran tener nuevos enfoques y los elementos necesarios sufrirán varios cambios, los cuales serán tomados en cuenta al momento del análisis económico.

Debido a la gran variedad de ambientes habitacionales, es preciso limitar las posibles variables, debemos especificar tanto áreas como el numero de unidades habitacionales.

3.2.1.1 Descripción Física

En la presente sección especificaremos las dimensiones físicas más importantes que tendrá el conjunto habitacional base que usaremos como referencia para los diseños de última milla con las tecnologías Ethernet, xDSL y WiFi.

Comenzaremos por citar el número de unidades habitacionales que posee nuestro conjunto, el cual será de 22, esta cifra sugiere un conjunto de tamaño moderado sin ser pequeño, a su vez este número de casas asegura que las instalaciones dejadas por el constructor sean las necesarias para tener accesos apropiados tales como ductos y plantas internas telefónicas, etc.

Otro punto a tomar en consideración es la distribución interna del conjunto habitacional, es decir sus casas están juntas o se encuentran con separaciones tanto de áreas verdes o de terrenos, para que el modelo se acerque mas a un estándar, supondremos que las casas poseen separación entre ellas y además de existen áreas verdes que en algunos casos se encuentran entre las viviendas.

Debido a estas características, es preciso dar el tamaño de un terreno promedio en vez de las dimensiones de la casa construida, así como medidas generales del conjunto; para el terreno tenemos 15 metros por 25, y el área comunal es de 960 metros cuadrados.

Para las viviendas se establecerá que el área de construcción promedio es de 180 metros cuadrados.

3.2.1.2 Descripción Humana

Al igual que para un edificio de departamentos, es necesario limitar el componente humano dentro de las inmediaciones, dichas limitaciones se revisaran en la presente sección del documento.

Se había establecido que se tendrían 22 unidades habitacionales dentro del conjunto residencial, limitaremos por consiguiente el numero de familias a 22, cabe destacar que este numero de familias es mucho mayor al establecido para edificios, por lo tanto no se espera que todos los residentes se acojan al servicio, sin embargo todos los diseños deben tener la flexibilidad necesaria para poder crecer.

Gracias a encuestas se ha determinado que se puede contar con un 50% de aceptación inicial por parte de los residentes, esto nos deja con 11 familias para los cálculos iniciales.

3.2.2 Requerimientos Básicos

Para una empresa proveedora de servicios de Internet en busca de captar mercados residenciales, debe tener cumplir con algunas pautas dentro de un conjunto residencial:

- ✓ Seguridad de la red.
- ✓ Privacidad entre los usuarios
- ✓ Transparencia de la tecnología.
- ✓ Escalabilidad de la red propuesta.

La seguridad en la red es un parámetro que debe ser tomado en cuenta, especialmente al trabajar con las tecnologías 802.11, ya que su naturaleza la vuelve propensa a brechas en la seguridad.

El parámetro de la privacidad entre usuarios debe manejado de forma eficiente, ya que no se debe tener una red de acceso que comprometa la privacidad entre los usuarios que acceden a los servicios mediante esta.

La transparencia de la tecnología para con el usuario es un parámetro que debe ser tomado en cuenta al momento de sopesar la eficiencia de las tecnologías, ya que no se desea tener problemas con el cliente debido a falta de familiaridad o complejidad de una u otra opción.

La escalabilidad es un nuevo parámetro que nace del mayor numero de clientes reunidos en un conjunto habitacional, si bien es cierto nuestro numero de clientes inicial es del 50%, no se debe descartar la posibilidad de captar una mayor cantidad de clientes.

3.2.3 Diseño Ethernet

Al igual que para edificios, los diseños que impliquen el uso de las tecnologías Ethernet, xDSL y WiFi son diseños híbridos de última milla, por lo tanto tendremos dos tramos, el primero inalámbrico y el segundo tramo que llega al cliente es Ethernet.

3.2.3.1 Primer Tramo

En la primera parte de la última milla, debido a la característica de dispersión de los conjuntos habitacionales dentro de un ambiente metropolitano, la mejor solución es utilizar enlaces de radio desde el ISP hasta los predios de las unidades habitacionales, estos enlaces son PMP, con espectro ensanchado, cuya naturaleza le permite soportar altos niveles de interferencia y garantizar la seguridad de la información.

A partir del enlace se continua mediante la tecnología Ethernet, ya sea basándonos en cobre o fibra óptica según las necesidades de la misma manera que se propuso para el diseño de edificios.

Estos enlaces se realizan con equipos de espectro ensanchado, usando espectro ensanchado de secuencia directa o DSSS; las bandas de frecuencia a ser usadas corresponden a 5.8 GHz o 900 MHz ya que son bandas libres y sin licencia dentro de nuestro territorio.

3.2.3.2 Segundo Tramo

El segundo tramo consiste en la implementación de un sistema Ethernet, es decir que debemos diseñar una red basada en la tecnología Ethernet y para ellos debemos usar las normas de cableado ANSI/TIA/EIA 568B.

En el planeamiento de este diseño se debe considerar los elementos activos y los pasivos; debido a las distancias que en este caso son mayores a los 100 metros, hemos propuesto dos diseños capaces de cumplir con las expectativas propuestas.

3.2.3.2.1 Primer Diseño Ethernet

Dentro de este diseño tenemos la división del conjunto habitacional en varios sectores, de tal forma de llegar con varias antenas al conjunto y construir la red de acceso con un cableado compuesto de cable UTP categoría 5e o 6, el propósito general de plantear esta solución es la de realizar implementaciones que permitan una expansión de acuerdo al numero de clientes.

Al sugerir que el cableado se realizara con cable UTP es de esperarse que cada antena y la red Ethernet inherente solo de acceso a un promedio de 6 casas dependiendo de las distancias que exista entre las viviendas.

La parte pasiva de nuestro diseño esta compuesta de un solo MDF, la existencia de este cuarto de equipos implica que el mismo se encuentre dentro de una casa o en un área de servicio comunal, de igual manera el primer tramo de la última milla llegara hasta una de estas inmediaciones.

Cabe destacarse que a cada vivienda se llegara con un punto de cableado, directo del MDF sin pasar por equipos intermedios. El uso de par trenzado mejorará los tiempos de instalación.

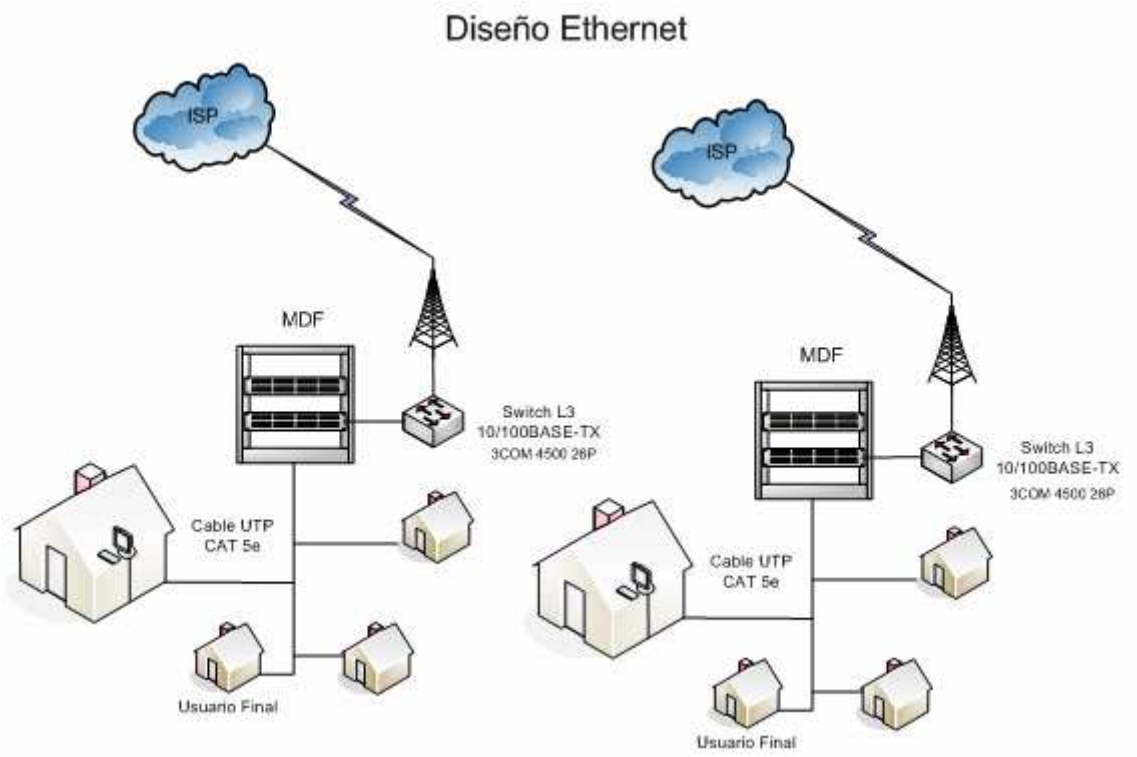


Figura 3.11. Primer Diseño Ethernet para Conjuntos Habitacionales

La parte activa de nuestro tramo Ethernet se verá caracterizada por un equipo de altas prestaciones, en nuestro caso es un switch de capa 3, administrable, y capaz de brindar QoS.

Al ser un equipo de capa 3 nos permite tener funciones básicas de ruteo y por consiguiente nos evita la utilización de un router.

Gracias a las características de administración nos es factible separar cada una de las interfases en VLAN's independientes, que junto a la disposición del cableado asegura la privacidad de cada cliente y su seguridad.

Finalmente al soportar parámetros de QoS y en especial su capacidad de limitaciones trafico, completa los requerimientos necesarios para ofrecer a cada cliente la flexibilidad y seguridad que necesita.

La escalabilidad de la red se ve cubierta por la decisión de utilizar más de una antena de última milla dentro del conjunto habitacional, ya que de esta manera cada vez que aparezcan nuevos clientes se puede habilitar una nueva zona.

El switch de capa 3 escogido para brindar las funciones necesarias es de la marca 3COM de la familia 4500 26 P.

3.2.3.2.2 Segundo Diseño Ethernet

Dentro de este diseño se tiene un solo acceso de primer tramo dentro del conjunto habitacional, por lo que el cableado ahora tendrá que cubrir la extensión completa del conjunto habitacional, por lo que se necesitara de cable UTP como fibra óptica.

Esta solución implica que se deben construir un MDF y varios IC para poder cubrir todo el conjunto habitacional, gracias al uso de fibra óptica las distancias entre el MDF y los IC pueden exceder fácilmente los 100 metros, para poder brindar la escalabilidad necesaria se deben construir los IC pese a la falta de clientes en la zona que dará servicio el IC.

De la misma manera que para nuestro primer diseño el MDF y los IC deben ubicarse en áreas comunales, y el primer tramo de la última milla llegara hasta la inmediación del MDF.

En este diseño, cada vivienda contara con un punto de cableado, sin embargo ahora se tendrá un medio sin compartido, para poder garantizar la privacidad de la red de acceso, los equipos de red activos deben ser cuidadosamente seleccionados.

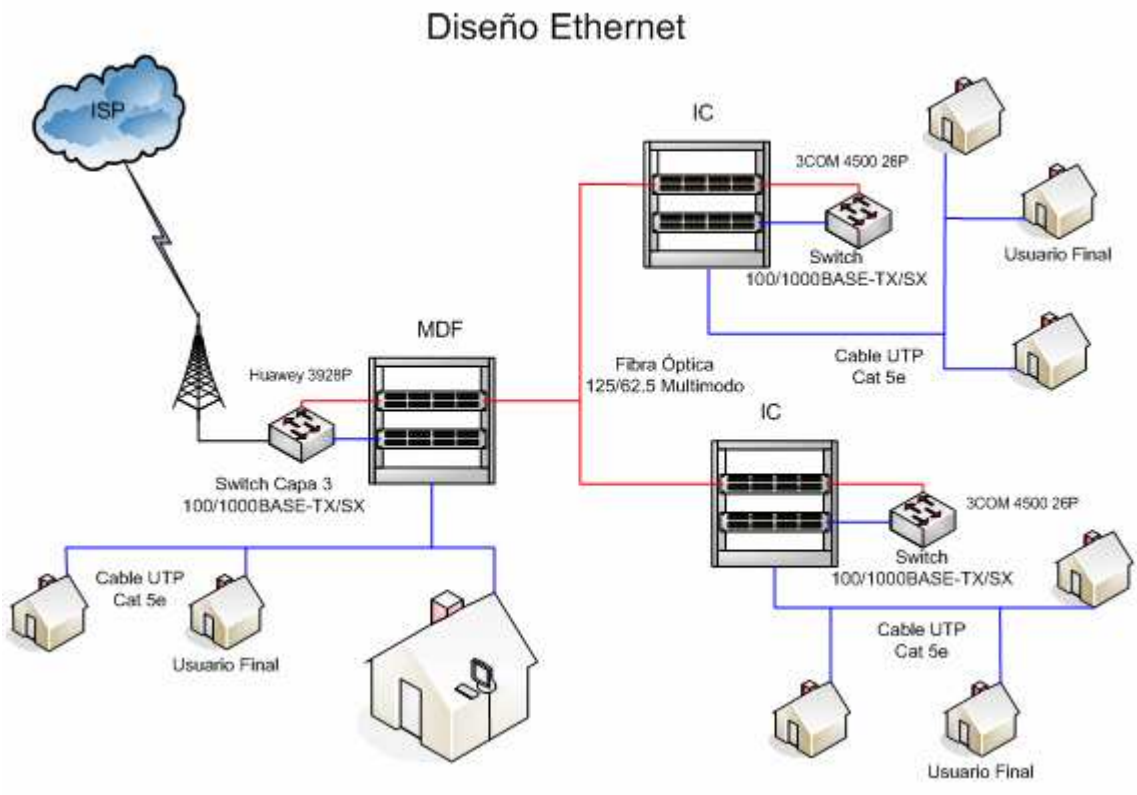


Figura 3.12. Segundo Diseño Ethernet para Conjuntos Habitacionales

La parte activa de nuestro tramo Ethernet esta compuesta de dos tipos diferentes de equipos, un equipo central para el MDF que debe tener características de capa 3 o superior, ofrecer QoS y soporte de VLAN's, mientras los equipos de IC deben ser de capa 2 o 3, ofrecer QoS y soporte de VLAN's; ambos tipos de equipos deben tener puertos de fibra óptica 1000 BASE SX.

El equipos de central es switch de capa 3 de altas prestaciones el cual nos facilitara el control y monitoreo de la red, sus habilidades de ruteo eliminan la presencia de un router, al ofrecer QoS podemos limitar el trafico de los clientes y asegurar la privacidad de los mismos gracias a la implementación de redes LAN virtuales por cada cliente; debido a que el MDF se enlazara como los IC mediante fibra óptica multimodo 62.5/125 los puertos 1000 BASE SX son indispensables para lograr dicha función.

Para los equipos que se encuentren en el IC, los requerimientos de capa tres son opcionales, sin embargo deben ofrecer QoS para poder limitar el tráfico de los clientes, la posibilidad de redes LAN virtuales nos permite evitar brechas en la privacidad de los clientes, la existencia de puertos de fibra óptica nos permite la conexión con el equipo central.

La escalabilidad de la red se ve cubierta por la decisión implementar los cuartos de interconexión a lo largo del conjunto habitacional, los que permitirán conectar a los clientes sin importar la distancia al MDF.

Los equipos que se escogieron son el switch Huawey 3928P para el MDF y equipos 3COM de la familia 4500 26 P mas su modulo de expansión 1000 BASE SX.

3.2.4 Diseño xDSL

Para el diseño xDSL de conjuntos residenciales, se presentan últimas millas híbridas, es decir que desde el ISP saldremos mediante una WLAN usando radios de última milla y el último tramo hasta el cliente se realizará utilizando equipos xDSL, compuestos por DSLAM y módems, además de utilizar las instalaciones de planta interna del conjunto.

Dentro del diseño xDSL debemos tomar en cuenta cual de las distintas variantes en la tecnología deseamos usar, en nuestro caso la tecnología ADSL es la que responde a las necesidades planteadas.

3.2.4.1 Primer Tramo

En la primera parte de la última milla, se utilizara enlaces de radio desde el ISP hasta los predios de las unidades habitacionales tal como se reviso para la tecnología xDSL para edificios, a partir de estas se continúa mediante la tecnología ADSL.

3.2.4.2 Segundo Tramo

El segundo tramo consiste en la implementación de un sistema ADSL, es decir que debemos diseñar una red basada en la tecnología ADSL, valiéndonos de las instalaciones de planta interna propiedad del conjunto.

Debido a que en este caso los elementos pasivos esta conformados por los pares telefónicos y el armario de distribución, solo se requiere de pequeñas modificaciones a las mismas para poder tener conectividad entre equipos sobre la infraestructura existente.

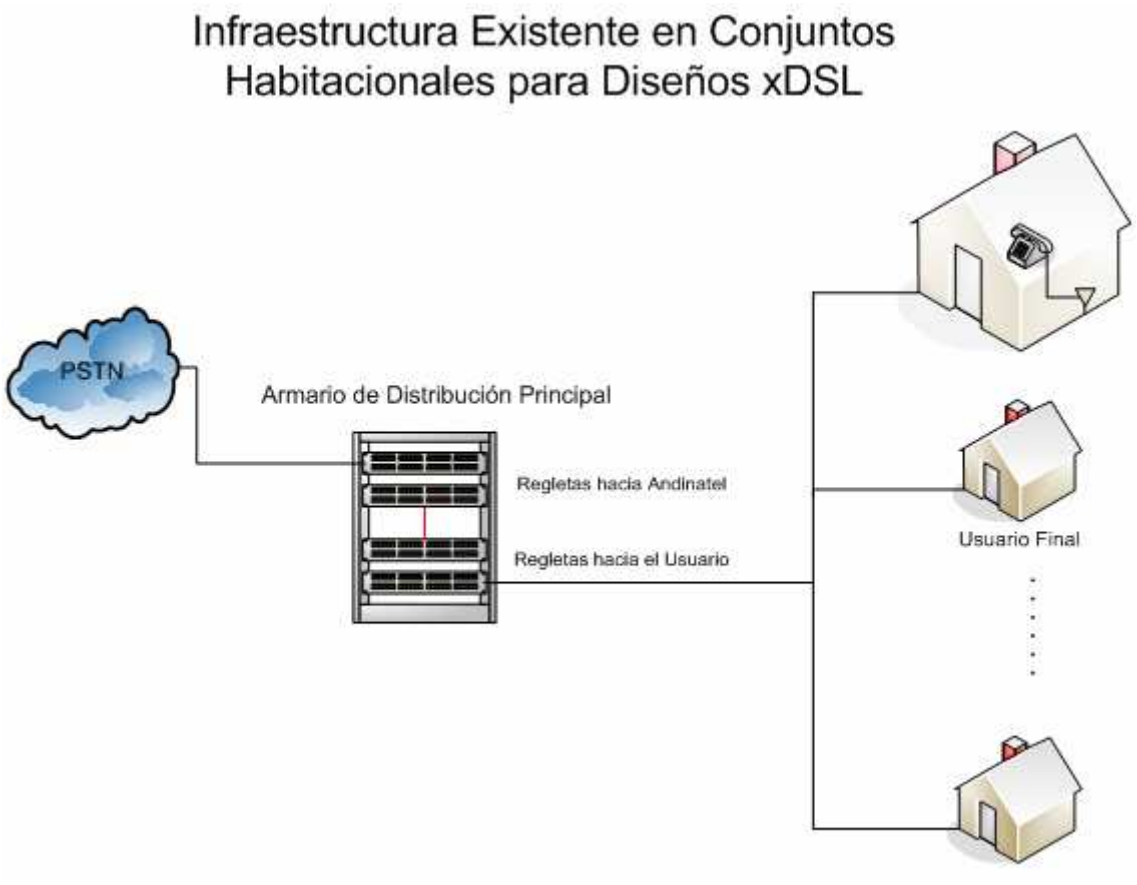


Figura 3.13. Infraestructura Existente en Conjunto Habitacionales para Diseños xDSL

La infraestructura de todo conjunto habitacional con más de 19 viviendas debe contar con su propia planta interna, consistente en el cableado telefónico a cada casa mediante multipar telefónico, generalmente categoría 3, los cuales parten del armario de distribución principal.

En el armario de distribución principal se diferencian dos grupos de regletas telefónicas, las que se dirigen en dirección del usuario y las que se dirigen en dirección al operador telefónico y su red PSTN, que en nuestro caso es Andinatel.

Como primer paso se debe montar un segundo armario, el cual nos servirá para montar los equipos ADSL y un nuevo grupo de regletas telefónicas, estas regletas servirán como un ‘espejo’ de las regletas existentes en el armario de distribución; dicho montaje nos

ayuda para separar a los clientes que deseen tomar el servicio de aquellos que no lo deseen o ya tengan un servicio xDSL en funcionamiento.

Al separar los clientes garantizamos un seguimiento de nuestros clientes para poder determinar fallas, ya sea de parte de los equipos o del servicio telefónico; no intervenimos de manera invasiva en el armario principal evitando posibles confrontaciones con el operador de servicio telefónico; no interrumpimos el servicio telefónico a usuarios ajenos; y, las reparaciones se facilitan.

La creación del armario espejo nos permitirá manejar fallas previstas o no y en caso de suspensión del servicio por parte de algún cliente, el regreso a la infraestructura inicial se logra en pocos minutos.

Dentro de este armario espejo se deben tener tomas eléctricas y ventilaciones necesarias ya albergarán equipos ADSL, en nuestro caso la unidad terminal ADSL central o ATU-C mejor conocida como DSLAM.

Las distancias entre los equipos centrales y los equipos de usuario o módems son de hasta 6 Km., distancia que nos permite cubrir con facilidad la mayor cantidad de conjuntos habitacionales dentro del área metropolitana. Finalmente en el extremo del usuario se debe instalar un splitter el cual se encargará de separar las señales de los equipos ADSL de las señales telefónicas.

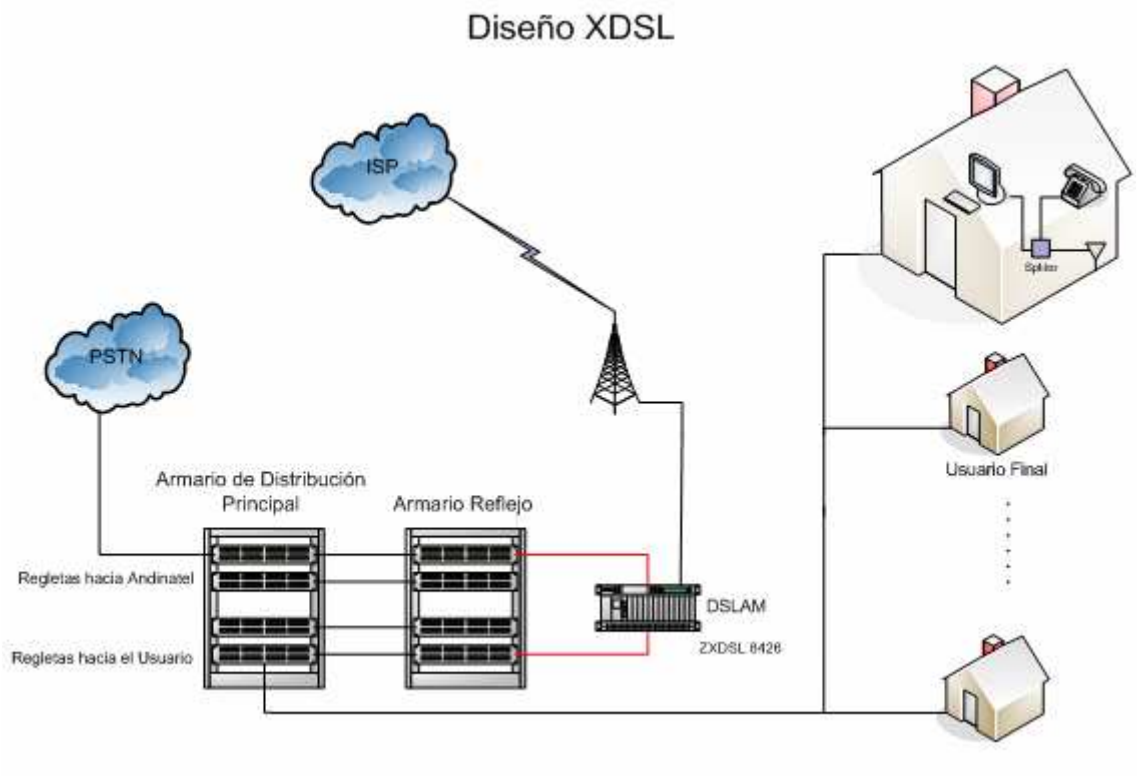


Figura 3.14. Diseño xDSL para Conjuntos Habitacionales

La parte activa en nuestro diseño xDSL esta compuesta de los equipos centrales y de usuario, es decir el DSLAM y los módems, las características que estos equipos deben cumplir son las normas g.dmt y g.lite, deben ser capaces de soportar trafico IP, tener características de capa 3 o superiores, brindar QoS y ser escalables.

Las normas g.dmt y g.lite describen el modo de operación para ADSL y SADSL, de las cuales nos interesa el modo de funcionamiento con o sin un splitter, esta característica nos permitirá resolver problemas relacionados con sistemas de alarmas o redes de telefónicas internas en las cuales el uso del splitter puede causar interferencia.

Generalmente los equipos xDSL están construidos bajo características de operación ATM, en nuestro caso no es relevante este medio de transmisión sino que pueda operar bajo premisas IP, esto además le brinda al cliente transparencia.

Al ser equipos de capa 3 o superior no permite simplificar el número de equipos necesarios, ya que el uso de un router no es necesario y se puede separar a cada usuario en VLAN´s independientes por puerto, asegurando la privacidad de los usuarios.

Soportar parámetros de QoS y en especial brindar limitaciones de tráfico, además de la escalabilidad de los equipos completa los requerimientos necesarios para ofrecer a cada cliente flexibilidad y seguridad.

El equipo que se ha tomado en cuenta para el diseño xDSL para equipos de terminales centrales es el ZXDSL 8426 de la marca ZTE, nos ofrece una gran flexibilidad, expansión y administración; mientras que para los usuarios, su complemento el ZXDSL 831 A, un modem con características avanzadas.

3.2.5 Diseño WiFi

Al igual que para Ethernet o xDSL, los diseños WiFi son diseños híbridos de última milla, es decir que desde el ISP saldremos mediante una WLAN usando radios de última milla y el último tramo hasta el cliente se realizará utilizando WiFi.

Para este diseño es necesario además de tener equipamiento WiFi para el segundo tramo, usar ciertas normativas de cableado para poder desplegar de manera eficiente nuestra red WiFi.

3.2.5.1 Primer Tramo

Este tramo inicial en el diseño WiFi es similar al ya presentado en edificios, con la diferencia de que usaremos más de un enlace dentro del conjunto habitacional al igual que el primer diseño Ethernet para conjuntos, esto debido a las limitaciones de cobertura que prestan los equipos WiFi.

3.2.5.2 Segundo Tramo

Los equipos que seleccionados deben cumplir con la norma 802.11g, tienen un rango de acción de hasta 100 metros considerando espacios sin obstáculos, en una implementación real dicha área de cobertura se verá limitada dependiendo de la geografía y características de la zona propuesta, es preciso utilizar equipos con antenas de mayor ganancia para asegurarnos de tener cobertura en ambientes exteriores, debido a ubicación de los mismos que serán en las zonas comunales o dentro de viviendas.

La parte pasiva de nuestro diseño se realiza de acuerdo a las normas de cableado estructurado, se debe instalar par trenzado categoría 5e para poder tener la oportunidad de utilizar equipos que soporten potencia sobre Ethernet o PoE; se debe optar por construir solo un MDF por cada acceso de primer tramo.

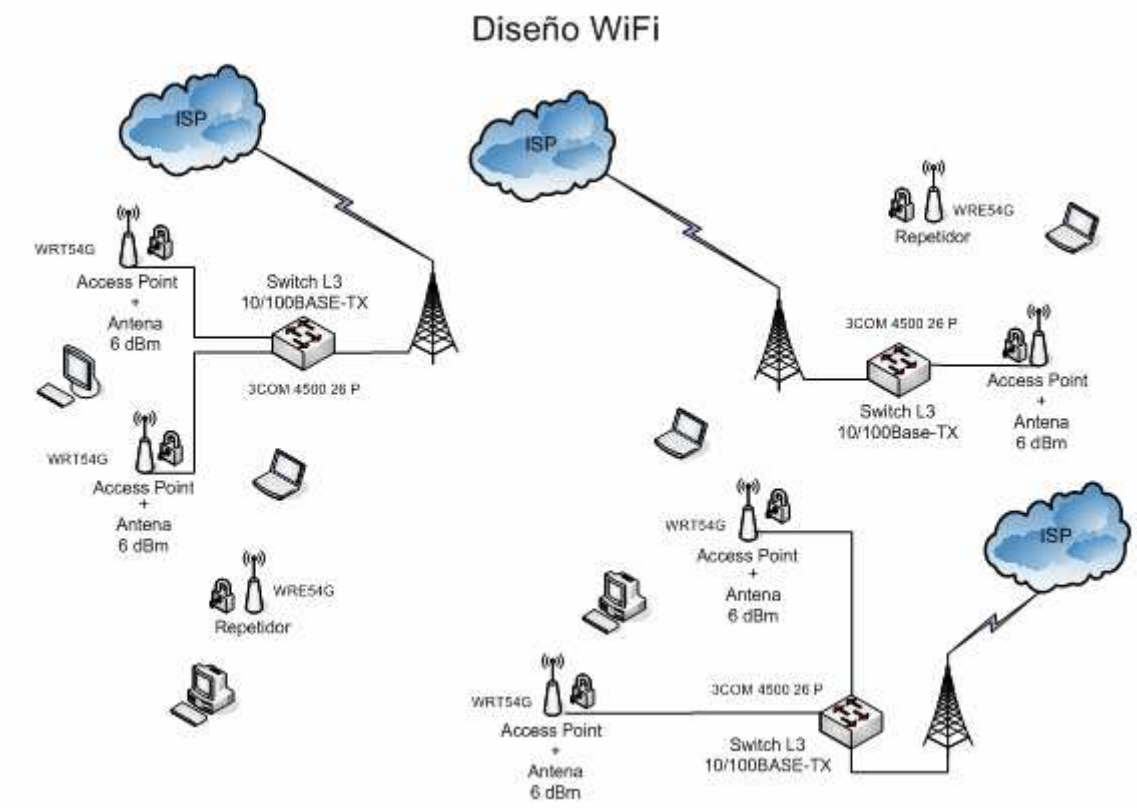


Figura 3.15. Diseño WiFi para Conjuntos Habitacionales

La parte activa de nuestro tramo WiFi esta compuesto por elementos tanto 802.3 como 802.11g, dentro de los elementos tendremos un switch de administrable capaz de soportar VLAN's, y los equipos inalámbricos deben ser todos access point de capa 3 al menos y que presten QoS a los clientes tanto en la parte inalámbrica como cableada y lo mas importante brindar acceso protegido WiFi (WPA) como requerimiento mínimo de seguridad.

El switch que acompañará a cada enlace de primer tramo debe soportar características básicas de ruteo, soportar limitaciones de trafico y soporte de VLAN's; esto facilitara la privacidad de los usuarios.

Los equipos inalámbricos que se usaran deben soportar acceso protegido WiFi para poder garantizar la seguridad de la red de acceso, las habilidades de capa 3 junto con QoS

nos ayudaran a limitar las funciones de la red, ya que solo tiene como propósito dar acceso a los servicio del ISP y no el de convertirse en una LAN para el conjunto, ya se comprometería la privacidad de los usuarios.

La selección de los equipos inalámbricos, no solo se limitara a los access point, debido a las distancias que se debe cubrir, es necesario aumentar el área de cobertura de los equipos, esto lo lograremos mediante la utilización de antenas de 6 dBm de ganancia o para áreas problemáticas con expansores de red, estos equipos son un bridge que amplia la cobertura de un equipo determinado.

Los equipos WiFi que se usaran son de la marca Linksys, específicamente el modelo WRT54G, para access point, las antenas de ganancia a usarse con las HGA7T que se ajustan al access point, mientras que los expansores son los WRE54G; mientras que el switch será de la marca 3COM de la familia 4500 26 P.

3.2.5.2.1 Diseño de la Cobertura

Como se menciono anteriormente los equipos WiFi funcionan en un rango de 100 metros sin obstáculos, pero al entrar en ambientes con paredes el área de cobertura de los equipos disminuye, esto significa que para cubrir cierta área se requieran más de un equipo, esto impacta severamente en la cantidad de recursos que se debe usar para poder brindar una red inalámbrica.

La cantidad de equipos a utilizarse depende de los materiales con los que se haya construido las unidades habitacionales, a continuación tenemos un survey con un AP dentro de una construcción de ladrillo, pasando por áreas verdes y tres viviendas tipo construidas con bloque.

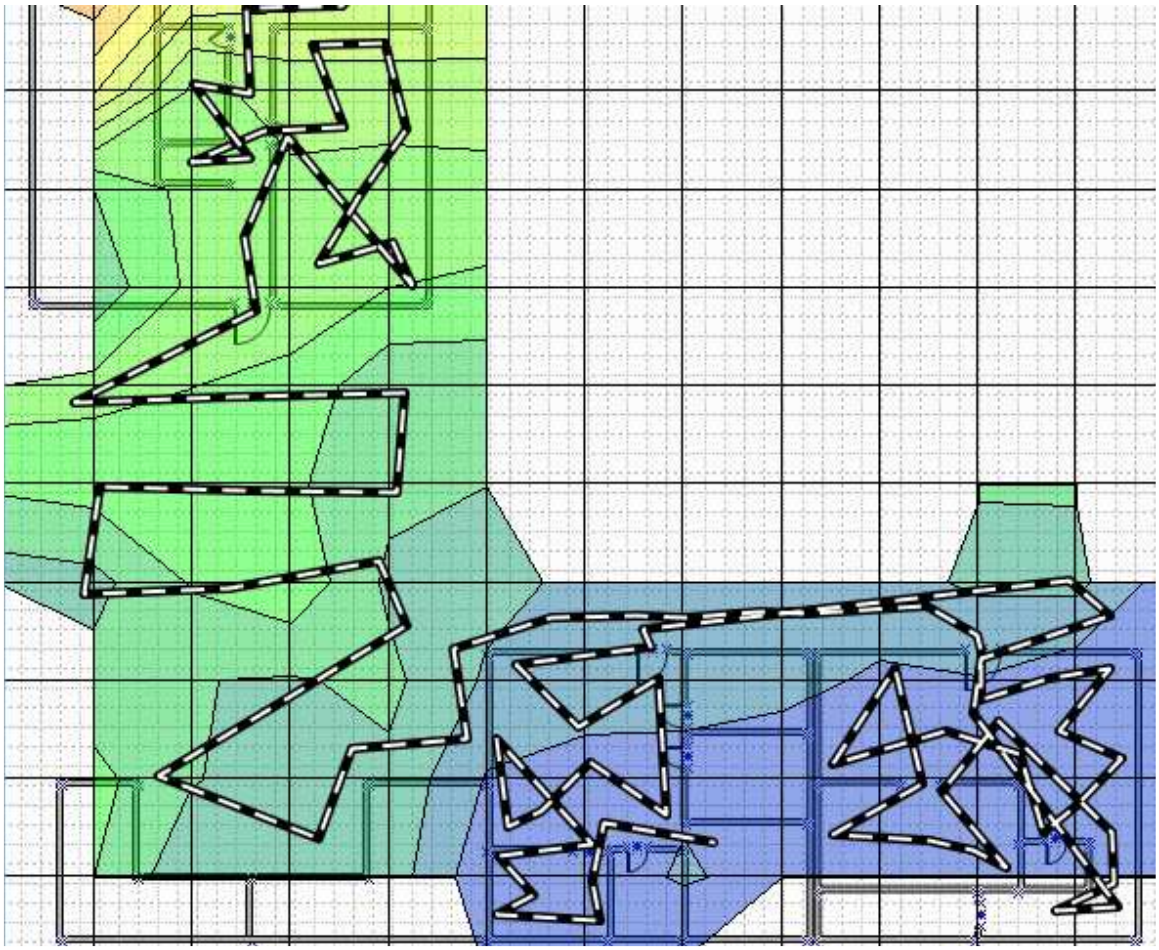


Figura 3.16. Survey WiFi en Varias Viviendas

En la figura se aprecian arriba a la izquierda la construcción de ladrillo con un access point irradiando señales WiFi, se nota que las señales sufren una caída severa debido al material, pero en la parte inferior se encuentran las viviendas construidas con bloque, la atenuación que se aprecia se debe a la distancia mas que a paredes.

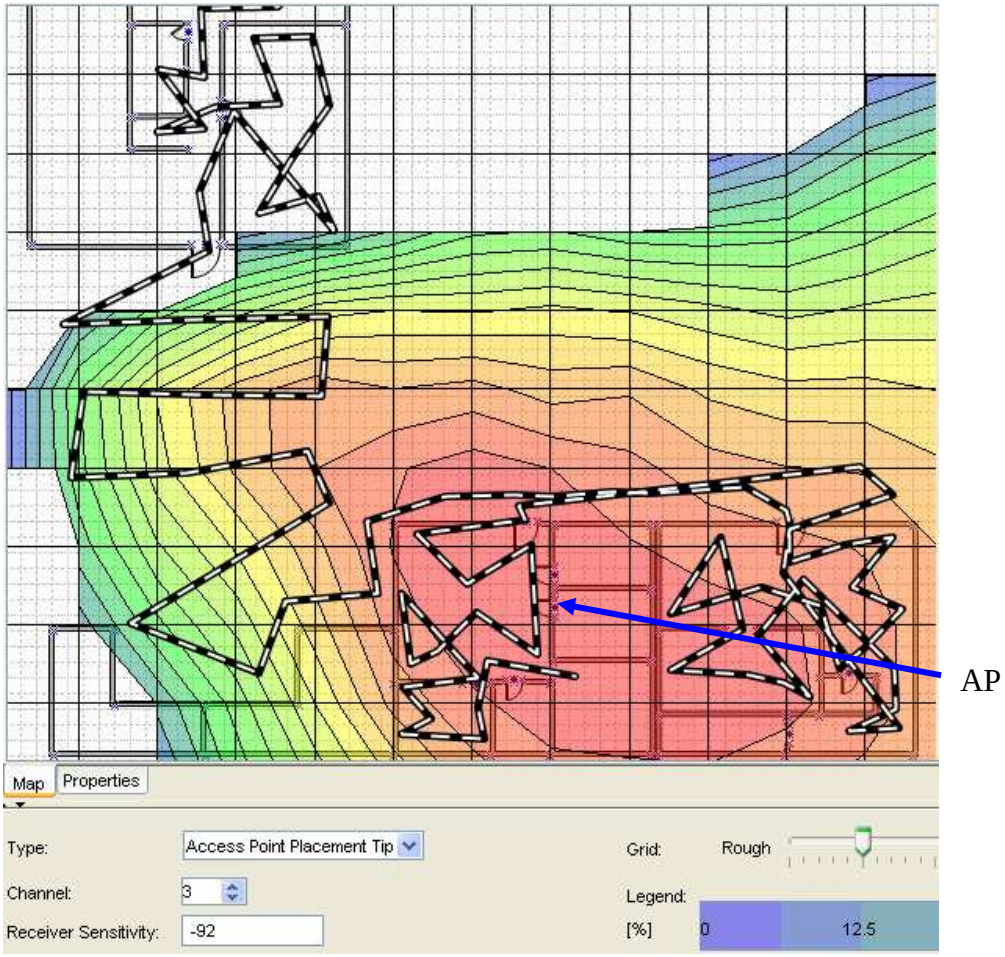


Figura 3.17. Predicción del Área de Cobertura para Conjuntos Habitacionales

Al realizar la predicción de access point necesarios para cubrir viviendas aledañas descubrimos que se requiere de un AP por cada tres viviendas, para asegurar que la cobertura estimada cumpla con los requerimientos, cada punto de acceso tendrá además antenas de 6 dBm de ganancia, es decir el doble de ganancia.

La predicción se realiza en el canal 3, debido a que tendrán áreas de cobertura solapadas, el equipo ubicado en la primera vivienda funciona en el canal 1, las coberturas se mejoran a medida exista separación entre canales, son embargo la cantidad de equipos a utilizarse imposibilitan dicha configuración.

Cabe destacar que la señal no solo dará servicio a las unidades habitacionales sino que se contara con servicio en todas las inmediaciones cercanas, es decir calles y áreas publicas de recreación, en caso de tener problemas de cobertura se puede optar por ampliar el rango de cobertura mediante los expansores de cobertura propuestos.

3.3 DISEÑO WIMAX PARA AREAS RESIDENCIALES

La tecnología WiMAX es capaz de dar acceso por igual a edificios de departamentos como para conjuntos habitacionales, esto gracias a las excelentes prestaciones de cobertura, en áreas metropolitanas no muy densas como las ciudades ecuatorianas la cobertura que se tiene es de 5 a 6 Km. Sin línea de vista, de hasta 10 Km. Con línea de vista.

Los equipos WiMAX nos ofrecen QoS y soportan varias clases de tráfico incluido IP, además de estar diseñada para una gran cantidad de clientes simultáneamente, tanto fijos como móviles, es una solución integral, que no solo promete un despliegue rápido sino puede reemplazar la infraestructura completa de ultima milla.

Gracias a estas prestaciones se propondrá un solo diseño WiMAX capaz de dar servicio a edificios como conjuntos habitacionales por igual.

3.3.1 Descripción de las Áreas Residenciales

Las áreas residenciales previstas para este diseño son corresponden tanto a edificios de departamentos como conjuntos habitacionales, las características tanto físicas como humanas son iguales a las descritas anteriormente.

El aspecto del cual debemos preocuparnos no es el físico sino el humano, ya que gracias a WiMAX cada unidad habitacional puede ser manejada de forma independiente, es decir que el numero de familias es el dato que se debe manejado para cálculos de equipamiento y económicos.

3.3.2 Requerimientos Básicos

Un ISP que busque captar el mercado residencial, debe tener en cuenta ciertas pautas a la hora de brindar sus servicios dentro de un edificio de departamentos o conjuntos habitacionales, entre ellas están las siguientes:

- ✓ Seguridad de la red.
- ✓ Privacidad entre los usuarios.
- ✓ Transparencia de la tecnología.
- ✓ Escalabilidad.

La seguridad en la red es un parámetro que debe ser tomado en cuenta, WiMAX es capz de prestar enlaces inalámbricos con altas seguridades, ya sea utilizando autenticación X.509 y llaves de encripción personales y grupales, garantizando la seguridad de la red.

El parámetro de la privacidad entre usuarios no es problema para la tecnología 802.16, ya que cada cliente tiene acceso a la red mediante unidades de subscriptor, las cuales son tratadas por la red como conexiones independientes.

La transparencia de la tecnología para con el usuario esta garantizada al soportar diferentes tipos de tráficos, el soporte de IP garantiza la transparencia para el usuario.

Finalmente los equipos propuestos deben ser capaces de crecer con el numero de clientes, debido a su estatus de nueva tecnología, los clientes iniciales serán limitados hasta la implementación de chips compatibles en dispositivos portátiles como Laptops o Pocket PC’s.

3.3.3 Diseño WiMAX

3.3.3.1 La Red WiMAX

El diseño WiMAX plantea un nuevo enfoque a la infraestructura de un ISP, debido a su gran capacidad de despliegue, no es necesario tener varios tramos dentro de la última milla, es decir 802.16 es capaz de llegar a clientes dispersos con QoS y accesos de banda ancha a servicios de Internet a costos competitivos.

WiMAX puede reemplazar la construcción de una la infraestructura de backhaul cableada mediante fibra óptica, por lo tanto sugiere un cambio a gran escala de infraestructura de acceso de un ISP.

Para abaratar los costos de implementación, cada estación base WiMAX estará conectada mediante los equipos de última milla existentes, pero eliminara el uso de los mismos para el uso de clientes, es decir se cambiaran los equipos de radio de clientes por terminales de subscriptor WiMAX.

El cambio de la infraestructura casi completa del ISP viene de la mano con un mejoramiento en su cobertura, nuevos servicios y mejoramiento del tráfico del proveedor de servicios de Internet; ahora puede tener el control de los anchos de banda de manera mas precisa, puede separa clientes elite o regulares, gracias a capacidades QoS WiMAX, que diferencian tipos de trafico (trafico en tiempo real, en tiempo real por demanda, por demanda, intermitente), mejorando el desempeño de la red; puede dar servicio a clientes sin línea de vista, característica que la mayoría de equipos de ultima milla no posee; y puede tener clientes no solo fijos sino móviles, dentro o entre las áreas de cobertura WiMAX.

Gracias a la gran disponibilidad de bandas de frecuencia en las cuales se puede encontrar el equipamiento 802.16, se puede seleccionar bandas licenciadas o de uso libre, permitiendo mantener en operación ambas redes, la existente y WiMAX sin conflictos de frecuencias, durante el periodo de transición.

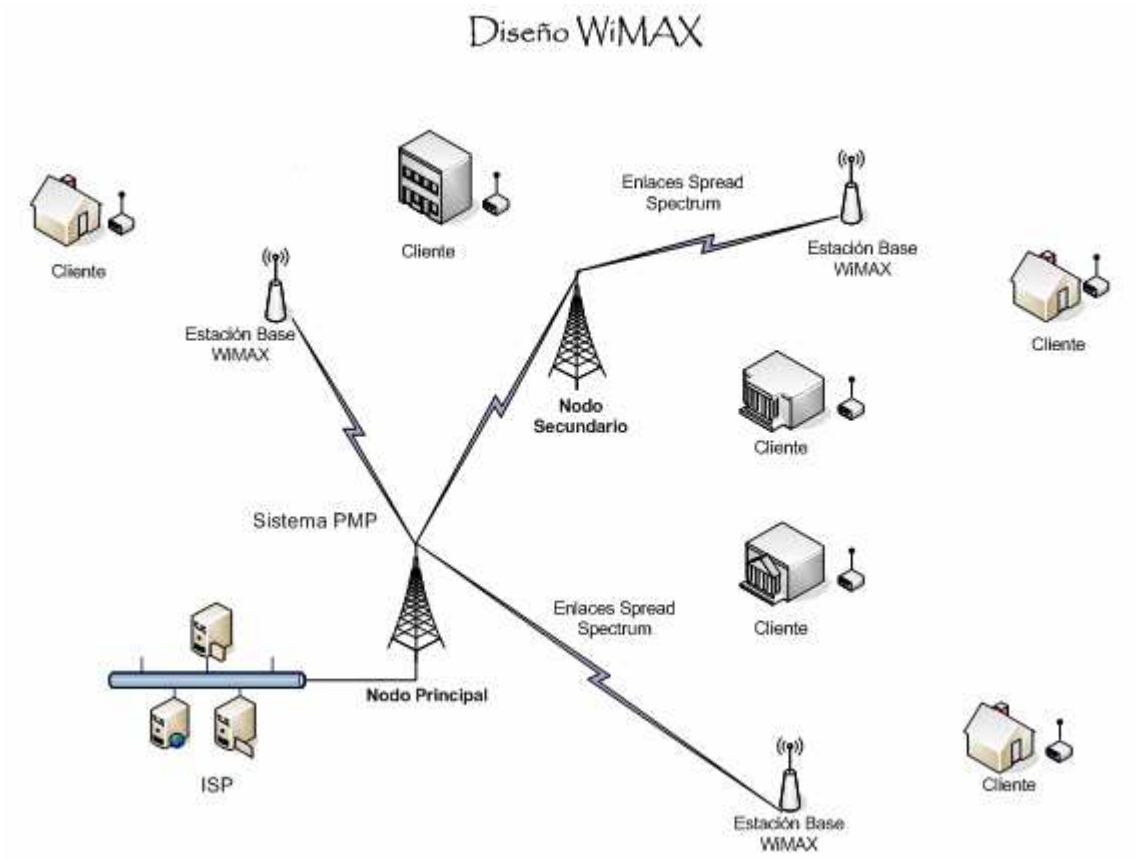


Figura 3.18. Diseño WiMAX

Dentro de este esquema se puede apreciar claramente que los enlaces inalámbricos PMP en espectro ensanchado llegan a las estaciones base 802.16, a partir de estas todo el tramo hasta el cliente es inalámbrico y con terminales WiMAX.

La gran capacidad de ancho de banda de los equipos 802.16 permite llegar a las unidades habitacionales sin distinción de su ubicación dentro de un edificio o conjunto habitacional.

3.3.3.2 Diseño de la Cobertura

Al reemplazar los equipamientos por estaciones WiMAX se debe tener en cuenta la zona de cobertura de una estación base, en zonas metropolitanas medianamente pobladas, se tiene un área de cobertura máxima de 10 Km operaciones LOS y de 5 a 6 Km. en operaciones NLOS, es decir que con pocas estaciones base se cubrirá el área de interés.

Dentro del Distrito Metropolitano de Quito se han identificado las zonas con mayor impacto comercial de uso de Internet a nivel residencial, dichas zonas son:

- ✓ El norte de la ciudad (Norte, Centro Norte)
- ✓ Valle de Tumbaco.
- ✓ Valle de Sangolquí.

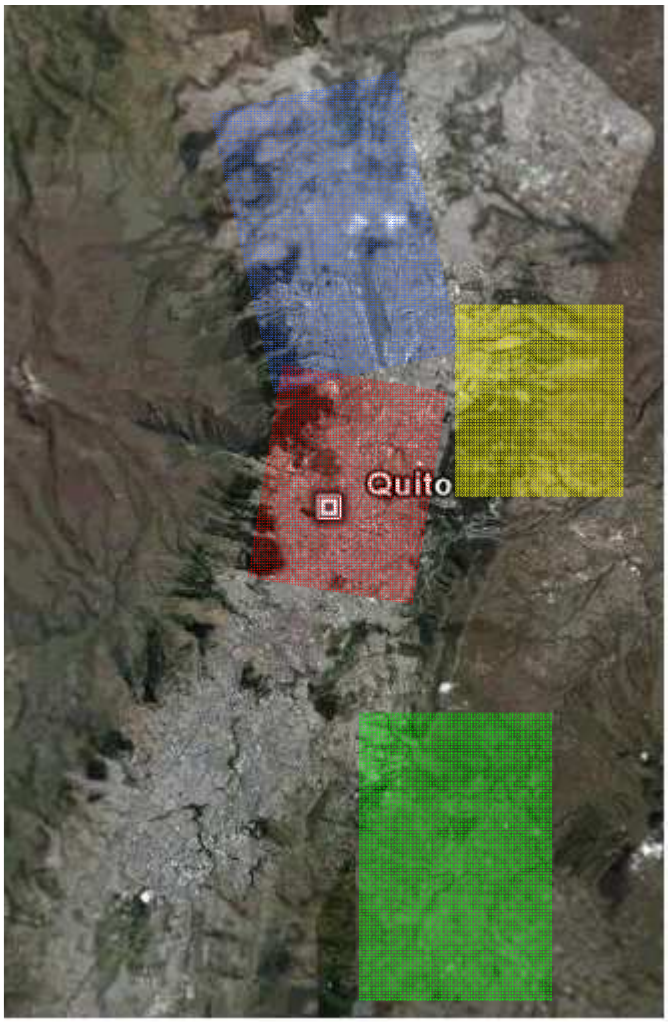


Figura 3.19. Diagrama de las Zonas de Interés WiMAX

Las tres zonas de interés dentro de la Ciudad de Quito se pueden cubrir con cuatro estaciones base WiMAX, las distancias de cada una de las celdas están dentro de los 7 Km. de largo por 5 Km. de ancho, tamaños de celdas medianas y dentro de las capacidades de despliegue 802.16.

La zona que mayor interés despierta, es la zona centro norte, la cual abarca el distrito comercial de la ciudad, por ende el sector mas denso, la estación base debe garantizar el funcionamiento NLOS dentro de esta zona de 2.77 Km. de largo por 4.58 Km. de ancho.

Figura 3.20. Distancias de la Zona Centro Norte

Debido a la situación geográfica de la ciudad de Quito, las estaciones base pueden estar equipadas ya sea con antenas omnidireccionales o con antenas direccionales, dependiendo de los sectores que se deseen cubrir.

CAPITULO IV

ANÁLISIS ECONÓMICO DEL PROYECTO

4.1 ANALISIS ECONOMICO PARA EDIFICIOS

Dentro del presente capitulo se detallan los precios de los elementos activos y pasivos utilizados en los diseños de última milla para edificios, costos adicionales y precios por el servicio de Internet.

4.1.1 Diseño Ethernet

4.1.1.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
M5830S-SU	Dual Band CPE 5.3/5.8 Internal Antenna	795	1	795
Quidway S3928P	Switch de Capa 3, 28 Puertos	1554.84	1	1554.84
Rack de Piso	Abierto 19"	185	1	185
Patch Panel	RJ45 24 Puertos	60	1	60
Cable UTP CAT 5e	305 m. 200 Mhz	45	2	90
Cajetines, Face Plate	Cajetín y Conector	9.56	6	57.36
Patch Cord	UTP RJ45 3 m.	2.12	13	27.56
Organizador de Cable	1 unidad	8.25	1	8.25
Total				**2778.01**

Tabla 4.1. Detalle de Precios Ethernet

Los costos de materiales y equipos llegan a un total de USD 2778.01.

4.1.1.2 Costos Adicionales

Debido a que debe trabajar en edificios ya construidos siempre surge la posibilidad de incurrir en alguna obra civil, se ha destinado un valor del 30% del costo de los materiales, teniendo un valor de USD 128.45.

4.1.1.3 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 109.37, este costo es para los 6 clientes del edificio.

4.1.1.4 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de los equipos de comunicación es rápida y un cliente promedio permanece un año con un ISP, dicho periodo es de 12 meses; el costo mensual que se cobrará a cada cliente es de USD 60.

$$ROI = \frac{4320}{4218.9} = 1.02$$

4.1.2 Diseño xDSL

4.1.2.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
M5830S-SU	Dual Band CPE 5.3/5.8 Internal Antenna	795	1	795
ZXDSL-831-A	MODEM ADSL	52,64	6	315,84
ZXDSL-8426	MINI DSLAM	1568	1	1568
Armario Telefónico	60x80x25	80	1	80
Regletas Telefónicas	10 pares	15	2	30
Total				**2788,84**

Tabla 4.2. Detalle de Precios xDSL

Los costos de materiales y equipos llegan a un total de USD 2788.84.

4.1.2.2 Costos Adicionales

Se deben realizar trabajos de obra civil para poder instalar el segundo armario telefónico, debido a este trabajo se ha destinado un valor del 30% del costo de los materiales, teniendo un valor de USD 33.

4.1.2.3 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 109.37, este costo es para los 6 clientes del edificio.

4.1.2.4 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de los equipos de comunicación es rápida y un cliente promedio permanece un año con un ISP, dicho periodo es de 12 meses; el costo mensual que se cobrará a cada cliente es de USD 60.

$$ROI = \frac{4320}{4134.28} = 1.04$$

4.1.3 Diseño WiFi

4.1.3.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
M5830S-SU	Dual Band CPE 5.3/5.8 Internal Antenna	795	1	795
3COM 4500 26P	Switch de Capa 3, 26 Puertos	695,45	1	695,45
WRT54G	Router Access Point 802.11g	68,32	12	819,84
Rack de Piso	Abierto 19"	185	1	185
Patch Panel	RJ45 24 Puertos	60	1	60
Cable UTP CAT 5e	305 m. 200 Mhz	45	2	90
Conectores	RJ45	0,25	12	3
Patch Cord	UTP RJ45 3 m.	2,12	13	27,56
Organizador de Cable	1 unidad	8,25	1	8,25
Total				**2684,1**

Tabla 4.3. Detalle de Precios WiFi

Los costos de materiales y equipos llegan a un total de USD 2684.1.

4.1.3.2 Costos Adicionales

Debido a que debe trabajar en edificios ya construidos siempre surge la posibilidad de incurrir en alguna obra civil, se ha destinado un valor del 30% del costo de los materiales, teniendo un valor de USD 112.14.

4.1.3.3 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 109.37, este costo es para los 6 clientes del edificio.

4.1.3.4 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de los equipos de comunicación es rápida y un cliente promedio permanece un año con un ISP, dicho periodo es de 12 meses; el costo mensual que se cobrará a cada cliente es de USD 60.

$$ROI = \frac{4320}{4108.68} = 1.05$$

4.2 ANALISIS ECONOMICO PARA CONJUNTOS HABITACIONALES

A continuación se detallan los precios de los elementos activos y pasivos utilizados en los diseños de última milla para conjuntos, costos adicionales y precios por el servicio de Internet.

4.2.1 Primer Diseño Ethernet

4.2.1.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
M5830S-SU	Dual Band CPE 5.3/5.8 Internal Antenna	795	2	1590
3COM 4500 26P	Switch de Capa 3, 26 Puertos	695,45	2	1390,9
Rack de Piso	Abierto 19"	185	2	370
Patch Panel	RJ45 24 Puertos	60	2	120
Cable UTP CAT 5e	305 m. 200 Mhz	45	4	180
Cajetines, Face Plate	Cajetín y Conector	9,56	11	105,16
Patch Cord	UTP RJ45 3 m.	2,12	24	50,88
Organizador de Cable	1 unidad	8,25	1	8,25
Total				**3815,19**

Tabla 4.4. Detalle de Precios Primer Diseño Ethernet

Los costos de materiales y equipos llegan a un total de USD 3815.19.

4.2.1.2 Costos Adicionales

Para la obra civil, se ha destinado un valor del 30% del costo de los materiales, teniendo un valor de USD 250.28.

4.2.1.3 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 200.52, este costo es para los 11 clientes del conjunto.

4.2.1.4 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de los equipos de comunicación es rápida y un cliente promedio permanece un año con un ISP, dicho periodo es de 12 meses; el costo mensual que se cobrará a cada cliente es de USD 60.

$$ROI = \frac{7920}{6471.71} = 1.22$$

4.2.2 Segundo Diseño Ethernet

4.2.2.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
M5830S-SU	Dual Band CPE 5.3/5.8 Internal Antenna	795	1	795
Quidway S3928P	Switch de Capa 3, 28 Puertos	1554,84	1	1554,84
3COM 4500 26P	Switch de Capa 3, 26 Puertos	695,45	1	695,45
3COM	Modulo de Expansión 1000BASE SX	465,76	1	465,76
Rack de Piso	Abierto 19"	185	3	555
Patch Panel	RJ45 24 Puertos	60	3	180
Cable UTP CAT 5e	305 m. 200 Mhz	45	4	180
Cajetines, Face Plate	Cajetín y Conector	9,56	11	105,16
Patch Cord	UTP RJ45 3 m.	2,12	24	50,88
Organizador de Cable	1 unidad	8,25	3	24,75
Fibra Óptica	Multimodo 62.5/125 2 pares	3,84	300	1152
Conectores	Conectores SC	4,32	8	34,56
Bandeja	Bandeja para Fibra Óptica	127,39	1	127,39
Total				**5920,79**

Tabla 4.5. Detalle de Precios Segundo Diseño Ethernet

Los costos de materiales y equipos llegan a un total de USD 5920.79.

4.2.2.2 Costos Adicionales

Para la obra civil, se ha destinado un valor del 30% del costo de los materiales, teniendo un valor de USD 722.92.

4.2.2.3 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 200.52, este costo es para los 11 clientes del conjunto.

4.2.2.4 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de los equipos de comunicación es rápida y un cliente promedio permanece un año con un ISP, dicho periodo es de 12 meses; el costo mensual que se cobrará a cada cliente es de USD 60.

$$ROI = \frac{7920}{9049.95} = 0.87$$

4.2.3 Diseño xDSL

4.2.3.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
M5830S-SU	Dual Band CPE 5.3/5.8 Internal Antenna	795	1	795
ZXDSL-831-A	MODEM ADSL	52,64	11	579,04
ZXDSL-8426	MINI DSLAM	1568	1	1568
Armario Telefónico	60x80x25	80	1	80
Regletas Telefónicas	10 pares	15	3	45
Total				**3067,04**

Tabla 4.6. Detalle de Precios xDSL

Los costos de materiales y equipos llegan a un total de USD 3067.04.

4.2.3.2 Costos Adicionales

Se deben realizar trabajos de obra civil para poder instalar el segundo armario telefónico, debido a este trabajo se ha destinado un valor del 30% del costo de los materiales, teniendo un valor de USD 37.5.

4.2.3.3 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 200.52, este costo es para los 11 clientes del conjunto.

4.2.3.4 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de los equipos de comunicación es rápida y un cliente promedio permanece un año con un ISP, dicho periodo es de 12 meses; el costo mensual que se cobrará a cada cliente es de USD 60.

$$ROI = \frac{7920}{5510.78} = 1.43$$

4.2.4 Diseño WiFi

4.2.4.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
M5830S-SU	Dual Band CPE 5.3/5.8 Internal Antenna	795	3	2385
3COM 4500 26P	Switch de Capa 3, 26 Puertos	695,45	3	2086,35
WRT54G	Router Access Point 802.11g	68,32	9	614,88
HGA7T	Antenas de 6 dBm de ganancia	57,02	9	513,18
WRE54G	Expansor de Rango WiFi	138,35	2	276,7
Armario	60x80x25	80	3	240
Armario	30x25x15	20	11	220
Cable UTP CAT 5e	305 m. 200 Mhz	45	4	180
Conectores	RJ45	0,25	18	4,5
Patch Cord	UTP RJ45 3 m.	2,12	12	25,44
Total				**6546,05**

Tabla 4.7. Detalle de Precios WiFi

Los costos de materiales y equipos llegan a un total de USD 6546.05.

4.2.4.2 Costos Adicionales

Debido a que debe trabajar en edificios ya construidos siempre surge la posibilidad de incurrir en alguna obra civil, se ha destinado un valor del 30% del costo de los materiales, teniendo un valor de USD 200.98.

4.2.4.3 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 200.52, este costo es para los 11 clientes del conjunto.

4.2.4.4 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de los equipos de comunicación es rápida y un cliente promedio permanece un año con un ISP, dicho periodo es de 12 meses; el costo mensual que se cobrará a cada cliente es de USD 60.

$$ROI = \frac{7920}{9153.27} = 0.86$$

4.3 ANALISIS ECONOMICO PARA DISEÑOS WiMAX

A continuación se detallan los precios, costos adicionales y precios por el servicio de Internet, para una implementación WiMAX, los equipos 802.16 escogidos son de la marca Redline y su división RedMAX.

4.3.1 Detalle de Precios

Equipo	Descripción	Valor Unitario	Unidades	Valor Total
AN-100U	Estación Base 802.16d/e	11900	4	47600
SU-I	Estación de Subscriptor	567,1	100	56710
Total				**104310**

Tabla 4.8. Detalle de Precios WiMAX

Los costos equipos llegan a un total de USD 104310, esta inversión es tan alta debido a que corresponde a una reestructuración de la empresa y su equipamiento a gran escala.

4.3.1.1 Costos Adicionales

Para poder preveer costos de instalación de estos equipos nuevos se ha destinado el 30% del costo de de los mismos, teniendo un valor de USD 31293.

4.3.1.2 Costos Servicio de Internet

El costo por la conexión al Internet mensualmente asciende a USD 2734.37, este costo es para los 100 clientes.

4.3.1.3 Retorno de la Inversión

Para poder calcular el retorno de la inversión es necesario determinar el tiempo en el que se planea recuperar la inversión, debido a que la depreciación de equipos WiMAX esta estimada en 36 meses, este plazo se aplica a los clientes debido a que los equipos pueden ser usados para clientes residenciales independientemente de su unidad habitacional, permitiendo realizar un re uso de equipos; el costo mensual que se cobrará a cada cliente es de USD 80, ya que se procederá a cargar USD 20 por valores de arrendamiento de equipos.

$$ROI = \frac{288000}{234040.5} = 1.23$$

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La tecnología que mejor se adapta para dar servicio a clientes residenciales, tanto en costos como tecnológicamente es WiMAX, esta solución representa un avance en la infraestructura del ISP, y le permite tener un control de sus clientes por encima del resto de tecnologías.

- Los servicios prestados por 802.16 a nivel de seguridad, tanto con protocolos de encriptación de llaves compartidas e individuales, así como procesos de autenticación X.509 permiten garantizar la seguridad de los clientes, a un nivel de una red cableada.

- La gran capacidad de ancho de banda disponible por sector de los equipos WiMAX, que es de 48 Mbps esta por encima de los tradicionales 10 Mbps de equipos de última milla actuales, permitiendo tener más clientes por sector.

- WiMAX responde a la tendencia actual de la convergencia de tecnologías, ya que puede ser capaz de captar varios tipos de tráficos sin perder las características de los mismos gracias al empleo de políticas QoS.

- La implementación de la tecnología WiMAX permitirá la incursión en primera instancia de clientes residenciales en edificios o conjuntos habitacionales, pero al mismo tiempo puede ser usada para dar servicio a clientes corporativos, sin tener que incurrir en nuevos gastos futuros.

- El mayor impedimento para el desarrollo de las otras tecnologías propuestas no es la escala de los diseños, ni sus costos, es el valor del acceso al Internet que el ISP debe absorber, costos que al momento de la elaboración del proyecto bordean los USD 3500 por una capacidad de 2048 Kbps.

- Para que los precios propuestos de costos de acceso al Internet se puedan alcanzar, en los diseños Ethernet, xDSL y WiFi la relación de ancho de banda compartido es de 1:12, valor que compromete la calidad del servicio prestado.

- Por otro lado la estupenda recuperación de la inversión manifestada por WiMAX permite que la relación de ancho de banda compartido baje a 1:8, esta relación puede mejorar si la inversión inicial se aumenta de 100 a 400 clientes.

- Los precios de equipos 802.16, son al momento elevados, sin embargo, se pronostica el descenso en precios a partir del primer trimestre del 2007, permitiendo bajar los costos de inversión, volviéndola aún más rentable.

- WiMAX es capaz de trabajar en bandas de frecuencia con licencia y sin licencia, permitiendo abaratar los costos de compra de licencias, valores elevados en nuestro medio.

5.2 RECOMENDACIONES

- Si se desea optar por una de las otras tecnologías para dar servicio de Internet, hasta poder montar la infraestructura WiMAX, se recomienda optar por la tecnología xDSL para los conjuntos habitacionales y WiFi para edificios, estas tecnologías permiten un despliegue rápido y económico.

- Se debe proponer a los organismos del estado CONATEL y SENATEL que intenten bajar los costos de acceso al Internet, mediante la creación de infraestructuras propias que nos conecten con los accesos de fibra óptica internacionales, para no tener que pagar altos costos a países vecinos.

- La tendencia de las tecnologías se ha volcado hacia IP, ofreciendo QoS o mediante el uso de IPv6, WiMAX esta orientado a soportar dicho tráfico y calidad de servicio bajo IP, su adopción permitirá no solo dar un mejor acceso a Internet, permitirá construir un backhaul en el país en zonas urbanas que al momento es casi inexistente.

- La puesta en escena del chip PRO/Wireless 5116 de Intel, indica que en cuestión de meses las nuevas computadoras portátiles tendrán capacidad WiFi y WiMAX, dejar de lado la tecnología 802.16 se convierte en un riesgo a la hora de captar nuevos mercados y oportunidades de expansión; es recomendable iniciar pruebas e inversiones WiMAX.

- Al tener organismos de control estatales atrasados en materia de certificación de equipos y parámetros de funcionamiento, se debe esperar para tomar una decisión respecto a las bandas de frecuencia de los equipos, pese a que el mercado nos indica que la banda a ser desarrollada con fuerza es la de 3.5 GHz.

REFERENCIAS BIBLIOGRÁFICAS

- ✓ http://www.yale.edu/pclt/COMM/TCPIP.HTM, Conceptos TCP/IP.
- ✓ http://en.wikipedia.org/wiki/Internet_history, Historia del Internet.
- ✓ http://www.faqs.org/rfcs/rfc793.html, Funcionamiento TCP.
- ✓ http://www.cs.fit.edu/~mmahoney/cse3103/tcpip.html, Estructura de Capa.
- ✓ http://www.networksorcery.com/enp/rfc/rfc3540.txt, Campos ECN de IP.
- ✓ http://www.networksorcery.com/enp/rfc/rfc791.txt, IPv4.
- ✓ http://www.networksorcery.com/enp/rfc/rfc3168.txt, IPv4.
- ✓ http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm, Nociones de Notación IP.
- ✓ http://www.faqs.org/rfcs/rfc791.html, IPv4.
- ✓ http://www.cisco.com/univercd/cc/td/doc/cisntwk/ito_doc/ethernet.htm, Conceptos Básicos Ethernet.
- ✓ http://standard.ieee.org/getieee802/download/802.3-2002.pdf, Estándar 802.3.
- ✓ RFC2460, Especificaciones Internet Protocol Version 6 (IPv6), Diciembre 1998.
- ✓ Recomendación G.992.1, International Telecomunication Union, Julio 2005.
- ✓ Estándar IEEE 802.11, Institute of Electrical and Electronics Engineers, Diciembre 2004.
- ✓ Estándar IEEE 802.11i, Institute of Electrical and Electronics Engineers, Diciembre 2004.
- ✓ Estándar IEEE 802.11g, Institute of Electrical and Electronics Engineers, Julio 2005.
- ✓ Estándar IEEE 802.16, Institute of Electrical and Electronics Engineers, Diciembre 2005.
- ✓ “Reglamento para la Prestación de Valor Agregado”, CONATEL, 20 de Febrero del 2002.

ANEXO 1

REGLAMENTO PARA LA PRESTACIÓN DE VALOR AGREGADO

REGLAMENTO PARA LA PRESTACION DE SERVICIOS DE VALOR AGREGADO

RESOLUCIÓN 071-03-CONATEL-2002-02-20

REGISTRO OFICIAL No. 545-1-ABRIL-2002

CONSEJO NACIONAL DE TELECOMUNICACIONES

CONATEL

CONSIDERANDO:

Que el literal d) del innumerado tercero del artículo 10 de la Ley Reformatoria a la Especial de Telecomunicaciones faculta al Consejo Nacional de Telecomunicaciones (CONATEL) a expedir normas de carácter general para regular los servicios de telecomunicaciones;

Que el cambio a un entrono de libre competencia y los adelantos tecnológicos han dado lugar a nuevos servicios de telecomunicaciones.

En uso de sus atribuciones legales y reglamentarias,

RESUELVE:

Expedir el siguiente:

REGLAMENTO PARA LA PRESTACIÓN DE SERVICIOS DE VALOR AGREGADO

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1. El presente Reglamento tiene por objeto establecer las normas y procedimientos aplicables a la prestación de servicios de valor agregado así como los deberes y derechos de los prestadores de servicios de sus usuarios.

ARTÍCULO 2. Son servicios de valor agregado aquellos que utilizan servicios finales de telecomunicaciones e incorporan aplicaciones que permiten transformar el contenido de la información trasmitida. Esta transformación puede incluir un cambio neto entre los puntos extremos de la transmisión en el código, protocolo o formato de la información.

Se entiende que ha habido transformación de la información cuando la aplicación redirecciona, empaqueta datos, interactúa con bases de datos o almacena la información para su posterior retransmisión.

ARTÍCULO 3. Las definiciones de los términos técnicos de telecomunicaciones serán las establecidas por la Unión Internacional de Telecomunicaciones – UIT, la Comunidad Andina de Naciones – CAN, la Ley Especial de Telecomunicaciones con sus reformas y el Reglamento General a la Ley Especial de Telecomunicaciones Reformada.

ARTÍCULO 4. El título habilitante para la instalación, operación y prestación del servicio de valor agregado es el Permiso, otorgado por la Secretaría Nacional de Telecomunicaciones (Secretaría), previa autorización del Consejo Nacional de Telecomunicaciones (CONATEL).

CAPÍTULO II

DE LOS TÍTULOS HABILITANTES

ARTÍCULO 5. El plazo de duración de los títulos habilitantes para la prestación de servicios de valor agregado será de diez (10) años, prorrogables por igual período de tiempo, a solicitud escrita del interesado, presentada con tres meses de anticipación al vencimiento del plazo original, siempre y cuando el prestador haya cumplido con los términos y condiciones del título habilitante.

ARTÍCULO 6. El área de cobertura será nacional y así se expresará en el respectivo título habilitante, pudiéndose aprobar títulos habilitantes con infraestructura inicial de área de operación local o regional.

ARTÍCULO 7. Las solicitudes deberán estar acompañadas de los siguientes documentos y requisitos:

a) Identificación y generales de ley del solicitante;
b) Descripción detallada de cada servicio propuesto;
c) Anteproyecto técnico para demostrar su factibilidad;
d) Requerimientos de conexión; y,
e) Certificado de la Superintendencia de Telecomunicaciones respecto de la prestación de servicios de telecomunicaciones del solicitante y sus accionistas incluida la información de imposición de sanciones en caso de haberlas.
f) En caso de renovación del permiso. La certificación de cumplimiento de obligaciones establecidas en el Permiso, por parte de la Secretaría Nacional de Telecomunicaciones y de la Superintendencia de Telecomunicaciones, a demás de la información de imposición de sanciones por parte de la Superintendencia.

La información contenida en los literales b), c), e) será considerada confidencial. Para el caso de pedido de ampliación de los servicios o el sistema, la Secretaría requerirá del solicitante la información de amparadas en los literales b), c) y d) de este artículo.

ARTÍCULO 8. El anteproyecto técnico, elaborado y suscrito por un ingeniero en electrónica y telecomunicaciones debidamente colegiado, contendrá:

a) Diagrama esquemático y descripción técnica detallada del sistema;
b) Descripción de los enlaces requeridos hacia y desde el o los nodos principales para el transporte de información internacional necesaria para la prestación de su servicio y entre los nodos principales y secundarios para el caso de enlaces nacionales en caso de requerirlo;
c) Identificación de requerimientos de espectro radioeléctrico, solicitando el título habilitante respectivo según los procedimientos determinados en el reglamento pertinente. Para efectos de conexión se aplicará lo dispuesto en el respectivo reglamento;
d) Ubicación geográfica inicial del sistema, especificando la dirección de cada nodo;
e) Descripción técnica de cada nodo del sistema.

ARTÍCULO 9. El título habilitante para la prestación de servicios de valor agregado especificará por lo menos lo siguiente:

a) Objeto;
b) La descripción técnica del sistema que incluya, infraestructura de transmisión, forma de acceso de conexión con las redes existentes;
c) Descripción de los servicios autorizados, duración, alcance y demás características técnicas específicas relativas a la operación de los servicios de valor agreado;
d) Las causales de extinción del permiso.

ARTÍCULO 10. No se otorgarán permisos de operación de índole genérica, abierta o ilimitada. Cuando la naturaleza de los servicios de valor agregado que proveerá el solicitante sea diferente, se requerirá de un permiso expreso por cada servicio.

CAPÍTULO III

DEL TRÁMITE DE LOS TITULOS HABILITANTES Y SUS AMPLIACIONES

ARTÍCULO 11. El procedimiento y los plazos máximos para el otorgamiento de títulos habilitantes para la prestación de servicios de valor agregado seguirán lo establecido en el Reglamento General a la Ley Especial de Telecomunicaciones Reformada.

ARTÍCULO 12. En el caso que el permisionario requiera ampliar o modificar la descripción técnica o la ubicación geográfica inicial del sistema deberá presentar la solicitud correspondiente a la Secretaría Nacional de Telecomunicaciones. El Secretario Nacional de Telecomunicaciones autorizará la ampliación o modificación mediante acto administrativo y se procederá a su respectivo registro, así como notificar a la Superintendencia de Telecomunicaciones para el respectivo control.

La solicitud deberá acompañarse con la descripción técnica de la infraestructura requerida para ampliar o modificar el sistema.

ARTÍCULO 13. En caso de rechazo de una solicitud de título habilitante, modificación o ampliación, el solicitante podrá interponer las acciones o recursos previstos en el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.

ARTÍCULO 14. Lo establecido en el artículo anterior no limita el derecho del solicitante a pedir la ampliación, modificación, o aclaración de los actos administrativos emitidos por el Consejo Nacional de Telecomunicaciones o la Secretaría Nacional de Telecomunicaciones. Las solicitudes de ampliación, modificación o aclaración de los actos administrativos expedidos por el CONATEL o la Secretaría Nacional de Telecomunicaciones se resolverán en un término de 20 días laborables. En el caso que no exista pronunciamiento expreso dentro del plazo antes señalado, se entenderá por el silencio administrativo, que la solicitud ha sido resuelta en sentido favorable al peticionario.

ARTÍCULO 15. Los solicitantes cuyos medios de transmisión incluyan el uso de espectro radioeléctrico, deberán solicitar el título habilitante que requieran, según la normativa vigente. La concesión para el uso de frecuencias se tramitará conjuntamente con el permiso para la prestación de servicios de valor agregado o posteriormente según las necesidades del permisionario. Cualquier ampliación que requiera de uso de espectro radioeléctrico podrá ser solicitada de acuerdo a la normativa vigente.

De conformidad con el artículo 67 del Reglamento General a la Ley Especial de Telecomunicaciones Reformada, la vigencia de la concesión del espectro radioeléctrico será hasta la fecha en que el permiso de Servicio de Valor Agregado estuviese vigente.

ARTÍCULO 16. La modificación de las características de operación de los servicios otorgados o la variación en la modalidad de los mismos, en tanto no se altere el objeto del título habilitante, requerirá de notificación escrita a la Secretaría. Caso contrario, las modificaciones propuestas deberán ser sometidas a conocimiento y resolución del Consejo Nacional de Telecomunicaciones. Una vez otorgado el permiso los cambios deberán informarse por escrito a la Secretaria Nacional de Telecomunicaciones y a la Superintendencia de Telecomunicaciones.

ARTÍCULO 17. En caso de solicitarse la autorización para más de un servicio y estos tengan naturalezas distintas entre sí, la documentación e información concerniente a la solicitud de cada título habilitante deberá ser presentada por separado a la Secretaría Nacional de Telecomunicaciones.

CAPÍTULO IV

DE LAS CONDICIONES DEL TITULO HABILITANTE, NORMAS DE OPERACIÓN Y LIMITACIONES

ARTÍCULO 18. El permisionario dispondrá del plazo de seis (6) meses para iniciar la operación; si vencido dicho plazo la Superintendencia informara a la Secretaría Nacional de Telecomunicaciones que el titular del permiso ha incumplido con esta disposición, caducará el título habilitante.

El permisionario podrá pedir, por una sola vez, la ampliación del plazo mediante solicitud motivada. La ampliación no podrá exceder de 90 días calendario. La Secretaria tendrá el plazo perentorio de 10 días para responder dicha solicitud. Ante el silencio administrativo se entenderá concedida la prórroga.

La Secretaría Nacional de Telecomunicaciones remitirá, mensualmente, a la Superintendencia de Telecomunicaciones, un listado con los permisos y las prórrogas otorgadas a fin de que la Superintendencia de Telecomunicaciones pueda verificar el cumplimiento de la presente disposición.

ARTÍCULO 19. El prestador de servicios de valor agregado no podrá ceder o transferir total ni parcialmente el título habilitante, ni los derechos o deberes derivados del mismo.

ARTÍCULO 20. Toda persona natural o jurídica que haya obtenido, de acuerdo con lo establecido en este Reglamento, un título habilitante para operar servicios de valor agregado y que a su vez tenga otros títulos habilitantes de telecomunicaciones, deberá sujetarse a las condiciones siguientes:

a. Todos los operadores deberán respetar el principio de trato igualitario, neutralidad y libre competencia. Los organismos de regulación, administración y control velarán por evitar prácticas monopólicas, de competencia desleal, de subsidios cruzados o directos y en general cualquier otra que afecte o pudiere afectar la libre competencia.

b. Todo poseedor de un título habilitante que preste varios servicios de telecomunicaciones o de valor agregado estará obligado a prestarlos como negocios independientes y, en consecuencia, a llevar contabilidades separadas que reflejen sus estados financieros. Quedan prohibidos los subsidios cruzados.

CAPÍTULO V

DE LA INFRAESTRUCTURA DE TRANSMISIÓN

ARTÍCULO 21. Los permisionarios para la prestación de servicios de valor agregado tendrán el derecho a conexión internacional, desde y hacia sus nodos principales, para el transporte de la información necesaria para la prestación de sus servicios y podrá realizarlo bajo cualquiera de las modalidades siguientes:

a. Infraestructura propia.- Para lo cual deberá especificarlo en la solicitud adjuntando el diagrama y especificaciones técnicas y conjuntamente deberá tramitar la obtención del titulo habilitante correspondiente necesario para su operación no pudiendo ser alquilada su capacidad o infraestructura a terceros sin un título habilitante para la prestación de servicios portadores.

b. Contratar servicios portadores.- Para lo cual deberá señalar en la solicitud correspondiente la empresa de servicios portadores que brindará el servicio.

ARTÍCULO 22. Los permisionarios para la prestación de servicios de valor agregado tendrán el derecho a conexión desde y hacia sus nodos principales y secundarios y entre ellos, para el transporte de la información necesaria para la prestación de sus servicios y podrá realizarlo bajo cualquiera de las modalidades siguientes:

a. Infraestructura propia.- Para lo cual deberá especificarlo en la solicitud adjuntando el diagrama y especificaciones técnicas y conjuntamente deberá tramitar la obtención del titulo

habilitante correspondiente necesario para su operación no pudiendo ser alquilada su capacidad o infraestructura a terceros sin un título habilitante para la prestación de servicios portadores.

b) Contratar servicios portadores.- Para lo cual deberá declarar en la solicitud correspondiente la empresa de servicios portadores que brindará el servicio.

ARTÍCULO 23. Los permisionarios para la prestación de servicios de valor agregado tendrán derecho de acceso a cualquier Red Pública de Telecomunicaciones autorizada de conformidad con las normas de conexión vigentes y las disposiciones de este Reglamento y del Reglamento General a la Ley Especial de Telecomunicaciones Reformada, para lo cual deberán suscribirse los respectivos acuerdos de conexión.

CAPITULO VI

DE LAS MODALIDADES DE ACCESO

ARTÍCULO 24. Los permisionarios para la prestación de servicios de valor agregado, para acceder a sus usuarios finales con infraestructura propia, requerirán de un título habilitante para la prestación de servicios finales o portadores de acuerdo con el tipo de servicio de valor agregado a prestar.

Artículo 25. Sin perjuicio de regular modalidades de acceso para diferentes servicios de valor agregado, se regulan específicamente las siguientes:

a. Los permisionarios proveedores de servicios de Internet:

1. Podrán acceder a sus usuarios a través de servicios portadores y/o finales.
2. Podrán acceder a sus usuarios mediante el uso de infraestructura propia siempre y cuando obtengan el título habilitante para la prestación de servicios portadores y/o finales.

b. Los permisionarios prestadores de los servicios KIOSKO (0-900) y VOTACIÓN DE SONDEO Y OPINIÓN (TELEVOTO 0-805) de plataforma inteligente podrán acceder a sus usuarios por medio de servicios de finales. Para tal efecto, celebrarán los correspondientes convenios de conexión, de conformidad con las normas aplicables.

CAPÍTULO VII

DE LAS TARIFAS Y LOS DERECHOS

ARTÍCULO 26. Las tarifas para los servicios de valor agregado serán libremente acordadas entre los prestadores de Servicios de Valor Agregado y los usuarios. Sólo cuando existan distorsiones a la libre competencia en un determinado mercado el Consejo Nacional de Telecomunicaciones podrá regular las tarifas.

ARTÍCULO 27. Todo permisionario para la prestación de servicios de valor agregado deberá cancelar previamente a la Secretaría Nacional de Telecomunicaciones, por concepto de derechos de permiso, el valor que el Consejo Nacional de Telecomunicaciones determine para cada tipo de servicio.

ARTÍCULO 28. Los costos de administración de contratos, registro, control y gestión serán retribuidos mediante tasas fijadas por los organismos de control y de administración, en función de los costos administrativos que demanden dichas tareas para cada uno de los organismos, como recursos de dichas instituciones.

CAPÍTULO VIII

DERECHOS Y OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE VALOR AGREGADO

ARTÍCULO 29. Los prestadores de servicios de valor agregado no podrán exigir el uso exclusivo de determinado equipo. El prestador se obliga a permitir la conexión a sus instalaciones, de equipos y aparatos terminales propiedad de los clientes, siempre que éstos sean técnicamente compatibles con dichas instalaciones.

ARTÍCULO 30 . Los prestadores de servicios de valor agregado garantizarán la privacidad y confidencialidad del contenido de la información cursada a través de sus equipos y sistemas.

ARTÍCULO 31. En caso de comprobarse el cometimiento de actos contrarios a la libre competencia, previo informe de la Superintendencia de Telecomunicaciones, la Secretaría Nacional de Telecomunicaciones procederá a la terminación unilateral del título habilitante.

ARTÍCULO 32. El concesionario de cualquier Red Pública de Telecomunicaciones sobre la cual se soporten Servicio de Valor Agregado, no podrá exigir que los equipos y sistemas de los prestadores del Servicio, sean ubicadas dentro de sus instalaciones. Igualmente el prestador de Servicio de Valor Agregado no podrá exigir que sus equipos y sistemas sean ubicados dentro de las instalaciones del operador de la red pública de telecomunicaciones.

ARTÍCULO 33. Cualquier concesionario para la prestación de servicios de telecomunicaciones portadores o finales, sobre cuyas redes se soporten servicios de valor agregado y que prevea modificar sus redes, de manera que afecte la prestación de los servicios de valor agregado, deberá informar con un plazo no inferior a los tres (3) meses anteriores a dicha modificación, a los prestadores de servicios de valor agregado que se soporten sobre dichas redes. De incumplirse con la presente disposición el operador de la red pública de telecomunicaciones será responsable de los daños y perjuicios causados a los prestadores de servicios de valor agregado incluido el lucro cesante y daño emergente, sin perjuicio de las sanciones a que hubiere lugar de conformidad con el título habilitante y el ordenamiento jurídico.

CAPÍTULO IX

DE LOS DERECHOS Y DEBERES DE LOS USUARIOS

ARTÍCULO 34. Sin perjuicio de otros derechos reconocidos por los contratos y el ordenamiento jurídico vigente, se reconocen especialmente los siguiente derechos y obligaciones del usuario:

a. El usuario tiene derecho a recibir el servicio de acuerdo a los términos estipulados en el contrato de suscripción de servicio.

b. El contrato seguirá un modelo básico que se aplicará a todos los usuarios previo registro en la Secretaría Nacional de Telecomunicaciones.

   No se procederá al registro del modelo de contrato en caso de existir una cláusula lesiva a los derechos de los usuarios. De la decisión denegatoria de registro expedida por Secretaría Nacional de Telecomunicaciones, el permisionario podrá recurrir ante el Consejo Nacional de Telecomunicaciones.

c. Los usuarios corporativos de los Servicios de Valor Agregado, acceso al Internet, deberán suscribir el contrato para la respectiva red de acceso con operadores finales y/o portadores debidamente autorizados.

d. El usuario tiene derecho a un reconocimiento económico que corresponda al tiempo en que el servicio no ha estado disponible, cuando la causa fuese imputable al prestador del servicio de valor agregado, que será por lo menos un equivalente al precio que el usuario hubiere pagado por ese tiempo de servicio de acuerdo a la tarifa acordada con el prestador

del Servicio de Valor Agregado. El usuario tiene la obligación de pagar puntualmente los valores facturados por el servicio en el lugar que el operador establezca.

e. El usuario tiene derecho a que, cuando el Superintendente de Telecomunicaciones resuelva que se suspendan los pagos de sus planillas, él pueda seguir recibiendo el servicio, dejando pendiente de pago su planilla.

f. El usuario tiene derecho a reclamar por la calidad del servicio, por los cobros no contratados, por elevaciones de tarifas por sobre los valores máximos aprobados por el Consejo Nacional de Telecomunicaciones, en el caso de que se los fijara y por cualquier irregularidad en relación con la prestación del servicio proporcionado por el prestador, ante la Superintendencia de Telecomunicaciones

CAPÍTULO X

DE LA EXTINCIÓN

ARTÍCULO 35. A más de las causales previstas en los artículos 18 y 31 del presente Reglamento, los títulos habilitantes podrán extinguirse con las condiciones establecidas en los mismos y, las que consten en el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.

ARTÍCULO 36. El incumplimiento por parte de un prestador de Servicio de Valor Agregado, de los procedimientos y obligaciones establecidos en este Capítulo, dará lugar a la terminación unilateral del Permiso por parte del CONATEL, previo informe de la Superintendencia de Telecomunicaciones y la Secretaría Nacional de Telecomunicaciones..

CAPÍTULO XI

DE LA REGULACIÓN Y CONTROL

ARTÍCULO 37. La operación de servicios de valor agregado esta sujeta a las normas de regulación, control y supervisión, atribuidas al Consejo Nacional de Telecomunicaciones, la Secretaría Nacional de Telecomunicaciones y la Superintendencia de Telecomunicaciones, de conformidad con las potestades de dichos organismos establecidas en la Ley.

ARTÍCULO 38. La Superintendencia de Telecomunicaciones podrá realizar los controles que sean necesarios a los prestadores de servicios de valor agregado con el objeto de garantizar el cumplimiento de la normativa vigente y de los términos y condiciones bajo los cuales se hayan otorgado los títulos habilitanes, y podrá supervisar e inspeccionar, en cualquier momento, las instalaciones de los Prestadores y eventualmente de sus usuarios, a fin de garantizar que no estén violando lo previsto en el presente Reglamento. Los Prestadores deberán prestar todas las facilidades para las visitas de inspección a la Superintendencia y proporcionarles la información indispensable para los fines de control.

DISPOSICIONES FINALES

PRIMERA. Los beneficiarios de permisos de Servicio de Valor Agregado otorgados con anterioridad a la fecha de vigencia del presente Reglamento podrán adecuarse a disposiciones establecidas en este Reglamento.

SEGUNDA. La Secretaría nacional de Telecomunicaciones elaborará, en el plazo de treinta (30) días para la aprobación del Consejo Nacional de Telecomunicaciones, el listado de los servicios de plataforma inteligente y sus características.

TERCERA. Esta resolución deroga el “Reglamento para la Prestación de Servicios de Valor Agregado”, aprobada mediante Resolución 35-13-CONATEL-96, publicado en el Suplemento del Registro Oficial 960 de 5 de junio 1996.

DISPOSICIONES TRANSITORIAS

El presente Reglamento entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en Quito 20 de febrero del 2002.

ANEXO 2

CATÁLOGO DE EQUIPOS PROPUESTOS

3Com Switch 4500 10/100 Family

DATA SHEET

Enables **Secure Converged Networks** with:

- End-to-end network security
- Smart PoE for convergence of VoIP and wireless LAN mobility
- Layer 2/3 switching and routing
- Scalable up to 384 users per stack

Product Overview

The 3Com® Switch 4500 family of managed, stackable 10/100 Ethernet switches provides secure, flexible LAN connectivity for enterprise and branch office networks. The Switch 4500 family offers Layer 2 switching and dynamic Layer 3 routing, as well as robust security, quality of service (QoS), and management features to deliver intelligent edge connectivity for essential business applications.

Four new switch models – stackable in any combination up to eight units – include:

- **3Com Switch 4500 26-Port**: 24 10/100 ports plus 2 dual-personality Gigabit ports
- **3Com Switch 4500 50-Port**: 48 10/100 ports plus 2 dual-personality Gigabit ports
- **3Com Switch 4500 PWR 26-Port**: 24 10/100 Power over Ethernet ports plus 2 dual-personality Gigabit ports
- **3Com Switch 4500 PWR 50-Port**: 48 10/100 Power over Ethernet ports plus 2 dual-personality Gigabit ports

Secures the Network

Essential security features provide user and device authentication, enforce access control for switch management, and enhance overall network security to protect critical resources and information.

The Switch 4500 also functions as an integral part of the 3Com Quarantine* solution, enabling automatic containment of security threats.

Empowers Application Convergence

The Switch 4500 family combines high performance switching, quality of service (QoS), and advanced traffic management features to ensure essential applications get priority. Additionally, 3Com Smart PoE delivers intelligent power management with dynamic allocation of available power resources.

Reduces Deployment Costs

Power over Ethernet provides electrical power and data connectivity over a single Ethernet cable - resulting in significant cost savings when deploying devices like IP phones, wireless access points, and IP security cameras.

Increases Flexibility and Scalability

The Switch 4500 family employs a flexible design with user-configurable "dual personality" Gigabit Ethernet interfaces, and the ability to stack up to eight switch units (384 10/100 connectivity ports) that can be managed as a single entity.

Enhances Management and Control

Easy to use and manage, the Switch 4500 family is designed to increase business productivity by reliably supporting business applications that drive productivity improvements.

* For details on the 3Com Quarantine solution, see http://www.3com.com/other/pdfs/products/en_US/3Com-400915.pdf

Key Benefits

Security
The Switch 4500 family ensures secure access to resources using standard 802.1X network access control combined with RADIUS authentication. Additionally, RADIUS Authenticated Device Access (RADA) enables authentication of attached devices via MAC address for an additional level of endpoint security. Port-based Access Control Lists (ACLs) effectively enable usage policies at each point of access to the network via the switch.

Secure Shell (SSHv2) and SNMPv3 support ensure secure management access to switches via authentication and encryption of management traffic.

Dynamic Voice over IP
Unique Voice VLAN feature detects the presence of IP phones* and dynamically assigns switch ports to the Voice VLAN, enabling automated configuration and prioritization of VoIP traffic. This powerful feature minimizes cost and complexity associated with adding or moving IP phones.

Performance
Designed for high-performance network connectivity, the Switch 4500 family features 26-port and 50-port models providing aggregate switching capacity up to 8.8 Gbps and 13.6 Gbps, respectively. Dual Gigabit uplinks on each switch unit enable high-speed connections to the network backbone or locally attached servers.

Prioritization and Bandwidth Management
Eight priority queues per port enable 802.1p Class of Service / Quality of Service (CoS/QoS). Bandwidth rate limiting and protocol filtering capabilities allow the Switch 4500 family to enforce controls on each port for efficient use of network resources and prioritization of "business-critical" or "time-sensitive" applications, including Voice over IP (VoIP).

Power over Ethernet (PoE)
Two models in the Switch 4500 family provide inline power to attached devices via industry-standard 802.3af Power over Ethernet (PoE). The internal power supply provides a power budget of 300 Watts, which is dynamically allocated to PoE ports. Supplemental power can be provided by an optional external DC power system, supplying up to 15.4 Watts of power to all PoE ports in a switch or stack.

Flexibility and Scalability
Two Gigabit ports on each model of the Switch 4500 family may be used for stacking or for high-speed uplink connectivity to the network backbone or to locally attached servers. Each Gigabit port offers a choice of copper or fiber media: 1000Base-T (via RJ45) or 1000Base-X (via optional "SFP" Small Form Factor Pluggable transceiver modules).

Stacking capability allows up to 8 units to be combined in a single managed stack, scaling up to as many as 384 10/100 ports. A comprehensive set of switching features, including multicast filtering and Rapid Spanning Tree Protocol support, act to further improve scalability and availability of network resources.

Management and Control
The Switch 4500 family is powered by the 3Com Operating System, the same proven software featured in 3Com premium enterprise switches - including the Switch 5500, Switch 7700, and Switch 8800 families. Network configuration and control features are accessible via command line interface (CLI), or by using SNMP management software such as 3Com Enterprise Management Suite (EMS) and 3Com Network Director.

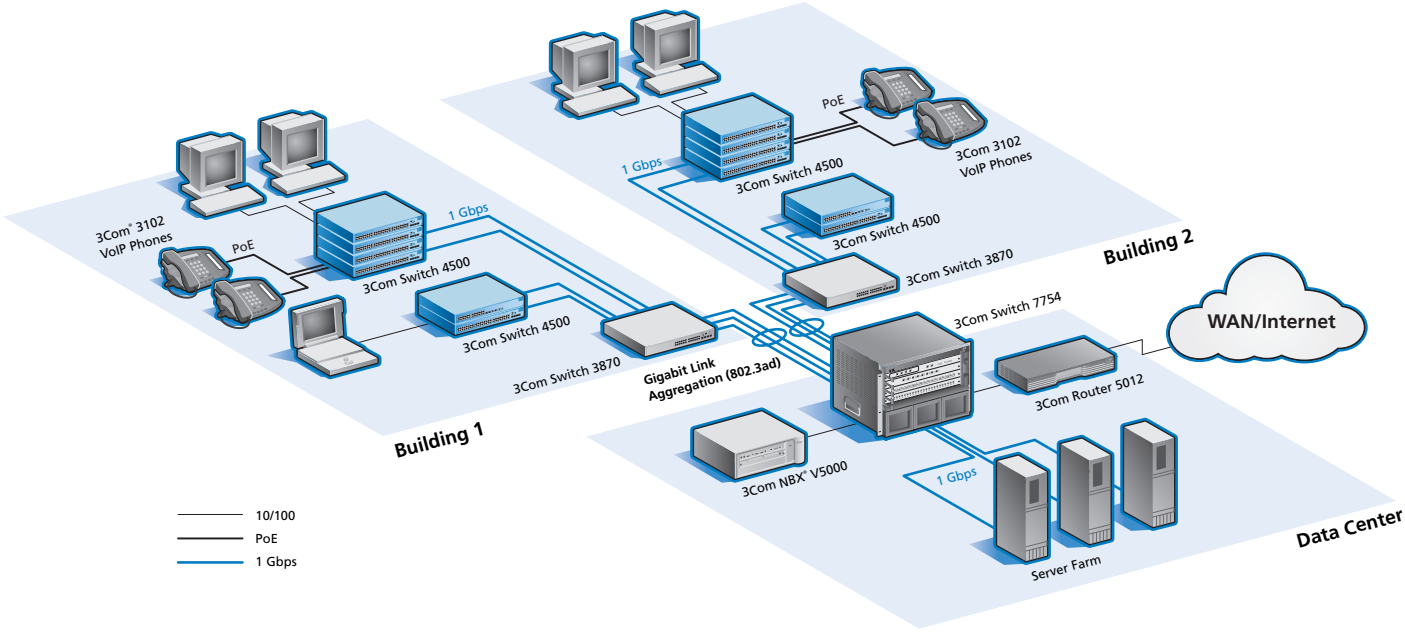
Ease of Use
Dynamic routing with RIP (Routing Information Protocol) allows automatic updating of Layer 3 network topologies. Speed and duplex mode on all ports are negotiated automatically, preventing the possibility for improper configuration. Switches detect and adjust to cross-over or straight through cable connections via "Auto MDI/MDIX" feature, eliminating the need for different cables to interconnect network devices.

Limited Lifetime Hardware Warranty
Limited Lifetime Hardware Warranty with Advance Hardware Replacement. See **www.3com.com/warranty** for details.

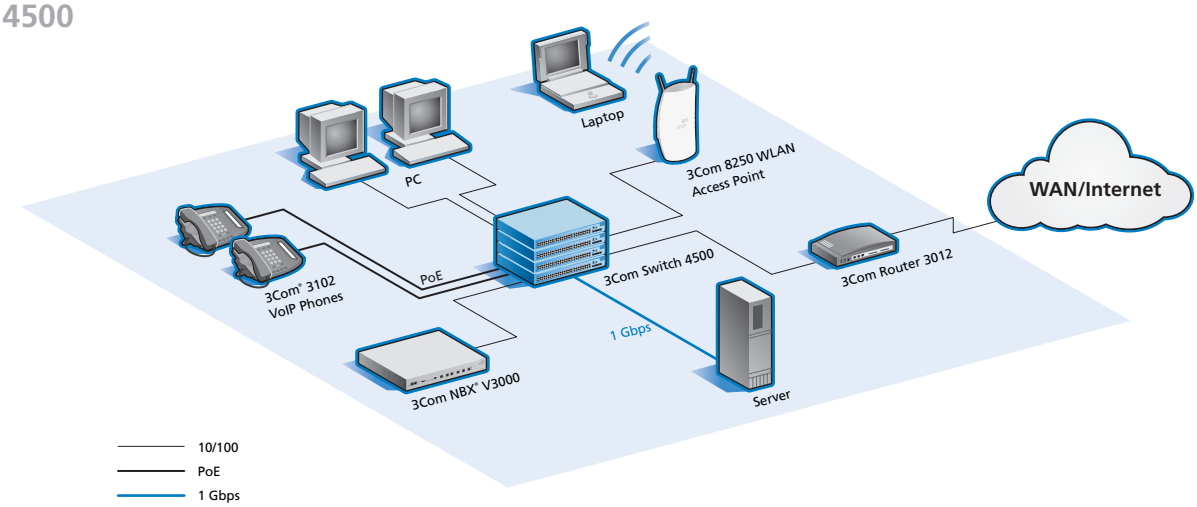
Service and Support
3Com products are backed by 3Com Global Services and authorized partners with demonstrated expertise in network assessment, implementation, and maintenance. Ask about 3Com's Network Health Check, installation services, and maintenance service packages available in your area.

* By default, the Switch 4500 will automatically recognize and classify IP phones from 3Com, Cisco, Pingtel, and Polycom. Additional manufacturer profiles can be defined by the user.

Sample campus LAN configuration supported by the Switch 4500



Sample small to medium LAN configuration supported by the Switch 4500



Features

PERFORMANCE	
Switching capacity, maximum	50-port models: 13.6Gbps; 26-port models: 8.8 Gbps
Forwarding rate, maximum	50-port models: 10.1Mpps; 26-port models: 6.5 Mpps Wirespeed performance across all ports within stack or fabric Store-and-forward switching; latency <10 µs
Stacking bandwidth	2 Gbps full-duplex stacking
LAYER 2 SWITCHING	
MAC address	8K MAC addresses Static MAC addresses: 12 in addition to the default address
VLAN	IEEE 802.1Q Port-based VLANs: 256
Link aggregation	IEEE 802.3ad Link Aggregation Control Protocol (LACP) Manual aggregation Trunk groups: 25 groups (50-port); 13 groups (26-port) 8 10/100 ports or 2 Gigabit ports per group
Auto-negotiation	Auto-negotiation of port speed and duplex
Traffic control	IEEE 802.3x full-duplex flow control Back pressure flow control for half-duplex
Spanning Tree/Rapid Spanning Tree	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) BPDU (Bridge Protocol Data Unit) protection included in Fast Start
Multicast snooping	Internet Group Management Protocol (IGMP) v1 and v2 snooping IGMP Querier Filtering for 128 multicast groups
LAYER 3 SWITCHING	
Routes	Hardware-based routing Static routes: 12 in addition to the default address Dynamic / static ARP (Address Resolution Protocol) entries : 1990 / 10
IP routing	IP interfaces: 4 RIP (Routing Information Protocol), v1 and v2: 2K via default route plus 10 locally learned routes
Multicast Routing	IGMP v1 and v2 snooping
Network protocol	DHCP Relay (Dynamic Host Configuration Protocol Relay): 2 KB max
STACKING	
Stacking	Eight units, or 384 Fast Ethernet ports Single IP address and management interfaces for stack-wide control
CONVERGENCE	
Priority queues	Eight hardware queues per port
Traffic prioritization	IEEE 802.1p Class of Service/Quality of Service (CoS/QoS) on egress DSCP EF (DiffServ Code Point Expedited Forwarding) for prioritization of VoIP traffic
Queue handling	Weighted Round Robin
Traffic shaping	Egress rate limiting, port-based Application and protocol blocking
SECURITY	
Network login	IEEE 802.1X user authentication: RADIUS authentication, multiple users per port by locking to the MAC address, automatic port assignment of VLANs, multiple RADIUS server realm definitions RADIUS Authenticated Device Access (RADA): authenticate devices based on MAC address against RADIUS server, authenticate multiple devices per port, automatic assignment of VLANs to a port specific to the devices attached PAP, CHAP, EAPoL (EAP over LAN) authentication, for multiple users per port and 1,024 users per fabric Port-based MAC address lockdown using Disconnect Unknown Device (DUD) with continuous learning
Packet filtering	Wirespeed packet filtering in hardware Layer 2/3/4 ACL filters: source and/or destination MAC address, 16-bit Ethertype, source and/or destination IP address, TCP source and/or destination port, UDP source and/or destination port
Switch protocol security	MD5 cipher-text authentication and clear-text authentication for RIP v2 packets and SNMP v3 traffic Trusted MAC and IP address Concurrent sessions; four access-privilege levels

Features, *continued*

Switch management	IEEE 802.1X network administrator authentication
	Secure management via SSH v2.0 or SNMPv3
	Management activity logs automatically recorded for detailed analysis
	Administrative password recovery
MANAGEMENT	
System configuration and management	CLI (Command Line Interface) via the console port or Telnet
	Embedded web management interface
	System configuration with SNMP v1, 2, and 3
	RMON (Remote Monitoring) groups: statistics, history, alarm, and events
	ACL/QoS statistics
	Comprehensive IP interface statistics and rates
Traffic redirection	1-to-1 port mirroring
	Ability to apply QoS profile to mirror port, forwarding only certain traffic types and preventing over-subscription of copy port
System maintenance	Detailed alarm/debug information
	Supports ping and traceroute
	Backup and restore of software image
	Network debugging tools: DHCP Relay, UDP Helper
	Multiple configuration file support
System file transfer mechanisms	Xmodem
	FTP (File Transfer Protocol)
	TFTP (Trivial File Transfer Protocol)
3Com Management Applications	3Com Network Director for comprehensive, turn-key network management for the enterprise.
	3Com Network Supervisor for basic, turnkey network management for small and medium businesses
	3Com Enterprise Management Suite for flexible, extensible management in advanced enterprise IT environments
POWER	
IEEE 802.3af Power over Ethernet (PoE)	DC power injection into Category 5 or 5e LAN wiring (PWR models only)
DC Supplemental Power System	Available Standards-based DC power supply from leading provider of integrated power systems
	(Provides supplemental DC power injection for Switch 4500 PWR models)

OPTIONAL SERVICE AND SUPPORT	
Network Health Check	An activity-auditing service focused on improving network performance and productivity
	Includes traffic monitoring, utilization analysis, problem identification, and asset deployment recommendations
	Extensive report provides blueprint for action
Network Design	Includes review of business plan, extensive inventory of requirements, and complete design document specifying implementation details
Network Installation	Experts set up and configure equipment and integrate technologies to maximize functionality and minimize business disruption
	Service may include physical site survey, network design, and engineering based on evaluation of business objectives
Project Management	Provides extra focus and resources that special projects demand
	3Com personnel manage entire process from initial specifications to post-project review
	Using structured methodology, requirements are identified, projects planned, and progress of implementation activities tracked
3Com Guardian℠ Maintenance Service	Provides comprehensive onsite support, including advance hardware replacement, telephone technical support, and software upgrades: • Telephone support backed by powerful call-tracking database and replication laboratory • Software upgrades ensure access to pertinent patches
3Com Express℠ Maintenance Service	Benefits customers who prefer to maintain own hardware
	Bolsters in-house resources with convenient and speedy access to 3Com hardware replacements, software upgrades, and telephone support

Specifications

All information in this section is relevant to all members of the 3Com Switch 4500 10/100 family, unless otherwise stated.

Connectors
24 or 48 auto-negotiating 10BASE-T/100BASE-TX ports configured as auto MDI/MDIX

2 dual-personality Gigabit port pairs: user configurable for RJ45 (copper) or SFP-based (fiber) interfaces.

RJ-45 console port

PWR switch models include IEEE 802.3af in-line power on all 10Base-T/100Base-TX ports and support redundant power supply (-48 VDC) connector

Security
RADIUS authentication

RADIUS session accounting

SSH v2.0

IEEE 802.1X network login

Access Control Lists (ACL)

Packet filtering

Private Ports

SNMP v3 encryption

Stacking
Up to 384 10/100 front panel ports

Performance
26-port
8.8 Gbps switching capacity, maximum

6.5 Mpps forwarding rate, maximum

8,000 MAC addresses supported

50-port
13.6 Gbps switching capacity, maximum

10.1 Mpps forwarding rate, maximum

8,000 MAC addresses supported

Reliability
(MTBF @ 25˚C)

26-port: 47 years (411,000 hours)

26-port PWR: 25 years (221,000) hours)

50-port: 38 years (334,000 hours)

50-port PWR: 22 years (189,000 hours)

Dimensions
Height: 43.6 mm (1.7 in or 1U)

Width: 440 mm (17.3 in)

Depth:
Non-PWR models: 270 mm (10.6 in)
PWR models: 427 mm (16.8 in)

Weight:
Non-PWR models: 3.3 kg (7.3 lb)
PWR models: 6.3 kg (13.9 lb)

Power Supply
AC Line Frequency: 50/60 Hz

Input Voltage: 90-240 VAC

Current Rating: 1.0A maximum

Environmental Requirements
Operating temperature: 0° to 40°C (32° to 104°F)

Storage temperature: -10° to 70°C (14° to 158°F)

Humidity (operating and storage): 10% to 95% non-condensing

Standard: EN 60068 (IEC 68)

Industry Standards Supported
IEEE 802.1D (STP)

IEEE 802.1p (CoS)

IEEE 802.1Q (VLANs)

IEEE 802.1w (RSTP)

IEEE 802.1X (Security)

IEEE 802.3 (Ethernet)

IEEE 802.3ad (Link Aggregation)

IEEE 802.3ab (1000BASE-T)

IEEE 802.3af (Power over Ethernet)

IEEE 802.3i (10BASE-T)

IEEE 802.3u (Fast Ethernet)

IEEE 802.3x (Flow Control)

IEEE 802.3z (Gigabit Ethernet)

IETF Standards
Management, including MIBs Supported
RFC 1213/2233 (MIB II)

RFC 1724 (RIP Version 2 MIB Extension)

RFC 1907 (SNMP v2c, SMI v2 and Revised MIB-II)

RFC 2021 (RMON II Probe Config MIB)

RFC 2233 (Interfaces MIB)

RFC 2571 (FrameWork)

RFC 2571-2575 (SNMP)

RFC 2613 (Remote Network Monitoring MIB Extensions)

RFC 2665 (Pause control)

RFC 2668 (IEEE 802.3 MAU MIB)

RFC 2674 (VLAN MIB Extension)

RFC 2819 (RMON MIB)

Emissions / Agency Approvals
CISPR 22 Class A

FCC Part 15 Class A

EN 55022 1998 Class A

ICES-003 Class A

VCCI Class A

EN 61000-3-2 2000, 61000-3-3

Immunity
EN 55024

Safety Agency Certifications
UL 60950

IEC 60950-1

EN 60950-1

CAN/CSA-C22.2 No. 60950-1-03

Management
SNMP and Telnet support

RMON Groups: Statistics, History, Alarms and Events

Statistics gathering and reporting

Command line interface

Management through 3Com management applications

- 3Com Network Supervisor

- 3Com Network Director

- 3Com Enterprise Management Suite

Warranty
Limited Lifetime Hardware Warranty with Advance Hardware Replacement, including Power Supply and fans. Limited Software Warranty for ninety (90) days. See www.3com.com/warranty for details.

Other Benefits
90 days of telephone technical support.

See www.3com.com/warranty for more detail.

Register products at http://eSupport.3com.com.

Service
Americas:
www.3com.com/products/en_US/global_services

International:
http://emea.3com.com/globalservices

Quidway® S3900 Series Intelligent and Resilient Switches

Quidway® S3900 Series Ethernet Switches are a new line of premier multi-layer switches that entirely fulfills the enterprise customers' requirement of designing and implementing a unified, highly resilient network. One of the most important and innovative highlights of the S3900 Series Ethernet Switches is the IRF technology (Intelligent Resilient Framework) which presents the very real advantage of stackable technology. IRF is a completely innovative technology, allowing network managers to build affordable networks with high resilience, flexibility and exceptional performance.

With flexible software options, the Quidway® S3900 Series Switches are available in the Standard Software Image (SI) and the Enhanced Software Image (EI), offering a cost-effective path for meeting current and future service requirements from enterprises and commercial businesses. The SI feature set includes advanced quality of service (QoS), rate-limiting, access control lists (ACLs), static and Routing Information Protocol (RIP) routing, and basic IRF function. In addition to these features, the EI feature set provides even richer enterprise-class features such as advanced hardware-based IP unicast, multicast routing, and advanced IRF functionality.

S3924-SI

S3928P-SI / S3928P-EI / S3928P-PWR-EI

S3952P-SI / S3952P-EI / S3952P-PWR-EI

S3928TP-SI

S3928F-EI

The Quidway® S3900 Series marks a new milestone in switches with the revolutionary Intelligent Resilient Framework technology

Product Specifications

IRF Technology

Intelligent Resilient Framework (IRF) is an innovative resilient network technology that allows enterprise customers to design and implement Fast Ethernet core and aggregation backbones that are affordable, providing exceptional performance, scalability and availability. With IRF technology, the Quidway® S3900 Series switches can be interconnected together to behave as a single logical switching entity called a Distributed Fabric. From management and configuration perspectives, the Fabric appears as a single device, while from a performance perspective, each switch in the Distributed Fabric can make its own forwarding decisions, both at Layer 2 and Layer 3 for traffic that appears on its ports.

Distributed Device Management (DDM)

Distributed Device Management is the control system for IRF technology, responsible for distributing management and control information across the IRF Distributed Fabric. DDM allows the entire IRF Distributed Fabric to be managed as a single logical entity. Management tasks are all performed across the Distributed Fabric, minimizing complexity and administration overheads. In addition, the management IP address is shared across all units in the IRF Distributed Fabric, ensuring continuous device management and monitoring, in the event of an outage in one of the interconnected switches.

Distributed Resilient Routing (DRR)

Distributed Resilient Routing, provided by Enhanced Image, is an advanced routing implementation that allows multiple interconnected switches in an IRF Distributed Fabric to behave as a single active routing entity. Unlike resilient Layer 3 implementations such as VRRP and HSRP, DRR intelligently distributes the routing load across all switches in the Distributed Fabric to optimize routing performance and make full use of bandwidth capacity.

Distributed Link Aggregation (DLA)

Distributed Link Aggregation, provided by Enhanced Image, allows networks and IRF Distributed Fabrics to be coordinated with switches at the edge of the network. With the ability to multi-home across different units in the IRF Distributed Fabric, the availability of the entire network is dramatically increased. Traffic is forwarded across all links in the Aggregated Link to the fabric to optimize the use of available capacity. DLA guarantees high levels of resiliency since failure in one of the members of the Aggregated Link results in automatic redistribution of traffic across the remaining links.

Excellent PoE(Power over Ethernet) Supply Function

The Quidway® S3900 Series Switches support PoE function for the LAN switching infrastructure, which provides power over a copper Ethernet cable to an endpoint (Powered Device). With the Quidway® S3900, up to 48 simultaneous full-fowered

10/100M PoE Ports at 15.4W ensures maximum device support for IP telephony and wireless LAN deployments. As PSE (Power Sourcing Equipment) devices, all Quidway® S3900 series are 802.3af compliant PoE switches. With PoE and Voice VLAN technology, these innovative switches can provide the perfect solution for a converged voice and data network.

Full wire-speed, multi-layer switching

The Quidway® S3900 Series offer L2/L3 wire-speed switching capability for all ports. The system offers 4 GE to meet one piece of equipment's requirement for multiple Gigabit uplinks and for access to the Gigabit server, thus great increase savings on equipment investment. The hardware supports L3 wire-speed switching, and is able to identify and process the application traffic flows from L2~L7. All ports have an independent data packet filter, and distinguish different application flows for different management and control.

Flexible security control policies

Based on the longest match routing policy, the Quidway® S3900 Series forward packets one by one ensuring equal forwarding performance. This function can guard the network against the attack by Code Red and Worm Blaster, thereby guaranteeing equipment security.

The Quidway® S3900 Series support 802.1x authentication to identify users who attempt to access the network. They can also prevent unauthorized access to the network by binding any combination of MAC, IP, VLAN and PORT.

Secure Shell (SSH) offers security information protection and powerful authentication function to safeguard the Ethernet switch from attacks such as IP address spoofing and plain text cipher interception.

High reliability

The Quidway® S3900 series support STP/RSTP and multi-VLAN based MSTP, greatly improving redundant back-up for links and fault tolerance capability, so that the network can run with stability.

The Quidway® S3900 Series support the optional RPS (Redundant Power Supply, provided by Enhanced Image) and can provide power redundancy for up to eight switches simultaneously, thus improving the fault tolerance capability and normal network operation duration.

The Quidway® S3900 series support VRRP (provided by Enhanced Image), and can build a VRRP back-up group with other L3 switches. They can build a redundant route topological structure when a fault occurs to guarantee communication continuity and reliability, keeping network status stable.

The Quidway® S3900 series implement redundant back-up routes by configuring multiple equivalent routes. When the active uplink route becomes faulty, it will automatically switch to the next back-up router, thus achieving multi-level back-up for uplink routes.

Abundant QoS policies

The Quidway® S3900 Series support L2~L7 complex flow classification based on source MAC address/destination MAC address/source IP address/destination IP address/ports/protocols.

The Quidway® S3900 Series support flexible queue scheduling algorithms, which can be set on the basis of port and queue at the same time. They support Strict Priority (SP), Weighted Round Robin (WRR), Weighted Fair Queuing (WFQ), SP+WRR, and SP+WFQ; 8 priority queues and 2 drop precedence; WRED congestion avoidance algorithm and port traffic shaping. The Quidway® S3900 Series also support Committed Access Rate (CAR) and limit the traffic speed in the 64Kbit/s granularity.

Diversified management modes

The Quidway® S3900 Series support Simple Network Management Protocol (SNMP) and can be managed by general network management platforms such as Open View, and the Quidview® network management system. In addition, Command Line Interface (CLI), Web network management, TELNET, and HGMP cluster management make the equipment management more convenient.

Revolutionary resilient network technology that delivers high scalability, reliability, maintainability and excellent performance

Specifications

Features	S3924-SI	S3928P-SI / S3928P-EI / S3928P-PWR-EI	S3928TP-SI	S3928F-EI	S3952P-SI / S3952P-EI / S3952P-PWR-EI
Performance					
Switching Capacity	4.8 Gbps	12.8 Gbps			17.6 Gbps
Throughput	3.57 Mpps	9.53 Mpps			11.78 Mpps
SDRAM	64M				
Buffer	32M				
Stackable	N/A	YES	YES	YES	YES

Features	S3900-SI	S3900-EI
Layer 2 Switching		
MAC Address	16K MAC addresses	
Flash	8M	16M
Latency	<10μs	
VLAN	4K VLANs (IEEE 802.1Q) Voice VLAN Support Port-based VLAN	
Link Aggregation	Dynamic link aggregation (DLA) through Link Aggregation Control Protocol (LACP)	Dynamic link aggregation through LACP and across devices
	Manual link aggregation through command lines Aggregation of FE/GE ports Up to 8 FE or 4 GE ports in each aggregation	
Flow Control	IEEE 802.3x full-duplex flow control Back pressure flow control for half-duplex	
STP/RSTP/MSTP	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol instances (MSTP)	
Stack	Support maximum of 8 units Support maximum bandwidth of 4Gbps Extend to maximum of 384FE and 16GE	
	N/A	IRF Stack supports DLA. DLA supplies the capacity that multiple switches in a stack can create a link aggregation connection. Loss of an individual switch will not affect connectivity to the other switches
RPS	N/A	Support

Layer 3 Switching		
IP Routing	Static routing RIP v1, v2 (Routing Information Protocol v1, v2)	
	1K IP Routes	8K IP Routes OSPF (Open Shortest Path First) 3 ECMP (Equal Cost Multipath Policy-based Routing)
Multicast	256 Multicast Numbers IGMP (Internet Group Management Protocol) snooping	
	N/A	IGMP v1 and v2 PIM-DM PIM-SM
Network Protocol	DHCP Snooping (Dynamic Host Configuration Protocol Snooping)	N/A
	DHCP Relay (Dynamic Host Configuration Protocol Relay) DHCP Client ARP (Address Resolution Protocol) NTP (Network Time Protocol) BOOTP (Bootstrap Protocol) UDP helper	
Convergence		
Priority Queues	Eight hardware queues per port	
QoS (Quality of Service)/ ACL (Access Control List)	Support bi-directional port rate-limiting with the granularity of 64kbps Packet redirection Support CAR (Committed Access Rate) with the granularity of 64 kbps WRED (Weighted Random Early Detect/Discard) Five scheduling algorithms that can be set based on port and queue at the same time: • SP (Strict Priority) • WRR (Weighted Round Robin) • WFQ (Weighted Fair Queue) • SP + WRR • SP + WFQ Packet tagging based on 802.1p or DSCP preference L2~L7 Packet filter providing filtering based on source/destination MAC address, source/destination IP address, port, protocol, VLAN, VLAN range, MAC address range, or invalid frame Time range setting QoS profile management, allowing QoS service scheme customization	

Security	
Network Login	Support IEEE 802.1X user authentication Support Centralized MAC address authentication Support Disconnect unauthorized device (DUD) authentication Support Port isolation Support MAC address black hole Prevent unauthorized access to the network by binding any combination of MAC, IP, VLAN and PORT Support SSH (Secure Shell)
Management	
System Configuration and Management	Support CLI (Command Line Interface) configuration mode Support Configuration via the console port Support Local/Remote configuration via Telnet Support Remote configuration via modem dial-up Support System configuration with SNMP v1, 2 and 3 Support RMON (Remote Monitoring) v1, 1/2/3/9 groups of MIBs Support Quidview network management system Support WEB management system Support Hierarchical alarms Support System log Support HGMP (Huawei Group Management Protocol) v2
System Maintenance	Detailed alarm/debug information Support Ping and Traceroute Support remote maintenance via Telnet

Hardware Configuration

Attribute	S3924-SI	S3928P-SI / S3928P-EI / S3928P-PWR-EI	S3928TP-SI	S3928F-EI	S3952-P-SI/ S3952P-EI/ S3952P-PWR-EI
Fixed Ports	(1) 24 10/100 BASE-TX Ethernet ports; (2) 1 console port	(1) 24 10/100 BASE-TX Ethernet ports; (2) 1 console port	(1) 24 10/100 BASE-TX Ethernet ports; (2) 2 10/100/ 1000 BASE-T Ethernet ports (3) 1 console port	(1) 24 100BASE-FX SFP ports; (2) 2 10/100/ 1000 BASE-T Ethernet ports (3) 1 console port	(1) 48 10/100 BASE-TX Ethernet ports; (2) 1 console port
Extended Slot	N/A	(1) 4 1000M SFP extended module slots	(1) 2 1000M SFP extended module slots		(1) 4 1000M SFP extended module slots

Extended Module	(1) SFP-GE-T (2) SFP-GE-SX(0.55km) (3) SFP-GE-LX(10km) (4) SFP-GE-LH40(1310nm, 40km) (5) SFP-GE-LH40(1550nm, 40km) (6) SFP-GE-ZX70(70km) (7) SFP-FE-SX(2km) (8) SFP-FE-LX(10km)
Outline Dimensions (HxWxD)mm	• S3924-SI: 43.6*440*260 mm • S3928P-SI: 43.6*440*260 mm • S3952P-SI: 43.6*440*260 mm • S3928TP-SI: 43.6*440*260 mm • S3928P-EI: 43.6*440*260 mm • S3952P-EI: 43.6*440*260 mm • S3928F-EI: 43.6*440*260 mm • S3928P-PWR-EI: 43.6*440*420 mm • S3952P-PWR-EI: 43.6*440*420 mm
Weight	• S3924-SI: 3kg • S3928P-SI: 3.5kg • S3952P-SI: 4kg • S3928TP-SI: 3.5kg • S3928P-EI: 3.5kg • S3952P-EI: 4kg • S3928F-EI: 3.5kg • S3928P-PWR-EI: 6kg • S3952P-PWR-EI: 6kg
Input Voltage	The S3900-SI series are AC-powered. The S3900-EI series can be AC-powered and DC-powered. AC: 100v ~ 240V AC50/60Hz DC: -48 ~ -60V DC
Maximum System Power Consumption	30W (S3924-SI) 40W (S3928P-SI/S3928P-EI/S3928TP-SI) 50W (S3952P-SI/S3952P-EI) 65W (S3928F-EI) 450W (S3928P-PWR-EI, AC input) • Dissipated power: 150W • PoE: 300W 430W (S3928P-PWR-EI, DC input) • Dissipated power: 60W • PoE: 370W 465W (S3952P-PWR-EI, AC input) • Dissipated power: 165W • PoE: 300W 820W (S3952P-PWR-EI, DC input) • Dissipated power: 80W • PoE: 740W
Environment	Operation temperature: 0˚C ~ 45˚C Storage temperature: -40˚C ~ 70˚C Relative humidity: 10% ~ 90%, non-condensing

Industry standards support

Ethernet Protocols

IEEE 802.1D (STP)
IEEE 802.1p (CoS)
IEEE 802.1Q (VLANs)
IEEE 802.1s (MSTP)
IEEE 802.1w (RSTP)
IEEE 802.1X (Security)
IEEE 802.3i (10BASE-T)
IEEE 802.3u (Fast Ethernet)
IEEE 802.3x (Flow Control)
IEEE 802.3z (Gigabit Ethernet)

Administration Protocols

RFC 1812 (IPv4)
RFC 826 (ARP)
RFC 959 (FTP)
RFC 783 (TFTP)
RFC 768 (UDP)
RFC 791 (IP)
RFC 792 (ICMP)
RFC 793 (TCP)
RFC 2622 (Routing policy)
RFC 2474 (Diffserv)
RFC 2131 (DHCP)
RFC 1058 (RIPv1)
RFC1723 (RIPv2)
RFC 2328 (OSPF v2)
RFC 2370 (OSPF Opaque LSA Option)
RFC 1587 (OSPF NSSA option)
RFC 1765 (OSPF Database Overflow)
RFC 2338 (VRRP)
RFC 2362 (PIM-SM)
RFC 1112 (IGMPv1)
RFC 2236 (IGMPv2)
RFC 2138 (Radius Authentication)
RFC 2139 (Radius Accounting)
RFC 2267 (Network Ingress Filtering)

Safety and Compliance

Emissions / Agency Approvals

CISPR 22 Class A
FCC Part 15 Class A
EN 55022 Class A
ICES -003 Class A
VCCI Class A
AS/NZS 3548 Class A
EN 61000-3-2
EN 61000-3-3

Immunity

Product conforms to:
EN 55024: 1998
EN 61000-4-2
EN 61000-4-3
EN 61000-4-4
EN 61000-4-5
EN 61000-4-6
EN 61000-4-11

Safety Agency Certifications

UL 60950 3rd ed.
IEC 60950: 1999, corr. Feb. 2000; all national deviations
EN 60950: 2000, ZB and ZC deviations
CSA 22.2 No. 950 3rd ed., 1995
AS/NZS 60950:2000, Australia;

LINKSYS®
A Division of Cisco Systems, Inc.

The All-In-One Wireless-G Networking Solution

The Linksys Wireless-G Broadband Router is really three devices in one box. First, there's the Wireless Access Point, which lets you connect both screaming fast Wireless-G (802.11g at 54Mbps) and Wireless-B (802.11b at 11Mbps) devices to the network. There's also a built-in 4-port full-duplex 10/100 Switch to connect your wired-Ethernet devices together. Connect four PCs directly, or attach more hubs and switches to create as big a network as you need. Finally, the Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

Once your computers are connected to the Router and the Internet, they can communicate with each other too, sharing resources and files. All your computers can print on a shared printer connected anywhere in the house. And your computers can share all kinds of files -- music, digital pictures, and documents. Keep all your digital music on one computer, and listen to it anywhere in the house. Organize all of your family's digital pictures in one place, to simplify finding the ones you want, and easing backup to CD-R. Utilize extra free space on one computer when another's hard drive starts to fill up.

Secure Easy Setup™

The new push button setup feature makes it easy to configure your wireless devices. Just push the button on the router and on your other SecureEasySetup-enabled wireless device to automatically create an encryption-secured wireless connection. Wi-Fi Protected Access™ 2 (WPA2) protects your data and privacy with up to 128-bit industrial-strength encryption. The Router can serve as a DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, supports VPN pass-through, and can be configured to filter internal users' access to the Internet. Advanced configuration is a snap with the web browser-based interface.

With the Linksys Wireless-G Broadband Router at the center of your home or office network, you can share a high-speed Internet connection, files, printers, and multi-player games with flexibility, speed,

All-in-one Internet-sharing Router, 4-port Switch, and Wireless-G (802.11g) Access Point

Shares a single Internet connection and other resources with Ethernet wired and Wireless-G and -B devices

Push button setup feature makes wireless configuration secure and simple

High security: Wi-Fi Protected Access™ 2 (WPA2), wireless MAC address filtering, powerful SPI firewall

Wireless-G
Broadband Router

Wireless

Product Data

Model No. **WRT54G**

Cisco Systems

Wireless-G
Broadband Router

Features

- Complies with 802.11g and 802.11b (2.4GHz) Standards
- Unsurpassed Wireless Security with Wi-Fi Protected Access™ 2 (WPA2)
- Enhanced Internet Security Management Functions including Internet Access Policies with Time Schedules
- All LAN Ports Support Auto-Crossover (MDI/MDI-X) - No Need for Crossover Cables
- SecureEasySetup push button makes it easy to configure your wireless devices

Specifications

Model Number	WRT54G
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Channels	11 Channels (US, Canada) 13 Channels (Europe and Japan)
Ports/Buttons	Internet: One 10/100 RJ-45 Port LAN: Four 10/100 RJ-45 Switched Ports One Power Port One Reset Button One SES Button
Cabling Type	UTP CAT 5
LEDs	Power, DMZ, WLAN, LAN (1, 2, 3, 4), Internet
RF Power Output	18 dBm
UPnP able/cert	able
Security features	Stateful Packet Inspection (SPI) Firewall, Internet Policy
Wireless Security	Wi-Fi Protected Access™ 2 (WPA2), WEP, Wireless MAC Filtering

Environmental

Dimensions W x H x D	7.32" x 1.89" x 7.87" (186 mm x 48 mm x 200 mm)
Weight	1.06 lbs. (0.482 kg)
Power	External, 12V DC, 0.5A
Certifications	FCC, IC-03, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM
Operating Temp.	32°F to 104F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)
Operating Humidity	10~85% Non-condensing
Storage Humidity	5~90% Non-condensing
Warranty	3-Years

Linksys
A Division of Cisco Systems, Inc.
18582 Teller Avenue
Irvine, CA 92612 USA

E-mail: sales@linksys.com
support@linksys.com

Web: http://www.linksys.com

Linksys products are available in more than 50 countries, supported by 12 Linksys Regional Offices throughout the world. For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.

Minimum Requirements

- 200 MHz or faster processor
- 64 MB of RAM
- Internet Explorer 5.5 or Firefox 1.0 or Higher for Web-based configuration
- CD-ROM Drive
- Windows 98SE, Me, 2000, or XP
- Network Adapter

Package Contents

- Wireless-G Broadband Router
- Setup CD-ROM with Symantec Internet Security
- User Guide on CD-ROM
- Power Adapter
- Ethernet Network Cable
- Registration Card

LINKSYS®
A Division of Cisco Systems, Inc.

Expand The Range Of Your Wireless Network!

Expand the range of your wireless network! The Linksys Wireless-G Range Expander is the easy way to increase the effective coverage of your wireless network.

Unlike adding a traditional access point to your network to expand wireless coverage, the Wireless-G Range Expander does not need to be connected to the network by a data cable. Just put it within range of your main access point or wireless router, and it "bounces" the signals out to remote wireless devices.
"
This "relay station" or "repeater" approach saves wiring costs and helps to build wireless infrastructure by driving signals into even those distant, reflective corners and hard-to-reach areas where wireless coverage is spotty and cabling is impractical. The Range Expander is perfect to help cover large areas in multi-story homes, warehouse environments, public spaces, and wireless "Hot Spots" -- anywhere you need extra coverage for your wireless network.

Installation is a snap with the Range Expander's Auto Configuration button. Just plug it in and press the button. The Expander will find your wireless network and configure itself automatically.

The Wireless-G Range Expander works with most Wi-Fi certified access points and wireless routers. And it works in both Wireless-G and Wireless-B modes so you'll get the benefits of increased coverage even with a mixed network.

So, expand your wireless network's effective coverage the easy way, with the Wireless-G Range Expander.

The easiest way to expand your wireless network's coverage or extend the signal into hard-to-reach areas	Save on wiring costs -- no wired connection to your network necessary	Easy installation -- one-touch auto configuration	Compatible with both Wireless-G and Wireless-B networking clients

Wireless-G
Range Expander

Wireless

Product Data

Model No. **WRE54G**

Cisco Systems

Wireless-G
Range Expander

Features

- Supports 64 / 128 bit WEP encryption in 802.11b/ 802.11g wireless LAN
- Configurable through your networked PC's Web browser or the included Setup Wizard
- Expand your wireless coverage to eliminate dead spots
- Works with both 802.11b and 802.11g wireless networks
- RJ-45 10/100 port for easy configuration

Specifications

Model Number	WRE54G
Standards	IEEE 802.11g, IEEE 802.11b
Buttons	Autoconfiguration, Reset
Cabling Type	Cat-5 (only used for configuration)
LEDs	Blue/Red-LINK, Blue-ACTIVITY
Transmit Power:	802.11g: Typ. 13 ± 1dBm @ Normal Temp Range 802.11b: Typ: 15 ± 1dBm @ Normal Temp Range
Security features	WEP, WPA Personal
WEP Key Bits	64/128

Environmental

Dimensions W x H x D	3.18" x 8.27" x 1.77" (80.7 mm x 210 mm x 45 mm)
Unit Weight	8.82 oz. (0.25 kg)
Power	3.3V
Certifications	FCC,CE, UL
Operating Temp.	32°F to 104F (0°C to 40°C)
Storage Temp.	32°F to 158°F (0°C to 70°C)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Warranty	3-Years Limited

Linksys
A Division of Cisco Systems, Inc.
18582 Teller Avenue
Irvine, CA 92612 USA

E-mail: sales@linksys.com
support@linksys.com

Web: http://www.linksys.com

Linksys products are available in more than 50 countries, supported by 12 Linksys Regional Offices throughout the world. For a complete list of local Linksys Sales and Technical Support contacts, visit our Worldwide Web Site at www.linksys.com.

Minimum Requirements

- 802.11b or 802.11g Wireless Network
- PC with 802.11b/g Wireless adapter installed
- TCP/IP Protocol Installed

Package Contents

- One WRE54G Wireless-G Range Expander
- Two Power Plates
- One Setup Wizard CD with User Guide in PDF format
- One Quick Installation Guide
- One registration card

Redline communications

www.redlinecommunications.com

RedMAX Base Station (AN-100U)

Features:

- PMP base station platform
- 2nd generation 802.16 MAC
- 3rd generation OFDM PHY
- WiMAX Forum Certified™ design
- Can be deployed in clusters of up to six sectors
- Compliance with 802.16-2004
- Strong encryption using AES or DES
- Hardware accelerated performance

The RedMAX Base Station (AN-100U) is an 802.16-2004 compliant, broadband wireless base station capable of delivering multiple services. Fully designed as a WiMAX-based solution, the RedMAX Base Station is interoperable with an emerging base of industry-wide, WiMAX-compatible equipment.

Easy and economical to deploy, the RedMAX Base Station system facilitates the rapid provisioning of new services by services providers. Its very low latency ensures reliable delivery of delay-sensitive services in particular, including circuit-switched voice traffic, voice-over-Internet Protocol (VoIP), video and prioritized data traffic. New subscribers can be provisioned dynamically with no downtime for existing users. Existing subscribers can have their contract changed dynamically.

Designed to be completely interoperable with WiMAX Forum Certified™ products, this carrier-class, point-to-multipoint (PMP) base station provides a scalable solution for any WiMAX access network. The RedMAX Base Station can be deployed in clusters of up to six (60 degree) sectors (up to six RedMAX BS can be co-located to form high capacity multisector cell deployments). The GPS time synchronization feature facilitates tight frequency reuse to make the most efficient use of available spectrum and channels, reducing interference when operating Time Division Duplexing (TDD) radios in close proximity.

The hardware is fully upgradeable in the field by software download, to accommodate future enhancements including IPv6 support, scalability, additional classifiers, alternative encryption standards, and continued development of the 802.16 standard. Adherence to stringent carrier-class NEBS Level 3 requirements provide high-reliability for mission critical deployments. Like all of Redline's 802.16-2004 products, the RedMAX Base Station addresses all of the relevant access frequency bands with ease and flexibility.

WiMAX FORUM | Leading the WiMAX Revolution

RedMAX Base Station System Specifications

System Capability:	LOS, Optical LOS, non LOS Cell-based point-to-multipoint
RF Band:	3.400-3.600 GHz (FWA band), TDD
Channel Size:	3.5, 5, 7, 10 MHz[1]
RF Dynamic Range:	> 40 dB
Spectral Efficiency:	Up to 5 bps/Hz (over the air)
Over The Air Rate:	Up to 35 Mbps (7 MHz channel), Up to 50 Mbps (10 MHz channel)
Ethernet Data Rate:	Up to 23 Mbps (7 MHz channel), Up to 34 Mbps (10 MHz channel)
Latency:	6-18 msec (depends on channel size, OFDM frame duration)
Maximum Tx Power:	+23 dBm across all modulation/coding levels (region specific)
Rx Sensitivity:	Better than -93 dBm @ BPSK 1/2 (based on BER of 1x10e-6)
IF Cable:	Maximum length up to 984 ft (300 m) using Redline recommended high-grade IF cable
Network Attributes:	Transparent bridge, 802.1Q VLAN, 802.1p network traffic prioritization, DHCP, client pass-through
Modulation/Coding Rates:	Dynamic adaptive modulation (bi-directional) Auto-select modulation: BPSK, QPSK, 16 QAM, 64 QAM Auto-select coding: 1/2, 2/3, 3/4
Over the Air Encryption:	DES and AES
MAC:	Cell-based PMP deployment 802.16-2004 compliant PMP 802.16-2004 packet convergence sub-layer mode TDMA Access Automatic repeat request (ARQ) error correction
Range:	Over 28 mi (45 km) LOS Over 2 mi (3 km) non LOS
Duplex Technique:	Dynamic TDD (time division duplex) HD-FDD (half duplex frequency division duplex)[1]
Wireless Transmission (PHY):	256 FFT OFDM (Orthogonal Frequency Division Multiplexing)
Network Connections:	Standard: 10/100 Ethernet (RJ-45); Optional: TDM (RJ-48c)
System Configuration:	HTTP (Web) interface, SNMP CLI via Telnet and Local Console
Network Management:	SNMP, standard and proprietary MIBs Full management by RedMAX Management Suite (RMS)
Power Requirements:	Auto-sensing 110/220/240 VAC 50/60 Hz Auto-sensing 18-72 VDC, 75 W maximum
Redundant Power:	Optional dual AC or dual DC power supply (dual cord) with automatic fail-over
Compliance:	EMC: EN 301 489-1, EN 301 489-4, EN 55022/CISPR 22; RF: EN 302 326; Safety: IEC 60950-1, EN 60950-1, UL 60950-1; Industry Canada: RSS-192
Operating Temperature:	IDU: 0 C to 40 C ODU: -40 C to 60 C
Dimensions	17 x 12 x 1.75 in (431.8 x 304.8 x 44.45 mm)
Weight:	5.5 lb (2.5 kg)
Humidity:	Up to 90% non-condensing

[1]Contact sales for availability.

About Redline Communications

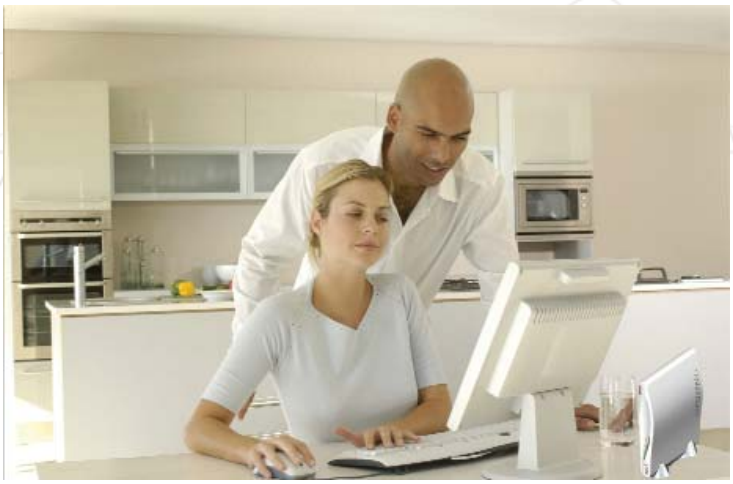
Redline Communications is a technology leader in the design and manufacture of standards-based broadband wireless access solutions. Using industry leading OFDM technologies, Redline's award-winning products provide unmatched high-capacity non line-of-sight capabilities with proven performance, reliability and security. Ideal for a variety of access, backhaul and private network applications, Redline products are meeting the needs of carriers, service providers and enterprises worldwide. Redline has over 15,000 installations in 75 countries across six continents through a global distribution network of 80+ partners.

302 Town Centre Blvd. - Suite 100 • Markham • ON • Canada • L3R 0E8 • Phone: +1.905.479.8344 • Toll-Free: +1.866.633.6669 • Fax: +1.905.479.7432 • www.redlinecommunications.com

Redline communications

www.redlinecommunications.com

RedMAX Subscriber Unit (SU-I)



Features:

- WiMAX Forum Certified™ design
- Intel® PRO/Wireless 5116
- Self Install
- Non-LOS PMP capability employing OFDM technology for high reliability
- Dynamic Quality of Service (QoS) settings
- 3.4 - 3.6 GHz frequency band

The RedMAX SU-I is an indoor broadband wireless access product designed to WiMAX Forum Certified™ specifications. Compliance to the IEEE 802.16-2004 standard ensures interoperability (as defined by the WiMAX Forum™) with an emerging industry-wide base of compatible Point to Multipoint (PMP) equipment.

The RedMAX SU-I is easy and economical to deploy, allowing service providers to quickly provision new services with bandwidth comparable to xDSL. This self-install desktop unit features an integrated antenna with signal strength LED's for quick setup.

Operating in the 3.4 - 3.6 GHz band, Redline's integrated 3rd generation, Orthogonal Frequency Division Multiplexing (OFDM) non Line of Sight (NLOS) technology helps overcome typical urban obstacles such as trees and buildings while maintaining high reliability. Stringent design standards and sophisticated techniques, including advanced forward error correction (FEC), combine to deliver wireline-equivalent high availability.

The very low latency of Redline's RedMAX SU-I ensures reliable delivery of delay sensitive mission critical services such as video, voice-over-IP (VoIP), and prioritized data traffic. WiMAX-based compatibility, high performance, and easy installation all combine to make the SU-I an excellent choice when deploying wireless broadband for business and residential access.

WiMAX FORUM | Leading the WiMAX Revolution

RedMAX Subscriber Unit (SU-I)

System Capability:	Non-LOS Cell-based Point-to-Multipoint
RF Band:	3.400 GHz to 3.600 GHz (FWA Band)
Channel Size:	3.5 MHz, 7 MHz
Spectral Efficiency:	Up to 5 bps/Hz (over the air) Up to 3 bps/Hz (net to Ethernet)
Over The Air Rate:	Up to 35 Mbps (@7 MHz, rates depend on channel size)
Data Rate:	Up to 18 Mbps average Ethernet rate (@7 MHz)
Maximum Tx Power:	Up to +20 dBm (region specific)
Rx Sensitivity:	Better than -93 dBm @ BPSK 1/2 (based on BER of 1x10e-6)
Network Attributes:	Transparent bridge 802.1Q VLAN 802.1p, TOS/DSCP and L2/L3 address traffic prioritization DHCP client and DHCP pass-through
Modulation/Coding Rates:	Dynamic adaptive modulation (bi-directional) Auto select: BPSK, QPSK, 16 QAM, 64 QAM
Coding Rates:	1/2, 3/4 and 2/3
Over the Air Encryption:	DES and AES
MAC:	Cell-based PMP deployment 802.16-2004 compliant PMP 802.16-2004 packet convergence sub-layer mode TDMA access Automatic repeat request (ARQ) error correction
Duplex Technique:	TDD (time division duplex) HD-FDD (Half Duplex Frequency Division Duplex)
Wireless Transmission (PHY):	256 FFT Orthogonal Frequency Division Multiplexing (OFDM)
Network Connections:	10/100 Ethernet (RJ-45)

System Configuration:	HTTP (Web) interface, SNMP, TFTP
Network Management:	SNMP, standard and proprietary MIBs Full management by RedMAX Management Suite (RMS)
Available Power Blocks:	Auto-sensing 110/220/240 VAC 50/60 Hz
Compliance:	EMC: EN 301 489-1, EN 301 489-4, EN 55022/CISPR 22; RF: EN 301 021, EN 301 753; Safety: IEC 60950-1, EN 60950-1, UL 60950-1; Industry Canada: RSS-192
Operating Temperature:	-5 C to 55 C
Antenna:	Integrated antenna and optional window mount

*Interface Options**

Ethernet Option

Standard:	10/100 Ethernet (RJ-45)
Optional:	4 port mini switch

Voice Interface Options

VoIP	SIP
POTS	1 to 4 FXO/FXS

*contact sales for availability

About Redline Communications

Redline Communications is a technology leader in the design and manufacture of standards-based broadband wireless access solutions. Using industry leading OFDM technologies, Redline's award-winning products provide unmatched high-capacity non line-of-sight capabilities with proven performance, reliability and security. Ideal for a variety of access, backhaul and private network applications, Redline products are meeting the needs of carriers, service providers and enterprises worldwide. Redline has over 15,000 installations in 75 countries across six continents through a global distribution network of 80+ partners.

302 Town Centre Blvd. - Suite 100 • Markham • ON • Canada • L3R 0E8 • Phone: +1.905.479.8344 • Toll-Free: +1.866.633.6669 • Fax: +1.905.479.7432 • www.redlinecommunications.com

APÉNDICE 1

CONFIGURACIÓN DE EQUIPOS WiFi Y xDSL

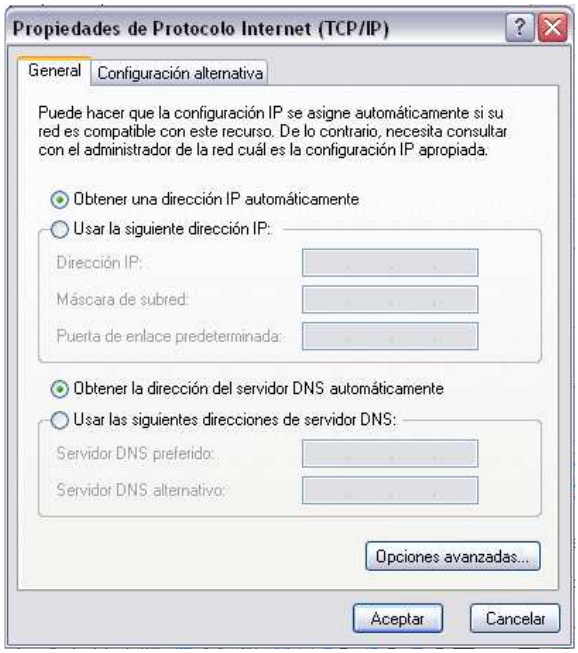
PROCESO DE CONFIGURACIÓN DEL ROUTER WIFI

El proceso de configuración que se muestra en el presente documento corresponde al equipo WRT54G de la marca Linksys, este equipo cuenta con, 4 puertos 10/100 Base TX de LAN, 1 puerto 10/100 Base TX de WAN y conexión inalámbrica 802.11g.

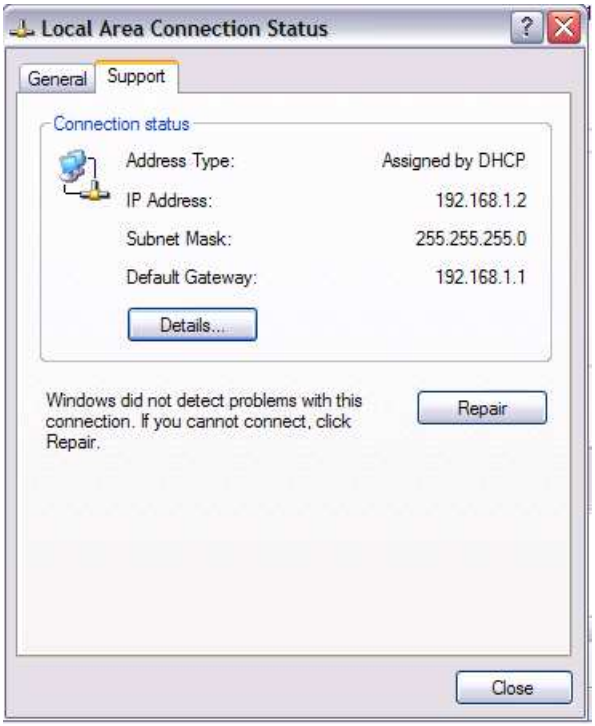
El proceso mostrado nos permitirá dar servicio a los clientes inalámbricos, y se configuraran las seguridades WPA.

1. Conectar el router a la toma eléctrica, conectar la PC con un cable directo o cruzado al puerto 1 de LAN.
2. Se debe configurar la conexión LAN del PC ingresando a las propiedades, y seleccionando el protocolo TCP/IP.

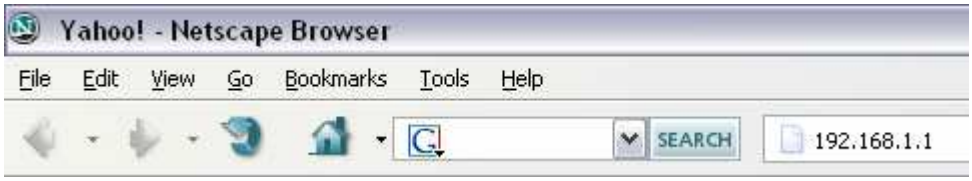
3. Escogemos obtener una IP automáticamente y obtener un DNS automáticamente.



4. Verificamos que se nos asigne una IP, una mascara de subred y un gateway mediante DHCP, en nuestro caso la IP que nos asigna el equipo de fábrica es la dirección 192.168.1.2.

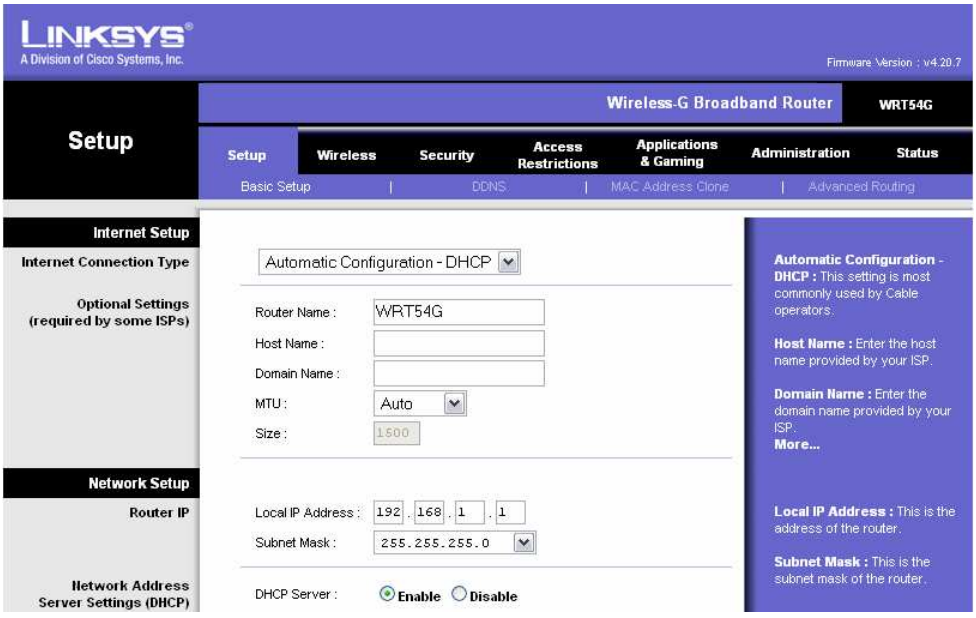


5. Para poder acceder a la configuración del router debemos ingresar mediante browser la dirección del gateway asignada automáticamente, es decir la dirección 192.168.1.1.

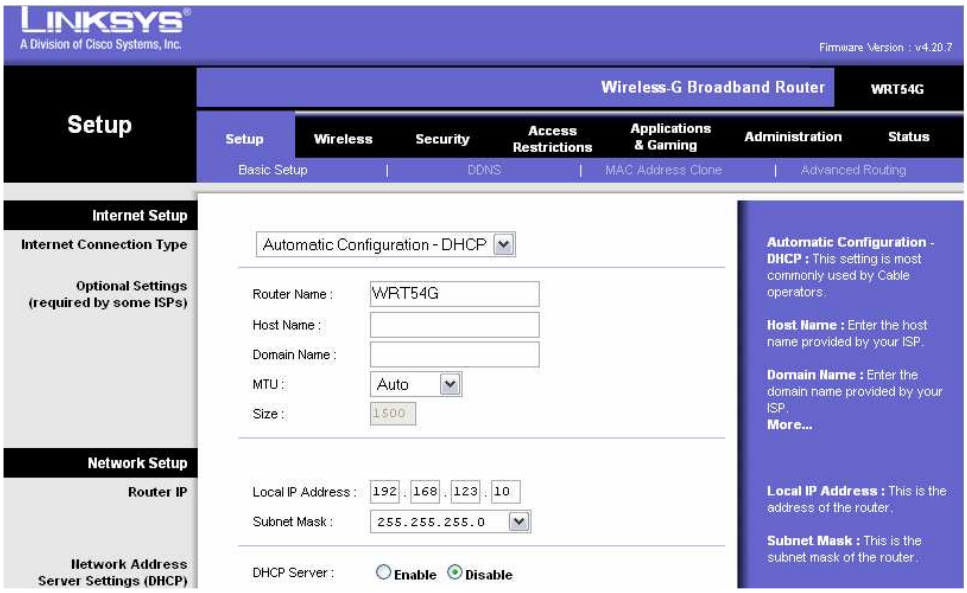


6. Una vez que se ha ingresado la dirección, se nos desplegará una pantalla que nos pide de usuario y contraseña.

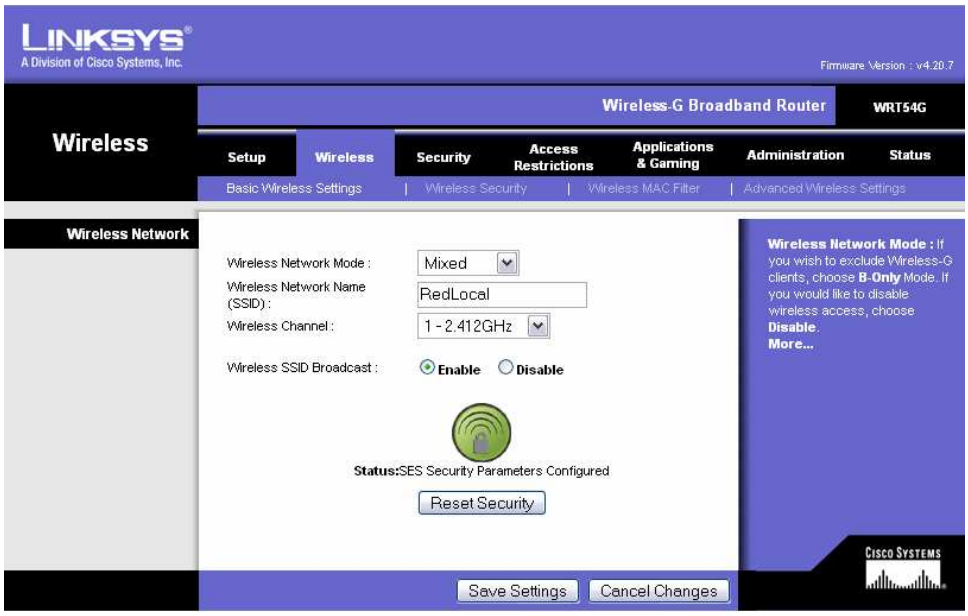
7. Al ingresar el usuario y la contraseña tendremos acceso a la pantalla de configuración principal, aquí podremos configurar el puerto de WAN, la dirección IP para la LAN y activar o desactivar el DHCP para la LAN.



8. En nuestro caso, dejaremos que la IP pública se asigne automáticamente, la IP local del equipo será la 192.168.123.10 y deshabilitaremos el DHCP, como medida de seguridad, ya que no buscamos tener un hot spot.



9. Seleccionamos del menú superior la opción Wireless para configurar el modo de operación, en nuestro caso sera Mixed para que se pueda tener clientes 802.11b y 802.11g, le damos el nombre a la red (SSID), que será RedLocal, y seleccionamos el canal de funcionamiento: 1 (2.412 GHz).



10. Pasamos a la opción Wireless Security, en donde podremos activar el tipo de seguridad, la seguridad WEP esta descontinuada, por lo que escogemos la seguridad WPA, usaremos el algoritmo TKIP que presta buen desempeño, escogemos una llave compartida para la autenticación y encriptación, será la palabra Red y determinamos un tiempo de renovación de llave de grupo, se sugiere 3600 segundos, para no tener problemas de lentitud de la red.

11. Una vez terminado este paso, el equipo esta listo para ser usado, todo cliente que desee conectarse deberá especificar la seguridad WPA e ingresar la llave compartida, las direcciones IP se asignarán manualmente.

PROCESO DE CONFIGURACIÓN DEL DSLAM Y MODEM ADSL

Configuración del DSLAM

El proceso de configuración que se muestra en el presente documento corresponde al equipos XZDSL 8426 de la marca ZTE, este equipo cuenta con 24 puertos ADSL, capaces de soportar las normas g.dmt y g.lite, 24 puertos para conexión a POTS, 1 puerto 10 Base T, 1 puerto 100 Base TX, y un puerto de consola RJ45.

El proceso mostrado nos permitirá dar servicio a 24 clientes, con una velocidad de 128 Kbps y se utilizará la norma g.dmt.

1. Conectar el DSLAM a la toma eléctrica y conectar el cable de consola del DSLAM a la PC (Cable RJ45 a serial RS232).
2. Conectar los puertos ADSL a las regletas correspondientes a las líneas telefónicas de los clientes y los puertos POTS hacia las regletas de Andinatel.
3. Para establecer comunicación serial se debe configurar el programa Hyper Terminal de Windows para que trabaje con un puerto serial, en nuestro caso el puerto COM1, y configurarlo con los parámetros mostrados a continuación:

4. Establecer la comunicación.
5. Una vez que la comunicación se haya establecido, la configuración del equipo se realiza mediante los siguientes comandos:

```
Login: root              (Ingreso de usuario)
Password: ****           (Ingreso de contraseña)

Welcome to ZXDSL 8426 Shell!

##HOME>>net                          (Cambio del modo de inicio HOME al modo NET)

##NET>>config           (Ingreso al modo de configuración)

##NET[conf]>>help                    (La ayuda del programa se accede en cualquier
                                     momento mediante el comando help)
Command List:
------------------------------------------------------------
01)help             Display the help information
02)home             Exit the current Configuration to Home
03)exit             return to normal mode
04)showperf         Display data statistic of net interface
05)setip            Set the IP address of the net interface
06)showip           Display the IP address of the net interface
07)showmac          Display the mac address of the net interface
08)showroute        dispaly system route
09)setgateway       set system gateway
10)delgateway       del system gateway
11)addroute         add a route in system
12)delroute         delete a route from system
13)lanmode          Set 100M lan port mode
14)ping             Ping destination host
------------------------------------------------------------
```

```
##NET[conf]>>setip
```
(Configuración de la IP de las interfases Ethernet)

```
Current have below Ethernet net:
        (1 ):  10M
        (2 ):  100M
Please choose: 2

IP Address(xxx.xxx.xxx.xxx): 69.65.151.130
MASK Address(xxx.xxx.xxx.xxx): 255.255.255.224

(C)ontinue or (E)xit:c

Set IP address successfully.

##NET[conf]>>setgateway
```
(Configuración del gateway de las interfaces Ethernet)

```
Input the gateway IP: 69.65.151.129

(C)ontinue or (E)xit:c

Set gateway address successfully.

##NET[conf]>>showroute
```
(Visualización de las IPs configuradas)

```
No  Destination        Mask             gateway       Interface
1    136.1.0.0       255.255.0.0      136.1.180.20      eth0
2    69.65.151.128   255.255.255.224  69.65.151.130     fec0
3    127.0.0.1       255.255.255.255  127.0.0.1         lo0
4    0.0.0.0         0.0.0.0          0.0.0.0           fec0

##NET[conf]>>home
```
(Cambio del modo NET al modo HOME)

```
##HOME[conf]>>atm
```
(Cambio del modo HOME al modo ATM)

```
##ATM[conf]>>setpvc
```
(Configuración del canal virtual)

```
Now you can set PVC at below two
        (1 ):  ADSL line
        (2 ):  IMA
Please input you choice: 1
```
(Selección de la línea ADSL)

```
Please input ADSL line No. (1--24 or 'a' to select all)a
Please input the VPI(0--255): 8
```
(Parámetros específicos del fabricante)

```
Please input the VCI(32--65535): 81
```
(Parámetros específicos del fabricante)

```
Set PVC successfully!!

##ATM[conf]>>showconfig
```
(Visualización de la configuración de canal virtual)

```
Now you can show PVC at below two
        (1 ):  ADSL line
        (2 ):  IMA
Please input you choice: 1
```
(Selección de la línea ADSL)

```
Please input ADSL line No. (1--24 or 'a' to select all)a

       line     VPI VCI
        1        8   81
        2        8   81
        3        8   81
        4        8   81
        5        8   81
        6        8   81
        7        8   81
```

```
        8       8   81
        9       8   81
        10      8   81
        11      8   81
        12      8   81
        13      8   81
        14      8   81
        15      8   81
        16      8   81
        17      8   81
        18      8   81
        19      8   81
        20      8   81
        21      8   81
        22      8   81
        23      8   81
        24      8   81

##ATM[conf]>>home          (Cambio del modo ATM al modo HOME)

##HOME[conf]>>dsl           (Cambio del modo HOME al modo DSL)

##DSL[conf]>>addprf                  (Configuración de un perfil de 128 Kbps simétrico)
Please select profile type:
        (1): Adsl Line Config
        (2): Adsl LineAlarm Config
Please input your choice or (E): 1   (Selección de la línea ADSL)

Please input name of AdslLineConf Profile(*.PRF)----------- : prf128s
    Atuc Channel Conf Fast Max Tx Rate(0...10000)---------[2048] : 128
    Atuc Channel Conf InterLeave Max Tx Rate(0...10000)---[2048] : 128
    Atuc Channel Conf InterLeave Max Delay(4 16 or 64)------[16] : 16
    Atur Channel Conf Fast Max Tx Rate(0...1000)-----------[512] : 128
    Atur Channel Conf InterLeave Max Tx Rate(0...1000)-----[512] : 128
    Atur Channel Conf InterLeave Max Delay(4 16 or 64)------[16] : 16

(A)dd Profile of the above? or (R)Modify? or (C)ancel?(default is 'C'):
a

Create AdslLineConf Profile successfully.

##DSL[conf]>>addprf          (Configuración de un perfil de 64 Kbps simétrico)
Please select profile type:
        (1): Adsl Line Config
        (2): Adsl LineAlarm Config
Please input your choice or (E): 1  (Selección de la línea ADSL)

Please input name of AdslLineConf Profile(*.PRF)----------- : prf64s
    Atuc Channel Conf Fast Max Tx Rate(0...10000)---------[2048] : 64
    Atuc Channel Conf InterLeave Max Tx Rate(0...10000)---[2048] : 64
    Atuc Channel Conf InterLeave Max Delay(4 16 or 64)------[16] : 16
    Atur Channel Conf Fast Max Tx Rate(0...1000)-----------[512] : 64
    Atur Channel Conf InterLeave Max Tx Rate(0...1000)-----[512] : 64
    Atur Channel Conf InterLeave Max Delay(4 16 or 64)------[16] : 16

(A)dd Profile of the above? or (R)Modify? or (C)ancel?(default is 'C'):
a

Create AdslLineConf Profile successfully.

##DSL[conf]>>showprf        (Visualización de los Perfiles)
```

```
Please select profile type:
        (1) Adsl Line Config
        (2) Adsl LineAlarm Config
Please input your choice or (E): 1  (Selección de la línea ADSL)

List of AdslLineConf Profile:
-----------------------------------------------------
(1) DEF2M.PRF
(2) DEF8M.PRF
(3) DEF1M.PRF
(4) DEFHM.PRF
(5) PRF128S.PRF
(6) PRF64S.PRF
-----------------------------------------------------
Please input Num of Profile : 4      (Selección de un perfil, en este caso uno de fabrica
                                      de 512 Kbps)

-----------------------------------------------------
    AdslLineConf Profile: DEFHM.PRF
-----------------------------------------------------
    AtucConfRateMode = AdaptAtStartUp
    AtucConfTargetSnrMgn = 60
    AtucConfMaxSnrMgn = 300
    AtucConfMinSnrMgn = 0
    AtucChanConfFastMaxTxRate = 512
    AtucChanConfInterleaveMaxTxRate = 512
    AtucChanConfMaxInterleaveDelay = 16
    AturConfTargetSnrMgn = 60
    AturConfMaxSnrMgn =
    AturConfMinSnrMgn = 0
    AturChanConfFastMaxTxRate = 512
    AturChanConfInterleaveMaxTxRate = 512
    AturChanConfMaxInterleaveDelay = 16

##DSL[conf]>>linecfg                  (Asignación del perfil de funcionamiento a las líneas
                                       de subscriptor)
Input line num(1-24 or 'a' to select all):a
Please input a Profile Name: prf128s.prf
Input LineType (2: fastOnly , 3: interleave):2
Imput LineMode (1: g.lite 2: g.dmt):2

Config ADSL card line all successfully!

##DSL[conf]>>showstatus               (Visualización de la configuración de las líneas de
                                       subscriptor)
Input line num(1-24 or 'a' to select all):a

1   FastOnly    g_dmt      PRF128S.PRF          0          0
2   FastOnly    g_dmt      PRF128S.PRF          0          0
3   FastOnly    g_dmt      PRF128S.PRF          0          0
4   FastOnly    g_dmt      PRF128S.PRF          0          0
5   FastOnly    g_dmt      PRF128S.PRF          0          0
6   FastOnly    g_dmt      PRF128S.PRF          0          0
7   FastOnly    g_dmt      PRF128S.PRF          0          0
8   FastOnly    g_dmt      PRF128S.PRF          0          0
9   FastOnly    g_dmt      PRF128S.PRF          0          0
10  FastOnly    g_dmt      PRF128S.PRF          0          0
11  FastOnly    g_dmt      PRF128S.PRF          0          0
11  FastOnly    g_dmt      PRF128S.PRF          0          0
12  FastOnly    g_dmt      PRF128S.PRF          0          0
13  FastOnly    g_dmt      PRF128S.PRF          0          0
14  FastOnly    g_dmt      PRF128S.PRF          0          0
15  FastOnly    g_dmt      PRF128S.PRF          0          0
```

```
16  FastOnly    g_dmt      PRF128S.PRF          0          0
17  FastOnly    g_dmt      PRF128S.PRF          0          0
18  FastOnly    g_dmt      PRF128S.PRF          0          0
19  FastOnly    g_dmt      PRF128S.PRF          0          0
20  FastOnly    g_dmt      PRF128S.PRF          0          0
21  FastOnly    g_dmt      PRF128S.PRF          0          0
22  FastOnly    g_dmt      PRF128S.PRF          0          0
23  FastOnly    g_dmt      PRF128S.PRF          0          0
24  FastOnly    g_dmt      PRF128S.PRF          0          0
```

```
##DSL[conf]>>showinfo
```

(Visualización del estado de las líneas de subscriptor)

```
Input line num(1-24 or 'a' to select all):a

DSLLine   UserCFG  DslCurStatus
1         enable   down
2         enable   down
3         enable   down
4         enable   down
5         enable   down
6         enable   down
7         enable   down
8         enable   down
9         enable   down
10        enable   down
11        enable   down
12        enable   down
13        enable   down
14        enable   down
15        enable   down
16        enable   down
17        enable   down
18        enable   down
19        enable   down
20        enable   down
21        enable   down
22        enable   down
23        enable   down
24        enable   down
```

```
##DSL[conf]>>enable
```

(Habilitación de las líneas de subscriptor)

```
Input line num(1-24 or 'a' to select all):a

Enable ADSL card line 1  successfully.
Enable ADSL card line 2  successfully.
Enable ADSL card line 3  successfully.
Enable ADSL card line 4  successfully.
Enable ADSL card line 5  successfully.
Enable ADSL card line 6  successfully.
Enable ADSL card line 7  successfully.
Enable ADSL card line 8  successfully.
Enable ADSL card line 9  successfully.
Enable ADSL card line 10 successfully.
Enable ADSL card line 11 successfully.
Enable ADSL card line 12 successfully.
Enable ADSL card line 13 successfully.
Enable ADSL card line 14 successfully.
Enable ADSL card line 15 successfully.
Enable ADSL card line 16 successfully.
Enable ADSL card line 17 successfully.
Enable ADSL card line 18 successfully.
Enable ADSL card line 19 successfully.
```

```
Enable ADSL card line 20 successfully.
Enable ADSL card line 21 successfully.
Enable ADSL card line 22 successfully.
Enable ADSL card line 23 successfully.
Enable ADSL card line 24 successfully.
```

```
##DSL[conf]>>home
```
(Cambio del modo DSL al modo HOME)

```
##HOME[conf]>>bridge
```
(Cambio del modo HOME al modo BRIDGE)

```
##BRIDGE[conf]>>default1
```
(Asignación del modo default1, cada línea de subscriptor una VLAN independiente)

```
Set to default vlan 1 mode config successfully.
```

```
##BRIDGE[conf]>>home
```
(Cambio del modo BRIDGE al modo HOME)

```
##HOME[conf]>>sys
```
(Cambio del modo HOME al modo SYS)

```
##SYS[conf]>>saveflash
```
(Guardado de la información)

```
All information in flash will be changed! (C)ontinue or (E)xit?c
Save Config to Flash successfully!
```

```
##SYS[conf]>>home
```
(Cambio del modo SYS al modo HOME)

```
##HOME[conf]>>logout
```
(Terminación de la comunicación)

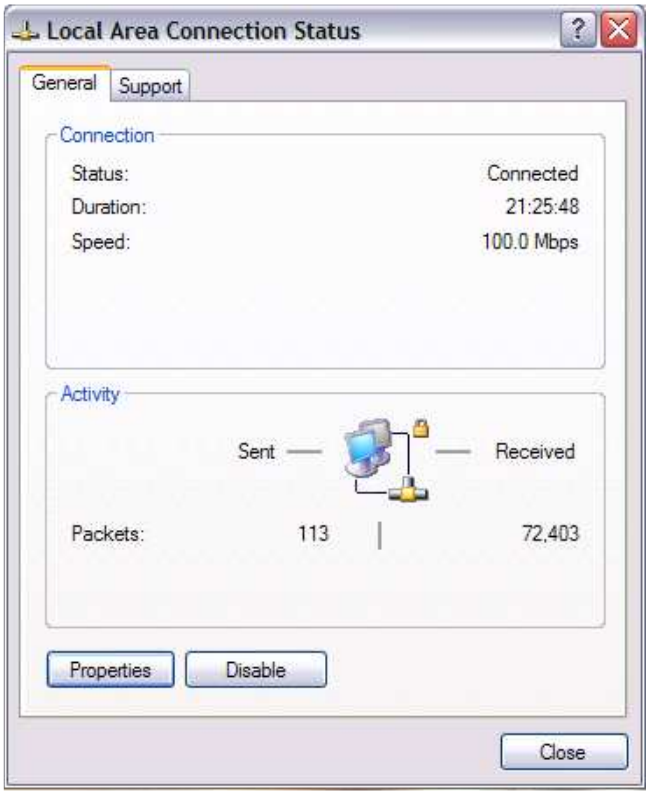
Configuración del Modem

El proceso de configuración del modem ADSL es el complemento del DSLAM, el equipos es el XZDSL 831 A de la marca ZTE, este equipo cuenta con 1 puerto ADSL RJ11, capaz de soportar las normas g.dmt y g.lite, 1 puertos para conexión 10/100 Base TX, y 1 puerto USB 2.0.

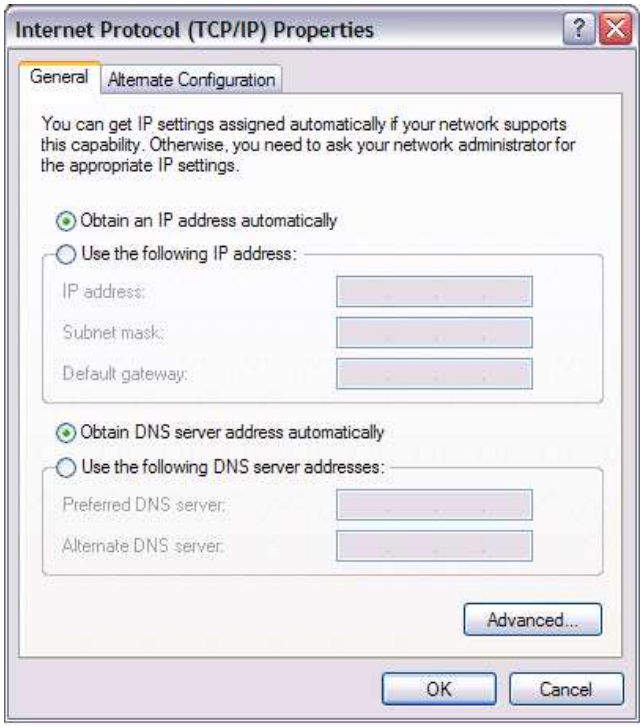
El proceso mostrado nos permitirá establecer conexión con el DSLAM y entre el modem y la PC del usuario.

1. Conectar el modem a la toma eléctrica, conectar el spliter a la línea telefónica y a su vez este al modem.
2. Para establecer comunicación entre la PC y el modem se debe utilizar el puerto RJ45 o el puerto USB 2.0, si se usa el puerto Ethernet se debe conectar un cable directo o cruzado entre el modem y la NIC del PC, si se usa el puerto USB, se debe utilizar un cable USB e instalar los controladores en caso de ser necesario, la PC reconocerá la conexión serial como una conexión de red.

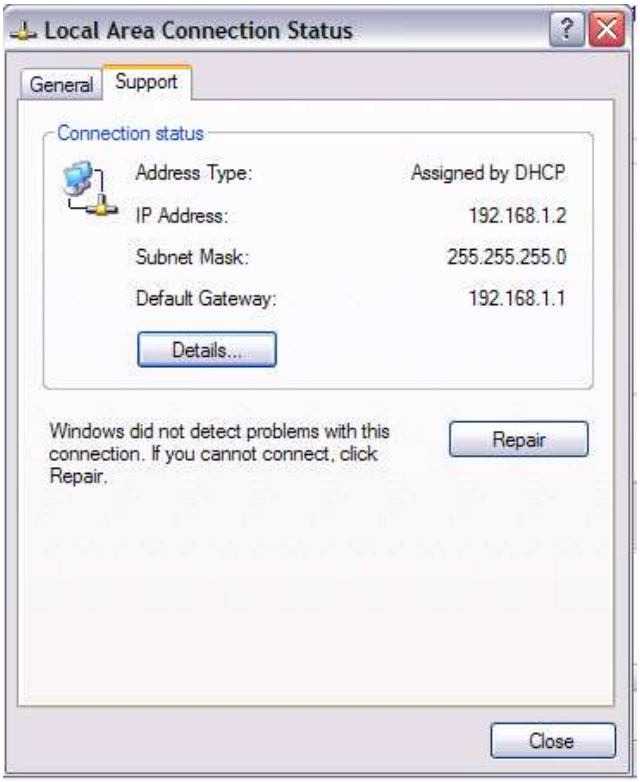
3. Se debe configurar la conexión LAN del PC ingresando a las propiedades, y seleccionando el protocolo TCP/IP.



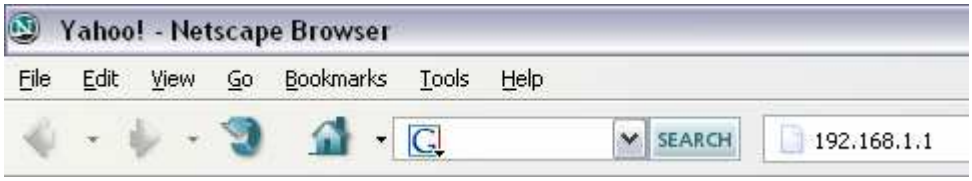
4. Escogemos obtener una IP automáticamente y obtener un DNS automáticamente.



5. Verificamos que se nos asigne una IP, una mascara de subred y un gateway mediante DHCP, en nuestro caso la IP que nos asigna el equipo de fábrica es la dirección 192.168.1.2.

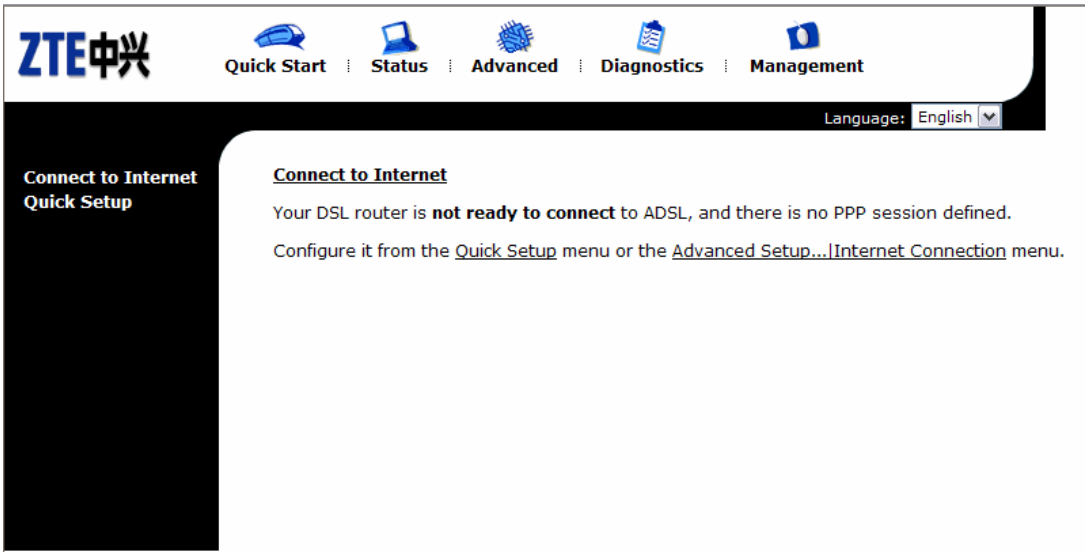


6. Para poder acceder a la configuración del modem debemos ingresar mediante browser la dirección del gateway asignada automáticamente, es decir la dirección 192.168.1.1.

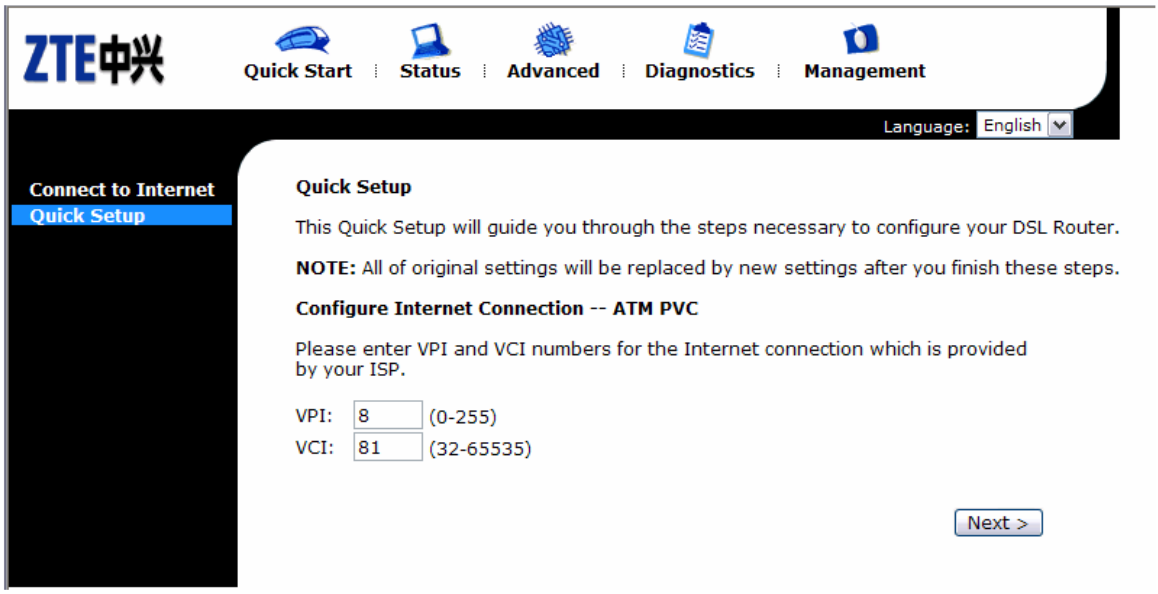


7. Una vez que se ha ingresado la dirección, se nos desplegará una pantalla que nos pide de usuario y contraseña.

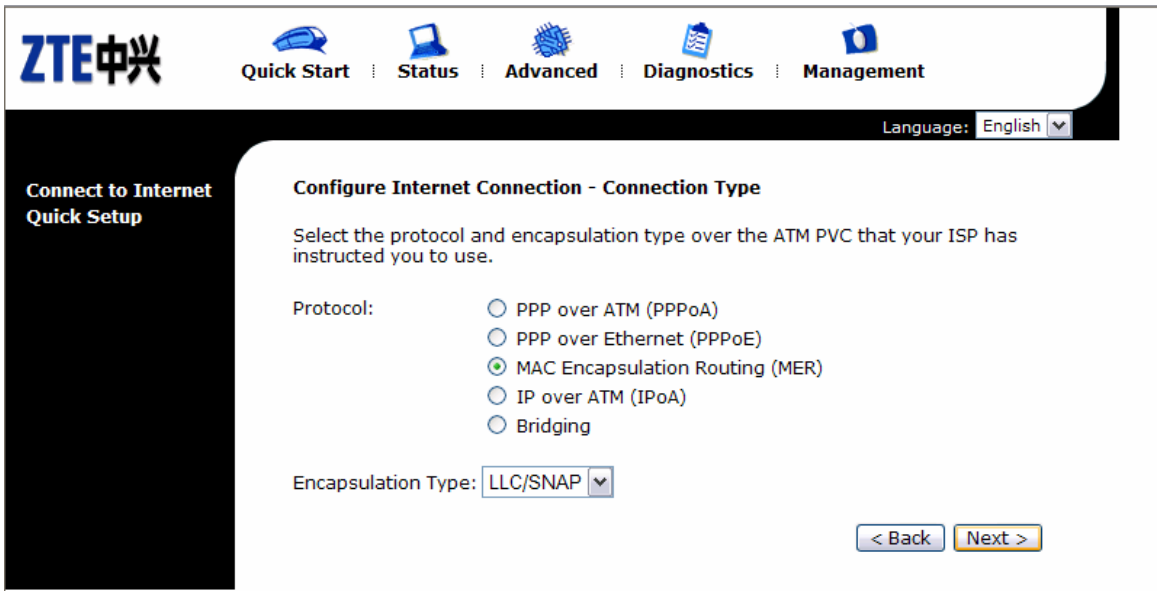
8. Al ingresar el usuario y la contraseña tendremos acceso a la pantalla de configuración principal, la cual nos indica que no hemos definido una configuración para poder conectarnos al Internet.



9. Escogemos del menú izquierdo el modo Quick Setup para configurar el modem.

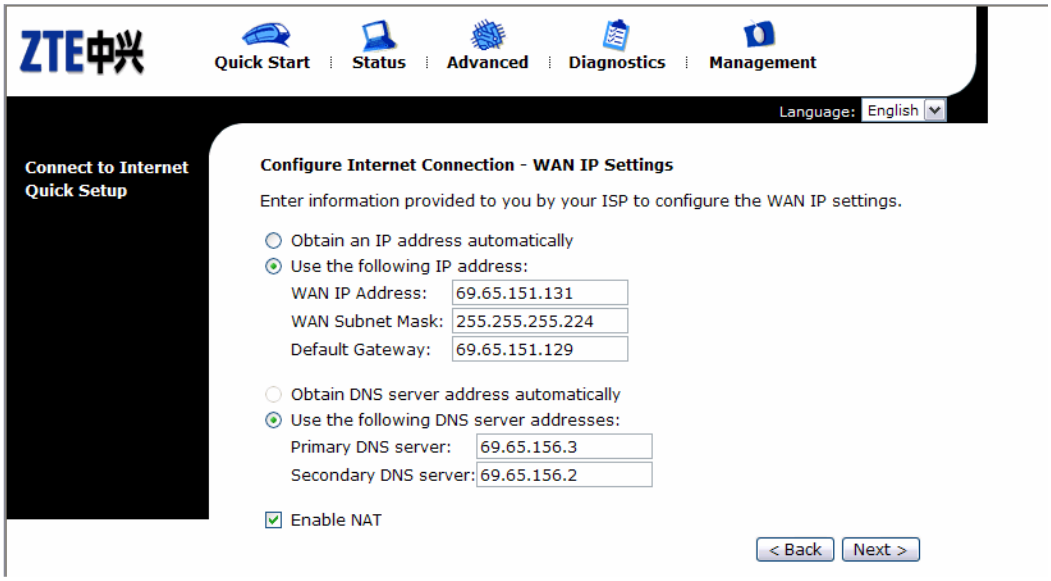


10. Seleccionamos el protocolo a ser usado, en nuestro caso ruteo mediante encapsulación MAC (MER), y la encapsulación LLC/SNAP.

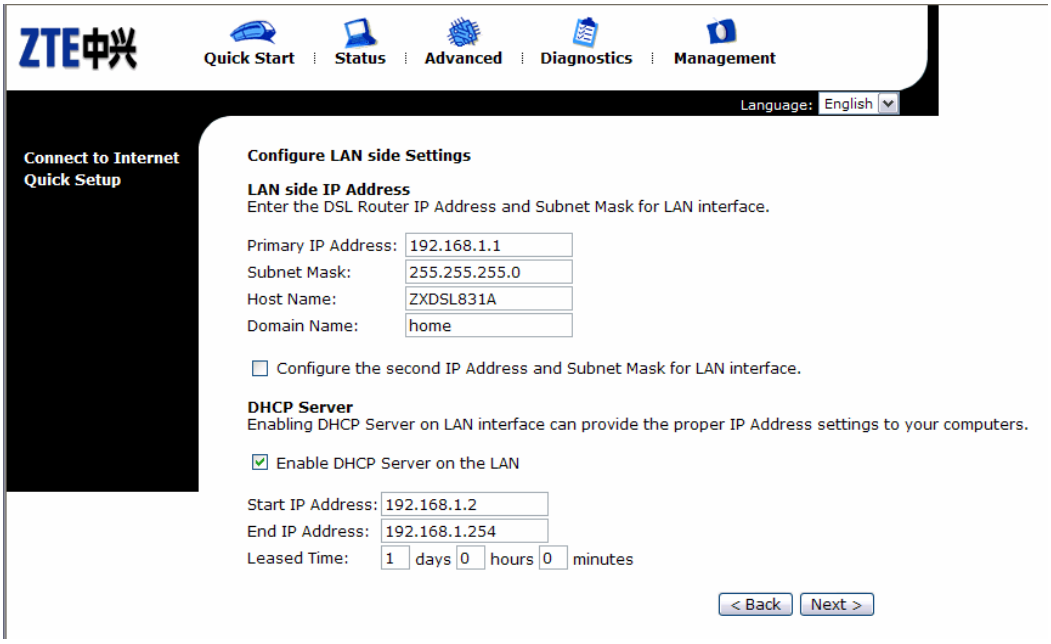


11. La siguiente pantalla nos preguntará si deseamos ingresar la IP pública del cliente o si se configurará mediante DHCP, en nuestro caso ingresaremos la IP directamente,

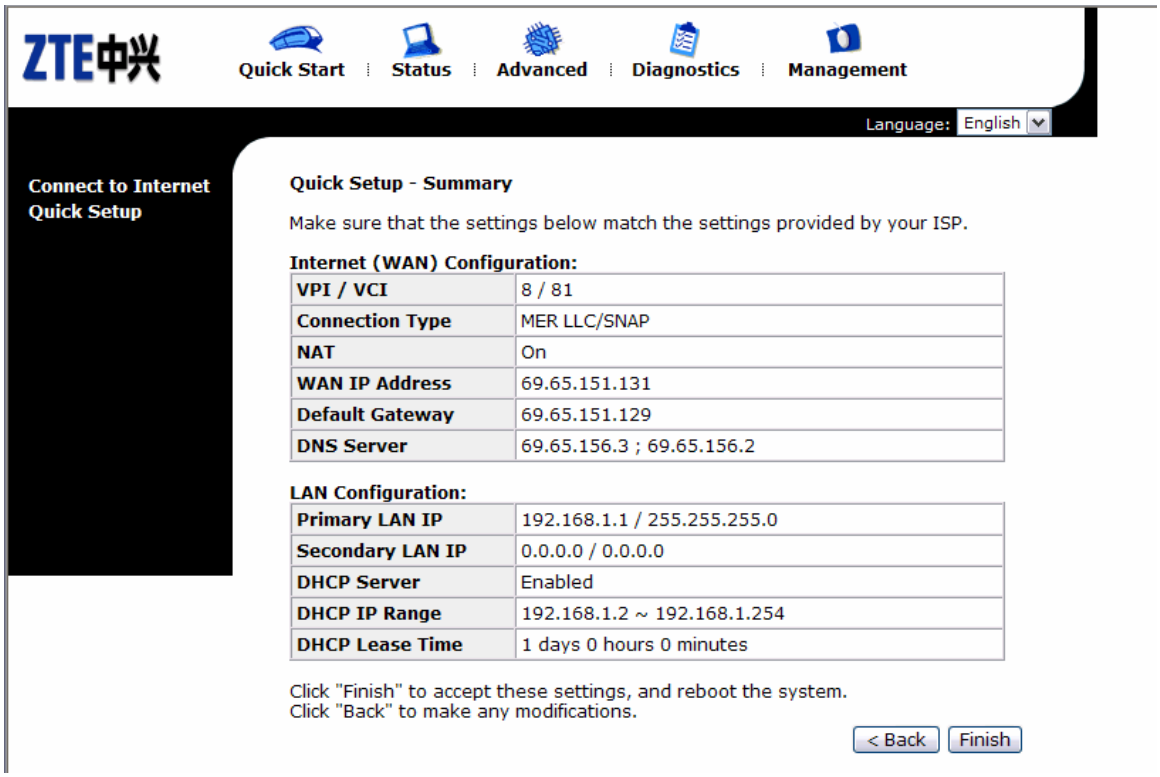
la mascará y el gateway deben coincidir con los establecidos en el DSLAM, debemos activar el uso del NAT para que el cliente pueda tener varias IP privadas.



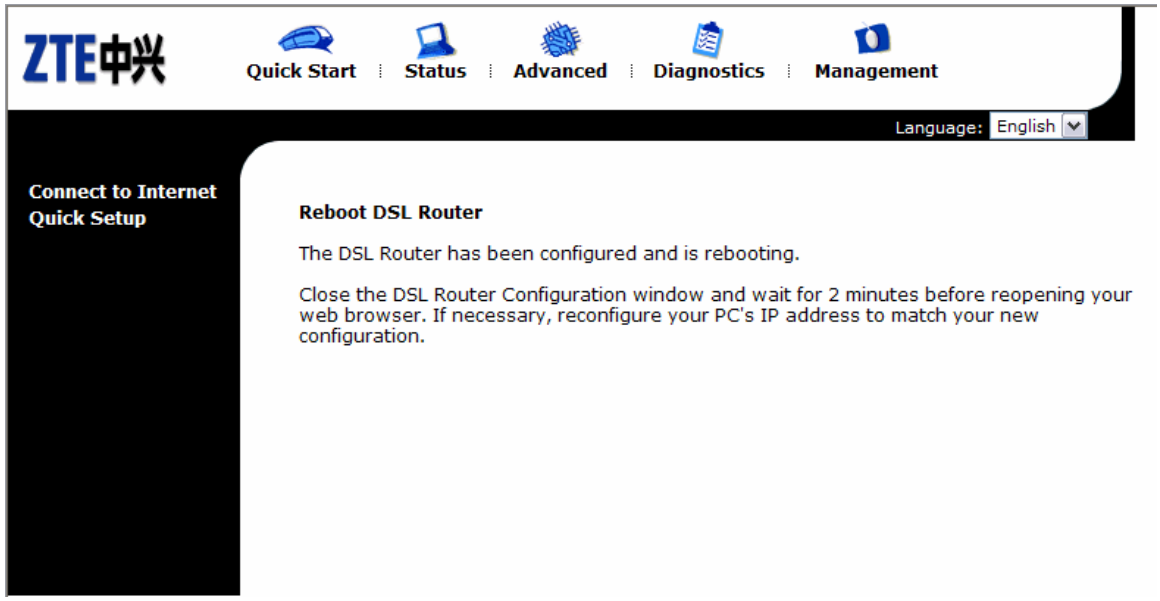
12. Después configuraremos la IP privada del cliente, asignamos una IP al modem y activamos el DHCP del lado de la LAN del cliente para que pueda conectarse sin mayores problemas.



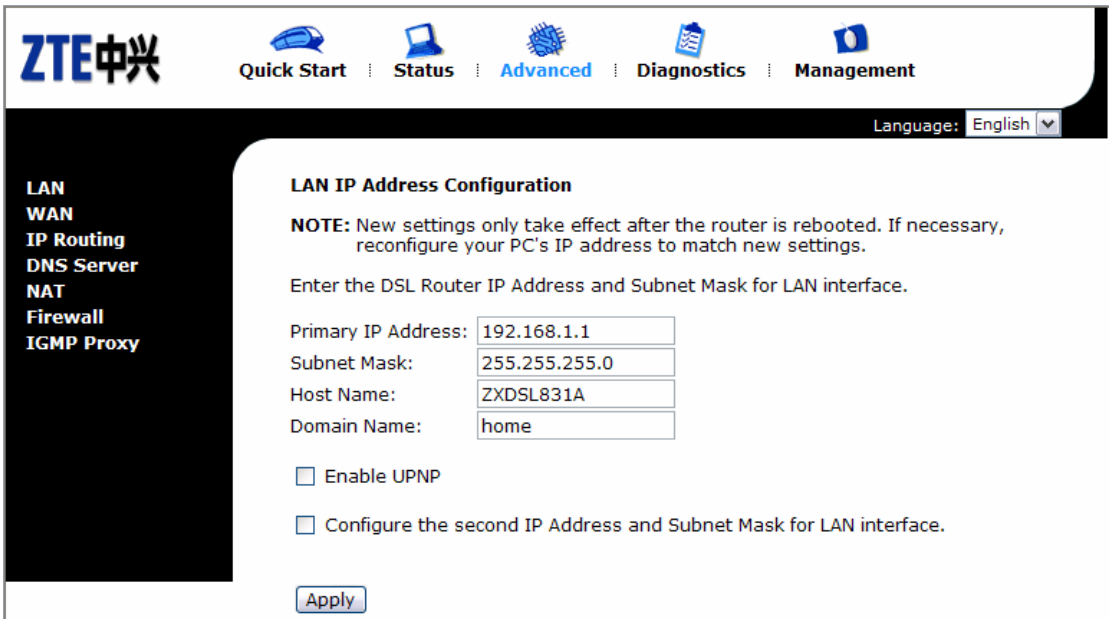
13. Una vez asignados estos parámetros se nos desplegará una pantalla mostrándonos un resumen de la configuración.



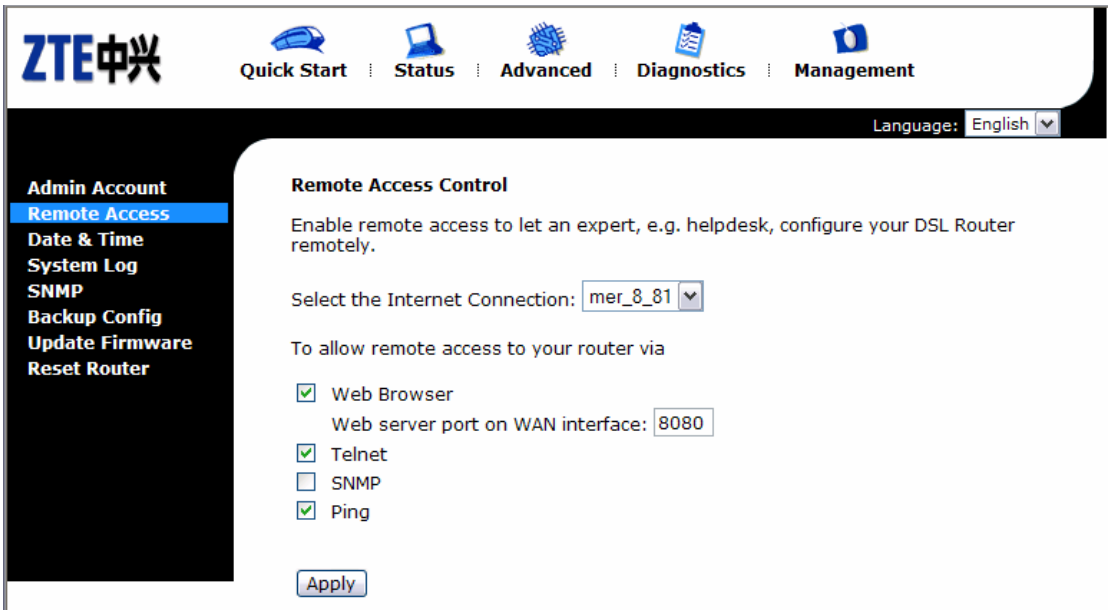
14. Finalmente el modem ADSL se reiniciará con la nueva configuración.



15. Para que no se tengan conflictos, en algunos casos se necesitará deshabilitar el servicio UPNP, para hacer esto se debe ir al menú Advanced y seleccionar el modo LAN, se desactiva la casilla y se aplica la configuración.



16. Finalmente si se desea realizar un monitoreo del equipo se debe activar el modo de control de acceso remoto, seleccionando el tipo de conexión entre el modem y el DSLAM que es mer_8_81 y el puerto 8080 para ingreso desde el browser o el telnet.



ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

Transmission Control Protocol / Internet Protocol (TCP/IP)	Es un protocolo compuesto sobre el cual se basa el funcionamiento de Internet, se encarga de establecer la conexión y el origen y destino de los datos.
Internet Service Provider (ISP)	Son compañías que se dedican a proveer a personas u otras empresas el acceso al Internet.
Consejo Nacional de Telecomunicaciones (CONATEL)	Órgano del estado encargado de elaborar las leyes de telecomunicaciones del Ecuador.
Secretaria Nacional de Telecomunicaciones (SENATEL)	Órgano del estado encargado de ejecutar las leyes de telecomunicaciones del Ecuador
Carrier Sense Multiple Access Collision Detect (CSMA/CD)	Protocolo usado en Ethernet que se encarga de censar y permitir el acceso al medio físico.
Media Access Control (MAC)	Segunda capa del modelo de referencia OSI, que se encarga de mantener el control del acceso al medio.
Digital Subscriber Line (DSL)	Es una tecnología que permite la transmisión de datos por el par telefónico.
Asymmetric Digital Subscriber Line (ADSL)	Línea de Subscriptor Digital Asimétrica en la cual el ancho de banda de bajada es mayor al ancho de banda de subida
ADSL Transceiver Unit at the CO (ATU-C)	Terminal ADSL que se encuentra en el extremo de oficina central.
ADSL Transceiver Unit at the Remote Terminal (ATU-R)	Terminal ADSL que se encuentra en el extremo del cliente.
Local Loop	En la tecnología DSL hace referencia al par telefónico por el se envían los datos.
Wireless Fidelity (WiFi)	Tecnología inalámbrica LAN estandarizada en las normas 802.11.
Worldwide Interoperability for Microwave Access (WiMAX)	Tecnología inalámbrica MAN estandarizada en las normas 802.16.
Point Multi Point (PMP)	Configuración de una red en la cual existe una estación central por la cual todo el tráfico de los demás equipos debe pasar para establecer la comunicación.
Quality of Service (QoS)	En los equipos de telecomunicaciones son parámetros que permiten tener un control de capa MAC y física, para cada conexión.
Certificado X.509	Es un certificado único, provisto por el fabricante, este certificado contiene la llave pública del equipo y su dirección MAC.

Sangolquí, 7 de Marzo del 2006

El proyecto de grado “Estudio Técnico Económico para Implementar Soluciones de Última Milla de Servicios de ISP en Ambientes Residenciales”, fue entregado a la Facultad de Ingeniería Electrónica.

ELABORADO POR:

Sr. Danny Ernesto Morales Briones

AUTORIDADES:

Sr. Xavier Martínez Carrera
Tnt. Crnl. Estado Mayor
Decano de la Facultad de Ingeniería Electrónica

Sr. Dr. Jorge Carvajal Rodríguez
Secretario Académico de la Facultad de Ingeniería Electrónica