

Apuntes
de
Redes de Ordenadores

Tema 6
Wireless LAN

Uploaded by

IngTeleco

<http://ingteleco.iespana.es>
ingtelecoweb@hotmail.com

La dirección URL puede sufrir modificaciones en el futuro. Si no funciona contacta por email

6.- REDES LOCALES INALÁMBRICAS (WLAN)

6.1.- Introducción

En los últimos años, el mercado de las comunicaciones inalámbricas ha experimentado un crecimiento espectacular, consiguiendo un desarrollo tal que cientos de millones de personas la utilizan para intercambiar información principalmente mediante teléfonos inalámbricos, pero cada vez más también con otros dispositivos digitales.

Hasta hace poco las LAN estaban limitadas a la infraestructura cableada de un edificio. Muchos usuarios, si embargo, precisan de las ventajas añadidas de una red que no esté limitada por las restricciones de un cableado fijo.

La mayor motivación y beneficio de las LANs inalámbricas (WLANs) es la movilidad. A diferencia de otras conexiones de red, las WLANs permiten que los usuarios puedan moverse casi sin ninguna restricción y acceder a las LANs prácticamente desde cualquier lugar, proporcionando, además una flexibilidad mayor. En otras ocasiones es el criterio económico el que aconseja la utilización de WLANs.

Todos estos motivos condujeron a que creciera el interés de los usuarios y fabricantes por la tecnología que permitiera el despliegue de este tipo de red y que dentro del IEEE se decidiera la creación de un comité específico para el desarrollo de un estándar. El PAR (Project Authorization Request) 802.11 inicial dice lo siguiente:

"...the scope of the proposed [wireless LAN] standard is to develop a specification for wireless connectivity for fixed, portable, and moving stations within a local area." The PAR further says, "...the purpose of the standard is to provide wireless connectivity to automatic machinery and equipment or stations that require rapid deployment, which may be portable, handheld, or which may be mounted on moving vehicles within a local area."

El estándar resultante, denominado oficialmente "IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications," define protocolos inalámbricos para dar soporte a redes LAN inalámbricas (WLAN) Como otros estándares IEEE 802 el principal servicio del estándar 802.11 es enviar MSDUs (MAC Service Data Units) entres dos LLCs (Logical Link Controls). Generalmente un NIC inalámbrico y un punto de acceso (AP) proporcionan la funcionalidad del estándar 802.11.

6.2.- Características de IEEE 802.11

El estándar 802.11 proporciona funcionalidades MAC y PHY para la conectividad inalámbrica de estaciones fijas, portátiles o móviles a velocidades pedestres o vehiculares dentro de un área local. Los aspectos más destacados recogidos en el estándar 802.11 son los siguientes:

- Soporte de un servicio de envío asíncrono y limitado en el tiempo.
- Continuidad del servicio dentro de áreas extendidas mediante un Sistema de Distribución (pe Ethernet).
- Acomodo de velocidades de transmisión de 1 y 2 Mbps
- Soporte de la mayoría de las aplicaciones del mercado
- Servicios multicast
- Servicios de gestión de red
- Servicios de registro y autenticación

El estándar 802.11 considera las siguientes diferencias significativas entre las LANs cableadas y las inalámbricas:

Gestión de la energía: Dado que la mayoría de los NICs LAN inalámbricos están disponibles son de tipo PCMCIA es posible disponer de conectividad WLAN en ordenadores portátiles e incluso agendas. El problema, sin embargo es que estos dispositivos funcionan en base a baterías. La adición del NIC LAN al portátil puede descargar las baterías rápidamente. El grupo de trabajo 802.11 se afanó en la búsqueda de soluciones que permitieran a los NICs inalámbricos conmutar a modos de bajo consumo energético periódicamente cuando no transmiten, reduciendo de este modo el consumo. El nivel MAC implemente por lo tanto funciones de gestión de energía, poniendo la radio en estado "durmiente" cuando no hay actividad de transmisión durante un tiempo específico o bien definido por el usuario. El problema, sin embargo es que la estación "dormida" puede perder transmisiones de datos críticas. 802.11 resuelve el problema incorporando buffers para encolar mensajes. El estándar recoge que las estaciones deben "despertar" periódicamente y recuperar todos los mensajes pendientes.

Ancho de banda: Las bandas de espectro expandido no proporcionan un gran ancho de banda, manteniendo las velocidades de transmisión de datos por debajo de lo deseado por algunas aplicaciones. El grupo 802.11, sin embargo, consideró métodos para comprimir los datos, haciendo un mejor uso del ancho de banda disponible.

Seguridad: Las WLANs transmiten señales en áreas mucho más grandes que los medios cableados. En términos de privacidad, por lo tanto, las WLANs tienen un área a proteger muy superior. El grupo 802.11 coordinó su trabajo con el comité IEEE 802.10 responsable del desarrollo de mecanismos de seguridad para todas las series 802.

Direccionamiento: La topología de una red inalámbrica es dinámica; por lo tanto, la dirección de destino no siempre corresponde a la localización del destino. Esto origina un problema cuando se encaminan los paquetes a través de una red a su destino final. Puede ser preciso utilizar un protocolo basado en TCP/IP, como MobileIP, para gestionar estaciones móviles.

6.3.- Nivel Físico

El estándar 802.11 contempla especificaciones para los niveles físico (PHY) y de control de acceso al medio (MAC). El estándar actual especifica tres alternativas para el nivel físico, cualquiera de las cuales puede subyacer bajo la misma especificación el nivel MAC. Los miembros del comité 802.11 consideraron necesaria la existencia de alternativas de modo que los diseñadores de sistemas e integradores pudieran elegir la tecnología que mejor se ajustara en precio y rendimiento a cada aplicación específica, además de la presión de los fabricantes por mantener su alternativa tecnológica.

Específicamente, el estándar contempla una solución óptica que utiliza luz infrarroja (IR) para transmitir datos y dos soluciones basadas en RF que emplean "direct sequence spread spectrum" o "frequency-hopping spread spectrum".

La solución infrarroja está limitada en alcance y puede ser implementada dentro de un local, por el contrario, la solución RF puede utilizarse para cubrir áreas significativas y permite desplegar configuraciones de tipo celular en campus enteros. El uso de IR se considera generalmente más seguro frente a intrusos, puesto que la transmisión IR precisa de enlaces perfectamente alineados a la vista mientras que las transmisiones de RF pueden penetrar paredes y ser interceptadas por terceras partes sin ser detectadas. Sin embargo, las transmisiones IR pueden ser afectadas por la luz solar y el protocolo de espectro expandido 802.11 proporciona algunos elementos de seguridad rudimentarios para las transferencias de datos típicas.

La especificación IR contempla velocidades de 1-Mbps con picos de 2-Mbps y se basa en "Pulse Position Modulation" (PPM). La solución RF incluye las alternativas "Direct Sequence Spread Spectrum" (DSSS) y "Frequency Hopping Spread Spectrum" (FHSS) choices. Como indican los propios nombres, tanto DSSS como FHSS ensanchan artificialmente la banda de transmisión de modo que la señal transmitida pueda ser adecuadamente recibida y decodificada en presencia de ruido. Las dos alternativas RF, sin embargo, aprovechan el ensanchamiento de modos sustancialmente diferentes.

Los sistemas FHSS utilizan esencialmente técnicas de transmisión de datos de banda estrecha convencionales pero cambian regularmente la frecuencia en la que transmiten. Los sistemas saltan en un intervalo de tiempo fijo alrededor de una banda ancha o extendida utilizando diferentes frecuencias en una secuencia predeterminedada. El fenómeno de salto permite al sistema FHSS evitar el ruido de la banda estrecha en porciones de la banda de transmisión. Los sistemas DSSS, por el contrario, ensanchan artificialmente el ancho de banda necesario para transmitir modulando la secuencia de datos con un código de ensanchamiento. El receptor puede detectar datos sin errores incluso si el ruido persiste en parte de la banda de transmisión.

En 802.11, el nivel PHY DSSS define velocidades pico de transmisión de datos de 1- y 2-Mbps. El primero utiliza "Differential Binary Phase Shift Keying" (DBPSK) y el segundo "Differential Quadrature Phase Shift Keying" (DQPSK). El estándar define el nivel PHY FHSS para operar a 1 Mbps y permite una operación opcional a 2-Mbps, utilizando modulación "Gaussian Frequency Shift Keying" (GFSK) de 2- o 4-niveles.

Las WLAN tanto DSSS como FHSS operarán en la misma banda de frecuencias, de 2.4 - 2.4835 GHz (en el caso de transmisión de espectro expandido), que es una banda no sujeta a licencia para uso de aplicaciones industriales, científicas y médicas. Para la transmisión IR se utilizará la banda de 300 - 428,000 GHz para transmisión IR.

6.3.1.- Canalización del nivel físico RF

Una de las ventajas clave del nivel PHY RF es la posibilidad de tener un número de canales distintos. La "canalización" permite a los usuarios WLAN co-localizar canales en la misma área o áreas adyacentes para aumentar el rendimiento agregado o desplegar una matriz de canales de tipo celular que soporte roaming para los clientes. En el caso de DSSS, los diferentes canales simplemente utilizan diferentes frecuencias, en el caso de FHSS, la secuencia de salto utilizada diferencia un canal del siguiente, pero todos operan en la misma banda ancha de frecuencia.

Obviamente, DSSS y FHSS utilizan el espectro RF asignado de la banda de 2.4-GHz de modo diferente. Además, diferentes regiones del mundo, con regulaciones ligeramente distintas afectan a los esquemas exactos de canalización para ambos tipos de nivel PHY.

Generalmente, la especificación 802.11 define canales DSSS de 13-MHz que se utilizan para transportar una señal extendida de 1-MHz. Los canales se solapan con una nueva frecuencia central ubicada a intervalos de 5-MHz. Para el despliegue en los USA, el estándar define 11 canales DSSS independientes en el ancho de banda ISM asignado por la FCC. En la mayor parte de Europa y Asia que sigue los dictados de las agencias de regulación europeas, las implementaciones DSSS pueden utilizar 13 canales. En Japón, sin embargo, el ancho de banda asignado sólo soporta un único canal. En USA y Europa, la definición de canales asegura que tres canales de frecuencias aisladas están disponibles para su colocación.

Los sistemas FHSS, deben utilizar 79 saltos o frecuencias centrales en USA y Europa y 23 saltos en Japón. Generalmente, los sistemas FHSS dwell at each hop for 20 msecs. La especificación define 78 secuencias de salto diferentes, y cada secuencia de saltos independiente está definida como un canal. Prácticamente, sin embargo, sólo unos pocos canales pueden ser desplegados efectivamente en proximidad unos con otros.

6.4.- Topologías WLAN

Independiente del tipo de nivel PHY elegido, IEEE 802.11 soporta tres topologías básicas para WLANs, el "Independent Basic Service Set" (IBSS), el "Basic Service Set" (BSS), y el "Extended Service Set" (ESS). De hecho, el nivel MAC implementa el soporte de configuraciones IBSS, BSS, y ESS.

Las configuraciones IBSS también se conocen como configuraciones independientes o redes ad-hoc. Lógicamente, una configuración IBSS es análoga a una red de oficina punto a punto en la que no es preciso que un nodo funcione como servidor. Las WLANs IBSS incluyen varios nodos de estaciones inalámbricas que se comunican directamente entre sí sobre una base ad-hoc punto a punto. Generalmente, las implementaciones IBSS cubren un área limitada y no están conectadas a una red mayor.

Las redes 802.11 utilizan un bloque constructivo básico que es el conocido como BSS, y que proporciona un área de cobertura donde las estaciones del BSS se encuentran completamente conectadas. Una estación puede moverse libremente dentro del BSS, pero no puede comunicarse directamente con otras estaciones si abandona el BSS.

Las configuraciones BSS se basan en un "Access Point" (AP) que actúa como servidor lógico para una célula WLAN simple o canal. Las comunicaciones entre dos nodos A y B realmente van desde A al AP y desde el AP al nodo B. En principio puede parecer que el AP añade un nivel de complejidad innecesario, pero el AP permite bastantes capacidades de 802.11 que describiremos más adelante. Además, un AP es preciso para efectuar las funciones de bridging y conectar múltiples células WLAN o canales, y para conectar células WLAN a redes LAN cableadas.

Las configuraciones WLAN ESS consisten precisamente en múltiples células BSS que están enlazadas bien por backbones de cable o inalámbricos. IEEE 802.11 soporta configuraciones ESS en las que múltiples células utilizan el mismo canal, y configuraciones en las que múltiples células utilizan diferentes canales para aumentar el rendimiento agregado.

El sistema de distribución soporta los tipos de movilidad 802.11 proporcionando los servicios lógicos necesarios para gestionar la asignación dirección-a-destino y la integración transparente de múltiples BSSs. Un AP es una estación direccionable, con un interfaz al sistema de distribución para estaciones ubicadas en varios BSSs. Las redes BSS y ESS son transparentes al nivel LLC.

6.5.- Nivel MAC

El objetivo del nivel MAC es proporcionar funciones de control de acceso (direccionamiento, coordinación de acceso, generación de secuencias de comprobación de trama y su chequeo y delimitación de PDUs LLC).

Mencionar, en primer lugar, que el protocolo MAC 802.11 fue desarrollado para operar sin problemas con el estándar Ethernet de modo que se asegurase que los nodos cableados o no fueran lógicamente indistinguibles. El nivel MAC 802 difiere necesariamente del MAC Ethernet cableado, pero las diferencias son enmascaradas por un AP que conecta un canal WLAN con un backbone LAN.

802.11 define un formato de trama y un esquema MAC que difieren del estándar Ethernet. De hecho, este formato de trama robusto proporciona aspectos tales como reconocimiento rápido, gestión de estaciones ocultas, gestión de energía y seguridad de datos.

Para este nivel MAC, el estándar 802.11 especifica un protocolo de acceso múltiple con detección de portadora y eliminación de colisión (CSMA/CA). En este protocolo, cuando un nodo recibe un paquete

para transmitirlo, escucha para asegurarse que ningún otro nodo está transmitiendo; si el canal está libre, transmitirá el paquete. En caso contrario, elige un factor de retraso aleatorio que determina el tiempo que el nodo debe esperar hasta que puede transmitir su paquete. Durante períodos en los que el canal está libre, el nodo transmisor decrementa su contador de retraso y cuando este alcanza el valor cero, el nodo transmite el paquete. Dado que la probabilidad de que dos nodos elijan el mismo contador de retraso es pequeña, las colisiones entre paquetes se minimizan. La detección de colisiones, tal y como se utiliza en Ethernet no puede utilizarse en transmisiones de radio frecuencia, debido a que cuando un nodo está transmitiendo no puede escuchar a ningún otro nodo del sistema que está transmitiendo puesto que su propia señal ocultará a cualquier otra que llegue al nodo.

6.5.1.- Reconocimiento en el nivel MAC

La recepción de reconocimientos de trama proporciona un buen ejemplo de las diferencias entre los niveles MAC de 802.11 y Ethernet, y de la ventaja que proporcionan estas diferencias a un sistema inalámbrico. La mayor parte de las LANs se basan en que un nodo receptor envía un mensaje de reconocimiento para verificar que recibió una trama de datos. En Ethernet y en la mayoría de las LANs cableadas, sin embargo, el reconocimiento es gestionado por encima del nivel MAC.

El estándar 802.11 especifica que el nivel MAC gestiona los reconocimientos y que este mismo nivel es el responsable de retransmitir las tramas para conseguir una utilización más eficiente del ancho de banda y un reconocimiento más rápido. El formato de trama 802.11 se basa en un espaciado entre tramas de 50 μ s. El estándar precisa que la estación receptora envíe un reconocimiento 10 μ s después del fin de cada trama, siempre que la comprobación del CRC sea correcta. El límite de 10 μ s asegura que la estación receptora puede tomar inmediatamente el control del medio en lugar de competir con otros nodos por el acceso al mismo, como sería preciso si la espera fuera superior a los 50 μ s de espacio entre tramas. Las LANs que gestionan los reconocimientos en los niveles superiores al nivel MAC no pueden ajustarse a requisitos temporales precisos y por lo tanto las estaciones deben esencialmente competir por el acceso al medio y enviar una trama estándar para cada reconocimiento. La implementación del nivel MAC elimina las latencias del acceso al medio y permiten a los reconocimientos utilizar parte del período de espacio entre tramas en el que no se produciría ninguna actividad en cualquier caso.

La eficiencia del ancho de banda resulta doblemente importante en las configuraciones BSS o ESS porque muchas tramas deben ser enviadas do veces —del nodo A a un AP y desde el AP al nodo B. En tales casos, el AP debe enviar un reconocimiento al nodo A y el nodo B envía un reconocimiento al AP.

6.5.2.- Solución a las estaciones ocultas

Un fenómeno bastante común de las instalaciones WLAN, el de la estación oculta es el motivo de otro de los aspectos de 802.11.

En una configuración BSS o ESS la WLAN pueden producirse colisiones originadas por una estación oculta. En dichos casos, la estación A puede comunicarse con el AP sin problema y la estación B comunicarse con el AP sin problema, pero las estaciones A y B están físicamente separadas por suficiente distancia para evitar comunicaciones directas.

Dado que A y B no se comunican directamente en una configuración ESS, el problema de la estación oculta no afecta a las comunicaciones reales sino a la competencia por el acceso al medio. El esquema de eliminación de colisiones adoptado por 802.11 requiere que una estación evite transmitir cuando otros nodos lo están haciendo; sin embargo, el nodo A no sería capaz de detectar que el nodo B estaba transmitiendo al AP en el ejemplo de la estación oculta.

802.11 incluye la opción de un Request To Send (RTS)/Clear To Send (CTS) para proteger de las interferencias de una estación oculta. Todos los receptores 802.11 deben soportar RTS/CTS, pero el soporte es opcional para los transmisores. Para utilizar la facilidad, el nodo transmisor (B en este caso) envía una petición RTS al AP pidiendo la reserva de una cantidad de tiempo fija necesaria para transmitir una trama de una longitud determinada. Cuando el medio está disponible, el AP difunde un mensaje CTS que todas las estaciones pueden escuchar, asegurando al nodo B acceso durante el tiempo solicitado.

La opción de utilizar RTS en el transmisor puede ser aprovechada por el fabricante de equipos 802.11 o en algunos casos por el administrador o usuario de la WLAN. Por ejemplo, un fabricante de tarjetas interfaz de red (NIC) podría elegir no soportar la opción RTS para minimizar costes, especialmente porque este fenómeno no se utiliza en muchas instalaciones. Alternativamente, el fabricante de NIC puede implementar la opción y permitir al usuario utilizar selectivamente RTS. Si el usuario tiene la certeza de que todas las estaciones están dentro del alcance, deshabilitando el RTS puede aumentar el aprovechamiento del ancho de banda eliminando el tráfico RTS/CTS.

El modo en el que está implementado el carácter opcional del uso de RTS en el transmisor es mediante un "umbral de longitud". Se puede fijar un umbral de la longitud de un mensaje y cuando un transmisor quiere transmitir un mensaje mayor que dicha longitud, utiliza el mecanismo RTS/CTS. Fijando el umbral de longitud a un valor máximo, el transmisor no utilizará realmente nunca RTS. El modo en que se utilizaría este umbral es por ejemplo en un AP, donde no se da el problema del nodo oculto y donde se desconectaría la opción RTS. En un cliente puede decidirse activarlo fijando algún umbral (debemos tener en cuenta que siempre existe un compromiso entre introducir más sobrecarga y menos retransmisión de mensajes debido al problema del nodo oculto). La situación en la que RTS/CTS resulta muy útil es la de un entorno exterior punto a multipunto en donde el problema del nodo oculto puede ser muy importante.

6.5.3.- Sistema de distribución inalámbrico

Hay también bastantes aspectos del nivel MAC de 802.11 que resultan clave para optimizar las comunicaciones inalámbricas. Por ejemplo, la mayoría de las WLANs existentes hasta el momento requerían APs con puertos separados para soportar las funciones de bridging. Un AP que tenía un WLAN radio y una conexión Ethernet cableada podía intercambiar paquetes entre el canal inalámbrico y el backbone cableado. La WLAN de radio no podía gestionar simultáneamente comunicaciones con los nodos locales y comunicaciones troncales inalámbricas con un segundo AP.

El estándar 802.11 añade un sistema de distribución inalámbrico o capacidad de backbone inalámbrico sobre un solo canal por medio de soporte de bridging de nivel MAC. El bridging de canal único opera utilizando un mecanismo de reenvío de tramas. Cuando un AP recibe una trama para un nodo con el que no está conectado, puede enviar la trama a otro AP conectado por el mismo canal inalámbrico. Dichos backbones de canal único resultan muy económicos porque cada AP precisa de un solo canal de radio. Además, ofrece un rendimiento perfectamente aceptable en muchos casos, aunque la red entera está limitada al rendimiento agregado disponible sobre un canal simple.

6.5.4.- Fragmentación

El nivel MAC también soporta un concepto denominado fragmentación, que proporciona flexibilidad en el diseño del transmisor/receptor, y puede resultar útil en entornos con interferencias RF. Un transmisor 802.11 puede dividir mensajes opcionalmente en fragmentos más pequeños para su transmisión secuencial. Un receptor puede recibir de modo más fiable las ráfagas de datos más breves porque la menor duración de cada fragmento reduce la probabilidad de errores debido a ruidos o pérdidas de señal. Además, los fragmentos menores tienen más probabilidad de escapar de interferencias en forma de ráfagas como las de un emisor microondas.

El estándar 802.11 indica que todos los receptores deben soportar la fragmentación, pero deja opcional el soporte en los transmisores. Los diseñadores y los usuarios finales potenciales pueden determinar cuando utilizar la fragmentación. Por ejemplo, el diseñador del producto podría desarrollar un esquema adaptativo que habilitara la fragmentación dinámicamente en presencia de ruido o interferencias.

Los diseñadores podrían añadir la capacidad de que el usuario final pudiera permitir la fragmentación cuando los errores de transmisión se convierten en un problema. Los fabricantes pueden utilizar también la fragmentación como un compromiso precio/rendimiento. Asumiendo la fragmentación permanente en un transmisor, el receptor puede ser diseñado con componentes más baratos, resultando un receptor de menor sensibilidad. La fragmentación, sin embargo, produce sobrecarga en cada fragmento en lugar de en cada trama, reduciendo por tanto el rendimiento agregado de la WLAN y el rendimiento pico alcanzable entre estaciones.

6.5.5.- Roaming

La provisión de "roaming" implementada en 802.11 también proporciona numerosas ventajas. Por ejemplo, la mayoría de las WLANs existentes precisan nodos clientes que "roam" de un AP a otro utilicen todos el mismo canal. Generalmente, los APs están conectados mediante un backbone cableado. Como se ha mencionado anteriormente, cuando todos los APs utilizan el mismo canal, la capacidad agregada disponible para toda la red está limitada al rendimiento de un canal. Esta limitación es bastante necesaria porque ofrecer una cobertura del 100% en un esquema de tipo celular requiere que los clientes estén a menudo dentro del alcance de varias APs.

El estándar 802.11 incluye mecanismos para permitir a un cliente "roam" entre varios APs que pueden ser operados en el mismo canal o en canales separados. Cada AP transmite una señal de "beacon" cada 100 encuentros. El beacon incluye una marcha de tiempo (time stamp) para la sincronización de clientes, un mapa de tráfico, una indicación de las velocidades de transmisión de datos soportadas y otros parámetros. Los clientes de roaming utilizan el beacon para medir la fortaleza de una conexión existente a un AP. Si la conexión se juzga débil, la estación que hace roaming puede intentar asociarse con un nuevo AP.

La estación roamer realiza en primer lugar un escaneo para localizar un nuevo AP en el mismo o en diferente canal. El cliente puede enviar pruebas a un número de APs y recibir respuestas a las mismas desde cada uno para estimar el AP más fuerte. Una vez encontrada la señal más fuerte, el cliente envía una petición de reasociación al nuevo AP, que debe aceptar y reconocer la petición para completar el procedimiento de roaming. El AP debe enviar una indicación de la reasociación a través de la ESS LAN o el sistema de distribución.

6.5.6.- Ahorro de energía

El tema del roaming sugiere que por su naturaleza muchos clientes WLAN serán sistemas portátiles, y el hecho de que estos sistemas operen habitualmente con baterías lleva a otra área de especialización de la especificación MAC 802.11. Específicamente, se contemplaron aspectos en el MAC que permitieran maximizar la duración de las baterías en los clientes portátiles mediante esquemas de gestión de energía.

La gestión de energía crea problemas con los sistemas ALAN porque los esquemas de gestión típicas ponen al sistema en modo "durmiente" (sleep mode) cuando no se produce actividad durante un período de tiempo específico o determinado por el usuario. Desdichadamente, un sistema durmiente puede perder transmisiones de datos críticas.

Para dar soporte a clientes que periódicamente entran en modo "durmiente", 802.11 especifica que los APs deben incluir buffers para encolar los mensajes. A los clientes dormidos se les pide que despierten periódicamente y recuperen todos los mensajes. Se permite a los APs que eliminen los mensajes no leídos después de pasar un tiempo especificado aunque los mensajes no hayan sido recuperados.

La implementación del esquema de gestión de energía es relativamente simple en una configuración BSS o ESS porque el AP siempre está presente. Además, el AP no opera con baterías y nunca entra en modo durmiente. En una configuración IBSS, sin embargo, no existe un AP permanente y todos los sistemas pueden entrar en modo durmiente.

802.11 no proporciona ahorro de energía en una configuración IBSS. Esencialmente, todos los clientes en la configuración IBSS deben estar despiertos cada vez que se envía un beacon. Los clientes alternan aleatoriamente la tarea de transmitir un beacon. Inmediatamente después de la transmisión de cada beacon, comienza un breve período de tiempo denominado Announcement Traffic Information Message (ATIM). Durante esta ventana ATIM cualquier estación puede indicar la necesidad de transferir datos a otra estación durante la siguiente ventana "daLa-transmission". Los clientes sin tramas entrantes o salientes pueden reentrar en modo durmiente durante la la ventana "daLa-transmission".

La capacidad de ahorro de energía de 802.11 se refiere primordialmente a los NICs. La gestión de energía en el ámbito de sistema de un cliente permanece en el dominio del diseñador de sistema. Obviamente, sin embargo, el NIC debe ser capaz de despertar independientemente del sistema cliente y el NIC debe ser capaz de despertar al cliente cuando detecta la existencia de tramas entrantes pendientes.

6.5.7.- Privacidad equivalente al cableado

Uno de los últimos aspectos diferenciales entre 802.11 y cualquiera de las LANs cableadas o de las ALAN implementadas anteriormente es la seguridad de los datos. El estándar define un mecanismo por el cual las WLANs pueden proporcionar una privacidad equivalente al cableado, "Wired Equivalent Privacy" (WEP). El mecanismo WEP opcional es especialmente importante porque las transmisiones RF, incluso en transmisiones de espectro expandido, pueden ser interceptadas más fácilmente que las transmisiones cableadas.

802.11 contempla el mecanismo WEP dentro del MAC que cubre la transmisión estación-estación. El estándar especifica la utilización del algoritmo de seguridad RC4 del RSA. El esquema se basa en una clave de 40-bit para encriptar el campo de datos de las tramas. El grupo de trabajo eligió el algoritmo RC4 en parte porque el Gobierno USA no restringe la exportación de productos que utilizan el método de encriptación RC4. Por el contrario, otros algoritmos como DES sólo pueden ser exportados en unas pocas aplicaciones específicas. Además, los tests realizados por miembros de 802.11 probaron que RC4 ofrece un grado de seguridad que se ajusta o excede de la privacidad alcanzable por la Ethernet estándar cableada.

6.6.- Continuación dentro del IEEE 802.11

Mientras los fabricantes están poniendo en el mercado productos compatibles 802.11, los miembros del comité y las compañías que han desarrollado el estándar continúan su trabajo buscando futuros desarrollos que proporcionen una mejora continua del estándar. Por ejemplo, 802.11 permite el roaming siempre que todos los APs en una instalación ESS fueran del mismo fabricante. El estándar no asegura que los clientes puedan hacer roaming entre APs de fabricantes diferentes.

Para conseguir un roaming multivendedor, Aironet Corp, Digital Ocean, y Lucent Technologies han colaborado para desarrollar la especificación del Protocolo entre puntos de acceso (Inter Access Point Protocol). El IAPP extenderá los beneficios de la interoperabilidad multivendedor 802.11 con protocolos de roaming comprensibles. Hay dos protocolos de transferencia definidos dentro de IAPP, uno para LANs lógicas simples y otro para atravesar los límites de un router utilizando UDP/IP. Los nodos que hacen roaming atravesando los límites de un router precisan también de software de IP móvil. Otras varias compañías, incluyendo IBM, han anunciado soporte para el IAPP como una parada necesaria hacia la real interoperabilidad multivendedor.

6.6.1.- Velocidades de transmisión mayores

Si bien 802.11 ofrecerá un rendimiento agregado comparable con la red Ethernet de 10-Mbps, algunas aplicaciones como las multimedia demandan velocidades de pico mayores. Además, picos más rápidos permitirían a más nodos conectarse con efectividad a una WLAN mediante un simple canal. El siguiente paso en la evolución de 802.11 es probablemente un estándar para mayores velocidades de transmisión, del orden de 10 Mbps y superiores. En la última reunión del IEEE, se preparó un borrador de una petición de autorización de proyecto (PAR) para 20 Mbit/s en la banda 5.2 GHz.

En la banda de 2.4 Ghz, también se han producido discusiones acerca de velocidades mayores.

Mientras tanto, Lucent Technologies ha desarrollado en sus laboratorios un esquema ALAN base DSSS que puede extender picos de velocidades de datos desde los 2 Mbps a 10 Mbps. Además, el esquema asegura la compatibilidad con los productos existentes de Lucent y con IEEE 802.

El esquema, denominado Direct Sequence/Pulse Position Modulation (DS/PPM), varía la temporización de los símbolos de datos y dicha varianza se utiliza para acondicionar bits adicionales de los datos en cada símbolo. Esta técnica PPM acelera las velocidades DS normales de 2-Mbps a 8

Mbps. DS/PPM también utiliza Quadrature Amplitude Modulation (QAM) mientras que las WLANs DS 802.11 utilizan Phase Shift Keying (PSK) modulation. Combinando QAM y PPM alcanza las velocidades DS/PPM de 10- Mbps.

Mientras que DS/PPM desembocará en productos significativamente más rápidos, dichos productos serán compatibles con las NICs y APs 802.11. El esquema DS/PPM utiliza las mismas bandas de frecuencia definidas para las WLANs DS de 2-Mbps en 802.11. esta nueva implementación de la tecnología permitirá que los dispositivos de 2 y 10-Mbps operen indistintamente en el mismo canal y a un dispositivo de 10-Mbps bajar automáticamente a la velocidad de 2-Mbps para comunicarse con nodos 802.11.

6.- REDES LOCALES INALÁMBRICAS (WLAN)	1
6.1.- Introducción	1
6.2.- Características de IEEE 802.11	2
6.3.- Nivel Físico	2
6.3.1.- Canalización del nivel físico RF	3
6.4.- Topologías WLAN	4
6.5.- Nivel MAC	4
6.5.1.- Reconocimiento en el nivel MAC	5
6.5.2.- Solución a las estaciones ocultas	5
6.5.3.- Sistema de distribución inalámbrico	6
6.5.4.- Fragmentación	6
6.5.5.- Roaming	7
6.5.6.- Ahorro de energía	7
6.5.7.- Privacidad equivalente al cableado	8
6.6.- Continuación dentro del IEEE 802.11	8
6.6.1.- Velocidades de transmisión mayores	8