Tecnologías Wireless y Movilidad en IPv4/IPv6

Luis Marrone | Andrés Barbieri | Matías Robles

Tecnologías Wireless y Movilidad en IPv4/IPv6

cacic2011 XVII CONGRESO ARGENTINO DE CIENCIA DE LA COMPUTACIÓN

XV ESCUELA INTERNACIONAL DE INFORMATICA

FACULTAD DE INFORMÁTICA
Universidad Nacional de La Plata

RedUNCI

Editorial de la Universidad de La Plata

Gil Costa, Graciela Verónica
Consultas sobre espacios métricos en paralelo. - 1a ed. -
La Plata: Universidad Nacional de La Plata, 2011.
136 p.; 24x16 cm.

ISBN 978-950-34-0721-9

1. Estrategias. 2. Procesamiento. 3. Web. I. Título
CDD 005.3

Tecnologías Wireless y Movilidad en IPv4/IPv6

Luis Marrone | Andrés Barbieri | Matías Robles

Coordinación Editorial: Anabel Manasanch
Corrección: María Eugenia López, María Virginia Fuente, Magdalena Sanguinetti y Marisa Schieda.
Diseño y diagramación: Ignacio Bedatou | Andrea López Osornio

Editorial de la Universidad Nacional de La Plata (Edulp)
47 N° 380 / La Plata B1900AJP / Buenos Aires, Argentina
+54 221 427 3992 / 427 4898
editorial@editorial.unlp.edu.ar
www.editorial.unlp.edu.ar

Edulp integra la Red de Editoriales Universitarias (REUN)

Primera edición, 2011
ISBN Nº 978-950-34-0721-9

Queda hecho el depósito que marca la Ley 11.723

Impreso en Argentina

Agradecimientos

Agradecemos la colaboración del Ing. Matías Cattaneo en los datos referidos al uso y asignación del espectro radioeléctrico en nuestro país.

Índice

Prefacio

Sin lugar a dudas estamos en un hito particular en la historia de Internet y de las redes en general que es la irrupción de las redes inalámbricas y la proliferación de dispositivos inalámbricos con la posibilidad de integrarse a diversos tipos de redes cada vez en un número mayor.

Fue algo muy difícil de prever que un experimento allá por 1979, que consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica y publicados en el volumen 67 de los Proceeding del IEEE, llegara a considerarse como el punto de partida de esta tecnología.

Las aplicaciones de las redes inalámbricas se multiplican diariamente. De momento van a crear una nueva forma de usar la información, pues ésta estará al alcance de todos a través de Internet en cualquier lugar.

Algo también muy importante, la ubicuidad que las acompaña ya ha producido cambios de hábito en los usuarios, en el trabajo y en la educación.

Muy pronto todos aquellos dispositivos con los que hoy contamos evolucionarán hacia aquellos en los cuales estarían reunidas las funciones de teléfono móvil, agenda, terminal de vídeo, reproductor multimedia, equipo portátil, etc.

En un futuro también cercano la conjugación de las redes Mesh, con las redes inalámbricas y las redes Grid podría llevar a cabo al nacimiento de nuevas formas de computación que permitan realizar cálculos inimaginables hasta el momento.

Los autores nos sumergimos en la aventura de esta publicación pensando que con este humilde aporte lograremos dar a conocer las bases de esta tecnología, su estado actual y su evolución y para que cuando estemos sentados a la mesa de un café accediendo a una página web o chateando con nuestros amigos disfrutemos más el momento que sólo el conocimiento de lo que ocurre nos brinda.

CAPÍTULO 1

Tecnologías WLAN 802.11

1.1 Introducción

En estos últimos tiempos las redes inalámbricas han experimentado un importante crecimiento. Su utilización se ha llevado a todos los ámbitos: empresariales, militares, gubernamentales y en nuestros propios hogares. Este capítulo, dentro de la diversa gama de tecnologías inalámbricas (**wireless**) utilizadas en redes de datos, se concentrará en brindar ejemplos prácticos sobre escenarios de protocolos WLAN (Wireless en redes de área local: LAN), explicando mediante estos su funcionamiento. Todos los ejemplos brindados serán protocolos de la familia de estándares IEEE 802, en particular se estudiará 802.11. En la figura 1.1 se muestra la relación entre algunos de los estándares IEEE 802 y su ubicación según el modelo OSI estandarizado por la ISO.

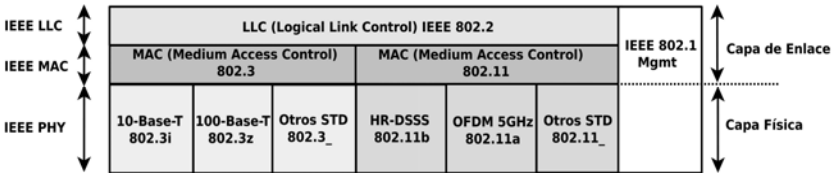


Figura 1.1 Estructura en capas de algunos estándares IEEE

Los protocolos estandarizados por IEEE en el conjunto 802 abarcan las dos primeras capas de acuerdo al modelo OSI: 1) Capa Física (PHY) y 2) Capa de Enlace (LNK). Esta última habitualmente se subdivide en dos sub-capas: 2.1) Sub-capa de Acceso al Medio (MAC - Medium Access Control) y 2.2) Sub-capa de Control Lógico de Enlace (LLC - Logical Link Control). Por cuestiones de complejidad la capa física también se la suele dividir en una capa dependiente del medio y otra que realiza tareas en un nivel superior. En el caso de 802.11 las dos sub-capas físicas son: 1.1) Sub-capa Asociada al Medio (PMD -Physical Media Dependent- y 1.2) Sub-capa Física de Procedimientos de Convergencia (PLCP- Physical Layer Convergence Procedure). 802.11, de la misma forma como sucede con otros estándares IEEE, abarca la mitad inferior de la capa de enlace (sub-capa MAC) y la capa física completa. Ver figura 1.2. En la figura 1.3 se muestra parte de la estructura del estándar IEEE 802.11.

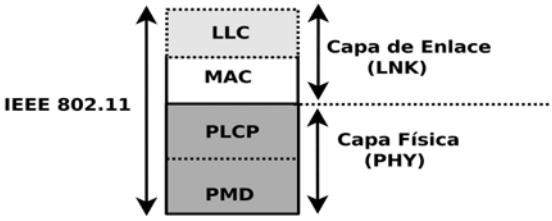


Figura 1.2 Parte de la estructura del estándar IEEE 802.11

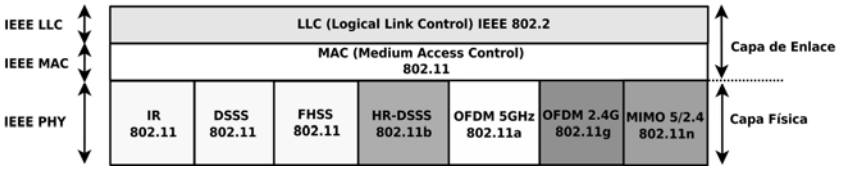


Figura 1.3 Algunas implementaciones del estándar IEEE 802.11

1.1.1 Algo de historia

En el año 1997, después de siete años de trabajo, la IEEE lanzó el estándar **802.11** como parte de la familia STD-802. La arquitectura es similar a la de los demás estándares de redes de datos, como por ejemplo 802.3 (Ethernet) u 802.5 (Token Ring). 802.11 define una arquitectura, procedimientos e infraestructura para desarrollar una red wireless de área local, comúnmente llamadas WLAN.

Implementaciones basadas en el primer documento fueron lanzadas al mercado en el mismo año en que estándar fue aprobado. En su definición original este incluía tres opciones de nivel físico: una sub-capa **Infrarroja (IR)**, que nunca fue muy difundida y ulteriormente eliminada en las siguientes revisiones y agregados del estándar, y otras dos utilizando radio frecuencias (RF) con la técnica de **Spread Spectrum (SS)** operando en la banda de ISM en 2,4GHz.

La tecnología en su principio permitía tasas de transferencia de 1 y 2Mbps. Para que lograse ser aceptada y difundida se necesitaron varias modificaciones y agregados al estándar original. Estos atacaban distintos puntos débiles del mismo. En el año 1999 la tasa de transferencia fue mejorada por dos nuevas versiones del estándar: **802.11a**, llevaba la tasa máxima a 54Mbps cambiando radicalmente la capa física, y **802.11b** que permitía alcanzar 11Mbps manteniendo compatibilidad con la versión anterior. Posteriormente, en 2003 con **802.11g**, se lograba alcanzar los 54Mbps con cambios similares a 802.11a, pero permitía, a tasas más bajas, seguir la compatibilidad con 802.11b a nivel físico. Este conjunto de protocolos, conocido como

a/b/g, permitieron desarrollar otras tecnologías que llegaban a los 108Mbps, aunque no fueron estandarizadas. Otro cuestión importante fue resuelta en el año 2005 por el estándar IEEE **802.11e**, el cual se ocupó de brindarle QoS. En tiempos más recientes, año 2009, el estándar **802.11n** utilizando la tecnología **MIMO (Multiple Input-Multiple Output)** promete alcanzar los 600Mbps.
802.11 es un grupo de protocolos pensados para la LAN, para redes MAN (Metropolitan Area Network) desde 2001 ha evolucionado el estándar IEEE 802.16 conocido como **Wi-MAX** o Broadband Wireless. Las redes Wi-MAX presentan un escenario diferente y serán estudiadas en otro capítulo.

1.1.2 Certificación Wi-Fi

De forma complementaria a los estándares IEEE 802.11, surge la necesidad técnica y comercial de asegurar la interoperabilidad entre los diferentes productos de los diversos fabricantes y vendedores. Para este propósito se creo la **Wi-Fi Alliance** (http://www.wi-fi.org/). Esta es una organización sin fines de lucro con el objetivo de promover el crecimiento de las tecnologías WLAN. Una de sus tareas consiste en certificar productos 802.11 compatibles. El término "Wi-Fi" y el logo (ver figura 1.4) son marcas registradas de la Wi-Fi Alliance y se utilizan para distinguir los productos 802.11 certificados por la misma. La Wi-Fi Alliance está conformada por una gran cantidad de personas y organizaciones en todo el mundo. Ésta fue creada en 1999, y, entre algunas de las organizaciones y empresas miembros, se pueden mencionar: Motorola, Cisco, Sony, Intel, Microsoft, Nokia, Samsung, Broadcom, Apple, AT&T, Juniper, AMD, etc.

Figura 1.4 Logo de la Wi-Fi Alliance

1.1.3 Objetivo de las redes WLAN

El objetivo de las redes WLAN definidas por los estándares IEEE 802.11 es proveer una funcionalidad similar a la que provee 802.3 o Ethernet para las redes LAN cableadas (wired) sin la necesidad de una infraestructura de conexión a través de medios guiados. Se debe mencionar que **no son un reemplazo** de las redes cableadas, sino una

alternativa a ser evaluada en el momento del diseño y el despliegue de una LAN. Es evidente que el tiempo de puesta en marcha de una WLAN es mucho más corto, pero es posible que sus características no se adecúen al escenario. Este tipo de redes deben ser consideradas como una extensión de las redes tradicionales. Dentro de sus principales ventajas se puede mencionar la movilidad del usuario sin pérdida de conectividad y el alcance a lugares donde sería casi imposible acceder con las redes LAN tradicionales.

1.2 IEEE 802.11: capa física

Como cualquier sistema de comunicaciones una red WLAN estará compuesta por componentes físicas, diversas codificaciones y señales. Este texto no tiene como objetivo tratar minuciosamente estas cuestiones ni llegar en profundidad a temas de "bajo nivel" (en el sentido de un modelo en capas). En esta sección se incluyen los elementos de forma de dar completitud pero sin ahondar en detalles especialmente físicos. Para obtener más información se propone consultar al lector la siguiente bibliografía: [SKL01],[GAS05].

1.2.1 Componentes físicos de una WLAN

Para construir una red de área local, y en particular una red wireless, se deben contemplar las siguientes componentes físicas esenciales:

Estaciones Terminales (nodo): llamadas habitualmente con el término inglés **station** o su abreviatura **STA**. Cualquier red de datos tendrá como propósito transferir información entre sistemas finales: estaciones de trabajo, estaciones terminales o, simplemente, estaciones. Una estación es un dispositivo de cómputo el cual posee interfaces de red. Para el caso de una WLAN alguna de las interfaces de red que posea el dispositivo debe trabajar de forma inalámbrica. Comúnmente, las estaciones en un sistema wireless son equipos portátiles como laptops, netbooks, palmtops, handhelds, alimentados eléctricamente por baterías de energía. Esto no prohíbe la utilización de equipamiento "fijo" como computadoras de escritorios (desktops), equipos servidores (servers) u otros.

Dispositivos Concentradores: si bien no son completamente indispensables, y, tanto en el caso de redes cableadas como inalámbricas se puede prescindir de estos, los **concentradores**: e.g. Hub, Switches, Access Points, son en la mayoría de los casos componentes primordiales en una red local. Para las WLAN los concentradores son conocidos con el nombre de **Access Point (AP)**, Puntos de Acceso y tienen como función

concentrar y controlar el tráfico de las estaciones terminales a la red. Los AP deben brindar un punto de conexión con otra red (en la mayoría de los casos cableada) cumpliendo funciones de gateway (bridge o router) entre los dos entornos: el inalámbrico y el cableado. Son equipos considerados intermedios que, para cumplir su función, deben tener al menos dos interfaces: inalámbrica y alámbrica (cableada). Vale mencionar que un AP puede ser considerado, en determinadas situaciones, como una estación, debido a que posee las componentes de software y hardware para funcionar como tal.

Medio físico: la información que se transmite de una estación a otra o a través del concentrador debe propagarse por un medio físico. Físicamente, toda información será transformada en una señal de energía que luego será transportada. En el caso de las redes cableadas el medio de transporte es un medio guiado que puede estar constituido físicamente por un conductor eléctrico como el cobre o, de un material dieléctrico, reflejante/refractante de la luz, como lo es la fibra óptica. En el primer ejemplo se transportará señales eléctrica y en el segundo señales lumínicas. En el caso de las redes wireless el medio físico, **Wireless Medium (WM),** será el espacio. Para los protocolos, en particular de 802.11, inicialmente fueron definidas y estandarizadas señales de radio frecuencias (RF); microondas (MW) y comunicaciones infra-rojas (IR). Hoy en día, el estándar 802.11 ha descartado las señales infrarrojas, quedando sólo el espectro de radio frecuencias de microondas[1].

Interfaces de Red: una interfaz o tarjeta de red, en términos de LAN conocida como NIC (Network Interface Card -habitualmente la letra "C" se la asocia con el término Controller) o NA (Network Adapter), es un circuito de hardware que conecta el bus del sistema de cómputo, estación o concentrador, con el medio físico por el cual se propagarán las señales de información. La interfaz de red, además de proveer la conexión física, tiene la "inteligencia" para transmitir los bits tomados del bus como señales por el medio y viceversa, recibir las señales y transformarlas en bits. Esta funcionalidad es nombrada transceptor o tranceiver, término que sugiere transmisión (Tx)/Recepción (Rx). Para el caso de una red wireless la NIC es llamada **WNIC (Wireless NIC)**. La WNIC tiene la función de controlar la transmisión y recepción de señales de radio

1)Se consideran microondas a las ondas electromagnéticas que abarcan un rango de frecuencias que oscila entre los 300MHz y los 300GHz) que se propagan por el espacio.

frecuencia sobre el espacio. Las interfaces de red wireless están equipadas con una antena la cual le permite transformar señales eléctricas en ondas de radio RF. Los sistemas inalámbricos pueden contar con una o más interfaces de red wireless y con cero o más interfaces "cableadas".

Antena: las antenas, término habitualmente abreviado como **ANT**, son componentes que sólo se encuentran en sistemas de comunicaciones inalámbricos. Una antena es un elemento físico que permite recibir las ondas de radio desde el medio físico y convertirlas en señales eléctricas. En un sistema de comunicaciones la antena también debe permitir el proceso inverso, es decir, transformar las señales eléctricas en RF. Las antenas, en el proceso de recepción, deben interceptar la energía irradiada de las ondas electromagnéticas y convertirlas en una magnitud eléctrica como voltaje. En la transmisión deben pasar de una corriente eléctrica a una onda electromagnética que será radiada en el espacio. Otra propiedad importante de las antenas es la formación del espectro de la señal irradiada, conocido como **beamforming**. Este término indica como la antena propaga la señal electromagnética, en qué dirección y a qué distancia. Otros parámetros definen la antena, como la frecuencia o la polaridad de la misma. Las interfaces de red de los sistemas wireless pueden contar con una o más antenas.

Sistema de Distribución: del inglés **Distribution System**, abreviado como **DS**. Los concentradores o AP inalámbricos se pueden combinar con otros concentradores inalámbricos o dispositivos que trabajan sobre una red cableada. En 802.11 un sistema de distribución se define como una componente que tiene el objetivo reenviar tramas para comunicar dispositivos inalámbricos con otros inalámbricos o alámbricos que están más allá de la cobertura de la celda wireless local, de esta forma permitiendo coberturas más amplias. Un DS se implementa "bridgeando" o "ruteando" las tramas entre los diferentes medios por los cuales se transmite y recibe la información. Habitualmente se lo llama también backbone o núcleo de la red.

En la figura 1.5 se muestra un diagrama de las componentes de un sistema WLAN y su relación.

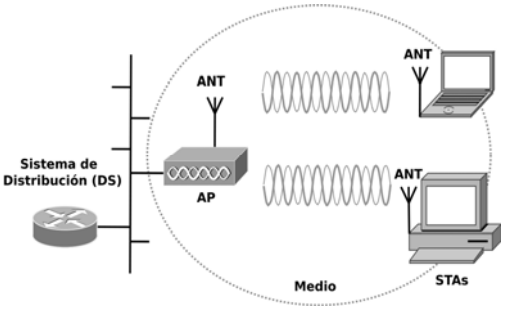


Figura 1.5 Diagrama de los componentes de un sistema WLAN

1.2.1.1 Antenas

Como ya se mencionó, la función de una antena es convertir la energía eléctrica en ondas de radio frecuencia cuando se transmite, y la operación inversa cuando se recibe información. De acuerdo a la teoría de antenas y campos electromagnéticos, la dimensión (tamaño) dependerá de la longitud de onda o de la frecuencia (la inversa de la longitud de onda) con la cual se trabaje en la transmisión de las señales. Para el caso de las redes WLAN estandarizadas por IEEE 802.11 las frecuencias están entre los 2GHz y los 5GHz, por lo cual su tamaño es pequeño y su alcance no supera una cobertura local[2].
Las antenas proveen 4 propiedades básicas a un sistema wireless:

- Polarización.
- Ganancia (en inglés Gain).
- Dirección.
- Patrón de radiación.

Es importante remarcar que las características de la antena dependerán de la relación entre sus dimensiones y la longitud de onda de la señal de RF que se transmita y/o reciba. Las antenas se diseñan para trabajar en un rango de frecuencias (banda), por eso una antena que trabaja en los 5GHz no serviría para la banda de los 2,4GHz.

1.2.1.2 Polarización de una antena

En términos simples se puede definir la polarización o polaridad como la forma en la cual se desplaza la señal en forma eléctrica con respecto al horizonte. Es la orientación de las ondas al "salir" desde la antena. Al momento de generarse la señal existen dos campos de energía, uno eléctrico y otro magnético, siendo uno perpendicular al otro

2)Si bien existen sistemas trabajando sobre estándares IEEE 802.11a o 802.11g que llegan a cubrir distancias de decenas de kilómetros, este no es el objetivo para el cual fue concebida la tecnología.

(desplazado 90 grados). La polaridad indica la forma de desplazarse del campo eléctrico generado. La figura 1.6 muestra un gráfico donde se incluyen los dos campos con respecto a la dirección en la que se transmiten los datos. La polaridad puede ser:

- Vertical: lineal, de arriba hacia abajo (más común).
- Horizontal: lineal, de derecha a izquierda.
- Circular: va cambiando en diferentes ángulos.

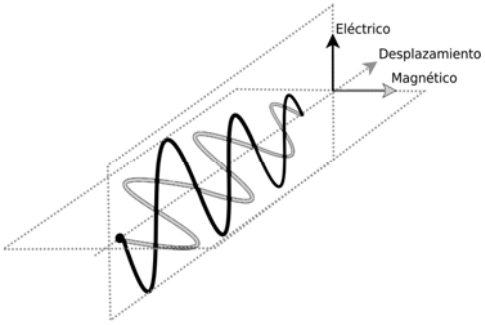


Figura 1.6 Campo magnético y eléctrico de acuerdo a la polaridad de la antena

Actualmente, se ven instalados equipos con una **Polaridad Lineal Oblicua**, desplazada 45 grados. En la figura 1.7.a se ve un ejemplo de una antena direccional con esta polaridad. La polaridad depende de la antena y como se la coloque. Las antenas habitualmente contienen una marca exterior indicando su polaridad. Es importante que la antena receptora y la transmisora tengan la misma polaridad para obtener un buen rendimiento en el enlace. En las figuras 1.7.b, 1.7.c y 1.7.d se muestra de forma gráfica tres ejemplos de polarizaciones diferentes (horizontal, vertical y circular).

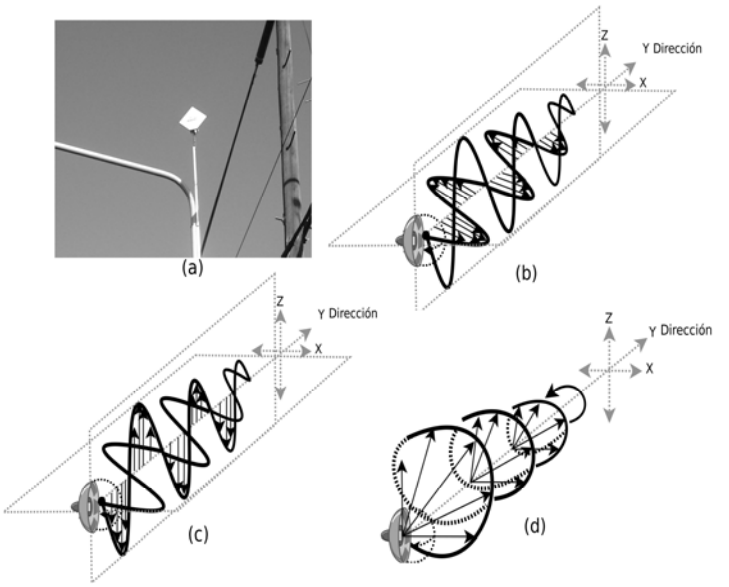


Figura 1.7 Antena con polarización oblicua y polarizaciones diferentes

La polaridad de la antena en la mayoría de los casos viene indicada en la misma con una etiqueta. En la figura 1.8 se muestra una foto de una antena tipo panel con un ejemplo de estas marcas que indican que posee una polarización circular.

Figura 1.8 Ejemplo de etiqueta que indica las polarización de una antena

1.2.1.3 Ganancia de una antena

La **ganancia (gain)** de una antena es la relación entre la potencia o energía de entrada con respecto a la potencia o energía de salida. Este valor se mide, habitualmente, en **dBi (decibelio isótropo)**. Esta magnitud compara la potencia máxima de salida de una antena particular con respecto a una antena de referencia **Isotrópica (Isotropic)**. Una antena isotrópica o dipolo perfecto es un caso "ideal" o teórico de un patrón de radiación esférico perfecto. En la figura 1.9 se muestra el patrón de radiación ideal de una antena isotrópica en el plano Vertical y Horizontal.

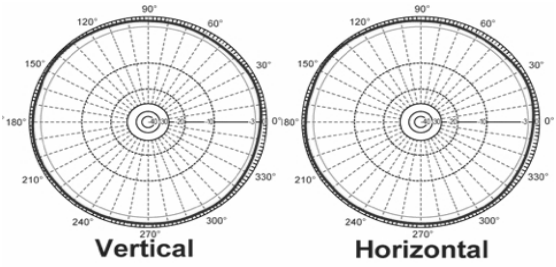


Figura 1.9 Patrón de radiación de una antena isotrópica

La potencia de entrada medida en Watts (Vatios en castellano) es la misma para las dos antenas. Es importante mencionar que una antena es un dispositivo pasivo, no consume energía ni aumenta la potencia. La antena para modificar la ganancia va a ofrecer diferentes patrones de radiación pudiendo así concentrar la energía en algunos puntos, a costa de perderla en otros que no son de interés. El patrón de radiación permite ofrecer mayor intensidad de la señal en determinadas áreas. La potencia de salida se mide en las áreas de mayor intensidad o mayor radiación. En estas mediciones no se consideran pérdidas ni ganancias externas. La siguiente ecuación muestra la definición de la ganancia en dBi.

$$Gain_{dBi} = \frac{DPower_{max}(ant)}{DPower_{max}(refant)} \frac{Watts}{m^2} \tag{1.1}$$

Una antena de mayor ganancia será aquella que tenga un patrón de radiación "más" direccional, es decir, que concentrará la energía en un espacio más acotado indicado en las zonas de radiación. Como el dBi se mide sobre una antena irreal (antena isotrópica) otra magnitud utilizada habitualmente es el **dBd**, que mide la ganancia con respecto a una antena real, similar a la isotrópica, antena **Dipolo (dipole)**. Un valor comparativo aproximado entre dBi y dBd es que $0.0dBd=2.2dBi$.

1.2.1.4 Dirección de una antena

La dirección o "directividad" de una antena se refiera a la medida de la concentración de la potencia radiada en una dirección en particular. Es la capacidad que tiene la antena para dirigir la energía radiada a una ubicación geográfica específica. Esta directamente relacionada con la **ganancia** y el **patrón de radiación**. Se compara la potencia en una dirección particular en comparación a la intensidad promedio isotrópica.

1.2.1.5 Patrón de radiación de una antena

El patrón de radiación de una antena es la medición de la direccionalidad de la antena en todos los puntos. Se suele representar con dos gráficos bidimensionales o con un gráfico tridimensional de la energía radiada. Para el caso de los gráficos bidimensionales se mide el patrón vertical y horizontal. El patrón Vertical o de Elevación (eje Z, eje X) y (eje Z, eje Y) es conocido como **E-plane**, y el patrón Horizontal o Azimuth (en castellano Azimut) (eje X, eje Y) conocido como **H-plane**. El E-Plane sería como ver la radiación desde un costado de la antena, o perfil, y el H-Plane sería como ver la radiación desde arriba o debajo de la antena. En la figura 1.9 se mostró el patrón de radiación de una antena isotrópica en ambos planos.
Las antenas se pueden clasificar básicamente en 2 categorías de acuerdo a la direccionalidad:

- Omni-direccionales
- Direccionales

Las antenas direccionales van a tener un patrón orientado a cubrir una región particular aumentando la ganancia. En cambio, las omni-direccionales buscarán cubrirla de forma más homogénea. Para un enlace punto a punto se utilizan antenas direccionales y, para dar conectividad en un aula, edificio o región a diversos usuarios se utilizan antenas omni-direccionales. Un importante fabricante de antenas y elementos asociados como amplificadores (amps/boosters), splitters y conectores a nivel mundial es HyperLink Technologies, recientemente comprada por L-com.
Para finalizar esta sección de antenas se incluyen de forma ilustrativa varias imágenes. En la versión impresa del texto se muestra en la figura 1.11 una antena direccional tipo yagui encapsulada, para el rango de frecuencias de 2,4 a 2,8 GHz con polarización vertical y una ganancia de 13.5 dBi. En la figura 1.12 se compara el tamaño de tres antenas omni-direccionales con diferente ganancia para la banda de 2,4GHz. La más chica es de 2.2dBi, la siguiente, en tamaño, es de 5.2dBi y la última de 5.8dBi. En la figura 1.10 (arriba) se muestra el patrón de radiación en ambos planos para una antena omni-direccional en 2.4GHz con una ganancia de 8dBi. En la figura 1.10 (abajo) se muestra el patrón de radiación, también en ambos planos, para una antena direccional tipo grid (parrilla) en 2,4GHz con una ganancia de 19dBi.

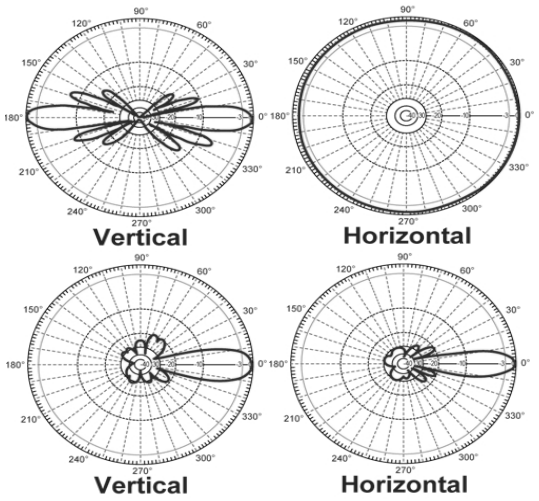


Figura 1.10 Patrones de radiación de una antena tipo dipolo y de otra grid direccional

Como material adicional, al que se puede acceder en el sitio http://sites.google.com/site/tecnologiaswirelessunlp/, se ofrecen varias fotografías digitales de antenas. En el archivo **wlan-ant/wlan-ant-dipole-2.4-2.0-dbi.jpg** se muestra una antena omni-direccional de 2.2dBi tipo dipolo para la banda de 2,4GHz utilizada en equipos cisco con conector RP-TNC. En **wlan-ant/wlan-ant-dipole-2.4-2.2-dbi.jpg** se observa otra antena omni-direccional dipolo usada en equipos Linksys (Cisco) en 2,4GHz con conector RP-SMA. En el archivo **wlan-ant/wlan-ant-omni-2.4-5.2-dbi.jpg** se muestra otra antena omni-direccional de 5,2 dBi para la banda de 2,4GHz con cobertura omni-direccional en el H-Plane (al patrón de radiación de un dipolo se lo comprime en el plano vertical dando mayor cobertura horizontal). En el archivo **wlan-ant/wlan-ant-grid-2.4-24dbi.jpg** se muestra una antena direccional tipo grid, de 24dBi para la banda de 2,4GHz. En la figura **wlan-ant/wlan-ant-dish-5-24dbi.jpg** se ve una antena direccional tipo plato (dish) para la banda de 5GHz con una ganancia de 24 dBi y, por último, en **wlan-ant/wlan-ant-yagi-2.4-13-dbi.jpg** se muestra la misma antena de la figura.

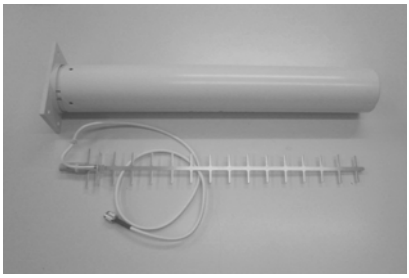


Figura 1.11 Ilustración de antena tipo yagui para 2,4GHz con 13,5dBi de ganancia

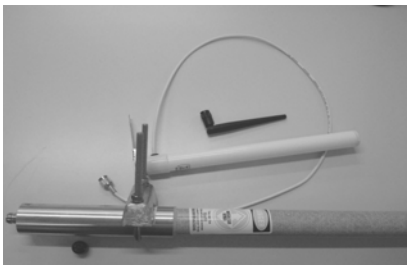


Figura 1.12 Ilustración de antenas omni-direccionales

1.2.1.6 Interfaces de red inalámbricas (WNICs)

Una interfaz de red inalámbrica (WNIC - Wireless NIC) se acopla al hardware de la estación o del AP mediante una conexión física que dependerá del bus del sistema host y del sub-sistema de entrada/salida del mismo. Algunos de los buses más comunes para una estación de escritorio son:

- PCI (Peripheral Component Interconnect).
- PCI-X.
- PCI-Express o PCI-e.

Actualmente, este último es el más difundido en equipos nuevos. El bus determinará la cantidad de líneas para la transferencia de datos: 16/32/64 ó más bits, la longitud del espacio direccionado, la velocidad de transferencia en ciclos por segundo (MHz), el manejo de las IRQ (interrupciones), la capacidad de "plug and play", voltajes y varios otros parámetros relacionados con el hardware. Para el caso de dispositivos laptops/netbooks se encuentran más comúnmente buses de los siguientes tipos.

- Mini-PCI.
- PCMCIA o PC Card (Personal Computer Memory Card International Association).

- Cardbus (versiones más nuevas de PCMCIA).
- Mini-PCMCIA o Express-Card, reemplazo de PCMCIA/Cardbus.

Cardbus es un bus PCI en el formato PC Card form factor y Express-Card un bus PCI-e. El bus USB (Universal Serial Bus) se encuentra igualmente difundido en ambos tipos de estaciones, utilizado con dispositivos wireless mediante una NIC USB externa que se acopla al sistema de entrada/salida. De acuerdo a la tecnología del bus serán las prestaciones que se puedan aprovechar, por ejemplo, el ancho de bus en bits, las frecuencias y velocidades de las líneas determinarán la tasa de transferencia máxima con la cual se puede trabajar. Otra cuestión importante es la alimentación eléctrica y el consumo de las WNIC que también determinará el tipo de bus necesario.

Dentro de la electrónica que conforma una WNIC la parte más importante es lo que se conoce como **Chipset**. El Chipset, o directamente chip, es un conjunto de circuitos integrados ensamblados en el mismo "dado" ("dice" en inglés) y diseñados para trabajar en forma conjunta. Un chipset usualmente incluye micro-procesadores, procesadores de señales (DSP), interfaces a buses, bancos de memoria y otras componentes. Algunos de los nombres de Chipsets más conocidos para WNICs son:

- Aironet (desarrollado por Cisco a partir del chipset Prism).
- Atheros (usado por Cisco, Ubiquiti y otros fabricantes).
- Broadcom (usados por varios fabricantes, entre otros DELL).
- Hermes/Orinoco (desarrollado por Lucent).
- Intel Centrino.
- Conexant, Prism (usados por ejemplo por 3Com).
- Realtek.

1.2.1.7 Ilustraciones de WNICs

Para ilustrar esta sección se incluyen dentro del material adicional algunas fotografías de WNICs. En la figura 1.13 se muestra una WNIC Cisco PCMCIA Aironet 350 con chipset Atheros que trabaja según el estándar IEEE 802.11b. En el archivo **wlan-wnic/wlan-wnic-802.11-lucent.jpg** se muestra una WNIC Lucent PCMCIA Wave LAN Turbo Bronze con chipset Orinoco que trabajaba según el estándar original de 1997 IEEE 802.11 en DSSS. En el archivo **wlan-wnic/wlan-wnic-fluke-802.11abg.jpg** se puede ver una WNIC Airmagnet PCMCIA distribuida con Fluke, WiFi Analyzer Pro-OptiView, que trabaja multi-banda según el estándar IEEE 802.11a/b/g en 2,4 y 5GHz. Esta WNIC posee un conector MMCX para agregarle una antena externa. En **wlan-wnic/wlan-wnic-802.11a-cisco-aironet-5ghz.jpg** se muestra

una WNIC Cisco PCMCIA Aironet con chipset Atheros que trabaja según el estándar IEEE 802.11a. El archivo **wlan-wnic/wlan-wnic-pcmcia-express-802.11n.jpg** muestra una WNIC DLINK PCMCIA-express (express-card) que trabaja según el estándar IEEE 802.11n en la banda de 2,4GHz (Fuente `http://www.dlink.com`).

Figura 1.13 Ilustración de WNIC Cisco PCMCIA 802.11b

En **wlan-wnic/wlan-wnic-802.11-lucent-isa.jpg** se muestra una WNIC de bus ISA donde se insertaba la placa Lucent PCMCIA Wave LAN Turbo Bronze. En la figura 1.14 (izquierda) se muestra una WNIC de bus PCI con una Cisco Aironet 350 trabajando en 802.11b. En los archivos digitales **wlan-wnic/wlan-wnic-minipci-mktk-802.11n.jpg**, **wlan-wnic/wlan-wnic-minipci-ubnt-802.11a.jpg** y la figura 1.14 (derecha) se muestran WNICs mini-pci con chipset Atheros, la primera es una Routerboard R52n 802.11n en 5GHz, la segunda una Ubiquiti 802.11a y la tercera (la figura de la derecha) una Routerboard R52-350 802.11a. Todos poseen un conector uFL para la antena (ver más adelante la sección de **Pigtails y Conectores**).

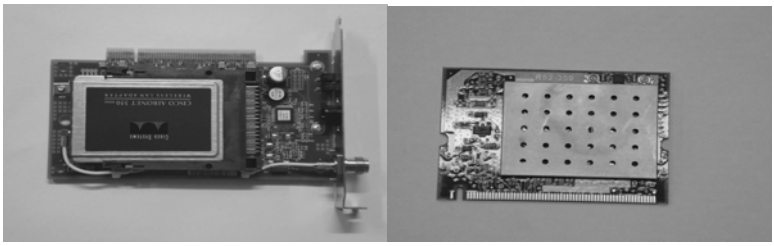


Figura 1.14 Ilustraciones de dos tipos de WNICs

1.2.1.8 WNICs: potencia de transmisión

La señal que genera una WNIC es de naturaleza electromagnética. La misma debe producirse con determinados niveles de energía y/o potencia para que se propague por el medio y sea captada por los

receptores. La potencia o fuerza de la señal (en inglés **signal strength**) va a depender en gran parte de la potencia con la cual trabaja la placa inalámbrica. Las WNIC pueden poseer amplificadores (signal boosters) que permiten aumentar la potencia de la señal generada. La unidad utilizada para la potencia es el Watt (W). El nivel de potencia con la cual la WNIC genera la RF se suele medir en decibelios de Watts (dBw) o de milliWatts (dBm). Los dB miden los valores en una escala logarítmica en base a un valor estándar, una razón (del inglés RATIO) entre el valor medido y el valor estándar conocido. En el caso de la potencia los valores de referencia son:

- dBm: el valor es comparado con estándar conocido de 1mW.
- dBW: el valor es comparado con estándar conocido de 1W.

$$Power_{dBm} = 10 \quad log_{10}\left(\frac{P_{out}}{P_{in}}\right) \qquad (1.2)$$

En la expresión matemática, P_{out} es el valor medido en la salida y P_{in} el estándar de referencia que se coloca en la entrada, en este caso 1mW ó 1W. Cuando el valor obtenido es mayor que el de entrada se obtienen números positivos, sino son negativos. Un valor negativo (–) significa una pérdida, uno positivo (+) significa ganancia. (0) significa que no hubo modificaciones sobre 1W ó 1mW. Las operaciones matemáticas se traducen a sumas y restas, ganancias y pérdidas.

1.2.1.9 Pigtails y conectores

Las WNIC además de los chips poseen una antena interna y/o un conector el cual permite adosarle una antena externa para acceder al medio wireless. Los conectores hacia las antenas externas pueden ser de diferente tipo. El cable que conecta la antena externa con la interna se conoce con el nombre de pigtail (cola de chancho). Un pigtail es un cable coaxil que transfiere microondas, en general corto, de 15 a 180 cm. aproximadamente, con un conector o interfaz física en cada extremo. Es extremadamente importante que este cable y sus interfaces (conectores físicos) tengan la menor pérdida posible. La pérdida, o atenuación de la señal, de la misma forma que la potencia o ganancia de una WNIC se mide en dBm o dBW y se combina como una resta en el cálculo de la potencia final. La pérdida aumentará acorde a la distancia del cable y al tipo del mismo. Por ejemplo cables de tipo LMR-100 tienen una pérdida de aproximada de 1.35 dB cada 100 cm utilizando frecuencias de 2500 MHz, LMR-400 son cables de menor pérdida 0.23 dB cada 100 cm. Es importante remarcar que la atenuación sufrida no es siempre la misma de acuerdo a la frecuencia. Existe una gran diversidad de conectores, algunos de estos que se encuentran en los pigtails son:

- Conector MC (utilizado en WNIC PCMCIA).
- Conector Type N y NM (usado comúnmente para conectar con la antena).
- Conector RP-TNC (usado comúnmente para conectar pigtail desde la antena en equipos Cisco y Senao).
- Conector MCX (utilizado por equipos Orinoco, Lucent, DELL o Proxim).
- Conector RP-SMA -Subminiature version A- (usado en equipos D-Link y Linksys).
- Conector MMCX (usado en WNICs Mini-PCI, Airmagnet y en equipos Cisco y Senao).
- Conector U.FL o uFL, son conectores miniatura para frecuencias de hasta 6GHz. (Utilizados comúnmente en WNICs Mini-PCI y en equipos laptops).
- Conector Coax BNC -Bayonet Neill Concelman- (usado en equipos viejos y en 10Base2).

Cada fabricante puede elaborar sus productos con diferentes conectores, luego, para obtener compatibilidad será necesario utilizar adaptadores, aunque estos puedan generar posibles pérdidas. Los conectores vienen en versiones male (macho) y female (hembra).

Para ilustrar al lector sobre algunos tipos de conectores se incluyen las siguientes fotos digitales como material adicional. El archivo **wlan-pgtail/wlan-pgtail-mc-female.jpg** muestra un conector MC hembra utilizado habitualmente para conectar a las WNIC PCMCIA una antena externa. El archivo **wlan-pgtail/wlan-pgtail-rp-tnc-male.jpg** muestra un pigtail con conector RP-TNC. En el archivo **wlan-pgtail/wlan-pgtail-mmcx-nf.jpg** se muestra un pigtail con conectores MMCX y NF(N female). En **wlan-pgtail/wlan-pgtail-n.jpg** se puede observar una antena con su conector N y atrás otro conector RP-TNC de otra antena. En la figura 1.15 se muestra un pigtail completo con conector UFL en un extremo y RP-SMA en el otro.

Figura 1.15 Foto de un pigtail con conectores UFL y RP-SMA

En la figura 1.16 se muestra un AP Cisco 1242G con conectores RP-TNC para antena externa utilizado en el laboratorio para componer el texto. Como material adicional el archivo **wlan-ap/wlan-ap-senao.jpg** contiene una foto de un AP Senao Long Range 802.11b con conector RP-TNC para antena externa. En **wlan-ap/wlan-ap-d-link-client.jpg** y **wlan-ap/wlan-ap-dlink-ap2100.jpg** se muestran dos viejos AP D-Link con conector RP-SNA para antena externa. En **wlan-ap/wlan-ap-ubnt-nanostation.jpg** se muestra un equipo Ubiquiti Nanostation el cual posee un panel interno y permite conectar externamente una antena vía un conector RP-SNA. En **wlan-ap/wlan-ap-ubnt-bullet.jpg** se muestra un Ubiquiti Bullet el cual se conecta a una antena mediante un conector N. El archivo **wlan-ap/wlan-ap-routerboard.jpg** muestra un integrado Routerboard 133 sin la WNIC mini-pci. En **wlan-ap/wlan-ap-symbol.jpg** se ve un antiguo AP Symbol 2,4GHz con conector BNC y su antena omni-direccional.
En los archivos indicados a continuación se encuentran fotos de cables pigtails completos. En la primera, **wlan-pgtail/wlan-pgtail-mmcx-n.jpg,** un cable LMR-195 para 5,8GHz de interior con conectores MMCX y N, en la segunda, **wlan-pgtail/wlan-pgtail-ufl-sma**, otro cable interior con conectores UFL y RP-SMA y, en la última, **wlan-pgtail/wlan-pgtail-rptnc-n.jpg**, un pigtail de exterior cable COAX LMR-400 con conectores RP-TNC y N.

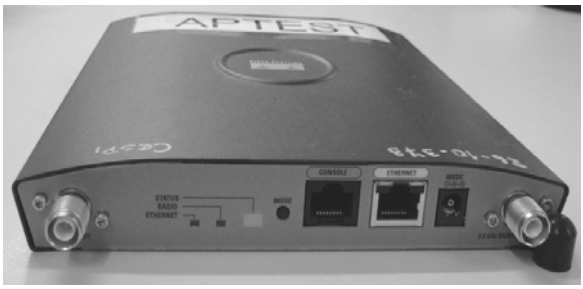


Figura 1.16 Foto de un AP Cisco 1242G usado para el texto

1.2.1.10 Potencia irradiada

El sistema transmisor de RF está compuesto por varias partes: WNIC, pigtail, antena, etc. Cada componente puede contribuir a aumentar o reducir la energía. Las regulaciones de potencia se realizan sobre la energía de la señal irradiada por el transmisor. Este valor medido se lo conoce como ERP (Effective Radiated Power) y es calculado en Watts (en ocasiones se lo encuentra expresado en dB). Otro valor relacionado es el EIRP (Effective Isotropic Radiated Power/Equivalent Isotropically Radiated Power), en español PIRE (Potencia Isotrópica Radiada

Equivalente). En el caso del EIRP, habitualmente es medido en dB, pero puede expresarse en Watts. El EIRP se mide en base a una antena isotrópica, en cambio el ERP es medido en base a una antena tipo dipolo de media onda. La ecuación para el cálculo del EIRP es la siguiente:

$$EIRP(dbm) = P - L + G \quad (1.3)$$

$$= PowerTx - LossCONN + GainANT \quad (1.4)$$

Donde *PowerTX* es la potencia de transmisión de la WNIC medida en dBm, *LossCONN* es la pérdida o atenuación incorporada por los pigtails y conectores de acople expresada en dBm y *GainANT* es la ganancia de la antena en dBi (medida con respecto a una antena isotrópica). Todos los parámetros tienen en cuenta la transmisión solamente. El EIRP permite estimar el área de servicio de la transmisión y regular la potencia con la cual trabajar de acuerdo a las normativas con el objetivo de limitar interferencia en lugares donde hay solapamiento de canales.
Este parámetro es regulado, por ejemplo, por la FCC o la ETSI internacionalmente, o por la CNC localmente y no debería superar determinados valores. Para equipos que funcionan como AP en 2,4GHz (802.11b/g), las regulaciones de la FCC indican que: considerando un **Maximum Transmitter Output Power** de 1W ó 1000mW, equivalente a 30dBm (este valor debería estar limitado en hardware para cumplir con las certificaciones de la FCC), el máximo EIRP permitido es de 36dBm (aprox. 4Watts de ERP), lo que consideraría una antena tipo de 6dBi y nula la pérdida de la conexión. Si se tiene una antena de mayor ganancia, se deberá disminuir la potencia en el transmisor. Algunos cálculos especifican hacer una relación 1:1 y otros 3:1, según regulación. De acuerdo se trabaje en un área cerrada (indoor) o un área abierta (outdoor) los parámetros cambian. En el caso de 802.11a/j (5GHz) -UNII Unlicensed National Information Infrastructure- según la FCC se disponen 3 bandas de un ancho de 100MHz, la primera destinada para espacios cerrados y las otras para espacios abiertos. Las regulaciones de la FCC son las siguientes:

- **UNII-1 (indoor):** 5,150GHz..5,250GHz. (2,5 mW/MHz). Max. potencia de Tx: 40mW = 16dBm + Antena 6dBi: 16dBm + 6dBi = 22dBm aprox. 160mW.
- **UNII-2 (indoor/outdoor):** 5,250GHz..5,350GHz. (12,5 mW/MHz). Max. potencia de Tx: 200mW = 23dBm + Antena 6dBi: 23dBm + 6dBi = 29dBm aprox. 800mW.
- **UNII-3 (outdoor):** 5,725GHz..5,825GHz. (50 mW/MHz). Max. potencia de Tx: 800mW = 29dBm + Antena 6dBi: 29dBm + 6dBi = 35dBm aprox. 3200mW.

Para enlaces punto a punto exteriores se permite utilizar los máximos de transmisión anteriores y aumentar la ganancia de la antena hasta un máximo de 23dBi, obteniendo una configuración con ganancia óptima. Más adelante se dedica una sección a las regulaciones en la República Argentina.

1.2.1.11 Pérdida en el trayecto completo

La pérdida en el trayecto completo, traducido del inglés **Path Loss**, tiene en cuenta la **Potencia Irradiada**, mediante el EIRP y, además, otros factores que tienen que ver con el medio por donde se propaga la señal y las características del receptor. Este parámetro se debe considerar para cada receptor posible. Algunos de los valores considerados son:

- EIRP.
- Ubicación geográfica de las antenas.
- Ganancia de la antena de recepción.
- Pérdidas en los cables y acoples en el receptor.
- Sensibilidad del receptor.

Una ecuación para estimarlo es la siguiente:

$$PathLoss\ (dB) = EIRP - (L + Lm) + (Gr - Lr) \qquad (1.5)$$

donde:

- *EIRP* es el Effective Radiated Power cuyo cálculo ya se explicó.
- *L* pérdida en el espacio libre, Free Space Loss.
- *Lm* son pérdidas misceláneas debido por ejemplo a la polarización incorrecta, "fading" (atenuación debido a multipath por rebotes) y otros posibles parámetros mal adaptados, medido en dB.
- *Gr* ganancia en la antena del receptor medida en dBi.
- *Lr* pérdidas en el receptor, por pigtails, conectores, etc. medido en dB.

Los valores para poder ser expresados en sumas y restas deben estar en dB. El cálculo de la Pérdida en el espacio libre *L* (Free Space Loss) se puede realizar con la siguiente ecuación y la unidad es en dB (en la primera parte de la ecuación la distancia y la longitud de onda se expresan en la misma unidad):

$$L_{FS}(dB) = 20 \times log[4\pi \times \frac{distance_{km}}{wavelength_{km}}] \qquad (1.6)$$

$$= 32{,}45dB + 20log[frequency_{MHz}] + 20log[distance_{km}] \qquad (1.7)$$

1.2.1.12 Umbral de ruido

A medida que la señal se traslada por el medio, se atenúa, degrada, pierde potencia. El parámetro **NF (Noise Floor)** (NF también se utiliza para indicar **Noise Figure**) se mantiene casi constante en el rango de cobertura pensado para 802.11, pero cuando se trabaja sobre distancias mayores la relación SNR (signal-to-noise ratio) en el receptor cambia notablemente, cuanto más lejos del punto central menores son los niveles de recepción. Si no existen obstáculos, la degradación de la señal puede ser calculada con la ecuación anterior. La pérdida en el espacio libre de obstáculos llamada **Free Space Loss** o directamente Path Loss, va a depender de la frecuencia de la señal y la distancia. Frecuencias mayores y distancias mayores significan valores peores para el Path Loss.
Un escenario más real es el cálculo de la **Interferencia Multi-camino (Multipath Interference)**. Este parámetro no puede ser calculado con una simple ecuación. En estos casos se debe tener en cuenta los problemas de la pérdida debido a la interferencia de los rebotes y otras señales. Esto ya es una cuestión que escapa a los objetivos del texto. Es importante aclarar que el ruido que afecta la señal, para hacer cálculos, es agrupado sumando todas las fuentes de interferencia que pueden afectar la misma. Este valor debe incluso considerar el ruido térmico. Con el valor agrupado se determina el NF que será el nivel de ruido por debajo del cual las señales recibidas no pueden ser detectadas en las mismas condiciones de medición. A mayor valor de NF, mayor potencia se requiere (aunque esto genera también mayor ruido térmico). Cuando la relación entre la señal recibida y el ruido agrupado en el factor NF no es suficiente, los datos no pueden ser interpretados. Los sistemas WLAN habitualmente calculan un umbral bajo el cual "toleran" el nivel de ruido. Se menciona este parámetro porque los equipos wireless habitualmente permiten configurarlo.
Otros parámetros a tener en cuenta en el cálculo de enlaces, del inglés **Link Budget Calculation**, son la **zona de Fresnel** y la curvatura de la tierra para enlaces de largo alcance, **Long Range**. La explicación del cálculo de estos términos trasciende los objetivos de este texto, se puede encontrar abundante material para su comprensión en libros da radiocomunicaciones [FRE99] o sitios de internet como: http://www.zytrax.com/tech/wireless/fresnel.htm

1.2.2 Capas físicas del Estándar 802.11

Como se mencionó, la capa física está dividida en dos sub-capas: Physical Medium Dependent (PMD) y Physical Layer Convergence Procedure (PLCP). La segunda es el nexo entre las trasmisiones sobre

el medio físico y la capa MAC. La PMD está relacionada directamente con el medio físico y se encarga de la transmisión/recepción de los bits "hablando" con la PLCP.

1.2.2.1 Capa dependiente del medio físico: PMD

Originalmente, en el estándar 802.11 de 1997 se definieron tres versiones de capa física sobre las cuales trabajar:

- Frequency-Hopping (FH) Spread-Spectrum (FHSS).
- Direct-Sequence (DS) Spread-Spectrum (DSSS).
- InfraRed light (IR), definida solo dentro del 802.11 original.

FHSS y DSSS trabajan en el rango de frecuencias conocido como ISM band 2,4GHz (Industrial Scientific Medical frequency, en español ICM: Industriales, Científicas y Médicas) y algunas implementaciones también funcionan sobre la banda ISM de 900MHz. La razón del uso de estas bandas de frecuencias se debió a que originalmente estaban reservadas en casi todo el mundo para RF (radio frecuencias) con propósitos de energía para la industria, médicos y científicos. En 1985, la FCC (Federal Communications Commission) en los Estados Unidos decidió liberarlas (no se exige un trámite formal ante el organismo regulador para su uso). Entidades reguladoras de las comunicaciones en otros países y/o regiones siguiendo la decisión de la FCC adoptaron medidas similares. En el momento del desarrollo del estándar la ventaja de no ser licenciadas en varios lugares geográficos del mundo y el hecho de no estar muy utilizadas en coberturas amplias[3] fueron las razones de su selección. Las tecnologías de IR para implementar 802.11 hoy en día son desaconsejadas. Más adelante en el tiempo, un rango de frecuencias en torno a los 5GHz se agregó.

Internacionalmente se conoce como "Bandas de Frecuencias no Licenciadas" a aquellas en las que se permite la operación de dispositivos de radiocomunicaciones sin una planificación centralizada por parte de la autoridad de comunicaciones competente. No se necesita un explícito permiso para cada equipo que permita asegurar la asignación del canal en forma exclusiva. Las bandas consideradas no licenciadas se utilizan sin subdivisión de canales por usuario, pero si se establecen ciertos requerimientos básicos de convivencia, tales como los que se mencionan más adelante, por ejemplo el límite de potencia radiada.

Cada país y/o región tiene sus propias entidades encargadas de la regulación de las comunicaciones. Las frecuencias sin licencias son definidas de acuerdo a las leyes locales. Existe un consenso casi

3)los hornos de microondas trabajan en las frecuencias de 2,45GHz y existen en casi todo el mundo, pero su alcance es muy reducido.

mundial en algunos puntos, por ejemplo otros organismos como el ETSI (European Telecommunications Standards Institute) con jurisdicción en Europa, y partes de Asia, el TELEC (Telecom Engineering Center) en Japón o la misma FCC de Australia y Nueva Zelanda han adoptado iguales medidas.
De cualquier forma el hecho de ser libres para su uso en estas regiones no implica que no existan controles, por ejemplo los fabricantes deben solicitar licencias para su producción. Otro punto importante es que la potencia utilizada en transmisiones en estas frecuencias debe ser limitada.
Para el caso de la Argentina el ente encargado de la regulación es la CNC (Comisión Nacional de Comunicaciones) y estas frecuencias en nuestro país no están completamente libres de licencias y uso. En este texto se dedica una sección con la información provista por la CNC que explica algunas regulaciones en nuestro país.
La capa física luego se extendió a otras nuevas tecnologías:

- Orthogonal Frequency Division Multiplexing (OFDM) en 5GHz, estandarizada dentro de 802.11a.
- High-Rate Direct-Sequence Spread-Spectrum (HR/DSSS) en 2,4GHz, estandarizada dentro de 802.11b.
- Orthogonal Frequency Division Multiplexing (OFDM) en 2,4GHz, Extended Rate Physical (ERP), estandarizada dentro de 802.11g.
- OFDM en 802.11a y ERP 802.11g con MIMO (Multiple-Input Multiple-Output) y otras técnicas que aumentan notablemente el rendimiento (throughput) estandarizada como 802.11n.

Debido a la utilización de bandas de uso compartido se requiere técnicas que permitan a la transmisión/recepción de las señales de información poder lidiar con la interferencia. La técnica utiliza en las tecnologías wireless 802.11 se conoce como **Spread Spectrum (SS)**, en español **Espectro Disperso** o **Espectro Ensanchado**. Este método de transmisión esparce la señal sobre una banda de frecuencias mucho más ancha que la necesaria para transmitir los datos que llevan la información. El resultado es una señal que ocupa más ancho de **Banda Analógico (wider bandwidth)** repartiendo la energía en el mismo. Se utiliza una función matemática que distribuye la potencia que se concentraba en un rango más estrecho en una banda más ancha. Esta técnica de SS, y otras de modulación digital como OFDM, para las bandas ISM en muchas regiones del mundo, no solo son necesarias para lograr mejor inmunidad al ruido externo, sino que son exigidas por las organizaciones reguladoras. Es importante mencionar que SS no es mágico ofreciendo total inmunidad al ruido y a la interferencia.

Si se tiene en una misma área muchas redes simultaneas utilizando las mismas frecuencias y sin controlar la potencia el resultado será una pobre, o casi nula conectividad.

1.2.2.2 "Bandas no licenciadas" en Argentina

Como se mencionó el ente regulador de la Rep. Argentina en la materia es la CNC (Comisión Nacional de Comunicaciones). La CNC es un organismo descentralizado que funciona en el ámbito de la Secretaría de Comunicaciones del Ministerio de Planificación Federal, Inversión Pública y Servicios, cuyas funciones son la regulación, contralor, fiscalización y verificación de los aspectos vinculados a la prestación de los servicios de telecomunicaciones, postales y de uso del Espectro Radioeléctrico. Las normas con respecto a su uso se materializan mediante resoluciones de esta entidad.
La terminología "Bandas no licenciadas" no es utilizada en la legislación local de comunicaciones, pero resulta muy difundida como término de uso en el sector. En las reglamentaciones de Argentina se utiliza el término "bandas de uso compartido". En el ámbito nacional, debido a que nuestro país se encuentre comprendido en la **Región 2 (Américas) de la ITU** (UIT en español, antiguamente llamada CCITT) comparte lo ordenado por el **Reglamento de Radiocomunicaciones de la ITU** sobre el uso del espectro en dicha área geográfica. Las condiciones imperantes dadas por usos y costumbres del mercado de equipos y servicios, resultan de igual forma determinantes en la orientación de las atribuciones de frecuencia de la administración argentina.
En nuestro país, siguiendo decisiones casi internacionales, se han destinado varias bandas para la modalidad de uso compartida. En el Reglamento de Radiocomunicaciones de la ITU se ha destinado a nivel mundial (y en algún caso, regional) bandas para uso primario para las aplicaciones Industriales, Científicas y Médicas (ISM). En el mismo se menciona las siguientes bandas:

- 13.553 .. 13.567 kHz (frecuencia central 13.560 kHz),
- 26.957 .. 27.283 kHz (frecuencia central 27.120 kHz),
- 40,66 .. 40,70 MHz (frecuencia central 40,68 MHz),
- 902,00 .. 928,00 MHz en la Región 2 (frecuencia central 915 MHz),
- 2400 .. 2500 MHz (frecuencia central 2450 MHz),
- 5725 .. 5875 MHz (frecuencia central 5800 MHz) y
- 24,00 .. 24,25 GHz (frecuencia central 24,125 GHz)

Éstas están designadas para aplicaciones ISM y los servicios de radiocomunicación que funcionan en dichas bandas deben aceptar la interferencia perjudicial resultante.

A esta descripción general dada por la ITU corresponde agregar una acotación sobre la modalidad de uso de estas bandas. Las mismas pueden ser utilizadas por usuarios particulares independientes por ejemplo, con teléfonos domiciliarios inalámbricos, o bien por un proveedor de determinado servicio, cuyo caso típico es el de acceso a Internet en áreas y localidades pequeñas. La modalidad de prestación está contemplada por diversos países, aunque con diferentes criterios. En el caso de Argentina, se lleva un registro (no restrictivo) de las estaciones concentradoras de tráfico o nodos, para los fines propios y para utilidad de los licenciatarios. De cualquier forma muy pocos son los registros realizados. Como sucede con las normativas internacionales, los equipos deberán estar inscriptos en los registros específicos del ente regulador, en este caso la CNC, es decir los fabricantes deben conseguir las licencias para su producción o los importadores licencia para su distribución.

La CNC define servicios primarios y servicios secundarios, dando que los secundarios no deberían interferir con los primarios. Los servicios de uso compartido, Sistemas de Spread Spectrum y de Modulación Digital de Banda Ancha (OFDM y modulaciones privadas), están atribuidos a la categoría secundaria. Esto significa que la operación de los sistemas está condicionada a no causar interferencia perjudicial a otros sistemas autorizados. Asimismo, deben tolerar la interferencia proveniente de otros equipos autorizados, contra la cual no estará protegido. En presencia de una denuncia de interferencia comprobada, generada por un sistema considerado secundario, se deberá suspender la operación del mismo hasta que se haya subsanado la situación. Por ejemplo, en la Res. 463/01 se menciona un sistema de multi-canales digitales existentes trabajando en la banda de 2,4GHz el cual es considerado primario y no debería ser interferido.

La Resolución 463/01 indica que los sistemas de comunicaciones Spread Spectrum en las bandas de 2400 MHz .. 2483,5 MHz y 5725 MHz .. 5850 MHz, tendrán la autorización sujeta a la presentación de información que describa sus características ante la CNC. Esta información incluye ubicación geográfica, frecuencias, anchos de banda digital, potencia y otras cuestiones indicadas en un anexo de la misma Resolución. Como se mencionó, son escasos los registros de acuerdo a la cantidad de redes inalámbricas existentes.

Adicional al **PIRE** o **EIRP**, se definen en las resoluciones de la CNC como parámetros para el control de potencia los siguientes términos:

Potencia Conducida de Cresta: es la potencia promediada máxima medida a la salida del transmisor, durante un intervalo de envolvente de modulación constante, bajo todas las condiciones posibles de modulación. La potencia máxima

promedio medida en la señal electromagnética de acuerdo a las Resoluciones de la CNC que indican el método de medición.

Densidad Espectral de Potencia conducida máxima: es la mayor densidad de potencia en la salida del transmisor medida dentro de la banda de emisión.

Potencia Radiada Aparente: la potencia suministrada a la antena multiplicada por la ganancia relativa de la antena, en una dirección dada.

La Resolución 302/98 indica limitaciones de potencia y características técnicas, para uso de Spread Spectrum con técnicas de secuencia directa (DSSS) y salto de frecuencia (FHSS) en las bandas de: 902 MHz .. 928 MHz, 2400 MHz .. 2483,5 MHz y 5725 MHz .. 5850 MHz. Para Modulación Digital de Banda Ancha, distinta de Spread Spectrum (en esta encuadra OFDM y técnicas propietarias) las normativas principales se incluyen en las Resoluciones 213/04 (para frecuencias de 2,4GHz) y 261/05, 288/02 (para frecuencias de 5GHz). Para otras bandas en 5GHz se encuentran las resoluciones 288/02 y 226/08.

Banda 902,00 MHz .. 928,00 MHz

Las especificaciones técnicas de la banda para trabajar en Spread Spectrum (DSSS y FHSS) se encuentran es su mayoría en la Resolución 302/98. Dentro de algunos parámetros se puede mencionar que la **potencia conducida de cresta máxima del transmisor** no debe superar **1 Watt** para sistemas con 50 ó más frecuencias de salto. Para sistemas con menos FH este valor es de 0.25 Watt. La ganancia de antena será tal que la **potencia aparente radiada máxima de cresta** no supere los **6 dBW**. En la actualidad existen equipos en 900MHz que trabajan en OFDM.

Banda 2400,00 .. 2483,50 MHz

Las especificaciones técnicas usando tecnologías de Spread Spectrum (DSSS y FHSS) se encuentran es su mayoría en la Resolución 302/98, se pueden consultar otras pertinentes como la Res. 463/01. Las características técnicas son básicamente limitaciones de potencia para evitar las interferencias mutuas y asegurar que se traten de emisiones de banda ancha. La potencia conducida de cresta máxima del transmisor en Spread Spectrum no debe superar 1 Watt. Para enlaces punto a punto, si la ganancia de la antena direccional supera los 6 dBi, se debe reducir 1 dB la potencia máxima del transmisor por cada 3 dB que dicha ganancia supere los 6 dBi. La anchura de banda de la emisión en DSSS no debe ser menor de 500 kHz para una atenuación de 6dB.

Para 2,4GHz con técnicas de modulación digital diferentes a Spread Spectrum según la Res. 213/2004 la potencia de cresta máxima

conducida tampoco debe exceder de 1 Watt y el **EIRP máximo es de 6dBW**. Los sistemas que se utilicen para transmisiones punto a punto podrán disponer de una ganancia de antena mayor de 6 dBi respetando la regla de disminuir la potencia conducida en 1 dB a partir de 1 Watt por cada 3 dB de exceso de ganancia de antena por encima de 6 dBi.
Se puede utilizar en modalidad compartida (Sistemas de Spread Spectrum y de Modulación Digital de Banda Ancha), tanto para uso privado como para prestación de servicios de telecomunicaciones de acuerdo a resolución 213/2004, excepto el servicio de Telefonía Básica en AMBA (Área Metropolitana de Buenos Aires)/ Ciudades Capitales de Estados Provinciales/Bahía Blanca/Mar del Plata/ Rosario) según Resolución 210/2004 que enmienda anteriores y acorde con 213/2004. Esta resolución para la limitación de ofrecer el servicio de Telefonía Básica queda sin efecto si el prestador se encontrarse brindando los servicios, o hubieren presentado la documentación tendiente a ello ante la CNC, con anterioridad a la publicación de la Res. 210/2004.
Esta banda, de acuerdo a la CNC, está contemplada en la Res, 30/30, donde la CNC habilitó los **Dispositivos de Baja Potencia** y otros con categoría secundaria, básicamente todos los dispositivos que emitan una **EIRP menor a 10 mW**, a que puedan funcionar sin autorización. Los dispositivos hogareños como routers inalámbricos, si bien son de uso privado y no requieren licencia, podrían necesitar registro de acuerdo a la potencia con la que trabajen. Si bien existe una planilla para hacer el registro y definir el recinto limitado de alcance (final de Res. 302/98), no es utilizado.
Esta banda es reconocida internacionalmente como parte de ISM, la CNC no adopta ninguna resolución aunque está aceptado este uso internacionalmente.

Banda 5725,00 .. 5850,00 MHz

De manera muy similar a la banda de los 2,4 GHz se puede utilizar tanto para uso privado como para prestación de servicios de Telecomunicaciones (excepto las áreas indicadas por Resolución 210/2004). Las características técnicas son básicamente limitaciones de potencia para evitar las interferencias mutuas y asegurar que se traten de emisiones de banda ancha. En la actualidad en este espectro no hay Dispositivos de Baja Potencia.
Las tecnologías empleadas son: SS (DSSS y FHSS) (Res. 302/98) y Modulación Digital de Banda Ancha, distinta de Spread Spectrum, por ejemplo OFDM u otras tecnologías propietarias (reguladas mayormente por Res. 288/02 y Res. 261/05). Estas son usadas para servicios secundarios, los cuales no deben interferir con los primarios.
Las limitaciones de potencia para Spread Spectrum son iguales que

para 2,4GHz, pero la ganancia de antena a antena para enlaces punto a punto fijos puede superar los 6 dBi sin que sea preciso reducir la potencia máxima del transmisor. Las especificaciones técnicas para Spread Spectrum encuentran en la Res. 302/98.
Para Modulación Digital de Banda Ancha, distinta de Spread Spectrum, la **Potencia Conducida de Cresta** para la banda de 5725 .. 5825 MHz no deberá exceder de **1 Watt**. La ganancia de antena puede ser de **hasta 23 dBi.** En caso que se supere ese valor, se disminuirá el valor de la potencia conducida de cresta y de la densidad de potencia conducida máxima en tantos dB como la ganancia supere dicho límite.

Otras bandas en 5GHz: 5150 .. 5250 MHz / 5250 .. 5350 MHz / 5470 .. 5725 MHz

Éstas son de **Uso Privado**, no pueden prestarse servicios de telecomunicaciones. Sólo pueden utilizarse Modulaciones Digitales de Banda Ancha (como OFDM) distintas a Spread Spectrum. Resoluciones relacionadas 288/02 y 226/08.
Según la Res. 288/02 para la banda de 5250 .. 5350 MHz la **potencia conducida de cresta** no debe exceder los **250mW**. y los parámetros de la antena son iguales que para la banda de 5725 .. 5825 MHz con Modulación Digital de Banda Ancha, distinta de Spread Spectrum.
Los requerimientos técnicos para la banda de 5150 .. 5250 MHz según la Res. 226/08 indican que se restringirán las emisiones a la operación en el interior de edificios, la **máxima potencia conducida** en la banda de operación no excederá de **50 mW** y la ganancia de antena podrá tomar valores tales que mantenga un **EIRP de 200 mW como máximo**.
Los requerimientos técnicos para la banda de 5470 .. 5725 MHz, según la Res. 226/08, indican que la **máxima potencia conducida** en la banda de operación no excederá de **250 mW**, la densidad espectral de potencia no excederá de 11 dBm en cualquier segmento de 1 MHz, y la ganancia de antena podrá tomar valores tales que mantengan un **EIRP de 1 Watt como máximo**.

1.2.3 Modulación y Codificación en 802.11

Para colocar la información de los datos a ser transmitidos sobre la señal de RF se utilizan dos operaciones: **codificación** y **modulación**.
La codificación es como se genera a partir de la señal de información una secuencia de 1s (unos) y 0s (ceros) apropiada para luego ser modulada y transmitida como RF. En este caso la información es digital y la codificación que se genera también es digital.
La modulación consiste en tener una señal **portadora** (en inglés CS: carrier signal) la cual es "combinada" con la señal de información, señal **moduladora**. En el caso de 802.11, la señal de información

moduladora es digital. El resultado será la señal **modulada**. En la modulación se trabaja modificando algunas propiedades de la portadora CS, como puede ser: frecuencia, fase y/o amplitud.

- Modulación por cambio de Amplitud: ASK (Amplitude Shift Keying).
- Modulación por cambio de Frecuencia: FSK (Frecuency Shift Keying).
- Modulación por cambio de Fase: PSK (Phase Shift Keying).
- Combinación de técnicas, trabajando con amplitud, fase y/o frecuencia.

Esta modificaciones se hacen de acuerdo a las valores de la señal de información de los datos digitales sobre la portadora. Los valores generados por la modulación son llamados símbolos. Las técnicas combinadas de codificación y modulación utilizada en los estándares IEEE 802.11 actuales son:

- DSSS y HR-DSSS (Direct Sequence Spread Spectrum y High Rate DSSS).
- OFDM (Orthogonal Frequency Division Multiplexing).
- OFDM Multi-stream Modulation (MIMO).

1.2.3.1 Frequency Hopping Spread Spectrum

FHSS es una tecnología que se consideró en el primer estándar, pero luego fue quitada. Los sistemas Frequency-Hopping trabajan saltando de una frecuencia en otra, en una serie pseudo-aleatoria, conocida previamente por emisor y receptor. Este patrón de frecuencias es recorrido en la transmisión enviando pequeñas ráfagas de datos en cada sub-frecuencia o sub-canal. Esta tecnología de capa física (FH PHY) se utilizó en la primera versión del estándar IEEE 802.11 permitiendo alcanzar tasas de 1Mbps y 2Mbps. Cada sub-canal en FHSS tiene un ancho de banda analógico de 1 MHz. En este sistema la frecuencia de portadora no es constante, varía a intervalos fijos bajo control de la moduladora (secuencia de codificación).

1.2.3.2 Direct Sequence Spread Spectrum

DSSS es la segunda variante a nivel físico considerada en el estándar inicial IEEE 802.11. En sus principios se uso con las tasas de 1Mbps y 2Mbps, pero luego permitió operar a velocidades mayores, desplazando directamente a FHSS. En la segunda versión del estándar de 1999 con esta capa física se permitían tasa de 5,5Mbbps y 11Mbps. En un sistema de espectro ensanchado o DSSS se modula con un código de dispersión de alta velocidad, “moduladora”, que se combina con la secuencia de bits de datos de información, “portadora”. La

secuencia del código de dispersión es la causante directa del ensanchamiento de la señal a ser transmitida ("señal modulada").

1.2.3.3 Codificación DSSS

Con esta técnica se utiliza en la codificación lo que se llaman **Chips** de información. Un chip de información es una porción de datos digital aún más pequeña que un **bit**. Para conformar el valor de un bit se requieren varios chips de información. Es el mismo principio que se utiliza en CDMA (Code Division Multiple Access).
Los chips son generados a partir de una secuencia pseudo-aleatoria que tiene una frecuencia mucho más alta que la del stream (flujos) de bits, por lo tanto, cada chip tienen una duración mucho más corta que un bit. Los chips de codificación que conforman la secuencia pueden valer +1 ó -1 y son parte de lo que se conoce como **CSeq (Chip-sequence)**, la cual tiene una duración finita y luego vuelve a repetirse (similar a la cadena de frecuencias de FHSS). Esta secuencia de **chips de codificación** habitualmente es llamada señal de ruido, en inglés: **noise signal**.
Cada bit de información es combinado con la secuencia de chips de codificación dando como resultado una secuencia de **chips de información**. A partir de un bit se genera una señal mucho más ancha en el espectro de las frecuencias. Por ejemplo, en DSSS el valor de un bit es "esparcido" a un valor de 11 símbolos o chips de información.
El receptor y el emisor deben conocer la secuencia de chips de codificación. En el caso de DSSS se utiliza una técnica que no requiere que estén completamente sincronizados: **asincrónico**. Si la señal se viera afectada por interferencias, con la redundancia agregada en el proceso de codificación o "chipificación", el receptor aún podría lograr reconstruir el bit original de las áreas no afectadas por el ruido. En la figura 1.17 se muestra gráficamente un ejemplo de SS.

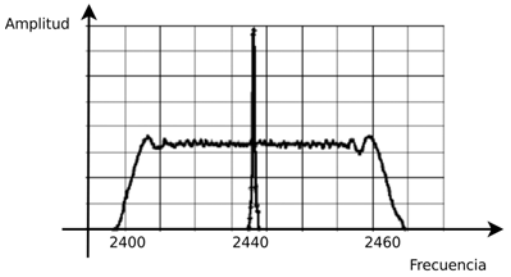


Figura 1.17 Ilustración del funcionamiento de la técnica de SS

En 802.11 para las velocidades de 1Mbps y 2Mbps se utiliza en el proceso de codificación una secuencia de chips llamada **BC (Barker**

Code). Los 11 chips utilizados son: <1,-1,1,1,-1,1,1,1,-1,-1,-1> o expresado en binario 10110111000. Esta secuencia posee propiedades matemáticas que la hacen ideal para la modulación en RF.
Para mayores velocidades Barker Code no es apropiado. En 802.11b para velocidades de 5,5Mbps y 11Mbps se utiliza una codificación llamada **CCK (Complementary Code Keying)**. Esta permite representar más bits por secuencia, utilizando más series de chips (Barker Code solo tiene 1 secuencia de 11 chips). Para 5,5Mbps se usa CCK-16 (4 secuencias) y para 11Mbps CCK-128 (64 secuencias).
Los anchos de los canales utilizados para cada transmisión son de entre 20 y 22 MHz. La señal no se distribuye completamente de forma uniforme sobre los 22MHz, en la parte central se concentra más energía, en los sectores adyacentes al central se filtra hasta 30dB de la potencia en el centro, y en los sectores periféricos se filtra a umbrales aún mayores, 50dB con respecto al centro. Esto permite que la interferencia de canales que se superponen en los bordes no afecte de manera importante la señal. En la figura 1.18 se muestra gráficamente la máscara del espectro en DSSS.

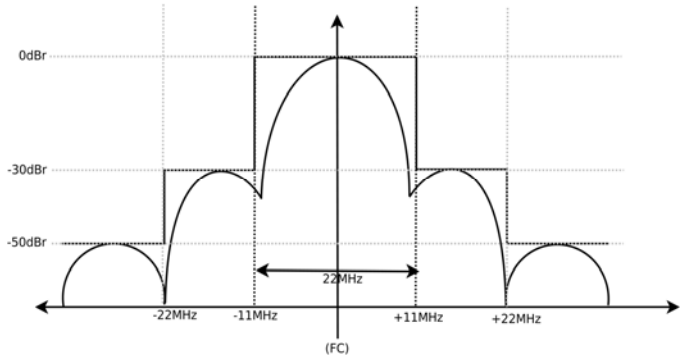


Figura 1.18 Diagrama de la máscara del espectro utilizada en DSSS

1.2.3.4 Modulación DSSS

Luego de codificar con Barker o CCK, se aplica la modulación. En la modulación cada bit se traduce a símbolos. Existen modulaciones 1 a 1 (donde cada bit está representado por un símbolo) o modulaciones que permiten agrupar más de 1 bit en 1 símbolo. IEEE 802.11 ha definido dos modulaciones para DSSS:

- DBPSK (Differential Binary Phase Shift Keying).
- DQPSK (Differential Quadrature Phase Shift Keying).

DBPSK es un método de PSK donde solo se utilizan 2 fases, dando 1 bit por símbolo. Al ser diferencial no trabaja con valores absolutos sino relativos al símbolo anterior. Esta modulación es solo usada para

tasas de transferencia de 1Mbps. DQPSK permite trabajar con 2 bits por símbolo y es utilizada para tasas superiores como: 2Mbps, 5,5Mbps y 11Mbps.

1.2.3.5 Orthogonal Frequency Division Multiplexing

OFDM es una técnica utilizada tanto en redes cableadas (e.g. xDSL) como inalámbricas. OFDM habitualmente no es considerada como técnica Spread Spectrum, aunque de alguna forma también "esparce" las señales de información sobre un ancho de banda analógico más amplio. OFDM es en sí una combinación de codificación y modulación.
OFDM divide un canal de RF en pequeños sub-canales, cada uno con su sub-carrier (sub-portadora). Cada sub-carrier es una portadora en si usada para transportar datos de streams de información en paralelo. Cada sub-canal puede llevar información independiente de los otros, aunque en la práctica, en 802.11, se utilizan para llevar información de la misma transmisión. La diferencia con FDM tradicional, es que FDM requiere canales de guarda entre cada frecuencia reduciendo así la capacidad total a utilizar por los datos. En OFDM los canales se superponen parcialmente pero no interfieren entre sí. Las **frecuencias fundamentales son ortogonales (orthogonal sub-carriers)**, están separadas espacialmente de forma mínima, permitido por la ortogonalidad entre ellas, de esta forma se evita la interferencia entre los distintos streams. La ortogonalidad de las frecuencias es una propiedad que se obtiene matemáticamente y su explicación detallada esta fuera de los objetivos de este texto. Cada portadora podría ser modulada con una técnica, como QAM o PSK, cada una tendría una baja tasa de transferencia de símbolos (symbol rate), siendo la suma de estos la señal original sin descomponer (single-carrier). De esta forma se pueden alcanzar altas tasas de transferencia sumando las transferencias de cada sub-carrier. Una ventaja que provee OFDM como las demás técnicas de SS es que la interferencia o ruido puntual solo afectará a una parte de la señal, pudiéndose reconstruir esta a partir de las regiones del espectro no afectado. En la figura 1.19 se muestra un gráfico con un ejemplo de OFDM donde se distingue el single-carrier de múltiples carriers.

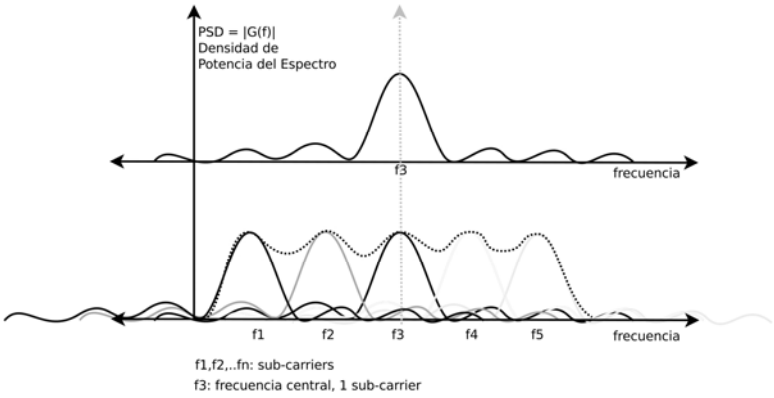


Figura 1.19 Ilustración de cómo funciona la técnica OFDM

El estándar IEEE 802.11a/g utiliza 52 sub-carriers en un canal con un ancho total de 20MHz. Se usan 48 sub-carriers para datos y 4 para pilots (canales de sincronización entre los carriers de información). Se utilizan sub-bandas exteriores reservadas para protección entre diferentes canales. Los sub-carriers utilizados para datos son: -26..-1,1..26 menos los sub-carriers utilizados para pilots: -21, -7, 7, y 21. La frecuencia 0 (cero) identificada como la componente continua (DC) no es utilizada. En la figura 1.20 se muestra esquemáticamente un ejemplo de la distribución de las sub-carriers de datos y los pilots en OFDM.
La primera utilización de OFDM en el estándar fue con IEEE 802.11a/j en 1999, luego se traslado esta técnica al más reciente IEEE 802.11g. Los anchos de analógico de cada sub-canal son de 300 kHz. Los canales completos forma similar a DSSS ocupan un ancho de 20MHz. OFDM también es utilizado en 802.11n con algunos agregados.

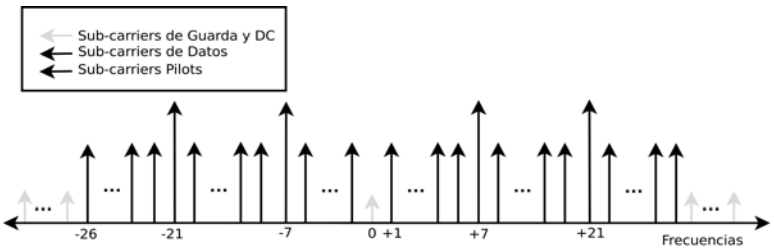


Figura 1.20 Diagrama de los sub-carriers y su separación en OFDM

1.2.3.6 Modulación OFDM

OFDM agrega el uso de nuevas modulaciones a DBPSK y DQPSK. Estás son:

- 16QAM (16 Quadrature amplitude modulation).
- 64QAM (64 Quadrature amplitude modulation).

Estas técnicas combinan modificaciones de amplitud y fase sobre la portadora para modular más bits en un mismo símbolo. De esta forma, con más bits por símbolos se obtienen tasas de transferencias superiores. 16QAM permite 4 bits por símbolo y 64QAM 6 bits. En la figura 1.21 se muestra el diagrama de constelación de la modulación 16QAM (Fuente: Wikipedia: Quadrature amplitude modulation: http://en.wikipedia.org/wiki/Quadrature_amplitude_modulation. Licencia del gráfico: GNU Free Documentation License).

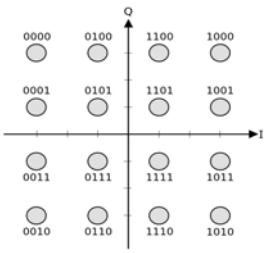


Figura 1.21 Diagrama de constelación de la modulación 16QAM

1.2.3.7 Codificación OFDM

OFDM trabaja codificando los datos en los diferentes sub-carriers que genera. El método de codificación se conoce como **Convolution Coding (CC)**. Esta codificación utiliza algunos sub-carriers para llevar datos y otros para generar códigos de corrección de errores, de forma similar que lo hace un bit de paridad o un CRC. De acuerdo a la cantidad de sub-canales que usa para datos en relación con los utilizados para la corrección/detección de errores va a ser la tasa de transmisión obtenida. La cantidad de sub-canales máxima para 802.11g, como ya se mencionó es de 48. De estos 48 algunos son usados para datos puros y otros para los errores. Esta relación se la denomina *R*. Sus valores pueden ser de 1/2, 2/3 ó 3/4. En el caso de 1/2 se utilizan la mitad de los sub-canales para corrección de errores, en el caso de 3/4 sólo 1/4 de los sub-canales de datos, o sea 12 se usan para detectar y corregir errores. La cantidad de sub-símbolos por segundo siempre es de 250000 en c/sub-canal. En el cuadro 1.22 se muestra la relación de la codificación con los bits por símbolos y las modulaciones de acuerdo a la tasa de transferencia. Por ejemplo, la tasa más baja es de 6Mbps se usa DBPSK (1bit, 1 símbolo) con 24 bits de datos y 24 bits de corrección de errores dando: 24*250*Ksps*=6*Mbps*. Para 9Mbps también se usa DBPSK, pero con 36 sub-canales para datos dando: 36*250*Ksps*=9*Mbps*. Para 54Mbps se usan 64QAM (6 bits por símbolo) y 36 sub-canales de datos dando la tasa máxima: 36*250*Ksps**6*bits*=54*Mbps*.

Speed (Mbps)	Modulation and coding rate (R)	Coded bits per carrier	Coded bits per symbol	Data bits per symbol
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216

Figura 1.22 Tabla de modulaciones utilizadas con OFDM

1.2.3.8 Intervalos de Guarda en OFDM

El retardo (delay) de los símbolos modulados y transmitidos en OFDM depende del entorno en el cual se trabaje. En un entorno cerrado, indoor, estos valores pueden ser chicos, en cambio en un entorno abierto pueden variar notablemente. La velocidad de propagación va a depender de la frecuencia. Tomando como referencia la velocidad de la luz, *c*, se considera que las RF de WLAN se propagan a este valor, 30 cm/ns. La señal de RF al transmitirse también puede rebotar en el entorno y de esta forma se producirán múltiples caminos con diferentes tiempos de arribo (debido al eco y la reflexión). Los diferentes caminos pueden generar interferencia entre sí, produciendo lo que se conoce como **ISI (Inter Symbol Interference)**. La diferencia entre los tiempos de arribo está entre 50 y 200ns (lo normal 100ns). Para evitar la ISI con otros datos transmitidos del mismo flujo se utilizan espacios, "buffers" de tiempo en la transmisión para que el receptor pueda acomodar los símbolos que arriban tarde o desfasados. Estos tiempos se conocen como **Intervalos de Guarda**, en inglés **Guard Intervals (GI)**. Comúnmente en 802.11a/g se establecen a 4 veces el valor máximo del delay, considerando un delay máximo de 200ns, 200ns * 4 = 800ns. La duración de los símbolos es mucho más grande que este GI. La selección de la duración de los datos transmitidos como símbolos debe ser al menos 5 veces el GI, dando un tiempo de 4µs, 800ns * 5 = 4000ns. En el caso de 802.11n el tiempo de GI es acortado. En la figura 1.23 se muestra la utilización del GI.

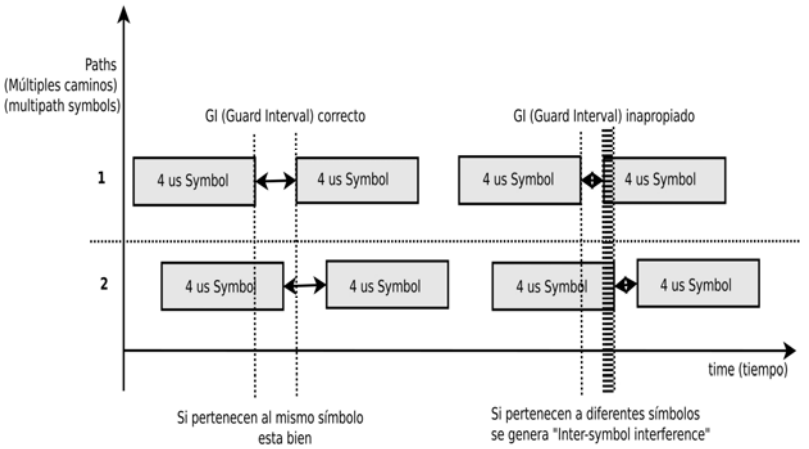


Figura 1.23 Diagrama de la utilización de los intervalos de guarda (GI)

1.2.3.9 Codificaciones adicionales en 802.11g

Las codificaciones usadas por DSSS en 802.11b pueden ser Barker Code o CCK. Un pre-estándar conocido como **802.11b+** incorporaba una nueva codificación llamada **PBCC (Packet Binary Convolutional Coding)**, la cual permitía a 802.11b lograr el doble de "velocidad": 22Mbps, manteniendo la compatibilidad. Luego, 802.11g genera varias posibles especificaciones para el nivel físico. Este conjunto se lo conoce como **Extended Rate PHY (ERP)**. Las diferentes alternativas son:

ERP-DSSS / ERP-CCK: modo compatibilidad hacia el primer estándar: 802.11 (1Mbps y 2Mbps) y hacia el segundo 802.11b (5,5Mbps y 11Mbps)

ERP-OFDM: el modo principal de 802.11g el cual permite alcanzar mayores velocidades: (6, 9, 12, 18, 24, 36, 48, 54 Mbps). Solo son obligatorias para cumplir con el estándar: 6, 12 y 24Mbps.

ERP-PBCC: extensión opcional que utiliza una nueva codificación. Permite alcanzar 22Mbps y 33Mbps. No se implementa en la mayoría de los casos.

DSSS-OFDM: modo híbrido que usa ambas codificaciones. Se termina modulando en OFDM, por lo cual no es compatible con 802.11b. Tampoco está muy difundida su implementación.

1.2.3.10 HiperLAN, HiperLAN/2 a nivel Físico

HiperLAN (High Performance Radio LAN) es un estándar para WLAN realizado en Europa por la ETSI. En muchos aspectos es

similar a 802.11a, por ejemplo usa las mismas bandas y alcanza los mismos rates (tasa de transmisión). No es compatible con 802.11. A nivel físico HyperLAN/1 trabaja con FSK (Frecuency Shift Keying) y GMSK. HyperLAN/2 trabaja con BPSK, QPSK, 16QAM y 64QAM. HyperLAN/2 es el que tiene más similitud con 802.11a. Algunas características físicas de HiperLAN como Dynamic Frequency Selection (DFS) y Transmit Power Control, fueron trasladadas a los estándares 802.11a y 802.11n.

1.2.3.11 PMD en 802.11n

802.11n [802.11n] es una modificación/agregado al estándar 802.11-2007 [802.11]. En el año 2004 el **IEEE 802.11 Task Group N (TGn)** fue formado para analizar y trabajar las formas de llevar el rendimiento de estas tecnologías wireless a 100Mbps. Se presentaron 4 propuestas: MITMOT ("Mac and mImo Technologies for More Throughput"), TGnSync, WWiSE y Qualcomm, de las cuales quedaron dos: TGnSync, esponsoreada entre otros por Intel y Philips; y WWiSE generada por Broadcom. En el año 2005 ambas se consolidan bajo un borrador de la IEEE. En septiembre de 2009 se ratifica el borrador del protocolo 802.11n y pasa de TGn Draft 2.0 a estándar.
Previo al estándar IEEE 802.11n existieron varias extensiones para permitir superar la barrera de los 54Mbps. Algunas fueron las siguientes:

- **125HSM:** permitía hasta 125Mbps, 125 High Speed Mode, desarrollada por Broadcom, utilizaba la técnica de frame-bursting y compresión. Implementada por Linksys con el nombre de **SpeedBooster**.
- **Super G:** permitía hasta 108Mbps, desarrollada por Atheros, utilizaba frame-bursting, compresión y channel-bonding. Implementada por Toshiba, Sony, D-LINK. Sobre 802.11g.
- **Super AG:** permitía hasta 108Mbps. Desarrollada también por Atheros. Es la tecnología **Super G** llevada a las frecuencias de 802.11a. Conocido como **Turbo-Mode**. Aprovechada por ejemplo por el fabricante Mikrotik sobre chips Atheros y Ubiquiti.
- **NStream:** técnica que utiliza frame-bursting, MIMO y pares de WNICs (dual NStream), propietaria del fabricante Mikrotik, utilizada para enlaces punto a punto.

Algunas tecnologías que aportaron al estándar:

- **WWiSE:** el consorcio WWiSE conformado por varios fabricantes de chips genero un pre-estándar que incorporaba las tecnologías de agregación y ráfagas de tramas con optimización de los

ACKs. A nivel físico incorporaba algunas modificaciones a 802.11a.

TGnSync: este consorcio también estaba conformado por varias compañías del rubro. El aporte principal de este grupo fue el channel-bonding y el formato de las tramas. Incorporaba otras técnicas como compresión de encabezados y agregación de tramas.

IEEE 802.11n trabaja sobre las frecuencias de 802.11a y/o de 802.11b/g, siendo compatible hacia atrás. Es un estándar abierto, certificado por Wi-Fi Alliance (Desde Draft 2.0). El objetivo del estándar es lograr mayores tasas de transferencias que las propuestas hasta el momento para redes WLAN, logra potencialmente hasta 600Mbps (nominal, lo que se obtiene efectivamente en transferencia de datos de usuarios oscila entre 100 y 200Mbps real. Permite lograr mayores coberturas, e.g: 30mts con 802.11a/b/g contra 50mts con 802.11n. En la sub-capa PMD trabaja con OFDM y los principales agregados a este nivel son:

- MIMO (Multiple Input - Multiple Output): PHY Layer.
- Canales más anchos: de 20MHz a 40MHz: PHY Layer.

1.2.3.12 MIMO (Multiple Input - Multiple Output)

MIMO es una modificación de capa física (PHY), permite aprovechar el uso de múltiples antenas para transmisión y recepción dando lugar a varios **Radio Chains**: múltiples caminos físicos. En los estándares previos, a/b/g el **multipath**, es "destructivo" ya que aumenta el ruido, pues se produce interferencia entre las mismas transmisiones al llegar a destiempo.

Previo a la técnica de MIMO se utilizaba lo que se conoce como **Diversity con Múltiples Antenas**. Los AP a/g con múltiples antenas no funcionan con MIMO, utilizan para recibir solo la antena que mejor capta la señal, amplitud más alta, en cada momento (una por vez, no en paralelo). Para la transmisión solo seleccionan una, la cual se podía ir cambiando. En el archivo **wlan-phy/wlan-phy-diversity.jpg** se muestra un ejemplo de está técnica con 2 (dos) antenas.

- Ventajas MIMO:
  - Permite alcanzar mayores tasas de transmisión.
  - Permite mayor cobertura.
  - Mantiene el la potencia de transmisión sin requerir mayor bandwidth analógico.
- Desventajas MIMO:
  - Requiere CPUs/DSP más potentes, consume más energía.
  - Requiere más antenas, hardware más sofisticado, mayor costo.

Dentro de las técnicas MIMO se puede enumerar las siguientes:

Beamforming (TxBF): significa dar forma al espectro/haz electromagnético. En el caso de single-layer (una frecuencia) en lugar de irradiar la señal en forma omni-direccional, intenta detectar donde se encuentra el cliente/estación y trata de dar forma al espectro para optimizar la recepción en este. Se realiza aumentando la ganancia y la amplitud relativa en algunas antenas y bajándola en otras. Se deben alterar las fases de transmisión. Al transmitir desfasado, múltiples caminos pueden llegar en fase, así se mejora la amplitud de la señal recibida. De esta forma se logra el **Multipath Constructivo**. En el receptor se debe realizar la combinación de las señales mediante **MRC: Maximum Ratio Combining**, para agrupar múltiples señales recibidas de forma lineal, incrementando así la calidad de la recepción. Esta técnica es utilizada en espacios abiertos y contra un solo receptor. Beamforming no es "optimizable" para varios receptores o broadcast/multicast y permite trabajar con clientes sin soporte de MIMO.

El **Precoding:** es un concepto más general que Beamforming: **Multi-stream Beamforming**. El objetivo también es maximizar la potencia de la señal en el receptor/los receptores, pero en transmisiones multi-layers (usa múltiples antenas y múltiples frecuencias: diferentes **dominios de beamforming**).

El **Precoding/Beamforming Adaptativo** mejora el rendimiento. Este requiere "feedback" del receptor. Esto se logra mediante una técnica llamada **Channel State Information (CSI)**. Se puede obtener de forma estadística a largo plazo, **SCSI (Statistics CSI)** o instantánea **ICSI (Instant CSI)**. En el caso de recibir la retroalimentación se llama de lazo cerrado, **CSI de Closed-loop**. Si se puede predecir por el emisor sin obtener el "feedback", se llama de lazo abierto, **CSI de Open-Loop**.

Spatial Multiplexing (SM/SMX): otra técnica de MIMO. Consiste en dividir un stream de datos en varios (múltiples) de menor "velocidad" que se transmiten por diferentes antenas compartiendo la misma frecuencia. Cada sub-stream lleva diferentes datos. La separación temporal (diferentes fases) entre los streams generados debe permitir al receptor distinguirlos y luego poder juntarlos para obtener la señal original. Se puede usar con CSI (feedback) o sin CSI. No trabaja con clientes No-MIMO. En la figura 1.24 se muestra un ejemplo de SMX.

Diversity Coding: en esta técnica se transmite un solo stream de datos codificado con **Space-time Code (STC)**. Se transmiten

múltiples copias, esperando que al menos una sobreviva. La señal es emitida desde cada antena transmisora, con codificaciones ortogonales. No utiliza CSI (feedback). No hay posibilidad de beamforming con esta técnica, ya que es Open-Loop. Utiliza técnicas complejas de codificación, e.g. Trellis Codes. Útil en medio con mucho ruido, SNR bajos.

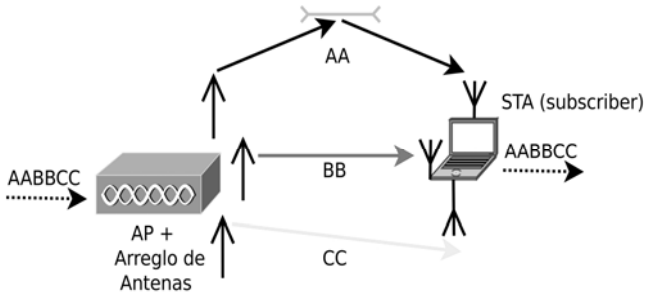


Figura 1.24 Ejemplo de la técnica MIMO SMX

Beamforming no es parte del estándar IEEE 802.11n hasta ahora. Esta técnica es utilizada en WiMAX (802.16) y tecnologías de cell-phones. 802.11n utiliza SMX y/o Diversity Coding. Se pueden configurar algunas antenas para recepción y otras para transmisión o usar todas al mismo tiempo para transmisión o para recepción (en este caso se trabaja en HDX). Para que el Spatial Multiplexing funcione de forma adecuada se debe asegurar la separación de las señales en la dimensión espacial. Esto significa tener las antenas separadas por al menos **1/2 (media) longitud de onda (wave length)**. Para los estándares: LAMBDA-802.11a es λ=55*mm*, LAMBDA-80211bg es λ=120*mm* (la separación debe ser la mitad de los lambda).

1.2.3.13 802.11n: Configuraciones MIMO

Los Radio Chains (compuestos por frecuencia, antena, mixer, amp, DAC/ADC, etc.) permiten generar varios **Spatial Streams** (flujos de datos espaciales). La cantidad de **Spatial Streams** que se pueden generar estarán limitados por los radio chains, que exteriormente se observan por la cantidad de antenas de recepción y transmisión. El cálculo se logra: *min*(*At*,*Ar*) limitación algebraica. En general se cumple que *N* caminos: *N*-plican la capacidad.
Algunas configuraciones permitidas:

- Máxima 4x4:4 (4 Tx antenas, 4 Rx antenas: 4 spatial streams). Sólo con ésta se pueden alcanzar los 600Mbps.
- Más utilizadas, soluciones empresariales: 2x3:2 (2 Tx antenas, 3 Rx antenas: 2 spatial streams). Se pueden alcanzar 300Mbps.

- Más económica, buena performance: 2x2:2 (2 Tx antenas, 2 Rx antenas: 2 spatial streams).
- 3x3:3 mayor performance que las 2 anteriores.

En el archivo complementario **wlan-phy/wlan-phy-mimo-3x3.jpg** se muestra una configuración con múltiples Radio Chains dando como resultado 3 **Spatial Streams**.
Complementariamente los Radio Chains fijos los datos pueden tomar múltiples caminos (**Multipath Signal**) debido a la reflexión, refracción y/o "scattering" producida por el entorno, por ejemplo reflexión en ambientes metálicos. Para 802.11a/b/g los múltiples caminos generan interferencia y los datos se pierden, en cambio 802.11n intenta tomar ventaja de esta característica y aprovechar para aumentar la tasa de transmisión. En la figura 1.25 se muestra un ejemplo de MIMO con multipath.

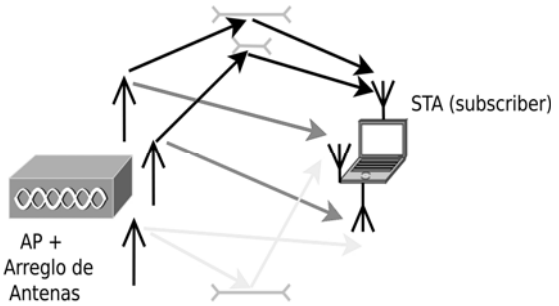


Figura 1.25 Ejemplo de la técnica MIMO con multipath

1.2.3.14 802.11n: Intervalos de Guarda Cortos

En 802.11n se puede acortar a la mitad, el GI (Guard Interval), ir del valor de 800ns a 400ns, llamado en este caso **SGI (Short Guard Interval)**. Esto se recomienda si existe buena calidad RF y sólo si todos los equipos trabajan en 802.11n, término que se indica con la palabra **Greenfield**. Los espacios deben ser más reducidos, preferentemente cerrados.

1.2.3.15 802.11n: Agrupamiento de Canales

802.11n para obtener mejor rendimiento permite agrupar 2 (dos) canales de 20MHz en uno de 40MHz, término en inglés referido como **Channel Bonding**. Para ser compatible con el estándar IEEE 802.11n un canal de 20MHz es obligatorio, la agrupación de canales es opcional. Uno de los canales es considerado de control, "master", o **primario**, y el otro secundario. Este último se puede ubicar por encima o por debajo del de control. En la figura 1.26 se muestra el

agrupamiento de los canales y se contrasta la máscara del espectro de 20MHz usada en 802.11a/g contra la de 802.11n.
Se estudió que 802.11a/g tiene 52 sub-carriers en una banda de 20MHz, de los cuales usa 48 para los datos y 4 para pilots de sincronización. Con el nuevo estándar se permiten utilizar más canales
en 20MHz, 56 sub-carriers totales, de los cuales se toman 52 para datos y 4 para pilots. Al producirse el agrupamiento sobre 40MHz ya no se requieren sub-bandas exteriores reservadas para protección/guardas entre los canales agrupados (en el medio). En la figura 1.26 se puede ver este hecho. De esta forma se permite tener una configuración de 114 sub-carriers, de los cuales se usan 108 para datos y 6 para pilots. En la misma ilustración se muestra la estructura y se remarca que un canal debe ser primario y otro secundario. Los mensajes de control y los broadcast deberán enviarse por el primario.

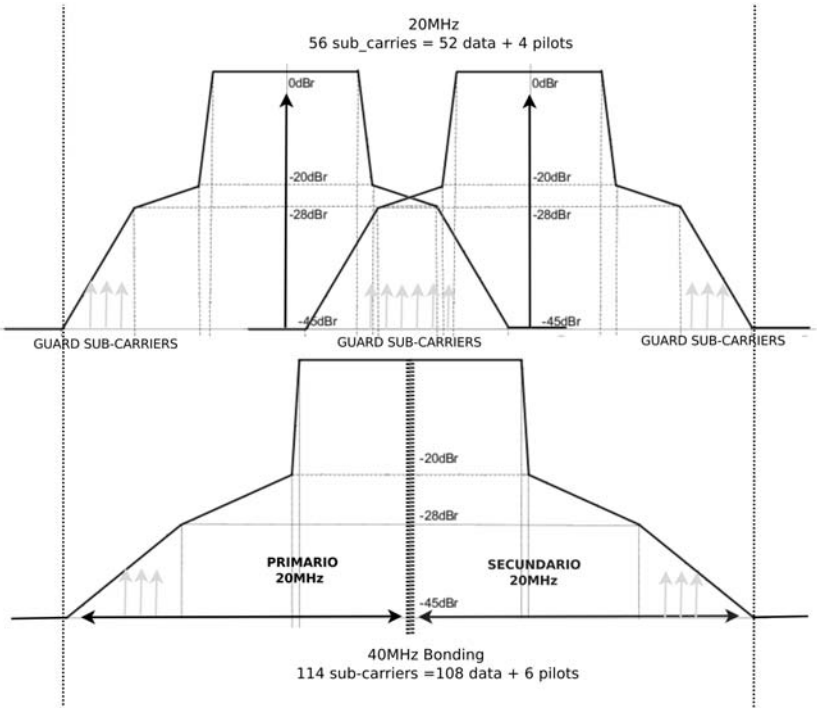


Figura 1.26 Channel Bonding y la máscara del espectro usado en 802.11n contra 802.11a/g

1.2.3.16 802.11n: Modulaciones y Codificaciones

802.11n define varias codificaciones y modulaciones, llamadas **Modulation and Coding Scheme (MCS)**. Los primeros 77, MCS

(0..76), son las tasas definidas por el estándar. Los valores 77..127 están reservados para uso futuro. Los primeros 8 son obligatorios y en los equipos en el mercado se implementan comúnmente los primeros 16 (MCS 0..15). Según el *802.11n draft 2.0* se puede alcanzar hasta 300Mbps. De la misma forma que sucede con los otros estándares con la modulación y la codificación el mejor MCS es seleccionado de acuerdo a las condiciones del medio. Para los clientes se indican en preámbulo PLCP HT-SIG. En las figura 1.27 se muestran algunas combinaciones de modulaciones y codificaciones asociadas a los índices.

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
21	3	64-QAM	2/3	156.00	173.30	324.00	360.00
22	3	64-QAM	3/4	175.50	195.00	364.50	405.00
23	3	64-QAM	5/6	195.00	216.70	405.00	450.00
24	4	BPSK	1/2	26.00	28.80	54.00	60.00
25	4	QPSK	1/2	52.00	57.60	108.00	120.00
26	4	QPSK	3/4	78.00	86.80	162.00	180.00
27	4	16-QAM	1/2	104.00	115.60	216.00	240.00
28	4	16-QAM	3/4	156.00	173.20	324.00	360.00
29	4	64-QAM	2/3	208.00	231.20	432.00	480.00
30	4	64-QAM	3/4	234.00	260.00	486.00	540.00
31	4	64-QAM	5/6	260.00	288.80	540.00	600.00

Figura 1.27 Algunos MCS (Esquemas de Modulaciones y Codificaciones) usados en 802.11n

1.2.4 Canales para Tecnologías WLAN

1.2.4.1 Canales para 802.11b/g/n

El espectro de Radio para 802.11b/g tiene un máximo 14 canales de 22MHz separados por 5MHz con superposición en la periferia de los

22MHz. Los canales que se pueden utilizar dependen de los entes reguladores de acuerdo a la región. En los siguientes puntos se hace un resumen del panorama en el mundo:

EE.UU. (FCC)/Canada (IC): canales 1 .. 11, rango de frec. 2,412-2,462 GHz.

Europa, sin España (ETSI): canales 1 .. 13, rango de frec, 2,412-2,472 GHz.

Japón (MIC): canales 1 .. 14, rango de frec. 2,412-2,462 GHz y 14 2,484 GHz.

España: canales 10 .. 11, rango de frec. 2,457-2,462 GHz.

Sólo se encuentran sin solapar los canales 1, 6 y 11 en redes WLAN de 2,4GHz. En algunas regiones se le pueda agregar un cuarto que es el 14. En la figura 1.28 (arriba) se muestran los canales en 2,4GHz (Fuente: Wikipedia: IEEE 802.11 http://en.wikipedia.org/wiki/IEEE_802.11, Autor: Gauthierm, la imagen tiene licencia Creative Commons Attribution-Share Alike 3.0 Unported). En la figura 1.28 (abajo) se muestran los canales que no se solapan (Fuente: Wikipedia: IEEE 802.11 http://en.wikipedia.org/wiki/IEEE_802.11, Autor: Liebeskind, la imagen tiene licencia GNU Free Documentation License).

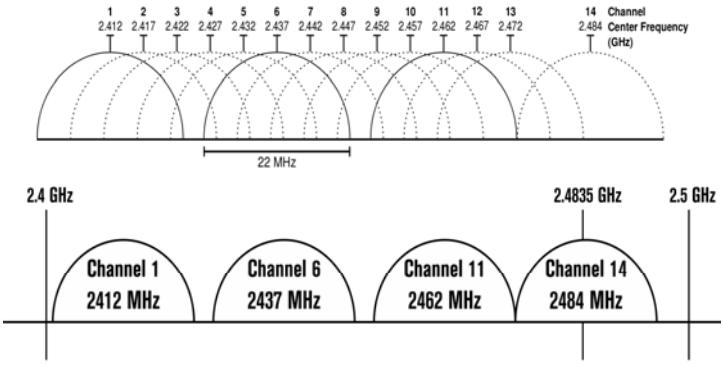


Figura 1.28 Canales físicos en 802.11b/g y aquellos que no se superponen

1.2.4.2 Canales para 802.11a/j/n

El espectro de Radio para 802.11a/j/n es mucho más amplio y posee mayor cantidad de sub-bandas. El estándar 802.11j es una enmienda al 802.11 para el mercado de Japón y permite usar desde los 4,9GHz. En la figura 1.29 se muestra esquemáticamente su distribución y límites de potencia internacionales, aunque cada región aplica regulaciones sobre los canales y los máximos valores admitidos. En la sección **Potencia Irradiada** se ofreció un panorama de esto. Las bandas son llamadas UNII, Unlicensed National Information Infrastructure, y se

dividen en 3 categorías de 100MHz cada una según la FCC. La cantidad de canales sin solaparse en UNII-1..UNII-3 son 12 (doce).

UNII-1 (indoor): 5,150GHz..5,250GHz. (lower-band).

UNII-2 (indoor/outdoor): 5,250GHz..5,350GHz. (middle-band).

UNII-3 (outdoor): 5,725GHz..5,825GHz. (upper band).

Existe una banda llamada **UNII-2 extended** que extiende el rango UNII-2. Éstas se permiten utilizar en indoor u outdoor. Japón admite bandas extras con los siguientes límites de potencia:

- (4,920 .. 4,980 GHz) y (5,040 .. 5,080 GHz): 250 mW EIRP.
- (5,150 .. 5,250 GHz): 200 mW EIRP.

Se requiere en la reglamentación algunas regiones para las frecuencias que se utilice capacidades de Dynamic Frequency Selection (DFS) y Transmit Power Control (TPC), estandarizadas por IEEE 802.11h, para evitar interferencia con sistemas de radares meteorológicos y de aplicaciones militares.

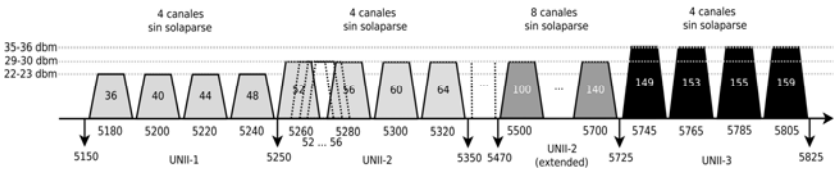


Figura 1.29: Canales físicos en 802.11a/j

1.2.4.3 PLCP para DSSS en 802.11

La capa PLCP agrega 6 campos de encabezado a la trama recibida desde la capa MAC. El contenido de estas tramas se llama **PLCP Service Data Unit (PSDU)**. La figura 1.30 muestra los campos de las tramas a nivel PLCP en DSSS.

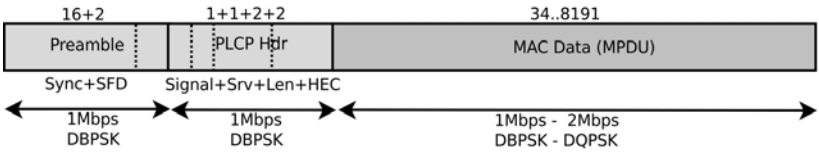


Figura 1.30: Trama PLCP en DSSS

Preámbulo (Preamble): sirve para sincronizar relojes de receptor y transmisor. Compuesto por el campo **Sync** y el **SFD (Start Frame Delimiter)** para indicar dónde comienza la trama PLCP en sí. Es transmitido a la velocidad más baja del estándar, 1Mbps. El SFD posee el valor binario: 0000010111001111. El

preámbulo original tiene una longitud total de 128 bits + 16 bits = 144 bits. El encabezado de sync original tiene 128 bits en 1 (uno). Luego se realiza el **"scrambling"**. El "scrambling" significa cambiar algunos bits, por ejemplo a través de funciones XOR con diferentes máscaras o CRCs.

Encabezado (Header): el encabezado PLCP continúa luego del preámbulo. Este contiene el campo **Señal (signal)** usado para identificar la tasa de transmisión con la que se envía la PSDU (trama MAC). En DSSS los valores admitidos son:

- 0x0A para 1Mbps.
- 0x14 para 2Mbps.

Luego, continúa el campo **Servicio (Service)**, que en DSSS no es usado y está configurado a 0 (cero). El campo **Longitud (length)** indica la duración en microsegundos. El campo **CRC** se calcula con CRC-16 sobre el encabezado solamente. El encabezado es, de la misma forma que el preámbulo, transmitido a la velocidad más baja, 1Mbps.

Algunos parámetros físicos de DSSS se puntualizan a continuación. Sus significados se estudiarán en la sección de la capa MAC:

- **Max MAC frame length:** 8191 bytes.
- **Slot time:** 20 μs.
- **SIFS time:** 10 μs (a partir de éste se derivan los demás valores).
- **CW:** 31..1023 slots.
- **Minimum sensitivity:** -80 dBm.

1.2.4.4 PLCP para HR-DSSS en 802.11b

Para HR-DSSS se consideran velocidades de transmisión mayores, se conservan 1Mbps y 2Mbps y se adicionan 5,5Mbps y 11Mbps. La longitud del "overhead" para la versión original de DSSS reduce notablemente el rendimiento. Para poder trabajar con 5,5Mbps y 11Mbps se utiliza una trama nueva llamada corta, **"short frame"**, en contraposición a la del original: trama larga, **"long frame"**. En 802.11b esta trama de nivel PLCP se propone como opcional y sólo debe ser utilizado si todas las estaciones de la red lo soportan. Sino se debe volver al formato original para mantener la compatibilidad. Al día de la fecha casi no se encuentran clientes que no soporten el "short frame". Para trabajar con el nuevo formato los AP deben enviar mensajes de "Probe" y esperar que los clientes respondan en un escaneo activo. En la figura 1.31 se muestra la estructura de la trama PLCP. El nuevo formato contempla los siguientes campos.

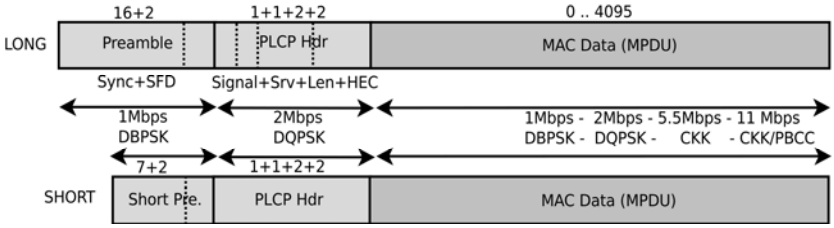


Figura 1.31 Trama PLCP en HRDSSS

Preámbulo Corto (short preamble): tiene el campo **Short Sync** y **Short SFD (Short Start Frame Delimiter)**. Es transmitido a la velocidad más baja del estándar, 1Mbps. El **Short Sync** tiene un tamaño de 56 bits y el Short SFD cambia al valor: 1111001110100000. El preámbulo corto tiene una longitud total de 56 bits + 16 bits = 72 bits. El encabezado de sync es generado con 56 bits en 0 (cero), de forma inversa que el original.

Encabezado (Header): el PLCP nuevo posee los mismos campos que el original. El campo **Señal (signal)** es usado para identificar la tasa de transmisión con la que se envía la trama MAC. Los valores para el campo signal son:

- 0x0A para 1Mbps.
- 0x14 para 2Mbps.
- 0x37 para 5,5 Mbps.
- 0x6E para 11 Mbps.

El campo **Servicio (service)** se utiliza para indicar el tipo de reloj (timing) que tiene el emisor, y la modulación: CKK o PBCC. El campo **Longitud (length)** indica la duración en microsegundos (μs). El campo **CRC** se calcula con CRC-16 sobre el encabezado solamente. En el caso de usar el Preámbulo Corto se trasmite a 2Mbps, en lugar de 1Mbps.

Algunos parámetros físicos de HR-DSSS se puntualizan a continuación. Sus significados se estudiarán más adelante en la sección de la capa MAC:

- **Max MAC frame length:** 4095 bytes.
- **Slot time:** 20 μs.
- **SIFS time:** 10 μs (a partir de éste se derivan los demás valores).
- **CW:** 31..1023 slots.
- **Minimum sensitivity:** -76 dBm.

1.2.4.5 PLCP para OFDM en 802.11a/j

Para OFDM, si bien se tiene un preámbulo y un encabezado, se agregan algunos campos y se codifica de forma diferente. En la figura 1.32 se muestra la estructura de la trama PLCP en OFDM para 802.11a.

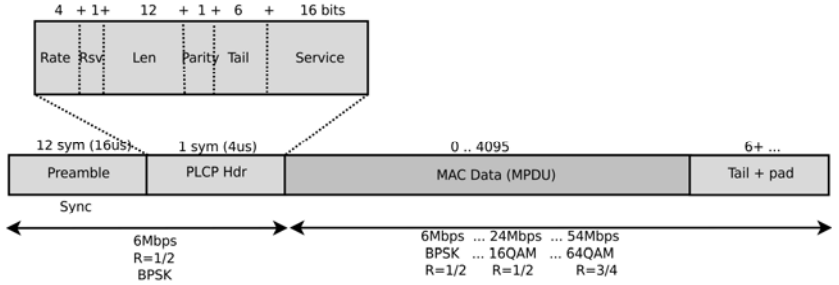


Figura 1.32 Trama PLCP en OFDM

Preámbulo (preamble): el preámbulo dura 16μs y se divide en una primera parte destinada a sincronizar permitiendo al receptor seleccionaruna antena (si éste utiliza varias). La primera parte se llama **short training sequence** y está compuesta por 10 símbolos. La segunda parte es transmitida con una guarda previa dividida en dos **long training sequences**. Es importante destacar que en OFDM se utilizan guardas en la mayoría de los campos. Las guardas son espacios de 0.8μs, los cuales pueden combinarse.

Encabezado (Header): el PLCP de OFDM lleva el campo **Señal (signal)** usado para identificar las parámetros que determinan la tasa de transmisión con la que se envía las trama MAC. Este tiene una estructura más compleja que las anteriores con DSSS. Dentro de este campo está codificada la tasa de transferencia, la longitud y un bit de paridad. Los valores posibles para las "velocidades" codificadas en 4 bits son: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. El encabezado también posee un campo **Servicio (service)**, otro **Cola (tail)** y **Relleno (pad)**.

La sensibilidad en el receptor determinará la velocidad a utilizar. Para trabajar a 18 o 24Mbps, se requiere aprox. -75dBm. Para hacerlo en 36Mbps, -70dBm, y para 54Mbps son necesarios -65dBm. Algunos parámetros físicos en OFDM se puntualizan a continuación. Sus significados se estudiarán más adelante en la sección de la capa MAC:

- **Max MAC frame length:** 4095 bytes.
- **Slot time:** 9 μs.
- **SIFS time:** 16 μs (a partir de éste se derivan los demás valores).

- **CW:** 15..1023 slots.
- **Minimum sensitivity:** -65..-82 dBm.

1.2.4.6 PLCP para HR-DSSS/OFDM en 802.11g

Para que 802.11g pueda ser compatible con 802.11b y no degradar el rendimiento notablemente, el estándar implementa un mecanismo llamado de **protección a Extended Rate PHY (ERP)**. El mecanismo funciona de la siguiente forma:

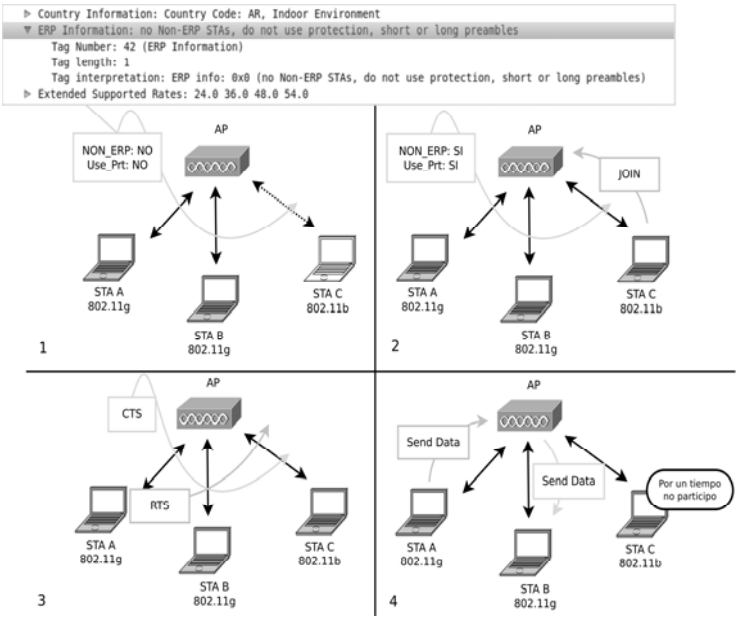


Figura 1.33 Mecanismo de protección en 802.11g

1. El AP con capacidad 802.11g asume que no hay clientes 802.11g y envía los mensajes **Beacon** pertenecientes a la capa MAC indicando que no existen equipos 802.11b en la red, NON_ERP_Protection=0, y, por lo tanto, no se requiere de protección, USE_Protection=0 (NO). Los Beacon son codificados como si se trabajase en 802.11b.
2. Los clientes 802.11g podrán aprovechar las características extras de este protocolo al comunicarse entre sí pasando por el AP, sin usar el mecanismo de protección.
3. Si un cliente se asocia al AP respondiendo al Beacon, sin mirar la información extra, de esta forma se asume que trabaja sólo en 802.11b; el AP debe comenzar a propagar los nuevos Beacon con los valores: NON_ERP_Protection=1 (SI) y USE_Protection=1 (SI).

4. Ahora los clientes 802.11g antes de enviar información solicitarán el acceso al medio a partir de mensajes **RTS (Request to Send)** en 802.11b esperando que los equipos antiguos los vean y cedan el tiempo indicado para enviar. El concentrador (el AP) deberían enviar un **CTS (Clear to Send)** para permitir el acceso a las estaciones 802.11g. Los clientes 802.11g podrían usar **CTS-to-Self**, pero no evitarían el problema del nodo oculto. El mecanismo de **RTS/CTS** y el problema del **Nodo Oculto** se explican en la capa MAC, en la sección **DCF: CSMA/CA**.
5. Durante la transmisión en nivel físico 802.11g los clientes 802.11b se abstienen de acceder, pues la capa física ahora es incomprensible para estos.
6. Los AP que sean vecinos, pero no tengan clientes asociados 802.11b deben enviar en los mensajes Beacon: NON_ERP_Protection=1 (NO) y USE_Protection = 1 (SI). Los AP vecinos de esta forma evitan generar ruido en la misma zona de cobertura sobre el mismo canal forzando a usar el mecanismo de protección.

Si se configura un AP para sólo utilizar 802.11g no activará este mecanismo de protección. En la figura 1.33 se muestra gráficamente un ejemplo. La protección no es requerida para las capas físicas ERP-PBCC ni DSSS-OFDM PHY, ya que trabajan con encabezados 802.11b compatibles.

El formato de la trama de PLCP en 802.11g con PHY de ERP-OFDM es muy similar al usado en 802.11a. La diferencia principal según [GAS05] es que la trama es seguida por un tiempo de 6µs considerado como extensión del campo **Señal (Signal Extension)**.

En cambio, cuando no se usa OFDM puro (single carrier), por ejemplo con ERP-PBCC o DSSS-OFDM PHY, el formato de la trama en PLCP es idéntico al utilizado en DSSS puro (802.11b). En el caso DSSS-OFDM se utiliza la modulación OFDM sobre el cuerpo de la trama (payload). DSSS-OFDM, a diferencia de OFDM, a nivel de PLCP hace algunas modificaciones extras.

En resumen, de acuerdo a los niveles de "calidad" de la señal y la velocidad configurada para trabajar serán las codificaciones y modulaciones utilizadas.

- Para 54Mbps: OFDM + 64QAM (Quadrature Amplitude Modulation) con -73dBm de sensibilidad en la señal recibida (Rx Sensity).
- Para 36Mbps: OFDM + 16QAM con -80dBm de sensibilidad en la señal recibida.

- Para 22Mbps: versiones de 802.11b+/802.11g utilizaban como codificación PBCC (Convolutional Coding).
- Para 18Mbps: versiones de 802.11b+/802.11g utilizaban PBCC + QPSK (Quadrature Phase Shift Keying). Mayormente se implementa OFDM + QPSK con -87dBm de sensibilidad en el receptor.
- Para 11Mbps: CCK (Complementary code keying), DQPSK con -88dBm.
- Para 5,5Mbps: CCK, DBPSK con -91dBm.
- Para 1-2Mbs: Barker 11, DBPSK con -94dBm.

1.2.4.7 PLCP para OFDM en 802.11n

Para compatibilidad con protocolos anteriores, 802.11b y 802.11g, en 802.11n se requieren mecanismos de protección. Esta protección se agrega en diferentes niveles. A nivel PHY, en la sub-capa PLCP, se encuentra el primer agregado. Este mecanismo es el más eficiente porque no agrega sobrecarga a nivel MAC y trabaja modificando el preámbulo. 802.11n define varios modos en PLCP de preámbulos:

- Modo Legado.
- Modo Mixto.
- Modo Greenfield.

Los dos últimos, Mixto y Greenfield, son considerados modos **HT (High Throughput)**.

802.11n PLCP: Formato Modo Legado

Modo Legado, **NON HT**, trabaja en modo SISO (Single-Input Single Output) y en la mayoría de las configuraciones no usa channel bonding, trabaja únicamente en una banda de 20MHz. El formato físico del preámbulo es igual al de protocolos anteriores 802.11a/g y es obligatorio. Sobre los 64 sub-carriers posibles se usan los mismos 52 que para 802.11a/g: -26..-1,1..26, considerando los 4 pilots. Los campos **Legacy Short Training Frame (L-STF)**, **Legacy Long Training Frame (L-LTF)** se usan para sincronizar y son transmitidos a baja velocidad, igual que en 802.11a/g. En el campo **L-SIG (Legacy Signal)** se indica la tasa de transmisión y la longitud. En la figura 1.34 se muestra una trama PLCP en este modo.

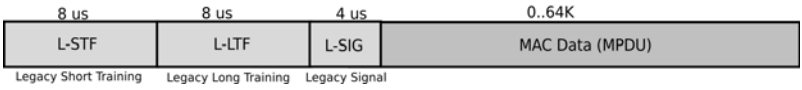


Figura 1.34 Trama PLCP 802.11n modo legado

802.11n PLCP: Formato Modo HT-Mixto

En el modo HT-Mixto PHY las tramas 802.11n son transmitidas precedidas por preámbulos 802.11a/g, el cual es obligatorio. El formato es conocido como **L-SIG TXOP** y se debe usar este modo si se detectan equipos legados (protocolos anteriores) en el rango de alcance. El "overhead" según pruebas de este modo es menor al 0,1%. Se utilizan más sub-carriers que en el modo Legado, 56: 28..-1,1..28. Puede usar dos canales en bonding, en este caso los broadcasts y el control solo se envían por uno. Sobre los 40MHz del bonding los sub-carriers utilizados son: -58..-2,2..58 y se modifican algunos para hacerlo compatible con los dos canales de 20MHz de otros sistemas vecinos. Con el preámbulo L-SIG, los sistemas legados pueden detectar cuánto dura la transmisión. Este campo tiene un significado diferente que en el modo Legado. Se agregan Preámbulos propios de HT, HT-SIGs con información propia de 802.11n: MCS, bonding, frame aggregation (frame-bursting), short GI, etc. En la figura 1.35 se muestra una trama PLCP en este modo.

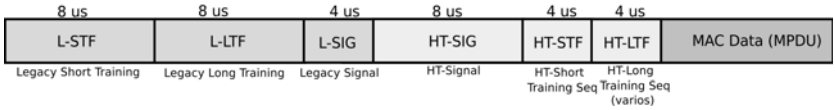


Figura 1.35 Trama PLCP 802.11n modo mixto

802.11n PLCP: Formato Modo HT-Greenfield

En el modo **Greenfield** o "Espacio sin Restricciones" no se utiliza protección, pero es solo compatible con equipos 802.11n. Este nombre es dado a redes "N" puras y es el de mejor rendimiento. Se utiliza un preámbulo especial para este modo. Se recomienda si existe buena calidad de RF y, por supuesto, todas las estaciones son 802.11n. Aprovecha al máximo los espacios cortos: RIFS. En la figura 1.36 se muestra una trama PLCP en este modo.

802.11n modifica la capa PLCP generando intervalos DIFS más cortos llamados **RIFS (Reduced Interframe Spacing)**. En IEEE 802.11b/g según lo visto, el intervalo es de 10µs, en IEEE 802.11a de 16µs. Para IEEE 802.11n es mucho más corto, solo de 2µs. Compatible únicamente en una red tipo Greenfield.

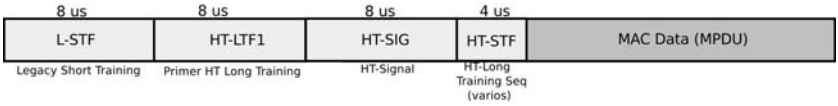


Figura 1.36 Trama PLCP 802.11n modo Greenfield

1.2.5 PoE

En la gran parte de las situaciones los dispositivos wireless no están ubicados en lugares donde se les pueda suministrar energía eléctrica de forma fácil. Debido a esto, las tecnologías que permiten "alimentarlos" utilizando los cables de comunicaciones son habitualmente indispensables en redes inalámbricas. El estándar IEEE STD-802.3af-2003 compatible con Ethernet/802.3 en 10/100/1000 Base-T lo permite. La tecnología es conocida globalmente como **PoE (Power over Ethernet)**. La potencia máxima de salida suministrada por un dispositivo funcionando bajo el estándar IEEE es de 15,4W por puerto. En el estándar se definen tres términos para identificar a los equipos:

End-Point PSE (Power Source Equipment): es el dispositivo que entrega energía, como puede ser un switch con PoE y se comunica directamente con el dispositivo alimentado.

Mid-span PSE: dispositivo que entrega energía, y se encuentra conectado al medio entre el dispositivo de comunicaciones y el dispositivo alimentado.

PD (Powered Device): dispositivo alimentado, como puede ser un AP, un teléfono VoIP, etc.

El estándar indica que se puede alimentar utilizando dos grupos de pares de cables:

- Pares de Datos (1, 2; 3, 6) referido como **Phantom Power**.
- Pares libres (spare) (4, 5; 7, 8).

Los **Mid-span PSE** solo pueden usar los pares libres y no deben utilizarse para llevar energía en 1000BaseT que utiliza los 4 (cuatro) pares. Solo los **End-Point PSE (Power Source Equipment)** pueden usar los pares de datos y se permite llevar energía en 1000BaseT. Los PSE ofreciendo PoE deben detectar de forma física si tienen conectado un dispositivo que lo soporta. La técnica definida por el estándar utiliza corriente continua, DC, aplicando un voltaje determinado entre el par de recepción y el de transmisión, luego mide la diferencia de potencial (voltaje) y la intensidad de corriente (amperes). Si el PD soporta el PoE estándar deberá cerrar el circuito para permitir que la electricidad fluya y suministrar una resistencia de 25K ohms. Si no se detecta, se quita la tensión. Si se detecta se prosigue con la etapa de detección del nivel de tensión requerido por el PD. Algunos pre-estándares, como el de Cisco, trabajaba con AC (corriente alterna) usando los FLP (Fast Link Pulse) de Ethernet para detectar si el PD soporta efectivamente el PoE. El estándar a través del circuito eléctrico permite que el PD indique el consumo requerido. Las clases de consumo definen los siguientes valores:

- Clase 0: Default 15,4W.

- Clase 1: Opcional 4,0W.
- Clase 2: Opcional 2,0W.
- Clase 3: Opcional 15,4W.
- Clase 4: Reservada.

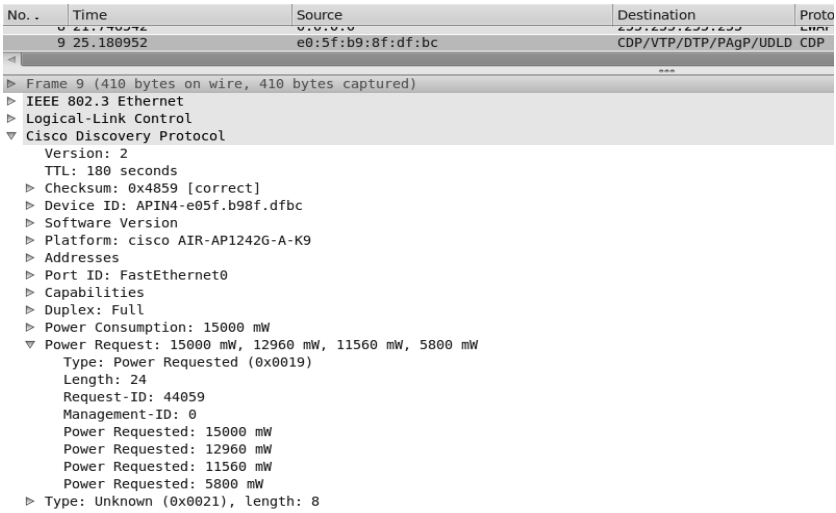


Figura 1.37 Captura de trama CDP con información de PoE

La clasificación generada por 802.3af para optimizar el consumo es opcional. Para los valores intermedios entre las clases existen propuestas de usar protocolos como CDP (Cisco Discovery Protocol) o LLDP (Link Layer Discovery Protocol) entre el PD y el End-Point PSE permitiendo negociar la cantidad de energía adecuada. Muchos PD, para no generar una sobrecarga de consumo sobre el PSE, consumen lo mínimo hasta estar seguros de la energía que requieren y que el PSE puede entregar. Los PD requieren negociar este parámetro.
A menudo 15,4W no es suficiente, más hoy en día con equipos 802.11n que requieren más energía. La actualización IEEE 802.3at-2009 [802.3at] conocida como **PoE+** permite proveer hasta 25,5W. Otras variantes no estándares permiten llevar más energía usando los 4 pares o incluso cables extras. En la figura 1.37 se muestra una captura de un mensaje CDP donde indica los niveles de consumo de acuerdo a las clases.

1.2.6 Ejemplos de Configuración de Parámetros Físicos

A continuación, a modo ilustrativo, se muestra la forma de configurar algunos parámetros estudiados en la sección. Los ejemplos son realizados sobre dos equipos diferentes, el primero un Mikrotik

corriendo RouterOS con una WNIC 802.11a y el segundo un AP Cisco 1242G. Primero se muestra la configuración de los niveles de potencia y el NF. Es importante tener en cuenta que, si la potencia se configura manualmente se deben seguir las regulaciones locales.

```
[admin@MikroTik] >
/interface wireless set wlan1 tx-power-mode=
 TxPowerMode ::= all-rates-fixed | card-rates | default | manual-
table
  card-\rates -- Use card default rates
  all-rates-fixed -- Use one transmit power value for all rates
  manual-table -- Use the transmit powers as defined in
     '/interface wireless manual-tx-power-table'
  default -- Use transmit power as defined by tx-power setting

/interface wireless set wlan1 tx-power=
 TxPower ::= [-]Num
  Num ::= -30..30    (integer number)

/interface wireless set wlan1 noise-floor-threshold=
 NoiseFloorThreshold ::= Default | Threshold
  Threshold ::= [-]Num
    Num ::= -128..127    (integer number)
  Default ::= default
```

Sobre el equipo Cisco.

```
aptest(config-if)#power ?
  client  Client radio transmitter power level
  local   Local radio transmitter power level

aptest(config-if)#power client ?
  <1 - 100>  One of: 1 5 10 20 30 50 100
  local      Set client power to Access Point local power
  maximum    Set client power to allowed maximum

aptest(config-if)#power local ?
  cck   Set local power for CCK rates
  ofdm  Set local power for OFDM rates

aptest(config-if)#power local ofdm ?
  <1 - 30>  One of: 1 5 10 20 30
  maximum   Set local power to allowed maximum
```

La selección de la frecuencia y la banda es otro parámetro configurable. En el caso de los equipos Mikrotik se admiten, de acuerdo a la WNIC, trabajar en diferentes bandas (multi-banda), incluso a costo de bajar la velocidad. También, se puede reducir el ancho de la misma de 20-22MHz a 5-10MHz con el objetivo de tener menor interferencia y una cobertura más sectorial. Para el caso de los turbo-channels lo que se obtiene es lo contrario, se ensancha de 20-22MHz a 40MHz.

```
/interface wireless info print
 0 interface-type=Atheros AR5213
   chip-info="mac:0x5/0x9, phy:0x43, a5:0x36, a2:0x0, eeprom:0x4008"
   pci-info="00:04.0" capabilities=tx-power-control,ack-timeout-control,
                                   virtual-ap,alignment-mode,noise-floor-
                                   control,scanning,burst-support,nstreme,
                                   sniffing,compression,power-channel,wmm
   default-periodic-calibration=enabled
   supported-bands=5ghz,5ghz-turbo,5ghz-10mhz,5ghz-5mhz
   5ghz-channels=5180:0,5185:0,5190:0,5195:0,5200:0,5205:0,5210:0,5215:0,
                 5220:0,5225:0,5230:0,5235:0,5240:0,5260:0,5265:0,5270:0,
                 5275:0,5280:0,5285:0,5290:0,5295:0,5300:0,5305:0,5310:0,
                 5315:0,5320:0,5745:0,5750:0,5755:0,5760:0,5765:0,5770:0,
                 5775:0,5780:0,5785:0,5790:0,5795:0,5800:0,5805:0,5810:0,
                 5815:0,5820:0,5825:0
   5ghz-turbo-channels=5210:0,5250:0,5255:0,5260:0,5265:0,5270:0,5275:0,5280:0,
                       5285:0,5290:0,5760:0,5765:0,5770:0,5775:0,5780:0,5785:0,
                       5790:0,5795:0,5800:0
   5ghz-10mhz-power-channels=5175:0,5180:0,5185:0,5190:0,5195:0,5200:0,5205:0,
                             5210:0,5215:0,5220:0,5225:0,5230:0,5235:0,5240:0,
                             5245:0,5255:0,5260:0,5265:0,5270:0,5275:0,5280:0,
                             5285:0,5290:0,5295:0,5300:0,5305:0,5310:0,5315:0,
                             5320:0,5325:0,5740:0,5745:0,5750:0,5755:0,5760:0,
                             5765:0,5770:0,5775:0,5780:0,5785:0,5790:0,5795:0,

/interface wireless set wlan1 band=
 Band ::= 2.4ghz-b | 2.4ghz-b/g | 2.4ghz-g-turbo | 2.4ghz-onlyg | 2ghz-10mhz |
...
  5ghz -- IEEE 802.11a up to 54 Mbit
  5ghz-turbo -- IEEE 802.11a with Atheros turbo extension up to 108Mbit

/interface wireless set wlan1 frequency=
 Frequency value in MHz.
 Allowed values depend on selected band, and are restricted by <country>
 setting and wireless card capabilities.
 This setting has no effect if interface is in any of station modes,
 or in 'wds-slave' mode, or if DFS is active.

 Frequency ::= 0..4294967295    (integer number)
```

Para el caso del equipo Cisco, no se obtiene tanta flexibilidad y sólo se puede seleccionar el canal indicado por la frecuencia. Al trabajar como AP se le puede configurar que seleccione el canal menos congestionado, haciendo un previo escaneo. Esto se realiza al arrancar el equipo.

```
aptest(config-if)#channel ?
  <1-2462>         One of: 1 2 3 4 5 6 7 8 9 10 11 2412 2417 2422
                   2427 2432 2437 2442 2447 2452 2457
                   2462
  least-congested  Scan for best frequency
```

Otro parámetro físico seleccionable es la tasa de transferencia soportada. Se pueden escoger múltiples, y, de acuerdo a la sensibilidad detectada y a los clientes, serán las velocidades utilizadas.

```
/interface wireless set wlan1 supported-rates-a/g=
 SupportedRatesAG                                                    ::=
6Mbps|9Mbps|12Mbps|18Mbps|24Mbps|36Mbps|48Mbps|54Mbps
                      [,SupportedRatesAG*]

/interface wireless set wlan1 supported-rates-b=
 SupportedRatesB ::= 1Mbps|2Mbps|5.5Mbps|11Mbps[,SupportedRatesB*]

ap(config-if)#speed ?
  1.0          Allow 1 Mb/s rate
  11.0         Allow 11 Mb/s rate
  12.0         Allow 12 Mb/s rate
  18.0         Allow 18 Mb/s rate
  2.0          Allow 2 Mb/s rate
  24.0         Allow 24 Mb/s rate
  36.0         Allow 36 Mb/s rate
  48.0         Allow 48 Mb/s rate
  5.5          Allow 5.5 Mb/s rate
  54.0         Allow 54 Mb/s rate
  6.0          Allow 6 Mb/s rate
  9.0          Allow 9 Mb/s rate
  basic-1.0    Require 1 Mb/s rate
  basic-11.0   Require 11 Mb/s rate
  ...
  basic-9.0    Require 9 Mb/s rate
  default      Set default rates
  ofdm         How to place OFDM rates in rates elements
  range        Set rates for best range
  throughput   Set rates for best throughput (includes non-OFDM rates
               and may cause ERP protection to be used)
```

A nivel de PLCP se pueden configurar los preámbulos en ambos equipos.

```
/interface wireless set wlan1 preamble-mode=
 PreambleMode ::= both | long | short
  long -- Has a long synchronization field in a wireless packet (128
bits)
  short -- Has a short synchronization field in a wireless packet (56
bits)
  both -- Supports both - short and long preamble

aptest(config-if)#preamble-short ?
  <cr>
```

Para 802.11n a nivel físico se tienen nuevos parámetros configurables. Para el caso de channel bonding se le indica la ubicación del secundario con respecto al primario.

```
/interface wireless set wlan1...
   ht-extension-channel= above-control | below-control | disabled
```

Para los múltiples Radio Chains de acuerdo a las antenas que tiene el sistema se le configura cual utilizar para transmisión y cual para recepción. En este caso, el equipo tiene una WNIC MikroTik Routerboard R52n que tiene 2 (dos) conectores, main(0) y aux(1).

```
/interface wireless set wlan1...
   ht-rxchains = 0,1,2 -- any combination of these e.g. 0,1  0
   ht-txchains = 0,1,2 -- any combination of these e.g.  0,1  1
```

Intervalo de guarda (GI), los valores son: any=400ns, old=800ns.

```
/interface wireless set wlan1...
   ht-guard-interval= any | long
```

El MCS en 802.11n.

```
/interface wireless set wlan1...
   ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3,mcs-4,mcs-5,mcs-6,
                    mcs-7,mcs-8,mcs-9,mcs-10,mcs-11,
                    mcs-12,mcs-13,mcs-14,mcs-15
```

1.3 IEEE 802.11: Capa MAC

1.3.1 Tipos de Redes Wireless

Una red LAN wireless es definida por una serie de parámetros, como el canal (frecuencia), la codificación, la modulación, el nombre, el área de cobertura (celda física), las estaciones participantes y otros. El nombre que recibe en el estándar es **Basic Service Set (BSS)**. En el documento original del estándar 802.11 se definen dos modos de redes o conjuntos de servicios (BSS) posibles:

- Red en modo Ad-hoc o Independent BSS, referido como IBSS.
- Red en modo Infraestructura o Infrastructure BSS, referido directamente como BSS.
  Luego se agrega un tercero:
- Red en modo Infraestructura Extendido, referido directamente como ESS (Extended Service Set).

1.3.1.1 Modo Ad-hoc

El modo **ad-hoc,** o independiente, es el más sencillo. Se utiliza comúnmente cuando dos o más estaciones desean comunicarse

directamente sin requerir del soporte de un concentrador, AP. La red se conforma temporalmente, dura lo que requiere la comunicación y luego se puede deshacer. Se requiere que todas las estaciones participantes acuerden, previamente, los parámetros para conformar el BSS. Un ejemplo usual de una red funcionando en el modo independiente es cuando se utiliza la tecnología wireless para establecer un vínculo punto a punto. En este caso ninguno de los dispositivos requerirá tener el rol de AP. Comúnmente, para este tipo de configuración, se utilizan dos APs configurados para que trabajen en modo ad-hoc enlazándose entre sí. Ambos funcionarán como bridges wireless conectando una red cableada con la otra mediante un vínculo inalámbrico. En la figura 1.38 se muestran ejemplos de estas redes.

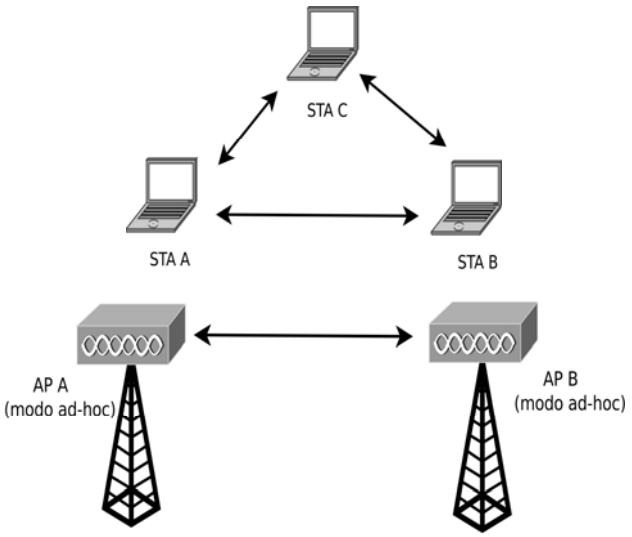


Figura 1.38 Ilustración de modos de IBSS

1.3.1.2 Modo Infraestructura

El modo **infraestructura** requiere de un dispositivo central que concentre las comunicaciones de todas las estaciones que pertenezcan al mismo BSS. En este modo cualquier dato entre dos o más estaciones requiere pasar obligatoriamente por el concentrador, AP. Previo a poder participar, las estaciones del BSS deben cumplir con un procedimiento de autenticación y asociación controlado por el AP. El concentrador wireless en la mayoría de los casos tiene una conexión a una red Ethernet y permite acceder a los clientes inalámbricos a los recursos de la otra red. En el caso que esta red de infraestructura

cableada permita vincular diferentes BSS se la llama **Sistema de Distribución** en inglés **Distribution System (DS)**. En las figura 1.39 se muestra un ejemplo de este tipo de red.

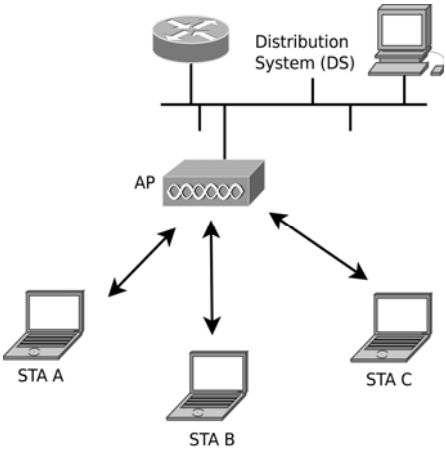


Figura 1.39 Ilustración de modo BSS

1.3.1.3 Modo de Infraestructura Extendido

Extra a los dos modos de BSS, ad-hoc e infraestructura, una red LAN wireless puede extenderse dando nuevas variantes a los tipos de redes. A partir del DS y varios BSS interconectados permite crear un BSS con una mayor cobertura y complejidad. El estándar IEEE 802.11 refiere a esta combinación como **Extended Service Set (ESS)**, compuesto por la unión de BSS a través de la infraestructura del DS. Según el estándar, el DS que se usa como backbone no es parte del ESS. Los diferentes BSS que componen el ESS pueden estar físicamente en el mismo espacio solapándose o a distancias en las cuales las celdas cubiertas no tienen ningún punto en común. Las estaciones se unen sólo a un AP y pueden ir cambiando de uno a otro a medida que se mueven de acuerdo al nivel de señal que detectan. Los AP se pueden comunican entre sí. El proceso de cambiar de un AP a otro por parte de las estaciones (clientes) es llamado en inglés **roaming**, traducido como movilidad. El roaming funciona siempre que exista un solapamiento de las celdas cubiertas por los AP comunicados por el mismo DS. Los clientes seleccionarán el AP que detecten con mejor nivel de señal y al percibir que éste cambia y encuentran uno mejor podrán unirse a otro AP con mayor nivel de recepción. El DS en el estándar está orientado a una red cableada, aunque podría también implementarse de forma inalámbrica, no estando esto bien definido en el mismo. Las formas de implementar el DS son:

- De forma cableada: DS (Distribution System Standard).
- De forma inalámbrica: WDS (Wireless Distribution System).

Un **Wireless Distribution System (WDS)** permite interconectar APs mediante una red inalámbrica. Los AP pueden funcionar al mismo tiempo como Access Point para las estaciones y en modo ad-hoc o cliente/AP para los demás APs. Lo recomendable para cuando se configura este modo es que los APs puedan trabajar en canales o mejor, en tecnologías diferentes para la función de AP y para la función de inter enlace. Cuando se busca cubrir una gran área con varios APs, existiendo regiones donde los patrones de radiación se solapan para permitir el roaming, lo recomendable es configurar de forma que las celdas adyacentes no utilicen la misma frecuencia. En IEEE 802.11b/g sólo existen tres canales que no se solapan: 1, 6 y 11.
Para poder inter-enlazar APs con bandas diferentes a las usadas por los clientes o con diferente tecnología (e.g. 802.11a para conexión de AP-AP y 802.11g para los clientes) es necesario tener al menos dos radios (WNICs+antenas). Es posible enlazar los APs usando el mismo BSS que se usa para proveer el servicio, aunque no es recomendable por cuestiones de rendimiento. En este último caso con solo un radio es suficiente. Habitualmente, el modo WDS en el cual se configuran los dispositivos utiliza el mismo BSS, es decir, todos tienen configurado el mismo canal y en este caso se considera que trabaja como repetidor. En la figura 1.40 se muestra un ejemplo de un ESS.

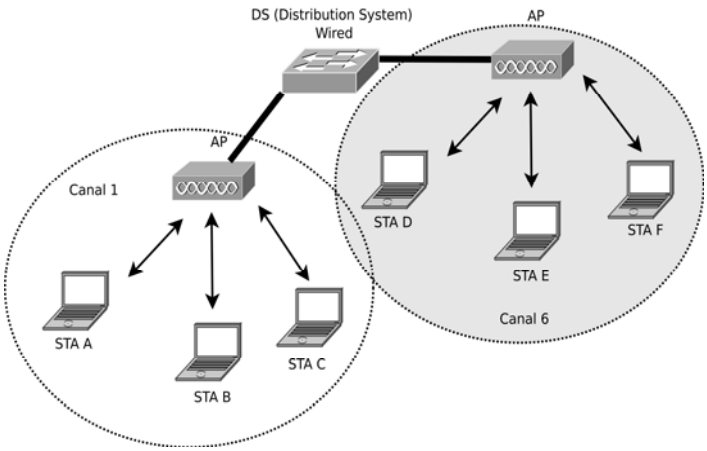


Figura 1.40 Ilustración de modo ESS

1.3.1.4 Conectividad AP-AP: Modos Bridge y Repetidor

Los diferentes fabricantes han realizado extensiones a las topologías definidas por el estándar. A través de una conexión inalámbrica dos o más AP pueden vincularse entre sí. Este vínculo puede ser dedicado, solo para comunicar los dispositivos, de forma inalámbrica y luego poder pasar tráfico entre las redes cableadas a las cuales están conectados. Este caso sería una conexión en modo ad-hoc, ya que no permitirían la conexión de otras estaciones (no funcionarían como AP) y además estarían funcionando como **Bridge**, ya que conmutarían el tráfico de la red cableada a la red inalámbrica y viceversa. Ambos AP funcionando en este modo deberían trabajar en el mismo canal. Los dispositivos funcionando en modo bridge pueden soportar trabajar en modo punto a punto (point-to-point) y punto-multipunto (point-to-multipoint). En la figura 1.41 se muestra un ejemplo de este modo de funcionamiento.

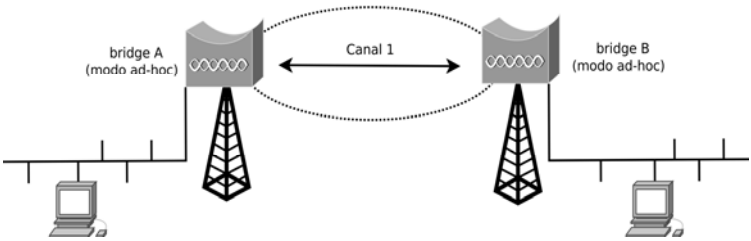


Figura 1.41 Ilustración de modo bridge

Una configuración similar se puede encontrar cuando existe un AP que no tiene una conexión a la red cableada y funciona para dar servicio a otros clientes. La forma de conectarlo al DS, teniendo un solo radio, es vincularlo con otro AP que le brinda conexión utilizando el mismo canal afectado para el servicio. El AP no conectado directamente a la red cableada funciona como tal y, además, se vincula con el otro AP. Este modo de funcionamiento se lo conoce como **Repetidor (Repeater)** y no está contemplado de esta forma en el estándar IEEE. En este escenario, el AP cumple rol de AP y cliente a la vez. Otro nombre utilizado para este rol es **Range Extender**, ya que permite extender la cobertura física de la celda del BSS. Es posible encadenar varios AP en este modo, pero, por una cuestión de rendimiento, se recomienda no más de dos. En la figura 1.42 se muestra un ejemplo gráfico de esta configuración.

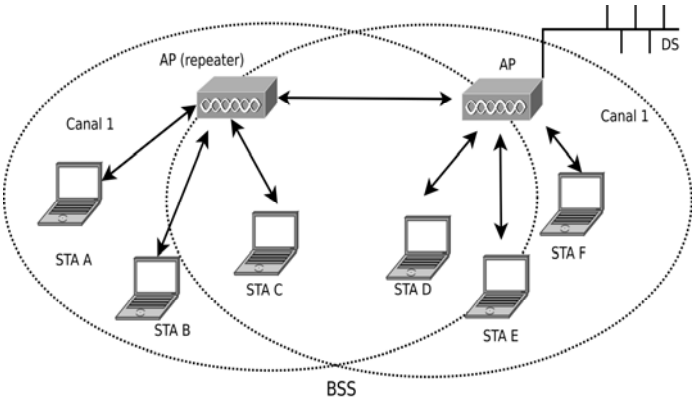


Figura 1.42 Ilustración de modo repetidor

1.3.1.5 Modo Cliente

Un AP posee toda las condiciones para funcionar como cliente, estación. Podría configurarse para que se conecte a otro AP y funcione como tal. Un AP es una participante más de la red WLAN posiblemente equipado con más capacidades.

1.3.2 Identificación del Basic Service Set

Cuando se trabaja tanto en modo infraestructura como ad-hoc los dispositivos distinguen la WLAN o "celda" lógica en el momento de la asociación por un nombre. Este nombre se lo llama Service Set Identifier o simplemente SSID. Este nombre es obligatorio por el estándar, aunque a menudo se lo suele ocultar. El formato debe ser de 2 a 32 caracteres ASCII y es sensitivo a mayúsculas y minúsculas. Se lo suele llamar a menudo con el término ESSID. Este valor sirve para identificar la WLAN al momento de conectarse, le da un nombre distintivo a la red. Si el cliente conoce el nombre de la WLAN o "celda" a la cual conectarse directamente lo utilizará. Si el cliente no conoce el nombre debe esperar que el dispositivo AP lo envíe de forma broadcast para luego poder seleccionar a que red conectarse, este último modo se lo conoce como Guest Mode o Broadcast SSID. Los AP pueden tener la capacidad también de trabajar con múltiples SSID, MSSID, donde cada SSID identificará una WLAN y puede ofrecer características diferentes en cuanto a seguridad, QoS, protocolos de red soportados, etc. Habitualmente se asocia un SSID con una red local, LAN cableada distinta. Esto se logra trabajando con VLANs 802.1Q [802.1Q] en la interfaz cableada Ethernet del AP. Cuando el cliente identifica la WLAN a la cual se quiere conectar, las tramas wireless llevarán el identificador del AP a través del cual

pasará el tráfico. Este identificador se conoce como Basic Service Set Id (BSSID), no confundir con el SSID que es el nombre de la red. El BSSID es una dirección otorgada por la IEEE, en este caso una dirección MAC-48/EUI-48. En el caso de una red de infraestructura el identificador es una MAC de la WNIC del AP. En el caso de una red ad-hoc es un valor con formato de MAC generado de forma aleatoria. En el caso que se trabaje con múltiples SSIDs se requiere un identificador BSSID (dirección MAC) diferente para cada red. Esta configuración se llama Multiple Basic Set Service Id (MBSSID) y los valores se generan a partir de una dirección MAC base sumándole 1 (uno) cada nuevo SSID.

1.3.3 Modos de Acceso Wireless

Los estándares IEEE 802.11, como la mayoría de los protocolos LAN, fueron diseñados para permitir el acceso al medio de forma múltiple, varias estaciones intentando acceder al medio para transmitir al mismo tiempo. Similar a como funcionaba la versión original de Ethernet, el medio es compartido, pero solo una estación puede transmitir al mismo tiempo. El acceso al medio es controlado por funciones llamadas de coordinación. Dentro de las funciones de coordinación se contemplan dos tipos principales dentro del estándar:

- Acceso distribuido sin coordinación central: Distributed Coordination Function (DCF).
- Acceso controlado de forma centralizada: Point Coordination Function (PCF).

La primera función es similar a la que tiene Ethernet, ninguna estación, incluso el AP, tiene el control de la red y todas deben competir entre sí para obtener el acceso al medio. El otro tipo de acceso requiere una estación especial, en particular el AP, que cumpla el rol de coordinador central. Este servicio es libre de contención y apropiado para aplicaciones que requieran un método de acceso determinístico como pueden ser aquellas de tiempo real. Según el estándar, DCF es obligatorio, no así PCF. En la mayoría de las implementaciones, el PCF no se considera. Posteriormente se definió un método de acceso híbrido:

- Acceso Híbrido con coordinación central: Hybrid Coordination Function (HFC).

Este ofrece un servicio intermedio entre PCF y DCF que sólo puede ser provisto en modo infraestructura. De la misma forma que sucedía con PCF, no es obligatorio. Brinda sobre un acceso con contención, diferentes niveles de Quality of Service (QoS), sin ser tan estricto como PCF. Parte de su definición está dada por el documento del estándar IEEE 802.11e [802.11e]. Su implementación se realiza a

través del manejo de distintas colas con prioridades. Más adelante se dedica una breve sección al estándar 802.11e. En la figura 1.43 se muestra un diagrama con la relación de las diferentes funciones de coordinación para acceder al medio.

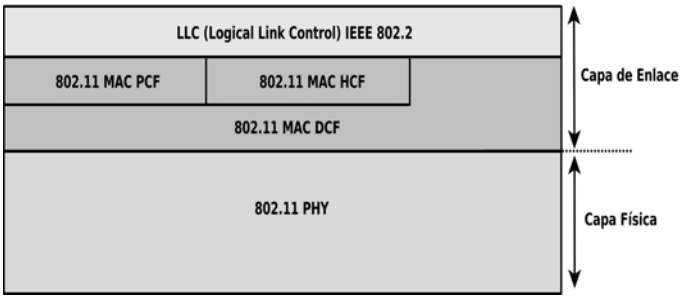


Figura 1.43 Diagrama con la relación de las funciones de coordinación para acceder al medio

1.3.3.1 DCF: CSMA/CA

En DCF, el mecanismo de acceso al medio es del tipo CSMA/CA. Como sucede con Ethernet/802.3, antes de empezar a transmitir la estación debe verificar que el medio no esté ocupado (no exista otra transmisión activa), a esto se refiere con CS (Carrier Sense), sensado de portadora. Como es un protocolo de medio compartido el acceso puede ser múltiple, es decir pueden existir varias estaciones intentando acceder: MA (Multiple Access). Hasta aquí el método de acceso es igual al de su "pariente cableado": Ethernet. La gran diferencia radica en que Ethernet puede detectar las colisiones mientras está transmitiendo, CD (Collision Detect), en cambio, en redes wireless como 802.11 esto es casi imposible y sino muy costoso. La detección de colisiones se hace dificultosa en un medio wireless al utilizar la misma banda para transmitir y recibir, debido a que la energía o potencia de la señal de transmisión es muy superior en la salida con respecto a la de la recepción. La señal de recepción se ve "opacada" por la de transmisión en las cercanías de la estación transmisora, de esta forma es casi imposible detectarla. Según la tecnología actual sería posible, pero a costos de hardware muy altos que la harían poco apropiada. Incluso con el hardware apropiado existen condiciones que no serían detectadas con la "escucha" sobre el medio físico. Un ejemplo de esto pueden existir cuando dos nodos no están al alcance uno de otro (no tienen puntos en común en el área de cobertura física, la celda), por lo tanto uno no podría detectar al otro cuando transmite. Si bien su comunicación es posible mediante un área común definida

por el AP, cada nodo estaría oculto del otro: problema del nodo oculto (ver más adelante en esta sección).
El método de acceso de 802.11 utiliza CA (Collision Avoidance) en lugar de CD, de esta forma se reducen la cantidad de colisiones haciendo más eficiente el acceso al medio. CA no significa que no existan colisiones, pero se tratan de evitar. De acuerdo a la forma de acceso CSMA/CA explicada, 802.11 es un protocolo que sólo puede trabajar en forma Half Duplex (HDX). Antes de transmitir se indicó que las estaciones deben sensar el medio para determinar si existe o no una transmisión en tránsito. Para esto 802.11 lo debe hacer de dos formas:

Sensado Físico: primero colaborando con la capa física, la capa MAC debe determinar si físicamente hay señales siendo transmitidas en su frecuencia. Para la primera forma el estándar define una máquina de estados finita llamada: Carrier Sense/Clear Channel Assessment (CS/CCA). Esta máquina corre con funciones de la capa física e intenta detectar señal en el medio. La misma máquina de estados se utiliza para detectar la señal que tiene como destino la estación. Clear Channel Assessment significa detectar que el canal está libre u ocupado, informando de esto a la capa MAC cuando lo solicita. En la figura 1.44 se muestra una relación entre las tres principales máquinas de estados de la capa física. La figura es tomada del documento estándar IEEE-802.11-2007 [802.11] (figura 14-5).

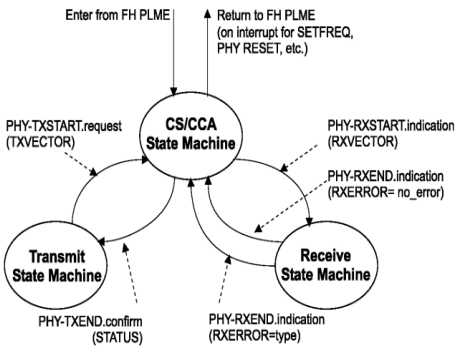


Figura 1.44 Principales máquinas de estados de la capa física y su relación

Sensado Virtual: además del sensado físico, IEEE 802.11 agrega el sensado a través de la observación de los encabezados de las tramas. Este se conoce por el estándar: **Virtual Carrier Sense (VCS)**: en español, Sensado Virtual. Para llevarlo a cabo cada estación está provista de un temporizador llamado **Network**

Allocation Vector (NAV) en castellano Vector de Reserva de Red. El tiempo del NAV se mide en microsegundos. Este funciona tratando de estimar el tiempo necesario que le llevará realizar una determinada transmisión. Calcula cuánto es el tiempo que le llevará a una estación realizar la transferencia exitosa contemplando todo el intercambio de tramas necesario. La mayoría de las tramas 802.11 contienen un campo en el encabezado llamado **"Duration"** (duración) que puede ser utilizado para indicar a las demás estaciones la duración de la transmisión actual. Existen tramas especiales como **PS-Poll** en que la porción del encabezado de la trama ocupada por este campo tiene otro significado. Cuando las estaciones observan los valores que indican la duración de una transmisión actualizan su NAV sumándole los valores de la trama en curso. El NAV se va decrementando de forma automática conforme pasa el tiempo y se incrementa cuando se detectan transmisiones o cuando la estación, previo a transmitir calcula el valor de la ventana de contención: **CW (Contention Window)**. Cuando el NAV llega a 0 (cero) se considera que el VCS indica que el canal esta libre. Cuando su valor es mayor que 0 (cero) se considera que el medio está ocupado.

Extensión del Sensado Virtual: Las estaciones, previo a enviar datos, pueden hacer una reserva del canal configurando el campo "Duration" en tramas especiales de control: RTS (Request to Send). Con estas tramas cortas de control una estación puede solicitar la reserva del medio por un determinado tiempo. Todas las estaciones que vean la reserva van a posponer sus futuras transmisiones y aumentar el NAV, el tiempo observado. El NAV se debe considera de forma atómica con la confirmación de la trama. Para que el envío se pueda hacer efectivo se requiere enviar un RTS al coordinador, el coordinador, que es el AP, debe otorgar el permiso con un mensaje de confirmación CTS (Clear to Send). Recién en esta instancia las demás estaciones deben actualizar el NAV con el valor anunciado por el coordinador, que se calcula restando el "handshake" **RTS/CTS** al NAV original enviado por la estación que reserva el canal. Puede utilizarse una optimización del mecanismo de reserva llamada **CTS-to-self**. En este caso, el mensaje CTS lo envía la misma estación transmisora llevando como ID destino a ella misma. Esta solución es más eficiente porque consume menos tiempo de aire y se obtiene un acceso más rápido. Según [GAS05], 802.11 para una transmisión completa de 428µs, con CTS-to-self requiere: 557µs, en

cambio con RTS/CTS la misma requiere 774µs. El conflicto que tiene este mensaje es que no resuelve el problema mencionado como **Nodo Oculto** ya que esta trama de control puede no ser vista por estaciones que no están al alcance de la celda física del emisor. Es importante remarcar que el sistema de VCS base, sin CTS/RTS, solo mirando el campo "Duration" tampoco funciona de forma adecuada en la presencia de este problema. Los mensajes RTS/CTS y CTS-to-self son utilizados también como un mecanismo de protección para las estaciones antiguas que no entienden las codificaciones y modulaciones usadas en la capa física de OFDM.

La figura 1.45 (izquierda) muestra el funcionamiento del método virtual con los mensajes de control RTS y CTS. El emisor hace uso de una trama RTS en la cual envía el valor de la duración para que se actualicen los contadores NAV. El receptor (el AP) contesta y confirma con el NAV actualizado. La figura 1.45 (derecha) muestra la aplicación del mensaje enviado directamente por la estación.

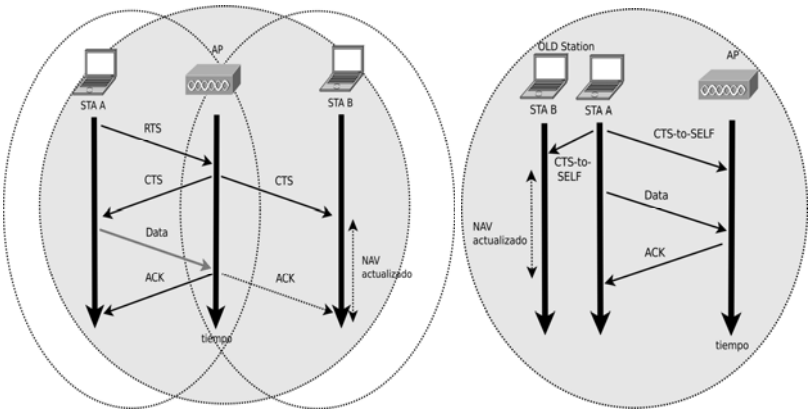


Figura 1.45 Utilización de los mensajes RTS/CTS y CTS-to-SELF

Problema del Nodo Oculto (Hidden Node Problem)

En una red cableada, cuando una estación envía un mensaje al medio, éste "se encarga" de que la señal generada sea recibida por todos los nodos conectados al mismo. Una estación es capaz de comunicarse con cualquier otra de la misma red. Las redes wireless tienen el problema de que dos o más estaciones pertenecientes al mismo BSS (celda lógica) no puedan comunicarse entre sí porque las celdas físicas son disjuntas. El área de cobertura de recepción y el patrón de radiación de cada estación no tienen puntos en común. Esto se conoce como problema del **Nodo**

Oculto (hidden node problem) y se muestra en el gráfico 1.46 (Fuente: Hidden Node Problem: http://en.wikipedia.org/wiki/Hidden_node_problem). En la figura se puede observar que la estación A se encuentra fuera del área de cobertura de la estación B y viceversa, sin embargo, ambas estaciones tienen en común el concentrador (HUB, AP) que les permitirá, actuando como intermediario, comunicarse. Si la estación A transmite directamente, la estación B no podrá detectarlo y, por lo tanto, podrán colisionar sin que sea percibido físicamente.

1.3.3.2 PCF

PCF está construido sobre DCF y solamente se puede ejecutar en el modo infraestructura. La función PCF se ejecuta en un nodo especial llamado Point Coordination (PC, Punto de Coordinación), que reside en el AP. Éste es el que determina qué estación tiene derecho a transmitir. El PC consulta a las estaciones para ver si alguna tiene tramas para transmitir. Al hacer que las estaciones transmitan por turno se crea un método de acceso libre de contención y de colisiones. Si este servicio se implementase en una red de infraestructura, debería intercalarse con el DCF. No está permitido que la red funcione sólo con PCF. En un mismo BSS pueden existir estaciones funcionando en DCF y en PCF simultáneamente, aunque el acceso al medio se hará de una por vez. Las estaciones utilizando el método PCF tiene prioridad sobre otra que usa DCF y esto se verá cuando se expliquen los intervalos de tiempos usados por el protocolo.

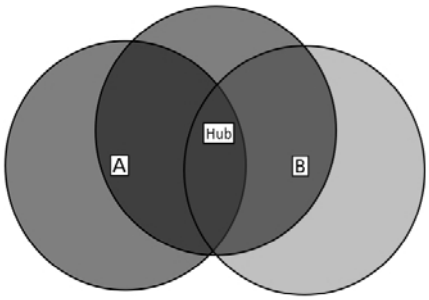


Figura 1.46 Ilustración del problema del nodo oculto

1.3.3.3 Intervalos entre Tramas

Para regular el acceso al medio en forma coordinada con los tres métodos se definen diferentes intervalos de tiempo entre tramas consecutivas, llamados **Espacio entre Tramas, Interframe Space (IFS)**. Se indican cinco **IFS** diferentes que permiten dar prioridades cuando se utilizan los de tiempos más cortos.

SIFS (Short Interframe Space): es el más corto, utilizado por las tramas de mayor prioridad como ACK, RTS/CTS y la fragmentación. Su valor se mide en **SlotTime**s y este varía de acuerdo al estándar de capa física (PHY).

PIFS (PCF Interframe Space): es el tiempo que continúa en duración. Es utilizado por estaciones que están operando en un entorno PCF durante el período libre de contención. Al tener una duración menor que DIFS, tendrán mayor prioridad. Su valor es:

$$PIFS = SIFS + SlotTime \tag{1.8}$$

DIFS (DCF Interframe Space): las estaciones operando con DCF deben esperar un tiempo **DIFS**, como mínimo, para empezar a transmitir sus tramas de datos y administración. Si el medio ha estado libre por un periodo mayor al DIFS, puede ser accedido.

$$DIFS=SIFS+2SlotTime \tag{1.9}$$

AIFS (Arbitration Inter-Frame Space): es usado cuando se trabaja con QoS, por ejemplo tramas de datos con QoS o tramas de administración, y en algunas tramas de control (PS-Poll, BlockAckReq, etc). En el caso de tramas de datos con QoS permite priorizar clases de tráfico sobre otras. Permite achicar los espacios para algunas "clases de tramas", estirarlos para otras, de acuerdo al índice *AC*(*AccessCategory*/*Class*) o *i*.

$$AIFS[i] = AIFSN[i]\ SlotTime + SIFS \tag{1.10}$$

El valor *AIFSN* depende la clase de acceso de acuerdo al tráfico.

EIFS (Extended Interframe Space): este tiempo debe ser considerado bajo DCF. No es un intervalo fijo y se usa únicamente cuando la capa física detecta un error en la transmisión de una trama. El intervalo comienza cuando la capa física le indica a la capa MAC que el medio está libre después de detectar una trama errónea. Es el más largo de los tiempos entre tramas.

En el gráfico 1.47 se puede observar una relación entre estos tiempos de espaciado de trama. La fuente del gráfico es el estándar IEEE 802.11-2007 [802.11] (figura 9-3).

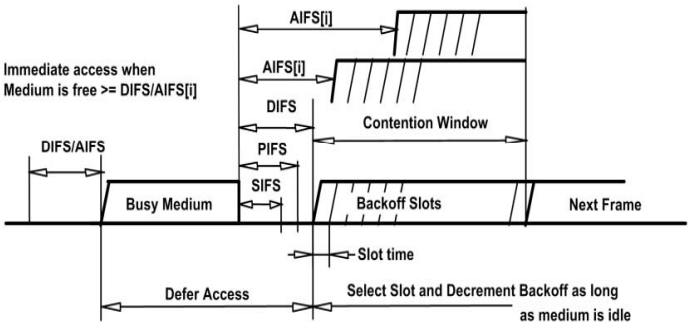


Figura 1.47 Intervalos usados por 802.11 y su relación

1.3.3.4 Algoritmos de Acceso al Medio y de Backoff

El método CSMA/CA en DCF es el que utilizan la mayoría de las tramas para ser enviadas. El objetivo es evitar que se produzcan las colisiones a raíz de transmisiones simultáneas o solapadas. Los pasos para el algoritmo de acceso son los siguientes:

1. La estación debe asegurarse que el medio esté libre.
   (a) Primero lo logra escuchando los niveles de señal en el medio. Método físico de detección, colaborando con la capa física a través de CCA (Clear Channel Assesment).
   (b) También debe tener en cuenta el método de detección de portadora virtual: VCS, mediante el temporizador NAV, y los mensajes CTS/RTS.
2. Una vez que se aseguró que el medio está libre de forma física y virtual debe esperar un tiempo DIFS escuchando si sigue libre o no. En el caso que la última trama recibida se detectó con errores, por ejemplo, a partir del chequeo de CRC, en lugar de esperar **DIFS** debe esperar un tiempo mayor, la cantidad determinada por **EIFS**.
3. Si el medio sigue libre luego del DIFS/EIFS, transmite.
4. Si la trama es unicast, el receptor debe confirmarla. La confirmación debe ser la trama inmediata a la trama de datos recibida. No se utiliza un mecanismo de ventana deslizante. Las confirmaciones son atómicas a la transmisión de los datos. Todos los ACKs deben ser positivos o directamente no se envían. Para confirmar, el receptor debe detectar el medio libre, esperar el tiempo más corto, **SIFS**, y, a continuación, si el medio sigue libre enviar la trama de confirmación. Si la trama es broadcast/multicast no se usan ACK.

5. Cuando el emisor recibe el ACK considera transmitida exitosamente la trama, sino la trata como una pérdida y debe volver a intentarlo. En los reintentos, la Ventana de Contención (CW) se va ir incrementando por el algoritmo de backoff dando tiempos de espera más grandes para acceder al medio.

En la figura 1.48 se muestra un diagrama de esta situación. El escenario es diferente si se detecta que el medio está ocupado luego de haber esperado el tiempo de DIFS/EIFS o si no se recibe el ACK.

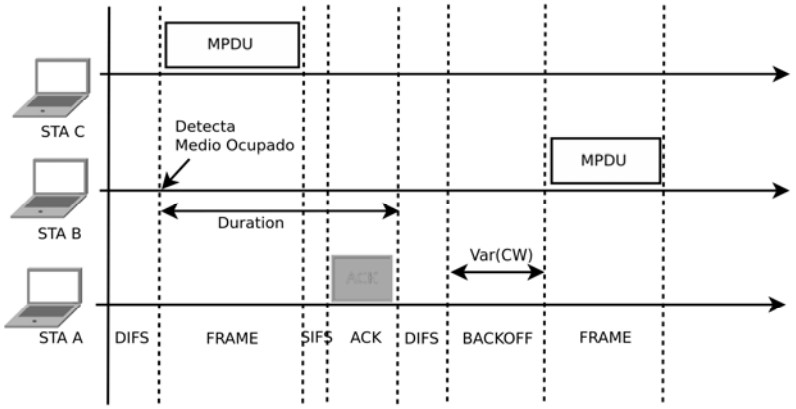


Figura 1.48 Ejemplo de acceso al medio sin backoff para "C"

1. La estación debe asegurarse que el medio esté libre.
2. La estación espera el intervalo DIFS/EIFS.
3. Si lo detecta ocupado luego del intervalo debe esperar por el tiempo que dure la transmisión en curso. En el estándar esto se llama **Acceso Diferido (Access Deferral)**
4. Al finalizar la transmisión en curso, debe esperar un tiempo DIFS sensando que el medio sigue libre de tramas.
5. Al terminar este tiempo no va a intentar enviar directamente, como sucedió en el primer intento, sino que va aplicar un algoritmo de espera exponencial conocido como el algoritmo de backoff. Éste es el encargado de determinar el tiempo que deben diferir su transmisión cada una de las estaciones que están esperando que cese la actividad. Este tiempo es aleatorio y se llama **Tiempo de Backoff (Backoff Timer)**. Indica la cantidad de TimeSlots que debe esperar una estación para poder empezar a transmitir. Notar la diferencia con 802.3/Ethernet aplicando **CD.** En Ethernet, el backoff se corre sólo si se produjo una colisión, en IEEE 802.11 con **CA** se corre para evitar la colisión, debido a que se obtuvo un **Acceso Diferido**, ya que el medio estaba ocupado. La otra condición necesaria para correr el algoritmo de backoff es porque

no se recibió un ACK. CSMA/CA intenta evitar las colisiones, para esto "obliga" a las estaciones que desean transmitir, después de que cesó la actividad en el medio, a esperar un tiempo aleatorio previo. Este mecanismo no es totalmente libre de colisiones, ya que dos o más estaciones podrían escoger el mismo tiempo de backoff y sus transmisiones colisionarán. El cálculo del backoff, al igual que sucede en Ethernet, se va realizando de forma exponencial en cada intento fallido. La fórmula para calcularlo es la siguiente:

$$BackoffTimer = rand[0..CW] * SlotTime \qquad (1.11)$$

CW, **Ventana de Contención (Contention Window)**, es un parámetro que toma un valor dentro de un rango [*CWmin*..*CWmax*]. Estos valores límites son definidos en la capa física e indican el valor mínimo y máximo que puede tomar la ventana. En el primer intento de transmisión, el valor de CW es igual a *CWmin*=0 (no hay backoff). Por cada intento fallido de retransmisión se incrementa el tamaño de la ventana. Este incremento se produce en valores de potencia de 2 menos 1, 2^n-1, (3, 7, 15, 31, 63, etc.) hasta alcanzar un valor máximo, *CWmax*. Los valores, después del cero, saltan de acuerdo al medio físico a 15 ó 31. El tamaño de la ventana vuelve a su valor original, 0 (cero), cuando la transmisión que disparó el algoritmo es exitosa o porque se agotaron todos los intentos de retransmisión de la trama corriente. Haber agotado todos los intentos genera un error que se reporta a las capas superiores, similar como sucede con 802.3/Ethernet. De acuerdo a las probabilidades, cuanto más grande sea el valor de CW existen menos posibilidades de que varias estaciones elijan el mismo valor y se produzcan colisiones.

6. Una vez agotado el DIFS y el BackoffTimer (se decrementan de a SlotTime) en la espera, la estación tendrá la oportunidad de transmitir. La que obtenga el menor BackoffTimer será la que gane el acceso al medio.
7. Mientras se decrementa el BackoffTimer, las estaciones deben continuar escuchando. Si en ese tiempo detectan otra transmisión activa, "congelan" el BackoffTimer y esperan que la transmisión finalice.
8. Cuando la estación que ganó el acceso al medio terminó de transmitir y pasó un tiempo DIFS, las demás estaciones reanudarán el proceso de backoff interrumpido ("congelado") previamente.

En la figura 1.49 se muestra un diagrama de la situación cuando se debe aplicar el algoritmo de backoff. Cada trama tendrá asociado un contador de retransmisiones, **Retry Counter.** Como se trabaja en forma **Stop & Wait** debido a que los ACK son atómicos, con uno basta. En la implementación se definen dos contadores de retransmisiones, uno para tramas cortas, **Short Retry Count,** y otro, **Long Retry Count,** para tramas largas. Existe un umbral que determina que trama son consideradas cortas y cuáles no, este es el **RTS threshold**.

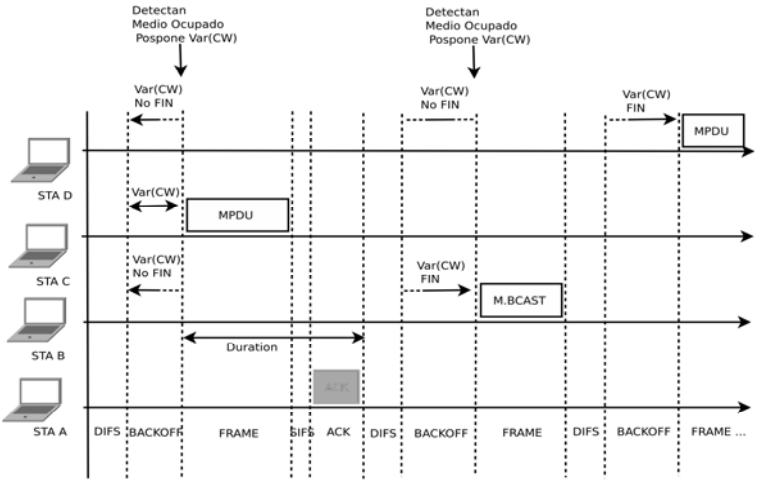


Figura 1.49 Ejemplo de acceso al medio con backoff para "D"

1.3.3.5 CTS/RTS

Los mensajes RTS/CTS tienen el propósito de protección cuando conviven redes 802.11b y 802.11g con OFDM y agregan la capacidad de tener una reserva del canal para enviar tramas de datos. El mecanismo RTS/CTS a través del concentrador es necesario para evitar el problema del nodo oculto. Como método de protección se explicó cómo se utiliza en la sección **PLCP para HR-DSSS/OFDM en 802.11g** en presencia de ERP (Extended Rate PHY). RTS/CTS también puede ser utilizado para el envío de tramas de datos sin necesidad de estar en presencia de equipos con 802.11b y ERP (Extended Rate PHY). Los equipos mantienen un umbral llamado **RTS threshold** que determina que tramas son consideradas largas. Las tramas largas deben ser transmitidas, previa reserva del canal, debido a que una retransmisión sería más costosa que hacer la reserva y la probabilidad de colisión sería más alta. Este método de transferencia permite una mejor recuperación en un sistema en el cual

existe mucha interferencia o está muy cargado. Si la carga del sistema es normal y las tramas no son demasiado largas su uso reduciría el ancho de banda digital (available digital bandwidth) produciendo una sub-utilización del medio. El valor puede ser configurado manualmente y por default en gran cantidad de equipos tiene el valor de 2346 bytes. El valor mínimo en varias implementaciones puede ser 0 (cero), significa que siempre se utilice. El estándar lo llama **dot11RTSThreshold**. En la figura 1.50 se muestra un diagrama de esta situación utilizando para acceder al medio el mecanismo CTS/RTS. A continuación, a modo ilustrativo, se muestra cómo se pueden configurar estos valores en dos equipos diferentes, el primero un Mikrotik corriendo RouterOS y el segundo un AP Cisco 1242G.

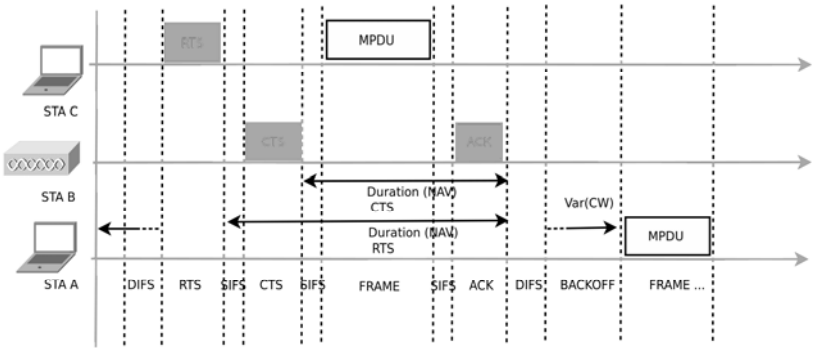


Figura 1.50 Ejemplo de acceso al medio con RTS/CTS

```
/interface wireless set wlan1 hw-protection-threshold=
 HwProtectionThreshold ::= 0..65535    (integer number)

/interface wireless set wlan1 hw-protection-mode=
 cts-to-self  none  rts-cts
```

Vista de configuración en el equipo cisco 1242G.

```
aptest(config)#interface dot11Radio 0
aptest(config-if)#rts threshold ?
  <0-2347>  threshold in bytes

aptest(config-if)#rts threshold 700
```

1.3.3.6 Confirmaciones: ACK 802.11

Como se explicó anteriormente, la recepción de una trama de confirmación (ACK) es la única prueba de que una trama unicast fue recibida correctamente por el destino. Si no se recibe la trama ACK, el emisor considera que hubo un error en la transmisión. Antes de

realizar la retransmisión de la trama se debe ejecutar el algoritmo de backoff. Si la trama unicast no llega o tiene un error detectado por el CRC, el receptor no hará nada, no hay mensajes de solicitud de re-transmisión. El tiempo de espera para el ACK es menor que para una trama de datos, por esto tiene mayor prioridad. Es importante remarcar que el envío de la trama de datos y la confirmación deben ser atómicas, es decir, producirse una seguida de la otra sin interrupciones de otras transmisiones. El temporizador asociado con los mensajes de ACK en algunos equipos puede ser modificado. A continuación se muestra la forma de lograrlo en un equipo Mikrotik.

```
/interface wireless set wlan1 ack-timeout=
 AckTimeout ::= dynamic | indoors
   dynamic -- Ack-timeout is chosen automatically
   indoors -- Standard constant for indoor usage
```

1.3.3.7 Fragmentación MAC 802.11

Los mensajes recibidos por las capas inferiores son habitualmente de tamaño mayor del soportado. Parte de la tarea de fragmentación es realizada por la capa de red, ya sea por los routers y extremos en IPv4 o por los extremos en IPv6. La fragmentación a nivel MAC puede ayudar a trabajar con menos errores en presencia de interferencia. Se fragmenta en el caso en que los mensajes enviados por la capa superior superan el umbral de fragmentación: **Fragmentation threshold**. Los fragmentos son manejados con contadores y con parte de los campos de control específicos. Los fragmentos son enviados en ráfagas y cada uno requerirá de su confirmación correspondiente. Cada fragmento reservará el NAV para el próximo y el último indicará el NAV como 0 (cero). La separación entre fragmentos se realiza con espacios SIFS y comienzan de acuerdo a su tamaño con un "handshake" RTS/CTS. El valor habitual que se configura es igual al del **RTS threshold**, 2346 bytes. El estándar lo llama **dot11FragmentationThreshold**. El valor mínimo permitido por varias implementaciones es de 256 bytes. A continuación se muestran ejemplos de configuración.

```
/interface wireless set wlan1 hw-fragmentation-threshold=
 HwFragmentationThreshold ::= disabled | Num
  Num ::= 256..3000    (integer number)

/interface wireless set 0 hw-retries=
 HwRetries ::= 0..15    (integer number)

aptest(config-if)#fragment-threshold ?
  <256-2346>
```

1.3.3.8 HiperLAN, HiperLAN/2 a nivel MAC

HiperLAN, a diferencia de 802.11 (CSMA/CA), trabaja a nivel MAC con un método de acceso determinístico **Dynamic TDMA** y tiene el manejo de QoS incorporado. HiperLAN trabaja con ARQ con retransmisión selectiva y es orientado a conexión.

1.3.4 Tramas MAC 802.11

Se definen diferentes unidades de encapsulamiento de acuerdo a la capa en la que se trabaja. La unidad más baja es la secuencia de Bits y Símbolos que conforma el PDU (Protocol Data Unit) de nivel físico (PHY) sub-capa PMD. A continuación sigue la trama de sub-nivel PLCP:

PPDU: PLCP Protocol Data Unit. Trama a nivel PLCP, sub-capa física superior: Physical Layer Convergence Procedure. Éstas llevan como payload las tramas MAC. El encapsulamiento y funcionamiento se explicó en la sección **PLCP (Physical Layer Convergence Procedure**).

Continuando hacia arriba, está la trama MAC.

MPDU: MAC Protocol Data Unit. Es el mensaje en formato de trama que intercambian las entidades a nivel MAC. Las MPDU pueden ser de tamaño mayor que las MSDU (MAC Service Data Unit). Un MPDU puede incluir varios MSDUs como resultado de agregación de tramas. También puede suceder que un MSDU genere varios MPDU en el caso de que exista fragmentación/segmentación. Los MPDU van dentro de los PPDU. Los MPDU son también llamados **PSDU (PLCP Service Data Unit)**.

Continúan las tramas de nivel superior:

MSDU: MAC Service Data Unit. Son las unidades recibidas desde la sub-capa LLC (Logical Link Control). Las MSDU van dentro de las tramas MAC, MPDU.

En la figura 1.51 se diagrama la relación entre las diferentes unidades, las capas y sub-capas. Las redes wireless estandarizadas por IEEE 802.11, si bien tienen varias similitudes con las redes cableadas 802.3, en varios aspectos son mucho más complejas. Para el caso de las redes 802.3/Ethernet las tramas se diferencian directamente por el campo **EtherType**, pero a nivel MAC son consideradas todas como tramas de datos. Para el caso de las redes IEEE 802.11 se distinguen tres tipos de tramas:

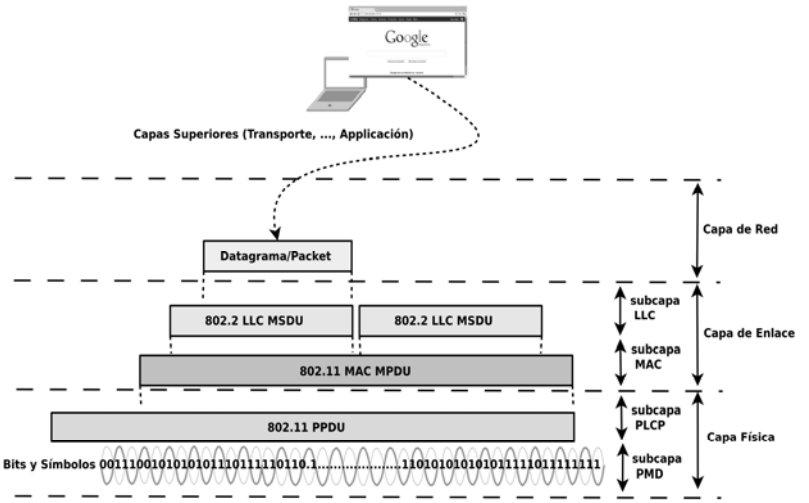


Figura 1.51 Diagrama de la relación entre los PDUs, las capas y sub-capas

Tramas de Datos (Data frames): tramas conteniendo datos de usuario o protocolos de nivel superior según el modelo OSI.

Tramas de Administración (Management frames): tramas usadas para administrar la conexión a la celda (BSS), operaciones como: descubrimiento, autenticación, asociación, etc.

Tramas de Control (Control frames): tramas usadas para controlar el acceso al medio y confirmaciones (ACK). Tramas operativas. Una gran diferencia entre 802.3/Ethernet y IEEE 802.11 es que este último agrega a nivel de enlace (LNK) confirmaciones.

Todas las tramas a nivel MAC, llamadas PSDU o MPDU, tienen la misma composición. Están divididas en tres partes:

Cabecera MAC (MAC Header): incluye información de control, direcciones MAC, etc.

Cuerpo de la trama (Body): cuerpo, un campo de longitud variable que contiene información específica de la trama, llamado también payload.

Cola de la trama (Trailer): contiene la Secuencia de chequeo de trama **FCS (Frame Check Sequence)** también identificado como **CRC (Cyclic Redundancy Code)** formado por un campo de 32 bits para detección de errores. Intenta controlar la integridad de la trama.

A modo de comparación con 802.3/Ethernet se pueden puntualizar las siguientes características similares:

- Medio Broadcast: soporta broadcast y multicast.
- Utiliza el mismo formato de direcciones MAC.

- Calcula un CRC de 32 bits.
- Puede utilizar encapsulamiento 802.2 para las capas superiores.

Como características diferenciadoras:

- Se definen tramas de diferentes tipos: datos, administración y control.
- El formato de la trama es más complejo.
- Utiliza ACK (Acknowledgment) positivos. Las operaciones de envío son atómicas, cada trama de datos que se envía requerirá la correspondiente confirmación. Las tramas de broadcast y multicast no necesitan ACK.
- Las tramas unicast pueden ser fragmentados.
- El encapsulamiento usado en redes cableadas es el de Ethernet según RFC-894 [RFC894], en cambio en IEEE 802.11 se usa 802.2.

1.3.4.1 Entorno de Pruebas 802.11bg

El capítulo trata de explicar el funcionamiento de los protocolos a través de ejemplos. En esta sección se introduce uno de los entornos usados para generar las pruebas y capturar el tráfico que más tarde se analizará. El diagrama del entorno se muestra en la figura 1.52. En este contexto se tiene un AP Cisco 1242G, dos estaciones inalámbricas: una con chipset Intel y la otra con una WNIC Cisco Aironet 350. Además, se cuenta con una red cableada materializada por un switch y se agregan dos estaciones LAN, una cumpliendo el rol de router y servidor de DHCP. A continuación se muestran las características del AP:

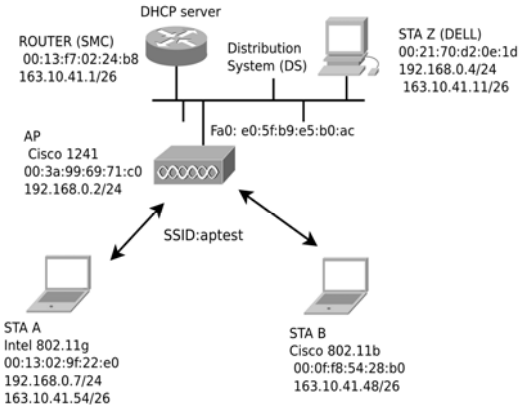


Figura 1.52 Entorno de laboratorio para las pruebas de infraestructura

```
aptest>show version
Cisco IOS Software, C1240 Software (C1240-K9W7-M), Version
12.4(21a)JA1,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 16-Sep-09 19:06 by prod_rel_team

ROM: Bootstrap program is C1240 boot loader
BOOTLDR: C1240 Boot Loader (C1240-BOOT-M) Version 12.4(13d)JA,
RELEASE SOFTWARE (fc2)

aptest uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash:/c1240-k9w7-mx.124-21a.JA1/c1240-k9w7-
mx.124-21a.JA1"
...

cisco AIR-AP1242G-A-K9     (PowerPCElvis) processor (revision A0)
with 24566K/8192K bytes of memory.
Processor board ID FTX1504B3AP
PowerPCElvis CPU at 262Mhz, revision number 0x0950
Last reset from power-on
1 FastEthernet interface
1 802.11 Radio(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: E0:5F:B9:E5:B0:AC
...
Product/Model Number                : AIR-AP1242G-A-K9

Configuration register is 0xF
```

Se configura para que trabaje en modo infraestructura con el SSID **"aptest"** y se "bridgea" la interfaz wireless con la LAN Ethernet para que se comunique con el DS. Se configura un bridge transparente. No se configura seguridad, Autenticación "Open System" y no se cifra, para poder ver el tráfico mejor. Se lo configura en el canal 2 (2,417GHz).

```
aptest#show running-config
...
hostname aptest
!
dot11 ssid aptest
   authentication open
   guest-mode !!! Broadcast SSID
!
!!! Modo de BRIDGE, se puede rutear y bridgear de forma simultánea
pasando
!!! tráfico entre estas:  Integrated Routing and Bridging (IRB).
(Conf Default).
bridge irb
!
```

```
!!!!!! Interfaz de RADIO !!!!!!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid aptest
 !
 antenna gain 3  !!! Ganancia de la ANT, dipolo de 2.2dbi
 channel 2417 !!! channel 2
 station-role root  !!! Modo AP ROOT
 world-mode dot11d country-code AR indoor
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
!!!!!! Interfaz CABLEADA !!!!!!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
!!!!!! Interfaz VIRTUAL de Admin !!!!!!
interface BVI1
 ip address 192.168.0.2 255.255.255.0
 no ip route-cache
!
bridge 1 route ip
end
```

Con el siguiente comando se puede analizar la interfaz de radio:

```
aptest>show interfaces Dot11Radio 0
Dot11Radio0 is up, line protocol is up
  Hardware  is  802.11G  Radio,  address  is  003a.9969.71c0  (bia
003a.9969.71c0)
  MTU 1500 bytes, BW 54000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:02:08, output 00:00:00, output hang never
  ...
```

Y, ahora lo mismo con la interface LAN Ethernet:

```
test>show interfaces FastEthernet 0
FastEthernet0 is up, line protocol is up
```

```
  Hardware is PowerPCElvis Ethernet, address is e05f.b9e5.b0ac (bia
e05f.b9e5.b0ac)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  ...
```

Se observan los SSID configurados y las asociaciones. Todavía no hay ninguna estación asociada.

```
aptest#show dot11 bssid
Interface      BSSID         Guest  SSID
Dot11Radio0   003a.9969.71c0  Yes  aptest

aptest#show dot11 associations
```

Luego, se configuran los dos clientes wireless para que se asocien. En este caso se lo hace de línea de comando. Ambos son equipos GNU/Linux.

```
root@STA-A:~# uname -a
Linux STA-A 2.6.32-33-generic #71-Ubuntu SMP Wed Jul 20 17:27:30 UTC
2011 x86_64
GNU/Linux

root@STA-A:~# ifconfig wlan0 down

root@STA-A:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:13:02:9f:22:e0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1955 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1236 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:451242 (451.2 KB)  TX bytes:209288 (209.2 KB)

root@STA-A:~# iwconfig wlan0
wlan0     IEEE 802.11abg  ESSID:"..."
          Mode:Managed   Frequency:2.462   GHz   Access   Point:   Not-
Associated
          Tx-Power=14 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Se activa la interfaz y se realiza un “scanning” de las redes:

```
root@STA-A:~# ifconfig wlan0 up
```

```
root@STA-A:~# iwlist wlan0 scan
wlan0     Scan completed :
          Cell 01 - Address: 00:15:6D:AD:BE:6F
                    Channel:11
                    Frequency:2.462 GHz (Channel 11)
                    Quality=70/70  Signal level=-38 dBm
                    Encryption key:on
                    ESSID:"support"
                    Bit Rates:1 Mb/s;2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s
                    Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
                    Mode:Master
                    Extra:tsf=000000b008a60071
                    Extra: Last beacon: 1356ms ago
                    IE: Unknown: 0007737570706F7274
                    IE: Unknown: 010882848B0C12961824
                    IE: Unknown: 03010B
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (2) : CCMP TKIP
                        Authentication Suites (1) : PSK
                    IE: Unknown: 2A0100
                    IE: Unknown: 32043048606C
                    IE: Unknown: DD26000C420000000...

          Cell 02 - Address: 00:3A:99:69:71:C0
                    Channel:2
                    Frequency:2.417 GHz (Channel 2)
                    Quality=64/70  Signal level=-46 dBm
                    Encryption key:off
                    ESSID:"aptest"
                    Bit Rates:1 Mb/s;2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s
                    Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
                    Mode:Master
                    Extra:tsf=000000000620c18c
                    Extra: Last beacon: 1448ms ago
                    IE: Unknown: 0006617074657374
                    IE: Unknown: 010882848B0C12961824
                    IE: Unknown: 030102
                    IE: Unknown: 0706415249010B1A
                    ...
                    IE: Unknown: DD050040961400

          Cell 03 - Address: 00:17:59:FB:0D:60
                    Channel:3
                    Frequency:2.422 GHz (Channel 3)
                    Quality=28/70  Signal level=-82 dBm
                    Encryption key:on
                    ESSID:"cespi"
                    Bit Rates:1 Mb/s;2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s
                    Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
                    Mode:Master
```

```
                    Extra:tsf=0000017017a72197
                    Extra: Last beacon: 1472ms ago
                    IE: Unknown: 00056365737069
                    IE: Unknown: 010882040B0C12161824
                    ...
                    00000000004000025
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (1) : TKIP
                        Authentication Suites (1) : PSK
                    IE: Unknown: DD06004096010100
                    IE: Unknown: DD050040960304
                    IE: Unknown: DD1600409604000...
                    IE: Unknown: DD050040960B01
                    IE: Unknown: DD180050F20...
                    ...
```

Luego, se asocia la estación a la celda.

```
root@STA-A:~# iwlist wlan0 scan | grep aptest
                    ESSID:"aptest"

root@STA-A:~# ifconfig wlan0 down

root@STA-A:~# iwconfig wlan0 essid aptest channel 2
root@STA-A:~# iwconfig wlan0
wlan0     IEEE 802.11abg  ESSID:"aptest"
          Mode:Managed    Frequency:2.417  GHz    Access  Point:  Not-
Associated
          Tx-Power=15 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@STA-A:~# ifconfig wlan0 up
root@STA-A:~# iwconfig wlan0 ap any

root@STA-A:~# iwconfig wlan0
wlan0     IEEE 802.11abg  ESSID:"aptest"
          Mode:Managed      Frequency:2.417   GHz      Access   Point:
00:3A:99:69:71:C0
          Bit Rate=54 Mb/s   Tx-Power=15 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=56/70  Signal level=-54 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Se configura la capa de red y se prueba contra sí misma (no usa los servicios de DS) y luego contra el AP.

```
root@STA-A:~# ifconfig wlan0 192.168.0.7 up
```

```
root@STA-A:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:13:02:9f:22:e0
          inet       addr:192.168.0.7             Bcast:192.168.0.255
Mask:255.255.255.0
          inet6 addr: 2800:340::213:2ff:fe9f:22e0/64 Scope:Global
          inet6 addr: fe80::213:2ff:fe9f:22e0/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:2600 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1299 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:493495 (493.4 KB)  TX bytes:219966 (219.9 KB)


root@STA-A:~# ping 192.168.0.7
PING 192.168.0.7 (192.168.0.7) 56(84) bytes of data.
64 bytes from 192.168.0.7: icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from 192.168.0.7: icmp_seq=2 ttl=64 time=0.033 ms
^C
--- 192.168.0.7 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.033/0.036/0.040/0.007 ms

root@STA-A:~# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=4.01 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.814 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.810 ms
^C
--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.810/1.879/4.013/1.508 ms
```

A continuación se configura la otra estación:

```
root@STA-B:~# iwconfig eth4
eth4      IEEE 802.11-DS  ESSID:"tsunami"
          Mode:Managed  Frequency:2.437 GHz  Access Point: Invalid
          Bit Rate:11 Mb/s   Tx-Power=20 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=-112 dBm  Noise level=-93 dBm
          Rx invalid nwid:59  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:414   Missed beacon:0

root@STA-B:~# ifconfig eth4
eth4      Link encap:Ethernet  direcciónHW 00:0f:f8:54:28:b0
          DIFUSIÓN MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:0 errores:18 perdidos:0 overruns:0 frame:18
          Paquetes TX:10 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:0 (0.0 B)  TX bytes:1716 (1.7 KB)
          Interrupción:3 Dirección base: 0x3100
```

```
root@STA-B:~# iwconfig eth4 essid aptest channel 2

root@STA-B:~# ifconfig eth4 up
root@STA-B:~# iwconfig eth4 ap any

root@STA-B:~# iwconfig eth4
eth4      IEEE 802.11-DS  ESSID:"aptest"
          Mode:Managed  Frequency:2.417 GHz  Access Point: 00:3A:99:69:71:C0
          Bit Rate:11 Mb/s   Tx-Power=20 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=100/100  Signal level=-40 dBm  Noise level=-91 dBm
          Rx invalid nwid:1771  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:24557   Missed beacon:0

root@STA-B:~# ifconfig eth4
eth4      Link encap:Ethernet  direcciónHW 00:0f:f8:54:28:b0
          Dirección inet6: fe80::20f:f8ff:fe54:28b0/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:420 errores:332 perdidos:0 overruns:0 frame:332
          Paquetes TX:62 errores:6 perdidos:0 overruns:0 carrier:6
          colisiones:0 long.colaTX:1000
          Bytes RX:23454 (23.4 KB)  TX bytes:8781 (8.7 KB)
          Interrupción:3 Dirección base: 0x3100
```

La estación en la LAN, “Z”, está previamente configurada:

```
root@STA-Z:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:21:70:d2:0e:1d
          inet addr:192.168.0.11  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::221:70ff:fed2:e1d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3853 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3658 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3344465 (3.3 MB)  TX bytes:651589 (651.5 KB)
          Interrupt:29 Base address:0xe000
```

Con estas configuraciones es suficiente para estudiar la primera parte del comportamiento del protocolo. A continuación se muestran las asociaciones de estaciones.

```
aptest#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [aptest] :

MAC Address    IP address      Device        Name  Parent         State
000f.f854.28b0 192.168.0.4     350-client    -     self           Assoc
0013.029f.22e0 192.168.0.7     unknown       -     self           Assoc
```

Es importante notar que se requiere que uno de los equipos capture tráfico. Para esto se utiliza la misma estación conectada directamente a la LAN usando el programa AirCrack Next Generation.

```
root@STA-Z:~# dpkg -l aircrack-ng
...
||/ Name                 Version       Description
+++-====================-=============-==================================
ii  aircrack-ng          1:1.0-1       wireless WEP/WPA cracking utilities
```

Primero configurar la WNIC para que trabaje en modo monitor y luego lanzar el programa `airodump-ng` que viene como parte de la suite: `aircrack-ng`.

```
root@STA-Z:~# ifconfig wlan0 down

root@STA-Z:~# iwconfig wlan0 mode Monitor

root@STA-Z:~# iwconfig wlan0
wlan0     IEEE 802.11abg  Mode:Monitor  Frequency:2.437 GHz  Tx-Power=15 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

root@STA-Z:~# ifconfig wlan0 up

root@STA-Z:~# airodump-ng -b bg -c 2 -w infr-aptest-raw wlan0
```

Luego la salida se puede analizar con la herramienta Wireshark (comando `wireshark`) y/o el comando `tcpdump`.

```
root@STA-Z:~# tcpdump -n -r infr-aptest-raw.cap | head -4
reading from file cap4/infr-aptest-raw.pcap, link-type IEEE802_11 (802.11)
13:22:17.905708 Data IV:1b7c7c Pad 20 KeyID 1
13:22:17.905736 Beacon (aptest) [1.0* 2.0* 5.5* 6.0 9.0 11.0* 12.0 18.0 Mbit]
                ESS CH: 2
13:22:18.126440 Beacon (HPC73189) [1.0* 2.0* 5.5* 11.0* Mbit] IBSS CH: 1
13:22:18.489452 Data IV:1d7c7c Pad 20 KeyID 1
```

1.3.4.2 Campos de las Tramas MAC

En la figura 1.53 se muestra un diagrama de una trama 802.11 de datos y en la figura debajo de una trama Ethernet para su comparación. Las tramas IEEE 802.11 contienen los siguientes campos:

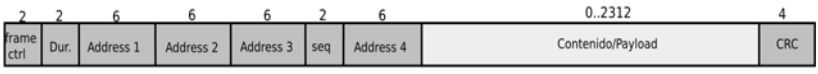


Figura 1.53: Trama MAC 802.11 y trama Ethernet

Control de Trama (Frame Control): en este campo de 16 bits (2 bytes) se codifican los siguientes datos:

Versión del Protocolo - Protocol (0..1): protocol version. Por ahora solo cero (0).

Tipo de Trama - Type (2..3): si es de datos, administración, control o reservado.

```
00: Management Frame.
01: Control Frame.
10: Data Frame.
11: Reservado.
```

Sub-tipo - Subtype (4..7): dentro del tipo de trama a que sub-tipo pertenece. En la tabla/figura 1.54 se muestran algunos valores.

Type	Subtype	Descripción
00	0000	Association Request
	0001	Association Response
	0100	Probe Request
	0101	Probe Response
	1000	Beacon
	1011	Authentication
01	1011	Request to Send
	1100	Clear to Send
	1101	Ackowledgment
10	0000	Data
	0001	Data+CF-Ack
	0100	Null Data
	1000	QoS Data (802.11e)

Figura 1.54 Tabla con subtipos de valores para las tramas 802.11

Hacia el DS/Desde el DS (8..9): de acuerdo al modo indican, por ejemplo, si la trama va desde el AP hacia una estación, o desde una estación al AP. Puede ser que el sentido sea de bridge a bridge (WDS) o de estación a estación. De acuerdo a estos valores serán los campos direcciones que se utilicen y el significado de estos. En la tabla/figura 1.55 se muestran las combinaciones que pueden tomar. La combinación (0,0) es en modo ad-hoc y el campo BSSID se genera de forma aleatoria, la combinación (0,1) es en modo infraestructura, la trama es reenviada del AP (BSSID) a una estación (DA) a

partir del origen (SA). Combinación (1,0), la trama es enviada al AP (BSSID), para que la reenvíe a otra estación (DA). En ninguno de estos tres casos se usa la cuarta dirección. Por último la combinación (1,1) en modo bridge WDS, un AP-bridge (TA) transmisor, le envía a otro AP-bridge (RA) receptor, siendo la estación origen (SA) y destino final (DA).

Más Fragmentos - More Fragments Bit (10): 1 es fragmentado.

Retransmisión - Retry Bit (11): 1 es una trama retransmitida.

Adm. de Potencia - Power Management Bit (12): 1 está en modo **PS (Power Save)**.

Más Datos - More Data Bit (13): 1 el AP tiene más tramas para una estación en PS.

Trama Protegida - Protected Frame Bit (14): 1 significa que el payload está cifrado.

Bit de Orden - Order Bit (15): 1 significa que los fragmentos son transmitidos en orden.

Campo Opcional de QoS: un campo opcional de 2 bytes se agrego para trabajar con 802.11e.

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

Figura 1.55 Tabla con las combinaciones que pueden tomar los campos direcciones

Duración / ID (Duration / ID): en este campo de 16 bits (2 bytes) se codifica el valor del NAV (Network Allocation Vector). Si la trama es transmitida en PCF (Contention-free) lleva el valor 32768. Las tramas broadcast/multicast llevan el valor 0 debido a que no requieren ACK, no son parte de una transmisión atómica. Si el bit MD (More Data) está en 0 significa que sólo se reserva el tiempo hasta el ACK. Si el bit MD (Mora Data) está en 1 significa que siguen más fragmentos, en la primera se reserva el tiempo para 2 (dos) ACK, 3 (tres) SIFS y el próximo fragmento. Un NAV no final funciona como un RTS. Ver figura 1.56. Este campo puede tener otros significados de acuerdo al tipo de trama. En una trama **PS-Poll (Power Save Poll)** indica el **Association Identifier (AID)**.

Dirección (Address): los campos direcciones pueden ser varios y

dependen del campo **Control de trama**. Como ya se explicó respectivamente de acuerdo a los bits de **To DS**, **From DS** tienen diferente significado. Sus valores también cambian de acuerdo al tipo, por ejemplo tramas en un entorno con WDS llevan 4 (cuatro) direcciones, tramas de datos en BSS llevan 3 (tres) direcciones, las tramas de control RTS llevan 2 (dos) direcciones y los ACK llevarían 1 (una) sola. El formato de las direcciones son IEEE MAC-48 / EUI-48.

Control de Secuencia (Sequence Control): 16 bits (2 bytes) dividido en 2 sub-campos:

Número de Fragmento (Fragment Number): 4 bits. El primero lleva el valor (0) y el máximo alcanzado 15 (quince).

Número de Secuencia (Sequence Number): 12 bits. Se incrementa en 1 (uno) en cada trama, al llegar a 4095 se vuelve a comenzar de 0 (cero) –wrap around–.

El campo es utilizado para identificar los fragmentos que pertenecen a una misma trama original y su orden dentro de ésta. Permite identificar campos duplicados. Tener en cuenta que 802.11, en la mayoría de sus versiones, utiliza como ARQ (Automatic Repeat Request) la técnica de Stop & Wait (SW) y no usa los números de secuencias con Go-back-N o re-transmisión selectiva. Este método es adecuado debido que el tiempo de propagación es corto, existe alta tasa de errores y las velocidades no son muy rápidas. A partir de 802.11n y 802.11e se incorporan nuevos métodos como **BurstACK**.

Contenido / Carga Útil (Payload): cuerpo de la trama. Lleva los datos de las capas superiores. La carga "cruda" máxima está definida como 2312 bytes. Si se la agrega el encabezado 802.2 LLC de 8 bytes deja lugar para una carga útil de 2304 bytes. Si en lugar de enviar los datos directamente se le agrega el encabezado **MIC (Message Integrity Check)** y/o **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol** o **CCMP (CCM mode Protocol)** de 8 ó 16 bytes quedan finalmente 2296 bytes (IEEE 802.2 en este caso va dentro del payload asegurado). Debido a que no tiene como Ethernet un campo **EtheType** para indicar la capa superior a la cual se le debe entregar el contenido (o de quien proviene) se requieren encabezados adicionales como el de IEEE 802.2 (LLC) para este propósito. No se utiliza relleno (padding) como en Ethernet. La fragmentación en capas superiores en general es reducida al utilizar MTU de 1500 ó aplicar el proceso de Path MTU Discovery (RFC 1191)

[RFC1191].

Control de Errores (Frame Check Sequence) (Cyclic Redundancy Check): campo de 32 bits (4 bytes). Trailer de la trama calculado sobre la trama completa con el polinomio generador CRC-32. Es el mismo método usado en Ethernet. Si el control es correcto y es una trama unicast se debe enviar el correspondiente ACK, sino se descarta y se espera la re-transmisión.

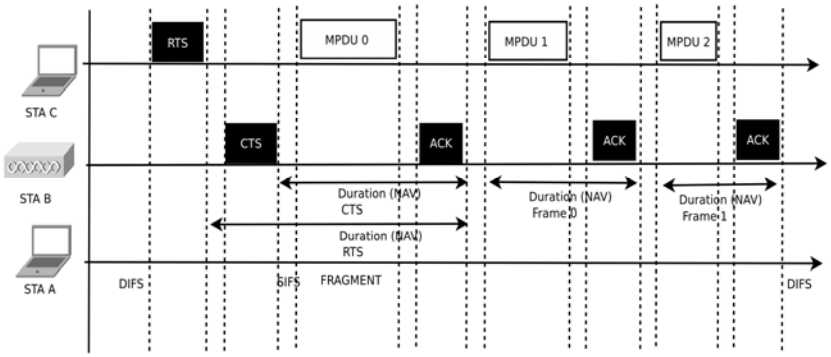


Figura 1.56: Escenario de fragmentación

1.3.4.3 Tramas de Datos

En la figura 1.57 se muestra una trama de datos analizada con la herramienta Wireshark que lleva información ICMP de una estación a otra (en este caso de "STA A" (192.168.0.7) al AP (192.168.0.2)). En la misma se puede observar todos los campos descriptos anteriormente: **Frame Control**, **"Duration"**, las 3 (tres) direcciones MAC y el campo de **Sequence Number**. En el campo **Frame Control** se muestra la versión del protocolo, el tipo y el sub-tipo, en este caso versión 0, tipo 2 (10), subtipo 8 (1000) debido a que lleva Datos con encabezado de QoS. El tiempo de la transmisión de acuerdo al campo **"Duration"** es de 44μ. Las direcciones MAC son: BSSID=MAC base de la interfaz wireless del AP, SA=MAC wireless de la estación STA "A" y DA=MAC Ethernet del AP que es la que se asocia con la interfaz de administración lógica: BVI (Bridged Virtual Interface). El campo **Sequence Number** indica que lleva el orden 17.

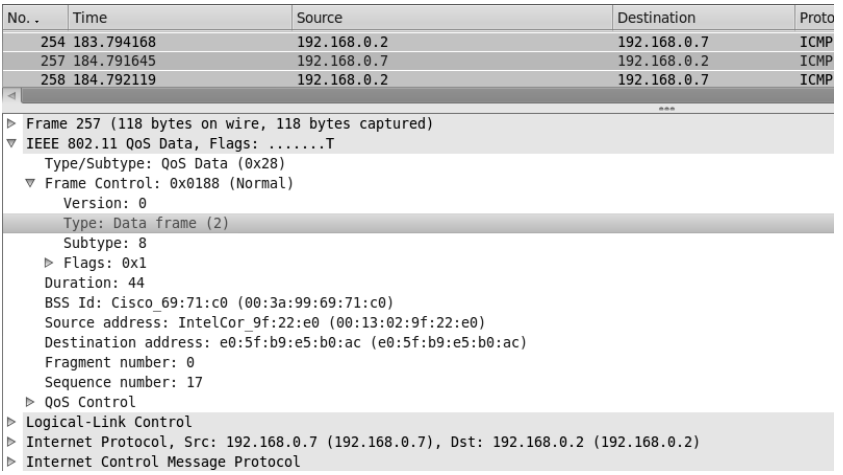


Figura 1.57 Trama 802.11 de datos llevando mensaje ICMP

(El archivo de captura utilizado es `infr-aptest.pcap` en el cual se filtra todo lo relacionado con el BSSID=00:3a:99:69:71:c0, que es el del AP utilizado, luego sobre la captura se muestran solo los mensajes ICMP).
A modo de comparación en la figura 1.58 se muestra una trama Ethernet inspeccionada con la misma herramienta. Se puede observar que el formato de trama es mucho más simple.

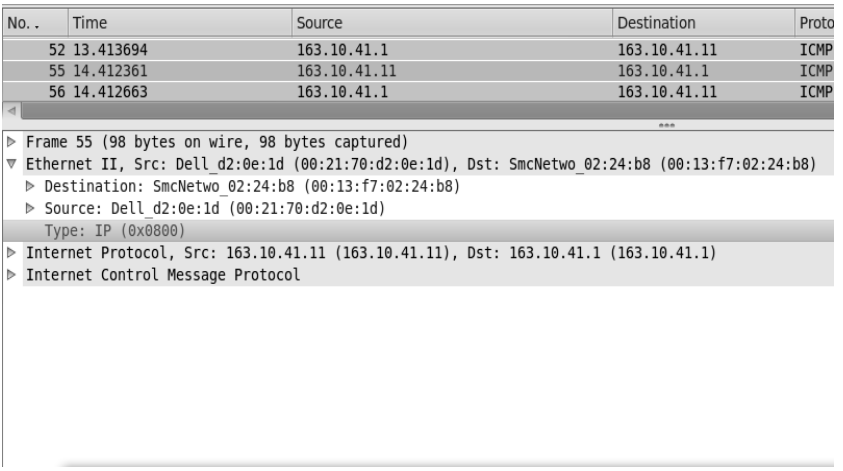


Figura 1.58 Trama Ethernet analizada con la herramienta Wireshark

Volviendo a la trama 802.11 en el campo **Sequence Number** se muestra el número de secuencia, 17, y se puede ver que es el primer fragmento, el cero (0) (en este caso no hay fragmentos). Si se pasa

desde el mensaje capturado 257 al 260, ver figura 1.59, se puede observar que el próximo número de secuencia será el 18. Desplegando los valores de los flags del número de captura 257, figura 1.60, se ve que es una trama que va desde una estación hacia el AP. Si se salta a la próxima captura de mensaje ICMP Echo Reply, número 258, se ve que los flags están en el orden inverso, viene desde el AP, figura debajo.

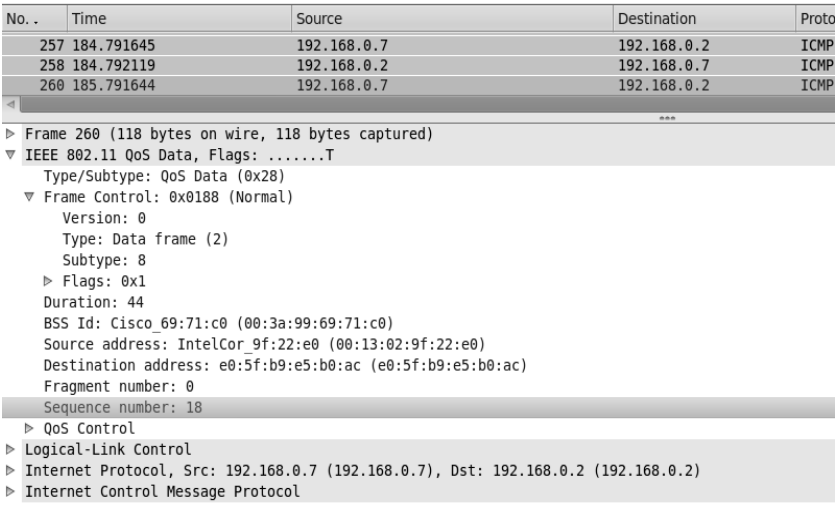
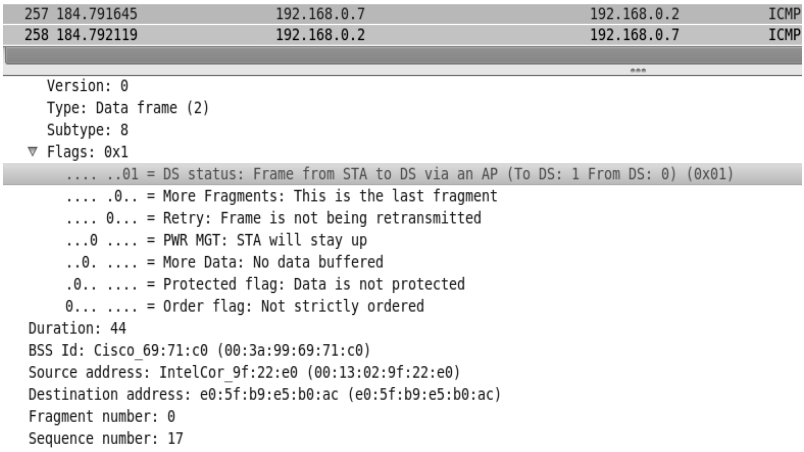


Figura 1.59 Trama 802.11 siguiente a la analizada llevando ICMP



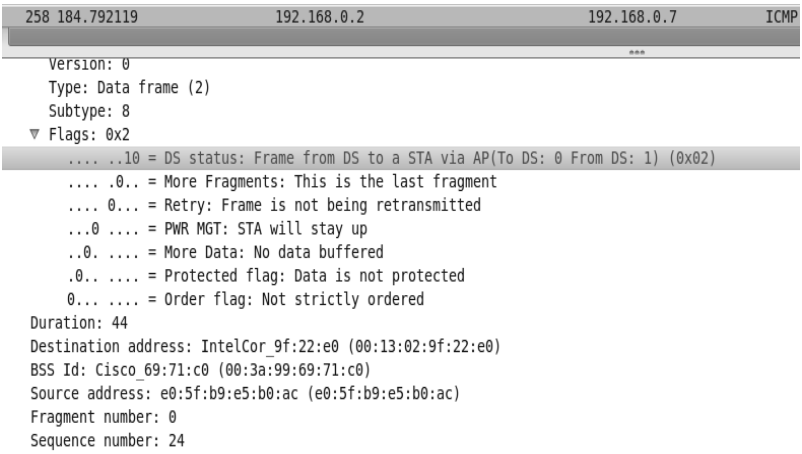


Figura 1.60 Flags de las tramas que indican el sentido de las mismas

1.3.4.4 Encapsulamiento de Capas Superiores

802.11, igual que Ethernet puede transportar cualquier protocolo de capas superiores. La diferencia principal reside en que 802.11 utiliza los servicios de LLC 802.2, a diferencia de Ethernet que usa el campo EtherType. Dos métodos están disponibles para el encapsulamiento, uno descripto por la RFC-1042 [RFC1042], que es usado por IPv4 e IPv6, y otro definido por el estándar 802.1H. Estos métodos son configurables y ambos derivan en el Sub-network Access Protocol (SNAP) de la IEEE. Este posee un encabezado con los valores de DSAP y SSAP, Destination/Source Service Access Point. El tipo de control derivado de los valores de HDLC es el de trama de información no numerada, 0x03 (Unnumbered Information -UI-). La diferencia entre los dos modos es que 802.1H utiliza el valor 00-00-F8 (Ether Tunnel) en el campo Organizationally Unique Identifier (OUI) y RFC-1042 lo configura a 0 (cero). En la figura 1.61 se muestra el encapsulamiento según RFC-1042.
A continuación se muestra como puede modificarse el encapsulamiento:

```
ap(config-if)#payload-encapsulation ?
  dot1h    use 802.1H as default
  rfc1042  use RFC1042 SNAP as default
```

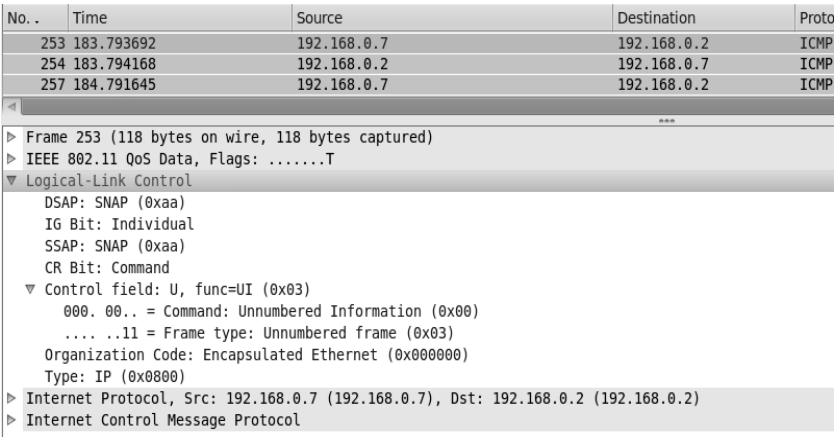


Figura 1.61 Trama con encapsulamiento según RFC-1042

1.3.4.5 Tramas de Datos: Tramas Null

Dentro de las tramas de datos vale mencionar que existe un tipo especial conocido como **Null Frame**. Una trama de estas es aquella que está vacía, es decir no tiene payload, solo encabezado (header) y cola (trailer). Estas tramas son usadas por estaciones móviles para avisar al AP que pasan a trabajar en un modo de ahorro de energía, **PS (Power-Save)**, para esto envían el bit **Power Management** en 1. De esta manera pueden dormir, o hibernar, esperando que el AP haga "buffering" de los mensajes destinados a la misma. Más adelante se explica el proceso de "buffering" y recuperación de mensajes en modo **Power Management**. En la figura 1.62 se muestra una captura de una trama de este tipo.

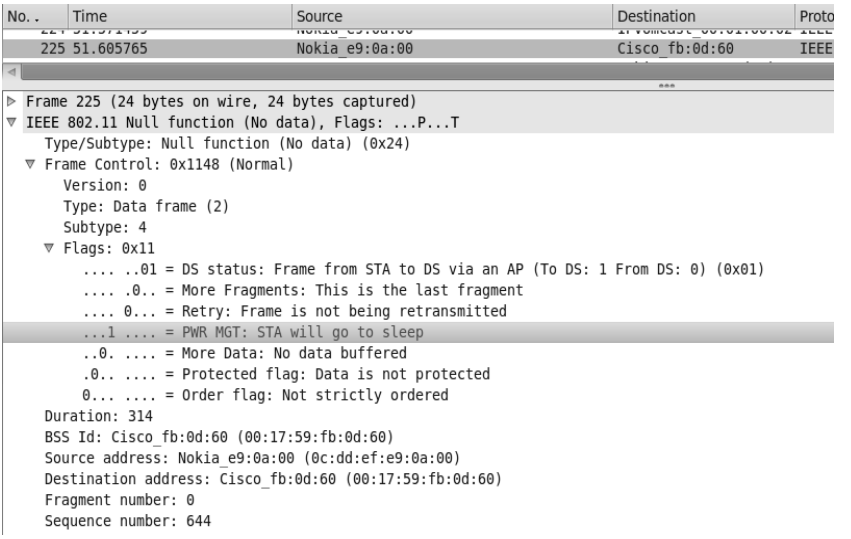


Figura 1.62 Trama Null indicando que el cliente pasa a “dormir”

1.3.4.6 Tramas de Datos: Fragmentación

Se puede configurar el umbral de fragmentación para verla funcionar.

```
aptest(config)#interface dot11Radio 0

aptest(config-if)#fragment-threshold ?
  <256-2346>

aptest(config-if)#fragment-threshold 500
```

Para ver la fragmentación de IEEE 802.11 sin que fragmente IP se envían tamaños menores que el MTU pero mayores al umbral de fragmentación. El archivo de captura utilizado es `infr-aptest-frag.pcap`. En la figura 1.63 se muestran el anteúltimo y el último fragmento.

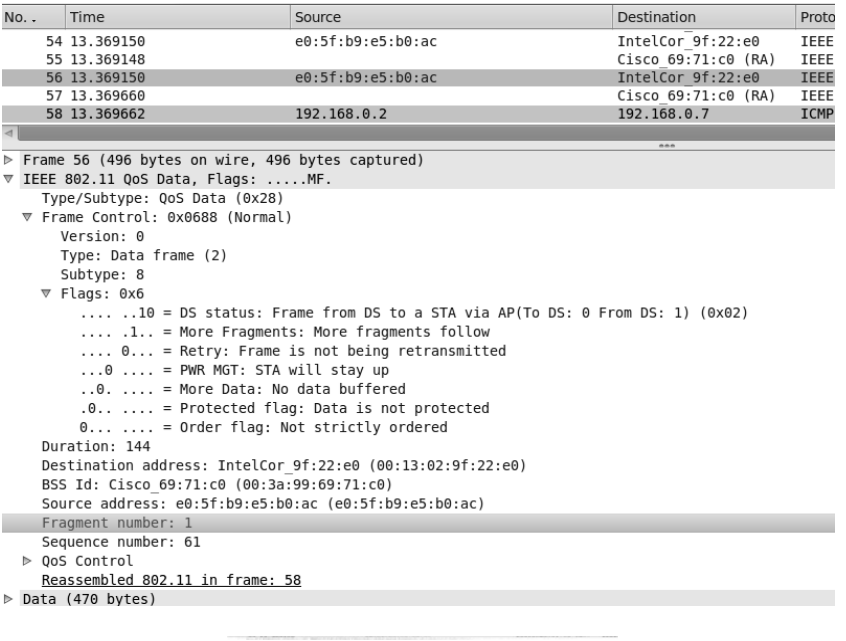


Figura 1.63 Tramas que muestran como funciona la fragmentación en 802.11

```
root@STA-A:~# ping -s 1000 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 1000(1028) bytes of data.
1008 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=1.46 ms
1008 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=1.44 ms
1008 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=1.46 ms
^C
--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.445/1.460/1.468/0.010 ms
```

1.3.4.7 Tramas de Control

Las tramas de control utilizadas por IEEE 802.11 son las siguientes:

- ACK (Acknowledgment).
- RTS (Request to Send).
- CTS (Clear to Send).
- PS-Poll (Power-Save Poll).

1.3.4.8 Tramas de Control: Acknowledge

Las tramas de confirmación son muy sencillas. Si se toma el archivo de captura incluyendo las tramas de control del mismo tráfico analizado con las tramas de datos ICMP (en la captura analizada anteriormente sólo se tomaron las tramas en determinado BSSID,

quedando afuera las tramas de control) se pueden observar las confirmaciones a nivel MAC para los mensajes ICMP.
(El archivo de captura utilizado es `infr-aptest-ctrl.pcap` en el cual se filtra todo lo relacionado con el BSSID=00:3a:99:69:71:c0 y se incluyen tramas de control).
El mensaje correspondiente con el número 257 en el nuevo archivo de captura es el 307. El mensaje de ACK para el mismo es el 308 que se muestra en la figura 1.64. En la misma se observa que tiene sólo 3 campos en el encabezado: Control Frame, "Duration" y dirección MAC de la estación destino. La duración es 0 (cero), lo que indica que es la última trama de la transmisión.

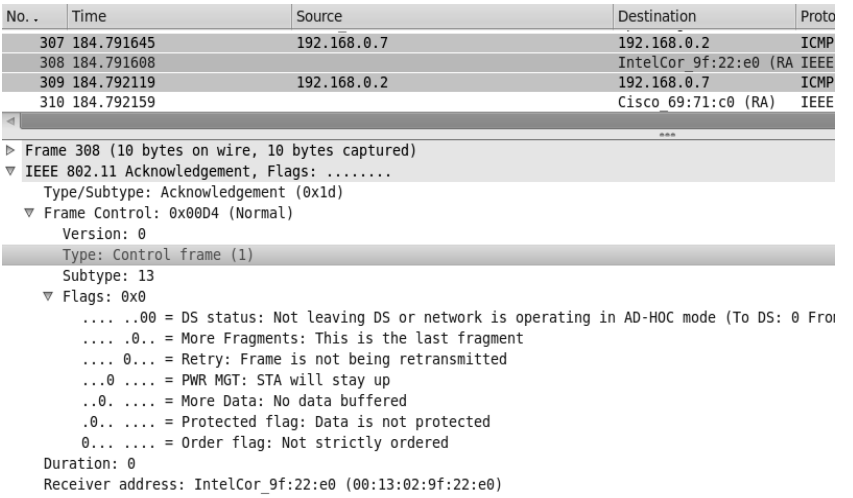


Figura 1.64 Trama MAC 802.11 de ACK

1.3.4.9 Tramas de Control: CTS/RTS

Las tramas de CTS pueden estar ligadas a un RTS o directamente ser enviadas a sí mismo, lo que se conoce como CTS-to-self. En la captura de ejemplo con tramas de control se pueden observar tramas CTS-to-self enviadas por el mismo AP. Esta trama se muestra en la figura 1.65.

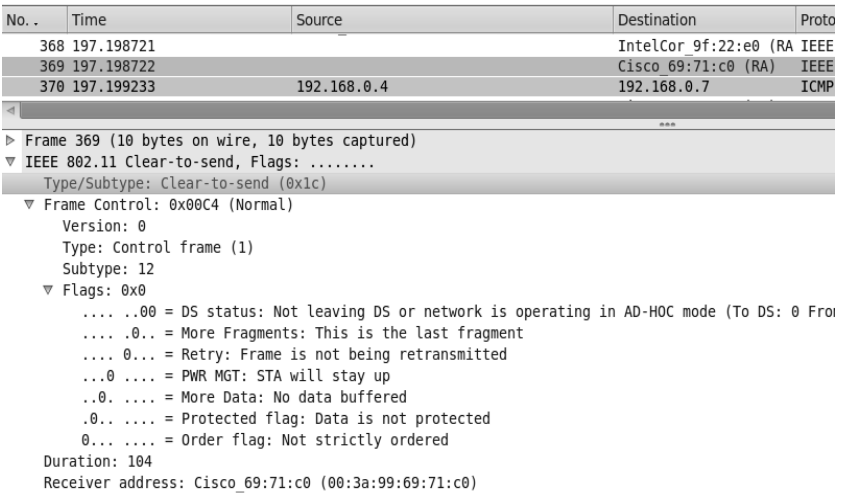


Figura 1.65 Trama MAC 802.11 de CTS-to-SELF

Para ver que se generan tramas RTS y CTS se puede configurar el **RTS threshold** a un valor más bajo del tamaño de las tramas que se generan y luego capturar el tráfico.

```
aptest(config)#interface dot11Radio 0
aptest(config-if)#rts threshold ?
  <0-2347>  threshold in bytes

aptest(config-if)#rts threshold 700
```

A continuación, se configura y asocia la estación.

```
root@STA-A:~# iwconfig wlan0 ap 00:3a:99:69:71:c0 essid aptest channel 2

root@STA-A:~# ifconfig wlan0 192.168.0.7 up

root@STA-A:~# iwconfig wlan0
wlan0     IEEE 802.11abg  ESSID:"aptest"
          Mode:Managed  Frequency:2.417 GHz  Access Point: 00:3A:99:69:71:C0
          Bit Rate=54 Mb/s   Tx-Power=15 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-24 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Por último, se envía un `ping` (ECHO request) de 1500 bytes superando los 700.

```
root@STA-A:~# ping 192.168.0.2
```

```
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=4.45 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=0.831 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=0.825 ms
^C
--- 192.168.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.825/2.035/4.451/1.708 ms
root@STA-A:~# ping 192.168.0.4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
^C
--- 192.168.0.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4032ms

root@STA-A:~# ping -s 1500 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 1500(1528) bytes of data.
1508 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=2.65 ms
1508 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=2.22 ms
1508 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=2.16 ms
1508 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=2.17 ms
1508 bytes from 192.168.0.2: icmp_seq=5 ttl=255 time=2.09 ms
1508 bytes from 192.168.0.2: icmp_seq=6 ttl=255 time=2.13 ms
^C
--- 192.168.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 2.094/2.239/2.654/0.197 ms
```

En la captura obtenida a partir del archivo: `infr-aptest-rts-cts.pcap`, el AP antes de enviar el primer fragmento de la respuesta al ICMP envía un RTS indicando que el destino es la estación "A" (DA = 00:12:02:9f:22:e0) y el origen el mismo AP (TA = 00:3a:99:69:71:c0). En este caso, el CTS se lo envía el mismo AP. Se debe tener en cuenta que en este ejemplo los fragmentos no son de nivel MAC, sino a nivel IP. La figura 1.66 muestra la captura del mensaje RTS que envía el AP.

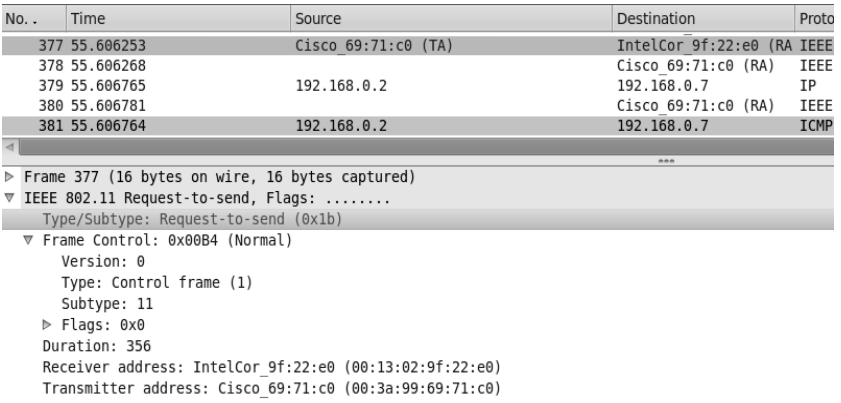


Figura 1.66 Trama MAC 802.11 de RTS

De la misma forma que se usa el RTS desde el AP se puede hacer desde la estación.

```
root@STA-A:~# iwconfig wlan0 rts 700

root@STA-A:~# iwconfig wlan0
wlan0     IEEE 802.11abg  ESSID:"aptest"
          Mode:Managed  Frequency:2.417 GHz  Access Point: 00:3A:99:69:71:C0
          Bit Rate=1 Mb/s   Tx-Power=15 dBm
          Retry  long limit:7   RTS thr=700 B   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-27 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
...

root@STA-A:~# ping -s 1500 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 1500(1528) bytes of data.
1508 bytes from 192.168.0.2: icmp_seq=1 ttl=255 time=2.17 ms
1508 bytes from 192.168.0.2: icmp_seq=2 ttl=255 time=2.21 ms
1508 bytes from 192.168.0.2: icmp_seq=3 ttl=255 time=2.25 ms
1508 bytes from 192.168.0.2: icmp_seq=4 ttl=255 time=2.75 ms
1508 bytes from 192.168.0.2: icmp_seq=5 ttl=255 time=2.23 ms
1508 bytes from 192.168.0.2: icmp_seq=6 ttl=255 time=2.28 ms
^C
--- 192.168.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 2.170/2.317/2.753/0.201 ms
```

1.3.4.10 Tramas de Control: Administración de Energía

A través de las tramas de datos **Null** una estación avisa al AP que va a entrar en modo de ahorro de energía, por lo tanto, le solicita al AP que

almacene temporalmente los datos destinados al equipo. Cuando la estación "despierta", dejando el modo de ahorro de energía, transmite tramas de Control **PS-Poll** queriendo descargar los mensajes "buffereados" por el AP. Para distinguirse estas tramas tienen los bits 14 y 15 configurados a 1 (uno) y, en el lugar que ocupa el campo "Duration", contiene el AID (Association ID) que obtuvo del AP al momento que se asoció. El AP para cada ID mantendrá un buffer para tramas unicast, para broadcast/multicast utiliza el buffer en el ID común 0. Para que los buffers no se sobrecarguen, los AP envían en las tramas Beacon un valor llamado TIM (Traffic Indication Map). Este valor funciona como un bitmap o vector de 2008 bits donde las estaciones están marcadas en la posición de su ID si tienen tráfico en los buffers del AP. El TIM está presente en todos los Beacons. Las estaciones deben despertarse a escuchar estos mensajes y, si encuentran que tienen tráfico almacenado, deben consultarlo mediante las tramas **PS-Poll. A**nte estos mensajes, el AP envía de a una las tramas y va indicando con el bit **More Data** si tiene más datos. El receptor debe confirmar cada trama enviada.

Para las tramas broadcast/multicast existe un período más grande llamado **DTIM period** (Delivery Traffic Indication Map). En estos períodos se envían mensajes **DTIM Beacons** y luego los mensajes en los buffers destinados a direcciones broadcast/multicast. Los mensajes enviados en períodos DTIM postergan los requeridos por **PS-Poll**.

En modo ad-hoc, IBSS, existe un mecanismo similar en el cual las estaciones pueden almacenar mensajes para otras. En este caso, cada determinado tiempo envían mensajes **ATIM (Announcement Traffic Indication Messages)** para comunicar a las estaciones que están en modo de ahorro de energía tienen datos almacenados. Todas las estaciones en un IBSS deben escuchar los ATIM a intervalos regulares.

Las estaciones para poder coordinar la escucha de los mensajes TIM deben estar sincronizadas. Para las tecnologías 802.11 los mensajes Beacon son utilizados para este propósito. En estos los AP envían una marca de tiempo (timestamp) llamado TSF (Timing Synchronization Function). En la figura 1.67 se muestra una trama de Beacon que lleva el timestamp (estampilla de tiempo) y el intervalo cada cuanto se envían.

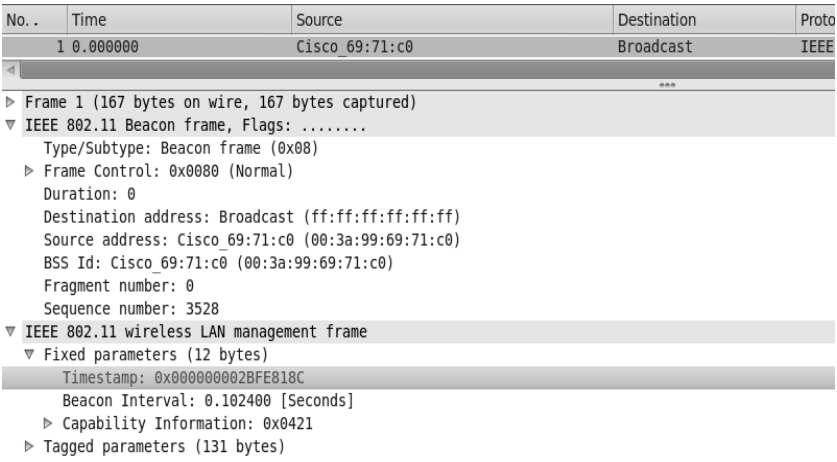


Figura 1.67 Trama MAC 802.11 de Beacon con timestamp

El tiempo DTIM es configurable en cada AP de la misma forma que sucede con en tiempo de Beacon.

```
aptest(config-if)#beacon ?
  dtim-period  dtim period
  period       beacon period
  ...
```

1.3.4.11 Tramas de Administración

Dentro de las tramas de administración (management) utilizadas por IEEE 802.11 se pueden destacar las siguientes:

- Asociación (Association Request).
- Respuesta de Asociación (Association Response).
- Tramas de Des-asociación (Disassociate).
- Tramas de Re-asociación (Reassociation Request y Reassociation Response).
- Tramas de Sondeo (Probe Request).
- Respuesta al Sondeo (Probe response).
- Tramas Baliza/Guía (Beacon).
- Tramas de Autenticación (Authentication y Deauthentication).

En una red de infraestructura, BSS, se debe cumplir cierto protocolo para poder utilizar sus servicios. Antes de poder enviar o recibir información hay que unirse a la red, y, previo a esto, se la debe encontrar. Esto último se lo puede hacer de dos formas.

1.3.4.12 Tramas de Administración Probes:

Probes y Beacons Sensado/Escaneo Pasivo (Passive Scanning)
De esta forma la estación que quiere unirse a una red WLAN va "saltando" de canal en canal tratando de escuchar los mensajes Beacon que envían los AP. En cada Beacon hay información sobre las características de la red (BSS). Este método no requiere que la estación envíe nada, simplemente escucha los mensajes que se envían a la dirección broadcast. Los AP pueden configurarse para que envíen los Beacon cada determinado intervalo de tiempo, o incluso que lo oculten (no envían estos mensajes). En los mensajes Beacon se propaga a toda la celda el nombre de la WLAN (SSID), la MAC del AP (BSSID), tasas de transferencia y otros parámetros. Cuando los AP envían estos mensajes se lo considera al BSS como un **Guest BSS**, ya que los clientes no necesitan saber de forma previa los parámetros. Cuando se configura que se "esconda" el SSID, **hide SSID** o **non-broadcast SSID,** el AP no envía estos mensajes, aunque pueden ser escuchados a partir de otras comunicaciones. Habitualmente se sugiere, como procedimiento de seguridad, esconder el SSID, pero esto no es una técnica que brinde demasiada seguridad en la red.
En la figura 1.68, tomada del archivo de captura `infr-aptest-mgmt.pcap`, se muestra el Beacon que manda el AP de la red. En la misma se puede apreciar que las direcciones MAC usadas son las del AP y como destino se utiliza la de broadcast: FF:FF:FF:FF:FF:FF. En el mismo mensaje se propaga el SSID "aptest", el canal sobre el cual se trabaja, canal 2, el rango de canales posibles de acuerdo a la configuración del país, los valores para trabajar con ERP y las tasas de transferencias soportadas entre otros datos. Con respeto al ERP (Extended Rate PHY), en la sección **PLCP para HR-DSSS/OFDM en 802.11g** se explicó cómo funciona el mecanismo de protección. En este caso se observa en la figura que aún no es necesario activarlo: **ERP: do not use protection**.

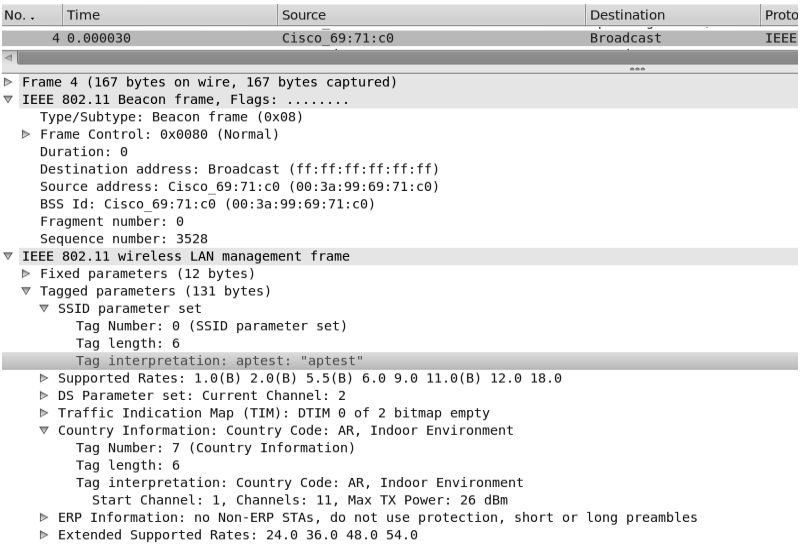


Figure 1.68 Trama MAC 802.11 de Beacon con SSID

El intervalo al cual son enviados los mensajes Beacon es configurable en cada AP.

```
aptest(config-if)#beacon period ?
  <20-4000>  Kusec (or msec)
```

Sensado/Escaneo Activo (Active Scanning)

De esta otra forma las estaciones a medida que van barriendo los canales pueden ir enviando mensajes para descubrir las redes (BSS) que están disponibles. Este mecanismo exige que antes de enviar se sigan las reglas de acceso al medio de DCF vistas previamente. Una vez que logra ganar el acceso al medio, la estación enviará un mensaje de **Probe Request** en el cual no se indica un SSID particular, sino un SSID broadcast. Luego esperará un tiempo **MinChannelTime** por un **Probe Response**, si no obtiene respuesta supone que no hay una WLAN activa a la que se pueda asociar y salta al próximo canal. Los AP que tienen configurado non-broadcast SSID, no responden a estos mensajes, si deberían responder a mensajes Probe Request específicos de su SSID. En las figuras 1.69 se puede observar un Probe Request, este va dirigido a la dirección de broadcast, en cambio en la figura siguiente se ve el Probe Response el cual va como respuesta unicast. En la figura 1.70 se muestra una Probe Request que lleva el SSID específico.

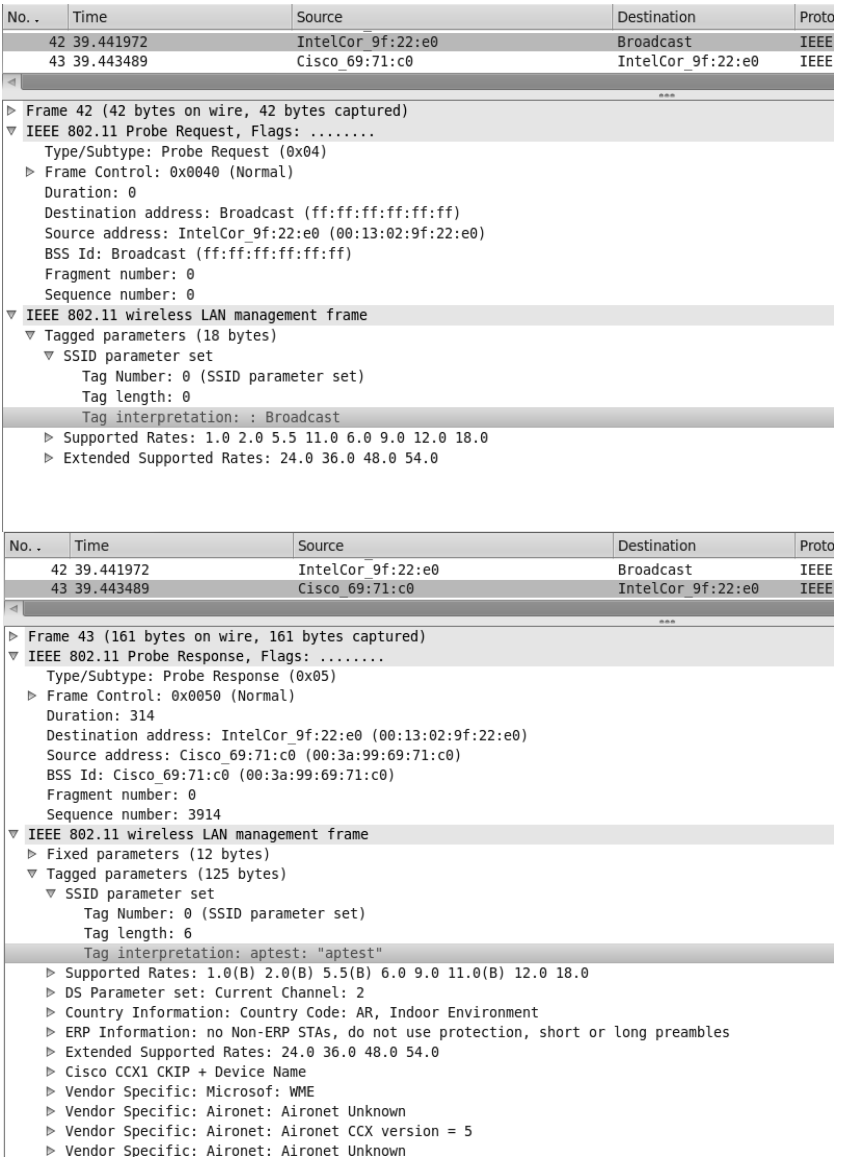


Figura 1.69 Tramas MAC 802.11 de Probe Request y Probe Response

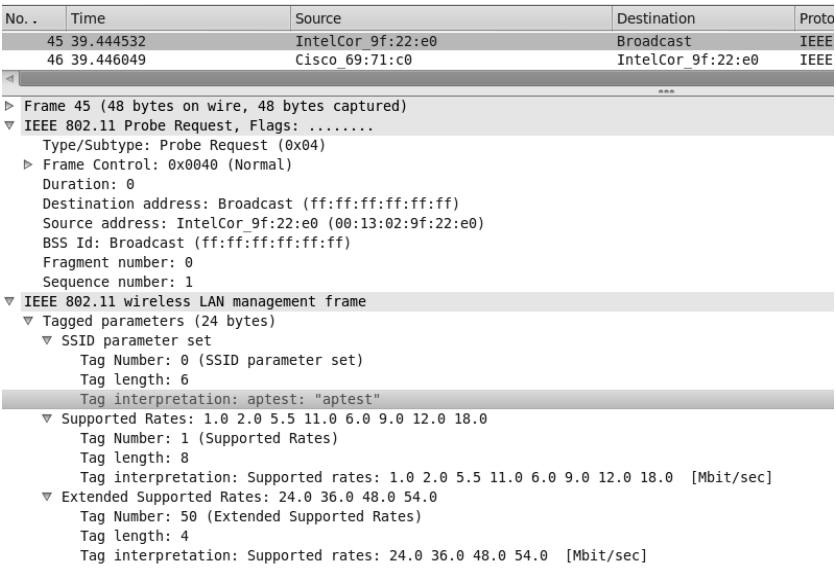


Figura 1.70 Trama MAC 802.11 de Probe Request a un SSID específico

1.3.4.13 Tramas de Administración: Autenticación

Una vez descubierta la red la estación debe unirse a ella. Para unirse primero debe autenticarse y luego asociarse. Los detalles de la autenticación se verán en el capítulo **Seguridad en 802.11**. El documento del estándar original 802.11 define dos tipos de autenticación:

- Abierta, **Open system** (sin autenticación).
- Clave compartida, **Shared Key**.

Para la autenticación abierta la estación y el AP intercambian mensajes indicando que van a utilizar este método. Los mensajes son 2 (dos), el requerimiento desde la estación hacia el AP y la respuesta desde el AP. En el mensaje de **Authentication Request** va codificado como ID del algoritmo el (0) cero que identifica open-system y el número de transacción en 1 (uno) indicando que es la primera trama de la secuencia. El AP debe responder con el mismo ID si acepta y con el número de transacción en 2 (dos). En la figura 1.71 se ven los mensajes. El que se detalla es el primero, Authentication Request, que es seguido por un **ACK** y luego por un **Authentication Response**.

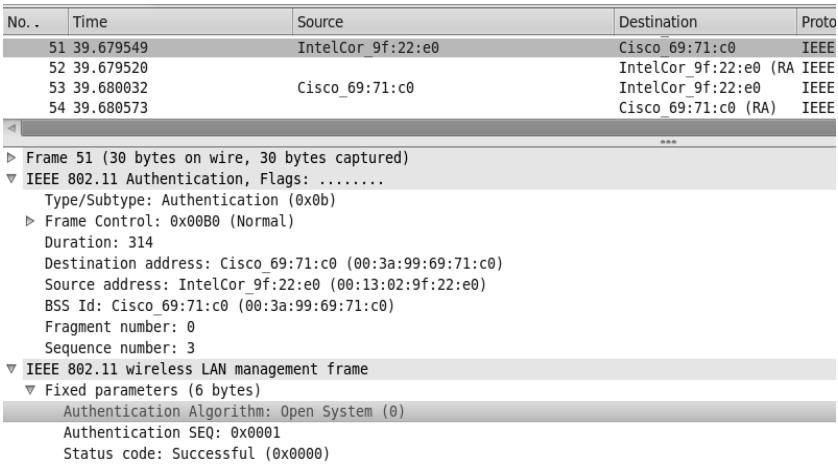


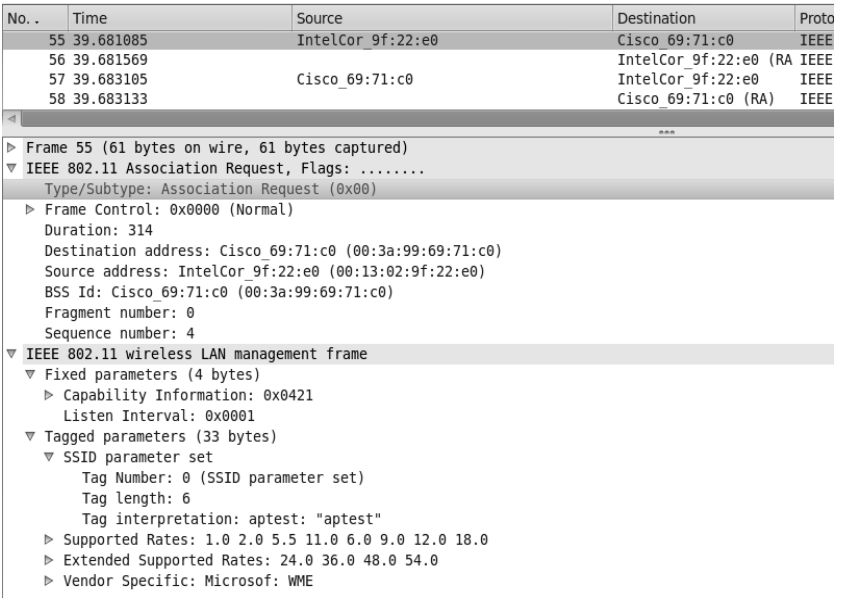
Figura 1.71 Trama MAC 802.11 de Autenticación

El método **Shared Key** utiliza una clave común que es cifrada usando el mecanismo de seguridad WEP (Wired Equivalent Privacy). Previo a autenticarse, una estación debe conocer la clave.
Luego, a partir del estándar IEEE 802.11i, se agregan métodos de seguridad de Pre-Shared Key y 802.1X a través de EAPoL, EAP (WPA, WPA2), RADIUS, etc. Técnicas previas al estándar 802.11i utilizaban el filtrado en base a direcciones MAC. Estas técnicas dan algo de seguridad pero no es muy recomendado ya que las direcciones MAC soportadas se pueden cambiar una vez cargadas por el sistema operativo y por lo tanto se pierde la unicidad de las mismas.

1.3.4.14 Tramas de Administración: Asociación

Una vez completada la autenticación la estación debe asociarse al BSS vía el AP. La asociación le permite al AP llevar la contabilidad de todas las estaciones que están en el BSS o ESS. La asociación es iniciada por la estación mediante el envío de un mensaje de **Association Request**. Si no está autenticado recibirá desde el AP un mensaje **Deauthentication**. El AP si concede la asociación debe responder con un **Association Response** con el código (0) cero (éxito) y el Association ID (AID) asignado a la estación. El AID es un identificador lógico usado para las estaciones móviles en el caso que el AP debe hacer "buffering" como se explicó en el proceso de PS-Poll. Este ID vale en el rango de 1 a 2007. Podría suceder que el AP no acepte la asociación, en ese caso el **Association Response** debe llevar un código de Error.

Existen mensajes de Des-asociación y Re-asociación usados cuando una estación se mueve desde un AP a otro. Para esto último se utiliza el estándar IEEE 802.11f IAPP (Inter-Access Point Protocol). Este protocolo permite que los APs de un ESS dialoguen y autentiquen contra una entidad centralizada como por ejemplo un servidor RADIUS. En el caso de una Re-asociación, la estación debe enviar un mensaje de asociación al nuevo AP, pero indicando la dirección MAC del AP al cual estaba asociada. El nuevo AP debe comunicarse vía IAPP con el viejo para verificar que la asociación existe. Para este proceso hay disponibles varias extensiones propietarias. Si se comprueba que no está previamente asociado envía un mensaje de Deauthentication. Una estación sólo puede estar asociada a un AP al mismo tiempo.
En las figuras 1.72 se muestra el requerimiento para la asociación y, a continuación, la respuesta exitosa con la asignación del ID=1.



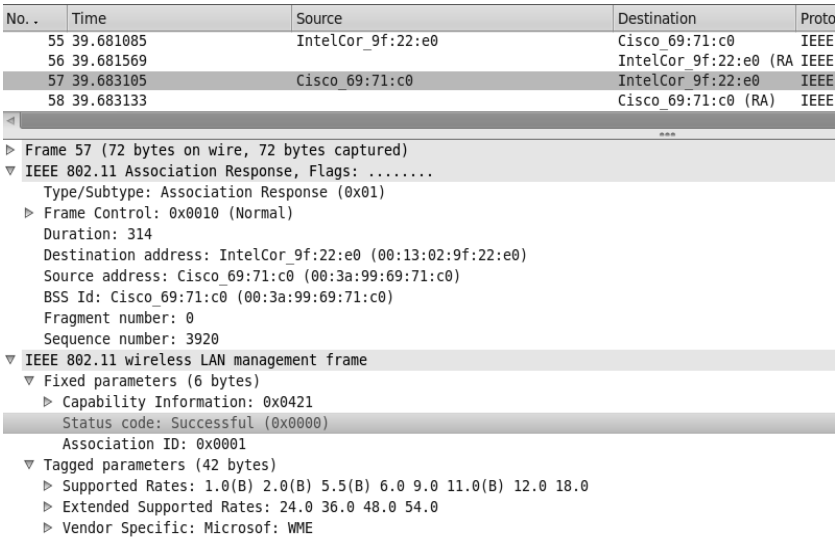


Figura 1.72 Tramas MAC 802.11 de Asociación

En la figura 1.73 se muestra la secuencia completa para lograr la asociación. La cantidad máxima de estaciones es 2007 (Max AID), aunque en la práctica para que el sistema funcione son muchas menos. Este valor se puede cambiar en la configuración, por ejemplo:

```
    /interface wireless
set wlan1  max-station-count=20
```

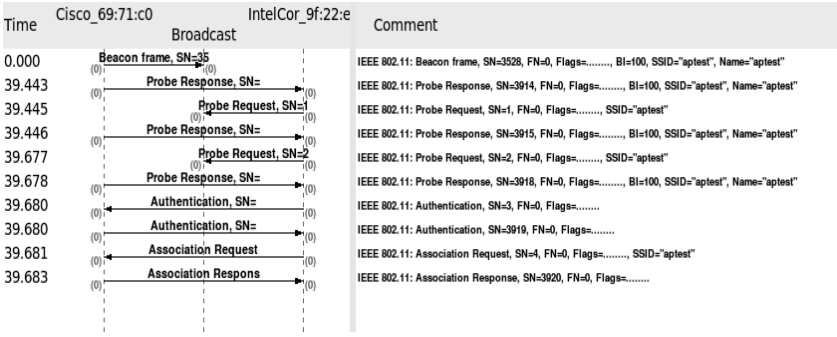


Figura 1.73 Diagrama del proceso de asociación

1.3.5 Capa MAC en 802.11n

A nivel MAC, 802.11n realiza varios agregados. Uno es la agrupación o agregación de tramas. **Frame Aggregation** se logra agrupando varios payloads de tramas en una más grande. Todas las tramas agrupadas deben ir dirigidas al mismo destino, permitiendo empaquetar varios MSDUs (contenido de 802.11) o MPDUs (tramas de 802.11n) en una misma trama MAC. La agregación se realiza en dos niveles:

- Agregación de MAC Service Data Units (MSDUs) sobre el nivel MAC: A-MSDU.
- Agregación de MAC Protocol Data Units (MPDUs) debajo del nivel MAC: A-MPDU.

De esta forma se permite bajar el "overhead" y el número de colisiones potenciales. El tamaño de trama máximo es llevado de 4KB a 64KB. Para MSDUs se cambia de 2K(2304) a 8K(7965B). Para que esta técnica funcione se requiere que las tramas sean demoradas hasta agruparlas, se logra mayor rendimiento, a costa de agregar un mayor retardo. Algunas tramas, por ejemplo, aquellas provenientes de aplicaciones de tiempo real, no deben retenerse. El dispositivo agrupador deberá comparar los campos de QoS para determinar cómo agrupar. La técnica de agrupar mediante A-MSDU es más eficiente (menos "overhead" Ethernet que 802.11).

- A-MSDU agrupa tramas Ethernet, y genera un **Jumboframe** 802.11. La seguridad se agrega a la trama agrupada.
- A-MPDU agrupa tramas Ethernet, pasa cada una a 802.11 y luego las agrupa, sin volverlas a encapsular en otra 802.11. Agrega PLCP. La seguridad se agrega a cada trama 802.11.

Como técnica asociada a la agrupación de tramas se provee en 802.11n las confirmaciones en bloques: **Block Acknowledge (BlockACK)**.

- 64KB limitado por 16-bit HT Length en HT-SIG.
  En 802.11 se requiere que cada trama unicast sea confirmada atómicamente, un ACK por cada trama. A partir de 802.11e, con la calidad de servicio, se agrega el concepto de **BlockACKs** que es un vector de bits indicando ACKs. Cuando se agrupa mediante A-MPDU se requiere BlockACKs, y son utilizados en 802.11n. Con los BlockACKs sobre 802.11e se requería previamente enviar mensajes **Block Ack Request (BlockAckReq)**. En 802.11n no se necesitan, está implícito si recibe un A-MPDU, aunque podrían utilizarse. Si se agrupa mediante A-MSDU se confirma con un solo ACK todo.

Otra mejora a nivel MAC de 802.11n es sobre la fragmentación.

1.3.6 Ejemplos de Modos de Trabajo

1.3.6.1 Ejemplo de Modo Ad-Hoc IBSS

En el siguiente ejemplo se muestra una configuración de una red ad-hoc con su correspondiente captura de tráfico. La figura 1.74 muestra la disposición de la red IBSS.

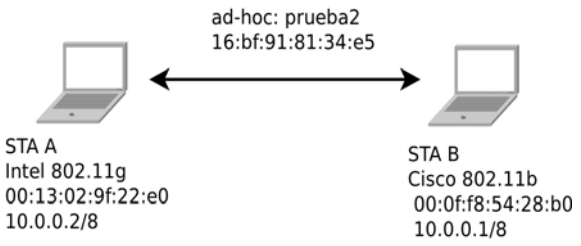


Figura 1.74 Disposición del laboratorio para las pruebas en modo ad-hoc

Para el ejemplo primero se configura una estación:

```
root@STA-A:~# ifconfig wlan0 down

root@STA-A:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:13:02:9f:22:e0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4050 (4.0 KB)  TX bytes:11337 (11.3 KB)

root@STA-A:~# iwconfig wlan0
wlan0     IEEE 802.11abg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=15 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

root@STA-A:~# iwconfig wlan0 mode ad-hoc

root@STA-A:~# iwconfig wlan0 channel 2

root@STA-A:~# iwconfig wlan0 essid prueba2

root@STA-A:~# ifconfig wlan0 10.0.0.2 up

root@STA-A:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:13:02:9f:22:e0
          inet addr:10.0.0.2  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::213:2ff:fe9f:22e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4050 (4.0 KB)  TX bytes:15175 (15.1 KB)

root@STA-A:~# iwconfig wlan0
wlan0     IEEE 802.11abg  ESSID:"prueba2"
          Mode:Ad-Hoc  Frequency:2.417 GHz  Cell: Not-Associated
          Tx-Power=15 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Luego se configura la otra estación:

```
root@STA-B:~# ifconfig eth4 down

root@STA-B:~# ifconfig eth4
eth4      Link encap:Ethernet  direcciónHW 00:0f:f8:54:28:b0
          DIFUSIÓN MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:0 errores:18 perdidos:0 overruns:0 frame:18
          Paquetes TX:10 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:0 (0.0 B)  TX bytes:1716 (1.7 KB)
          Interrupción:3 Dirección base: 0x3100

root@STA-B:~# iwconfig eth4 mode ad-hoc

root@STA-B:~#  iwconfig wlan0 channel 2

root@STA-B:~# iwconfig eth4 essid prueba2

root@STA-B:~# ifconfig eth4 10.0.0.1 up

root@STA-B:~# ifconfig eth4
eth4      Link encap:Ethernet  direcciónHW 00:0f:f8:54:28:b0
          Direc. inet:10.0.0.1  Difus.:10.255.255.255  Másc:255.0.0.0
          Dirección inet6: fe80::20f:f8ff:fe54:28b0/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:0 errores:18 perdidos:0 overruns:0 frame:18
          Paquetes TX:28 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:0 (0.0 B)  TX bytes:4431 (4.4 KB)
          Interrupción:3 Dirección base: 0x3100

root@STA-B:~# iwconfig eth4
eth4      IEEE 802.11-DS  ESSID:"prueba2"
          Mode:Ad-Hoc  Channel:0  Cell: 16:BF:91:81:34:E5
          Bit Rate:11 Mb/s   Tx-Power=20 dBm   Sensitivity=0/65535
          Retry limit:16   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=100/100  Signal level=-20 dBm  Noise level=-90 dBm
          Rx invalid nwid:11  Rx invalid crypt:0  Rx invalid frag:0
```

```
          Tx excessive retries:0  Invalid misc:3176   Missed beacon:0
```

La dirección MAC que se genera como BSSID es a partir de un valor aleatorio. El bit individual/group se coloca en 0 (individual) y el bit universal/local se coloca en 1 (local). Luego, se realizan las pruebas desde una estación:

```
root@STA-B:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.036 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.029/0.033/0.036/0.005 ms

root@STA-B:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=4.94 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=3.03 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.61 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=1.64 ms
```

Por último, se da de baja el enlace.

```
root@STA-B:~# ifconfig eth4 down

root@STA-A:~# ifconfig wlan0 down
```

En las figuras 1.75 se muestran los Beacons generados para redes ad-hoc y un mensaje ICMP. El archivo de captura utilizado es `ad-hoc-prueba2.pcap`.

Figura 1.75 Tramas MAC 802.11, Beacon y de datos, en modo ad-hoc

1.3.6.2 Ejemplo de Modo Repetidor

En el gráfico 1.76 se muestra un diagrama de la disposición de los equipos.

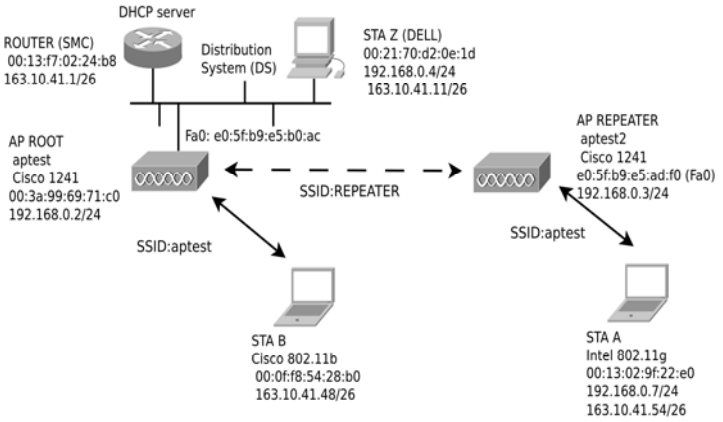


Figura 1.76 Disposición del laboratorio para las pruebas en modo repetidor

Configuración del AP repetidor (Repeater):

```
aptest2#show running-config
...
hostname aptest2
!
dot11 ssid REPEATER
   authentication open
   infrastructure-ssid
!
dot11 ssid aptest
   authentication open
   guest-mode
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid REPEATER
 !
 ssid aptest
 !
 antenna gain 5 !!! Antena Omni de 5.2dBi
 parent 1 003a.9969.71c0 !!! MAC del AP ROOT
 station-role repeater !!! Modo Repetidor
 world-mode dot11d country-code AR both
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
```

```
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 192.168.0.3 255.255.255.0
 no ip route-cache
!
end
```

El comando `infrastructure-ssid` indica que SSID debe ser utilizado para que otros AP se conecten usando bridges y repetidores. Si no se configura, cualquiera podría ser utilizado. Al AP `aptest` se le agrega el SSID de infraestructura y queda como raíz (Root):

```
aptest#show running-config
...
!
hostname aptest
!
dot11 ssid REPEATER
   authentication open
   infrastructure-ssid
interface Dot11Radio0
 !
 ssid REPEATER
 !
end
```

Luego se puede ver la asociación entre los equipos y las estaciones:

```
aptest#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [REPEATER] :

MAC Address    IP address      Device        Name     Parent         State
0013.029f.22e0 163.10.41.54    Rptr-client   -        e05f.b9e5.adf0 Assoc
e05f.b9e5.adf0 192.168.0.3     ap1240-Rptr   aptest2  self           Assoc

SSID [aptest] :

MAC Address    IP address      Device        Name     Parent        State
000f.f854.28b0 163.10.41.48    350-client    -        self          Assoc

aptest2#show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:

SSID [REPEATER] :

MAC Address    IP address      Device        Name     Parent         State
003a.9969.71c0 192.168.0.2     ap1240-Parent aptest   -              Assoc

SSID [aptest] :

MAC Address    IP address      Device        Name     Parent         State
0013.029f.22e0 163.10.41.54    unknown       -        self           Assoc
```

En este ejemplo, en lugar de utilizar direcciones IP asignadas manualmente, se usa el servicio de DHCP del DS (Distribution System). Luego, se lanza el ICMP para probar la red y capturar tráfico.

```
root@STA-B:~# ping 163.10.41.54
PING 163.10.41.54 (163.10.41.54) 56(84) bytes of data.
64 bytes from 163.10.41.54: icmp_seq=1 ttl=64 time=12.0 ms
...
64 bytes from 163.10.41.54: icmp_seq=8 ttl=64 time=5.58 ms
64 bytes from 163.10.41.54: icmp_seq=9 ttl=64 time=3.47 ms
64 bytes from 163.10.41.54: icmp_seq=10 ttl=64 time=3.48 ms
^C
--- 163.10.41.54 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 3.452/4.815/12.010/2.491 ms
```

En las figuras 1.77 se muestra la secuencia de mensajes para que el ICMP Echo Request llegue desde un AP a otro. Se puede observar claramente cómo van cambiando las direcciones MAC, sólo el mensaje que va desde un AP hacia otro lleva cuatro direcciones MAC, los otros dos deben llevan las tres necesarias para trabajar en modo infraestructura.

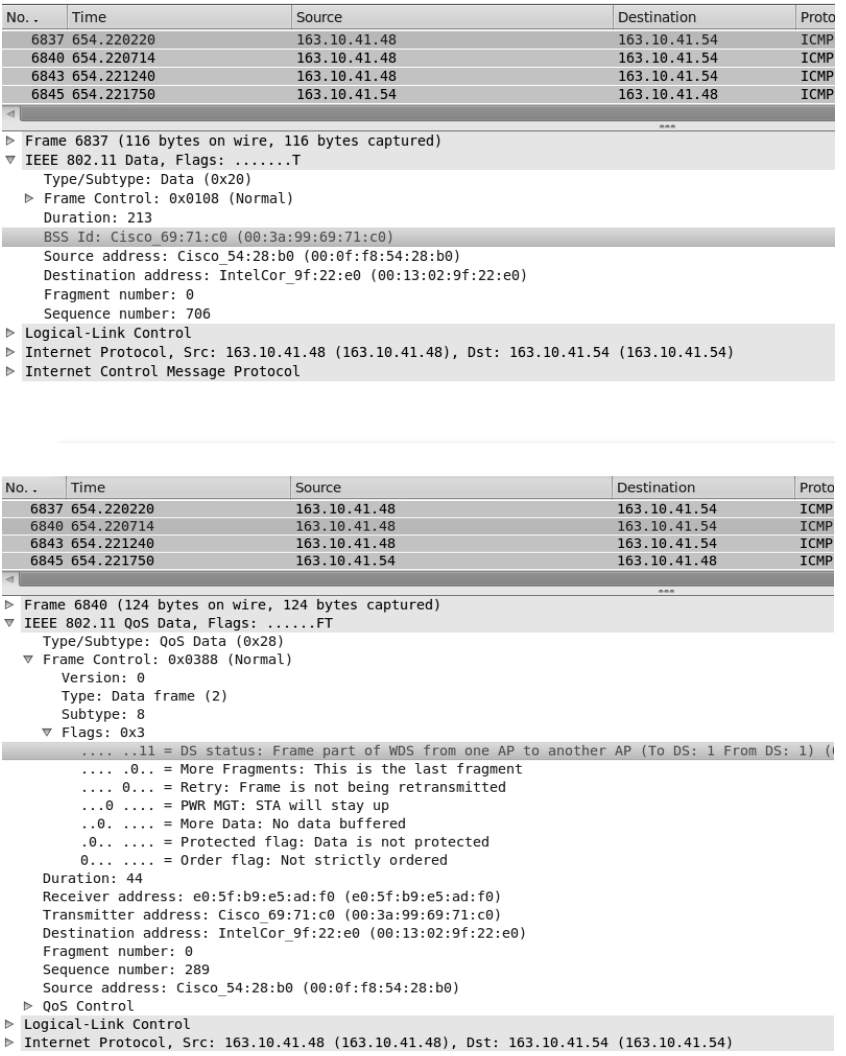


Figura 1.77 Tramas MAC 802.11 en modo repetidor

1.3.6.3 Ejemplo de enlaces Punto a Punto

Los ejemplos a continuación se realizan sobre equipos Mikrotik Routerboards corriendo RouterOS. Los equipos tienen conectadas placas mini-PCI que trabajan con 802.11a. La distribución física, y como se los conecta, se muestra en la figura 1.78.

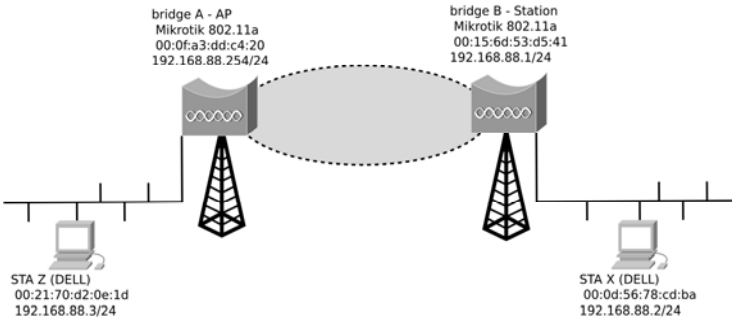


Figura 1.78 Disposición del laboratorio para las pruebas en modo bridge

Esta combinación de hardware y software es muy versátil, permitiendo trabajar como router o como bridge. A nivel wireless, los equipos permiten ser configurados en diversos modos como **AP-bridge**, **Bridge**, **Station**, etc. Para configurar un enlace **Punto-a-Punto** existen varias alternativas. Una es colocar cada equipo en modo **Bridge** wireless. Los equipos Mikrotik en modo **Bridge** a nivel wireless permiten la conexión de un cliente únicamente, por lo tanto, sólo se asociarán mutuamente. De forma adicional al modo se debe configurar a ambos para que trabajen con **WDS**. En este caso, el WDS se configura de forma dinámica, es decir, automáticamente se descubren por el mismo SSID y se asocian. Otra cuestión importante es crear una interfaz de bridge que abarque la LAN inalámbrica y la Ethernet. En los ejemplos para capturar el tráfico analizado se uso el siguiente comando.

```
root@STA-Z:~# airodump-ng -b a --channel 36 wlan0 -w mktk-802.11a-raw
```

Configuración en modo Bridge (Lado llamado AP):

Primero se configura uno de los equipos bridge (llamado AP). Antes de proceder con la configuración se muestra la salida de las interfaces que posee.

```
[admin@MikroTik] > /system identity set name=AP-MikroTik

[admin@AP-MikroTik] > /interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME       MTU   MAC-ADDRESS       ARP        MASTER-PORT      SWITCH
 0 R  ether1     1500  00:0C:42:27:18:CD enabled

[admin@AP-MikroTik] > /interface wireless print
Flags: X - disabled, R - running
 0  R name="wlan1" mtu=1500 mac-address=00:0F:A3:DD:C4:20 arp=enabled
 interface-type=Atheros AR5213 ...
```

Luego se configura la interfaz inalámbrica de acuerdo a lo indicado.

```
[admin@AP-MikroTik] >
/interface wireless
set wlan1 mode=bridge wds-mode=dynamic band=5ghz frequency=5180 \
    security-profile=default wds-default-bridge=bridge1 ssid=TEST
```

La configuración completa de todos los parámetros se muestra a continuación.

```
[admin@AP-MikroTik] > /interface wireless export
/interface wireless
set wlan1 ack-timeout=dynamic adaptive-noise-immunity=none allow-sharedkey=no \
    antenna-gain=0 antenna-mode=ant-a area="" arp=enabled band=5ghz \
    basic-rates-a/g=6Mbps basic-rates-b=1Mbps burst-time=disabled comment="" \
    compression=no country=no_country_set default-ap-tx-limit=0 \
    default-authentication=yes default-client-tx-limit=0 default-forwarding=\
    yes dfs-mode=none disable-running-check=no disabled=no \
    disconnect-timeout=3s frame-lifetime=0 frequency=5180 frequency-mode=\
    manual-txpower hide-ssid=no hw-retries=4 mac-address=00:0F:A3:DD:C4:20 \
    max-station-count=2007 mode=bridge mtu=1500 name=wlan1 \
    noise-floor-threshold=default on-fail-retry-time=100ms \
    periodic-calibration=default periodic-calibration-interval=60 \
    preamble-mode=both proprietary-extensions=post-2.9.25 radio-name=\
    000FA3DDC420 rate-set=default scan-list=default security-profile=default \
    ssid=TEST station-bridge-clone-mac=00:00:00:00:00:00 \
    supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,54Mbps \
    supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps tx-power-mode=default \
    update-stats-interval=disabled wds-cost-range=50-150 wds-default-bridge=\
    bridge1 wds-default-cost=100 wds-ignore-ssid=no wds-mode=dynamic \
    wmm-support=disabled
```

Se debe construir un bridge entre la interfaz Ethernet y la wireless. Se asigna una dirección IP a la interfaz Ethernet, que es accesible desde cualquiera de los segmentos físicos pertenecientes al mismo bridge (en otra configuración podría asignarse directamente al bridge).

```
[admin@AP-MikroTik] >
/interface bridge port
add bridge=bridge1 comment="" disabled=no edge=auto external-fdb=auto \
    horizon=none interface=wlan1 path-cost=10 point-to-point=auto priority=\
    0x80
add bridge=bridge1 comment="" disabled=no edge=auto external-fdb=auto \
    horizon=none interface=ether1 path-cost=10 point-to-point=auto priority=\
    0x80

/interface bridge
add admin-mac=00:00:00:00:00:00 ageing-time=5m arp=enabled auto-mac=yes \
    comment="" disabled=no forward-delay=15s max-message-age=20s mtu=1500 \
    name=bridge1 priority=0x8000 protocol-mode=none transmit-hold-count=6

/ip address
```

```
add address=192.168.88.254/24 broadcast=192.168.88.255 comment=\
    "default configuration" disabled=no interface=ether1 network=192.168.88.0
```

Al final se muestra el estado de la interfaz y se ve que el otro extremo aún no está registrado ya que no se ha configurado aún.

```
[admin@AP-MikroTik] > /interface wireless print
mode=ap-bridge ssid="TEST" frequency=5180
      band=5ghz scan-list=default antenna-mode=ant-a wds-mode=dynamic
      wds-default-bridge=bridge1 wds-ignore-ssid=no
      default-authentication=yes default-forwarding=yes default-ap-tx-limit=0
      default-client-tx-limit=0 hide-ssid=no security-profile=default
      compression=no

[admin@AP-MikroTik] > /interface wireless registration-table print
 # INTERFACE   RADIO-NAME       MAC-ADDRESS       AP  SIGNAL... TX-RATE UPTIME
```

Configuración en modo Bridge (lado llamado Station):

La configuración es idéntica, sólo cambia el nombre y la dirección IP que se le asigna.

```
[admin@MikroTik] > /system identity set name=Station-MikroTik

[admin@Station-MikroTik] >

/interface wireless
set wlan1 mode=bridge wds-mode=dynamic band=5ghz frequency=5180 \
    security-profile=default ssid=TEST

/ip address
add address=192.168.88.1/24 broadcast=192.168.88.255 comment=\
    "default configuration" disabled=no interface=ether1 network=192.168.88.0


/interface bridge port
...

/interface bridge
...
```

Una vez configurado se asocian los equipos.

```
[admin@Station-MikroTik] > /interface wireless registration-table print
 # INTERFACE   RADIO-NAME       MAC-ADDRESS       AP  SIGNAL... TX-RATE UPTIME
 0 wlan1       000FA3DDC420     00:0F:A3:DD:C4:20 yes -71dBm... 54Mbps  5s
```

Se pueden observar los interfaces WDS creadas de forma dinámica.

```
[admin@AP-MikroTik] > /interface wireless wds print
Flags: X - disabled, R - running, D - dynamic
 0  RD name="wds1" mtu=1500 mac-address=00:0F:A3:DD:C4:20 arp=enabled \
```

```
       master-interface=wlan1
       wds-address=00:15:6D:53:D5:41

[admin@Station-MikroTik] > /interface wireless wds print
Flags: X - disabled, R - running, D - dynamic
 0  RD name="wds1" mtu=1500 mac-address=00:15:6D:53:D5:41 arp=enabled \
       master-interface=wlan1
       wds-address=00:0F:A3:DD:C4:20
```

A continuación se generan mensajes ICMP para probar que todo funcione de forma adecuada y poder obtener el tráfico a analizar.

```
[admin@AP-MikroTik] > ping 192.168.88.1
192.168.88.1 64 byte ping: ttl=64 time=8 ms
192.168.88.1 64 byte ping: ttl=64 time=3 ms
192.168.88.1 64 byte ping: ttl=64 time=1 ms
192.168.88.1 64 byte ping: ttl=64 time=1 ms
...

[admin@Station-MikroTik] > ping 192.168.88.254
192.168.88.254 64 byte ping: ttl=64 time=5 ms
192.168.88.254 64 byte ping: ttl=64 time=7 ms
192.168.88.254 64 byte ping: ttl=64 time=7 ms
192.168.88.254 64 byte ping: ttl=64 time=6 ms
...

root@STA-Z:~# ping 192.168.88.2
PING 192.168.88.2 (192.168.88.2) 56(84) bytes of data.
64 bytes from 192.168.88.2: icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from 192.168.88.2: icmp_seq=2 ttl=64 time=0.049 ms
...
```

De la misma forma que se generan los WDS de forma dinámica se lo puede configurar manualmente, WDS estáticos. Para esto se debe colocar la dirección MAC del otro extremo en cada AP.

```
[admin@AP-MikroTik] >

/interface wireless wds add master-interface=wlan1 name=wds-station \
       wds-address=00:15:6D:53:D5:41

/interface wireless wds print
Flags: X - disabled, R - running, D - dynamic
 0  R  name="wds-station" mtu=1500 mac-address=00:0F:A3:DD:C4:20 arp=enabled
       master-interface=wlan1 wds-address=00:15:6D:53:D5:41

/interface wireless wds set wds-station disabled=no
/interface wireless set wlan1 wds-mode=static
```

El resultado final es el mismo que la configuración del WDS de forma dinámica.

Configuración de Modo Station:

Si se configura un equipo como **Station** (estación) y el otro como AP o Bridge (AP con un solo cliente), un equipo atrás del equipo con el rol de Station, no puede llegar de forma adecuada al resto de los equipos (al revés, de los que están atrás del AP, sí). Esto sucede al configurar el enlace como bridge transparente. El problema surge debido a que en este modo solo se tienen 3 direcciones MAC, la del equipo Station la del Bridge (BSSID) y restaría una que la usaría el equipo que consulta, en este caso falta la del equipo destino. Funcionaría si el equipo como Station en lugar de configurarse como birdge transparente se lo pusiera como router. En el ejemplo se configura un AP en modo **Bridge** y el otro en modo Station. El AP en modo Station tiene la dirección IP: 192.168.88.1, el otro la 192.168.88.254.

```
[admin@AP-MikroTik] > /interface wireless print
Flags: X - disabled, R - running
 0  R name="wlan1" mtu=1500 mac-address=00:0F:A3:DD:C4:20 arp=enabled
      interface-type=Atheros AR5213 mode=bridge ssid="TEST" frequency=5180
      band=5ghz scan-list=default antenna-mode=ant-a wds-mode=disabled
      wds-default-bridge=none wds-ignore-ssid=no default-authentication=yes
      default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0
      hide-ssid=no security-profile=default compression=no

[admin@Station-MikroTik] > /interface wireless print
Flags: X - disabled, R - running
 0  R name="wlan1" mtu=1500 mac-address=00:15:6D:53:D5:41 arp=enabled
      interface-type=Atheros AR5213 mode=station ssid="TEST" frequency=5180
      band=5ghz scan-list=default antenna-mode=ant-a wds-mode=disabled
      wds-default-bridge=none wds-ignore-ssid=no default-authentication=yes
      default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0
      hide-ssid=no security-profile=default compression=no
```

Luego, haciendo las pruebas desde el equipo que se encuentra conectado directamente al AP que está en modo Station se ve que no funciona correctamente.

```
root@STA-B:~# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1) 56(84) bytes of data.
64 bytes from 192.168.88.1: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.88.1: icmp_seq=2 ttl=64 time=0.909 ms
^C
--- 192.168.88.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.909/0.984/1.060/0.081 ms

root@STA-B:~# ping 192.168.88.254
PING 192.168.88.254 (192.168.88.254) 56(84) bytes of data.
From 192.168.88.2 icmp_seq=2 Destination Host Unreachable
From 192.168.88.2 icmp_seq=3 Destination Host Unreachable
```

```
^C
--- 192.168.88.254 ping statistics ---
4 packets transmitted, 0 received, +2 errors, 100% packet loss, time
3014ms
...

[admin@Station-MikroTik] > ping 192.168.88.254
192.168.88.254 ping timeout
192.168.88.254 ping timeout
192.168.88.254 ping timeout
4 packets transmitted, 0 packets received, 100% packet loss

root@STA-B:~# tcpdump -n -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
16:23:08.483201    ARP,    Request    who-has    192.168.88.254    tell
192.168.88.1, length 46
16:23:09.483098    ARP,    Request    who-has    192.168.88.254    tell
192.168.88.1, length 46
16:23:10.502967    ARP,    Request    who-has    192.168.88.254    tell
192.168.88.1, length 46
16:23:11.502881    ARP,    Request    who-has    192.168.88.254    tell
192.168.88.1, length 46
```

Para que se puedan enlazar como bridges, el equipo debe estar en modo **Station-WDS** (nombre particular usado por Mikrotik y protocolo propietario) o modo **Station-Pseudobridge** (nombre particular usado por Mikrotik), que es igual que el modo **Station** pero realiza traducciones de direcciones MAC (MAC address translation) sobre todo el tráfico "bridgeado", por lo tanto, no es un bridge totalmente transparente.

Configuración de Modo Station-WDS:

El Modo Station-WDS es propietario, por lo tanto, sólo funciona entre equipos con RouterOS. Se negocia la conexión y se genera una interfaz WDS separada de las creadas en WDS estándar. Se establece una conexión Punto a Punto entre la estación y el equipo como AP. Todo el tráfico enviado por la WDS del AP es directamente llevado a la estación y todo el tráfico que envía la estación es recibido por el AP a través de la interfaz de WDS. Las direcciones L2 (MAC) son conservadas, por lo tanto, cumple el rol de bridge transparente. Este modo utiliza 4 (cuatro) direcciones MAC en 802.11. Ejemplo de configuración:

```
[admin@AP-MikroTik] > /interface wireless set wlan1 wds-mode=dynamic \
                      wds-default-bridge=bridge1

[admin@AP-MikroTik] > /interface wireless print
Flags: X - disabled, R - running
```

```
 0  R name="wlan1" mtu=1500 mac-address=00:0F:A3:DD:C4:20 arp=enabled
      interface-type=Atheros AR5213 mode=bridge ssid="TEST" frequency=5180
      band=5ghz scan-list=default antenna-mode=ant-a wds-mode=dynamic
      wds-default-bridge=bridge1 wds-ignore-ssid=no default-authentication=yes
      default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0
      hide-ssid=no security-profile=default compression=no
```

Luego se configura la estación.

```
[admin@Station-MikroTik] > /interface wireless set wlan1 mode=station-wds

[admin@Station-MikroTik] > /interface wireless print
Flags: X - disabled, R - running
 0  R name="wlan1" mtu=1500 mac-address=00:15:6D:53:D5:41 arp=enabled
      interface-type=Atheros AR5213 mode=station-wds ssid="TEST" frequency=5180
      band=5ghz scan-list=default antenna-mode=ant-a wds-mode=disabled
      wds-default-bridge=none wds-ignore-ssid=no default-authentication=yes
      default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0
      hide-ssid=no security-profile=default compression=no
```

Se observa la interfaz WDS creada de forma dinámica en el AP. En el cliente no se crea de la forma tradicional.

```
[admin@AP-MikroTik] > /interface wireless wds print
Flags: X - disabled, R - running, D - dynamic
 0  RD name="wds1" mtu=1500 mac-address=00:0F:A3:DD:C4:20 \
       arp=enabled master-interface=wlan1
       wds-address=00:15:6D:53:D5:41
```

Se realizan las pruebas para observar que el enlace funciona correctamente.

```
root@STA-B:~# ping 192.168.88.3
PING 192.168.88.1 (192.168.88.3) 56(84) bytes of data.
64 bytes from 192.168.88.3: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.88.3: icmp_seq=2 ttl=64 time=0.909 ms
^C
--- 192.168.88.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.909/0.984/1.060/0.081 ms

root@STA-Z:~# ping 192.168.88.2
PING 192.168.88.2 (192.168.88.2) 56(84) bytes of data.
64 bytes from 192.168.88.2: icmp_seq=1 ttl=64 time=9.67 ms
64 bytes from 192.168.88.2: icmp_seq=2 ttl=64 time=1.13 ms
^C
```

En la figura 1.79 se muestra una captura de la trama generada mediante el ejemplo.

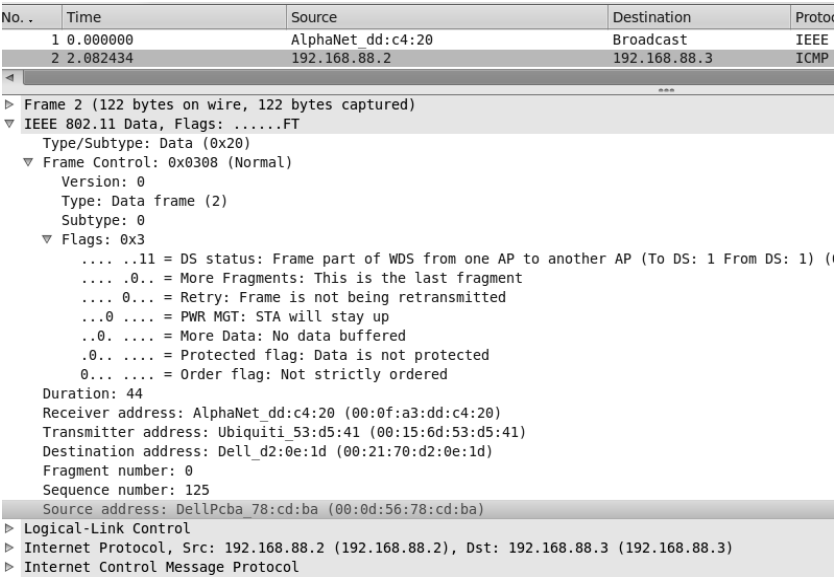


Figura 1.79 Trama MAC 802.11 en modo station-WDS

Configuración de Modo Station-Pseudobridge:

El modo **Station-Pseudobridge** funciona como una estación pero debe realizar traducciones de direcciones MAC. Su funcionalidad como L2 bridge es limitada, no es transparente. La traducción se realiza mediante una tabla de traslaciones IPv4-to-MAC que mantiene el dispositivo. Para esto debe realizar una inspección del contenido L2 (encabezados L3 (IPv4)). Cuando envía el mensaje reemplaza la dirección origen con la MAC del AP, y almacena la relación (IP origen, MAC origen), cuando vuelve la respuesta cambia la MAC por la almacenada de acuerdo a la dirección IP. Sólo usa tres direcciones y trabaja contra cualquier AP (no es propietario). Para traducir protocolos que no sean IPv4, no funciona adecuadamente y sólo mantiene la MAC de la primera estación que aprendió (single MAC address translation). Todas las tramas recibidas por el AP al enviarse a la red cableada son modificadas reemplazando la MAC por esta única que aprendió. En la figura 1.80 se muestra una captura de la trama.

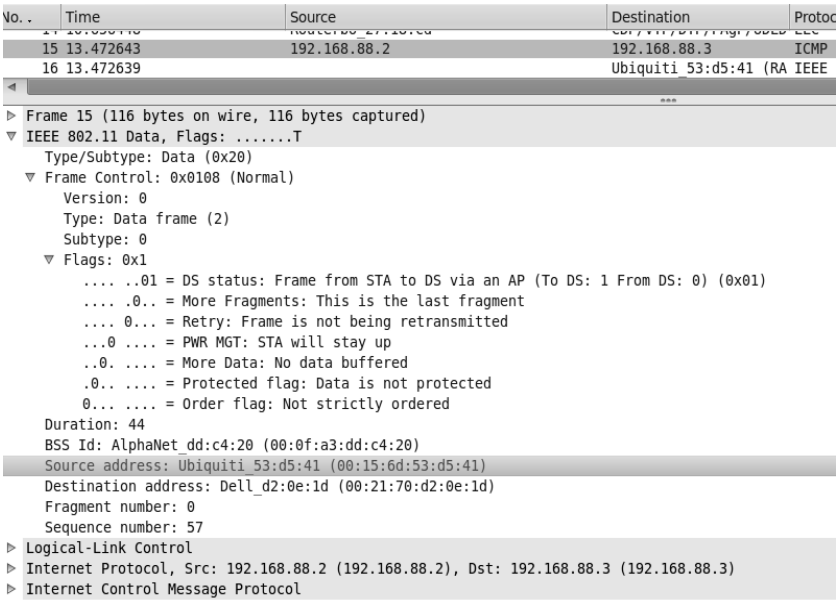


Figura 1.80 Trama MAC 802.11 en modo pseudobridge

1.4 Calidad de Servicio (QoS) con 802.11e

Calidad de Servicio **(QoS, Quality of Service)** es un término usado para definir la capacidad que tiene una red de proveer diferentes niveles de atención a los distintos tipos de tráfico. Permite que la red pueda asignar a determinadas clases de paquetes prioridad sobre otros garantizando así la provisión de un nivel de servicio.

Debido al desarrollo de nuevos tipos de aplicaciones (e.g: Voz sobre IP, Videoconferencia sobre IP, streaming, etc.), la necesidad de implementar técnicas de calidad de servicio es imperiosa. El protocolo estándar IEEE 802.11 no provee ninguna forma de diferenciar los distintos tipos de tráficos, todos son tratados en forma equitativa. A partir del estándar 802.11e se enmiendan los problemas presentados por el estándar original sobre este tema. Dentro de los métodos de acceso definidos por 802.11 nombramos DCF y PCF, el primero sólo provee un servicio de "mejor esfuerzo", **Best-Effort**. PCF, si bien es adecuado en algunos puntos, presenta tres problemas o deficiencias para ofrecer QoS. Primero define un método de asignación del medio de tipo Round-Robin que no permite manejar los diferentes requerimientos de Calidad de Servicio de las distintas aplicaciones. El mecanismo establece la transmisión de una trama Beacon cada un tiempo **TBTT (Target Beacon Transmission Time),** pero el AP, que es el encargado de enviar dicho trama, debe

disputar el acceso al medio con las demás estaciones. Si el medio está ocupado en el momento en el que se vence el TBTT, la emisión del Beacon podría ser retrasada. Otro problema que presenta es que las estaciones están autorizadas a transmitir aún cuando la transmisión finalice vencido el tiempo del siguiente TBTT. Si se retrasa la transmisión del Beacon, los datos esperando para ser transmitidos en el periodo libre de contención también sufrirán un retardo. De esta forma es muy difícil para el AP controlar el tiempo de transmisión de una estación consultada. Una estación puede transmitir tramas de hasta una longitud máxima de aproximadamente 2K bytes, lo que puede introducir retardos variables en una transmisión. La velocidad de transmisión puede cambiar de acuerdo a las condiciones variables del canal, por lo tanto, el AP no es capaz de predecir de manera segura el tiempo de transmisión.
La Wi-Fi Alliance ha desarrollado una especificación llamada **Wi-Fi Multimedia (WMM)** que contempla un subconjunto de las definiciones de 802.11e.

1.4.1 Métodos de Acceso del Estándar 802.11e

El estándar 802.11e define un conjunto de mejoras a la capa MAC del estándar 802.11 para proveer QoS. En 802.11e se implementa una nueva función de la capa MAC que se llama Función de Coordinación Híbrida **(HCF, Hybrid Coordination Function)**, la cual combina las funciones de DCF y PCF con algunas mejoras, mecanismos específicos de QoS y nuevos tipos de tramas. HCF tiene dos modos de operación llamados Acceso al Canal Distribuido Mejorado **-Enhanced Distributed Channel Access (EDCA)-** y Acceso al Canal Controlado HCF - **HCF Controlled Channel Access (HCCA)-** que son compatibles con los métodos heredados de 802.11. EDCA se puede utilizar únicamente durante el periodo de contienda, mientras que HCCA puede operar en ambos periodos (con y sin contienda) pero el estándar 802.11e recomienda su uso solamente en el periodo sin contienda.
802.11e se refiere a una estación que soporta QoS como **QSTA**, al AP con QoS como **QAP** y al BSS como **QBSS**. En un QBSS existe un controlador centralizado llamado **Hybrid Coordinator (HC)** encargado de implementar la secuencia de intercambio de tramas y las reglas de manejo de los MSDUs. El HC opera durante los dos periodos. Es el encargado de asignar los TXOPs y de iniciar los intervalos de contención controlada (CCI, Controlled Contention Interval). Normalmente, el HC reside en un QAP.
Un **TXOP (Transmission Opportunity)** es una oportunidad de transmisión y está definido por un tiempo de inicio y una duración

máxima. Se define como el intervalo de tiempo en el cual una estación tiene derecho a transmitir una serie de tramas. Una estación puede obtener un TXOP en cualquiera de los dos modos de acceso. Si lo hace durante el periodo de contención de acuerdo a las reglas del mecanismo EDCF es definido como EDCF-TXOP. Si el TXOP es obtenido durante el periodo de acceso al canal controlado se lo define como HCCA-TXOP.
Una QSTA implementa un superconjunto de las funcionalidades de una estación sin QoS, lo que implica que una estación con soporte para QoS debería poder asociarse con un AP que no lo soporta.

1.4.1.1 EDCA (Enhanced Distributed Channel Access)

EDCA es una extensión para mejorar el mecanismo de acceso DCF y provee acceso con prioridad al medio inalámbrico. Forma parte del modo HCF, no es una función de coordinación separada. Define un mecanismo de categorías de acceso (AC, Access Category) que provee soporte para las prioridades en las estaciones. Cada estación puede tener hasta 4 (cuatro) AC para 8 (ocho) prioridades de usuario **(UP, User Priorities)**. Una o más prioridades de usuario son asignadas a una categoría de acceso. Las estaciones acceden al medio basado en la categoría de acceso de la trama a ser transmitida. Cada AC es una variante mejorada de DCF que disputa las oportunidades de transmisión (TXOPs) utilizando los parámetros de EDCA.
Para que una AC con una mayor prioridad obtenga acceso al medio con anterioridad a las demás ACs con menor prioridad se le asigna un tiempo de backoff menor, lo que implica que la AC con mayor prioridad tenga que esperar menos tiempo. Esto se hace colocando los valores de los parámetros, específicos para cada AC, *CWmin*[*AC*] y *CWmax*[*AC*] que no son fijos como en DCF sino que son variables. Estos valores, que definen el rango del cual se obtiene el *CW*[*AC*], son menores cuando más prioritaria es la AC. Además, para lograr una mayor diferenciación entre las distintas ACs se introducen diferentes espacios entre tramas, IFS.
En lugar de DIFS se utiliza un nuevo IFS llamado **AIFS (Arbitration Inter-Frame Space)**, específico para AC, que indica el tiempo que debe esperar esa AC antes de intentar transmitir o empezar el algoritmo de backoff. La fórmula del AIFS se mostró en la sección **Intervalos entre Tramas**.
Las prioridades definidas en el estándar tienen un mapeo con las distintas AC. Las prioridades son las mismas definidas en el estándar IEEE 802.1p. Habitualmente en los QAP se realiza un mapeo de este valor al DSCP de IP.
El acceso al medio de este método funciona de la siguiente forma: si

el medio se detecta libre, la transmisión puede comenzar inmediatamente. Si no es así, la estación suspende su transmisión hasta que la estación que está ocupando el medio lo libere. Cuando esto sucede, la estación espera un tiempo *AIFS*[*AC*] para comenzar su procedimiento de backoff. El intervalo de backoff es un número aleatorio derivado del rango [0..*CW*[*AC*]]. Cada AC dentro de una estación se comporta como una estación virtual. Compite por el acceso al medio inalámbrico e independientemente comienza su tiempo de backoff después de sensar el medio como libre por al menos un tiempo AIFS. Las colisiones entre las distintas ACs dentro de una misma estación son resueltas dentro de la estación para lograr que las ACs con mayor prioridad reciban más rápido el TXOP. Si el tiempo de backoff de dos o más categorías de tráfico alcanza cero en el mismo instante, un planificador interno a la estación evita la colisión virtual dándole el acceso al medio a quien tenga mayor prioridad. Una colisión entre distintas ACs se trata como si fuese una colisión externa. También, cuando más prioridad tiene la AC mayor es el intervalo de TXOP, lo que implica que por cada turno puede transmitir más cantidad de paquetes.
En la figura 1.81, tomada del documento estándar IEEE 802.11e-2005 (figura 62a), se muestra el modelo de referencia de EDCA. Cada cola corresponda a un AC, por encima llegan las tramas con diferentes prioridades y por debajo se encuentra el planificador. Cada cola tiene sus propios parámetros. El estándar permite que se definan más colas. Algunos parámetros específicos para cada cola son el AIFS, el CW y el TXOP.

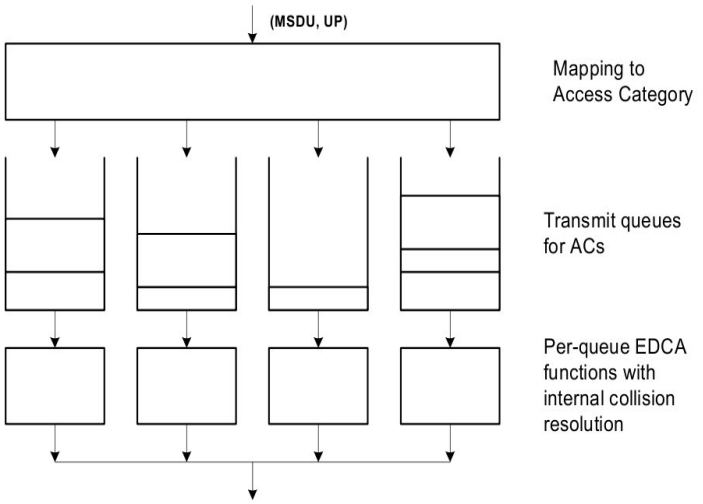


Figura 1.81 Modelo de referencia EDCA con cuatro colas

1.4.1.2 HCCA (HCF Controlled Channel Access)

El esquema de consulta de PCF es extendido en 802.11e mediante el uso de la función llamada Hybrid Coordination Function (HCF). Con este método existe una funcionalidad extra provista por un HC, Coordinador Híbrido, generalmente ubicado en el AP. Éste difiere del PC, utilizado en PCF, en varios aspectos pero, principalmente, en que puede funcionar en ambos periodos, el de contienda y el libre de contienda, lo que implica que no es obligatorio que utilice el periodo libre de contiendas para transferir datos de Calidad de Servicio. Otra diferencia es que el HCF puede consultar a las estaciones que soportan Calidad de Servicio y otorgarles TXOPs.
El HC obtiene el control del medio wireless cuando necesita enviar tráfico de datos o alguna trama específica a las estaciones que soportan QoS. Para lograr esto, el HC espera una menor cantidad de tiempo entre transmisiones al que tienen que hacerlo el resto de las estaciones usando los procedimientos de EDCA.
Para evitar que una STA, estación sin soporte de QoS, intente transmitir en un periodo libre de contenciones (como la estación no soporta QoS no entiende los nuevos parámetros definidos en el estándar 802.11e), el HC puede incluir el tiempo de duración del periodo de contención en los Beacons para que la estación pueda establecer el valor del NAV y no intente transmitir mientras ese valor sea mayor a cero. Esto causa que la estación suponga que existe un PC en el QBSS.
Previamente a obtener el medio para comenzar un periodo libre de contienda, o un TXOP en el periodo de contienda, el HC debe sensar el medio. Si está libre por un lapso igual a PIFS, el HC transmitirá la primera trama del intercambio correspondiente, indicando la duración del TXOP o del periodo libre de contienda. En este intervalo de tiempo, llamado Fase de Acceso Controlado, **Controlled Access Phase (CAP)**, el medio está bajo el control del HC. Si pasa un tiempo PIFS desde el final del TXOP y el HC no reclama el medio, el CAP finaliza.
El HCF también puede operar como un PC consultando a las estaciones que no tienen la capacidad de soportar Calidad de Servicio; para esto usa los formatos de las tramas, secuencia de intercambio de tramas y todas las demás reglas especificadas para PCF.

1.4.2 Agregados 802.11e a nivel MAC

El estándar 802.11e, además de los métodos de acceso nuevos, agrega otras mejoras en la capa MAC. Estas se definen a continuación.

1.4.2.1 Formato de Trama de Datos

Se agrega un nuevo campo al encabezado de la trama de datos. Es un

campo de 16 bits que ubicado al final del encabezado. De acuerdo al tipo de trama es el significado de su valor. Para una trama de datos con QoS se codifican en este campo la prioridad de igual forma que 802.1p, el esquema de ACK y el TXOP o el estado de la cola en el QAP. En la figura 1.82 se muestra una captura con los valores para estos campos.

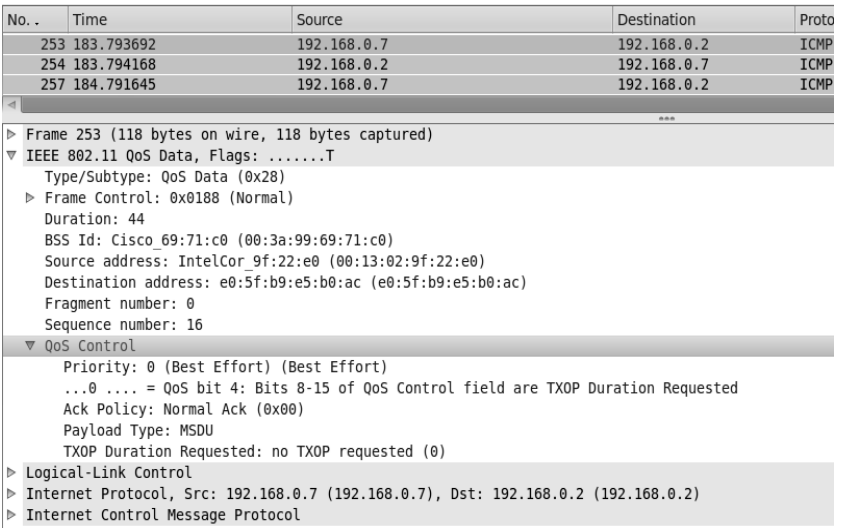


Figura 1.82 Trama MAC 802.11e con encabezado de QoS

1.4.2.2 Ráfaga Libre de Contención

Contention Free Burst (CFB)

Permite que una estación, o AP, pueda enviar varias tramas seguidos sin tener que disputar el acceso al medio. Una vez que un nodo obtiene su TXOP, puede enviar tramas continuamente y lo hace mientras le quede tiempo en el TXOP obtenido. Para poder asegurarse el acceso al medio, el tiempo entre tramas es SIFS. Esto es lo que se vió como **Frame Bursting** o Agregación de tramas, que incorpora 802.11n.

1.4.2.3 Protocolo de enlace directo

Direct Link Protocol (DLP)

En una red infraestructura, según la especificación original del estándar 802.11, si dos estaciones se quieren comunicar entre ellas lo deben hacer a través del AP. DLP permite que dos estaciones se puedan comunicar directamente sin necesidad de usar el AP. Esto sólo puede funcionar si cada estación se encuentra dentro del área de cobertura de la otra.

1.4.2.4 Nuevas reglas de acuse de recibo

New Acknowledgement Rules

De acuerdo a lo estudiado en 802.11, para cada trama unicast se requiere una de control ACK. 802.11n cambia las reglas. Los cambios son basados en los agregados en 802.11e. 802.11e para HCF agrega dos nuevas opciones que son especificadas en el campo de control de QoS de cada trama de datos. Una opción es trama **Sin ACK** que, con el fin de mejorar la eficiencia de determinadas aplicaciones, no se requiere el envío de ACKs. Opción útil en aplicaciones de baja latencia como voz sobre IP. La otra opción es el **Bloque ACK** que permite confirmar varias tramas con un vector de bits de ACKs. Esta opción permite funcionar de forma inmediata, solicitando un BlockACK vía un BlockACKReq, luego que se enviaron varias tramas en CFB. También puede funcionar de forma diferida, al recibir el BlockACK Request, se confirma parcialmente indicando que los ACKs van a ser demorados. Los métodos de confirmación en bloques permiten explotar la técnica de "piggybacking".

1.4.3 Ejemplo de Configuración de QoS

A continuación se muestra comandos sobre un AP Cisco que permite configurar las clases de QoS.

```
aptest(config)#interface dot11Radio 0
aptest(config-if)#dot11 qos ?
  class  Access class parameters
  mode   Type of QOS control to use

 dot11 qos mode ?
  wmm  Enable WMM clients

 dot11 qos class ?
  background   Parameters for the background access class
  best-effort  Parameters for the best effort access class
  video        Parameters for the video access class
  voice        Parameters for voice access class

aptest(config-if)#dot11 qos class background
aptest(config-if-qosclass)#?
Access class configuration commands:
  admission-control  Require admission control
  admit-traffic      Set Admission Control Configuration
  cw-max             802.11 contention window maximum
  cw-min             802.11 contention window minimum
  exit               Exit from access class sub mode
  fixed-slot         802.11 fixed backoff slot time
  no                 Negate a command or set its defaults
  transmit-op        Transmit opportunity in usec
```

```
aptest(config-if-qosclass)#cw-max ?
  <0-10>  CwMax will be ( 2 to the power of the entered value ) - 1

aptest(config-if-qosclass)#transmit-op ?
  <0-65535>  Transmit opportunity time in microseconds
```

CAPÍTULO 2

Seguridad en 802.11

2.1 Introducción

Debido a las características inherentes de las comunicaciones wireless, la seguridad es uno de los temas más importantes. Una estación 802.11 se comunica con otras estaciones utilizando radiofrecuencias como señal portadora. Los datos son enviados en forma broadcast al medio inalámbrico, lo que implica que todos los nodos dentro del área de cobertura del emisor recibirán esas transmisiones, inclusive aquellos que no deberían hacerlo. Sin los mecanismos de seguridad adecuados, el envío de información sensible podría ser leído por personas no autorizadas. Desde su inicio, los diseñadores del estándar 802.11 tuvieron en cuenta este problema y para solucionarlo definieron dos componentes de seguridad: autenticación y cifrado. Sin embargo, debido a distintas fallas que les fueron encontradas a través del tiempo, los algoritmos que implementaban esos componentes han tenido que ir modificándose para solucionar tales problemas, y, debido a la gravedad de las deficiencias halladas, se han introducido nuevas soluciones.

La especificación original 802.11 definió dos métodos de autenticación: Open System y Shared-Key, y uno para cifrado: Wired Equivalent Privacy (**WEP**) que se mantuvieron sin modificaciones en posteriores enmiendas, como son **802.11a** y **802.11b**. Para 2001, dos años después de que el estándar se publicase, ya estaban disponibles herramientas diseñadas para "crackear" WEP. Esto causó una gran preocupación en la comunidad wireless: sin una buena seguridad, el futuro de las redes inalámbricas estaba seriamente comprometido. Para resolverlo, a principios de 2001 la IEEE formó el Task Group "i" para que se encargue de desarrollar nuevos mecanismos de seguridad. Pero, el proceso de definir un nuevo estándar lleva demasiado tiempo, algo que la comunidad wireless no iba a tolerar: sin seguridad, las redes wireless tenían las horas contadas.

Para satisfacer las necesidades de la industria, que no podía esperar hasta la ratificación final del estándar, la Wi-Fi Alliance adoptó una nueva propuesta de seguridad basada en el draft 3 de la **IEEE 802.11i** [802.11i] que llamó **WPA** (Wi-Fi Protected Access). Esta nueva solución transitoria, que en el estándar 802.11i recibe el nombre de Transition Security Network (**TSN**), debía correr en el hardware

existente, es decir, los usuarios no serían obligados a cambiar sus equipos wireless.
Es importante explicar porque no alcanzaba con una simple actualización del software o firmware de los dispositivos wireless. La mayoría de las tarjetas wireless están compuestas de cuatro partes (Radio Frecuencia, MODEM, Medium Access Control y Host Interface). La mayor parte del protocolo IEEE 802.11 se encuentra implementado en la sección Medium Access Control (MAC). Debido a que tiene que realizar tareas a gran velocidad, la MAC está implementada como una combinación de firmware y hardware. Entre estas funciones se encuentran, generalmente, las de encriptar y desencriptar. A causa de esto, la implementación de WEP casi siempre depende de funciones del hardware, que no pueden ser modificadas después que se manufacturaron.
La propuesta WPA incluye la mayoría de las características del estándar 802.11i. Como métodos de autenticación se puede elegir entre dos opciones: usar un servidor de autenticación **802.1x** (WPA-Enterprise) o trabajar con una PreShared Key (**PSK**, WPA-Personal). Para encriptar utiliza un nuevo protocolo llamado Temporal Key Integrity Protocol (**TKIP**). Además, define un nuevo método para comprobar la integridad de los paquetes en reemplazo del CRC-32.
La especificación definitiva IEEE 802.11i define un nuevo tipo de redes wireless: Robust Security Network (**RSN**). Son similares a las redes wireless tradicionales, pero deben cumplir con un conjunto de nuevas características de seguridad. En una verdadera red RSN, el AP sólo permite que se conecten dispositivos con capacidad RSN. No soporta dispositivos que solamente conocen WEP, o pre-RSN como se los llama en el estándar. Para adoptar esas nuevas características fue necesario, además de la lógica actualización del software, cambiar el hardware para que soportase las nuevas operaciones criptográficas. Dentro de la Wi-Fi Alliance, el nuevo estándar recibió el nombre de **WPA2** y, en consecuencia, los métodos de autenticación reciben el nombre de WPA2-Personal y WPA2-Enterprise.

2.2 Autenticación

La autenticación es el proceso a través del cual una red puede verificar la identidad de una estación wireless que está intentando conectarse. Antes de que una estación pueda unirse a una WLAN, debe identificarse. En una red de tipo infraestructura, el AP es el encargado de realizar la autenticación, en cambio, en una red ad-hoc, la misma se realiza entre las estaciones que componen la red. Se debe tener en cuenta que estos modos de autenticación pertenecen a las estaciones (a

las placas de red para ser más específicos) y no a los usuarios.
El estándar 802.11 define dos tipos de autenticación:

- Autenticación Abierta (Open System)
- Autenticación de Clave Compartida (Shared Key)

2.2.1 Autenticación Abierta (Open System)

Existe una contradicción en este punto porque, si bien se la describe como un método de autenticación, el acceso es permitido a todos los usuarios. Cualquier usuario que se encuentre dentro del área de la red tiene, en principio, acceso a la misma. Semánticamente, su significado es equivalente a "no autenticación". Sin embargo, se produce un intercambio de paquetes entre la estación que quiere acceder a la red y el autenticador. Los frames se mandan en texto plano, aunque esté habilitada la encriptación WEP. Es el algoritmo de autenticación usado cuando no se selecciona ninguno alternativo. La figura 2.1 muestra el intercambio de paquetes correspondiente a este método.

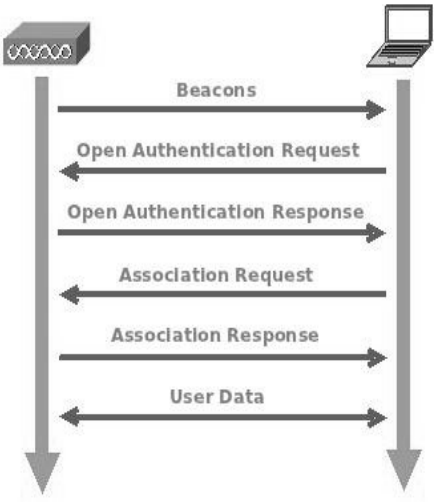


Figura 2.1 Autenticación Abierta (Open System)

Después de encontrar la red a la que se quiere asociar, la estación envía un frame, o trama, de tipo Management, del subtipo Authentication, al AP, en el cual le indica el tipo de autenticación utilizado. A continuación se muestra el frame correspondiente (no se muestran los campos innecesarios para este tema):

```
.....
802.11 MAC Header
  Version:              0
  Type:                 %00     Management
  Subtype:              %1011   Authentication
Frame Control Flags:    %00000000
                        0... .... Non-strict order
```

```
                        .0.. .... WEP Not Enabled
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System
  Destination:          00:0F:F8:58:B5:D6
  Source:               00:0F:F8:54:28:B8
  BSSID:                00:0F:F8:58:B5:D6
  Seq. Number:          11
  Frag. Number:         0
802.11 Management - Authentication
  Auth. Algorithm:      0
  Auth. Seq. Num.:      1
  Status Code:              0
```

Estos son los campos más importantes que componen la solicitud de Autenticación:

- **Auth. Algorithm:** 0
  Indica que se usa el sistema de autenticación abierta.
- **Auth. Seq. Num.:** 1
  Se utiliza para indicar que este es el primer frame de la secuencia.
- **Status Code:** 0
  Este código se utiliza para indicar el resultado de una operación. Como no se realizó ninguna acción, su valor es 0.

Una vez recibido este frame, el AP le envía un frame Ack a la estación solicitante. Luego, procesa la solicitud de autenticación y le contesta con un frame del mismo tipo y subtipo que el primer frame. A continuación se muestra la conformación del frame:

```
.....
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1011  Authentication
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... WEP Not Enabled
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System
  Destination:          00:0F:F8:54:28:B8
  Source:               00:0F:F8:58:B5:D6
  BSSID:                00:0F:F8:58:B5:D6
  Seq. Number:          291
  Frag. Number:         0
802.11 Management - Authentication
  Auth. Algorithm:      0
  Auth. Seq. Num.:      2
  Status Code:          0
```

Los campos de la autenticación en la respuesta son similares a los del primer frame. Si por algún motivo el AP no aceptase a una estación (por ejemplo, porque está saturado), el valor del Status Code, que sería diferente a 0, indicaría el tipo de error.

- **Auth. Seq. Num.:** 2
  Indica que es el segundo paquete de la secuencia.
- **Status Code:** 0
  El código 0 dice que la operación fue exitosa.

2.2.2 Autenticación Clave Compartida (SharedKey)

La autenticación de clave compartida (Shared-Key) hace uso de WEP (Wired Equivalency Privacy) y, por lo tanto, sólo se la puede usar en productos que lo implementen. Además, el estándar 802.11 requiere que cualquier estación que implemente WEP debe soportar este tipo de autenticación. El término clave secreta compartida se refiere al hecho de que todas las estaciones conocen la misma clave (o conjunto de claves).
A diferencia del método anterior que necesita el intercambio de dos frames para realizar su trabajo en éste son necesarios cuatro. Este intercambio de paquetes se puede observar en la figura 2.2.

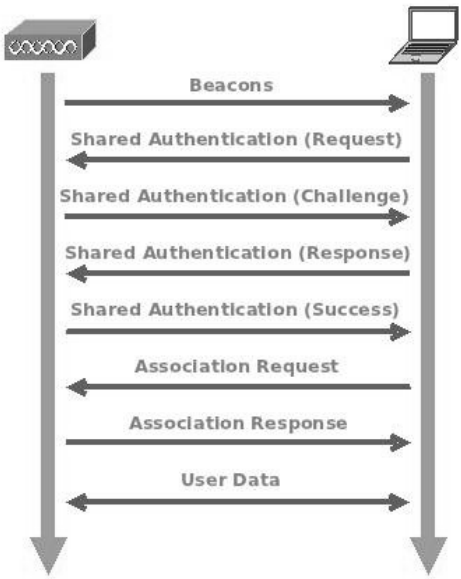


Figura 2.2 Autenticación Clave Compartida (Shared Key)

El primer frame es enviado desde la estación que desea asociarse a la red wireless. Es del tipo de Management, subtipo Authentication, y contiene los mismos campos que el primer frame utilizado en la

Autenticación Abierta. Sólo se modifica el valor del campo *Auth. Algorithm,* se establece a 1, para indicar que se está usando la Autenticación de Clave Compartida. Éste es el contenido del primer frame del proceso:

```
.....
802.11 MAC Header
  Version:                0  [0 Mask 0x03]
  Type:                   %00  Management  [0]
  Subtype:                %1011  Authentication  [0]
Frame Control Flags:      %00000000  [1]
                          0... .... Non-strict order
                          .0.. .... WEP Not Enabled
                          ..0. .... No More Data
                          ...0 .... Power Management - active mode
                          .... 0... This is not a Re-Transmission
                          .... .0.. Last or Unfragmented Frame
                          .... ..0. Not an Exit from the Distribution System
                          .... ...0 Not to the Distribution System
  Destination:            00:0F:F8:58:B5:EB  [4-9]
  Source:                 00:0F:F8:54:28:B2  [10-15]
  BSSID:                  00:0F:F8:58:B5:EB  [16-21]
  Seq. Number:            1817  [22-23 Mask 0xFFF0]
  Frag. Number:           0  [22 Mask 0x0F]
802.11 Management - Authentication
  Auth. Algorithm:        1  Shared Key  [24-25]
  Auth. Seq. Num.:        1  [26-27]
  Status Code:            0  Reserved  [28-29]
FCS - Frame Check Sequence
  FCS (Calculated):       0xEC9CF93C
```

Después de enviar el ACK correspondiente, el nodo autenticador le contesta al solicitante con un frame de igual tipo y subtipo que el anterior. A diferencia del primer método, el acceso a la red no es otorgado indiscriminadamente. El solicitante debe ser capaz de resolver un desafío que le planteará el autenticador. Éste le envía un número aleatorio de 128 bytes (siempre es de este tamaño) que recibe el nombre de "challenge text" (texto desafío). A continuación se muestra el segundo frame del proceso:

```
.....
802.11 MAC Header
  Version:                0  [0 Mask 0x03]
  Type:                   %00  Management  [0]
  Subtype:                %1011  Authentication  [0]
Frame Control Flags:      %00000000  [1]
                          0... .... Non-strict order
                          .0.. .... WEP Not Enabled
                          ..0. .... No More Data
                          ...0 .... Power Management - active mode
                          .... 0... This is not a Re-Transmission
                          .... .0.. Last or Unfragmented Frame
                          .... ..0. Not an Exit from the Distribution System
                          .... ...0 Not to the Distribution System
  Destination:            00:0F:F8:54:28:B2  [4-9]
  Source:                 00:0F:F8:58:B5:EB  [10-15]
  BSSID:                  00:0F:F8:58:B5:EB  [16-21]
  Seq. Number:            673  [22-23 Mask 0xFFF0]
  Frag. Number:           0  [22 Mask 0x0F]
802.11 Management - Authentication
  Auth. Algorithm:        1  Shared Key  [24-25]
  Auth. Seq. Num.:        2  [26-27]
```

```
  Status Code:          0  Successful  [28-29]
Challenge text
  Element ID:           16  Challenge text  [30]
  Length:               128  [31]
  Value:
0xA39B9A2E427580288A6DD6539BB3272A07D54E0E3400A3F47EDA6128278CD123B5D5421C
14F3C74EC0D4597FC1A2EED8254FDA5ABCA674B9F4C29EF0E7CD4B7C01573E7BD6E292A8D7
205A54D3B293B585626E5C82F929117F961276D19BFFE2F4A8E92B33549DE9F5B0D61C2C53
885C1543758A1ECEAD4412C6B28D58D4825C  [32-159]
FCS - Frame Check Sequence
  FCS (Calculated):     0xD1CE0157
```

En esta etapa del proceso el autenticador podría denegar la solicitud de autenticación estableciendo el Status Code a un valor distinto de 0, lo que abortaría toda la operación. El valor del Status Code en 0 indica que la operación aún está en proceso, no que se ha otorgado el acceso. Al recibir el segundo frame, la estación solicitante debe contestar el desafío. Lo que hace es extraer el "challenge text" del mensaje, lo encripta con WEP utilizando la clave secreta compartida y se lo envía al autenticador. Este tercer frame se muestra a continuación:

```
.....
802.11 MAC Header
  Version:              0  [0 Mask 0x03]
  Type:                 %00  Management  [0]
  Subtype:              %1011  Authentication  [0]
Frame Control Flags:    %01000000  [1]
                        0... .... Non-strict order
                        .1.. .... WEP Enabled
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System
  Destination:          00:0F:F8:58:B5:EB  [4-9]
  Source:               00:0F:F8:54:28:B2  [10-15]
  BSSID:                00:0F:F8:58:B5:EB  [16-21]
  Seq. Number:          1818  [22-23 Mask 0xFFF0]
  Frag. Number:         0  [22 Mask 0x0F]
WEP Data
  WEP IV:               0x8A00FB  [24-26]
  WEP Key Index:        0  Key ID=1  [27 Mask 0xC0]
  WEP Data:
  *=....u.J.......  2A 3D F7 D0 0E C0 75 A7 4A 06 17 A2 05 EA DB 94  [28-43]
  iq4..p.EU2D|...}  69 71 34 05 E8 70 D9 45 55 32 44 7C 95 A5 0D 7D  [44-59]
  j.5Md.\=.|..t9..  6A 8B 35 4D 64 7F 5C 3D B0 7C BF E3 74 39 A9 B2  [60-75]
  %...+....3..S...  25 09 8B E6 2B D1 01 FA EB 33 B7 E3 53 0A F6 0D  [76-91]
  .z....*.,.KH.k..  92 7A A1 F7 D5 B1 2A 2E 2C FB 4B 48 04 6B 15 B9  [92-107]
  .9..?dm:~.[03...  F7 39 B9 DA 3F 64 6D 3A 7E A5 5B 30 33 CE FA BE  [108-123]
  .0...?{.0.....U.  A1 30 A6 E1 A4 3F 7B 0D 30 A4 81 C9 EA D2 55 8A  [124-139]
  .2.k..;w".......  82 32 D7 6B A4 E1 3B 77 22 AB 1D 0E B1 AC 17 AE  [140-155]
  .*..Ci..          D4 2A AF DA 43 69 B8 EB  [156-163]
  WEP ICV:              0x9F17B056  [164-167]
FCS - Frame Check Sequence
  FCS (Calculated):     0xED52345B
```

Cuando recibe el frame, el autenticador debe desencriptar el mensaje para obtener el "challenge text". Si coincide con el valor previamente enviado, la encriptación se realizó con la clave secreta correcta, de lo que se deduce que el solicitante conoce dicha clave. Los campos de WEP se explican en la sección correspondiente.

El frame final es enviado al solicitante para informar del resultado del proceso. Al setear el campo Status Code en 0, el autenticador le indica al nodo solicitante que el proceso tuvo éxito, por lo cual, ya tiene acceso a la red.

```
.....
802.11 MAC Header
  Version:              0  [0 Mask 0x03]
  Type:                 %00  Management  [0]
  Subtype:              %1011  Authentication  [0]
Frame Control Flags:    %00000000  [1]
                        0... .... Non-strict order
                        .0.. .... WEP Not Enabled
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System
  Destination:          00:0F:F8:54:28:B2  [4-9]
  Source:               00:0F:F8:58:B5:EB  [10-15]
  BSSID:                00:0F:F8:58:B5:EB  [16-21]
  Seq. Number:          674  [22-23 Mask 0xFFF0]
  Frag. Number:         0  [22 Mask 0x0F]
802.11 Management - Authentication
  Auth. Algorithm:      1  Shared Key  [24-25]
  Auth. Seq. Num.:      4  [26-27]
  Status Code:          0  Successful  [28-29]
FCS - Frame Check Sequence
  FCS (Calculated):     0x9F8A6CD5
```

Este proceso es muy simple de ejecutar, sin embargo presenta una deficiencia muy importante que puede brindarle información sensible a un posible atacante. El "challenge text" se envía en texto claro y encriptado, como se acaba de mostrar. Si alguien captura este intercambio de mensajes está en condiciones de obtener el keystream usado para encriptar el "challenge text", lo que le permitirá inyectar información en la red, aun sin conocer la clave secreta

2.3 WEP (Wireless Equivalent Privacy)

Los objetivos de WEP, según el estándar, son:

- razonablemente fuerte
- eficiente
- exportable
- opcional
- auto-sincronizado

Por auto-sincronizado se entiende que cada paquete debe ser encriptado en forma separada, por lo tanto, una clave y un paquete debería ser toda la información necesaria para desencriptarlo. No es necesario ningún dato adicional.

El trabajo de WEP se centra en dar seguridad en el medio wireless

únicamente. No hace nada para dar seguridad a los paquetes una vez que estos ingresaron a la red cableada. WEP utiliza para encriptar los mensajes el cifrador RC4, de la empresa RSA Security.
RC4 es un protocolo de clave simétrica, usa la misma clave secreta para encriptar y para desencriptar. Es muy fácil de implementar y no realiza ninguna operación compleja o que consuma demasiado tiempo de procesamiento. Esto permite que se pueda implementar en software y firmware, con lo cual se lo puede integrar en Access Points (AP) y PC Cards. Pertenece al grupo de los cifradores de "stream cipher", lo cuales no dividen los datos en bloques para encriptar como lo hacen los cifradores de bloque sino que trabajan sobre unidades más pequeñas, como puede ser un bit. Un stream-cipher es mucho más rápido que los cifradores de bloque y, a diferencia de estos, si se cifra dos o más veces el mismo mensaje produce distintos resultados. Mientras los datos son procesados, el estado interno del cifrador es continuamente actualizado. Esta clase de cifradores toma una "semilla" y la expande a un "keystream", que es una cadena pseudoaleatorio de caracteres, de la misma longitud del mensaje a encriptar. La fortaleza del cifrador reside enteramente en la aleatoridad de ese keytream.
Un requisito fundamental de RC4 es que el keystream se debe regenerar por cada paquete que se quiera encriptar, lo que implica que la semilla utilizada para generarlo se debe modificar por cada nuevo paquete que se encripta. El componente encargado de realizar esta tarea es el Generador de Número Pseudoaleatorios (PseudoRandom Number Generator, PRNG), y es sumamente crítica su función porque se encarga de transformar una semilla en un keystream. La semilla está compuesta por una clave secreta que se combina con un número de 24 bits que debería cambiar para cada paquete que se encripta. Este número recibe el nombre de Initialization Vector (IV) y se transmite, sin encriptar, en la cabecera de cada paquete encriptado. Esto debe ser así para posibilitar que el receptor pueda formar la misma semilla que utilizó el emisor para realizar el cifrado. El estándar aconseja el uso de diferentes IV para cada paquete, pero no es obligatorio.
La clave secreta, a su vez, debe tener una longitud de 40 ó 104 bits, según la especificación de WEP. El estándar original sólo definía claves de longitud de 40 bits, pero en enmiendas posteriores se incluyó el tamaño de 104 bits. Esta clave secreta se debe compartir entre el emisor y el receptor. Las especificaciones de algunos productos suelen decir que soportan seguridad de 64 ó 128 bits. Esto no es totalmente cierto, ya que toman como parte de la clave al IV, que nunca es secreto. Actualmente existen vendedores que ofrecen dispositivos que soportan claves WEP de 256 bit. Las claves secretas tienen las siguientes características:

- longitud fija: 40 ó 104 bits.
- estática: el valor de la clave no se modifica, excepto cuando se la reconfigura manualmente.
- compartida: el AP y todas las estaciones tienen la misma clave.
- simétrica: misma clave para encriptar y desencriptar.

Además de encriptar los mensajes, la integridad de los mismos es otra de las finalidades de WEP. Es por esto, que antes de la encriptación de los paquetes, se ejecuta sobre los mismos un algoritmo de chequeo de integridad que genera un valor de 4 bytes llamado Integrity Check Value (ICV). El ICV es el resultado de la función CRC-32, la misma función que es utilizada como Frame Check Sequence en Ethernet e IEEE 802.3. El valor obtenido se concatena detrás del mensaje antes de ser encriptado. El receptor del frame debe calcular el ICV nuevamente y compararlo con el recibido en el frame (después de desencriptarlo). Esto es para verificar que lo que fue recibido es igual al frame que fue enviado por el emisor, es decir, no fue alterado en el camino.

2.3.1 ¿Cómo trabaja WEP?

En la figura 2.3 se muestran y explican los pasos involucrados en la encriptación de un paquete:

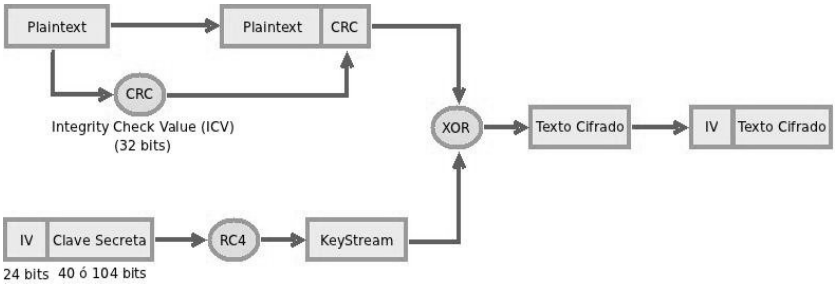


Figura 2.3 Proceso de encriptación e integridad en WEP

Observando la figura 3.2 se podría decir que el proceso tiene dos ramas que se unen en un punto determinado. Este proceso siempre comienza con un mensaje de texto plano. A partir de éste se siguen los siguientes pasos:

- Se calcula el ICV del mensaje en texto claro.
- El ICV obtenido en el paso anterior se concatena al final del mensaje.
- Se obtiene el IV al cual se le concatena la clave secreta produciendo la semilla que ingresa el PRNG de RC4.

- La semilla obtenida en el paso anterior es pasada a través del PRNG para obtener el keystream de igual longitud que la combinación del mensaje en texto claro a encriptar más el ICV que se le concatenó en pasos anteriores.
- Se realiza un XOR (OR exclusivo) entre el mensaje en texto plano y el keystream. Se obtiene el texto cifrado.
- Por último, el IV (sin encriptar) es insertado delante del mensaje encriptado para ser enviado junto con éste al receptor.

Para desencriptar un mensaje recibido, el receptor realiza el mismo procedimiento pero en reversa. Utilizando el valor del IV que se encuentra en el mensaje, junto con la clave secreta, que tanto el emisor como el transmisor conocen, se genera la semilla que luego se pasa por el PRNG para obtener el keystream. Luego, se realiza un XOR entre el keystream y el texto cifrado, del cual se obtiene el texto plano (o sin cifrar). Por último, se ejecuta nuevamente el CRC-32 sobre el mensaje y se compara con el ICV que se encontraba en el paquete recibido. Si coinciden, el paquete es aceptado. En caso contrario, se rechaza. Así se compone un paquete con WEP habilitado:

…..

```
802.11 MAC Header
  Version:               0  [0 Mask 0x03]
  Type:                  %10  Data  [0]
  Subtype:               %0000  Data Only  [0]
Frame Control Flags:     %01000010  [1]
                         0... .... Non-strict order
                         .1.. .... WEP Enabled
                         ..0. .... No More Data
                         ...0 .... Power Management - active mode
                         .... 0... This is not a Re-Transmission
                         .... .0.. Last or Unfragmented Frame
                         .... ..1. Exit from the Distribution System
                         .... ...0 Not to the Distribution System
  Destination:           01:00:5E:00:00:01  McastDoD RFC 1112:00:00:01[4-9]
  BSSID:                 00:0F:F8:58:B5:EB  [10-15]
  Source:                00:0F:F8:58:B5:EB  [16-21]
  Seq. Number:           676  [22-23 Mask 0xFFF0]
  Frag. Number:          0  [22 Mask 0x0F]
WEP Data
  WEP IV:                0x030029  [24-26]
  WEP Key Index:         0  Key ID=1  [27 Mask 0xC0]
  WEP Data:
  .'...s...}._b.(.  F0 27 A4 CC B4 73 82 03 88 7D 9D 5F 62 90 28 F3  [28-43]
  j&...q.:<BY.1...  6A 26 90 1E CB 71 F3 3A 3C 42 59 E4 31 E8 10 E4  [44-59]
  .......G...f3$..  D1 16 DC E6 A8 C4 E7 47 AB 10 7F 66 33 24 DF BF  [60-75]
  P.....            50 19 D7 9E E7 C7  [76-81]
  WEP ICV:               0x744D6B7C  [82-85]
FCS - Frame Check Sequence
  FCS (Calculated):      0x787B19E1
```

A continuación se explican los campos de mayor relevancia:

- **WEP Enabled:** .1.. ....
  Mediante este bit seteado en 1 se indica al receptor que el paquete está encriptado con WEP.

- **WEP IV:** 0x030029
  Este valor es el IV (Initialization Vector) que deberá utilizar el receptor para poder desencriptar el paquete.
- **WEP Key Index:** 0
  Sirve para indicar que clave secreta fue utilizada para encriptar. En WEP se pueden definir hasta 4 claves diferentes y cualquiera de ellas puede ser utilizada en cualquier momento. Es por esto, que el emisor debe indicarle al receptor cual es la clave secreta que tiene que utilizar para desencriptar el paquete.
- **WEP Data:** ...s...}._b.(. F0 27 A4 CC B4 73 82 03 88 7 …
  Los datos del usuario encriptados por WEP.
- **WEP ICV:** 0x744D6B7C
  Este valor es utilizado para lograr la integridad de los datos y es el resultado de calcular el CRC sobre el mensaje original.

2.3.2 Problemas con WEP

A medida que se iba incrementando la utilización de las redes wireless, también crecía el interés de la comunidad criptográfica en encontrar vulnerabilidades en los mecanismos de seguridad del estándar. Las primeras vulnerabilidades de WEP se empezaron a detectar a mediados del 2000, y para finales del 2001 ya comenzaron a verse las primeras herramientas para atacar esas fallas. Estos son algunos de los problemas encontrados:

- No tiene definido un mecanismo de key management (administración de claves) que permita la distribución de claves en forma automática entre todos los usuario. Debe hacerse en forma manual. Si la red tiene muchos usuarios esto se vuelve problemático.
- WEP usa la función CRC-32 para el chequeo de integridad. Ésta no es una función hash, por lo tanto su validez es prácticamente nula. A pesar de estar encriptado es muy fácil encontrar el ICV: son los 4 bytes que preceden al FCS del frame.
- Tamaño del IV corto. El PRNG podría reutilizar la misma semilla para generar el keystream lo que viola el principio de fortaleza del RC4: el keystream debe ser distinto para cada paquete a encriptar. Aunque permite hasta 16.777.215 valores distintos, en una red con alta carga de transmisiones este valor puede alcanzarse en cuestión de horas.
- No tiene forma de evitar los ataques de tipo “replay attacks” (ataque de repetición). Un atacante puede capturar un frame

válido y, sin conocer el contenido del mismo, puede enviarlo nuevamente a la red y ésta lo aceptará como un frame válido.

- Fluhrer, Mantin and Shamir (FMS) Attack. Este fue el ataque más devastador que sufrió WEP. Los diseñadores de este ataque notaron que ciertos tipos de claves, llamadas claves débiles, provocaban que los primeros bytes del keystream no fuesen lo suficientemente aleatorios. Si se captura una cierta cantidad de paquetes cifrados con este tipo de claves débiles entonces es posible derivar la clave secreta.

Algunas de las fallas de la implementación del cifrador RC4 en WEP es que en el estándar no se especifica cómo se genera el IV. Recordar que la necesidad del IV es para asegurar que la semilla que se ingresa al PRNG de RC4 sea siempre distinta, aspecto sobre el cual RC4 es sumamente claro. ¿Cómo se elige el valor del IV? ¿En forma aleatoria? ¿Se inicia el IV en 0 y se lo incrementa de a 1? ¿Empieza en el valor más alto del IV y se lo decrementa? En la parte donde se explica TKIP veremos de qué manera soluciona todos estos problemas.

2.4 IEEE 802.11i/WPA/WPA-2

2.4.1 Autenticación

Uno de los principales problemas de WEP es que no especifica ningún protocolo de establecimiento de clave sino que confía en el concepto de clave secreta compartida que debe ser establecida mediante algún mecanismo "out-of-band". La solución a este problema requiere el soporte de nuevos componentes y protocolos en la arquitectura.

802.11i define dos entornos de seguridad, home (hogar) y enterprise (empresa) los llamó la Wi-Fi Alliance, con distintos requerimientos de seguridad e infraestructura, por lo tanto, especificó dos arquitecturas con diferentes niveles de seguridad. En una red empresarial se utiliza el protocolo 802.1x para el establecimiento de claves y la autenticación. Pero, como 802.1x requiere el uso de un servidor de autenticación (por ejemplo, RADIUS) que, generalmente, no es factible de implementar en redes pequeñas u hogareñas, 802.11i también permite el uso de mecanismos de establecimiento de claves "out-of-band".

Otro gran problema de WEP es que utiliza, directamente, la clave secreta ingresada por el usuario para encriptar los datos, lo que produce una gran exposición de la misma y la hace más vulnerable. En 802.11i, sin importar el entorno elegido (home o enterprise), se

resuelve este problema al reducir esa exposición. Ambos métodos deducen la "Pairwise Master Key (PMK)" a partir de la información brindada por el usuario o administrador de la red. La diferencia radica en la manera en que deducen esa PMK. Una vez que se obtiene la PMK, el proceso de autenticación es igual en ambos métodos. A partir de la PMK se obtienen las claves que se utilizan realmente para los procesos de integridad y encriptación.
Estos métodos son flexibles acerca de como la PMK es establecida. Puede ser del tipo preshared key (clave precompartida) que se conoce como Autenticación WPA-PSK, o WPA2-PSK, o derivada de un proceso de autenticación tipo 802.1x, Autenticación WPA-802.1x o WPA2-802.1x. Recordar que WPA y WPA2 son los nombres utilizados por la Wi-Fi Alliance en sus implementaciones de los mecanismos de autenticación y encriptación definidos en el estándar IEEE 802.11i.
Es importante aclarar el siguiente punto: sin importar el tipo de autenticación que se utilice, el proceso de autenticación Open System se sigue realizando. Obviamente, también se realiza el paso de asociación. Esto se debe a que, antes de cualquier intercambio de mensajes, la estación debe estar asociada al AP y la secuencia es siempre la misma: primero la autenticación, luego la asociación. Sin embargo, el AP no aceptará mensajes de datos del usuario hasta que el proceso de autenticación sea exitoso, solamente procesará los mensajes propios de la autenticación.

2.4.2 Autenticación PSK

Al igual que en WEP, los sistemas configurados para utilizar PSK comparten una misma clave secreta, o pass-phrase, de 8 a 32 caracteres de longitud, ingresada por los usuarios, pero, a diferencia de aquel, no es utilizada directamente para realizar las tareas de encriptación. A partir de esta PSK, los dispositivos derivan la Pairwise Master Key (PMK), que es un número de 256 bits (32 octetos). Como una clave de 32 octetos puede ser muy larga para ser ingresada por el usuario, el sistema puede permitir que se ingrese una clave de menor longitud, a la que el sistema se encargará de expandirla al tamaño correcto.
La PMK no es utilizada directamente por ninguna operación de seguridad, sino que se usa para derivar un conjunto de claves que son las que se emplearán para proteger la comunicación entre dos dispositivos. Aunque representa una gran mejora con respecto a WEP, aún presenta una deficiencia fundamental: la PreShared Key.

2.4.3 Autenticación 802.1x

En ámbitos de trabajo donde la seguridad de las redes no es un tema muy importante, PSK es una alternativa a considerar. En cambio, para redes en las cuales la seguridad es un tema crucial se tiene que pensar en otro tipo de solución. El estándar propone utilizar el protocolo 802.1x. Además de proveer mayor seguridad, la ventaja que presenta es que la validación se puede hacer a nivel de usuario.
802.1x es un mecanismo para controlar el acceso a la red a nivel de puerto, donde un puerto es un punto de acceso a la red. La arquitectura de 802.1x está compuesta por tres entidades funcionales, aunque no es necesario que cada entidad funcional se corresponda con un dispositivo físico:

- Autenticador: este es el puerto que requiere la autenticación antes de permitir el acceso a los servicios accesibles a través de este puerto (por ejemplo, un switch o el AP).
- Servidor de Autenticación: es quien, en nombre del autenticador, toma las decisiones de autorización en base a la información provista por el cliente e indica si es éste un usuario válido o no (por ejemplo, un servidor RADIUS).
- Suplicante: el cliente o usuario que quiere utilizar los servicios ofrecidos por la red (una PC conectada un puerto de un switch).

En redes 802.1x, el acceso a los usuarios está restringido hasta que se validen. Antes que un cliente esté validado por el servidor de autenticación, el autenticador establece el puerto como no controlado (no autorizado). Solamente permite el intercambio de mensajes de autenticación entre el cliente y el servidor de autenticación. Cualquier otro tipo de mensajes está bloqueado. Cuando el suplicante es autenticado exitosamente, el puerto controlado cambia su estado a autorizado y permite todo tipo de tráfico.
802.1x utiliza el protocolo Extensible Authentication Protocol (EAP). No es un protocolo de autenticación en sí mismo sino un framework que define un intercambio de mensajes entre dispositivos. Es utilizado por distintos mecanismos de seguridad para enviar su información de seguridad, entre los que se encuentran: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-OTP (One-Time Password), etc.
El proceso de autenticación se realiza entre el suplicante y el servidor de autenticación. El autenticador, el AP en las redes wireless, es un mero retransmisor de mensajes. El tipo y la cantidad de mensajes intercambiados entre esos dispositivos dependen del mecanismo de seguridad seleccionado. Si el proceso termina exitosamente, el suplicante y el servidor de autenticación contienen la PMK. Sin

embargo, la integridad y la encriptación se realizan entre el suplicante y el autenticador, es por esto que la PMK tiene que ser enviada en forma segura desde el servidor de autenticación al autenticador. A partir de este momento, el suplicante y el autenticador están en condiciones de deducir las Pairwise Transient Keys (**PTK**).

2.4.4 Derivación de las PTKs - 4-way handshake

Tras la autenticación exitosa, la estación y el AP deben generar las PTKs, es decir, las claves temporales de sesión. Además, el AP utiliza este paso para comprobar que la estación realmente conoce la PMK. Este proceso de derivación de las claves temporales, para el que se necesita un total de cuatro mensajes, es muy simple y recibe el nombre de "4-way handshake (saludo de 4 vías)".

Como se puede observar en la figura 2.4, en WPA/WPA2 se utilizan múltiples claves en diferentes niveles. Esta jerarquía comienza con una Pairwise Master Key (PMK), que puede ser derivada en uno de los dos métodos explicados anteriormente. Esta clave no se utiliza directamente para encriptar sino que, a partir de ella, se derivan un conjunto de claves que servirán para proteger una conexión entre un dispositivo móvil y el AP. Dependiendo del método de encriptación que se vaya a utilizar es la cantidad de claves que se derivan. En la figura 2.4 se derivan un total de 4 claves distintas y es la cantidad necesaria cuando se encripta con Temporal Key Integrity Protocol (**TKIP**). En cambio, si la encriptación se hace con Advanced Encryption Standard (**AES**) solamente se necesitan 3 claves.

La pregunta que surge de esto es por qué son necesarias 4 claves. Esto se debe a que hay dos capas o niveles a proteger. Uno es el propio proceso de derivación de las claves, el 4-way handshake, que se explicará a continuación, y el otro es el intercambio de datos de los usuarios. Tener en cuenta que en cada uno de esos niveles se realizan dos funciones criptográficas: integridad y encriptación.

Estas claves son temporales porque son generadas cada vez que el dispositivo móvil se asocia al AP. El conjunto de claves, que se conoce como PTK, es único para cada asociación entre un AP y un dispositivo móvil y se deriva a partir de los siguientes datos: la PMK, conocida por los dos dispositivos, direcciones MAC de ambos dispositivo, y dos números pseudoaletarios generados cada uno por cada dispositivo. Todo este proceso se explica detalladamente a continuación.

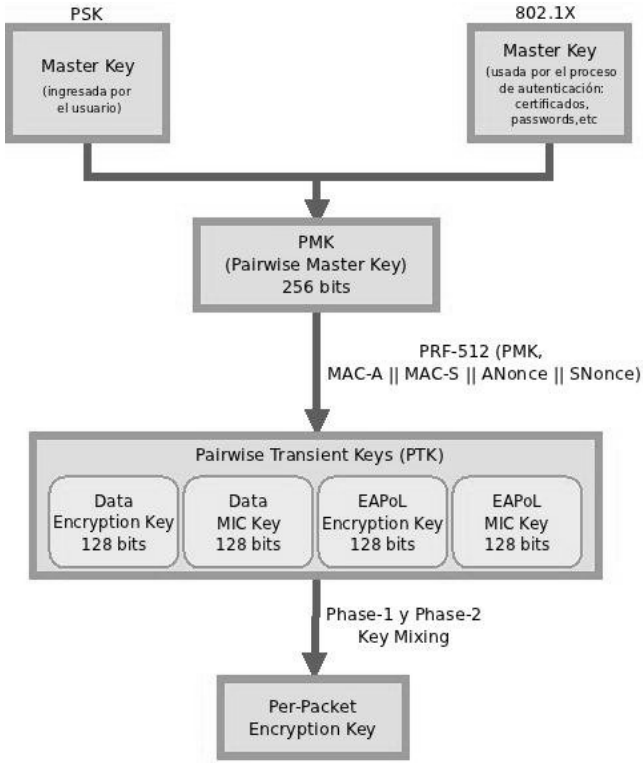


Figura 2.4 Derivación de la jerarquía de claves

Antes de empezar el intercambio, cada nodo debe generar un valor random llamado *nonce.* Estos valores son independientes, no hay relación entre ellos. El nonce generado por el Autenticador, o AP, se llama **ANonce** y el del Suplicante, **SNonce.**

El primer mensaje lo envía el Autenticador al Suplicante. Este mensaje no está encriptado ni protegido contra adulteraciones del contenido. Esto tiene que ser así porque los nodos todavía no conocen las claves. Si el mensaje es modificado, el proceso fallará más adelante. El contenido del mensaje es el siguiente:

```
.....
802.11 MAC Header
  Version:              0
  Type:                 %10  Data
  Subtype:              %0000  Data Only
Frame Control Flags:    %00000010
                        0... .... Non-strict order
                        .0.. .... WEP Not Enabled
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..1. Exit from the Distribution System
                        .... ...0 Not to the Distribution System
```

```
  Destination:          00:0E:35:DF:14:90
  BSSID:                00:0F:F8:58:B5:D6
  Source:               00:0F:F8:58:B5:D6
  Seq. Number:          1307
  Frag. Number:         0
802.2 Logical Link Control (LLC) Header
  Dest. SAP:            0xAA  SNAP
  Source SAP:           0xAA  SNAP
  Command:              0x03  Unnumbered Information
  Vendor ID:            0x000000
  Protocol Type:        0x888E  802.1x Authentication
802.1x Authentication
  Protocol Version:     1
  Packet Type:          3  EAPOL - Key
  Body Length:          95
EAPOL - Key
  Type:                 254  SSN key descriptor
  Key Information:      %0000000010001001
                        xxx. .... .... .... Reserved
                        ...1 .... .... .... Pairwise Key
                        .... 00.. .... .... Key index 0
                        .... ..0. .... .... Not Install/Tx
                        .... ...1 .... .... Ack
                        .... .... 0... .... Not MIC
                        .... .... .0.. .... Not secure
                        .... .... ..0. .... No Error
                        .... .... ...0 .... Not Request
                        .... .... .... xxxx Reserved
  Key Length:           32
  Replay Counter:       0x0000000000000001
  Key Nonce:            0x1F9731AA0F30840AA5BB432157E61B1FF9940DE644806…
  Key IV:               0x00000000000000000000000000000000
  Key Sequence Counter: 0x0000000000000000
  Key ID:               0x0000000000000000
  Key MIC:              0x00000000000000000000000000000000
  Key Data Length:      0x0000
FCS - Frame Check Sequence
  FCS (Calculated):     0xA3ABC39F
```

Entre los campos más interesantes se encuentran los siguientes:

- **Type:** 254
  Valor único que indica que el descriptor es WPA.
- **Packet Type:** 3
  Indica que el paquete es del tipo EAPOL-Key.
- **Key Information:**

```
xxx. .... ....          Reserved
...1 .... .... ....     Pairwise Key
.... 00.. .... ....     Key index 0
.... ..0. .... ....     Not Install/Tx
.... ...1 .... ....     Ack
.... .... 0... ....     Not MIC
.... .... .0.. ....     Not secure
.... .... ..0. .... .   No Error
.... .... ...0 ....     Not Request
.... .... ... xxxx      Reserved
```

  Este campo ocupa 2 bytes y contiene varios sub-campos que proveen información del tipo de clave y como debería ser usada. También contiene varios bits de control que son usadas por el procedimiento de intercambio de clave. Los campos seteados a 1 son los siguientes:

- **Pairwise Key:** indica si el mensaje de clave es del tipo pairwise o de grupo. Es decir, si el frame es parte del proceso 4-way handshake para derivar la PTK.
- **Ack:** el Autenticador requiere que el Suplicante le conteste con un mensaje EAPOL-Key. La respuesta debe usar el mismo valor Replay Counter que este mensaje. Si ninguna respuesta es recibida antes de que se venza el timeout, el autenticador puede reenviar el mensaje (hasta 3 veces). Los mensajes reenviados deben tener el valor del campo Replay Counter igual al valor del mensaje original porque, si el suplicante recibió el mensaje original, puede deducir que se trata de un duplicado.

- **Key Length:** 32
  Indica la longitud de la Pairwise Temporal Key en bytes. Ocupa dos bytes de longitud. Además, la longitud de la clave define que cipher-suite se debe usar (32 = TKIP, 16 = CCMP, 5 = WEP-40, 13 = WEP-104).
- **Replay Counter:** 0x0000000000000001
  Este campo ocupa 8 byte y es inicializado a cero. Se utiliza para detectar frames duplicados. Su valor es incrementado con cada nuevo paquete, excepto cuando el frame es en respuesta a una solicitud de ACK. En este caso, el valor del campo es igual al valor del Replay Counter del frame que solicitó el ACK.
- **Key Nonce:** 0x1F9731AA0F30840AA5BB432157E6…..
  Este campo tiene una longitud de 32 bytes y contiene el ANonce generado por el Autenticador
- **Key IV:** 0x00000000000000000000000000000000
  Contiene el Initialization Vector utilizado con KEK (EAPOL-Key Encryption Key). Si no se necesita, su valor debe ser cero. Ocupa 16 bytes.
- **Key Sequence Counter:** 0x0000000000000000
  Este campo tiene 8 bytes de longitud. Contiene el contador de secuencia recibido (RSC, Receive Sequence Counter) para el Group Temporal Key que está siendo instalado
- **Key ID:** 0x0000000000000000.
  Este campo no es usado en WPA. Está reservado y ocupa 8 bytes.
- **Key MIC:** 0x00000000000000000000000000000000
  Este campo contiene el valor de chequeo de integridad (MIC, Message Integrity Check) y ocupa 16 bytes de longitud.

- **Key Data Length:** 0x0000
  Este campo ocupa 2 bytes de longitud. Contiene, en bytes, la longitud del campo Key Data.

Al recibir el frame, el Suplicante controla que los valores de los campos tengan un valor determinado. Si alguno de los valores no son los esperados, el frame será descartado. Los únicos campos que pueden tener valores distintos a 0 son el Replay Counter y el ANonce. Si alguien modifica el Replay Counter, el frame debería ser rechazado. Si modifica el ANonce, el Suplicante obtendrá claves temporales erróneas y el proceso entero fallará. Por lo tanto, que el mensaje no esté protegido no compromete la seguridad.

Después de recibir el mensaje y comprobar que es correcto, el Suplicante tiene una copia del ANonce. Con este nonce más su propio nonce, las direcciones MAC (origen y destino) y la PMK es capaz de generar las claves temporales o PTKs. Luego, le envía la contestación al Autenticador. Este mensaje tampoco se encripta, pero, usando la clave EAPOL-Key Integrity, se calcula y envía el valor de chequeo de integridad (MIC). Con esto, además de prevenir que alguien modifique el mensaje sin ser detectado, el Suplicante le prueba al Autenticador que conoce la PMK. Este es el contenido del mensaje:

```
.....
802.1x Authentication
  Protocol Version:      1
  Packet Type:           3  EAPOL - Key
  Body Length:           121
EAPOL - Key
  Type:                  254  SSN key descriptor
  Key Information:       %0000000100001001
                         xxx. .... .... .... Reserved
                         ...1 .... .... .... Pairwise Key
                         .... 00.. .... .... Key index 0
                         .... ..0. .... .... Not Install/Tx
                         .... ...0 .... .... Not ACK
                         .... .... 1... .... MIC
                         .... .... .0.. .... Not secure
                         .... .... ..0. .... No Error
                         .... .... ...0 .... Not Request
                         .... .... .... xxxx Reserved

  Key Length:            0
  Replay Counter:        0x0000000000000001
  Key Nonce:             0x45A04DD1A2B5F1C6492CA7F44D726E5CB84EC9C138…
  Key IV:                0x00000000000000000000000000000000
  Key Sequence Counter:  0x0000000000000000
  Key ID:                0x0000000000000000
  Key MIC:               0x7D190C06535C23B272D957091D1C77E8
  Key Data Length:       0x001A
  OUI:                   0x00-0x50-0xF2-0x01
  Version:               0001
  Multicast cipher OUI:  0x00-0x50-0xF2-02  TKIP
  Number of unicast      0001
  Unicast cipher OUI:    0x00-0x50-0xF2-02  TKIP
  Number of auth         0001
  Auth OUI:              0x00-0x50-0xF2-02  SSNPSK

.....
```

Los siguientes son los campos más relevantes del frame:

- **Key Information**
  En este mensaje, el Suplicante utiliza dos sub-campos para proveerle cierta información al Autenticador:
  - **Error:** como en el mensaje anterior no hubo MIC, se indica que no hubo error de integridad.
  - **MIC:** setea a 1 el valor de este sub-campo para indicar que se está utilizando el cheque de integridad.
- **Key Length:** 0
  No indica el tipo de cipher-suite porque ya lo hizo el Autenticador.
- **Replay Counter:** 0x0000000000000001
  Debe ser igual al valor del mismo campo del mensaje anterior.
- **Key Nonce:** 0x45A04DD1A2B5F1C6492CA7F44D726...
  SNonce del Suplicante. Es utilizado por el Autenticador para calcular sus claves temporales.
- **Key MIC:** 0x7D190C06535C23B272D957091D1C77E8
  Contiene al resultado del chequeo de integridad.

Además, el Suplicante incluye, dentro del mensaje, toda la información de seguridad que se negoció durante la fase de autenticación. Esto lo hace para evitar que otro dispositivo móvil modifique los parámetros de seguridad después de la negociación inicial.

Al recibir el mensaje, el Autenticador aún no ha calculado las claves temporales porque no conoce el SNonce. Debe hacerlo para poder comprobar la integridad del mensaje. Como no está encriptado, el SNonce puede ser extraído. Con el conocimiento de ambos nonces, el Autenticador puede calcular las claves temporales. Luego, usando la clave correspondiente, debe verificar el valor del MIC. Solo continúa a la siguiente fase si el resultado de este paso es correcto.

En este punto, ambos lados han derivado las cuatro claves temporales (o 3 dependiendo del proceso de seguridad elegido) y el Autenticador ha verificado que el Suplicante conoce la PMK. Sin embargo, ninguno de los dispositivos ha comenzado a encriptar. Los dos mensajes siguientes son utilizados para asegurar que las claves se instalen en forma sincronizada.

El tercer mensaje es enviado por el Autenticador para indicarle al Suplicante que ya está listo para comenzar a encriptrar. Es necesario coordinar esta operación para que ninguno de los dispositivos comience a encriptar antes que el otro esté listo. Si esto no se cumple, la conexión se rompe. El contenido del mensaje se muestra a continuación:

```
.....
802.1x Authentication
  Protocol Version:      1
  Packet Type:           3  EAPOL - Key
  Body Length:           119
EAPOL - Key
  Type:                  254  SSN key descriptor
  Key Information:       %0000000111001001
                         xxx. .... .... .... Reserved
                         ...1 .... .... .... Pairwise Key
                         .... 00.. .... .... Key index 0
                         .... ..1. .... .... Install/Tx
                         .... ...1 .... .... Ack
                         .... .... 1... .... MIC
                         .... .... .0.. .... Not secure
                         .... .... ..0. .... No Error
                         .... .... ...0 .... Not Request
                         .... .... .... xxxx Reserved

  Key Length:            32
  Replay Counter:        0x0000000000000002
  Key Nonce:             0x1F9731AA0F30840AA5BB432157E61B1FF9940DE644806…
  Key IV:                0x00000000000000000000000000000000
  Key Sequence Counter: 0x0000000000000000
  Key ID:                0x0000000000000000
  Key MIC:               0xD7A20E6AA74B6F7804060CAA400438E9
  Key Data Length:       0x0018
  OUI:                   0x00-0x50-0xF2-0x01
  Version:               0001
  Multicast cipher OUI: 0x00-0x50-0xF2-02  TKIP
  Number of unicast      0001
  Unicast cipher OUI:    0x00-0x50-0xF2-02  TKIP
  Number of auth         0001
  Auth OUI:              0x00-0x50-0xF2-02  SSNPSK
.....
```

Este mensaje es similar a los intercambiados anteriormente, y los siguientes son los campos más importantes:

- **Key Information**
  El Autenticador utiliza el siguiente sub-campo para pasarle información al Suplicante:
  - **Install/Tx:** le indica al Suplicante que debe instalar sus claves temporales para comenzar a encriptar.
- **Key Secuence Number:** 0x0000000000000000
  Este campo le indica al nodo móvil cual es el número de secuencia inicial que el Autenticador intentará usar. Normalmente es cero.

Si el valor del campo Replay Counter ya ha sido usado o si el valor del ANonce de este mensaje es distinto del que recibió en el primer mensaje del proceso, el Suplicante debe descartar el frame de forma silenciosa. Lo mismo sucede si la información de seguridad recibida no coincide con la negociada al principio de la conexión.

Hasta que no reciba el último mensaje, el Autenticador no instala las claves temporales para encriptar. Si lo hiciese después de enviar el tercer mensaje podría suceder que este tuviese que ser reenviado. Al

haber instalado las claves, el reenvío iría encriptado y el Suplicante no sería capaz de desencriptarlo. No tiene las claves instaladas. Lo hace al recibir la indicación en el tercer mensaje del proceso.
El último mensaje, sin encriptar, finaliza el proceso de handshake y es enviado desde el Suplicante para indicar que va a instalar las claves y, por lo tanto, comenzará a encriptar. Al recibir este mensaje, el Autenticador también instala sus claves y, en consecuencia, sus próximos mensajes estarán todos encriptados. A continuación se muestra el último mensaje.

```
.....
802.1x Authentication
  Protocol Version:     1
  Packet Type:          3  EAPOL - Key
  Body Length:          95
EAPOL - Key
  Type:                 254  SSN key descriptor
  Key Information:      %0000000100001001
                        xxx. .... .... .... Reserved
                        ...1 .... .... .... Pairwise Key
                        .... 00.. .... .... Key index 0
                        .... ..0. .... .... Not Install/Tx
                        .... ...0 .... .... Not ACK
                        .... .... 1... .... MIC
                        .... .... .0.. .... Not secure
                        .... .... ..0. .... No Error
                        .... .... ...0 .... Not Request
                        .... .... .... xxxx Reserved

  Key Length:           0
  Replay Counter:       0x0000000000000002
  KeyNonce:             0x0000000000000000000000000000000000000000…
  Key IV:               0x00000000000000000000000000000000
  Key Sequence Counter: 0x0000000000000000
  Key ID:               0x0000000000000000
  Key MIC:              0x6D92302DADD4700A25B2C7D9B01BF133
  Key Data Length:      0x0000
.....
```

El contenido del mensaje es similar a los anteriores. El valor del campo Replay Counter es igual al recibido en el tercer mensaje y, además, se calcula y envía el MIC.
Si durante este intercambio de mensajes un atacante modifica el contenido de los nonces, los dispositivos generarán claves diferentes y, como resultado, el chequeo de integridad de los mensajes fallará.
A partir de este momento, el Autenticador y el Suplicante han obtenido, calculado e instalado las claves para encriptar y calcular la integridad de los mensajes que intercambien. Además, el AP le envía encriptada la clave de grupo. Ésta es utilizada por el AP para encriptar los mensajes broadcast o multicast. Recordar que cada estación que se une a la red genera su propio conjunto de PTKs.

2.5 Encriptación

El estándar define dos nuevos métodos de encriptación. Uno, llamado Temporal Key Integrity Protocol (TKIP) soluciona las deficiencias que existen en WEP. El otro método, desarrollado desde cero, se basa en el estándar de encriptación recomendado por los Estados Unidos: Advanced Encryption System (AES).

2.5.1 TKIP (Temporal Key Integrity Protocol)

TKIP, como su nombre lo indica, es una solución intermedia y existe por una razón, permitir a los sistemas WEP actualizarse para volver a ser seguros hasta que un nuevo procedimiento de seguridad realmente fuerte fuese introducido. Una actualización del firmware es todo lo que se necesita para que el protocolo TKIP sea implementado. Teniendo que utilizar muchas características heredadas de WEP, entre ellas, la implementación de RC4 en hardware, la solución no consiste en el reemplazo de WEP sino en agregar un conjunto de herramientas correctivas alrededor del hardware. A continuación se muestran los cambios de WEP a TKIP:

- TKIP usa un procedimiento de handshake (saludo) que consiste en el intercambio de mensajes para generar claves nuevas.
- Incrementa el tamaño del Initialization Vector (IV) de 24 a 48 bits.
- TKIP define un proceso de dos pasos para generar una nueva clave en cada MSDU que se encripta (TKIP Key Mixing).
- Un algoritmo de integridad especialmente diseñado llamado Michel es usado para la protección de integridad de los MSDUs.
- Indica claramente como se debe inicializar e incrementar el valor del IV para detectar ataques conocidos como “replay attack”.

La colisión de claves, por la reutilización del IV, y la generación de claves débiles eran dos de las fallas detectadas en WEP. Para solucionar el primero de los problemas se incrementó a 48 bits el tamaño del IV. Este contador siempre debe comenzar en 1 e incrementarse monótonamente. Si en algún momento se agotan los valores del IV, se lo reinicia y las claves de sesión se deben generar nuevamente. Además, se agrega un byte más al IV, llamado “dummy byte” (en la figura 2.5 se representa con una letra d), para evitar que se generen claves débiles.

La prevención de “replay attacks” se hace con el TKIP Sequence Counter (TSC), que es el IV. Se incrementa en 1 por cada nuevo frame

que se envía, excepto en las retransmisiones que se mantiene igual al del mensaje original (el receptor detecta que es una retransmisión porque tiene el bit de duplicado seteado a 1). Un nodo no acepta un mensaje con un TSC igual o menor al anterior recibido.
TKIP, mediante un proceso de dos fases llamado "per packet key mixing" evita que una clave se reutilice para encriptar dos mensajes diferentes. Cada fase soluciona una falla específica de WEP. La primera fase elimina la posibilidad de usar la misma clave en distintos dispositivos al utilizar el valor del campo Address 2 de un frame 802.11, que es la dirección del transmisor, y la segunda suprime la relación entre el IV y la clave de encriptación de cada frame. Además, al utilizar una clave para cada paquete enviado, se resuelve el problema de ataque FMS.
Por último, para mejorar el mecanismo de integridad de los paquetes se desarrolló un nuevo nuevo algoritmo conocido como Michael. Éste es un algoritmo hash que no usa operaciones complejas para realizar los cálculos sino que lo hace mediante operaciones simples (sumas y corrimientos). Si bien ofrece una defensa débil contra la alteración de mensajes es lo mejor que se pudo lograr que funcione eficazmente con la mayoría del hardware heredado. TKIP MIC, que tiene un tamaño de 8 bytes, mejora el desempeño de WEP ICV pero no lo reemplaza. Éste se sigue calculando pero cumple otras funciones. Ayuda a evitar detecciones falsas de fallas en MIC que provocarían que las medidas para prevenir ataques sean invocadas.
La clave para calcular el MIC se obtiene del proceso "4-way handshake". Si alguien modifica un paquete debe conocer esta clave para regenerar el MIC y, así, lograr que dicha alteración no sea detectada por el receptor. Si existen más de dos fallas en un lapso no mayor de 60 segundos en mensajes recibidos del mismo receptor, éste debe ser desasociado, esperar un minuto y asociarlo nuevamente. Esto dificulta el accionar del atacante porque no le permite realizar muchos ataques en un corto plazo. Como una medida de seguridad adicional, se deben regenerar las claves de encriptación e integridad.
En la figura 2.5 se muestra el proceso realizado por TKIP. Como se puede observar es más complejo que el realizado por WEP, especialmente todo el trabajo previo a la encriptación. El módulo WEP sigue existiendo, pero la información que recibe lo hace menos vulnerable a ataques. La primera fase, Per-Packet Key Mixing - Fase 1, trabaja con la mayoría de datos estáticos: la MAC del transmisor, la clave secreta de sesión y los primeros 32 bits del IV. Este último valor cambia cada 2^{16} paquetes que se encriptan, por lo tanto, esta fase se tiene que recalcular en ese momento. Por su parte, en la fase 2 se incluye la parte que cambia por cada paquete que se encripta, los 16 bits de más bajo orden del IV.

La dirección MAC del transmisor se incluye para evitar que se produzcan colisiones entre dos dispositivos que se están comunicando y utilizan una clave de sesión compartida (recordar que en proceso 4-way handshake ambos dispositivos deducen las mismas claves). Si los dos nodos utilizan el mismo IV y la misma clave compartida se producirán colisiones de IV. Por la tanto, al incluir la dirección MAC dentro de la generación del proceso per-packet key se resuelve este problema.
Por otro lado, el proceso Michael para calcular la integridad se calcula sobre el MSDU, no sobre cada uno de los MPDUs, a diferencia de la encriptación que si se calcula sobre los MPDUs. Al computar la integridad en el MSDU no es posible incluir el valor del IV en el cálculo del MIC. Michel utiliza su propia clave secreta que es distinta de la que se utiliza para encriptar.

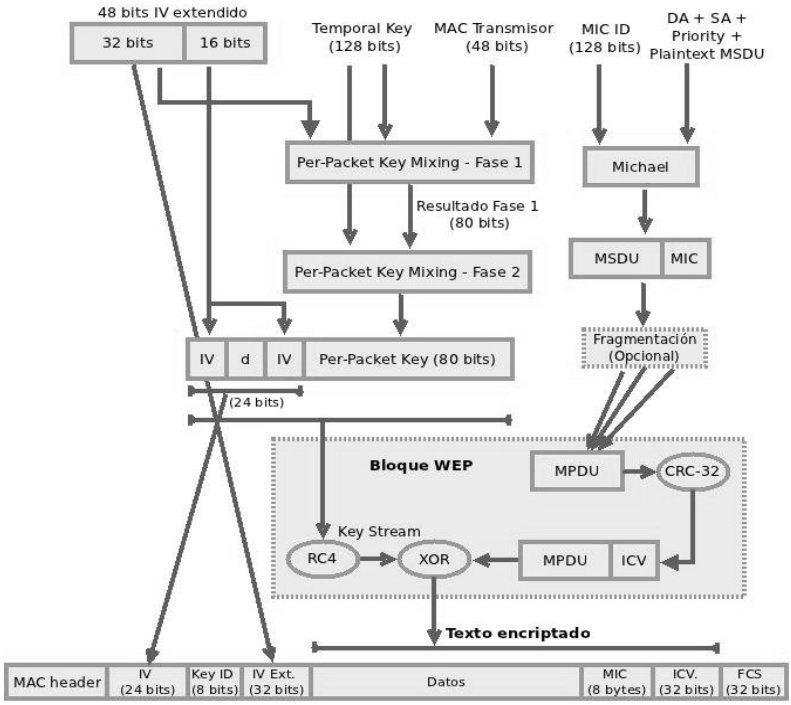


Figura 2.5 Proceso de encriptación e integridad en TKIP

Todo el proceso anterior queda reflejado en la composición del siguiente frame encriptado con TKIP. En la parte de los flags se utiliza el mismo que se usaba con WEP para indicar que el frame está encriptado.
.....

```
802.11 MAC Header
  Version:              0
  Type:                 %10  Data
  Subtype:              %0000  Data
Frame Control Flags:    %01000010
                        0... .... Non-strict order
                        .1.. .... Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..1. Exit from the Distribution System
                        .... ...0 Not to the Distribution System
  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF
  BSSID:                00:0F:F8:58:B5:D6
  Source:               00:0E:35:DF:14:90
  Seq Number:           1871
  Frag Number:          0
802.11 Encrypted Data
  IV:                   0x0121BE
  Key Index:            %01100000
                        01.. .... Key Index 2
                        ..1. .... Has Extended IV
                        .... xxxx Reserved
  Extended IV:          0x00000000
  Encrypted Data:
  .... !.........  B9 91 E0 E9 20 21 BD BE 9D 03 0D F7 EF CC FF DF  [28-43]
  .U.q..n......../  F3 55 AD 71 9C 89 6E 93 FC 87 E4 E5 1D CB D7 2F  [40-55]
  .......Y.X7.3x..  A4 7F E4 BE 07 B3 BB 59 AB 58 37 86 33 78 A4 AE  [52-67]
  ._,L.:..4.F.....  13 5F 2C 4C 8D 3A F8 0A 34 A8 46 92 AE 98 1B 11  [64-79]
  3.                33 A7  [76-77]
FCS - Frame Check Sequence
  FCS:                  0x0892FD87
```

Debido a que el IV aumenta de 24 a 48 bits, también es necesario extender el tamaño del frame en 4 bytes (además de los 8 bytes que se extendió para contener el MIC) para que pueda contener los 3 bytes del nuevo IV más el byte conocido como "WEP seed" o "dummy byte". A continuación se explican los campos más significativos del frame.

- **IV:** 0x0121BE
  Representan los dos bytes menos significativos del IV junto con el "dummy byte" o "WEP seed", que en este caso es el valor 0x21.
- **Key Index:**
  - **01.. …. Key Index 2**
    Indica cuál es la clave que se usó para encriptar, que es la que debería usar el receptor para desencriptar el frame.
  - **..1……. Has Extended IV**
    Permite que el receptor determine si la parte extendida del IV se está transfiriendo, es decir, si se está utilizando TKIP o no. Al estar en 1, se está utilizando TKIP.
- **Extended IV:** 0x00000000
  Contiene los 4 bytes más significantes del IV.

- **MIC:** 0x73FF538C5B154226
  Resultado de aplicar el algoritmo Michael al frame. 8 bytes de longitud. Observar que además del MIC, WEP sigue calculando el WEP ICV.

2.5.2 AES (Advanced Encryption System)

Sin dudas, TKIP provee una gran mejora a WEP, pero sigue teniendo problemas o vulnerabilidades. Por esto, los ingenieros de la IEEE decidieron utilizar un algoritmo de encriptación de bloques cuando rediseñaron la seguridad de 802.11. Como el cifrador de bloque considerado más seguro en aquel momento era AES, y aún lo es, su elección fue más que obvia. AES no es un protocolo de seguridad, es un cifrador. En una red RSN, el protocolo de seguridad desarrollado en torno a AES es llamado Counter Mode-CBC MAC Protocol (CCMP). En decir, CCMP define las reglas que utiliza AES para habilitar la encriptación y la protección de los frames de datos 802.11. AES también está incluido en WPA2.
AES, que está basado en el algoritmo Rijndael, es un cifrador de bloque simétrico que utiliza operaciones lógicas y matemáticas. Puede operar con distintos tamaños de bloque y longitudes de claves, pero 802.11i establece que se deben usar bloques y claves con un tamaño de 128 bits. Para proveer confidencialidad, AES es usado en "counter mode". Este modo requiere un contador que comienza en un valor predeterminado y se incrementa en una manera específica por cada bloque a encriptar. El cifrador AES es usado para encriptar el contador, no el bloque de datos, dando como resultado un keystream de 128 bits. Éste es utilizado para realizar un XOR con un bloque de datos de 128 bits tomado del mensaje original. Por cada bloque del mensaje original, el contador se incrementa. Esto se hace para evitar el problema de los cifradores de bloque que es que el resultado de encriptar un mismo bloque es siempre igual.
La otra parte de la seguridad es la integridad del mensaje. CCMP utiliza "counter mode" en conjunto con un método de autenticación de mensajes llamado "cipher block chaining (CBC)" que es utilizado para producir un "message integrity code (MIC)". Como al MIC se lo conoce como "message authentication code (MAC)" se deduce el nombre CBC-MAC.
Al igual que los protocolos anteriores, CCMP encripta la parte de datos únicamente, no el header. A cada frame a transmitir le agrega 16 bytes de campos adicionales. Pero, a diferencia de TKIP, en la jerarquía de claves solo se necesitan 3 claves porque CCMP utiliza la misma clave para encriptar y para calcular la integridad de los

mensajes de datos del usuario. Las otras dos claves se utilizan en el proceso 4-way handshake, igual que en TKIP.
Al igual que en TKIP, Address2 es la dirección del transmisor.
El header CCMP se transmite en texto claro y tiene dos propósitos. Primero, provee el "Packet Number", de 48 bits, que sirve para detectar "replay attacks" y ayuda al receptor a derivar el valor del "nonce" usado en la encriptación. Segundo, en el caso de multicast, le indica al receptor que "group key" fue utilizada.
Por último, el "Additional Authentication Data (AAD)" se compone de determinados campos del header del frame que deben ser autenticados por el receptor, pero no pueden estar encriptados. Permite, al receptor, comprobar que esos campos no han sido alterados por nadie. En la figura 2.6 se muestra el proceso realizado por AES/CCMP para brindar seguridad a las redes wireless.

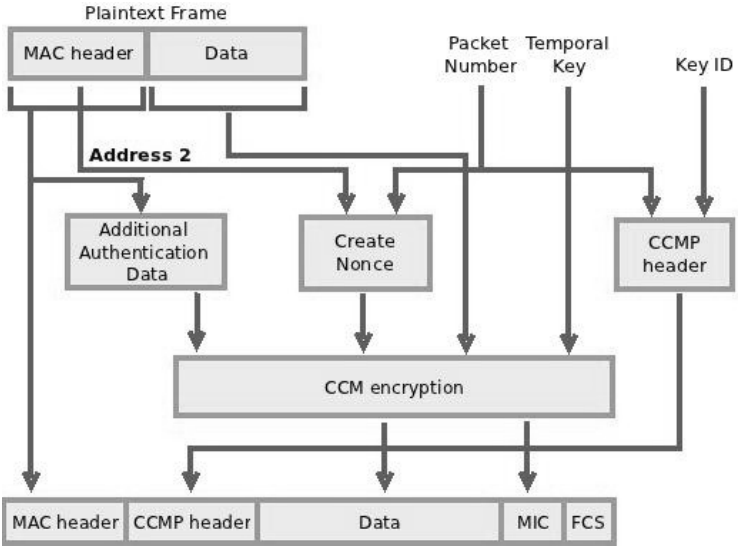


Figura 2.6 Proceso de encriptación e integridad en AES/CCMP

CAPÍTULO 3

Bluetooth

3.1 Introducción

En el año 1994, en Suecia, la empresa de telecomunicaciones Ericsson Mobile Communications comenzó a investigar la factibilidad de una interface de radio de bajo costo y poca potencia con el fin de conectar los teléfonos móviles con sus accesorios sin la necesidad de utilizar cables. Esta investigación causó el interés de otras empresas como IBM, Intel, Nokia y Toshiba, que junto con Ericsson, formaron, en 1998, el "Bluetooth Special Interest Group (SIG). En diciembre de ese mismo año, el SIG incorporó a Microsoft, Lucent, 3Com y Motorola. A esta sociedad se la conoce como "SIG Promoters". En la actualidad más de 14000 miembros.

Esta nueva tecnología wireless fue denominada con el nombre código "Bluetooth" en honor al rey vikingo danés Harald Blåtand (Blåtand significa, traducido al inglés como, "blue tooth" (diente azul)), que gobernó Dinamarca entre los años 940 a 985 y fue quien unificó al país. En 1998, el SIG adoptó el nombre Bluetooth definitivamente.

El Bluetooth SIG quería hacer que la IEEE adopte la especificación de Bluetooth y la convierta en un estándar IEEE 802. La IEEE estableció el grupo 802.15 para las WPAN, Wireless Personal Area Networks, que cubren las redes de bajo costo, poca potencia y cobertura pequeña. Entre sus actividades se encuentra el "working group" 802.15.1 para la especificación de Bluetooth.

La primera especificación de Bluetooth es la 0.7 del año 1998 que incluía únicamente la Baseband y el Link Manager Protocol. En las siguientes especificaciones, 0.8 y 0.9, se fueron agregando nuevas partes como Radio Specification, L2CAP, RFCOMM, SDP, etc. En julio de 1999 se publicó, por primera vez, una especificación, la 1.0, en el sitio web público de Bluetooth. La versión 1.1 actualizó la 1.0 con una "fe de errata". En la 1.2 de Noviembre de 2003 se produjo un gran cambio en la estructura del documento, además de agregarle nuevas partes y funcionalidades, al dividirlo en volúmenes. En 2004, se publicó la versión 2.0 + EDR, la cual fue actualizada en Julio de 2007 por la versión 2.1 + EDR. Una nueva versión se publicó en Abril de 2009, la 3.0 + HS, que define un nuevo controlador de alta velocidad: AMP. La última especificación es de Junio de 2010, la 4.0, y agrega una nueva característica: Low Energy (LE)

3.2 Arquitectura Bluetooth

La tecnología wireless Bluetooth [BLUE] ha sido optimizada para dispositivos personales de tamaño pequeño con el fin de ser utilizada en enlaces de alcance corto. Existen dos sistemas dentro de esta tecnología: Basic Rate (BR) y Low Energy (LE). Ambos permiten los procesos de descubrimiento de dispositivos, establecimiento de conexiones y mecanismos de control. BR, por su parte, incluye el Enhanced Data Rate (EDR) y el Alternate Media Access Control and Physical (AMP) como características opcionales. A su vez, LE está diseñado para ser utilizado por dispositivos y aplicaciones que requieran velocidades de datos más bajas, con menor consumo de batería y de menor costo que BR.
El núcleo del sistema Bluetooth cubre las cuatro capas más bajas de la especificación: Radio, BaseBand, Link Manager y L2CAP (nombradas en orden desde abajo hacia arriba y que serán explicadas más adelante), junto con los protocolos de control asociados, además de determinados protocolos, como por ejemplo: Service Discovery Protocol (SDP) y Generic Access Profile (GAP). Está dividido en dos grandes subsistemas: Host y Controladores (Controller). El subsistema Host consiste de la parte lógica definida por sobre el Host-to-Controller Interface (HCI) y por debajo de las aplicaciones de los usuarios. Por su parte, el Controlador, que también es una entidad lógica, se encuentra por debajo del HCI y ocupa las 3 capas inferiores, todas menos L2CAP. El HCI es opcional y, en caso de existir, sus funcionalidades pueden encontrarse en una capa individual o pueden estar repartidas entre el Host y el Controlador. Se definen dos tipos de controladores: Controladores Primarios y Controladores Secundarios. Una implementación de Bluetooth debe tener un único controlador primario que puede tener una de las siguientes configuraciones:

- Controlador BR/EDR
- Controlador LE
- Controlador BR/EDR y Controlador LE combinados

Además, puede tener 0, 1 ó más controladores secundarios:

- Controlador Alternate MAC/PHY (AMP)

En la figura 3.1 se pueden observar distintas combinaciones entre los dos tipos de controladores, no siendo estas únicas posibles.

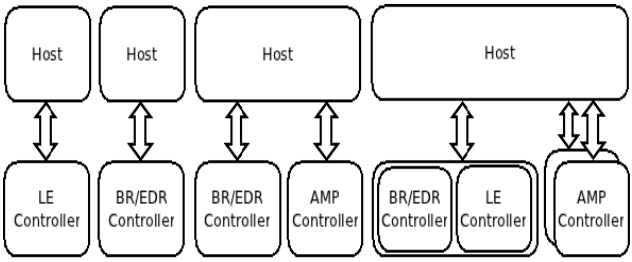


Figura 3.1 Combinación de controladores[4]

La figura 3.2 muestra la arquitectura de Bluetooth que, en comparación con otras arquitecturas, es bastante más compleja. No es necesario que una implementación se corresponda en forma exacta con esta arquitectura. Como se puede observar, está dividida en dos grandes componentes, Host y Controlador (Controller), separados por la interface opcional HCI. De los tres controladores existentes, BR/EDR es el que existe desde el principio de la especificación y es el más utilizado en la actualidad, por lo tanto, es el que se va a explicar con mayor detalle. Una breve explicación de los otros dos modos se encuentra el final del capítulo.

El funcionamiento del sistema Bluetooth está dividido en bloques o capas que se comunican entre ellos mediante mensajes pertenecientes a distintos protocolos de señalización o control. Además, cada capa intercambia mensajes con las capas equivalentes en otros dispositivos para lograr interoperabilidad entre distintos sistemas Bluetooth. También están definidos en la especificación Bluetooth los mensajes intercambiados entre el Host y cada una de las Controladoras que, en caso de estar implementada, este intercambio es a través de la capa HCI. En la figura 3.2, las flechas más claras indican los mensajes de control o señalización y las oscuras los mensajes de datos.

Además, el sistema ofrece servicios a los demás componentes de la arquitectura a través de un número de puntos de acceso al servicio que en el diagrama se muestran como elipses. Estos servicios son los que permiten el control del sistema Bluetooth y se los puede dividir en 3 grupos, de los cuales los dos primeros pertenecen al plano de control (C-plane) y el otro al plano de usuario (U-plane):

- Servicios de control del dispositivo: permiten modificar el funcionamiento y el modo del dispositivo.
- Servicios de control del transporte: crean, modifican y liberan los links y canales por donde se envía y recibe el tráfico.

[4] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

- Servicios de datos: usados para enviar datos para transmitirlos por los canales y links definidos por los servicios de control de transporte.

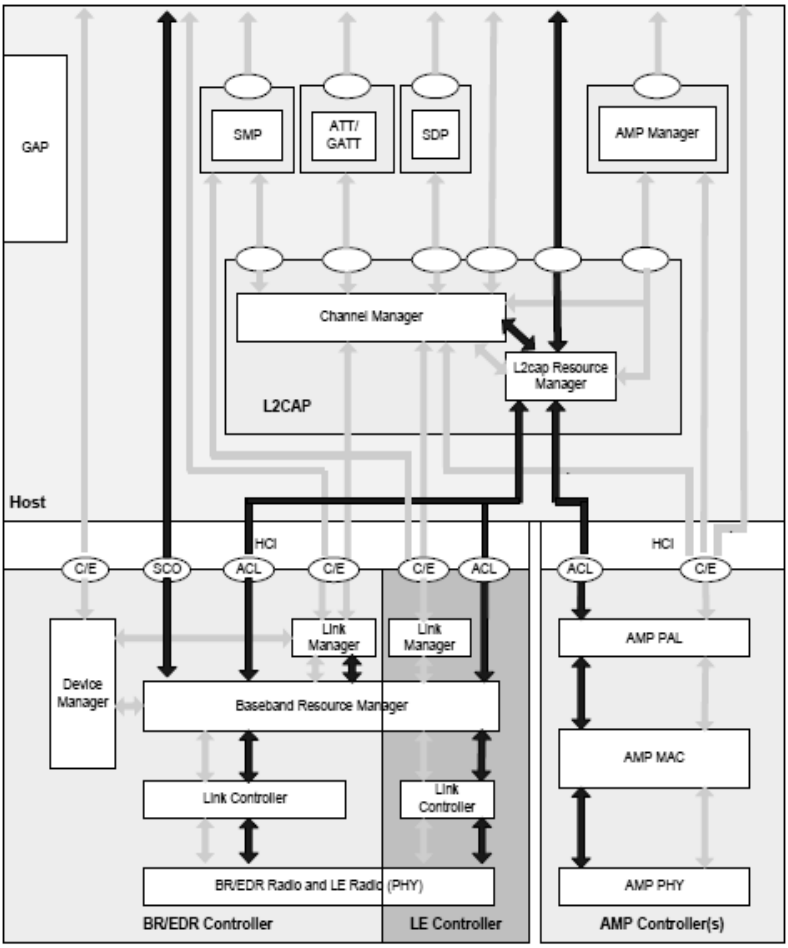


Figura 3.2 Arquitectura Bluetooth correspondiente a la especificación 4.0[5]

Al definir la arquitectura de Bluetooth con la posibilidad de separarla en Host y Controlador comunicadas por el HCI es necesario hacer algunas suposiciones: el controlador tendrá una cantidad de memoria limitada (por ejemplo, el controlador se implementará en hardware) en comparación con el Host lo cual hará que tenga capacidades limitadas de buffering. Esta funcionalidad deberá ser llevada a cabo por otra capa que, obviamente, estará ubicada en el Host.

[5] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

3.2.1 Host y Controlador: bloques componentes

A continuación se definen los bloques componentes de la arquitectura de Bluetooth que se muestran en el diagrama. Sólo se explicarán, tanto en la parte del Host como en la del Controlador, los pertenecientes al modo ER/BDR. Dentro del subsistema Host se encuentran los siguientes:

- Channel Manager (Administrador de canales): es el responsable de crear, administrar y cerrar los canales L2CAP utilizados para el transporte de los datos de las aplicaciones. Para realizar su trabajo usa el protocolo L2CAP que le permite interactuar con el channel manager de los dispositivos vecinos
- L2CAP Resource Manager (Administrador de recursos L2CAP): es el responsable de administrar el envío ordenado de los PDUs a la Baseband. Además, debe asegurar que los canales L2CAP que solicitaron cierto nivel de Calidad de Servicio lo reciban adecuadamente. También puede realizar políticas de conformidad para asegurar que las aplicaciones envíen datos dentro de los límites de QoS negociados

Por su parte, dentro del controlador BR/EDR se encuentran los siguientes bloques:

- Device Manager (Administrador del Dispositivo): controla el comportamiento general del dispositivo Bluetooth. Tiene a su cargo todas las operaciones que no están relacionadas con el envío y la recepción de datos, entre las que se encuentran: conectarse a un dispositivo Bluetooth remoto, hacer el dispositivo local detectable por otros dispositivos cercanos, buscar dispositivos cercanos, etc.
- Link Manager (Administrador del Enlace): en el responsable de la creación, modificación y liberación de los links lógicos y, si es necesario, sus transportes lógicos asociados, además de la actualización de los parámetros relacionados a los links físicos entre dispositivos. Utiliza el protocolo Link Manager Protocol (LMP). Entre sus tareas se encuentran la habilitación de la encriptación en los transportes lógicos, ajustar el seteo de la Calidad de Servicio en un link lógico o adaptar la potencia de transmisión del radio BR/EDR en un link físico
- Baseband Resource Manager (Administrador de Recursos de la Banda Base): es el responsable de todos los accesos al medio físico. Su principal tarea es otorgar tiempo de acceso de manera planificada y ordenada en los canales físicos a

todas las entidades que han negociado un contrato de acceso. Además, es esta capa la que se encarga de acordar esos contratos de acceso, que son compromisos para enviar tráfico con una determinada Calidad de Servicio

- Link Controller (Controlador del Enlace): es la responsable de enviar y recibir los datos. Además, se encarga de encriptar la información. También se encarga de regular el salto de frecuencias. Otras responsabilidades incluyen ARQ (Automatic Repeat Request) y FEC (Forward Error Correction) con el fin de detectar y corregir errores.
- PHY: este bloque, controlado por la baseband, es el responsable de transmitir y recibir los paquetes de información. En la versión 4.0 se lo comenzó a llamar PHY, en las versiones anteriores se lo llamaba RF, por Radio Frequency (Frecuencia de Radio)

3.3 Descripción general

3.3.1 Bluetooth Radio Layer

En un sistema Bluetooth, el radio es el dispositivo que permite la comunicación sin cables, y es la capa más baja definida por la especificación. Las comunicaciones wireless Bluetooth emplean la tecnología de radio frecuencia para comunicarse a través del aire. Al igual que las redes wireless 802.11, Bluetooth opera en la banda ISM de 2.4 GHz, ocupando entre 2400 - 2483,5 MHz. Este espectro está dividido en canales de 1 MHz cada uno, de los cuales en Bluetooth se utilizan 79 canales como máximo, empezando en 2402 MHz y finalizando en 2800 MHz. Los extremos del espectro no se utilizan para evitar interferencias con otras frecuencias. En algunos países solamente se permiten 23 canales como máximo.
Se definen dos modos de modulación. Uno obligatorio, llamado Basic Rate, que utiliza modulación binaria Frequency Modulation (FM), y otro opcional, llamado Enhanced Data Rate (EDR), que usa modulación Phase-Shift Key (PSK) en dos variantes: π/4-DQPSK y 8DPSK. En todos los modos de modulación el "symbol rate" es de 1 Megasymbol/s, lo que permite una velocidad de 1 Mbps para el modo BR, 2 Mbps para EDR usando π/4-DQPSK y 3 Mbps usando 8DPSK.
Bluetooth utiliza la técnica Frequency-Hopping Spread-Spectrum (FHSS) para transmitir sus señales. FHSS utiliza una señal portadora que cambia de frecuencia de manera aparentemente aleatoria. Obviamente, el transmisor y el receptor deben conocer la secuencia de saltos y moverse conjuntamente de canal en canal. Además, deben

coincidir en el tiempo en que permanecen en cada canal. En Bluetooth, este tiempo es de 625 microsegundos, lo que permite un total de 1600 saltos por segundo.
Aunque en mucha bibliografía se afirma que es full-duplex, inclusive lo dice la especificación de Bluetooth, el acceso al medio es half-duplex. El esquema que utiliza es Time Division Duplexing (TDD), que es una técnica de multiplexación por división de tiempo donde el tiempo de transmisión en un único canal de comunicación es dividido en intervalos sucesivos. El sentido de las transmisiones se va alternando entre dos sentidos en cada intervalo sucesivo, en un intervalo la transmisión es una dirección y en el siguiente es en la dirección contraria.

3.3.2 Bluetooth Baseband

La baseband es la parte del sistema Bluetooth que implementa el acceso al medio y los procedimientos de capa física para soportar el intercambio de tráfico de tiempo real, como voz, y streams de datos. Se encarga del manejo de los canales físicos y distintos tipos de links, además de brindar servicios como corrección de errores, data whitening, selección de saltos de FHSS, recepción de los bits del radio y su ensamblado en paquetes para ser procesados por las capas superiores, recepción de paquetes de las capas superiores y su envío al radio, operaciones básicas de seguridad, etc.
Si dos ó más dispositivos Bluetooth quieren comunicarse entre sí, primero deben establecer un canal de comunicación. Esta conexión puede ser punto-a-punto, si el canal físico es compartido, únicamente, entre dos dispositivos, o punto-multipunto, en caso de haber más de dos dispositivos usando el canal. Esto se puede ver en la parte (a) y (b) de la Figura 3.3. Sin importar la cantidad de dispositivos que la componen, a esta clase de redes se las llama “piconet”. Cada dispositivo tiene un rol dentro de la red, master o slave, y puede formar parte de más de una piconet simultáneamente, lo que se conoce como scatternet, parte (c) de la Figura 3.3, pero no puede ser master en más de una piconet a la vez. Esta capacidad no implica ninguna función de routing entre dos piconets.

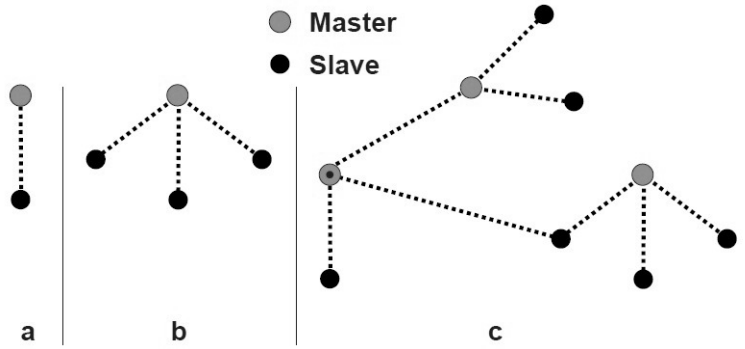


Figura 3.3 - Piconets. a) Punto a punto. b) Punto-Multipunto. c) Scatternet[6]

Cada piconet puede tener hasta 7 slaves activos simultáneamente, es decir, no puede haber más de 8 dispositivos activos en una piconet, los 7 slaves más el master, pero puede existir una cantidad adicional de dispositivos conectados a la piconet de manera parked. Estos no están activos en la red, pero permanecen sincronizados con el master y pueden volverse activos sin realizar el proceso de establecimiento de conexión.
Además de poder estar en los estados activo o parked, los slaves pueden encontrarse en otros modos: sniff y hold. Estos dos, juntos con el modo parked, le permiten a los dispositivos entrar en un estado de conservación de energía para alargar el tiempo de vida de las baterías. En el modo sniff, el slave escucha las transmisiones del master en un ritmo reducido, lo que reduce su ciclo de trabajo. Básicamente, el slave se vuelve activo cada un determinado tiempo que es negociado con el master. Éste le enviará el tráfico destinado al slave en esos intervalos de tiempo. Si el slave recibe algún paquete al comienzo del intervalo continuará recibiendo y transmitiendo paquetes, en caso contrario, se vuelve a "dormir" hasta el próximo intervalo. En cambio, en el modo hold, que es el modo de menor consumo de energía, el slave deja de estar activo en la piconet por un intervalo de tiempo determinado, pero, a diferencia del modo sniff que es periódico, lo hace una sola vez. En estos dos modos, a diferencia del parked, los dispositivos siguen perteneciendo a la piconet, solo que no están escuchando continuamente las transmisiones del master, como en el modo activo. Resumiendo, la baseband puede estar en dos estados diferentes: standby, cuando no se está asociado a ninguna piconet, o connected, en caso contrario. Dentro del estado connected, existen 4 modos: active, hold, sniff y parked
Los datos son transmitidos por el aire en paquetes. Estos tienen un formato específico según el modo de modulación. En el modo Basic

[6] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

Rate, el paquete está compuesto de 3 campos: access code, header y payload, en cambio, en el modo Enhanced Data Rate se requieren 6 campos: access code, header, guard period, synchronization sequence, payload y trailer. En las figuras 3.4 y 3.5 se pueden observar la estructura de los paquetes.

Figura 3.4 Formato paquete Basic Rate[7]

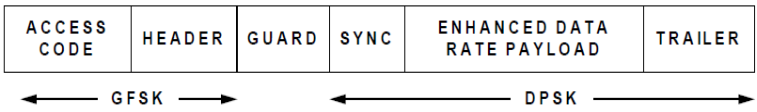


Figura 3.5 Formato paquete Enhanced Data Rate[8]

Una de las principales características del modo EDR es que la modulación es cambiada en el medio de la transmisión del paquete. El access code y el header del paquete son transmitidos con el modo de modulación GFSK de Basic Rate a una velocidad de 1Mbps, mientras que los siguientes campos (Synchronization Sequence, Payload y Trailer) lo hacen usando el modo de modulación PSK de EDR, que puede ser de 2 ó 3 Mbps (depende de la variante de PSK utilizada). Los campos Guard Time y Sync son utilizados para permitir que la capa física de los dispositivos cambie el esquema de modulación.

El access code (código de acceso), que indica al receptor el arribo de un paquete, puede tener un tamaño de 68 ó 72 bits. Si existe un campo Header a continuación, el access code ocupa un total de 72 bits. Todos los paquetes enviados en el mismo physical channel (canal físico) están precedidos por el mismo access code. Está compuesto de los siguientes campos:

- Preámbulo: 4 bits. Indica el arribo de un paquete.
- Sync Word: 64 bits. Permite al receptor sincronizarse con el transmisor.
- Trailer: 4 bits. Opcional. Sólo se agrega si existe un campo header a continuación.

Dependiendo del modo de operación en el que se encuentre un dispositivo Bluetooth, la función provista por el access code puede variar. Es por esto que existen diferentes tipos de access code:

- Channel Access Code (CAC): identifica una piconet. Está

[7] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

[8] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

incluido en todos los paquetes intercambiados en una piconet. Se deriva de una parte de la dirección MAC del master de la red

- Device Access Code (DAC): usado en el proceso de paging entre dos dispositivos Bluetooth que están estableciendo una canal de comunicación. Todos los mensajes intercambiados durante este proceso van inicializados por un DAC específico. Se deriva de la dirección de uno de los dos dispositivos (el que estaba escuchando por solicitudes para establecer una conexión)
- Inquiry Access Code (IAC): utilizado en el proceso de descubrimiento de dispositivos Bluetooth vecinos. Existe un IAC general, común para todos los dispositivos, y 63 IACs dedicados (DIAC), donde cada IAC es común para un grupo de dispositivos que comparten ciertas características. Se lo utiliza cuando se desea descubrir solamente dispositivos de uno de esos grupos

El header contiene información de control de link, consta de 6 campos. Ocupa 18 bits con una codificación 1/3 FEC, resultando en un total de 54 bits. Los campos son los siguientes:

- LT_ADDR: 3 bits. Se utiliza para distinguir entre los miembros activos participando en una piconet. A cada slave, el master le asigna una dirección temporaria para identificarlo. Al master no se le asigna ninguna dirección
- TYPE: 4 bits. Identifica el tipo de paquete. Hasta un total de 16 tipos de paquetes pueden ser distinguidos. Indica, entre otras cosas, la duración en slots de tiempo que demandará la transmisión del paquete
- FLOW: 1 bit. Usado para el control de flujo en un link asincrónico. Cuando el receptor no tenga más capacidad para recibir nuevos mensajes, le debe indicar el transmisor que deje de enviar datos (FLOW = 0). Solo afecta a los links asincrónicos. No se ven afectados por esto los paquetes de los links sincrónicos y los que llevan información de control. Cuando el receptor esté en condiciones de aceptar nuevos frames se lo hace saber al transmisor (FLOW = 1)
- ARQN: 1 bit. Permite informar al transmisor que el payload de un paquete arribó exitosamente. El chequeo se realiza mediante un CRC (Cyclic Redundancy Check)
- SEQN: 1 bit. Provee un esquema de numeración secuencial que le permite al receptor acomodar los paquetes en el orden correspondiente. El valor de este bit se invierte por cada paquete nuevo transmitido que contiene un nuevo CRC con

el fin de evitar que, debido a las retransmisiones, el destino reciba y acepte más de una vez el mismo paquete

- HEC (Header Error Check): 8 bits. Cada header tiene un HEC para chequear la integridad del header. Se calcula sobre los 10 bits de la cabecera. Si en el receptor no coincide, el paquete entero se descarta

La parte final de un paquete general es el payload. Su tamaño puede estar entre 0 y 2745 bits. Puede transportar datos sincrónicos, como voz (paquetes SCO y eSCO), asincrónicos, como datos del usuario, y de control (paquetes ACL). Para cada tipo de tráfico existen tipos de paquetes específicos que son indicados por el campo TYPE del Header del paquete. Existe un tipo de paquete que es una excepción porque permite enviar datos y voz en el mismo paquete. El payload de un paquete de tipo SCO, que sólo es soportado en el modo Basic Rate, contiene únicamente un campo de datos con una longitud fija, mientras que un paquete eSCO, que es soportado en los modos BR y EDR, consiste de dos segmentos: uno para los datos y otro para el código CRC, pero, en el caso de EDR se deben agregar los campos Guard Time, Sync y Trailer. Por su parte, en los paquetes ACL, que son soportados en ambos modos, el payload puede estar dividido en 2 ó 3 partes: un header (cabecera), un body (cuerpo) y, posiblemente, un CRC del body.

Un componente esencial de todos los dispositivos Bluetooth es el reloj nativo. Cada uno debe tener un reloj propio, que no tiene ninguna relación con el tiempo del día, con el fin de mantenerse sincronizado con el resto de los integrantes de la red. Todos los periodos críticos y la ejecución de los eventos son determinados por este reloj. Los tiempos en la piconet están bajo el control del master, por lo tanto, son los slaves los que deben sincronizar sus relojes contra los del master.

Otro punto importante es el direccionamiento. A cada dispositivo se le asigna una dirección de 48 bits, globalmente única, conocida como BD_ADDR. Como se puede ver en la figura 3.6, está dividida en 3 partes: lower address part (LAP), upper address art (UAP) y non-significant address part (NAP). La BD_ADDR y el reloj nativo están involucrados en muchas de las operaciones de la baseband.

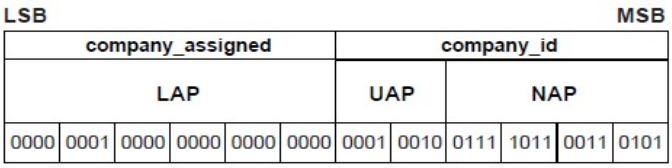


Figura 3.6 Formato dirección Bluetooth (BD_ADDR)[9]

[9] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

Dentro de la arquitectura de un sistema Bluetooth, la capa más baja es el canal físico. Un canal físico está caracterizado por una secuencia de saltos de frecuencia pseudoaleatoria, la duración del slot (el tiempo en que FHSS se mantiene en cada canal antes de moverse al siguiente canal), el access code y la codificación del header del paquete. Dos dispositivos que desean comunicarse entre sí deben establecer y utilizar un canal físico.

A cada canal físico se lo identifica con un access code que se encuentra al inicio de cada frame transmitido. Se define un total de 4 canales físicos BD/EDR, cada uno con un propósito diferente, pero un dispositivo puede usar uno de ellos por vez. Dos de esos canales, basic piconet physical channel y adapted piconet physical channel, sirven para la comunicación entre dispositivos conectados y asociados a la misma piconet. Por defecto, cuando se crea una piconet se utiliza el basic piconet physical channel. Ambos canales físicos son iguales, excepto por las siguientes características del adapted piconet physical channel. Primero, el slave transmite por la misma frecuencia que la transmisión precedente del master y, segundo, porque puede utilizar una cantidad menor a las 79 frecuencias utilizadas en el otro modo. De los restantes canales físicos, uno es utilizado para la operación de descubrimiento de nuevos dispositivos Bluetooth (inquiry scan physical channel) y el otro para la conexión con uno de los dispositivos descubierto en el proceso inquiry (page scan physical channel).

Todos los dispositivos que forman una piconet se van moviendo, en forma continua y sincronizada, siguiendo una secuencia de saltos pseudoaleatorio a través de los 79 canales de RF. Esta secuencia, única para cada piconet, está determinada por la BD_ADDR del master, específicamente las partes UAP y LAP, y la secuencia de saltos seleccionada (23 ó 79 canales según el país). Además, el reloj nativo del master se utiliza para determinar la fase de esa secuencia, es decir, en qué momento se debe saltar a la próxima frecuencia. Debido a esto, el master le debe enviar su reloj nativo a los slaves para que se sincronicen.

El master controla el acceso al canal mediante un esquema de polling. Transmite en los slots pares y, dependiendo del tipo de paquete, puede ocupar 1, 3 ó 5 slots. Por su parte, el slave lo hace en los impares y, también, puede ocupar la misma cantidad de slots. El salto de frecuencias se realiza entre la transmisión o recepción de paquetes, pero, si se transmite un paquete que ocupa más de un slot de tiempo, no se producen estos saltos de frecuencias. En la figura 3.7 se muestra el intercambio de paquetes entre un master y un slave.

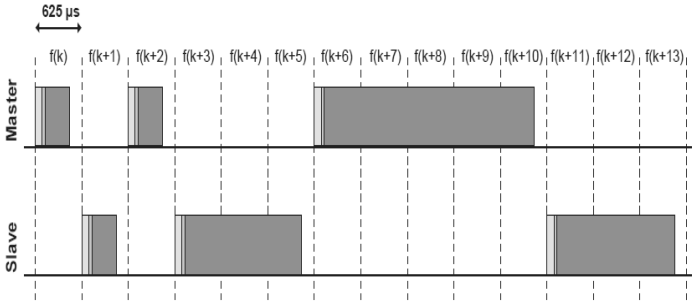


Figura 3.7 Intercambio de paquetes entre un master y un slave[10]

Cuando existen varios slaves en una piconet, un slave puede transmitir sólo si fue especialmente autorizado por el master en el slot de tiempo anterior (polling). Por ejemplo, si el master le envía un paquete al slave 1, en el siguiente slot de tiempo, sólo el slave 1 podrá enviarle algo master, los demás slaves deberán mantenerse en silencio.
Dentro de un canal físico se forma un link físico que es un link punto-a-punto entre el master y un slave, nunca se crea uno entre dos slaves directamente, y existe siempre que el slave esté conectado a una piconet. Puede estar en estado activo, si tiene un transporte lógico default ACL establecido, o parked, en caso contrario. Las transmisiones de los slaves al master son enviadas siempre por el link físico activo. Por su parte, el master puede transmitir por un solo link físico activo (a un único slave) o por varios (a un grupo de slaves).
Por sobre el link físico se encuentran los transportes lógicos. Cinco transportes lógicos han sido definidos:

- Synchronous Connection-Oriented (SCO)
- Extended Synchronous Connection-Oriented (eSCO)
- Asynchronous Connection-Oriented (ACL)
- Active Slave Broadcast (ASB)
- Parked Slave Broadcast (PSB)

En una piconet, a cada slave se le asigna una dirección primaria de 3 bits llamada "logical transport address (dirección de transporte lógica, LT_ADDR)". La dirección de todos ceros no se asigna, está reservada para el envío de mensajes broadcast. Esta dirección, LT_ADDR, es usada por el master para direccionar a un slave en particular. Es asignada por el master a los slaves cuando estos se unen a la piconet. Al master no se le asigna ninguna dirección. Todas las transmisiones de los slaves van dirigidas al master únicamente, no necesitan indicar

[10] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

el receptor. Recordar que el LT_ADDR es el primer campo del Header de un paquete, y un dispositivo tiene asignada una siempre que se encuentre en modo activo dentro de la piconet.
El SCO es un transporte lógico punto-a-punto entre el master y un slave dentro de la piconet. Se utilizan para intercambiar información que requieren baja latencia, como puede ser la voz. Para poder garantizar esto, los paquetes SCO son intercambios en slots de tiempo específicamente reservado para tal fin, por eso se lo suele considerar una conexión orientada a circuitos. Este intercambio se realiza de a pares, primero del master al slave y, a continuación, en forma inversa. Aun si el master no le transmitió en el slot anterior, un slave puede hacerlo en su slot reservado, pero esto no es posible si el master transmitió un paquete a un slave diferente en ese slot. Además, en un link SCO, los paquetes no se retransmiten. Un slave puede soportar hasta 3 SCO links provenientes del mismo master, pero no más de 2 si los links se originan en diferentes masters.
Al igual que el SCO, el eSCO es una conexión punto-a-punto entre el master y un slave específico. También, hace reserva de slots para realizar las transmisiones. Sin embargo, presenta una funcionalidad más flexible. Los links eSCO pueden ser simétricos o asimétricos. La otra diferencia con SCO es que soporta la retransmisión de paquetes dañados, aunque solo puede hacerlo en el slot siguiente al reservado.
El ACL provee una conexión packet-switched entre el master y todos los slaves participando de la piconet. Soporta servicios asincrónicos e isocrónico. El master y los slaves intercambian paquetes en los slots no reservados por los links SCO y eSCO. Es utilizado para transportar mensajes de control y datos de usuario de tipo best-effort. Entre el master y un slave determinado solamente existe un único link ACL. Además, permiten la retransmisión de paquetes hasta que lleguen correctamente al destino (o den timeout).
Para poder enviar un mensaje broadcast, el master utiliza el link ASB. Todos los slave activos en la piconet reciben el mismo mensaje. El tráfico es unidireccional, del master a los slaves, y estos no deben enviar ningún mensaje de acknowledgement, por lo tanto, es no confiable. Los mensajes enviados por este link tienen todos ceros en la dirección LT_ADDR. Pueden ser enviados por el master en cualquier momento. Ningún slave está autorizado a transmitir en el slot posterior a la recepción de un mensaje broadcast.
Por último, el PSB es usado por el master para comunicarse con los slaves que se encuentran en estado parked.
Si continuamos subiendo en las capas de Bluetooth, nos encontramos los links lógicos. Al igual que los transportes lógicos, también se definen un total de 5 links lógicos, cada uno con un fin específico:

- Link Control (LC)
- ACL Control (ACL-C)
- User Asynchronous/Isochronous (ACL-U)
- User Synchronous (SCO-S)
- User Extended Synchronous (eSCO-S)

El link lógico LC, que es usado para el control del link, es transportado en todos los paquetes, excepto en aquellos que no tienen Header. Se utiliza para transportar información de control de bajo nivel, como puede ser ARQ, control de flujo e información de las características del payload (tipo de paquete). Si se observan los campos que componen el Header de un paquete, la información del LC se transporta en estos. Todos los otros tipos de canales lógicos se transportan en el payload de cada paquete.

El intercambio de información de control entre los Links Manager del master y del slave utiliza el ACL-C. Este link tiene una prioridad más alta que los demás links lógicos. Se identifica por el código 11 del campo Logical Link ID (LLID) que se encuentra en el payload del paquete. Puede ser transportado por el transporte lógico SCO o por el ACL.

Por su parte, el ACL-U se utiliza para transportar información del usuario asincrónica e isocrónica de la capa Logical Link Control and Adaptation Protocol (L2CAP). Se identifican con el código 10 del campo LLID (si el paquete se fragmenta, el primer fragmento llevará el código 10 en el LLID y el resto usarán el código 01). El ACL-C es transportado por el transporte lógico ACL, aunque, dependiendo del tipo de paquete, podría ser enviado sobre el SCO.

Los links lógicos SCO-S y eSCO-S se utilizan para transferir información sincrónica sobre los transportes lógicos SCO y eSCO respectivamente.

La baseband es la encargada de realizar otras funciones para garantizar el funcionamiento correcto de la red. Para esto, el receptor, cada vez que se recibe un paquete, deber realizar un chequeo de errores. Lo primero que controla es el access code para evitar aceptar y procesar un paquete de otra piconet (el access code es derivado de LAP correspondiente a la BD_ADDR del master). Luego se controla que el HEC en el Header y el CRC en el payload sean correctos. Además del chequeo de errores, Bluetooth define 3 esquemas para la corrección de errores:

- 1/3 rate FEC: cada bit es repetido 3 veces. Es utilizado para todo el Header de cada paquete
- 2/3 rate FEC: un generador polinómico es usado para codificar 10 bits en una “codeword” de 15 bits. Permite

corregir todos los errores simples y detectar todos los errores dobles dentro de cada codeword

- Automatic Repeat Request (ARQ) para los datos: los paquetes son retransmitidos hasta que se recibe un acknowledgement afirmativo o se excede el time out. En este último caso, el paquete se descarta y se pasa al siguiente

El FEC en el payload se utiliza para reducir las retransmisiones, pero a costa de reducir el throughput de la red. Es por esto que su uso es opcional. En cambio, el Header está siempre protegido por el esquema 1/3 FEC (el tamaño del Header se incrementa de 18 a 54 bits).

3.3.3 Link Manager Protocol

El Link Manager Protocol es utilizado para controlar y negociar todos los aspectos de la operación de una conexión entre dos dispositivos Bluetooth. Entre sus tareas se encuentran el establecimiento y el control de los transportes lógicos y los links lógicos, la autenticación de los dispositivos, etc. Se comunica con el Link Manager (LM) del otro dispositivo mediante el Link Manager Protocol. Los mensajes de este protocolo se transfieren sobre el link lógico ACL-C en el transporte lógico ACL default. LMP opera en términos de transacción. Todos los paquetes que forman parte de una misma transacción contienen el mismo valor de identificación de transacción.
Después de la conexión inicial, LM ejecuta varias tareas de configuración y, luego se mantiene supervisando el intercambio de datos por si aparece algún paquete LMP para procesar. Finalmente, cuando el intercambio está completo, cada LM puede ejecutar la desconexión.
En general, los aspectos manejados por el LM se pueden agrupar en 3 categorías:

- Descubrimiento y configuración del link: después que el master y el slave están conectados dentro de la piconet deben descubrir las características del link (por ejemplo, soporte para paquetes multislot, RSSI, etc.) disponibles en el otro dispositivo. También existen paquetes LMP para setear la Calidad de Servicio, control de la potencia, y otras funciones de configuración mientras el link esté activo.
- Administración de la piconet: incluye conexión y desconexión de los slaves, establece los links SCO y maneja los modos de sniff, hold y park.
- Administración de la seguridad: maneja la mayoría de las implementaciones asociadas con la autenticación y encriptación del link Bluetooth.

3.3.4 Logical Link Control and Adaptation Protocol

La L2CAP se encuentra sobre la baseband y reside en la capa de enlace (data-link layer), en la parte del Host como se vio en la figura 3.2. Provee servicios de datos orientados a conexiones (del master a un slave y del slave al master) y sin conexiones (del master a varios slaves, tráfico broadcast) a los protocolos de la capas superiores. Realiza operaciones de multiplexación, segmentación y reensamblado de los datos recibidos y, además, control de flujo por cada canal y recuperación de errores mediante retransmisiones. Permite que los protocolos de nivel superior y las aplicaciones transmitan y reciban paquetes de hasta 64 Kbytes de longitud. Sin embargo, no tiene ninguna capacidad para la intercambio de tráfico en tiempo real, como voz. L2CAP está definida solamente para los links ACL, no para los links SCO o eSCO.

Al igual que LM, L2CAP confía que en el proceso de intercambio de paquetes la baseband se encargará de la integridad de los datos a través del ARQ y, posiblemente, el FEC. También asume que la baseband enviará los paquetes en forma ordenada, por lo que, la L2CAP no necesita numerar los paquetes para que el receptor pueda acomodarlos correctamente, como sucede con TCP/IP. Provee canales lógicos, llamados canales L2CAP, lo cuales son multiplexados sobre uno o más links lógicos.

La comunicación entre capas L2CAP está basada en canales a través de los cuales se envía el flujo de tráfico entre los endpoints de cada dispositivo. A cada endpoint de un canal se le asigna un channel identifier (CID) que es un identificador de 16 bits. Los CIDs se asignan dinámicamente y cada dispositivo lo hace independientemente de los demás. Sólo debe asegurarse de no asignar el mismo CID a dos conexiones activas simultáneamente. Cada slave tiene un canal de señalización L2CAP con el master. Este canal se crea tan pronto como el link ACL se establece, y es usado por L2CAP para establecer los demás canales por los cuales se realizarán los intercambios de datos del usuario. En la figura 3.8 se muestra el uso de los CIDs en una comunicación entre entidades L2CAP en diferentes dispositivos. La conexión orientada a canales de datos (connection-oriented data channel) representa una conexión entre dos dispositivos, donde un CID identifica cada endpoint del canal. Por su parte, los canales de datos sin conexión (connectionless data channel) restringen el flujo de datos a un única dirección. Estos canales se usan para enviar datos a un grupo de dispositivos remotos. Además, hay un número de canales reservados para propósitos especiales, como por ejemplo, el canal utilizado para señalización.

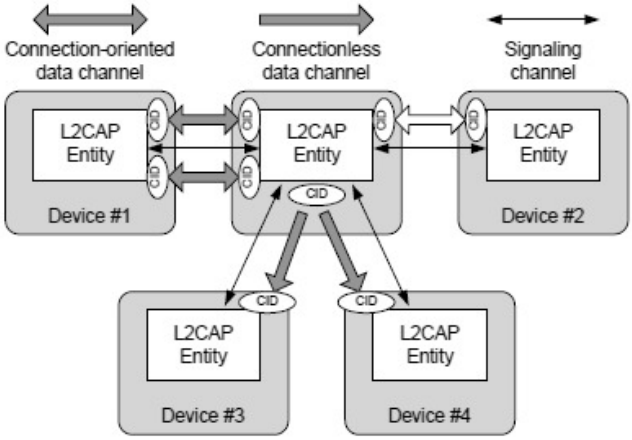


Figura 3.8 Canales L2CAP entre dispositivos[11]

Debido a que la baseband no contiene ninguna información que identifique el protocolo de capa superior que está siendo recibido, L2CAP se encarga de realizar la multiplexación, lo que le permite intercambiar información de varios protocolos de capa superior simultáneamente. Como solo existe un ACL link entre el master y un slave, todos los canales L2CAP comparten el mismo baseband. Otra función de esta capa es la de segmentación y reensamblado. El tamaño de paquete permitido por la baseband es de 339 bytes como máximo. Esto limita el uso eficiente del bandwidth por parte de los protocolos de capa superior que están diseñados para trabajar con tamaños de paquetes más grandes, hasta 64 Kbytes en algunos casos. Estos paquetes deben ser segmentados dentro de varios paquetes más chicos antes de ser transmitidos por la baseband. Obviamente, esos segmentos deben ser tomados por la capa L2CAP del receptor y reensamblarlos en el paquete original que la capa superior espera recibir.
Esta capa puede implementar un nivel de QoS para cada protocolo. Incluye ítems tales como requerimientos de bandwidth, latencia máxima y variación en el retardo (jitter). Por default, las conexiones son best-effort.

3.3.5 Service Discovery Protocol (SDP)

El protocolo SDP provee un método para que las aplicaciones de un cliente descubran qué servicios están disponibles en un dispositivo

[11] Fuente: Bluetooth Specification v4.0. Bluetooth SIG

servidor y, además, determinar cuáles son las características o atributos de esos servicios. Es un protocolo simple con requerimientos mínimos a las capas inferiores. Utiliza el modelo de solicitud/respuesta y las operaciones se realizan en transacciones. Cada transacción consiste de una solicitud y su respectiva respuesta. Estos mensajes son enviados utilizando una conexión L2CAP.
El servidor mantiene una lista de registros de servicios, uno por cada servicio disponible, que describen las características del servicio asociado con el servidor. Mediante una solicitud SDP, el cliente puede recuperar información de un registro desde el servidor. Para poder utilizar un servicio, una nueva conexión al proveedor del servicio debe ser abierta por el cliente. En un dispositivo sólo puede existir un servidor como máximo y, en caso de trabajar únicamente como cliente, puede no tener un servidor SDP. Obviamente, puede funcionar como cliente y servidor simultáneamente.
Un servicio es una entidad que puede proveer información, ejecutar una acción, o controlar un recurso en nombre de otra entidad. Puede ser implementado en software, hardware, o una combinación de las dos. Toda la información acerca de un servicio es mantenida dentro de un registro de servicio que consiste de una lista de atributos del servicio. Cada atributo, que define una única característica de un servicio, está compuesto de un Attibute ID (Identificador del atributo), que permite distinguir entre los distintos atributos de cada servicio, y un Attribute Value (Valor del atributo), que define el significado del atributo. Cada registro de servicio dentro de un servidor está identificado unívocamente por un número de 32 bits llamado "service record handle".
Además, cada servicio es una instancia de una clase de servicio. Ésta provee la definición de todos los atributos contenidos en un registro de servicio. A cada clase de servicio se le asigna un identificador único representado como un UUID (Universal Unique Identifier). Un UUID es un identificador universalmente único de 128 bits y, en cada clase de servicio está contenido en el atributo ServiceClassIDList. Dentro de cada clase de servicio, este atributo es una lista de todas las clases de servicios que depende. De esta manera, se forma una jerarquía de clases de servicios, donde los atributos se van heredando desde las clases hacia las subclases. Éstas, a su vez, contienen nuevos atributos.
Toda la funcionalidad de SDP puede realizarse por medio de dos operaciones: searching (búsqueda) y browsing (navegación). Searching significa buscar un servicio específico, mientras que browsing se utiliza para ver qué servicios están actualmente siendo ofrecidos por otro dispositivo.
Mediante el searching un dispositivo puede recuperar los "service

record handles" de determinados registros de servicios basado en valores de los atributos contenidos dentro de esos registros de servicios, es decir, el cliente busca servicios basado en algunas características deseadas y utilizando información previamente obtendida. Esta búsqueda solamente se puede realizar sobre atributos cuyos valores son UUIDs.
En el browsing, a diferencia del searching, el cliente desea descubrir cuáles son los registros de servicios existentes en un servidor, pero no cuenta con ninguna información previa acerca de esos servicios. Para poder realizar esta tarea, el SDP utiliza un atributo conocido por todas las clases de servicios llamado BrowseGroupList. Este atributo contiene una lista de UUIDs. Cada UUID representa un grupo de "browse" al cual un servicio puede estar asociado. Cuando un cliente desea conocer los servicios de un servidor SDP crea una consulta que contiene el UUID que representa el grupo de "browse" raíz. Todos los servicios son miembros de este grupo, es decir, contienen su UUID dentro del atributo BrowseGroupList.

3.3.6 Creación de una piconet

Una red Bluetooth es una tecnología de comunicación ad-hoc que requiere de un número de procedimientos, o pasos, para poder establecer una piconet. Estos procedimientos se aplican en diferentes capas de la arquitectura.
El primer paso es descubrir cuáles son los dispositivos cercanos. Este proceso, conocido como inquiry, es asimétrico. El dispositivo que intenta encontrar nuevos dispositivos, enviando inquiry requests, es conocido como inquiry device, y el que está disponible para ser encontrado es conocido como discoverable device.
El siguiente paso es el paging, que también es asimétrico. Un dispositivo, llamado paging device (quien inició el inquiry) se debe encargar de realizar el procedimiento page, y el otro, connectable device (sería el dispositivo que contestó en el proceso inquiry), estar en modo page scanning. A diferencia del inquiry, en cual todos los dispositivos que escuchan un inquiry request pueden responder, en el page, el proceso es realizado entre dos dispositivos específicos, es dirigido.
Tanto el procedimiento inquiry como el page utilizan canales físicos especiales, con access code especiales. En el inquiry se utilizan canales predeterminados que deben ser conocidos por todos los dispositivos, en cambio, para el page, el canal físico es determinado a partir de ciertos atributos propios del connectable device. Estos atributos son enviados por el discoverable device en el paso anterior, el inquiry. Por definición, el proceso que inicia una conexión mediante

el paging es el master de la piconet, aunque no es obligatorio. El rol de los dispositivos, master o slave, se puede modificar en el tiempo de vida de la red.
Con el proceso de conexión finalizado exitosamente, entre los dos dispositivos se ha formado un piconet physical channel, al cual ambos están conectados, junto con un physical link. Además, se crean, automáticamente, dos links lógicos: ACL-C y ACL-U para lo cual previamente se debe haber establecido un transporte lógico default ACL. En este modo, connected mode, es posible crear nuevos links lógicos y, también, eliminarlos. Esto lo realiza el Link Manager, mediante el intercambio de mensajes Link Manager Protocol, a través del logical link ACL-C.

3.3.7 Bluetooth Profiles

Para poder utilizar Bluetooth, un dispositivo debe ser capaz de interpretar ciertos profiles (perfiles) incluidos en Bluetooth. Estos son definiciones de posibles aplicaciones y especifican el comportamiento que deben adoptar los dispositivos Bluetooth para comunicarse entre si. Existen muchos tipos de profiles que describen distintos tipos de aplicaciones o modo de uso del dispositivo Bluetooth. En resumen, dos dispositivos Bluetooth se comunicarán entre ellos si comparten al menos uno de los profiles de Bluetooth. Por ejemplo, si dos dispositivos quieren compartir un archivo, los dos necesitan soportar el profile apropiado.
El Bluetooth SIG ha definido una gran cantidad de profiles y permite que un usuario agregue los propios siempre que respete la especificación de Bluetooth. No es necesario que un dispositivo soporte todos los profiles, como mínimo debe conocer los requeridos para realizar su tarea. No tiene sentido que una impresora soporte los profiles de intercambio de audio.
Existe un profile llamado Generic Access Profile (GAP) que es la base para todos los demás profiles. Representa la funcionalidad básica común a todos los dispositivos incluyendo descubrimiento de dispositivos, seguridad, autenticación, descubrimiento de servicios, etc. Debe ser soportado por todos los dispositivos.
Algunos de los profiles definidos en la especificación son los siguientes:

- Advanced Audio Distribution Profile (A2DP): define como se propaga el audio entre dos dispositivos Bluetooth
- Basic Printing Profile: permite el envío de documentos a una impresora
- File Transfer Profile (FTP): permite listar, modificar, copiar

y borrar archivos. Utiliza OBEX como transporte
- Headset Profile: permite el uso de auriculares con los teléfonos móviles. Utiliza canales SCO para transmitir audio codificado a 64 kbps
- Video Distribution Profile (VDP): permite el envío de video a un reproductor o televisor

3.3.8 Seguridad

Bluetooth provee autenticación y encriptación, tanto a nivel de enlace como de aplicación. Para mantener la seguridad en la "link layer" se usan 4 componentes diferentes: Bluetooth Device Address (BD_ADDR) de 48 bits, una clave de usuario privada de 128 bits para la autenticación, otra clave privada de usuario para encriptación de tamaño variable entre los 8 y los 128 bits, y un número aleatorio generado para cada nueva conexión de 128 bits.
Las claves secretas son generadas durante la inicialización de la conexión. Primero, se genera la clave de autenticación y, a partir de ésta, la de encriptación. A pesar de esta dependencia, ambas claves son totalmente diferentes y sus tiempos de vida no tienen que ser, necesariamente, iguales. Cada vez que se activa la encriptación, se genera una nueva clave para encriptar. Su tamaño no puede ser especificado por el usuario, debe estar preestablecido de fábrica.
Uno de los parámetros que se utiliza para generar la clave de autenticación es el PIN. Éste, en los casos donde sea posible, es ingresado por el usuario. Generalmente, consiste en un número decimal de 4 dígitos, pero, en situaciones donde se necesite más seguridad, es posible elegir un PIN con una longitud de hasta 16 octetos.
El master tiene una clave de encriptación separada por cada slave y, para el caso de necesitar enviar el mismo paquete a más de un slave, utiliza otra clave que es conocida por todos los integrantes de la piconet.
A través de las distintas especificaciones de Bluetooth se han ido definiendo un total de cuatro modos de seguridad. Cada dispositivo Bluetooth debe operar en uno de esos modos [NIST]:

- Security Mode 1: sin seguridad. Las funcionalidades de seguridad, autenticación y encriptación, son soslayadas, lo que deja a los dispositivos y sus conexiones susceptibles a los atacantes. Este modo es soportado, únicamente, en las versiones 2.0 + EDR y anteriores
- Security Mode 2: seguridad obligatoria a nivel de servicio. Permite controlar el acceso a determinados servicios y

dispositivos. Es posible definir diferentes políticas de seguridad y niveles de confianza específicos para cada aplicación brindando acceso a determinados servicios y denegándolo para otros

- Security Mode 3: la seguridad es realizada a nivel de link. Todas las conexiones entre dos dispositivos deben estar autenticadas y encriptadas
- Security Mode 4: este modo es similar al Mode 2, lo que cambia es que se utiliza una técnica llamada Elliptic Curve Diffie Hellman (ECDH) para el intercambio y generación de claves.

3.3 Bluetooth en Linux

3.3.1 Introducción e instalación

Para realizar las pruebas con Bluetooth se utilizó una notebook con sistema operativo Ubuntu 11.04 y un celular con soporte del protocolo.
En Ubuntu se utilizó el software BlueZ, que es la pila de protocolos oficial de Bluetooth en GNU/Linux. Desarrollado inicialmente por una empresa llamada Qualcomm, en la actualidad es un proyecto Open Source distribuido bajo licencia GNU General Public License (GPL). A partir de la versión 2.4.6, los módulos de BlueZ forman parte del kernel (www.bluez.org).
Windows también presenta soporte para Bluetooth. Lo hace desde el Windows XP con Service Pack 2 e incluye al Windows Vista y al Windows 7, ambos en todas sus versiones. Su línea de servidores, Windows 2000, Windows 2003 y Windows 2008 no tienen soporte integrado de esta tecnología, aunque existen drivers disponibles de otros fabricantes que pueden agregarse.
Como se detalló más arriba, la versión de GNU/Linux utilizada para las pruebas es Ubuntu 11.04 (Natty Narwhal) que tiene instalado el kernel 2.6.38-8:

```
root@bluetooth:~# uname -a
Linux bluetooth 2.6.38-8-generic #42-Ubuntu SMP Mon Apr 11 03:31:50 UTC 2011 i686
i686 i386 GNU/Linux
```

Para saber si el dispositivo Bluetooth es reconocido correctamente usamos el comando *dmesg*. Si el resultado no es similar al que se muestra a continuación, es posible que el dispositivo no esté soportado.

```
root@bluetooth:~# dmesg | grep -i blue
[   11.506872] Bluetooth: Core ver 2.15
```

```
[   11.506944] Bluetooth: HCI device and connection manager initialized
[   11.506947] Bluetooth: HCI socket layer initialized
[   12.107929] Bluetooth: Generic Bluetooth USB driver ver 0.6
[   45.138251] Bluetooth: L2CAP ver 2.15
[   45.138255] Bluetooth: L2CAP socket layer initialized
[   45.627230] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
[   45.627235] Bluetooth: BNEP filters: protocol multicast
[   46.215588] Bluetooth: SCO (Voice Link) ver 0.6
[   46.215592] Bluetooth: SCO socket layer initialized
[   46.916993] Bluetooth: RFCOMM TTY layer initialized
[   46.916999] Bluetooth: RFCOMM socket layer initialized
[   46.917002] Bluetooth: RFCOMM ver 1.11
```

Como muestra la salida del comando dmesg, el dispositivo Bluetooth aparece como USB. Con el comando *lsusb* se puede obtener más información, como por ejemplo, el fabricante del dispositivo (Broadcom).

```
root@bluetooth:~# lsusb | grep -i blue
Bus 003 Device 003: ID 413c:8126 Dell Computer Corp. Wireless 355 Bluetooth
Bus 003 Device 002: ID 0a5c:4500 Broadcom Corp. BCM2046B1 USB 2.0 Hub (part of BCM2046 Bluetooth)
```

Por último, utilizamos el comando *lsmod* para ver si se han cargado los módulos necesarios para poder utilizar el dispositivo:

```
root@bluetooth:~# lsmod | grep blue
bluetooth              65565  9 rfcomm,sco,bnep,l2cap,btusb
```

Ahora que está todo correctamente instalado, y en caso de no estar ejecutándose, iniciamos el servicio (en algunas distribuciones el nombre del servicio puede ser /etc/init.d/bluez-utils):

```
root@bluetooth:~# /etc/init.d/bluetooth start
Starting bluetooth                                                    [OK]
```

Esta versión del kernel ya tiene los módulos correspondientes a Bluetooth preinstalados. Estos módulos, sin ningún software adicional, no tienen demasiada utilidad. Es por esto que se deben instalar los daemons y herramientas que permitan ejecutar desde el shell de comandos las funciones implementadas en la pila de protocolos de Bluetooth. Actualmente, en las distribuciones de Linux que incorporan el núcleo de Bluez, la mayoría de los daemons (demonios) y herramientas se encuentran instaladas por defecto. Si no lo están, se pueden bajar de la página de BlueZ, (http://www.bluez.org), o, como en nuestro caso, usando la herramienta apt-get de Ubuntu:

```
root@bluetooth:~# apt-cache search bluez
bluez - Bluetooth tools and daemons
bluez-alsa - Bluetooth ALSA support
bluez-cups - Bluetooth printer driver for CUPS
bluez-gstreamer - Bluetooth GStreamer support
bluez-audio - Transitional package
bluez-btsco - Bluez Bluetooth SCO tool
bluez-compat - BlueZ 3.x compatibility binaries
bluez-hcidump - Analyses Bluetooth HCI packets
bluez-pcmcia-support - PCMCIA support files for BlueZ 2.0 Bluetooth
```

```
tools
bluez-utils - Transitional package
......
```

Con todos los módulos del kernel instalados y el servicio funcionando correctamente se listan todos los dispositivos Bluetooth instalados en la notebook. Generalmente, GNU/Linux los muestra como hciX, donde X es el número dado por el sistema a la interface, lo que se puede verificar con el comando *hciconfig*:

```
root@bluetooth:~# hciconfig
hci0:Type: BR/EDR  Bus: USB
     BD Address: 00:1C:26:F1:F8:5A  ACL MTU: 1017:8  SCO MTU: 64:8
     DOWN
     RX bytes:1631 acl:0 sco:0 events:51 errors:0
     TX bytes:719 acl:0 sco:0 commands:49 errors:0
```

El nombre de la interface del dispositivo Bluetooth es hci0 y es el único que está en el sistema, pero, en este caso, no está funcionando. Es necesario levantarlo con el siguiente comando:

```
root@bluetooth:~# hciconfig hci0 up
```

Usando nuevamente el comando *hciconfig*, ahora con la opción *-a*, obtenemos mayor cantidad de información:

```
root@bluetooth:~# hciconfig -a
hci0: Type: BR/EDR  Bus: USB
      BD Address: 00:1C:26:F1:F8:5A  ACL MTU: 1017:8  SCO MTU: 64:8
      UP RUNNING PSCAN ISCAN
      RX bytes:2288 acl:0 sco:0 events:72 errors:0
      TX bytes:1059 acl:0 sco:0 commands:70 errors:0
      Features: 0xff 0xff 0x8f 0xfe 0x9b 0xf9 0x00 0x80
      Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
      Link policy: RSWITCH HOLD SNIFF PARK
      Link mode: SLAVE ACCEPT
      Name: 'bluetooth-0'
      Class: 0x4a010c
      Service Classes: Networking, Capturing, Telephony
      Device Class: Computer, Laptop
      HCI Version: 2.0 (0x3)  Revision: 0x216f
      LMP Version: 2.0 (0x3)  Subversion: 0x41d8
      Manufacturer: Broadcom Corporation (15)
```

La salida de este comando brinda mucha información para analizar. El dispositivo soporta dos tipos de velocidades: BR (Basic Rate) y EDR (Enhanced Data Rate), es de tipo USB (coincide con lo visto más arriba) y su BD_ADDR es 00:1C:26:F1:F8:5A. Además, el dispositivo soporta dos tipos de links de datos: ACL y SCO. ACL tiene un MTU (Maximum Transmission Unit) de 1077 bytes y puede almacenar hasta 8 paquetes en el búfer y el SCO tiene un MTU de 64 bytes con la misma capacidad que ACL en el búffer. A continuación se muestran los distintos estados en que se encuentra la interface: está UP (arriba) y RUNNING (corriendo). Además, indica que el dispositivo está disponible para contestar a los eventos de scan (PSCAN) e inquiry

(ISCAN). PSCAN significa que el dispositivo está disponible para recibir mensajes de un dispositivo master que quiere establecer una piconet e ISCAN indica que está detectable para otro dispositivo en su "vecindad". Aunque ha transmitido, "TX Bytes" mayor que 0, y recibido información, "RX Bytes" mayor que 0, aún no ha establecido ningún "channel", ni sincrónico ni asincrónico, con algún vecino (acl = 0 y scl = 0). Solo envió y recibió datos de comandos y eventos.

El dispositivo soporta distintas características, Features, que son negociadas, al principio de la conexión, con el otro dispositivo por el protocolo Link Manager Protocol (LMP). Se representan como un "bit mask" cuando se transfieren en los mensajes LMP. Si el bit está en 1, el "feature" correspondiente está soportado. Un total de 8 bytes de "features" están definidos. Por ejemplo, el primer valor, 0xff, indica que todas las "features" del primer byte están soportadas, entre las que se encuentran: encriptación, hold mode, paquetes de 3 y 5 time-slots, Sniff Mode, Role Switch. En la especificación oficial de Bluetooth están todas las "features" detalladas.

A continuación se muestra la lista de los tipos de paquetes que soporta. Del total de 16 tipos de paquetes que soporta Bluetooth este dispositivo reconoce 9: DM1, DM3, DM5, DH1, DH3, DH5, HV1, HV2 y HV3. Los paquetes de tipo DM, definidos para la operación en BR, y DH, para la operación en EDR, se utilizan para enviar datos del usuario sobre el transporte lógico ACL. Ambos pueden usar 1, 3 y 5 slots de tiempo para transmitir, pero los paquetes de tipo DH permiten llevar más información porque el payload del DM van codificados con el método 2/3 FEC. Por ejemplo, en DM5 el payload puede tener hasta 226 bytes de información mientras que en DH5 puede llegar hasta los 341 bytes. Por su parte, los paquetes de tipo HV son usados en los transportes lógicos SCO. Los paquetes HV no incluyen CRC y no son retransmitidos. HV1 está protegido por 1/3 FEC, HV2 por 2/3 FEC y HV3 no está protegido. La longitud del payload es de 240 bits, pero, según el tipo de paquete, se modifica la cantidad de información útil transportada. En HV1 son 80 bits, en HV2 son 160 bits y en HV3 los 240 bits.

El "Link Policy" indica cuales son los estados en que es capaz de ponerse el dispositivo (HOLD, SNIFF y PARK) y que, además, tiene la capacidad de llevar adelante la operación de cambios de roles (RSWITCH). En el medio del funcionamiento de la piconet, el dispositivo puede pasar de ser un slave a ser el master de la red y, también, el proceso inverso.

Si recibe una solicitud de conexión, el dispositivo permanecerá en estado SLAVE, no solicitará ser el MASTER de la piconet, de acuerdo al valor del campo "Link Mode".

Todos los dispositivos Bluetooth tienen un nombre "amigable" para poder ser identificados con mayor facilidad que, en este dispositivo, es "bluetooth-0". Este puede ser de hasta 248 bytes.
El parámetro Class, que ocupa 3 bytes, sirve para indicar el tipo de dispositivo y cuales son los servicios que soporta. Es intercambiado durante el proceso de descubrimiento (inquiry). De esos 3 bytes, 11 bits, entre los bits 13 y 23, llamado Major Service Class, son utilizados para definir las clases de servicios. Los siguientes 11 bits permiten definir la clase de dispositivo y está dividido en dos campos. El segmento entre los bits 8 y 12, llamado Major Device Classes, define un agrupamiento mayor de clase de dispositivos, y los bits restantes, entre el 2 y el 7, determinan un dispositivo específico dentro del agrupamiento mayor. El significado de este último segmento varía en función del valor del segmento mayor. De acuerdo a esto, este dispositivo es una "Computer (Major Device Class), Laptop (Minor Device Class)" y soporta los servicios de Networking, Capturing y Telephony.
Por último se muestran información específica del dispositivo, como son las versiones del HCI y del protocolo LMP, junto con el fabricante de la placa.
Estos parámetros pueden ser cambiados con el mismo comando, *hciconfig*. Por ejemplo, para modificar el nombre del dispositivo:

```
root@bluetooth:~# hciconfig hci0 name post-unlp
root@bluetooth:~# hciconfig hci0 name
hci0: Type: BR/EDR  Bus: USB
      BD Address: 00:1C:26:F1:F8:5A  ACL MTU: 1017:8  SCO MTU: 64:8
      Name: 'post-unlp'
```

Todas las modificaciones realizadas de esta manera son temporales y se perderán cuando se inicie nuevamente la notebook. Si se quiere evitar que esto suceda, los cambios se deben realizar en los archivos de configuración que se encuentra en el directorio /etc/bluetooth.

3.3.2 Descubriendo dispositivos vecinos

Utilizando el comando *hcitool* podemos escanear y obtener cuales son los dispositivos Bluetooth activos que se encuentran en nuestro alcance junto con información adicional de cada uno los dispositivos descubiertos. Además, este comando brinda la posibilidad de configurar las conexiones Bluetooth.
Con la opción "scan" es posible obtener el nombre de cada uno de los dispositivos activos y su dirección BD_ADDR.

```
root@bluetooth:~# hcitool -i hci0  scan
Scanning ...
         00:1F:5D:E8:BF:D6   Nokia 5610 XpressMusic
root@bluetooth:~#
```

También es posible ejecutar el comando con la opción “inq” para que realice el proceso de “inquiry”. El resultado del comando es, por cada dispositivo encontrado, la BD_ADDR, el clock offset y el class. Si se analiza el valor del último campo (class) podemos descubrir qué clase de dispositivo es y cuáles son los servicios que soporta.

```
root@bluetooth:~# hcitool -i hci0  inq
Inquiring ...
        00:1F:5D:E8:BF:D6   clock offset: 0x7f2e         class: 0x5a0204
root@bluetooth:~#
```

De acuerdo al valor del campo “class” y, teniendo en cuenta lo explicado anteriormente, el dispositivo es un “Phone” dentro del Mayor Device Class, y Cellular, dentro del Minor Device Class. También, es posible determinar que soporta los servicios de: Telephony, Object Transfer, Capturing y Networking.
Si se quiere obtener más información del dispositivo remoto se puede utilizar el siguiente comando:

```
root@bluetooth:~# hcitool -i hci0 info 00:1F:5D:E8:BF:D6
Requesting information ...
           BD Address:  00:1F:5D:E8:BF:D6
           Device Name: Nokia 5610 XpressMusic
           LMP Version: 2.0 (0x3) LMP Subversion: 0x2222
           Manufacturer: Broadcom Corporation (15)
           Features: 0xbf 0xee 0x0f 0xce 0x98 0x39 0x00 0x00
               <3-slot packets> <5-slot packets> <encryption> <slot offset>
               <timing accuracy> <role switch> <sniff mode> <RSSI>
               <channel quality> <SCO link> <HV3 packets> <u-law log>
               <A-law log> <CVSD> <paging scheme> <power control>
               <transparent SCO> <EDR ACL 2 Mbps> <EDR ACL 3 Mbps>
               <enhanced iscan> <inquiry with RSSI> <extended SCO>
               <AFH cap. slave> <AFH class. slave> <3-slot EDR ACL>
               <5-slot EDR ACL> <AFH cap. master> <AFH class. master>
               <EDR eSCO 2 Mbps>
root@bluetooth:~#
```

BlueZ tiene un comando análogo al ping, llamado *l2ping*, que permite comprobar que existe conectividad entre dispositivos vecinos. Su nombre se refiere al hecho de que intenta crear una conexión al otro dispositivo usando el protocolo L2CAP. En muchas ocasiones, la falla en la conectividad puede encontrarse en las aplicaciones de nivel superior. Usando este comando se puede determinar si es posible establecer una conexión básica con un dispositivo remoto lo que puede ayudar a aislar el origen de un problema de conectividad. A continuación se realiza un *l2ping* desde la notebook al celular:

```
root@bluetooth:~# l2ping 00:1F:5D:E8:BF:D6
Ping: 00:1F:5D:E8:BF:D6 from 00:1C:26:F1:F8:5A (data size 44) ...
0 bytes from 00:1F:5D:E8:BF:D6 id 0 time 32.77ms
0 bytes from 00:1F:5D:E8:BF:D6 id 1 time 8.81ms
0 bytes from 00:1F:5D:E8:BF:D6 id 2 time 11.77ms
0 bytes from 00:1F:5D:E8:BF:D6 id 3 time 19.86ms
0 bytes from 00:1F:5D:E8:BF:D6 id 4 time 5.75ms
0 bytes from 00:1F:5D:E8:BF:D6 id 5 time 28.79ms
^C6 sent, 6 received, 0% loss
```

Cada dispositivo Bluetooth provee determinados servicios. Ejecutando la herramienta *sdptool*, que hace uso del protocolo Service Discovery Protocol (SDP), es posible detectar qué servicios están siendo anunciados por los dispositivos remotos y, obviamente, ver que "perfiles" están implementados. Además, permite una configuración básica de los servicios SDP que ofrece el dispositivo local. A continuación, mediante el comando sdptool, se descubren los servicios que brinda el teléfono celular Nokia 5610. Con el fin de abreviar, solamente se muestran 3 servicios de los 11 que soporta el teléfono.

```
root@bluetooth:~# sdptool browse 00:1F:5D:E8:BF:D6
Browsing 00:1F:5D:E8:BF:D6 ...
Service Name: Network Access Point Service
Service Description: Personal Ad-hoc Network Service which provides access to a
network
Service RecHandle: 0x10000
Service Class ID List:
  "Network Access Point" (0x1116)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 15
  "BNEP" (0x000f)
    Version: 0x0100
    SEQ8: dd 6
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Network Access Point" (0x1116)
    Version: 0x0100
          Service Name: OBEX Object Push
Service RecHandle: 0x10001
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 9
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
          Service Name: OBEX File Transfer
Service RecHandle: 0x10002
Service Class ID List:
  "OBEX File Transfer" (0x1106)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 10
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX File Transfer" (0x1106)
    Version: 0x0100
```

3.3.3 Establecimiento de una conexión

En este punto se muestra el intercambio de paquetes entre la notebook y el teléfono celular al momento de establecerse una conexión entre

ambos, junto con la ejecución del comando l2ping. La conexión es iniciada en la notebook. Se utiliza la herramienta hcidump para capturar los mensajes y el programa Wireshark para ver su contenido.
A continuación se muestra este intercambio de mensajes y, posteriormente, se brinda una explicación detallada de este proceso (en la explicación los mensajes se referencian por número de línea).
En realidad lo que se captura son todos los eventos y comandos intercambiados entre el Host y el Controlador

No.	Time	Protocol	Info
1	0.000000	HCI_CMD	Periodic Inquiry Mode
2	0.002651	HCI_EVT	Command Complete (Periodic Inquiry Mode)
3	0.116730	HCI_EVT	Inquiry Result With RSSI
5	0.818655	HCI_EVT	Inquiry Result With RSSI
6	1.139765	HCI_EVT	Inquiry Result With RSSI
7	1.539781	HCI_EVT	Inquiry Result With RSSI
8	1.700789	HCI_EVT	Inquiry Result With RSSI
9	2.090794	HCI_EVT	Inquiry Result With RSSI
10	2.252716	HCI_EVT	Inquiry Result With RSSI
11	5.161044	HCI_CMD	Exit Periodic Inquiry Mode
12	5.164795	HCI_EVT	Command Complete (Exit Periodic Inquiry Mode)
13	5.164833	HCI_CMD	Create Connection
14	5.166793	HCI_EVT	Command Complete (Inquiry Cancel)
15	5.168793	HCI_EVT	Command Status (Create Connection)
16	5.547832	HCI_EVT	Connect Complete
17	5.547866	HCI_CMD	Read Remote Supported Features
18	5.550809	HCI_EVT	Read Remote Supported Features
19	5.552808	HCI_EVT	Command Status (Read Remote Supported Features)
20	5.552835	HCI_CMD	Remote Name Request
21	5.555808	HCI_EVT	Command Status (Remote Name Request)
22	5.567814	HCI_EVT	Max Slots Change
23	5.616898	HCI_EVT	Remote Name Req Complete
24	5.616940	HCI_CMD	Authentication Requested
25	5.620913	HCI_EVT	Command Status (Authentication Requested)
26	5.622832	HCI_EVT	Link Key Request
27	5.623015	HCI_CMD	Link Key Request Negative Reply
28	5.624833	HCI_EVT	PIN Code Request
29	5.626817	HCI_EVT	Command Complete(Link Key Request Negative Reply)
30	5.626844	HCI_CMD	PIN Code Request Reply
31	5.633408	HCI_EVT	Command Complete (PIN Code Request Reply)
32	19.817318	HCI_EVT	Auth Complete
33	19.817583	HCI_CMD	Authentication Requested
34	19.817896	L2CAP	Sent Information Request
35	19.821272	HCI_EVT	Link Key Notification
36	19.825284	L2CAP	Rcvd Information Response
37	19.825351	L2CAP	Sent Connection Request
38	19.829275	HCI_EVT	Number of Completed Packets
39	19.831307	L2CAP	Rcvd Connection Response
40	19.831344	L2CAP	Sent Configure Request
41	19.833302	L2CAP	Rcvd Configure Request
42	19.833318	L2CAP	Sent Configure Response
43	19.837292	HCI_EVT	Number of Completed Packets
44	19.837303	L2CAP	Rcvd Configure Response
45	19.837446	SDP	Sent SDP_ServiceSearchAttributeRequest
46	19.839286	HCI_EVT	Command Status (Authentication Requested)
47	19.842284	HCI_EVT	Auth Complete
48	19.849316	SDP	Rcvd SDP_ServiceSearchAttributeResponse [Malformed]
49	19.849723	SDP	Sent SDP_ServiceSearchAttributeRequest
50	19.854374	HCI_EVT	Number of Completed Packets
51	19.891311	SDP	Rcvd SDP_ServiceSearchAttributeResponse
52	19.891567	SDP	Sent SDP_ServiceSearchAttributeRequest
53	19.900387	SDP	Rcvd SDP_ServiceSearchAttributeResponse
54	19.915528	SDP	Sent SDP_ServiceSearchAttributeRequest
55	19.938314	HCI_EVT	Number of Completed Packets
|56	19.941389	SDP	Rcvd SDP_ServiceSearchAttributeResponse
|57	22.212290	L2CAP	Sent Disconnect Request
58	22.224388	L2CAP	Rcvd Disconnect Response
59	22.353464	HCI_EVT	Number of Completed Packets
60	24.225353	HCI_CMD	Disconnect
61	24.227452	HCI_EVT	Command Status (Disconnect)
62	24.390456	HCI_EVT	Disconnect Complete
63	122.600149	HCI_CMD	Inquiry
64	122.602635	HCI_EVT	Command Status (Inquiry)

```
65   123.731744   HCI_EVT   Inquiry Result With RSSI
66   126.262827   HCI_EVT   Inquiry Result With RSSI
67   126.573771   HCI_EVT   Inquiry Result With RSSI
68   127.134758   HCI_EVT   Inquiry Result With RSSI
69   127.225787   HCI_EVT   Inquiry Result With RSSI
70   131.668901   HCI_EVT   Inquiry Result With RSSI
71   132.318927   HCI_EVT   Inquiry Result With RSSI
72   132.720040   HCI_EVT   Inquiry Result With RSSI
73   132.840968   HCI_EVT   Inquiry Complete
74   148.657960   HCI_CMD   Create Connection
75   148.661477   HCI_EVT   Command Status (Create Connection)
76   149.898528   HCI_EVT   Connect Complete
77   149.898578   HCI_CMD   Read Remote Supported Features
78   149.901497   HCI_EVT   Read Remote Supported Features
79   149.901776   L2CAP     Sent Echo Request
80   149.903497   HCI_EVT   Command Status (Read Remote Supported Features)
81   149.903520   HCI_CMD   Remote Name Request
82   149.906496   HCI_EVT   Command Status (Remote Name Request)
83   149.918507   HCI_EVT   Max Slots Change
84   149.935561   L2CAP     Rcvd Echo Response
85   149.967505   HCI_EVT   Remote Name Req Complete
86   150.102610   HCI_EVT   Number of Completed Packets
87   150.936117   L2CAP     Sent Echo Request
88   150.973570   L2CAP     Rcvd Echo Response
89   151.102569   HCI_EVT   Number of Completed Packets
90   151.974092   L2CAP     Sent Echo Request
91   151.984578   L2CAP     Rcvd Echo Response
92   152.227605   HCI_EVT   Number of Completed Packets
93   152.985157   L2CAP     Sent Echo Request
94   152.991627   L2CAP     Rcvd Echo Response
95   153.227709   HCI_EVT   Number of Completed Packets
96   153.991911   L2CAP     Sent Echo Request
97   153.997648   L2CAP     Rcvd Echo Response
98   154.227670   HCI_EVT   Number of Completed Packets
99   156.609312   HCI_CMD   Disconnect
100  156.612738   HCI_EVT   Command Status (Disconnect)
101  156.764737   HCI_EVT   Disconnect Complete
```

El evento 1, enviado por la notebook, es el que inicia todo el proceso. Debido a este evento, el controlador BR/EDR de la notebook entra en el modo Inquiry y envía, automáticamente, paquetes Inquiry cada determinado tiempo. Por cada uno de estos que es enviado se recibe un evento Inquiry Result with RSSI que el controlador BR/EDR se lo pasa al Host tan pronto como recibe un Inquiry Response de un dispositivo remoto. Indica que otro Controlador BR/EDR ha contestado al proceso Inquiry. En este caso, todas las contestaciones provienen del mismo controlador, el del teléfono celular. El RSSI (Received Signal Strength Indication), que es una medida de la potencia de la señal recibida, es opcional y es medido cuando se recibe cada paquete enviado por dispositivo remoto. Además, cada dispositivo envía su BD_ADDR, qué tipo de dispositivo es y qué operaciones soporta (explicado en el resultado del comando hciconfig –a), y el clock offset.

En la línea 13, el Host envía el comando Create Connection al controlador BR/EDR para que éste cree una conexión ACL, a través del Link Manager, que con este fin inicia el proceso de Page, con un dispositivo remoto. Para esto le envía la dirección BD_ADDR de ese dispositivo, que la recibió en el mensaje Inquiry Result with RSSI. En este paquete le indica qué clase de paquetes soporta y cuál es su clock offset. Con el evento Connect Complete, en la línea 16, el controlador

BR/EDR le indica al Host si la conexión se estableció exitosamente o no. En este último caso, le envía el código del error. También le comunica el tipo de link que se creó, si la encriptación a nivel de link está habilitada o no, y un Connection Handle que es usado para identificar a una conexión entre dos controladores BR/EDR.
A continuación, en la línea 17, el componente Host de la notebook envía el comando Read Remote Supported Features para solicitarle al dispositivo remoto la lista de todas las características que soporta, quien, en el siguiente evento, se las envía y, entre las que se encuentran el tipo de paquetes que soporta (3 ó 5 slots de tiempo), encriptación, control de flujo, si soporta links SCO, EDR (2 ó 3Mbps), clase de paquetes (HV, EV u otro), etc. Luego, la notebook le solicita al teléfono su nombre "amigable", que es el nombre que le permite al usuario distinguir entre distintos controladores, con el comando Remote Name Request. La contestación es recibida en el evento de la línea 23, Remote Name Req Complete.
Entre las líneas 24 y 33 se realiza el proceso de autenticación, que es iniciado por el Host de la notebook. Cuando el controlador BD/EDR recibe el comando para iniciar la autenticación, Authentication Requested, le envía el evento Link Key Request al Host para solicitarle una Link Key, que es necesaria para la conexión con el dispositivo remoto. Como el Host no tiene almacenada ninguna Link Key le contesta con un Link Key Request Negative Reply indicando que no tiene la clave solicitada. Esto se debe a que no se había establecido una conexión previa entre estos dos dispositivos o, si la hubo, los datos correspondientes fueron eliminados. A causa de esto, el controlador le solicita un PIN al Host para poder formar la Link Key con el evento PIN Code Request, en el cual le indica la longitud del PIN. Éste, que es enviado en el comando PIN Code Request Reply, también debe ser ingresado en el teléfono celular por teclado. Como todo el proceso resulta exitoso, el controlador le envía el evento Auth Complete al Host. Además, el controlador, mediante el evento Link Key Notification, le envía la nueva Link Key al Host para que éste la almacene en su propio espacio y la pueda utilizar en futuras conexiones.
Con la conexión establecida correctamente, más precisamente el transporte lógico ACL default creado, el protocolo L2CAP comienza a intercambiar información propia del canal L2CAP. Mediante el comando Information Request se le solicita al otro extremo del canal información específica de la implementación, es decir, las funcionalidades que tendrá el canal, entre las que se encuentran: control de flujo, retransmisiones, streaming, FCS, tamaño de ventana extendido, etc. Con esta información conocida, que es recibida en el

evento Information Response, se envía el comando Connection Request para establecer el canal L2CAP. Para que el otro extrema sepa a qué canal se utilizará para el intercambio de datos, el CID (Channel ID) elegido es enviado en el mensaje. La respuesta se puede ver en el Connection Response y, obviamente, este nodo también recibe el CID elegido por el otro extremo. El siguiente intercambio de mensajes, Configure Request y Configure Response, es utilizado para negociar diferentes requerimientos de la conexión. Por ejemplo, en esta conexión se negocia el MTU del canal, que queda establecido en 65535 bytes. Todo este intercambio de mensajes de configuración del canal L2CAP se realiza sobre el canal L2CAP con CID 0x0001 que está reservado para el envío de información de señalización L2CAP.

El siguiente intercambio de mensajes, entre las líneas 45 y 57, corresponde al protocolo Service Discovery Protocol (SDP). Para toda esta actividad, SDP utiliza el canal L2CAP generado en el proceso anterior. Como la respuesta al mensaje SDP de descubrimiento de servicios de la línea 45 volvió con errores, lo que se puede ver en la línea 48, el mensaje enviado nuevamente en la línea 49.

Cuando el protocolo SDP termina de realizar su intercambio se finaliza, también, el canal L2CAP. Para esto, se necesita enviar el comando Disconnect Request, línea 57, en el cual se indica el CID del canal L2CAP que se quiere desconectar. En esta oportunidad es la notebook quien inicia la desconexión y, el teléfono, que es el receptor, le debe contestar con un Disconnect Response, lo que hace en la línea 58. Esta operación es llevada a cabo por el Channel Manager y se utiliza el canal L2CAP con CID 0x00001.

En las líneas 60 y 62, el transporte lógico ACL creado entre las líneas 13 y 33 es destruido. El Link Manager es el encargado de realizar este proceso y la desconexión es iniciada por la notebook. A causa de esto, a partir de la línea 63 se vuelve a establecer una conexión previo proceso de Inquiry. Este procedimiento es diferente al realizado con anterioridad porque no es necesario ejecutar los pasos referentes a la autenticación debido a que los componentes Host de ambos dispositivos mantienen almacenados los datos de la autenticación anterior.

Con el canal L2CAP establecido nuevamente se empieza a enviar los mensajes generados por el comando l2cap. Se envían Echo Request y se reciben los correspondientes Echo Response. Estos mensajes se transmiten por el canal de señalización de L2CAP que, como se explicó más arriba, tiene el CID 0x00001.

3.3.4 Transferencia de archivos

Una de las tantas funcionalidades que nos brinda Bluetooth es la de transferencia de archivos entre dispositivos. Existen varios perfiles y protocolos que permiten realizar esta clase de operaciones. Para este ejemplo se utilizó el protocolo Object Exchange (OBEX).
OBEX utiliza el modelo cliente/servidor. El dispositivo Bluetooth que inicia la sesión OBEX es el cliente. Para su funcionamiento utiliza, como capa de transporte, RFCOMM que es un protocolo que emula una línea de cable serial de tipo RS-232 y que le provee, mediante la utilización del protocolo L2CAP y su capacidad de multiplexación, múltiples conexiones concurrentes.
A continuación se muestra el comando obexftp, que se ejecuta en la notebook, y que permite hacer un upload del archivo blue.pcap al teléfono celular cuya BD_ADDR está indicada con la opción -b.

```
root@bluetooth:~/Desktop# obexftp -b 00:1F:5D:E8:BF:D6 -p blue.pcap
Browsing 00:1F:5D:E8:BF:D6 ...
Connecting..\done
Tried to connect for 302ms
Sending "blue.pcap".../done
Disconnecting..-done
```

Estos serían los mensajes intercambiados entre el componente Host y el controlador BR/EDR de la notebook cuando se realiza la transferencia. La muestra comienza con el primer mensaje del protocolo RFCOMM.

```
 No.   Time         Protocol Info
122  54.594361  RFCOMM    Sent SABM DLCI=0
123  54.600305  RFCOMM    Rcvd UA DLCI=0
124  54.600356  RFCOMM    Sent UIH DLCI=0 MPX_CTRL DLC parameter negotiation
                                  (PN) Parameter Negotiation
125  54.604298  HCI_EVT   Number of Completed Packets
126  54.606303  RFCOMM    Rcvd UIH DLCI=0 MPX_CTRL DLC parameter
                                  negotiation (PN) Parameter Negotiation
127  54.606346  RFCOMM    Sent SABM DLCI=20
128  54.793393  HCI_EVT   Number of Completed Packets
129  61.267529  HCI_EVT   Link Key Request
130  61.267801  HCI_CMD   Link Key Request Reply
131  61.277510  HCI_EVT   Command Complete (Link Key Request Reply)
132  61.307518  HCI_EVT   Encrypt Change
133  61.307538  RFCOMM    Rcvd UA DLCI=20
134  61.307719  RFCOMM    Sent UIH DLCI=0 MPX_CTRL Modem Status Command
                                  (MSC) Model Status Command
135  61.309530  RFCOMM    Rcvd UIH DLCI=0 MPX_CTRL Modem Status Command
                                  (MSC) Model Status Command
136  61.309611  RFCOMM    Sent UIH DLCI=0 MPX_CTRL Modem Status Command
                                  (MSC) Model Status Command
137  61.310510  RFCOMM    Rcvd UIH DLCI=20 UID
138  61.312600  HCI_EVT   Number of Completed Packets
139  61.314514  RFCOMM    Rcvd UIH DLCI=0 MPX_CTRL Modem Status Command
                                  (MSC) Model Status Command
140  61.314590  RFCOMM    Sent UIH DLCI=20 UID
141  61.314610  OBEX      Sent Connect - Folder Browsing
142  61.319504  HCI_EVT   Number of Completed Packets
143  61.831557  OBEX      Rcvd Success - Folder Browsing
144  61.832149  RFCOMM    Sent Obex fragment
145  61.832179  RFCOMM    Sent Obex fragment
146  61.832544  RFCOMM    Rcvd UIH DLCI=20
147  61.839529  RFCOMM    Rcvd UIH DLCI=20
148  61.840536  HCI_EVT   Number of Completed Packets
149  61.842537  RFCOMM    Rcvd UIH DLCI=20
```

```
150  61.848550  RFCOMM    Rcvd UIH DLCI=20 UID
151  61.855553  RFCOMM    Rcvd UIH DLCI=20
152  61.892560  OBEX      Rcvd Continue
153  61.892796  RFCOMM    Sent Obex fragment
154  61.892828  OBEX      Sent Put continue
155  61.894544  RFCOMM    Rcvd UIH DLCI=20
156  61.895543  RFCOMM    Rcvd UIH DLCI=20
157  61.896555  RFCOMM    Rcvd UIH DLCI=20
158  61.900551  RFCOMM    Rcvd UIH DLCI=20
159  61.902546  HCI_EVT   Number of Completed Packets
160  61.903523  RFCOMM    Rcvd UIH DLCI=20
161  61.906539  OBEX      Rcvd Continue
162  61.907768  RFCOMM    Sent Obex fragment
163  61.907798  OBEX      Sent Put continue
164  61.911531  RFCOMM    Rcvd UIH DLCI=20
165  61.917538  HCI_EVT   Number of Completed Packets
166  61.918527  RFCOMM    Rcvd UIH DLCI=20
167  61.921539  OBEX      Rcvd Continue
168  61.921756  RFCOMM    Sent Obex fragment
169  61.921781  OBEX      Sent Put continue
170  61.924552  RFCOMM    Rcvd UIH DLCI=20
171  61.930623  HCI_EVT   Number of Completed Packets
172  61.931537  RFCOMM    Rcvd UIH DLCI=20
173  61.935540  OBEX      Rcvd Continue
174  61.935747  RFCOMM    Sent Obex fragment
175  61.935773  OBEX      Sent Put continue
176  61.936541  RFCOMM    Rcvd UIH DLCI=20
177  61.976564  RFCOMM    Rcvd UIH DLCI=20
178  61.978528  HCI_EVT   Number of Completed Packets
179  61.978547  RFCOMM    Rcvd UIH DLCI=20
180  61.981529  RFCOMM    Rcvd UIH DLCI=20
181  61.982532  RFCOMM    Rcvd UIH DLCI=20 UID
182  61.984551  OBEX      Rcvd Continue
183  61.984738  OBEX      Sent Put continue
184  61.988553  RFCOMM    Rcvd UIH DLCI=20
185  61.995554  RFCOMM    Rcvd UIH DLCI=20 UID
186  62.001557  RFCOMM    Rcvd UIH DLCI=20
187  62.007634  RFCOMM    Rcvd UIH DLCI=20
188  62.025569  RFCOMM    Rcvd UIH DLCI=20
189  62.165643  OBEX      Rcvd Success
190  62.165962  OBEX      Sent Disconnect
191  62.168555  HCI_EVT   Number of Completed Packets
192  62.168572  RFCOMM    Rcvd UIH DLCI=20
193  62.173637  RFCOMM    Rcvd UIH DLCI=20 UID
194  62.180544  RFCOMM    Rcvd UIH DLCI=20
195  62.186560  RFCOMM    Rcvd UIH DLCI=20
196  62.192550  RFCOMM    Rcvd UIH DLCI=20
197  62.380552  OBEX      Rcvd Success
198  62.380721  RFCOMM    Sent DISC DLCI=20
199  62.382543  RFCOMM    Rcvd UIH DLCI=20
200  62.383552  HCI_EVT   Number of Completed Packets
201  62.386555  RFCOMM    Rcvd UA DLCI=20
202  62.386606  RFCOMM    Sent DISC DLCI=0
203  62.392552  RFCOMM    Rcvd UA DLCI=0
204  62.392653  L2CAP     Sent Disconnect Request
205  62.397557  HCI_EVT   Number of Completed Packets
206  62.399570  L2CAP     Rcvd Disconnect Response
207  64.402659  HCI_CMD   Disconnect
208  64.406613  HCI_EVT   Command Status (Disconnect)
209  64.568639  HCI_EVT   Disconnect Complete
```

Una vez establecido el canal L2CAP, con CID 0x0041, cuyo proceso para establecerse se explica en el ejemplo anterior, el protocolo RFCOMM debe crear su propio canal de comunicación. Para esto, realiza el intercambio de frames que se envían en el payload de los paquetes L2CAP. Estos contienen el campo Protocol Service Multiplexing (PSM) que les permite multiplexar distintos protocolos de las capas superiores. Cuando transporta paquetes RFCOMM, el valor del campo es 0x0003. El primer mensaje, el número 122, es enviado por el Host de la notebook y es el comando SABM (Start Asynchronous Balanced Mode). También utiliza canales que son

identificados por un DLCI (Data Link Connection Identifier). El otro dispositivo, si está dispuesto a formar la conexión, le responde con un UA (Unnumbered Acknowledgement). Estos dos frames se intercambian utilizando el DLCI 0 que se usa para enviar información de señalización o control, por lo que es necesario establecer otro canal RFCOMM para poder transferir datos del usuario, lo que se empieza a hacer a partir de la línea 124. Los primeros dos comandos, Parameter Negotiation (PN), en las líneas 124 y 126, son frames de tipo UIH (Unnumbered Information with Header Check), que al ser enviados en el DLCI 0 son de señalización. Aunque el canal RFCOMM aún no está establecido, los extremos negocian algunos parámetros como pueden ser: tamaño máximo del frame, flow control, etc. El nuevo canal, con DLCI 20 (0x14), se comienza a establecer en la línea 127 al enviarse el frame SABM, pero, antes de recibir el correspondiente UA, el protocolo LMP realiza el proceso de autenticación requerido por el nuevo canal. No es necesario crear un nueva link key, sino que se utiliza la que fue generada cuando se estableció la piconet. El controlador BR/EDR se la solicita al componente Host en la línea 129, Link Key Request, quien se la envía en la siguiente línea, Link Key Request Reply. Recién en la línea 133 se recibe el UA correspondiente al DLCI 20.

Entre las líneas 134 y 139 se intercambian mensajes Modem Status Command (MSC) del protocolo RFCOMM. Contiene señales de control de una interface virtual V.24 que indican los seteos que los cables de control RS-232 tendrían si los mensajes RFCOMM estuviesen siendo transferidos a través de cables y no de una conexión Bluetooth. Entre las señales que intercambia están: FC (Flow Control), RTC (Ready To Communicate), RTR (Ready To Receive), etc. Con el canal RFCOMM establecido, el protocolo OBEX puede empezar a realizar su trabajo. Esto sucede a partir de la línea 141, en la cual se comienza a establecer una conexión. Además de enviar el pedido de conexión, el cliente puede indicar el servicio que se necesita. En la contestación, que se puede observar en la línea 143, el cliente recibe el Connection ID que es utilizado para poder multiplexar varios pedidos sobre la misma conexión RFCOMM. Con la sesión establecida, el archivo blue.pcap se empieza a enviar desde la notebook hacia el teléfono celular. Todo el intercambio de mensajes se realiza hasta la línea 183, en la cual, el cliente le indica el servidor que se envía la última parte de la operación. Al recibir esto, el servidor le contesta que la transferencia resultó exitosa mediante un mensaje OBEX Rcvd Success (línea 189). A continuación, en la línea 190, el cliente le envía un mensaje al servidor para terminar la sesión OBEX indicándole el Connection ID que se quiere terminar. La respuesta a

este mensaje, indicando la finalización exitosa de la sesión, se encuentra en la línea 197, OBEX Rcvd Success.
Debido a que no existen más sesiones OBEX abiertas, las conexiones RFCOMM también se empiezan a eliminar. La primera que se cierra es la que tiene el DLCI 20, entre las líneas 198 y 201, que se había creado para realizar el intercambio de datos (en nuestro caso para copiar un archivo desde la notebook al celular). Como se puede ver en la línea 198, el cliente, enviando el mensaje RFCOMM Sent DISC, es quien inicia el proceso de desconexión, el cual finaliza en la línea 201 con el mensaje RFCOMM Rcvd UA. La segunda, y última, conexión que se cierra es la que tiene DLCI 0, lo que sucede en las líneas 202 y 203. Aunque este canal tiene una funcionalidad diferente a los demás canales RFCOMM, la forma de cerrarlo es similar.
A continuación, el mismo dispositivo que inició el cierre del DLCI 0, es el encargado de desconectar el canal L2CAP. El cliente, en la línea 204, envía el comando L2CAP Sent Disconnect Request, para iniciar la desconexión del canal con el Channel ID (CID) 0x0041 en ambos extremos. La respuesta arriba en la línea 206 con el mensaje L2CAP Disconnect Response. Por último, se cierra la conexión ACL creada por Link Manager del Controlado BR/EDR. Esto procedimiento, que se realiza en las líneas 207 y 209, es el último paso de toda la transferencia del archivo

3.4 Modo de operación opcionales

3.4.1 Low-Energy (LE)

El sistema Low Energy incluye características diseñadas para permitir el desarrollo de productos que requieren un menor consumo de energía, una menor complejidad y un menor costo que el modo BR/EDR. Su finalidad es para ser utilizado por aplicaciones con bajas velocidades de datos.
El modo LE, al igual que el modo ER/BDR, opera en la banda no licenciada ISM de 2,4 GHz, utiliza la tecnología FHSS, y soporta un "symbol rate" de 1 Ms/s que, con mediante una modulación de frecuencia binaria, que le permite alcanzar una velocidad de 1 Mb/s. Emplea dos esquemas de acceso múltiple: Frequency Division Multiple Access (FDMA) y Time Division Multiple Access (TDMA).En el modo FDMA se utilizan 40 canales físicos separados por 2 MHz., de los cuales, 3 son usados para señalización y los restantes 37 para datos. A su vez, el modo TDMA se basa en un esquema de polling en el cual un dispositivo transmite un paquete en

un tiempo predeterminado y el otro dispositivo responde con un paquete después de un intervalo predeterminado.
El canal físico está sud-dividido en unidades de tiempo conocidos como eventos. Los paquetes de datos se transmiten en esos eventos. Existen dos tipos de eventos: “advertising” y “connection”. Los dispositivos que envían paquetes en los eventos advertising son llamados “advertisers” y los que reciben esos paquetes sin tener la intención de conectarse al dispositivo que envió el paquete se los llama “scanners”.
Los dispositivos que necesitan formar una conexión con otro dispositivo deben escuchar paquetes “connectable advertising” enviados por un advertiser en un canal advertising. Tales dispositivos son llamados “initiator”, quienes, cuando escuchan uno de esos paquetes, le envían una solicitud de conexión al advertiser, finalizan el evento advertising y comienzan el evento connection. Cuando se establece la conexión, el initiator asumirá el rol de master en la piconet y el advertiser será el slave. Los eventos connection se utilizan para enviar paquetes de datos, en forma alternada, entre el master y un slave. Durante esta etapa, los dispositivos van saltando entre los canales y ese salto ocurre al inicio del evento. Cada evento de conexión es iniciado por el master, quien lo puede finalizar en el momento que lo desee.
Al igual que en ER/BDR, LE se define una jerarquía de canales, links y protocolos compuesta de la siguiente manera: canal físico, link físico, transporte lógico, link lógico y canal L2CAP. Dentro de un canal físico, se forma un link físico entre el master y el slave, nunca entre dos slaves. Un slave solo puede tener un link físico a un master por vez. El link físico es utilizado por uno o más transportes lógicos para el envío de tráfico asincrónico. Si se usan varios links lógicos sobre el mismo link físico se los debe multiplexar y es el resource manager, mediante una función de planificación (scheduling), el encargado de asignar los turnos para transmitir. Además de los datos del usuario, por estos links se envían paquetes del protocolo de control “link layer (LL)” para las capas físicas y de enlace. Este protocolo de señalización es enviado por el transporte lógico LE asincróno que se crea por default cuando un dispositivo se une a la piconet. Arriba de la capa de enlace se encuentra la capa L2CAP que provee una abstracción de los links y canales a las aplicaciones y servicios, y al igual que en el modo BR/EDR realiza fragmentación y defragmentación de paquetes, y multiplexación. L2CAP tiene un protocolo de control que es transportado sobre el transporte lógico default.
LE define dos capas adicionales por sobre L2CAP. Una es la Security Manager Protocol (SMP) que se encarga de realizar las funciones de

seguridad entre dispositivos y la otra es la Attribute Protocol (ATT) que provee un método para comunicar pequeñas cantidades de datos sobre una canal L2CAP. También es usado para determinar las capacidades y servicios de otros dispositivos.
A primera vista, parecería que Bluetooth Low Energy se plantea como un posible competidor de ZigBee, que está definido en el estándar IEEE 802.15.4. Éste, que en sus orígenes fue un desprendimiento de Bluetooth con el fin de desarrollar un stack más pequeño y de menor potencia para aplicaciones que hagan uso eficiente de la energía, está orientado a un rango diferente de aplicaciones. Su diseño está orientado a las redes mesh, no en tipo estrella como Bluetooth, lo que le permite tener mayores áreas de cobertura, aunque, a diferencia de Bluetooth, los dispositivos tienden a tener menor movilidad. Las comunicaciones son asincrónicas, lo que significa que determinados dispositivos, funcionando como routers, deben estar *despiertos* todo el tiempo consumiendo mayor cantidad de energía, pero los nodos finales puede *despertarse* en cualquier momento y transmitir, sin esperar por un slot de tiempo específico. Los dispositivos pueden dejar de responder en cualquier momento por lo que la red debe encontrar caminos alternativos dinámicamente.

3.4.2 Alternate MAC/PHY (AMP)

AMP, que es el controlador secundario en el sistema Bluetooth Core, habilita el uso de capas físicas y MAC alternativas para el intercambio de grandes cantidades de datos, generalmente asociada con la tecnología 802.11. Con el fin de ahorrar energía, AMP puede ser habilitado o deshabilitado cuando se lo necesite.
El radio BR/EDR sigue siendo utilizado para ejecutar las operaciones de descubrimiento, asociación, establecimiento de conexión y mantenimiento de la conexión. Una vez que se estableció la conexión L2CAP entre dos dispositivos usando el radio BR/EDR, el manager AMP de cada dispositivo pueden descubrir si el otro dispositivo también tiene la capacidad de AMP. Si esto es así, el core provee los mecanismos para mover el tráfico de datos desde el controlador BR/EDR al controlador AMP.

CAPÍTULO 4

Redes inalámbricas de banda ancha

4.1 Introducción

Sin lugar a dudas la convergencia de las tecnologías inalámbricas con Internet está llegando a producir un cambio trascendente en los diversos escenarios de la vida cotidiana, tal que el acceso a Internet de banda ancha será algo ubicuo en nuestras vidas.

En esa convergencia, WiMAX (Worldwide Interoperability for Microwave Access), con su obligada traducción: "Interoperabilidad Mundial para Acceso por Microondas", actúa como agente catalizador en la difusión de Internet y sus servicios, sin necesidad de cables, a cada sala, computadora personal, teléfono, y dispositivos de mano.

Esos servicios requieren, día a día, ancho de banda considerable, existiendo un crecimiento exponencial en la demanda de los mismos. Las soluciones tradicionales que proveen acceso a Internet de esas características generalmente recurren a tecnologías cableadas, tales como ADSL, cable módem, fibra óptica, etc.

Los proveedores de servicios de Internet, ISPs, también recurren a ellas, pero no las despliegan en zonas apartadas o rurales dada la baja oportunidad de negocio que representan, básicamente debido al costo de infraestructura de esas tecnologías.

Mientras las redes troncales han madurado ostensiblemente y presentando un alto grado de confiabilidad, la "última milla" aún subsiste como cuello de botella a la hora de implementar servicios de banda ancha, tales como voz en IP, video conferencia, juegos interactivos, "streaming" de video, etc.

WiMAX resulta una alternativa válida a dicha situación, proveyendo acceso de banda ancha a redes como Internet y por otra parte, contribuyendo a saltear la brecha tecnológica en los países o zonas menos desarrollados.

Las redes Wi-Fi, basadas en IEEE 802.11 han provisto al momento una importante cobertura y diversidad en las redes inalámbricas, pero presentan el inconveniente de su corto alcance, calidad de servicio y seguridad.

WiMAX, basado en 802.16, ofrece acceso a datos fijos y móviles. El estándar 802.16-2004 referencia al acceso fijo y el agregado 802.16e referencia a acceso fijo y móvil. Ambos especifican por otra parte

seguridad y calidad de servicio, que al momento eran especificaciones normalmente destinadas a las capas superiores.
Si bien las especificaciones técnicas están dadas por el IEEE, un agente clave en esta tecnología es el "WiMAX Forum" (http://wimaxforum.org).
El foro es una organización sin fines de lucro controlada por la industria que certifica y promueve la compatibilidad e interoperabilidad de los productos inalámbricos de banda ancha basados en el estándar 802.16.
Su principal objetivo es acelerar la adopción, establecimiento y expansión de la tecnología WiMAX a nivel mundial. El mismo trabaja cercano a los proveedores de servicios y reguladores para asegurar que los productos certificados WiMAX Forum cumplen con los requisitos de los usuarios y de los entes reguladores.
Presentados los actores principales veamos más en detalle la inserción de WiMAX en el contexto de Redes de Banda Ancha Inalámbricas ("Broadband Wireless Networks").

4.2 WiMAX - Redes de Banda Ancha

El objetivo primordial de la tecnología de banda ancha inalámbrica es bastante ambicioso dado que busca brindar servicios de gran ancho de banda en un contexto inalámbrico. Esos servicios los va a brindar en dos modalidades.
Una de ellas provee servicios similares a los de banda ancha en un contexto fijo pero con medio inalámbrico. Esta modalidad representa una alternativa/competencia a las tecnologías de Línea de Abonado Digital (Digital Subscriber Line - DSL) y Cable Modem. La otra modalidad agrega las funcionalidades de portabilidad y movilidad.
Con anterioridad a WiMAX existieron varios desarrollos tratando de cubrir este objetivo con características diversas y tratando de abarcar los diferentes niveles, desde el físico hasta los servicios, que dicho objetivo implica. Esos desarrollos tuvieron un origen común que es la falta de un estándar y un resultado común como consecuencia de ello que es la falta de interoperabilidad.
Esos desarrollos, vinculados con lo que más tarde sería WiMAX, podemos decir que evolucionaron hacia él en aproximadamente cuatro etapas [AND07], no necesariamente secuenciales en el tiempo.
Una primera etapa como diversificación de los servicios de telefonía, velocidades bajas, hasta 128Kbps y con el inconveniente de requerir antenas en el usuario, motivos por los cuales no prosperaron.
Una segunda etapa en la que se desarrollan sistemas en las bandas de 2,5GHz y 3,5 GHz, con capacidades de cientos de Megabits/segundo.

Posteriormente se desarrollan en las bandas de 24GHz y 39GHz. Son los sistemas "Local Multipoint Distribution Systems" (LMDS), limitados por la instalación de antenas en los usuarios y corto alcance. A fines de los 90 aparece "Multichannel Multipoint Distribution Services" (MMDS) en la banda de 2,5GHz y 3,5GHz. A las mayores velocidades de LMDS se debe agregar un mayor alcance, llegando a los 50 Km con transmisores de alta potencia y con requerimientos de visión directa (LOS, Line-Of-Sight) y antenas en los usuarios, que constituyeron un factor limitante en su difusión pese a las nuevas ventajas logradas.

Una tercera etapa, en la que los sistemas se caracterizan por no necesitar visión directa, identificándoselos como del tipo "Non-Line-Of-Sight" (NLOS), con menores necesidades de infraestructura. Normalmente la NLOS va a ser lograda recurriendo a las técnicas de Multiplexación por División de Frecuencia Ortogonal (OFDM) y Acceso Múltiple por División de Código (CDMA). Se consiguieron velocidades de decenas de Megabits/seg y alcances de un par de kilómetros. La componente faltante en esta etapa es mayormente la interoperabilidad por la falta de un estándar.

Finalmente, la cuarta etapa, en la que aparece la IEEE. En 1998 se forma el grupo 802.16 para desarrollar el estándar Red de Área Metropolitana Inalámbrica ("Wireless Metropolitan Area Network).

Las bandas de frecuencia iniciales definidas fueron las de 10 GHz y 66 GHz. Tecnológicamente estaban cubriendo los sistemas LMDS con LOS. El estándar se aprobó en diciembre de 2001, bajo el título "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems". Indicamos expresamente el título dado que es significativo en cuanto refleja su alcance, especificar la interfaz para sistemas fijos de acceso inalámbrico de gran ancho de banda y enfatiza el rol del WiMAX en cuanto a que cubre aspectos no contemplados por éste.

En el nivel físico define el uso de portadora única y un control de acceso con Multiplexación por División de Tiempo (TDM) y soporte de División de Frecuencia y de Tiempo en Dúplex, es decir FDD y TDD respectivamente.

Luego, el grupo se dedica a especificar el acceso en las bandas licenciadas y no licenciadas, 2GHz-11GHz, con la posibilidad de contar con NLOS. Incorpora, Multiplexación por División de Frecuencia Ortogonal (OFDM), y Acceso Múltiple por División de Frecuencia Ortogonal (OFDMA). Este trabajo quedó reflejado en el ammendment IEEE 802.16a-2003.

Con el tiempo se le fueron haciendo revisiones al documento anterior, que quedaron incluidas en un único estándar: IEEE 802.16-2004. Es

importante mencionar este documento dado que fue la base del estándar desarrollado para las redes HIPERMAN ("High Performance Metropolitan Area Network") por la ETSI ("European Telecommunications Standard Institute"). En esos años, el grupo de trabajo comenzó a desarrollar una ampliación del estándar para el soporte de servicios móviles en bandas licenciadas. Así aparece IEEE 802.16e en diciembre de 2005.
En el 2009 se publica un único estándar, IEEE 802.16-2009, al que se le agrega en mayo de 2011 el IEEE 802.16m.
Este último estándar, a la hora de escribir esto, incorpora tecnologías de última generación como MIMO multi-usuario, multiportadora, redes colaborativas y celdas "femto" o "femtocelda" [ABI06]. Una femtocelda es una estación base pequeña en tamaño y potencia, diseñada para el uso domiciliario. Normalmente se conecta a la red del proveedor de servicio a través de una conexión de banda ancha cableada, típicamente DSL o cable.
Tal vez lo más importante es que ha sido reconocido por la UIT como una tecnología IMT Avanzada (IMT = "International Mobile Telecommunications"), y se encuadra dentro de WiMAX versión 2 propuesta por el Foro WiMAX.
Indicamos aquí las diferentes versiones/evolución del estándar:

- IEEE 802.16m-2011 - 06-Mayo
- IEEE 802.16h-2010 - 30-Julio
- IEEE 802.16j-2009 - 12-Junio
- IEEE 802.16-2009 - 29-Mayo
- IEEE 802.16g-2007 - 31-Diciembre
- IEEE 802.16k-2007 - 14-Agosto
- IEEE 802.16e-2005 - 28-Febrero
- IEEE 802.16f-2005 - 01-Diciembre
- IEEE 802.17a-2004 - 29-Octubre
- IEEE 802.16-2004 - 01-Octubre
- IEEE 802.1D-2004 - 09-Junio
- IEEE 802.16a-2003 - 01-Abril
- IEEE 802.16-2001 - 08-Abril

Nuevamente recordamos el amplio alcance de IEEE 802.16 por un lado y la necesidad de desarrollar soluciones compatibles usando las familias IEEE 802 por otro, difíciles de lograr con tamaño alcance. Ese trabajo será delegado en el Foro WiMAX, que surge como desprendimiento del Wi-Fi Alliance, y que a ese momento había desarrollado tests de interoperabilidad para productos de la familia 802.11.

4.3 WiMAX - 3G - Wi-Fi

WiMAX no es la única tecnología de acceso de banda ancha, 3G y 802.11 también se desarrollaron en el tiempo y están incursionando en el campo de banda ancha.
En el caso de 3G debemos mencionar los proyectos 3GPP (Third Generation Partnership Project) y 3GPP2.
3GPP opera y se funda como un foro con el objetivo de especificar un sistema telefónico móvil de tercera generación, 3G, aplicable globalmente en base a las especificaciones de GSM (Global System for Mobile Communications), dentro del alcance del proyecto de la UIT, IMT-2000 (International Mobile Telecommunications). El grupo se constituyó en diciembre de 1998 (http://www.3gpp.org).
Muchos de los estándares dados por el grupo reciben el nombre de "Releases" y a partir del Release 8 aparecen bajo el término LTE, (Long Term Evolution).
Por su parte, 3GPP2 especifica estándares para tecnología 3G basada en IS-95 (CDMA), difundida como CDMA2000.
Tal vez el obstáculo a vencer por 3G para convertirse en competencia de WiMAX es su arquitectura de voz-datos claramente con una concepción diferente a la de IP. Como contrapartida a esto, mantiene la ventaja de su performance en escenarios móviles.
El mejor competidor, posiblemente, sea Wi-Fi. Tengamos en cuenta la gran diversidad de equipamiento de RF para la banda utilizada por Wi-Fi, permitiendo alcances de hasta 300m. Sigue siendo un alcance menor al posible con WiMAX pero que se puede suplir con una mayor densidad de puntos de acceso. Otro punto a favor de Wi-Fi es la alta velocidad, según lo especificado en 802.11n.
En un rápido análisis podemos decir que WiMAX estaría a medio camino entre 3G y Wi-Fi considerando no sólo las características tecnológicas de las mismas sino, también, el escenario actual en cuanto a difusión y resultados en campo.

4.4 WiMAX - LTE

LTE, siglas de "Long Term Evolution" (Evolución a largo plazo), surge a partir del Release 8 del 3GPP. Se fija inicialmente los siguientes objetivos:

- Velocidades de transmisión de pico de 100 Mbps en downlink y 50 Mbps en uplink, mejorando la velocidad de transmisión obtenible en el extremo de la célula
- Latencia del plano de usuario en la red de acceso radio inferior a 10 ms

- Ancho de banda escalable
- Interoperabilidad con sistemas 3G y sistemas no 3GPP

En el contexto de la UIT, LTE se encuadra en la familia IMT-2000, ya que en realidad IMT-2000 no es una tecnología de acceso radio en sí misma, sino una familia de tecnologías que cumplen los requisitos establecidos por la UIT para IMT-2000 y que son aprobadas por la propia UIT. La principal recomendación IMT-2000 es ITU-R M. 1457 [ITUR1457]. Debemos notar que en ésta se incluyó IEEE802.16 como miembro de IMT-2000.

WiMax está basado en el estándar IEEE 802.16, y, como muchas otras iniciativas del IEEE, es un estándar abierto que fue debatido ampliamente por la comunidad de ingenieros antes de ser ratificado. Este nivel de estandarización y apertura hace que la tecnología WiMax sea fácil y barata de comprar. WiMax requiere su propia red independiente.

Los más interesados en LTE, por otra parte, son los herederos del acuerdo 3GPP que mencionamos anteriormente, mayormente integrado por compañías telefónicas y fabricantes de equipos más acostumbrados a soluciones propietarias.

En teoría, tanto WiMax como LTE pueden proporcionar velocidades teóricas de acceso de hasta 100Mbps, velocidad ampliamente superior a la requerida por los usuarios finales. LTE ofrece menores tiempos de latencia, lo cual lo hace ligeramente mejor que WiMax para servir información multimedia.

A las compañías telefónicas bien establecidas, en general, les interesa más LTE. A partir del año pasado se observa un vuelco hacia LTE de grandes prestadoras como Verizon y AT&T.

4.5 Otros estándares

Al momento podemos considerar los estándares 802.20 y 802.22 en los cuales las tecnologías involucradas presentan algunas prestaciones comunes con WIMAX. En el contexto de este cuadro general de WIMAX diremos que:

- 802.20 incorpora a las características de WIMAX la movilidad en altas velocidades, hasta 250 Km/h
- 802.22 incorpora acceso de banda ancha a zonas rurales con arquitectura propia llamada Redes Inalámbricas de Área Regional (WRAN-Wireless Regional Area Networks). La tecnología subyacente a este estándar recurre a las radios cognitivas [DOY09]. La Radio cognitiva es un paradigma de la comunicación inalámbrica en la cual tanto las redes como los mismos nodos inalámbricos cambian los parámetros

particulares de transmisión o de recepción para ejecutar su cometido de forma eficiente sin interferir con los usuarios autorizados. Esta alteración de parámetros está basada en la observación de varios factores del entorno interno y externo de la radio cognitiva, tales como el espectro de radiofrecuencia, el comportamiento del usuario o el estado de la red. Recurre también a la utilización del espectro VHF y UHF en desuso por el avance de la TV digital.

4.6 Espectro disponible para las redes inalámbricas de banda ancha en nuestro país

Hace ya varios años, con el advenimiento de los teléfonos celulares en sus distintas normas, que la regulación de los servicios se hace siguiendo el principio de 'neutralidad tecnológica', es decir, se reglamentan los servicios pero sin definir el tipo de tecnología, quedando a criterio del prestador (así como también el planeamiento de las redes corre por cuenta del prestador). La tecnología WiMAX (en su versión FIJA 802.16d) se encuadra en la categoría que se denomina SFDVA (Servicio Fijo de Datos y Valor Agregado, donde caen las redes de datos de banda-ancha, acceso a Internet, etc.).
Hasta la primera versión de celulares analógicos (AMPS) se hacían normas con especificaciones completas dado que no había otra tecnología (como en el caso de AMPS), pero luego, con la aparición de diversas tecnologías, se siguió con reglamentaciones que siguen la neutralidad tecnológica. Exceptuando los servicios de Radiodifusión, donde siguen funcionando los mismos transmisores o con definición de norma única (por ejemplo TV Digital ISDB-Tb), permitiendo especificar las 'Normas de Servicio' que establecen ciertos parámetros técnicos que deben cumplirse.
La UIT, organismo a nivel mundial, entre otras cosas se encarga de identificar las bandas de frecuencias adecuadas para la explotación de los distintos servicios. En ese sentido, la UIT ha identificado principalmente tres bandas donde podría emplearse la tecnología WiMAX:

- Banda 2,5 GHz (2500 - 2690 MHz)
- Banda 3,5 GHz (3400 - 3600 MHz)
- Banda 700 MHz (698 - 806 MHz) (Banda conocida como 'Dividendo Digital')

4.6.1 Banda 2,5 GHz

Esta banda es la más 'universal' dado que la UIT la ha reconocido en sus tres regiones (Argentina pertenece a Región 2).

En la Argentina, la banda de 2,5 GHz está atribuida para el uso de Servicios FIJOS (por lo que no es posible implementar 802.16e que es WiMAX móvil ni 802.20). A su vez, los servicios FIJOS habilitados en la banda se dividen según la zona del país:

- En el interior del país, la banda está atribuida para Servicio Fijo MMDS (31 canales analógicos de 6 MHz, para TV analógica)
- En el centro de Buenos Aires y 180 km alrededor de dicho punto, la banda está atribuida para SFDVA (Servicio Fijo de Datos y Valor Agregado), que es la categoría donde cae el Servicio de Internet de datos de banda-ancha fijos. En esta banda ya se han realizado asignaciones (cubriendo el 50% de la banda aproximadamente) y, desde el año 2001, se ha suspendido la posibilidad de nuevas asignaciones (con vistas a asignar la banda para 3G). La canalización de la banda puede consultarse en la Resolución CNC 256/2001 (son canales de 12 MHz + 12 MHz básicamente)

4.6.2 Banda 3,5 GHz

En la Argentina, la banda de 3,5 GHz está atribuida también para el uso de Servicios FIJOS (por lo que no es posible implementar 802.16e que es WiMAX móvil ni 802.20). El servicio que está habilitado (sin distinción de la zona del país) es SFDVA, el cual ya se encuentra asignado en las principales ciudades del país (por lo que es difícil conseguir nuevas asignaciones). En esta banda, por ejemplo, una empresa ha implementado la tecnología WiMAX Fijo (802.16d). La canalización de la banda puede consultarse en la Resolución CNC 869/98 Anexo I (son canales de 25 MHz + 25 MHz FDD básicamente aunque pueden utilizar un ancho de banda menor al implementar el sistema).

La banda de 3,5 GHz está resguardada para el uso de Servicios satelitales. En ese sentido, en el Reglamento de Radiocomunicaciones de la UIT, a través de notas de pie de página, se exceptuaron varios países de la implementación de servicios IMT (denominación UIT para los servicios de 3G/4G) en 3,5 GHz. En Argentina se atribuyó para SFDVA la banda 3400 a 3700 MHz (donde podría emplearse WiMAX 3,5 Fijo). Hay otras bandas cercanas (3300 - 3324 MHz en conjunto con 3376 - 3400 MHz) donde podría emplearse WiMAX 3,3 Fijo.

General para Banda 2,5 GHz y 3,5 GHz: Las normas básicas para Servicio SFDVA se encuentran en la Resolución CNC Nº 232/2005 (reemplaza el Anexo X de la Resolución CNC Nº 235/2001).

Banda 700 MHz: En Argentina está atribuida para Radiodifusión (con

transición de TV analógica a TV digital).
Resumiendo, en la Argentina NO están las bandas atribuidas (2,5 GHz y 3,5 GHz) para el Servicio Móvil donde podrían desplegarse IEEE 802.16e (WiMAX Móvil) o IEEE 802.20, pero sí está permitido implementar WiMAX Fijo en 2,5 GHz (aunque están suspendidas nuevas asignaciones) y 3,5 GHz.

4.7 Características técnicas a cumplir por el servicio de banda ancha inalámbrica

Entendemos que para que este servicio resulte competitivo debe, entre otras cosas, proveer un "throughput" del orden de varios Mbps con QoS para poder soportar a su vez diversidad de servicios tales como datos, voz y multimedia. En general, soportar toda clase de aplicaciones basadas en IP en forma eficiente.
Para poder cumplir con estos requisitos será necesario dotar a las componentes tecnológicas del servicio de diversas características que detallamos a continuación.

4.7.1 Nivel Físico

Recordemos que este servicio incorpora NLOS (No-Line-Of-Sight). En este caso tendremos una mejor calidad de enlace frente a obstáculos, pero mayor pérdida en función de la distancia, generándose así problemas de alcance que pueden ser significativos.
También, por las características de propagación, tenemos caminos múltiples que ocasionan variaciones bruscas y rápidas en el nivel de señal recibido que dificultan el proceso de recepción.
Esos caminos múltiples, además, provocan interferencia entre símbolos (ISI) por las diferencias de retardo que puede haber entre ellos. Este efecto se profundiza en los casos de altas velocidades y en parte es el que provocó la incorporación de OFDM, ya que logra disminuir este tipo de interferencias.
En el caso del servicio móvil debemos considerar la dispersión de frecuencia por efecto Doppler.
La disponibilidad relativa del espectro hizo que se adoptase una arquitectura celular. Uno de los aspectos distintivos de ésta es la reusabilidad de frecuencias, pero esa reusabilidad, en los casos de gran densidad de celdas, hace que crezca la probabilidad de interferencias.
En este tipo de servicio donde se comparte el espectro es necesario incursionar en nuevos métodos de acceso para aprovecharlo mejor.

4.7.2 Calidad de Servicio (QoS)

Hablar de Calidad de Servicio implica caracterizar el tráfico, dado que cada tipo de tráfico requerirá diferentes demandas de recursos. De alguna manera, en presencia de los temas mencionados anteriormente, los tendremos multiplicados por los diferentes tipos de tráfico que se especifiquen en la Calidad de Servicio a ofrecer. Algo importante a considerar en esta componente es que la Calidad de Servicio no queda restringida al acceso inalámbrico sino que se continúa de usuario a usuario, participando e incorporándose los problemas típicos de QoS en IP.

4.7.3 Movilidad

Sin dudas que la movilidad representa el gran atractivo para el usuario del servicio, con las dos componentes principales de la misma que son el "roaming" y el "handoff". Roaming digamos que es necesario por cuanto permitirá el acceso a los usuarios, independientemente de su ubicación geográfica ocasional. El problema a considerar es el eventual incremento de tráfico por los excesivos mensajes de actualización y "paging" que esto requiere.
El "handoff" pesa y determina ostensiblemente la calidad de servicio dado que le permite al usuario desplazarse sin perder la sesión de datos en curso, lo que provoca una mayor necesidad de recursos. Este factor está ligado al de la movilidad de IP que trataremos en otro capítulo.

4.7.4 Portabilidad

Ésta requiere que los dispositivos sean alimentados por batería y livianos. En cuanto a lo liviano hay una considerable mejora de materiales. No tanta mejora se observa en las baterías, o si se lo observa lo hace en detrimento de la liviandad del dispositivo. WiMAX incorpora mecanismos de ahorro de energía contribuyendo a la portabilidad del servicio. Un gran consumidor de batería es el procesador digital de señal (DSP), contribuyente fundamental de la capa física para lograr las altas prestaciones actuales.

4.7.5 Seguridad

La seguridad está provista por una subcapa específica para esa tarea. Provee autenticación, privacidad y confidencialidad. Todo el tráfico WiMAX va encriptado. Soporta dos estándares de cifrado: 3DES (Data Encryption Standard) y AES. También soporta dos métodos de autenticación: protocolo RSA y EAP.

4.7.6 Plataforma IP

Ya consideramos la ventaja de soportar la pléyade de protocolos y servicios basados en IP. Ocurre que no es un escenario muy adecuado para un protocolo "best effort" como IP.
Éste constituye un tema vigente en la comunidad científica y comercial, atacándose tanto protocolos de red como de transporte. Así tenemos el desarrollo de IP móvil, ligado al desarrollo de IPv6, pero no excluyente y el de métodos de control de congestión atendiendo el escenario inalámbrico. Debemos notar que muchas de las premisas de las cuales parten la mayoría de las acciones de los mecanismos de control de congestión resultan inconvenientes en este escenario. Lo veremos más en detalle en el capítulo de IP Móvil.

4.8 Arquitectura de WiMAX

4.8.1 Nivel Físico

La base de este nivel es la multiplexación por división de frecuencia ortogonal, OFDM. Este esquema de transmisión aparece también en DSL y Wi-Fi. En principio, podemos decir que es eficiente, permitiendo operar a altas velocidades, sin necesidad de visión directa, (NLOS) y en caminos múltiples.
OFDM pertenece a una familia de esquemas de transmisión llamada "modulación por multiportadora" que se basa en la idea de dividir un "stream" de alta velocidad en varios "streams" de baja velocidad y modulándolos a cada uno de ellos con portadoras diferentes, comúnmente llamadas subportadoras o tonos. Cabe aclarar que los esquemas con multiportadora contribuyen a disminuir la interferencia intersímbolos, ISI, dado que alargan el tiempo de símbolo resultando el retardo del canal inducido por caminos múltiples insignificante frente a éste y así reducir la amplitud de ISI. El tiempo de símbolo se alarga recurriendo a la división del stream de datos original en varios streams de datos en paralelo de menor velocidad. También por eso resulta tan trascendente este esquema en casos de alta velocidad donde la duración del símbolo resulta menor que en bajas velocidades.
Las subportadoras se eligen ortogonales entre sí, con la ventaja adicional que puede haber superposición de canales y no producirse interferencia. Con la elección adecuada de las subportadoras se consigue que la señal OFDM resulte equivalente a la transformada discreta inversa de Fourier, IDFT, fácilmente implementable a través de la transformada rápida inversa de Fourier gracias al avance de los procesadores digitales de señales, DSPs.
¿Cuál ha de ser el tamaño de la FFT? Cuanto mayor sea mejor

protección contra ISI se habrá logrado pero el efecto Doppler se hace más evidente resultando perjudicial para aplicaciones móviles.

4.8.1.1 Implementación de OFDM en WiMAX

La implementación de OFDM en WiMAX se hace teniendo en cuenta si se trata de un servicio fijo o móvil.

Servicio fijo:

La longitud de la FFT se definió en 256 con 192 subportadoras para datos, 8 como pilotos y sincronización y el resto como subportadoras de banda de guarda. En la implementación lo que suele hacerse es variar el tiempo de guarda, para lograr establecer un equilibrio entre la ocupación eficiente del espectro y el retardo. En la tabla a continuación se presentan los parámetros junto con los del servicio móvil.

Parámetro	WiMAX Fijo	WiMAX móvil			
FFT	256	128	512	1024	2048
Subportadoras de datos	192	72	360	720	1440
Subportadoras piloto	8	12	60	120	240
Subportadoras de guarda	56	44	92	184	368
Ancho de banda del canal (MHz)	3,5	1,25	5	10	20
Espacio de subportadora (KHz)	15,625	10,94			
Duración de símbolo (μs)	64	91,4			
Tiempo de guarda, 12,5%(μs)	8	11,4			

Servicio Móvil:

Aquí tenemos una variación posible en el tamaño de la FFT que va desde 128 a 2048. Si se recurre a un aumento del ancho de banda se incrementa ese tamaño resultando en un espacio de guarda constante de 10,94 KHz, como queda indicado en la tabla, que también resulta adecuado para un escenario móvil en lo que respecta a la incidencia del efecto Doppler.

Subcanalización:
Las subportadoras se dividen en varios grupos de subportadoras llamados subcanales. En el caso del servicio fijo tenemos una forma limitada de subcanalización y solamente en el "uplink". Se definen 16 subcanales, donde 1, 2, 4, 8, o la totalidad de ellos pueden asignarse a una estación suscriptora (SS). Esta canalización permite a las estaciones suscriptoras transmitir utilizando sólo una fracción muy pequeña del ancho de banda adjudicado (1/16). Esto trae una mejora considerable en la performance del enlace.
En el caso de móvil se permite subcanalización en "uplink" y "downlink". Se pueden asignar diferentes subcanales a diferentes usuarios conformando así un acceso múltiple, dándole el nombre al esquema utilizado, OFDMA.
Los subcanales se arman a partir de subportadoras contiguas o distribuidas en forma aleatoria a través del espectro disponible. Éste último por la diversidad de frecuencia que conlleva resulta de extrema utilidad en los escenarios móviles. WiMAX partió de una subcanalización de 15 subcanales para el "uplink" y 17 para el "downlink", luego definió 30 y 35 para el caso de mayor ancho de banda.

4.9 IEEE 802.16-2009

Veamos ahora con mayor detalle el modelo de referencia y alcance del estándar [IEEE Std 802.16™-09], ejemplificados en la Figura 4.1.

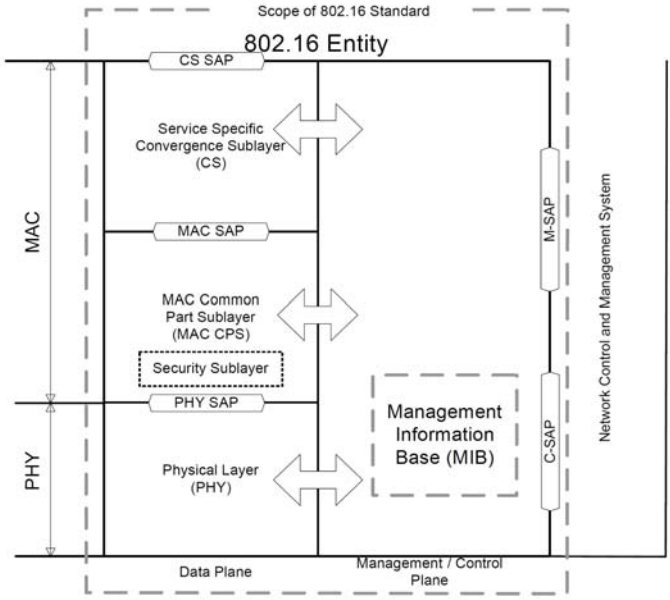


Figura 4.1 Modelo 802.16

El nivel MAC comprende tres subcapas. La Subcapa de Convergencia Específica del Servicio (CS) convierte lo recibido del nivel superior de servicio a través del Punto de Acceso del Servicio (CS SAP) en Unidades del Servicio de Datos de este nivel (MAC SDU), que a su vez será recibido por la Subcapa Común (MAC CPS), a través del Punto de Acceso MAC (MAC SAP). En este punto se incluye la clasificación de tráfico y su asociación al Identificador de Flujo de Servicio correspondiente (SFID) y al Identificador de Conexión (CID). Dada la presencia en cierta manera de un nivel extra, el de convergencia, en este punto puede tener lugar la compresión y/o remoción de encabezamientos (PHS). Aunque se han definido varias especificaciones de la subcapa de convergencia para una mejor interfaz con los niveles superiores, tales como ETHERNET, IP, ATM, etc.; WiMAX por el momento sólo soporta IP.

La MAC CPS provee las funcionalidades de acceso al sistema, asignación de ancho de banda, establecimiento de la conexión y mantenimiento. Aunque no está indicado en la figura tengamos en cuenta que también maneja componentes de calidad de servicio en la transmisión y en el despacho de los datos sobre el nivel físico (PHY).

La última subcapa es la de seguridad. MAC provee servicios de autentificación, intercambio de claves y encriptación.

MAC intercambia los mensajes de datos y control con el nivel físico (PHY) a través del Punto de Acceso correspondiente (PHY SAP). Al igual que en otros estándares, el PHY es dependiente de la implementación, especialmente del rango de frecuencias de trabajo.
El estándar reconoce tres tipos de dispositivos: Estaciones Base (BS). Estaciones Suscriptoras (SS) y Estaciones Móviles (MS).
Dado que estos dispositivos se podrán integrar a otras redes se incluye también como podemos ver en la figura 4.2 una capa de Control de Red y Administración del Sistema (NCMS). Esta capa permite que los niveles PHY y MAC se mantengan independientes de la arquitectura de la red, de la red de transporte y de los protocolos utilizados, consiguiendo así una mayor flexibilidad. Se instala en las BSs y SSs/MSs, y, para que pueda interactuar con niveles superiores, se definió un Punto de Acceso de Control y otro de Administración, C-SAP y M-SAP respectivamente. En la Figura 4.2 vemos el modelo de gestión que propone el estándar.

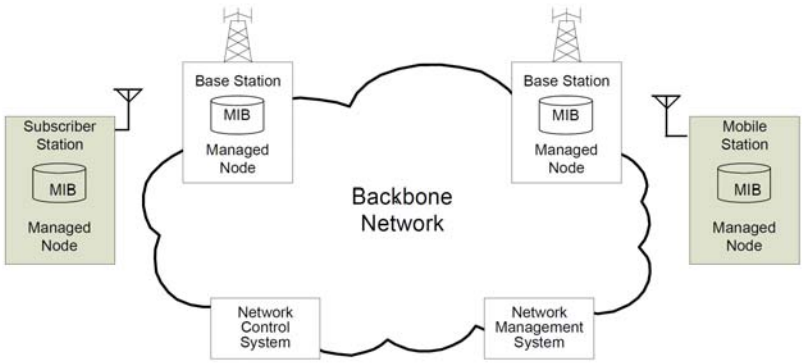


Figura 4.2 Modelo de gestión

Los nodos administrados, BS, MS y SS, adquieren los datos de gestión necesarios bajo la forma de objetos MIB. En este caso se los identifica como de Interfaz de Red Inalámbrica, (wmanIfMib) y de Dispositivo de Red Inalámbrica (wmanDevMib) que se envían al sistema de control bajo protocolo SNMP.
El sistema de control posee la información de flujo de datos y de QoS que las BSs necesitan conocer cuando una SS o MS ingresa a la red. Este intercambio de información se lleva a cabo bajo una segunda conexión. En caso de no estar disponible se debe dar la posibilidad de poder hacerlo a través de otras interfaces de dispositivo o a través de la capa de transporte en la conexión de datos. En la Figura 4.3 vemos la interacción del sistema de control con los dispositivos.

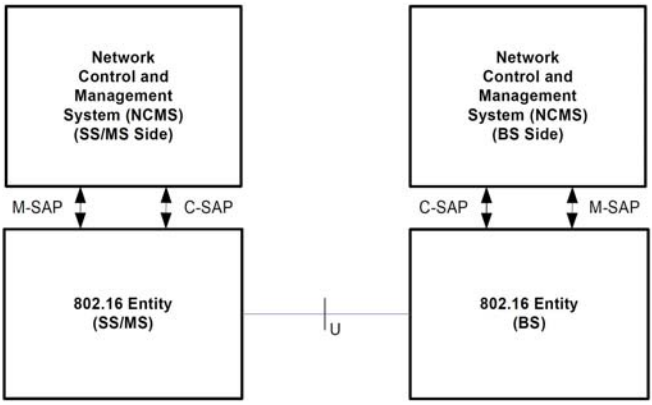


Figura 4.3 Sistema de control

Normalmente la división entre M-SAP y C-SAP se da en términos de las primitivas más o menos sensibles al retardo. Así tenemos:

M-SAP	C-SAP
Configuración del Sistema	Manejo de Handovers
Estadísticas de Monitoreo	Manejo de ahorro de energía
Notificaciones/Eventos	Reserva de ancho de banda
Administración de la Interfaz	Manejo del establecimiento de conexiones

Los objetos MIB se especifican acorde con el IETF RFC 2578.

4.9.1 Subcapa de Convergencia

Como se indicó más arriba, esta subcapa no es única sino que está especificada para varios protocolos a ser transportados por la trama 802.16. Precisamos más las funciones de esta subcapa:

- Clasificación del tráfico recibido
- Supresión del encabezado recibido (opcional)
- Entrega del paquete formateado según corresponda al MAC SAP, asociado con el flujo de servicio para su transporte al correspondiente peer MAC SAP. Esta entrega se hará acorde con la QoS, fragmentación, concatenación y toda otra función de transporte asociada con la conexión correspondiente.
- Recepción del CS PDU del correspondiente MAC SAP

- Rearmado de encabezado si corresponde (opcional)

4.9.2 MAC SDU

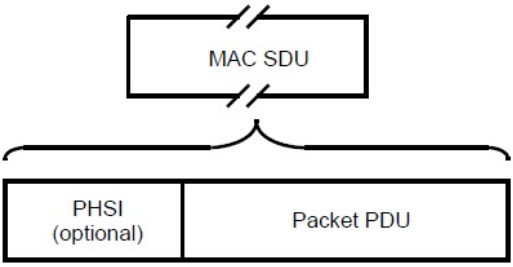


Figura 4.4 Estructura SDU

Una vez que el tráfico se ha clasificado la unidad de datos correspondiente se encapsula simplemente como se indica en la figura. El PHSI (Packet Header Supression Index) aparece sólo en el caso que se haya acordado la supresión de encabezado en la conexión correspondiente.

4.9.3 Clasificación

Este proceso asocia el MAC SDU a una conexión en particular que tenga en curso con su par MAC, considerando las características del tráfico y los requerimientos de QoS. Esto se implementa definiendo reglas de clasificación que se aplican a todo paquete que ingresa a la red IEEE 802.16.
Esta regla normalmente se especifica indicando algún criterio dentro del protocolo de red (dirección IP destino, por ejemplo), criterio de prioridad y referencia a un Identificador de Conexión (CID). Además dadas las características de tráfico y la aplicación del concepto de flujo de datos tenemos criterios a aplicar en el uplink (UL) por la SS y en el downlink (DL) por la BS según vemos en las Figuras 4.5 y 4.6 respectivamente.

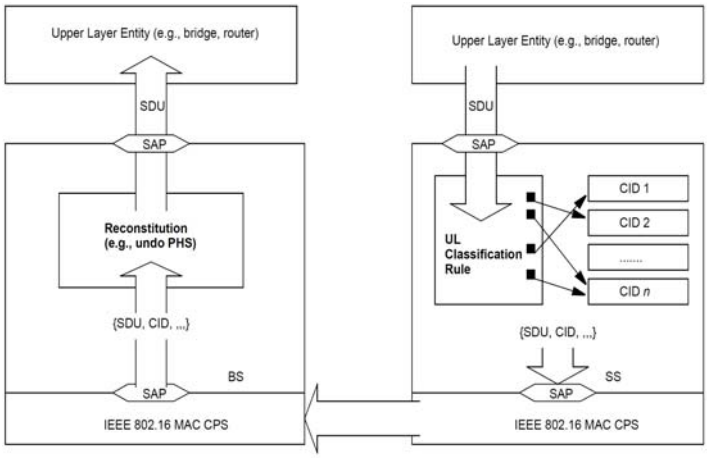


Figura 4.5 Criterios de UL

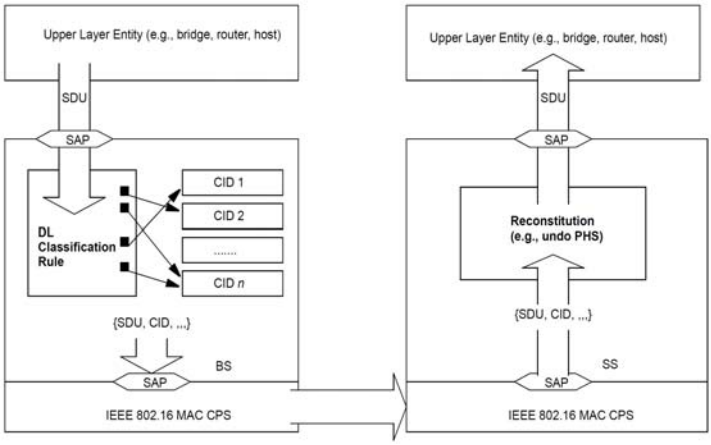


Figura 4.6 Criterios de DL

La subcapa de convergencia descarta aquellos paquetes que no encuadren en los criterios de clasificación fijados.

4.9.4 CS - Ethernet/IEEE802.3

El encapsulamiento se indica en las Figuras 4.7 y 4.8, sin y con supresión de encabezado respectivamente

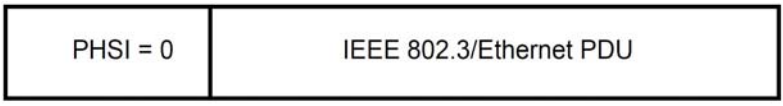


Figura 4.7 Sin supresión de encabezado

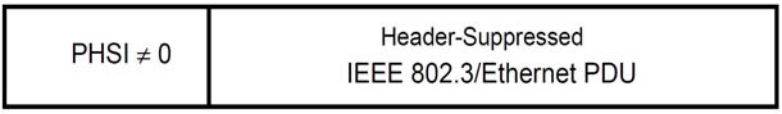


Figura 4.8 Con supresión de encabezado

El payload del PDU que vemos en las figuras anteriores no incluye el FCS de Ethernet. Puede sumarse a la supresión del encabezado de Ethernet la del de IP según RFC 3095 (ROCH), estableciéndose un canal ROCH según indica la citada RFC.
En cuanto a las reglas de clasificación típicas para este caso particular podemos mencionar parámetros de VLAN y encabezamientos de IP.

4.9.5 CS - IP

El encapsulamiento es similar al anterior y con las mismas prestaciones en cuanto a la supresión de encabezados de los paquetes de nivel superior como queda indicado en las figuras 4.9 y 4.10.

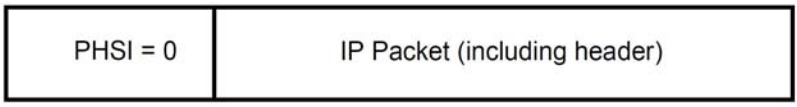


Figura 4.9 IP con header

Figura 4.10 IP sin header

Se contempla la posibilidad de recurrir a ROCH en lugar de PHS para comprimir los encabezados de IP [RFC3095]. En la Figura 4.11 se indica el proceso de ROCH.

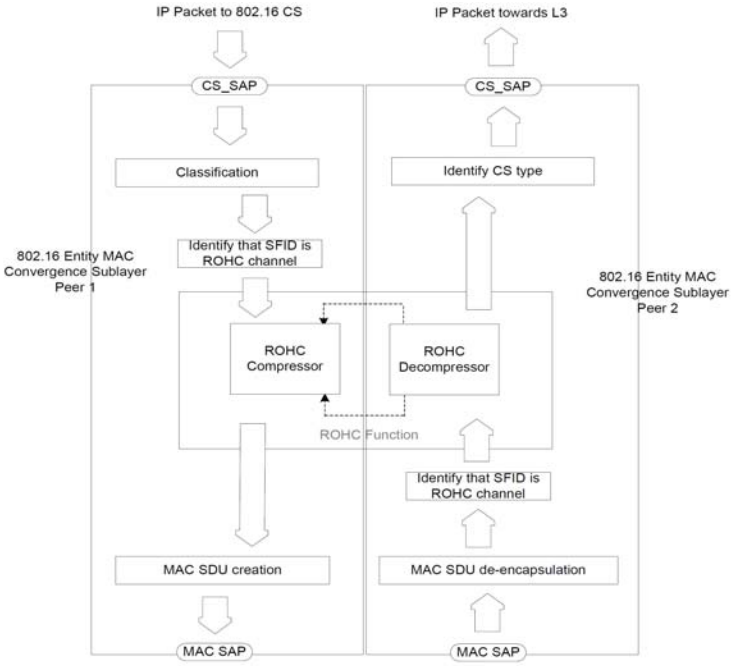


Figura 4.11 ROCH

Como reglas de clasificación normalmente se emplean campos de los datagramas IP y de los segmentos de los protocolos de transporte.

4.9.6 CS - Paquete Genérico

Se definió esta subcapa con la idea de proveer una estructura que se acomodase a diversidad de protocolos, como se indica en la Figura 4.12.

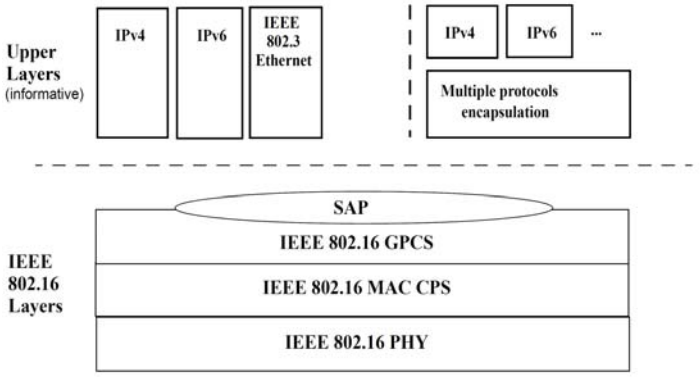


Figura 4.12 CS Genérico

Esta subcapa utiliza el GPCS SAP, un caso particular de implementación del CS SAP. La implementación es tal que el GPCS no necesita interpretar los encabezados de los protocolos de nivel superior para poder "mapear" los paquetes de nivel superior en conexiones MAC IEEE 802.16. Los parámetros claves de ésta estructura son:

- SFID (Service Flow ID): el identificador ya conocido. Será combinado con la dirección MAC para dar lugar a una conexión MAC y su correspondiente ID
- MAC Address: los 48 bits de siempre con la estructura definida en 802.3
- DATA: el campo de datos o payload
- Length: cantidad de bytes que ocupa el payload

4.9.7 Subcapa MAC común

El enlace propuesto por el estándar opera en el DL en forma de Punto-Multipunto. Dada una frecuencia y una antena, todas las estaciones reciben la misma transmisión. La BS es la única que transmite en esta dirección por lo que no necesita coordinar su operación con otras estaciones, excepto en el caso en que se esté operando en Duplexación por División de Tiempo (TDD) en la que hay tiempos alternados de transmisión de UL y DL. Todas las estaciones reciben el mensaje y chequeando el CID determinan el destino correspondiente.
La transmisión en el UL es por el contrario por demanda, donde dependiendo de la QoS contratada la SS podrá transmitir en forma permanente o sólo será autorizada por la BS después de haber enviado la solicitud de transmisión correspondiente. Se definen varios

mecanismos en el protocolo con el objeto de equilibrar la performance con los recursos utilizados.
Todo el equipamiento en este nivel tendrá una dirección MAC universal de 48 bits de acuerdo con IEEE Std 802, como se mencionó anteriormente. Esta dirección se utiliza en el establecimiento de la conexión inicial de la SS. También aparece en el proceso de autentificación entre la BS y la SS.
Las conexiones se identifican con un CID de 16 bits. En el proceso inicial de conexión se establecen dos pares de conexiones de administración, conexiones básicas (UL y DL) y conexiones primarias de administración (UL y DL). Puede llegarse a un tercer par de conexiones llamadas secundarias de administración, siempre entre la BS y la SS. Estos tres tipos de conexiones ejemplifican el hecho que haya tres niveles de QoS diferentes entre la BS y las SSs.
La conexión básica se utiliza para intercambiar mensajes de gestión o administración generalmente cortos y de respuesta rápida. La primaria para mensajes de mayor longitud y con cierta tolerancia al retardo. La conexión secundaria se utiliza para el envío de mensajes tolerantes a retardos y basados en protocolos estándar como DHCP, TFTP, SNMP, etc.

4.9.7.1 Estructura del MAC PDU

La estructura de datos definida para este nivel, MAC PDU, será como se indica en la Figura 4.13.

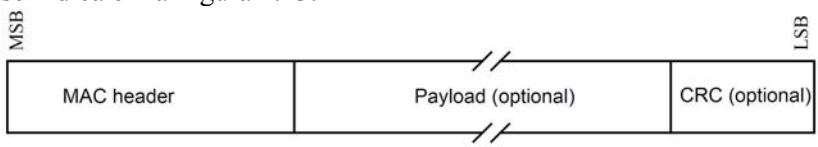


Figura 4.13 MAC PDU

El encabezado (Header) es de longitud fija, seguido del payload. Si está el payload puede contener subencabezados y más de un MAC SDU o fragmentos. El campo CRC es opcional, no así para OFDM y OFDMA del nivel PHY.
No existe un único encabezado sino que hay encabezados para UL y DL dependiendo del contenido que transportan.
Se define un encabezado MAC de DL que es el MAC Header genérico, que encabeza todo MAC PDU de DL, conteniendo mensajes de gestión o datos provenientes del CS.
Se definen dos formatos de MAC Header para UL. El primero es el MAC Header genérico que encabeza cada MAC PDU que contienen mensajes de gestión o de datos provenientes del CS, diferenciándose

porque el HT (Header Type) está en 0, como se indica en la Figura 4.14. El segundo es el formato de MAC Header sin payload en el que el HT está en 1. En este caso no existe payload ni CRC.
Veamos, a modo de ejemplo, los formatos de encabezado en general, tal como lo indica el IEEE 802.16, y a continuación la estructura del encabezado genérico.

Syntax	Size (bit)	Notes
MAC Header() {	—	—
HT	1	0 = Generic MAC header 1 = Bandwidth request (BR) header
EC	1	If HT = 1, EC = 0
if (HT == 0) {	—	—
Type	6	—
Reserved	1	Shall be set to zero
CI	1	—
EKS	2	—
Reserved	1	Shall be set to zero
LEN	11	—
}	—	—
else {	—	—
Type	3	—
BR	19	—
}	—	—
CID	16	—
HCS	8	—
}	—	—

Figura 4.14 Construcción de los encabezados

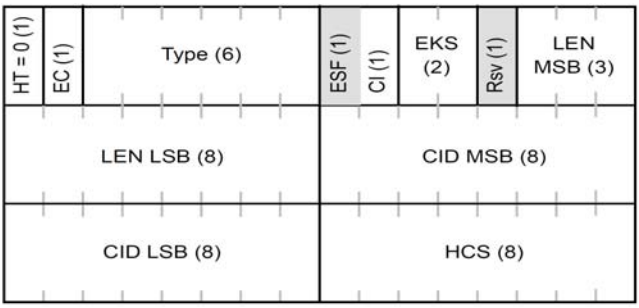


Figura 4.15 Encabezado de DL

A continuación se da un detalle de los campos:

Campo	Longitud (bit)	Descripción

HT	1	Tipo de encabezado, en este caso = 0
EC	1	Control de encriptado 0 = Payload ausente o sin encriptar 1 = Payload encriptado
Type	6	Identifica subencabezados y tipos de payload
ESF	1	Extensión de subencabezado. 0 = No hay extensión 1 = Hay extensión y está a continuación del encabezado genérico
CI	1	Indicador de CRC 0 = No incluye CRC 1 = Se incluye CRC a continuación del payload
EKS	2	Índice de la clave de encriptación y vector de inicialización para encriptar el payload
RSV	1	Sin uso por el momento
LEN	11	Indica la longitud en bytes del MAC PDU incluyendo el encabezado y el CRC si está presente
CID	16	Identificador de conexión
HCS	8	Verificador del encabezado. Es un CRC con polinomio generador x^8+x^2+x+1

Como indicamos anteriormente se define un encabezado sin payload, que será aplicable solamente a los mensajes de UL, de varios tipos: de señalización, de control, de reserva de ancho de banda, de monitoreo, etc. Remitimos al IEEE STD 802-16-2009 para el detalle completo.
A su vez se definen cinco tipos de subencabezados que acompañan al Header MAC genérico, cuatro subencabezados para PDU y uno para SDU. Los mismos se insertan a continuación del encabezado básico y en el caso de haber varios en un orden predeterminado. El único subencabezado de SDU es el PSH (Packing Subheader).
Otro tipo de mensaje definido es el de gestión de MAC. Los mismos se transportan en el payload del MAC PDU. Al momento se han definido 62. Presentan una estructura sencilla con un campo que identifica el tipo y, luego, según éste puede tener campos adicionales.

4.9.7.2 Armado del MAC PDU

No vamos a detallar todos los procesos que se llevan a cabo para la construcción del MAC PDU, pero consideramos oportuno describir la construcción a través de un diagrama de flujo, según Figura 4.16.

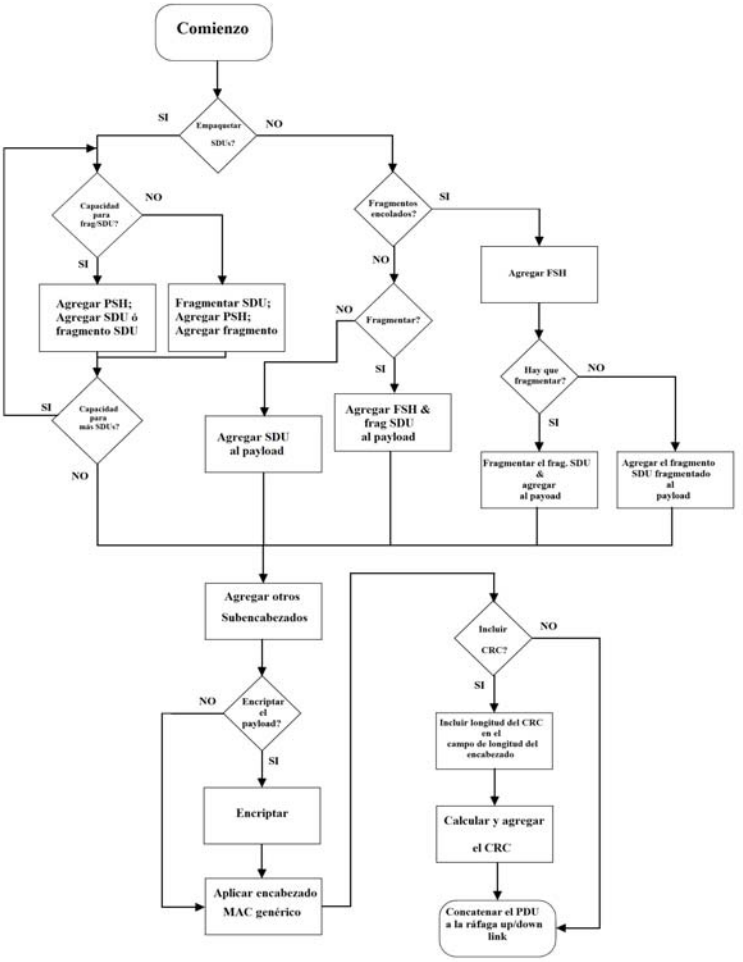


Figura 4.16 MAC PDU

A continuación vemos algunos MAC PDUs que pueden resultar del proceso anterior, Figura 4.17.

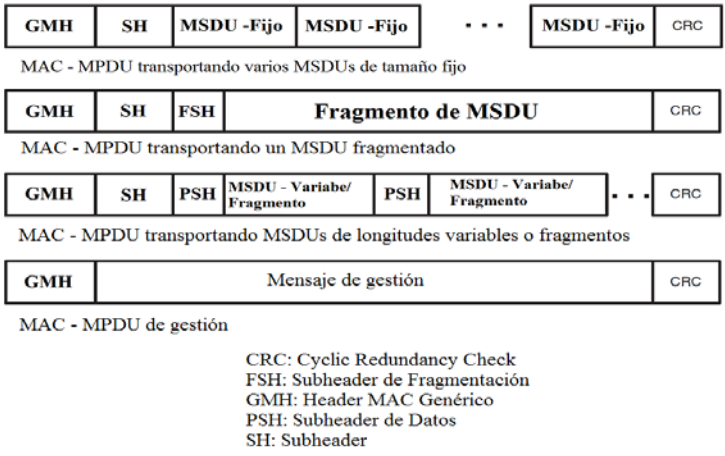


Figura 4.17 MAC PDUs

4.9.8 Algo más de la estructura de la trama

La unidad de recurso que WiMAX puede asignar, ya sea en frecuencia o en tiempo, es el "slot". Cada slot consiste de un subcanal sobre uno, dos o tres símbolos OFDM, dependiendo del esquema de subcanalización adoptado. Una serie contigua de slots asignados a un usuario constituye "la región de datos del usuario".

Como se indica en la Figura 4.18, la trama de WiMAX se divide en dos subtramas, downlink y uplink, separadas por una guarda. En el gráfico también se aprecia que puede trabajar con TDD y FDD simultáneamente.

El downlink comienza con un preámbulo para control del nivel físico como sincronización, estado del canal, etc. A continuación aparece un encabezado de control de trama (FCH) que contiene información de la configuración del canal, esquema de codificación y modulación empleados, etc. Los usuarios tienen asignadas las regiones de datos en la trama que se encuentran especificadas en los mensajes MAP tanto de uplink como de downlink, (UL MAP y DL MAP). Se incluye en ellos el perfil del canal de cada usuario. Dada la criticidad de este mensaje se lo suele enviar a través de un enlace confiable, típicamente BPSK con FEC 1/2.

Como esa información corresponde a cada usuario, el overhead que acarrea este tipo de mensaje es considerable por lo que se suele enviar a alta velocidad y, además, comprimido.

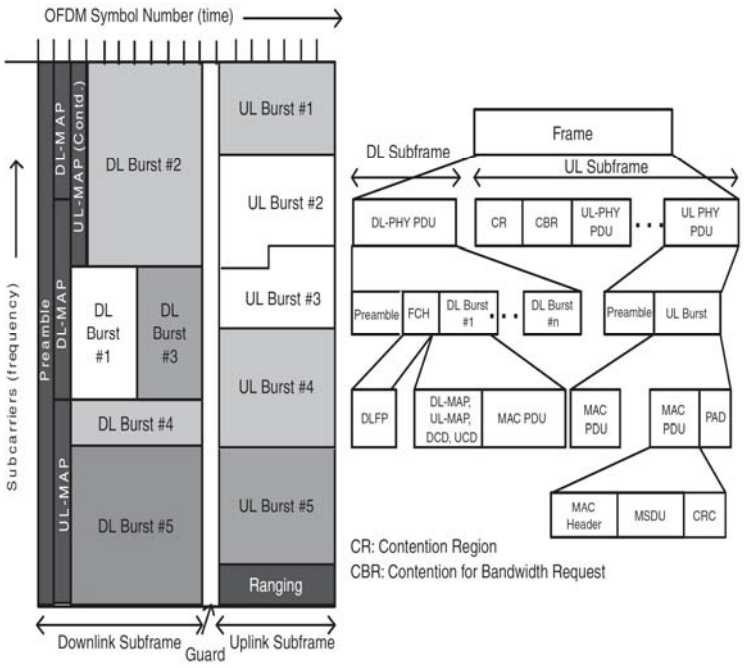


Figura 4.18 Trama MAC

No está predefinido un número máximo de bursts de usuarios en la trama. Es más, puede variar de una a otra, por lo que tenemos una longitud variable que, generalmente, va desde los 2 ms a los 20 ms.

El uplink está constituido por los bursts de usuario y una primera parte reservada para acceso por contención. Esa parte se utiliza para realizar ajustes de potencia al establecerse un nuevo enlace y para solicitar recursos de ancho de banda. Eventualmente se lo puede utilizar para transporte de datos con calidad de servicio best-effort, si el volumen a transportar es reducido.

Además, el uplink tiene un campo indicador de calidad de servicio del canal ("Channel Quality Indicator Channel" - CQICH) para que las estaciones envíen reporte de QoS y el controlador en la estación base pueda hacer las correcciones del caso. Habrá entonces un ajuste en el esquema de modulación y codificación de cada enlace según lo que reporten las estaciones.

Nos podremos encontrar entonces con un rango de velocidades en uplink y downlink que va desde los 950 Kbps (DL)-330Kbps (UL) en BPSK, FEC: 1/2 con un ancho de banda de 3,5 MHz y 256 OFDM, hasta 25.000 Kbps(DL)-6.800 Kbps(UL) con 64 QAM, FEC: 5/6 en un canal de 10 MHz y 1024 OFDMA.

Debemos tener en cuenta que en este tipo de red nos encontramos con los usuarios y la estación base, dado que la funcionalidad del nivel MAC dependerá del tipo de estación.
El nivel MAC de la estación base es responsable de asignar el ancho de banda a todos los usuarios, tanto en el uplink como en el downlink. En el caso en que una estación de usuario tenga varias sesiones con la estación base, la estación del usuario administrará el ancho de banda dado por la estación base entre las sesiones que tenga establecidas. En el caso del downlink la estación base puede asignar ancho de banda a cada estación, en función de las características del tráfico entrante, sin la participación de las estaciones. En el caso del uplink la asignación se realiza en función de las solicitudes enviadas por las estaciones.
Se definieron varios mecanismos para el pedido de ancho de banda. El mecanismo elegido por la estación para solicitar recurso dependerá de la QoS requerida por ésta y demás parámetros de tráfico. La estación base otorga el recurso con carácter dedicado o compartido. Éste es el proceso reconocido como de "polling" que puede hacerse en forma individual, o sea, estación por estación o por grupos definido como "multicast". Se recurre a esta modalidad cuando no se dispone del ancho de banda necesario para hacerlo individualmente. En este caso, el slot de tiempo asignado para hacer la petición del recurso es compartido y, por lo tanto, habrá contención del mismo por lo que se definió un mecanismo de acceso. Estos requerimientos podrán hacerse en forma de "piggyback" con la transmisión de datos en curso.
A continuación vemos algunas capturas de tramas WiMAX encapsuladas en Ethernet, Figuras 4.19 y 4.20, realizadas con Wireshark. Se puede apreciar en la primera de ellas el código de protocolo Type de Ethernet asignado a 802.16, "0x08F0". La misma presenta un encabezado MAC genérico, sin encriptación, no incluye CRC ni subencabezados. Se puede apreciar también la identificación de la sesión (CID = 65534)

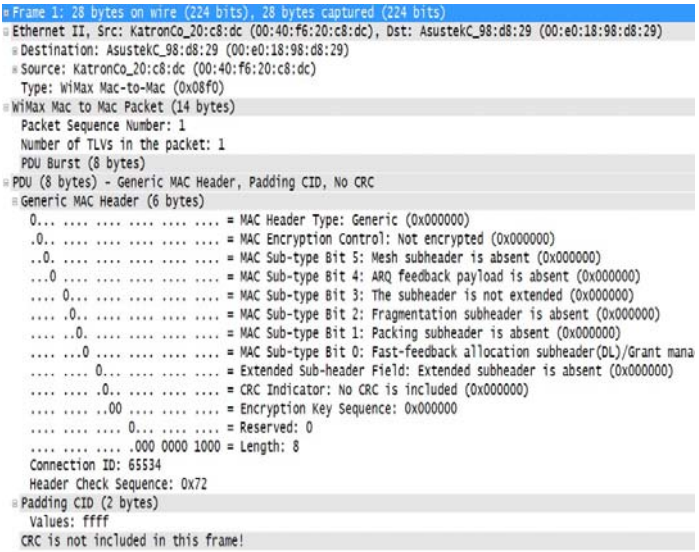


Figura 4.19 Captura 1

La segunda captura se trata de un encabezado MAC genérico, con empaquetado, incluyendo CRC, datos y gestión.

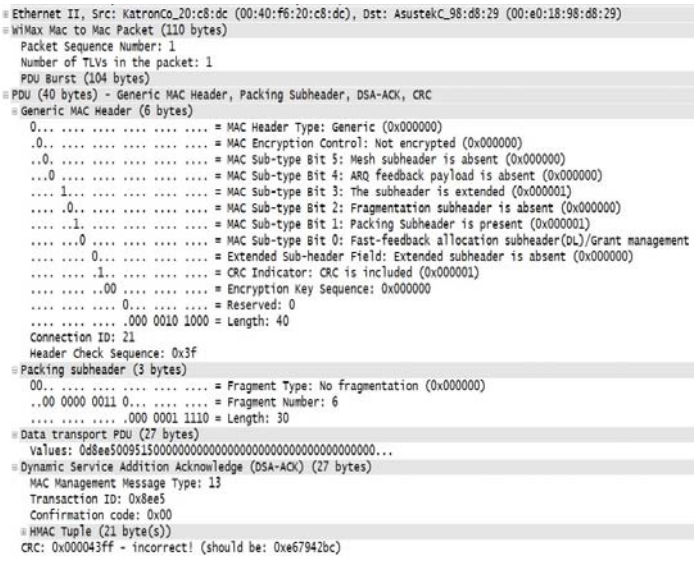


Figura 4.20 Captura 2

4.10 Calidad de Servicio

Incorporar Calidad de Servicio en este nivel es sin duda una

característica innovadora de este estándar, ya que al momento de su lanzamiento esta propiedad la encontrábamos especificada en niveles superiores dentro de las plataformas de IEEE.
Presenta similitudes con el estándar de cable modem, DOCSIS, y con conceptos empleados en IPsec, convirtiéndola en una plataforma orientada a la conexión. En los requerimientos para QoS el estándar incluye:

- Una función de configuración y registro para a su vez pre configurar los parámetros de flujo y tráfico de QoS basada en las estaciones suscriptoras
- Una función de señalización para establecer dinámicamente flujos con QoS habilitada y parámetros de tráfico
- Utilización del despacho a nivel MAC y parámetros de tráfico con QoS para flujos de servicio del UL (uplink).
- Ídem para DL (downlink)
- Mapear el flujo de datos a las clases de servicio establecidas, generando una suerte de agregación de tráfico según características del flujo

Previo al intercambio de datos se establece una conexión unidireccional entre la estación y la estación base. Es un resabio del "security association" de IPsec. Esa conexión queda identificada por el parámetro CID (Connection Identifier), de 16 bits. A esto se suma el concepto de flujo de servicio "service flow" también proveniente de IP. A este flujo identificado por el SFID ("Service Flow Identifier"), de 32 bits, se le van a asociar los parámetros propios de Calidad de Servicio.
Los mismos son entre otros, prioridad, máxima velocidad, mecanismo de reserva de recursos, retardos máximo y mínimo, jitter, etc. La estación base es la que asigna el SFID y lo asocia al CID correspondiente. No nos olvidemos que WiMAX está cubriendo el acceso del usuario a la red por lo que para tener Calidad de Servicio entre usuarios, o como suele decirse end-to-end, se deben y pueden asociarse los SFID con los "code points" de DiffServ o los "flow labels" de MPLS.
Con el objeto de estandarizar la operación entre la SS y la BS los atributos del "service flow" incluyen detalles de la modalidad bajo la cual una SS solicita ancho de banda de UL y de la operación del "scheduler" del UL por parte de la BS.
Además del SFID y CID mencionados anteriormente, los atributos son:

- ProvisoinedQoSParamSet: conjunto de parámetros de QoS provistos fuera del alcance del estándar

- AdmitedQoSParamSet: conjunto de parámetros para el cual la BS y posiblemente la SS reserven recursos. En general, el recurso será el ancho de banda y la memoria
- ActiveQoSParamSet: conjunto de parámetros de QoS que definen el servicio provisto normalmente al flujo de servicio
- Módulo de Autorización: una función lógica dentro de la BS que aprueba o rechaza los cambios a los parámetros de QoS y clasificadores asociados con un flujo de servicio dado

El ActiveQoSParamSet es un subconjunto del AdmittedQoSParamSet. Se definen tres tipos de flujo de servicios:

- Provisto (Provisioned): está dado por el aprovisionamiento externo, como por ejemplo a través del sistema de gestión, los conjuntos de AdmittedQoS y ActiveQoS son nulos.
- Admitido (Admitted): este flujo de servicio tienen recursos reservados por la BS para el conjunto de ActiveQoS, pero no están activos, el Conjunto de ActiveQoS es nulo.
- Activo (Active): tiene recursos comprometidos por la BS para el conjunto ActiveQoS.

4.10.1 Clases de Servicio

Las clases de servicio nos permiten identificar un conjunto de parámetros de QoS, por lo tanto, su uso es opcional. Un servicio identificado por una clase de servicio tendrá el mismo derrotero y recursos, una vez establecido, que un servicio que tenga los mismos parámetros de QoS especificados explícitamente.
De todas maneras presenta una ventaja desde el punto de vista del proveedor al configurar los flujos de servicio en las BSs en lugar de en los servidores correspondientes. El operador aprovisiona a la SS con la clase de servicio, explicitando el nombre correspondiente, cuya implementación tendrá lugar en la BS. Los parámetros de QoS se pueden especificar de tres maneras diferentes:

- Listando la totalidad de los parámetros explícitamente.
- Haciendo una referencia indirecta a un conjunto de parámetros al especificar una clase de servicio.
- Especificando una clase de servicio y eventualmente parámetros a modificar dentro de la clase dada.

Operativamente la clase se instancia en los parámetros que le corresponden una vez que la BS reconoce el flujo de servicio. Esa instanciación parte de mensajes enviados por la BS que incluyen una codificación del flujo de servicio que contiene el nombre de la clase de servicio asociada y los parámetros de QoS.

Todo cambio en los parámetros de QoS debe ser admitido por un módulo de autorización. El estándar propone dos modelos de autorización: estático y dinámico. En el estático no se admiten cambios una vez hecho el aprovisionamiento. El dinámico, a través de una interfaz adecuada con un servidor de políticas, admite cambios sobre flujos de servicios ya definidos y activos.
Para enmarcar los parámetros de QoS en Clases de Servicio WiMAX define cinco servicios de despacho ("scheduling"):

- Servicio sin solicitud (UGS-Unsolicited Grant Services): Destinado al tráfico de paquetes de longitud fija y velocidad constante (CBR).
- Servicio de tiempo real (rtPS-Real Time Polling Services): Destinado típicamente al tráfico de vídeo.
- Servicio de tiempo no-real (nrtPS-Non-real Time Polling Services): Destinado al tráfico con tolerancia al retardo y velocidad mínima
- Servicio "Best Effort": Destinado a tráfico que no requiere de niveles mínimos en los parámetros de calidad de servicio.
- Servicio extendido de tiempo real y tasa variable (ERT-VR, "Extended real-time variable rate Service/ErtPS-Extended Real Time Polling Services"): Destinado a tráfico de tiempo real de velocidad variable y especificaciones de retardo y tasa de transferencia.

La asociación de las clases de servicio con los parámetros de QoS es llevada a cabo por un "scheduler" residente en la estación base.

4.11 Ahorro de Energía

Esta prestación se contempla especialmente para el caso de estaciones móviles. Damos aquí una breve descripción como para completar el alcance de 802.16 que presentamos en este capítulo. Las cuestiones afines con escenarios móviles las veremos en el siguiente capítulo.
El ahorro de energía constituye un elemento importante especialmente en estaciones móviles. WiMAX define dos modos de ahorro de energía. Modo de hibernación y de estado ocioso.
El modo de hibernación la estación se apaga por períodos de tiempo predeterminados acordados con la estación base. Dentro de él existen tres clases:

- Clase 1: La ventana de hibernación se incrementa desde un valor mínimo a uno máximo de forma exponencial
- Clase 2: La ventana de hibernación tiene una duración fija
- Clase 3: La ventana de hibernación es de duración variable y debe establecerse cada vez que un período de hibernación se

inicia

El modo ocioso es opcional en WiMAX y logra un mayor ahorro de energía. Desconecta totalmente a la estación que ingresa en este modo. Para su recuperación se definen grupos de localización compuestos por estaciones base. Si aparece tráfico para una estación que se encuentra en este modo el grupo la localiza. Esta estación se despierta periódicamente para refrescar su pertenencia al grupo de localización.

4.12 Novedades en WiMAX

El desarrollo de las tecnologías de acceso a Internet de banda ancha corre parejo con el desarrollo de lo que se da en llamar IP móvil. Este punto lo abordaremos en el próximo capítulo. Justamente WiMAX acompaña a este desarrollo bajo la figura de WiMAX móvil. A su vez WiMAX sigue estrechamente ligada al grupo IEEE 802.16 con sus diversos "ammendments". Como siempre apuntando a servicios de red y no de acceso únicamente.

Es así que WiMAX móvil incorpora los avances de 802.16m, aprobada el 31 de marzo de 2011. Es importante mencionar que la misma logra un alto nivel de integración con "ITU-R/IMT-Advanced" para sistemas 4G.

CAPÍTULO 5

IP Móvil

5.1 Introducción

Hasta ahora hemos visto y desarrollado en mayor medida aspectos de nivel MAC vinculados a las redes inalámbricas. Nunca debemos olvidarnos del usuario y en este tipo de redes tenemos un tipo particular de dispositivo utilizado por los usuarios como es el caso de las "laptops", "netbooks", "notebooks", etc. que tienen una propiedad común que es su movilidad. Esta movilidad acompaña a la demanda del usuario actual de querer estar permanentemente conectado a Internet y cada vez con mayores exigencias en la Calidad de Servicio.
La propia movilidad exige dos propiedades que caracterizan el servicio prestado y que suelen confundirse con bastante frecuencia. Ellas son:

- Portabilidad: Poder conectarse a diferentes redes. Tener el acceso a las mismas disponible
- Movilidad: Mientras el usuario se traslade de una red a otra la conexión debe mantenerse

Dicho de otro modo, el traslado del usuario de una red a otra debe resultar transparente a la aplicación/conexión en curso. Lograr esto en la plataforma IP no es trivial dado que la misma no se armó teniendo en cuenta la movilidad como en el caso de la telefonía celular (GSM).
Detengámonos por un momento en analizar el uso de las direcciones IP. En primer lugar identifican unívocamente a los usuarios y a todo aquello que sea direccionable a través de la red. Además, la dirección destino en una conexión es necesaria y suficiente para que la red encuentre el camino al mismo. Si llevamos esto al mundo en el que el usuario se desplaza de una red a otra entraremos en una flagrante contradicción.
El usuario, sea o no móvil, necesita mantener su identidad (dirección IP) para permanecer visible en la red, pero al cambiar de lugar debe cambiar su ruta, algo imposible si mantiene su dirección. Es decir la contradicción se da entre la identidad y el ruteo. Veamos un ejemplo de lo dicho. En la Figura 5.1 un usuario X ejecuta el comando ping con Y como destino.

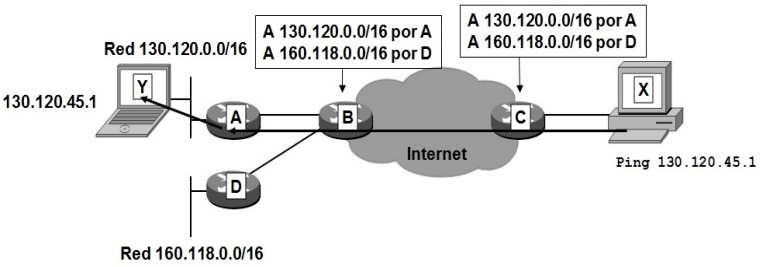


Figura 5.1 Usuario en red nativa

Conociendo la dirección IP del destino podemos ejecutar el comando ping correspondiente y el destino Y será alcanzable y procederá a enviar la respuesta para completar la ejecución del comando. Veamos en la Figura 5.2 qué ocurre al desplazarse a la red 160.118.0.0/16

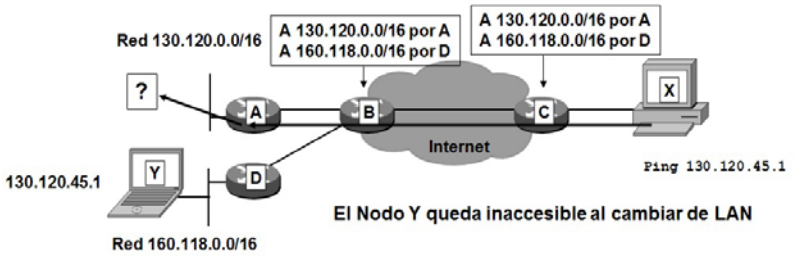


Figura 5.2 Usuario en otra red

El destino Y ahora resultará inalcanzable. Dado que la tabla de ruteo en B no se ha modificado seguirá enrutando el paquete hacia A. En el caso que aún conserve en su ARP cache la dirección MAC de Y, enviará el datagrama a la LAN donde Y no se encuentra. En caso de que A no tenga en su cache la entrada de Y acudirá a ARP con un "request" del que no tendrá respuesta y descartará el datagrama. Como era de esperar con el funcionamiento normal de IP si un host cambia de red manteniendo su dirección de red pierde por completo la conectividad.

Un primer intento de proveer servicios de portabilidad es a través de DHCP. En esta solución el usuario móvil con su equipo, Y, no mantiene su dirección IP sino que recibe una nueva dirección perteneciente a la red en la que ahora se encuentra. Esto crea un problema de transparencia en los niveles superiores, aunque puede compensarse con actualizaciones dinámicas del DNS. Las actualizaciones dinámicas permiten que el host Y solicite al servidor DNS principal del dominio del que depende que asocie la nueva

dirección IP con el nombre que le corresponde. Así por ejemplo si el host Y tiene el nombre www.unlp.edu.ar, cuando se ubique en la nueva red pedirá al servidor primario del dominio unlp.edu.ar que asocie a dicho nombre la dirección IP 160.118.2.3 en vez de la 130.120.45.1. Esta solución puede conseguir portabilidad pero nunca movilidad, puesto que las sesiones se interrumpen completamente cuando se cambia de dirección IP. En la Figura 5.3 ejemplificamos lo dicho.

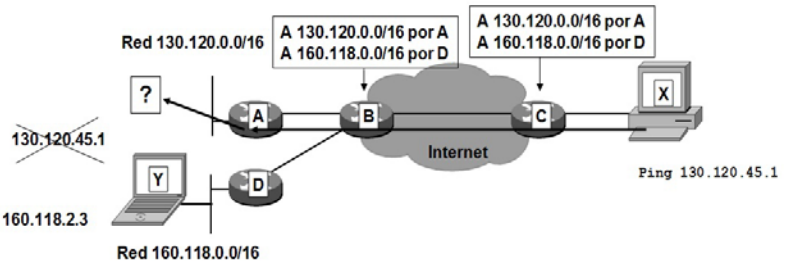


Figura 5.3 Portabilidad

Existen otras alternativas, como la de Cisco, propietaria, LAM (Local Area Mobility). Básicamente consiste en incluir en las tablas de ruteo direcciones de host. Es una solución no transparente para los routers, dado que deben soportar este protocolo, además de ser propietario. Sumado a esta desventaja está el hecho que la nueva entrada debe propagarse por toda la red lo que hace que resulte una convergencia lenta y además poco escalable. Producto de estas desventajas no resulta utilizable. En la Figura 5.4 vemos como resultaría.

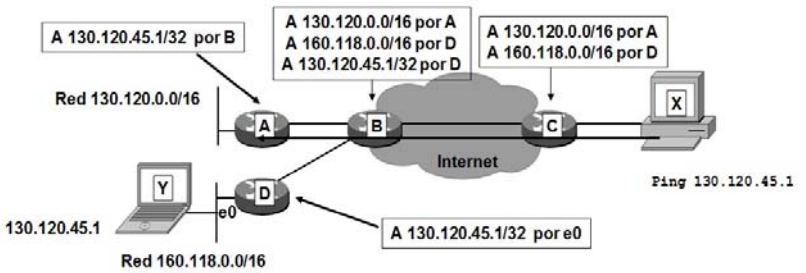


Figura 5.4 Solución LAM

5.2 IP Móvil (Mobile IP)

"Mobile IP" surge como respuesta a la solución de los problemas planteados. Fundamentalmente para cumplir con lo de portabilidad y

movilidad. El mismo se encuentra especificado en sus versiones para IPv4 e IPv6 como se puede observar en la siguiente tabla, en la cual se consigna la evolución del protocolo, tanto para IPv4 como para IPv6, con el correr del tiempo.

IPv4	IPv6
RFC 2002 – 10/1996	RFC 3775 – 06/2004
RFC 3220 – 01/2002	RFC 6275 – 07/2011
RFC 3344 – 08/2002	
RFC 5944 – 10/2010	

La solución planteada es una confluencia de tres mecanismos. Un mecanismo de descubrimiento de la nueva red en la que se encuentra el dispositivo móvil. El registro de la nueva ubicación en la red original y el tercer mecanismo es el que logra el enrutamiento de los datagramas al nuevo destino.
El host móvil mantiene en todo momento su dirección original, lo cual permite una total transparencia hacia el nivel de transporte y superiores. El pasaje/cambio de un router al otro se realiza de forma que, normalmente, no se pierden las conexiones activas, quedando condicionado esto a la velocidad de desplazamiento del nodo móvil y el alcance de las áreas de cobertura de los routers involucrados. Veamos en la Figura 5.5 la idea de Mobile IP en ejecución.

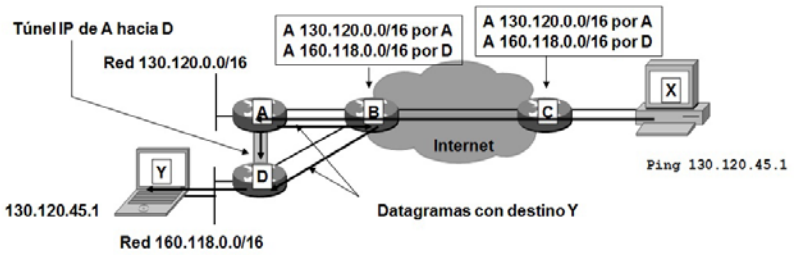


Figura 5.5 IP Móvil

Básicamente, el nodo móvil (Y) se registra a través del nuevo "Default Gateway" (D) en la red de visita con su "Default Gateway" original (A) y se establece un túnel entre ambos routers. Ese registro consiste en avisarle a su router nativo la dirección IP destino del túnel a establecerse.
Los routers que no participan del túnel mencionado no requieren ningún cambio o agregado en sus rutas. Tampoco se modifica nada en el host fijo que mantiene la conexión con el host móvil (X). Mobile IP se hará presente en el router en la red original (A), el router en la red visitada (D) y el propio host móvil (Y).

Sin ánimo de ser pesimistas aquí aparece uno de los principales inconvenientes que tiene IP móvil puesto que, generalmente, las comunicaciones no discurren por la ruta óptima ya que todo tráfico hacia Y pasa necesariamente por A.
Tal como se indicó más arriba se especifica IP móvil para las versiones 4 y 6 de IP por lo que las trataremos en apartados diferentes.

5.2.1 IPv4 Móvil

Con este protocolo aparecen nuevos actores en el escenario de IP y nuevos términos que aclaramos a continuación. En algunos casos preferimos dejarla en idioma original (inglés) dado que todavía no se ha extendido su uso por lo que existen las más diversas traducciones que consideramos no representan/reflejan el alcance correspondiente.

- Nodo Móvil (Mobile Node-MN): es todo host o router que cambia de una red o subred a otra. Cambia de ubicación sin cambiar su dirección IP. Puede conectarse a otros nodos utilizando siempre su dirección original.
- Red Nativa (Home Network-HN): la red a la que pertenece el nodo móvil y en la que se encuentra originalmente.
- Dirección Nativa (Home Address-HAd): la dirección del nodo móvil, perteneciente a la Red Nativa.
- Agente Local (Home Agent-HA): el router de la red nativa del nodo móvil que provee al túnel mencionado los datagramas al nodo móvil en el caso que éste se encuentre fuera de su red nativa. También mantiene actualizada la ubicación del nodo móvil.
- Red Visitada (Foreign Network-FN): la red transitoria que visita el nodo móvil.
- Agente Extranjero (Foreign Agent-FA): el router de la red visitada por el nodo móvil que provee enrutamiento al nodo móvil mientras éste se haya registrado. Desencapsula los datagramas recibidos a través del túnel iniciado en el Agente Local. Actúa como "Default Gateway" tradicional del nodo móvil.
- Nodo Corresponsal (Correspondent Node-CN): el nodo que está intercambiando datos con el nodo móvil.
- Care of Address (CoA): la dirección IP que tiene el túnel de IP móvil en el lado del FA.

Veamos todos estos actores y terminologías presentes en la Figura 5.6.

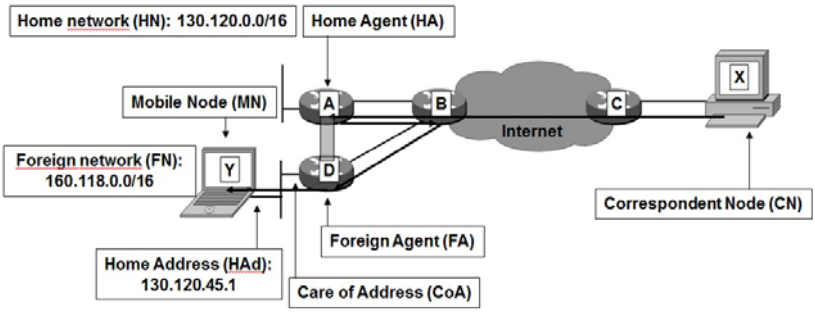


Figura 5.6 Elementos de IP Móvil

La dirección IP del nodo móvil tiene los mismos atributos y tratamiento que las direcciones de los nodos fijos. Cuando el nodo móvil se aparta de la red nativa se le asocia una dirección que identifica la ubicación actual del nodo ("Care-of-Address"). De todos modos utiliza siempre su dirección IP nativa como la dirección IP origen en todos los datagramas que envíe en sus sesiones de intercambio de datos. La única excepción a esto puede ser en el caso de intercambio de datagramas para control de la movilidad.
Los servicios adicionales provistos por Mobile IP son:

- Descubrimiento de Agente: el agente local o extranjero anuncia su disponibilidad como tal en la red a la cual está conectado. A su vez, el nodo móvil puede expresamente solicitar dicho anuncio.
- Registro: cuando el nodo móvil se encuentra fuera de su red nativa, registra su "care-of-address" con su agente local o a través de un agente extranjero que reenvía el registro al agente local.
- Descarte Silencioso: cuando corresponda el datagrama asociado a este servicio será descartado sin aviso alguno al nodo origen pero debe poder registrar el error producido junto con el contenido del datagrama descartado y llevar estadística de dichos eventos.

A continuación se puede ver un resumen de la operatoria de Mobile IP:

- Los agentes móviles, locales y extranjeros, publican su presencia a través de mensajes de Aviso de Agente o el nodo móvil lo solicita a través del mensaje de Solicitud de Agente. El nodo móvil recibe estos mensajes y determina si se encuentra en su red nativa o extranjera.
- Si el nodo móvil detecta que se encuentra en su red nativa opera normalmente sin servicios de movilidad. En el caso que

haya regresado a su red nativa, anula el registro con su agente local a través del intercambio de mensajes de Solicitud de Registro - Respuesta de Registro.

- Si se encuentra en otra red obtiene el "care-of-address" en la nueva red. Se obtiene a través del aviso del agente extranjero o por un mecanismo de asignación externa como ser DHCP ("care-of-address co-located"). El primero es el más utilizado dado que permite a varios nodos móviles compartir el "care-of-address". El segundo tiene la ventaja de no requerir un agente extranjero, pero requiere que en la red visitada se tenga un grupo de direcciones reservado para los nodos móviles visitantes.
- El nodo móvil del caso anterior registra este "care-of-address" con su agente local intercambiando mensajes de Solicitud de Registro – Respuesta de Registro, usualmente a través del agente extranjero.
- Los datagramas enviados a la dirección nativa del nodo móvil son interceptados por el agente local, que los encapsula en un túnel con destino en el "care-of-address" donde se desencapsula y envía al nodo móvil.
- En el otro sentido de la conexión, del nodo móvil a su corresponsal, los datagramas se envían normalmente a través de los mecanismos de ruteo tradicionales.

En la Figura 5.7 podemos apreciar la información disponible por los routers y relacionada con IP móvil, en este caso, la información dada por el router que actúa como agente local. El primer comando nos permite obtener un listado de los nodos móviles registrados con ese agente y el segundo nos entrega información detallada de cada uno de los nodos móviles registrados

```
show mobile-ip home-agent bindings
user@host> show mobile-ip home-agent bindings

Home address  NAI           Home agent   Care-of-address
10.1.1.3     abcde@def.com    10.1.1.1    50.50.50.1
30.1.1.3        -          55.55.55.1  50.50.50.1
20.1.1.3     def@def.com      20.1.1.1    60.50.50.1

show mobile-ip home-agent bindings ip-address
user@host> show mobile-ip home-agent bindings ip-address 10.1.1.3

Home address      : 10.1.1.3
NAI               : abcde@def.com
Home agent        : 10.1.1.1
Care-of-address   : 50.50.50.1
Lifetime Granted  : 180
Lifetime Remaining : 20
Tunnel Type       : IP-IP
Tunnel ID         : 10
Tunnel Source     : 10.1.1.1
Tunnel Destination : 50.50.50.1
Identification    : ABCD1234.4321ABCD
Revocation Support : Enabled
Notify MN of Revocation : Enabled
```

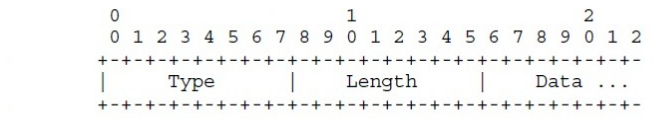
Figura 5.7 Monitoreo

5.2.1.1 Mensajes y extensiones de Mobile IPv4

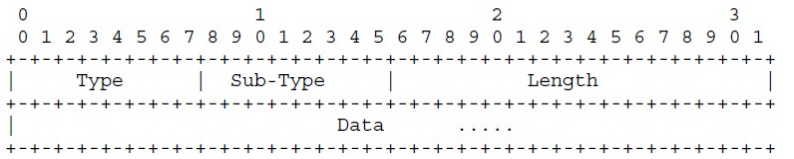
Se definen mensajes de control enviados por UDP a través del port bien conocido 434:

- Solicitud de Registro
- Respuesta de Registro

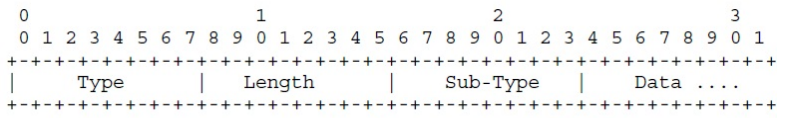
Para el descubrimiento de agentes se recurre a los mensajes de Aviso de Router y Solicitud de Router, definidos para el Descubrimiento de Router de ICMP. Para ampliar la capacidad y funcionalidad de estos mensajes se define un mecanismo general de Extensión que permite el envío de información adicional. Dicho mecanismo agrupa las extensiones en dos conjuntos, correspondientes a los mensajes de control, enviados a través de UDP y los de aviso, a través de ICMP. Más allá de la división de acuerdo al tipo de mensaje define tres formatos acorde con la longitud de la extensión. En Figura 5.8 los podemos apreciar:



Formato Simple



Formato Largo



Formato Corto

Figura 5.8 Formatos

Descubrimiento de Agentes

El Aviso de Agente se forma agregando la extensión de Aviso de Agente en el mensaje de Aviso de Router de ICMP. Para los interesados en conocer en detalle estos mensajes los remitimos a consultar el RFC 5944. Aquí indicaremos solamente algunas de sus particularidades. A nivel IP el TTL estará en 1, impidiendo de esta manera que el mensaje ingrese a otra red. A nivel ICMP diremos que el mensaje es enviado con una frecuencia 1/3 del tiempo de vida indicado en el encabezado de ICMP. Así se deja que el nodo móvil pierda hasta tres avisos sucesivos antes de borrar al agente de su lista de agentes válidos. Como siempre esta frecuencia se ajusta con un factor aleatorio para evitar sincronización de mensajes en la red. La novedad completa la tendremos en la extensión, que presenta la siguiente estructura indicada en la Figura 5.9.

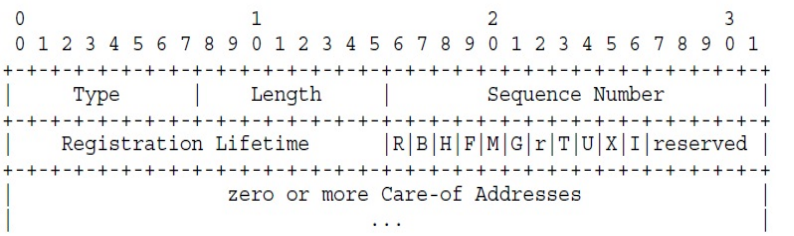


Figura 5.9 Aviso de Agente

Los campos contienen lo siguiente:

Type:	16
Length:	La longitud de la extensión en bytes, a partir del Sequence Number
Sequence Number:	Representa el número de mensajes enviados desde que se activó el agente
Registration Lifetime:	El tiempo de vida máximo que este agente aceptará en el pedido de registro recibido.
R:	Se requiere registro
B:	Ocupado. El agente no acepta más pedidos de registro
H:	El agente que envía este mensaje actúa como agente local (HA)
F:	Ídem para el caso que actúe como agente extranjero (FA)
M:	Recibe datagramas provenientes de túneles con encapsulamiento mínimo.
G:	Acepta datagramas provenientes de túneles con encapsulamiento de ruteo genérico (GRE).
r:	Fijo en 0
T:	Soporta túnel inverso
U:	Soporta túnel de UDP
X:	El agente soporta revocación de registro
I:	El agente soporta registro regional
reserved:	Por el momento sin uso, se transmiten los bits en 0

La solicitud de agente es idéntica al mensaje de solicitud de Router de ICMP. A nivel IP el TTL estará en 1.

Registro

Este mecanismo permite al nodo móvil anunciar su ubicación al agente local, renovar el registro próximo a expirar y anular el registro en caso que haya regresado a la red nativa. Adicionalmente le permite:

- Descubrir su dirección nativa.
- Mantener múltiples registros simultáneos. Esto produce que los datagramas que lo tengan por destino serán encapsulados en un túnel a cada "care-of-address" que esté registrado.
- Anular parcialmente los registros.
- Descubrir la dirección del agente local.

El registro se puede llevar a cabo a través de dos procedimientos, uno a través del agente extranjero, completando el registro con el agente local y otro directamente con el agente local.
Los mensajes de registro entre un nodo móvil y su agente local deben autentificarse. Para ello se recurre a una extensión definida para este requerimiento. La misma está basada en una clave hash MD5 y time stamp para evitar ataques. Es obligatoria para el registro del nodo móvil en el agente local y opcional en los demás casos de intercambio de este tipo de mensaje.
En la siguiente tabla resumimos los mecanismos y mensajes involucrados en la operación de IP móvil.

Operación	**Mecanismo**
Descubrimiento de agentes (HA, FA)	ICMP y extensiones
Registro	UDP
Túnel	IP-en-IP Encapsulado mínimo GRE

Registro con un Foreign Agent CoA

El nodo móvil recibe un aviso de agente de un FA y se registra con éste utilizando el FA CoA publicado. Veamos los campos relevantes del mensaje de solicitud de registro.
Campos en IP:
Dirección Origen: Dirección nativa del nodo móvil
Dirección Destino: La extraída de la dirección origen del aviso de agente recibido
TTL: 1
Campos en UDP:
Port Origen: Port efímero dado por el Sistema Operativo
Port Destino: 434
Campos de Solicitud de Registro
Type: 1
S=0, B=0, D=0, M=0, G=0
Lifetime = El tiempo de vida tomado del mensaje de aviso del agente.
Home Address = La dirección nativa del nodo móvil
Home Agent = La dirección IP del home agent del nodo móvil
Care-of-Address = el CoA copiado de la extensión del mensaje de

aviso
Identification = time stamp o Nonce
Extensions: La extensión de autentificación del Mobile Home.

Figura 5.10 Registro

Registro con una CoA local

Es el caso en que el nodo móvil ingresa a una red que no contiene un FA. Obtiene, entonces, una dirección por DHCP que la utiliza como CoA local. Supongamos, además, que el nodo móvil soporta todas las formas de encapsulamiento definidas, IP-en-IP, encapsulamiento mínimo y GRE; desea además una copia de los broadcasts de la red nativa.
Campos de IP:
Dirección Origen = CoA obtenido por DHCP
Dirección Destino = Dirección IP del home agent
TTL = 64
Campos de UDP:
Port Origen = Port efímero dado por el Sistema Operativo
Port Destino = 434
Campos de Solicitud de Registro:
Type = 1
S=0, B=1, D=1, M=1, G=1
Lifetime = 1800 (segundos)
Home Address = Dirección nativa del nodo móvil
Home Agent = Dirección IP del home agent del nodo móvil
Care-of-Address = el CoA dado por el servidor de DHCP
Identification = time stamp o Nonce
Extensiones:
La extensión de autentificación del Mobile-Home.

Anulación del Registro

El nodo móvil regresa a su red nativa y debe anular el registro del CoA con su home agent.

Campos IP:
Dirección Origen: Dirección nativa del nodo móvil
Dirección Destino: Dirección IP del home agent
TTL = 1
Campos UDP:
Port Origen = Port efímero dado por el Sistema Operativo.
Destination Port Destino = 434
Campos de Solicitud de Registro:
Type = 1
S=0, B=0, D=0, M=0, G=0
Lifetime = 0
Home Address = Dirección nativa del nodo móvil
Home Agent = Dirección IP del home agent del nodo móvil
Care-of-Address = Dirección IP del nodo móvil
Identification = time stamp o Nonce
Extensiones:
La extensión de autentificación del Mobile-Home.

5.2.1.2 Algunos inconvenientes

Hasta ahora hemos ejemplificado IP móvil en operación con un corresponsal fuera de la red del nodo móvil. Veamos el caso contrario, es decir si nos remitimos al escenario planteado en figuras anteriores, el nodo X, nodo corresponsal, pertenece a la misma red que Y. Queda indicado en la Figura 5.11

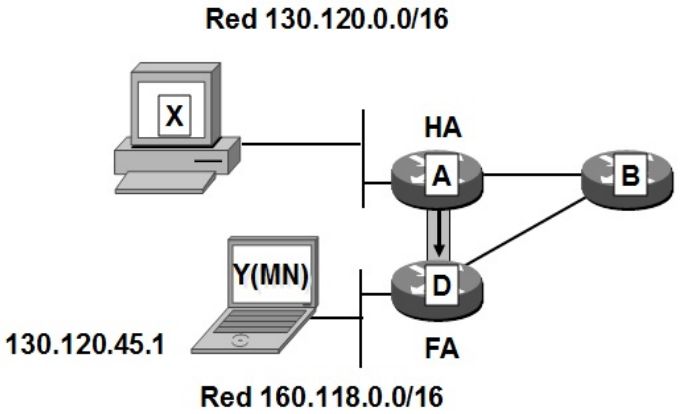


Figura 5.11 Nodo móvil y node corresponsal en la misma red

Los datagramas que Y, el nodo móvil, envía a X llegarán normalmente a destino según las tablas de ruteo de intervinientes en el recorrido D-B-A.

Sin embargo, los datagramas enviados por X hacia Y, si dejamos las cosas como están, no llegarán. La razón es que X, al ver que el host de destino pertenece a su misma red, procederá al envío del datagrama según el direccionamiento directo. Buscará su dirección MAC en la tabla de hosts. Si la encuentra armará la trama pero obviamente no llegará a Y. Si no lo tiene en su tabla acudirá a ARP, enviando un ARP request del que no tendrá respuesta alguna.

La solución a este problema es que el agente local (HA) A reemplace en la ejecución de ARP al nodo móvil y responda a los ARP request, como si fuera el nodo móvil Y. Este mecanismo se conoce como "Proxy ARP". El agente local empieza a funcionar como Proxy ARP para el nodo móvil no bien éste se registra desde un agente extranjero, es decir cuando se cree una asociación de movilidad para él.

Si queremos optimizar la performance tenemos para mejorar algo más. Antes mencionamos que X podría tener en su tabla de ARP la dirección MAC de Y, en cuyo caso no tendría respuesta. Pueden pasar minutos hasta que se actualice la tabla ARP de X. Para acelerar esa actualización se echa mano del mecanismo "ARP gratuito". No bien el agente local asocia la dirección IP del nodo móvil con el "care-of-address", envía un ARP broadcast anunciando la nueva dirección MAC de Y. Esto provoca la inmediata actualización de todas las tablas ARP que tuvieran una entrada para la IP del nodo móvil.

Si volvemos al caso en que el nodo móvil envía un datagrama a su corresponsal podríamos encontrarnos con que los datagramas no llegan al corresponsal. Dado que el nodo móvil genera datagramas que tienen por dirección IP origen la de una red ajena a la red desde donde se envían, muchas veces por razones de seguridad se crean listas de

acceso que actúan como filtro y entonces nos encontraremos con situaciones como la de la Figura 5.12.

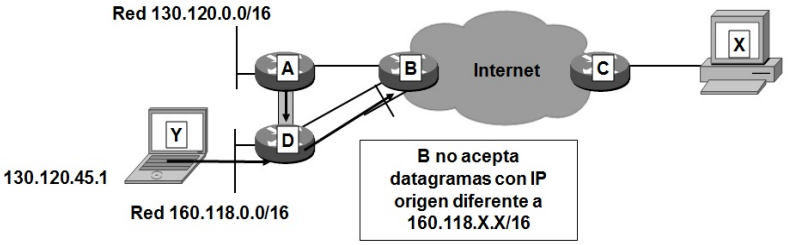


Figura 5.12 Filtrado

Para solucionar el problema anterior planteado se puede recurrir a la creación de un túnel en el sentido del Foreign Agent al Home Agent, es decir hacer bidireccional el túnel creado anteriormente para la comunicación de X a Y. De esta forma los datagramas enviados por Y a X serán encapsulados cuando lleguen Foreign Agent en otros datagramas que tendrán como dirección de origen la del Care of Address (en el Router D) que si es una dirección válida para B y no lo descartará. La Figura 5.13 ejemplifica lo dicho.

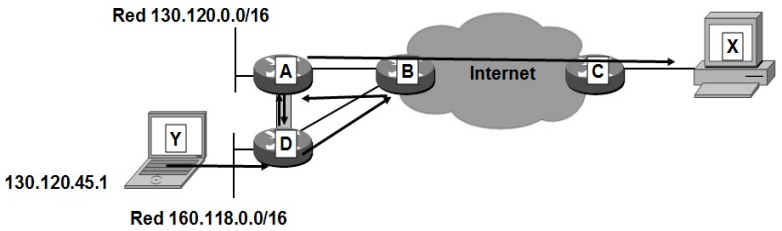


Figura 5.13 Una solución al filtrado

Sin duda el problema está resuelto pero con una mala performance dado el ida y vuelta que se da tanto en el router A (HA) como en el B.

Redes Móviles

Pueden presentarse otros escenarios más complejos como el caso en que el nodo móvil se conecte a una red que a su vez es móvil. Es decir, en esa red habrá un router móvil que juega el papel de FA para nuestro nodo móvil y éste a su vez está conectado a una red fija dónde habrá un router que actúa como FA para él.
Nuestro inquieto nodo Y normalmente conectado a su red fija tiene que hacer un viaje por tren y necesita seguir trabajando con su red. El

tren tiene servicio de IP Móvil. Y se habrá desconectado de su red y en el tren se conecta a la red móvil. Veamos en detalle lo que ocurre:

- Y se registra en esta red utilizando el CoAT (Care-of-Address del Tren) descubierto a través del anuncio que hizo el FAT (Foreign Agent del Tren). El router de la red fija de Y que actúa como Home Agent, llamémoslo HAY actualizará su tabla.
- La red del Tren es a su vez móvil. Supongamos que el FAT también es el router de "default" que conecta la red del Tren a Internet. Cuando el Tren está en la estación central el FAT se conecta a la red fija de la compañía en la cual habrá un router que actúa como HA, llamémoslo HAT (El Home Agent del Tren). Al ponerse en movimiento y dado que da el servicio de IP Móvil se registrará cada tanto con FA disponibles, llamémoslo FAD (Foreign Agent Disponible).
- Un nodo corresponsal X envía un datagrama a Y. Este datagrama será ruteado a la red fija de Y. El HAY capturará este datagrama y lo encapsulará en el túnel con la dirección del CoAT. El datagrama llegará a la red fija de la estación central donde estará el HAT.
- El HAT intercepta el datagrama y lo encapsula en el túnel al CoAD localizado en el FAD. Ha ocurrido un doble encapsulamiento del datagrama original. El primero por parte del HAY y el segundo por el HAT.
- El FAD desencapsulará el datagrama que recibe y lo enviará al FAT.
- El FAT desencapsula el datagrama y nuestro viajero Y finalmente lo recibirá.
-

5.2.2 IPv6 Móvil

La especificación de IPv6 en su versión móvil comienza en junio de 2004 con la RFC 3775 y por supuesto continúa. Traemos la tabla de RFCs asociadas a IPv6, en la que hemos eliminado aquellas que no están vigentes, como para poder apreciar el mayor desarrollo y actividad si lo comparamos con IPv4. [http://www.rfc-editor.org]. Por la especificidad de los títulos no los hemos traducido al castellano.

RFC	Título	Fecha	Estado
RFC6276	DHCPv6 Prefix Delegation for Network Mobility (NEMO)	Julio 2011	Estándar propuesto
RFC6275	Mobility Support in IPv6	Julio 2011	Estándar

			propuesto
RFC6224	Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains	Abril 2011	Informativo
RFC6179	The Internet Routing Overlay Network (IRON)	Marzo 2011	Experimental
RFC6139	Routing and Addressing in Networks with Global Enterprise Recursion (RANGER) Scenarios	Febrero 2011	Informativo
RFC6097	Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6	Febrero 2011	Informativo
RFC6089	Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support	Enero 2011	Estándar propuesto
RFC6059	Simple Procedures for Detecting Network Attachment in IPv6	Noviembre 2010	Estándar propuesto
RFC5846	Binding Revocation for IPv6 Mobility	Junio 2010	Estándar propuesto
RFC5844	IPv4 Support for Proxy Mobile IPv6	Mayo 2010	Estándar propuesto
RFC5779	Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server	Febrero 2010	Estándar propuesto
RFC5380	Hierarchical Mobile IPv6 (HMIPv6) Mobility Management	Octubre 2008	Estándar propuesto
RFC5213	Proxy Mobile IPv6	Agosto 2008	Estándar propuesto
RFC5149	Service Selection for Mobile IPv6	Febrero 2008	Informativo
RFC5096	Mobile IPv6 Experimental Messages	Diciembre 2007	Estándar propuesto
RFC5094	Mobile IPv6 Vendor Specific Option	Diciembre 2007	Estándar propuesto
RFC4980	Analysis of Multihoming in Network Mobility Support	Octubre 2007	Informativo
RFC4877	Mobile IPv6 Operation	Abril 2007	Estándar

	with IKEv2 and the Revised IPsec Architecture		propuesto
RFC4866	Enhanced Route Optimization for Mobile IPv6	Mayo 2007	Estándar propuesto
RFC4651	A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization	Febrero 2007	Informativo
RFC4584	Extension to Sockets API for Mobile IPv6	Julio 2006	Informativo
RFC4283	Mobile Node Identifier Option for Mobile IPv6 (MIPv6)	Noviembre 2005	Estándar propuesto
RFC3963	Network Mobility (NEMO) Basic Support Protocol	Enero 2005	Estándar propuesto

La estructura y operatoria de IPv6 aporta varios elementos al mundo de IP Móvil subsanando algunas de las desventajas encontradas en la versión para IPv4. Particularmente, la extensión del header tendrá un rol importante. También serán útiles la presencia y acción del los protocolos Neighbour Discovery [RFC4861] y Autoconfiguración de dirección sin estado [RFC4862]

En Mobile IPv6 se mantiene la operatoria básica, cuando el destinatario es el nodo móvil. Como sabemos, los datagramas se envían a la red nativa de éste y, luego, el home agent los despacha al CoA del nodo móvil. El cambio lo tenemos en el envío de los datagramas en sentido contrario dado que el nodo móvil no requerirá del foreign agent para obtener su CoA. Ahora en IPv6 tenemos las facilidades de autoconfiguración mencionadas en las dos referencias anteriores que evitan la necesidad de ese agente. También en IPv6 se aprovecha la extensión de header para incorporar opciones de destino que permiten mejorar la mala performance del ruteo que vimos en la sección anterior. Por ejemplo puede el nodo móvil en una extensión de header enviarle al nodo corresponsal actualizaciones de "binding" antes de su desplazamiento a la nueva red.

También, aprovechándose de las extensiones del header, los datagramas destinados al nodo móvil podrán enviarse con opciones de ruteo en las extensiones del header, sin necesidad de recurrir al encapsulado en túneles. Otra ventaja que encontraremos es que IPv6 está en cierto modo más independiente del nivel de enlace que su hermano mayor dado que recurre a Neighbour Discovery (nivel de red) en lugar de ARP (nivel de enlace). También logra con esto

hacerlo más robusto al protocolo.

5.2.2.1 Operación básica de IPv6 Móvil

Existen dos maneras de comunicación entre el nodo móvil y el corresponsal. La primera, a través de un túnel bidireccional. No necesita soporte del corresponsal y puede establecerse inclusive cuando el nodo móvil aún no se haya registrado. Como siempre los datagramas desde el corresponsal llegarán al home agent y luego se encapsularán en el túnel hasta el nodo móvil. Por otra parte los datagramas al nodo corresponsal se encapsulan desde el nodo móvil hasta el home agent y luego ya con un datagrama como que hubiese sido generado en la red nativa se enruta normalmente desde el home agent hasta el destino. El home agent recurre al proxy Neighbour Discovery para interceptar los datagramas destinados al nodo móvil. Luego se encapsularán según lo indica IPv6 en su especificación.
El segundo método, el de la "ruta óptima", si requiere que el nodo móvil haya registrado su CoA en el nodo corresponsal. Los datagramas desde el corresponsal se enrutan directamente al CoA del nodo móvil. El nodo corresponsal verificará en todo datagrama que despacha si existe alguna correspondencia de las direcciones destinos de esos datagramas con sus datos de "bindings". Si se da esa situación el nodo móvil acude a la extensión de ruteo establecida en IPv6, extensión tipo = 2.
De esta manera tenemos asegurado que la ruta resultante será la óptima y también se descarga el tráfico extra que hubiese tenido el home agent sin esta implementación. Con esta operatoria el corresponsal arma el datagrama colocando la dirección CoA del nodo móvil como dirección de destino. La extensión utilizada permite incorporar en la misma la dirección nativa del nodo móvil. En la figura 5.14 tenemos representada la estructura de esta extensión

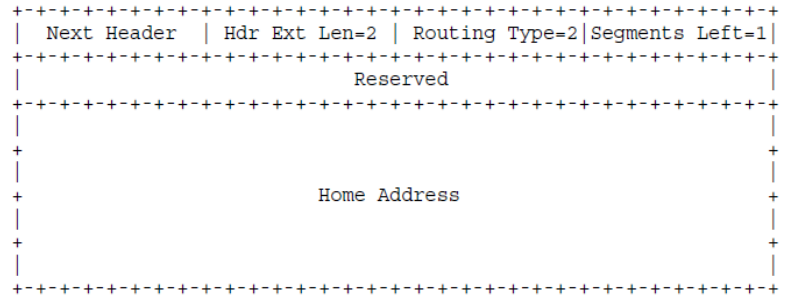


Figura 5.14 Extensión de Ruteo

De la misma manera, el nodo móvil, en todos los datagramas que envía, colocará como dirección origen la de su CoA y a través de una extensión de header, opción de dirección nativa en la que coloca su dirección permanente o fija. Veamos en la figura 5.15 la estructura de esta opción a modo de ejemplo

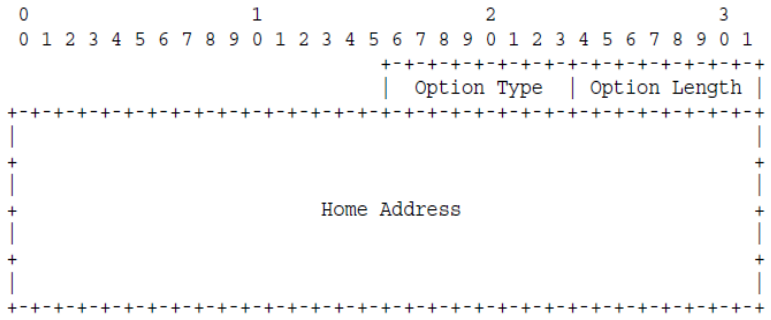
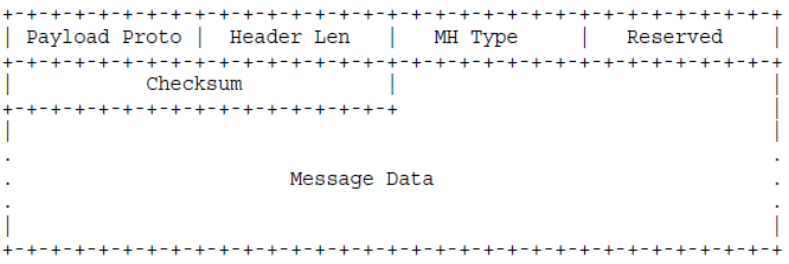


Figura 5.15 Extensión de opción nativa

Esta extensión está transportada por la extensión de destino con Type = 201.

Este protocolo no representa una nueva versión de IPv6 a la manera de las diferencias entre IPv4 e IPv6. Podemos decir que es una ampliación del mismo y con un alcance no sólo en IPv6 sino también que en protocolos auxiliares como ICMPv6.

En primer lugar nos encontramos con una nueva extensión del header, que es el header de movilidad. Será utilizado por los nodos móviles, los corresponsales y los home agents en todos los mensajes correspondientes a la creación y administración de "bindings". En la figura 5.16 se puede apreciar su estructura.



Fi

Figura 5.16 Header de Movilidad

Este header queda identificado por el código 135 en el next header precedente. Sus campos:

- Payload Proto: identifica el tipo de header que sigue a esta

extensión. Serán los headers de IPv6 tradicional.

- Header Len: longitud del header en unidades de 8 bytes.
- MH Type: identifica el mensaje de movilidad particular que transporta.
- Reserved: para uso futuro.
- Checksum: con una operatoria similar a la de IP conocida y con el agregado de un pseudo header con componentes relevantes del header del datagrama [RFC 2460]
- Message Data: contiene el dato acorde con tipo de header mobility que le corresponde.

Entre los varios tipos de mensajes de movilidad que transporta tenemos: Home Test Init, Home Test, Care-of Test Init, Care-of Test. Mensajes que le permiten al nodo corresponsal verificar la ubicación del nodo móvil. Es decir verificar el CoA asociado con la dirección IP del nodo móvil.

El resto de este tipo de extensiones está relacionado con el "binding", mensajes que va a enviar el nodo móvil al corresponsal y/o al home agent, como ser el de Binding Update, para confirmar su "binding" actual; el de Binding Acknowledge, el acuso de recibo enviado por los que recibieron el mensaje anterior; el de Binding Refresh Request, utilizado por el corresponsal para solicitar el envío del "binding"; típicamente lo va a enviar cuando esté por expirar el tiempo de vida del "binding".

Finalmente, el de Binding Error usado por el corresponsal y/o el home agent para indicar condiciones de error que tienen que ver con el uso de la opción de Home Address sin haberse establecido un "binding" o si no se pudo detectar el tipo de mensaje recibido.

En cuanto a ICMPv6 agrega cuatro nuevos tipos de mensaje. Dos mensajes son:

- Home Agent Address Discovery Request
- Home Agent Address Discovery Reply

Éstos son disparados por el nodo móvil para localizar a su home agent, el primero y el segundo la confirmación enviada por el agente ya descubierto. Los otros dos son los siguientes:

- Mobile Prefix Solicitation
- Mobile Prefix Advertisement

Son disparados por el nodo móvil para requerir los prefijos de red de su home agent, el tercero, y el cuarto es la respuesta correspondiente.

5.2.2.2 Seguridad en IPv6 Móvil

Está explícitamente considerada en este protocolo. Protege las actualizaciones de "binding", el aviso de prefijos y el transporte de datos

para todos los personajes principales de esta arquitectura, nodo móvil, corresponsal y home agent. Las actualizaciones están protegidas mediante IPsec o mediante la opción de "Binding Authorization". El aviso de prefijos y de datos corre por cuenta de IPsec.
El nodo móvil y el home agent, involucrados en la actualización y administración de bindings utilizan una asociación segura de IPsec del tipo Encapsulation Security Payload (ESP) [RFC 4303] y en la modalidad transporte.
En cambio, las actualizaciones de bindings a los corresponsales no requiere de la configuración de asociaciones de seguridad o de disponer de una infraestructura de autentificación entre los nodos móviles y sus corresponsales. Se lleva a cabo con mensajes y procedimientos de ruteo. Remitimos a [RFC 4225] para mayores detalles.

5.3 TCP Móvil

Hasta ahora hemos visto como se hace presente la movilidad en un entorno inalámbrico en los niveles físico, de enlace y red. ¿Es necesario ocuparse del nivel de transporte? Preguntándonos de otra forma, ¿se enteran TCP-UDP y/o afectan la performance y QoS desde el punto de vista del usuario el ambiente inalámbrico y móvil?
Lamentablemente, la respuesta es sí, aunque con una clara diferencia entre TCP [RFC0793] y UDP [RFC0768]. UDP es un protocolo "best effort" como IP, que provee acceso a servicios del nivel de aplicación y básicamente nada más de modo que todo lo que se haga a nivel de red, como es el caso de IP móvil que vimos en secciones anteriores es suficiente para el funcionamiento de UDP en el entorno mencionado.
TCP es seguro, con conexión, provee controles y además se encarga de realizar el control de congestión. Tal vez este trabajo extra es el que influye más en la performance. Recordemos que ya del vamos TCP trabaja con un modelo de control de congestión basado en los extremos (usuarios), lo que ya presenta una desventaja puesto que está controlando un fenómeno que se produce a nivel de red, es decir donde TCP está ausente. En nuestro escenario, tal vez esto tenga un mayor efecto. Si revisamos los diferentes mecanismos de control de congestión propuestos y utilizados nos encontraremos que regulan la ventana de congestión, la que está presente en el transmisor, iniciándola con un segmento y luego incrementándola por cada ACK recibido, mecanismo "slow start" [RFC5681].
Ese crecimiento se da hasta que se produce congestión en la sesión correspondiente. A partir de este punto es donde aparecen las diferencias entre ellos. Pero lo que nos importa considerar ahora es

que la detección de la congestión en la red es por la pérdida de segmentos, lo que llevará a que se agote el temporizador de retransmisión, (RTO) y/o se reciban ACK repetidos. Justamente no necesariamente habrá congestión en la red si ocurren los eventos anteriores. Es la consecuencia de un modelo "end-to-end", en el que se toma acción en el nivel de transporte para contrarrestar los efectos de un fenómeno que ocurre en otro nivel y lugar. Lo indicado anteriormente ocurre en todo escenario, tanto fijo como móvil. Justamente se ve más acentuado en el nuestro dado que son más frecuentes las pérdidas de segmentos debido al nivel físico y el método de acceso implementado por lo que se van producir en ausencia de congestión en la red y que TCP las interpreta erróneamente. Recordemos también que los mecanismos de control de congestión terminan en una reducción de la intensidad de tráfico, por lo que gratuitamente se verá afectado el servicio prestado a los usuarios sin causa valedera.
Tengamos en cuenta también que la movilidad por su cuenta puede producir pérdida de segmentos. Por ejemplo, puede ocurrir que haya segmentos en tránsito a un "foreign agent", mientras el nodo móvil se está acercando al nuevo FA. El FA anterior no podrá enviar los segmentos al nuevo FA. Otro caso que llevará a determinar por parte de TCP que ocurrió congestión.
Se implementaron varios mecanismos para adaptar propiamente TCP al escenario móvil. Rescatamos tres de ellos que comentaremos a continuación.

5.3.1 I-TCP (TCP Indirecto)

Dos puntos de vista opuestos llevaron al desarrollo de I-TCP [Bakre, A., Badrinath, B., "I-TCP: Indirect TCP for mobile hosts", proc. Fifteenth International Conference on Distributed Computing Systems (ICDCS), Vancouver, Canada, 1995]. Por un lado la mala performance de TCP en wireless y por otro la necesidad de cambiar la estructura de TCP, algo imposible y/o inviable. I-TCP divide la conexión TCP en una parte fija y otra inalámbrica, tal como se ve en la Figura 5.17, con un nodo móvil conectado a través de un enlace inalámbrico y un "acess point" a la red cableada donde reside el nodo corresponsal. El nodo corresponsal, a su vez podría recurrir a un acceso inalámbrico.

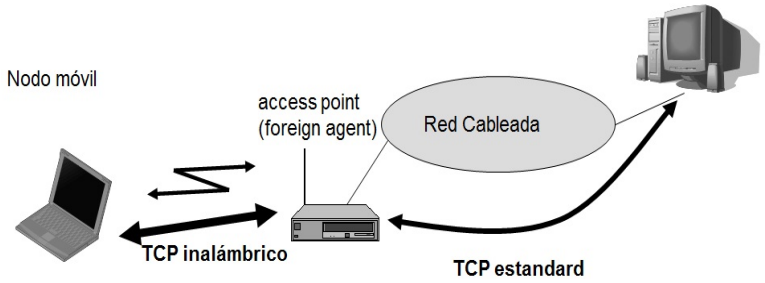


Figura 5.17 I-TCP

Como se indica en la Figura 5.17 el TCP estándar se utiliza entre el nodo fijo y el access point. La diferencia es que la sesión no termina en el nodo móvil sino en el access point, actuando como un proxy de TCP. Ahora el access point se ve como el nodo móvil para el nodo fijo y como el nodo fijo para el nodo móvil. El I-TCP estará presente entre el access point y el nodo móvil.

El FA controla la movilidad del nodo móvil y puede también manejar el desplazamiento del nodo móvil a otro access point que actúe como FA. El nodo corresponsal en la red fija no percibe el enlace inalámbrico y/o la segmentación de la conexión. El FA actúa como proxy y despacha los segmentos en ambas direcciones. Si el corresponsal transmite un segmento el FA lo valida (envía el ACK correspondiente) y lo transmite al nodo móvil.

Si el nodo móvil lo recibe entonces lo valida. De todos modos esta aceptación sólo queda en el FA. En el caso que se pierda un segmento en el tramo inalámbrico el nodo corresponsal no se enterará y será el FA quien realice la retransmisión en dicho tramo. En sentido contrario de la transmisión ocurrirá lo mismo.

Aparecerán tareas adicionales por parte de I-TCP en el caso que haya un desplazamiento del nodo móvil con “handover” (cambio de access point).

El access point actúa como un proxy almacenando temporariamente los segmentos a retransmitir. Una vez que el nodo móvil se encuentre registrado con el nuevo access point, el anterior deberá retransmitir los segmentos al nuevo porque ya ha validado los segmentos. Esto ocurre dado que el nuevo FA avisa al anterior de la nueva ubicación del nodo móvil y produce la retransmisión inmediata. También se trasladarán al nuevo FA los “sockets” del anterior dado que contienen el estado de la sesión TCP, como ser el número de secuencia, el port, la dirección IP. De esa manera se logra mantener la sesión aunque haya habido un cambio de FA. La Figura 5.18 ejemplifica lo dicho.

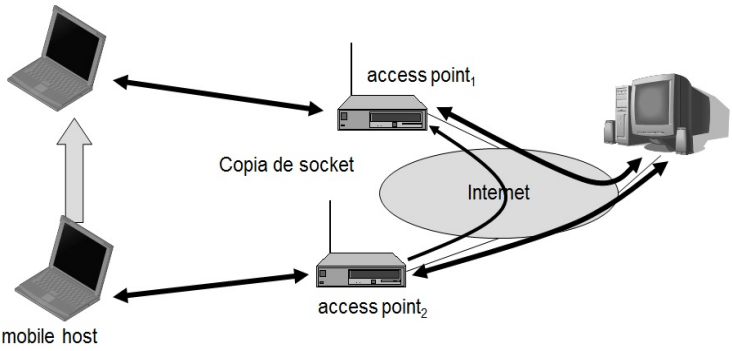


Figura 5.18 I-TCP Usuario en movimiento

Consideraciones a favor de I-TCP pueden ser:

- Dada la separación o división de la sesión en dos, los errores de transmisión que ocurran no se trasladarán de un lado al otro.
- No requiere de cambios de TCP en la zona fija y en todos aquellos nodos IP con acceso wireless que no participan de la conexión.
- Los cambios a introducir son solamente entre el nodo móvil y su FA, con el que tendrá normalmente una conexión directa. Lo que resulta que los cambios no se están instalando en actores directamente vinculados a Internet, con el riesgo que significaría presentar cambio en una red de la magnitud de Internet. Es más resulta de esta manera un escenario en el que se pueden llevar a cabo varias pruebas sin afectar la performance de una red de mayores dimensiones y además pública.
- Esa partición que se produce da lugar a que se implementen diferentes versiones y facilidades del protocolo de transporte en ambas secciones, pasando el FA a actuar como un "Gateway".
- Podemos también precisar algunas desventajas:
- La separación y pérdida de la sesión TCP end-to-end puede generar problemas en el caso que el FA salga de servicio. Todo aquel nodo que envía un segmento y recibe una validación entiende que el segmento llegó a destino correctamente. Ahora la recepción de una validación significa tanto para el nodo móvil como para el corresponsal que el FA recibió el segmento que transmitieron.
- La división producida no es visible para el corresponsal, de modo que una caída en el access point provocará una caída en

las aplicaciones presentes en el corresponsal sin motivo alguno para éste.

- Si la aplicaciones implementan encriptación end-to-end, se deberá integrar al FA a la infraestructura de seguridad acordada dado que ahora la sesión finaliza en él.
- Posible incremento de retardos en el caso que haya una migración del nodo móvil a otro FA.

5.3.2 Snoop TCP

A diferencia de I-TCP esta mejora trabaja en una modalidad totalmente transparente, manteniendo la sesión TCP end-to-end entre nodo corresponsal y nodo móvil. Básicamente lo que hace es almacenar cerca del nodo móvil los datos en un "buffer" con el objeto de realizar las retransmisiones locales en caso que se haya producido una pérdida de segmentos. El TCP con ese agregado residirá normalmente en el FA del IP Móvil. En la Figura 5.19 queda plasmada la idea.

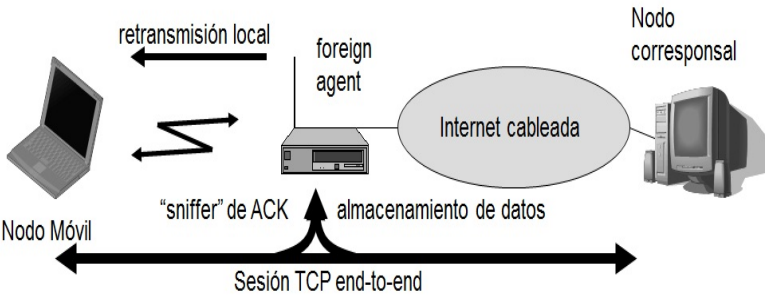


Figura 5.19 Snoop TCP

En este mecanismo el FA almacena los segmentos que tengan por destino el nodo móvil y monitorea el tráfico en ambas direcciones analizando los segmentos de ACK en particular [BAL95]. Por un lado almacena los segmentos destinados al nodo móvil para poder retransmitirlos en caso que sea necesario ante una pérdida. Los almacena hasta que recibe la validación correspondiente del nodo móvil. Si no recibe esa validación pudo haber ocurrido que se perdió el segmento o su validación. A corto o mediano plazo el FA comenzará a recibir ACKs duplicados, evidenciando también la pérdida de segmentos.
La retransmisión de segmentos tendrá lugar por cuenta del FA que siempre se llevará a cabo mucho antes que si la hubiera hecho el corresponsal. Además el FA no debe validar los segmentos al

corresponsal, manteniendo así la sesión TCP end-to-end.
Eso sí, el FA capturará y filtrará los ACKs repetidos para evitar innecesarias retransmisiones por parte del corresponsal. Paralelamente también se logra disminuir el tráfico en el segmento inalámbrico.
La transferencia de datos del nodo móvil al corresponsal se llevará a cabo de la siguiente manera:

- El FA revisa el flujo de datos para detectar alteraciones en la secuencia de segmentos, es decir se fija si se perdió un segmento.
- Tan pronto como lo detecta envía un NACK al nodo móvil.
- El nodo móvil retransmite inmediatamente el segmento.
- El reordenamiento de segmentos tendrá lugar en el corresponsal y además esto forma parte de la versión estándar de TCP.
- Veamos las ventajas de este mecanismo:
- Se mantiene la sesión TCP end-to-end. Si el FA sale de servicio el nodo corresponsal y el móvil tendrán actualizadas todas las variables y estado de la sesión TCP en curso a diferencia de lo que podría ocurrir con I-TCP. Hay una vuelta a TCP estándar si este mecanismo deja de funcionar.
- No se requieren cambios en el nodo corresponsal.
- No requiere una actualización del estado en el caso que el nodo móvil se desplace a otro FA. Si aún hay datos en el buffer del FA anterior que no se transfirieron al nuevo FA, habrá un timeout en el nodo corresponsal, lo que provocará la retransmisión de segmentos al nuevo CoA.
- No hay inconvenientes en el caso en que el nuevo FA no soporte este mecanismo, se produce una vuelta automática al TCP estándar.
- Algunas desventajas de esta solución son las siguientes:
- Monitorear los segmentos TCP no genera la separación/aislación entre el sector móvil y el sector fijo de la sesión como el caso de I-TCP. Eso hace que por problemas en el FA el enlace inalámbrico se puede hacer visible para el corresponsal. Se deberá llevar cuenta de los retardos de cada parte y eventualmente modificarlos para que no ocurra esta visibilidad.
- Para generar las retransmisiones por parte del nodo móvil se recurría al envío de un NACK por parte del FA. Por lo tanto habrá que incorporarlo al TCP que resida en los FA y en los móviles.
- En el caso de proveer seguridad a la sesión y en modalidad que implique la encriptación del header del segmento, como

es el caso de IPsec Security Payload, la retransmisión por parte del FA no resultará por cuanto la retransmisión por parte de éste puede ser considerada como un ataque de "replay". Para que no haya inconvenientes la encriptación deberá darse en niveles superiores.

5.3.3 MTCP (Mobile TCP)

Presentamos ahora un protocolo MTCP que va a emular la funcionalidad de TCP entre el nodo móvil y el fijo, apuntando a reducir la carga de procesamiento en el nodo móvil y reduce la ocupación del tramo inalámbrico. El escenario que plantea y sobre el cual se aplica es el del tramo inalámbrico en que el nodo móvil y el access point se conectan directamente, como en un nivel de enlace.
De esta manera nos vamos a encontrar con un protocolo con prestaciones típicas de un nivel de enlace, de modo que muchas funciones del TCP estándar serán simplificadas o eliminadas.
El paradigma que adopta es el de la división en tramo fijo y tramo inalámbrico del momento en que define un protocolo optimizado para el tramo inalámbrico. Con esto se evita que el flujo de datos o throughput sea controlado de la misma manera, ya sea por pérdidas de segmentos en el tramo inalámbrico que por congestión en la red entre la estación base o el access point.

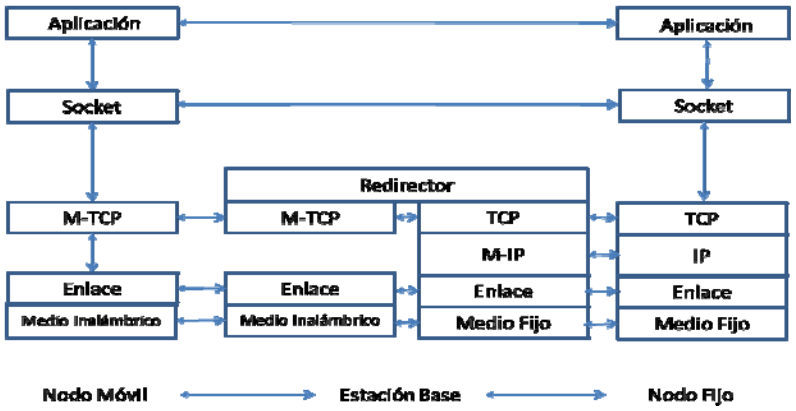


Figura 5.20 MTCP

Veamos las características distintivas del protocolo:

- Eliminación del procesamiento IP: dado que MTCP opera sobre un solo enlace no es necesario proveer capacidades de ruteo típicas de la capa de IP. Las características de direccionamiento y multiplexación de la plataforma TCP/IP,

si se implementan en MTCP. No es que se haya eliminado el nivel IP. Veamos en la Figura 5.20 la articulación de los diversos módulos de la arquitectura que propone MTCP

- Eliminar mecanismos de control de congestión: como las pérdidas en el tramo inalámbrico no se deben a congestión entonces MTCP no contempla este tipo de control. El control de congestión pasa a ser control de flujo. Se lo implementa a través de la ventana deslizante controlada por el receptor como en el TCP estándar.
- Compresión del encabezado: se elimina el encabezado de IP y se comprimen las direcciones IP destino y origen y los ports bajo la figura de un identificador.
- Técnicas de recuperación optimizadas: en el tramo inalámbrico se cuenta con la ventaja que los segmentos llegan en orden de manera que las técnicas de recuperación de errores resultan sencillas. Incluyen validaciones selectivas (SACK), solicitudes de retransmisión explícitas, etc.

Vemos en la Figura 5.21 las estructuras de los mensajes de control y de datos referidas al tramo inalámbrico, o sea MTCP.

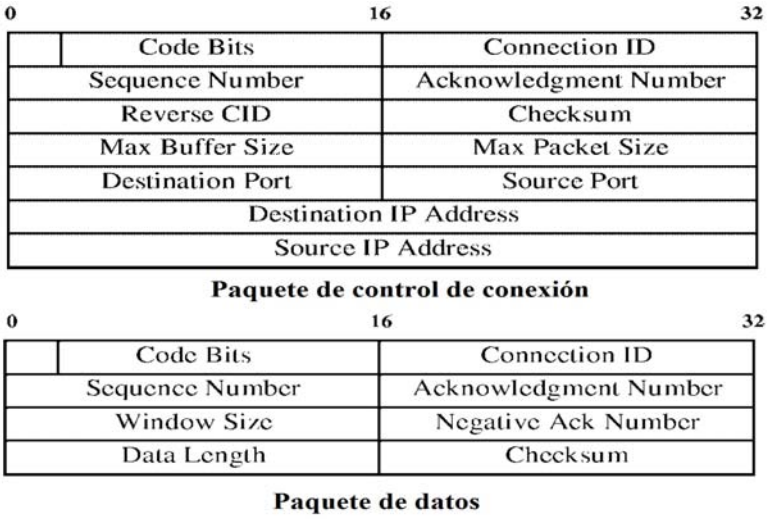


Figura 5.21 Estructuras MTCP

Dado que se han eliminado los encabezamientos de IP, MTCP incorpora la funcionalidad del direccionamiento en sus mensajes de control y de datos. MTCP codifica las direcciones IP y los Ports de TCP, generando un identificador de conexión, CID.

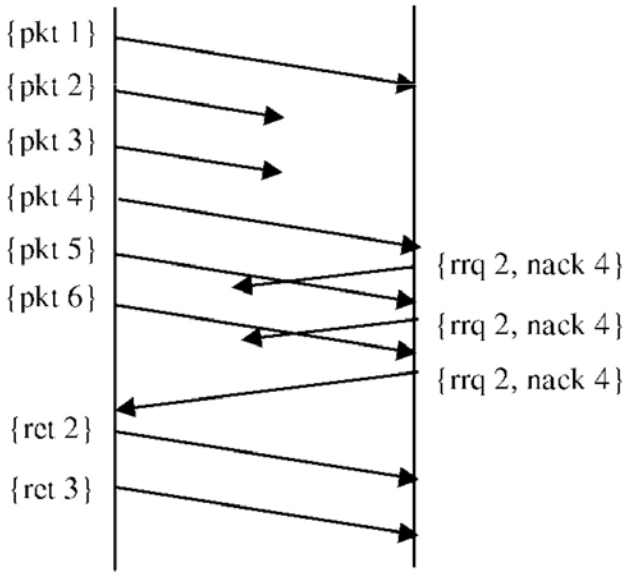
Con respecto al control de flujo, éste resulta más simple que en el caso de

TCP. Dado que no hay congestión en el segmento inalámbrico de la conexión el control de flujo en TCP queda reducido a emparejar el flujo de datos con la capacidad de recepción del receptor para evitar el "overflow" de sus buffers. Los mecanismos de control de congestión, típicos de TCP no estarán presentes en MTCP. El control de flujo implementado es similar al de TCP, a través de la ventana deslizante y dinámica controlada por el receptor. Recordemos entonces que la ventana máxima dependerá ahora de la capacidad del buffer del receptor. La performance conseguida será la típica con este tipo de control. Una capacidad de buffer por debajo del producto ancho de banda x RTT provocará una subutilización de la conexión inalámbrica y un valor por encima provocará buffers de tamaño excesivamente mayores.

El control de errores en MTCP se implementa tanto en le receptor como en el transmisor. Específicamente el receptor materializará el control de errores a través de la verificación del "checksum" y pérdida de secuencia. Cuando el receptor detecta un error lo reporta al transmisor retransmitiendo un ACK. El transmisor identifica estas pérdidas por la llegada de ACKs repetidos, tres de ellos, o por la ausencia de ACK en un intervalo de tiempo preestablecido.

Detectada la pérdida el transmisor retransmite los segmentos que correspondan con las siguientes diferencias respecto de TCP:

- Solicitud de retransmisión explícita(RRQ): Todos los segmentos en el tramo inalámbrico llegan en orden por lo que al tener el aviso de una pérdida MTCP dispara automáticamente la retransmisión en lugar de esperar al tercer ACK repetido como en el caso de TCP.
- ACK selectivos (SACK), para pérdidas en ráfaga: MTCP adopta la técnica de retransmisión selectiva [RFC 2018]. En este protocolo todo ACK duplicado contiene la secuencia del próximo segmento en orden que debería recibir. La Figura 5.22 lo ejemplifica.



- Figura 5.22 SACK

5.3.3.1 Performance de MTCP

Veamos algunos resultados de la aplicación de este protocolo [ZYG01]. En la Figura 5.23 tenemos representado el throughput conseguido en MTCP y TCP para diferentes tamaños de buffer en la que podemos observar una mejora del 40% para el caso de segmentos de 100 bytes y alrededor del 12% para segmentos de 1460 bytes. La mejora sustancial en los segmentos cortos a favor de MTCP indica que con éste se logra una mayor eficiencia de CPU que en el caso de TCP. Al aumentar el tamaño del buffer el tiempo de transmisión también aumenta y la optimización lograda en tiempo de procesamiento contribuye menos al aumento del throughput. También se puede verificar que la mejora en el throughput no se debe mayormente a la reducción del tamaño del encabezado a través de la curva identificada como MTCP_24 que corresponde a una implementación de MTCP con 24 bytes de encabezado.

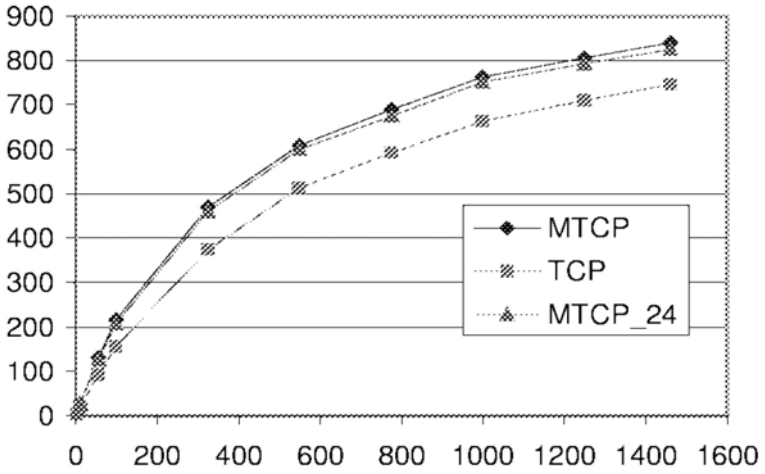


Figura 5.23 Performance de MTCP

5.4 Conclusión

Sin lugar a dudas que los dispositivos móviles y las redes móviles se han desarrollado en cuanto a diversidad de equipos con esas características como así también su integración a las redes fijas. Ello motiva la necesidad de contar con una plataforma TCPI/IP móvil confiable y comparable a la fija. Ya disponemos de IP móvil estandarizado. De esta manera se resolvió el problema de interoperabilidad que presentaba la integración de redes y dispositivos móviles a Internet. Resta por estandarizar TCP para los escenarios móviles. A partir de los esquemas presentados podemos concluir que TCP Móvil deberá:

- Evitar que se dispare el mecanismo de control de congestión erróneamente, por pérdida de segmentos y no por congestión real en la red.
- Manejar eficientemente la migración del usuario móvil de una estación base a otra.
- Tener en cuenta la menor capacidad de los enlaces inalámbricos y la menor disponibilidad de energía de los dispositivos móviles.
- Utilizar un tamaño de segmento variable controlado por la capacidad disponible en el enlace.
- Proveer la semántica end-to-end de TCP. Es decir, desde el usuario fijo al móvil y viceversa.
- Tratar de ser lo más transparente posible. Por lo menos no requerir cambios en los dispositivos de usuario.

Bibliografía

[802.1Q] IEEE Std 802.1Q-2005: IEEE Standards for Local and metropolitan area networks. Virtual Bridged Local Area Networks. Incorporates IEEE Std 802.1Q-1998, IEEE Std 802.1u-2001, IEEE Std 802.1v-2001,and IEEE Std 802.1s-2002.

[802.3at] IEEE Std 802.3at-2009: IEEE Standard for Information technology Telecommunications and information exchange between systems-Local and metropolitan area networks. Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements.

[802.11] IEEE Std 802.11-2007: IEEE Standard for Information technology Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[802.11e] IEEE Std 802.11e-2005: IEEE Standard for Information technology Telecommunications and information exchange between systems. Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements.

[802.11i] IEEE Std 802.11i-2004: IEEE Standard for Information technology Telecommunications and information exchange between systems. Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment: Medium Access Control (MAC) Security Enhancements.

[802.11n] IEEE Std 802.11n-2009: IEEE Standard for Information technology Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 5 Enhancements for Higher Throughput.

[802.16-09] IEEE Std 802.16-2009: IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems.

[ABI06] Femtocell Access Points: Fixed-Mobile Convergence for Residential, SMB, and Enterprise Markets, ABI Research. 2006.
[AMG08] Impact of Legacy Devices on 802.11n Networks. AirMagnet Whitepaper. 2008.
[AND07] Fundamentals of WiMAX-Understanding Broadband Wireless Networking. Andrews. Jeffrey G.- Ghosh, Arunabha. Prentice Hall. 2007.
[BAL95] Improving reliable transport and handoff performance in celular wireless networks. Balakrishnan, H., Seshan, S., Katz. R.H. Wireless Networks, J.C. Baltzer, no. 1, 1995.
[Bcom06] 802.11n: Next-Generation Wireless LAN Technology. Broadcom Whitepaper. 2006.
[BLUE10] Bluetooth Specification Version 4.0. Bluetooth SIG. 2010.
[CAR09] CCNA Wireless Official Exam Certification Guide (CCNA IUWNE 640-721). Brandon James Carroll. Cisco Press. 2009.
[CI09] 802.11n: The Next Generation of Wireless Performance. Cisco Network Whitepaper. 2009.
[COL09] Guide to Deploying 802.11n Wireless LAN. David Coleman. Fluke Networks. 2009.
[DOY09] Essentials of Cognitive Radio (The Cambridge Wireless Essentials Series). Doyle, Linda, Cambridge University Press, 2009.
[FRE99] Fundamentals of Telecommunications. 2nd. Ed. Roger L. Freeman. John Wiley & Sons. 1999.
[GAS05] Wireless Networks The Definitive Guide 2nd Ed. Matthew Gast. O' Reilly. 2005.
[GEI10] Designing and Deploying 802.11n Wireless Networks. Jim Geier. Cisco Press. 2010.
[ITUR1457] Detailed specifications of the radio interfaces of International Mobile Telecommunications-2000. Recommendation ITU-R M. 1457. 2000.
[NIST08] Guide to Bluettoh Security. Recommendations of the National Institute of Standards and Technology. Special Publication 800-121. Karen Scarfone, John Padgette. 2008.
[MKTK] Mikrotik Manual: http://wiki.mikrotik.com/wiki/Category: Manual.
[RFC793] Transmission Control Protocol. Request for Comments 793. J. Postel. RFC Editor. Septiembre 1981.
[RFC768] User Datagram Protocol. Request for Comments 0768. J. Postel. RFC Editor. Agosto 1980.
[RFC894] A Standard for the Transmission of IP Datagrams over Ethernet Networks. Request for Comments 894. Charles Hornig. RFC Editor. 1984.
[RFC1042] A Standard for the Transmission of IP Datagrams over Ethernet Networks. Request for Comments 1042. J. Postel, J. Reynolds. RFC Editor. 1988.

[RFC1191] Path MTU Discovery. Request for Comments 1191. J. Mogul, S. Deering. RFC Editor. 1990.
[RFC2018] TCP Selective Acknowledgment Options. Request for Comments 2018. M. Mathis, J. Mahdavi, S. Floyd, A. Romanow. RFC Editor. Octubre 1996.
[RFC2460] Internet Protocol, Version 6 (IPv6) Specification. Request for Comments 2460. S. Deering, R. Hinden. RFC Editor. Diciembre 1998.
[RFC3095] RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed. Request for Comments 3095. C. Bormann. RFC Editor. Julio 2001.
[RFC4303] IP encapsulating Security Payload (ESP). Request for Comments 4303. Kent, S. RFC Editor. Diciembre 2005.
[RFC4225] Mobile IP Version 6 Route Optimization Security Design Background. Request for Comments 4303. P.Nikander, J. Arkko, T.Aura, G. Montenegro, E. Nordmark. RFC Editor. Diciembre 2005.
[RFC4861] Neighbor Discovery for IP version 6 (IPv6).Request for Comments 4861. T. Narten, E. Nordmark, W. Simpson, H. Soliman. RFC Editor. Septiembre 2007.
[RFC4862] IPv6 Stateless Address Autoconfiguration. Request for Comments 4862. S. Thomson, T. Narten, T. Jinmei. RFC Editor. Septiembre 2007.
[RFC5681] TCP Congestion Control. Request for Comments 5681. M. Allman, V. Paxson, E. Blanton. RFC Editor. Septiembre 2009.
[SKL01] Digital Communications: Fundamentals and Applications, 2nd Ed. Bernard Sklar. Prentice Hall.2001.
[ZYG01] The design and performance of Mobile TCP for wireless networks. Zygmunt J. Haas, Abhijit Warkhedi. Journal of High Speed Networks, Vol 10 (2001) 187-207. IOS Press.

Esta publicación se terminó de imprimir
en el mes de octubre de 2011,
en la ciudad de La Plata,
Buenos Aires,
Argentina.