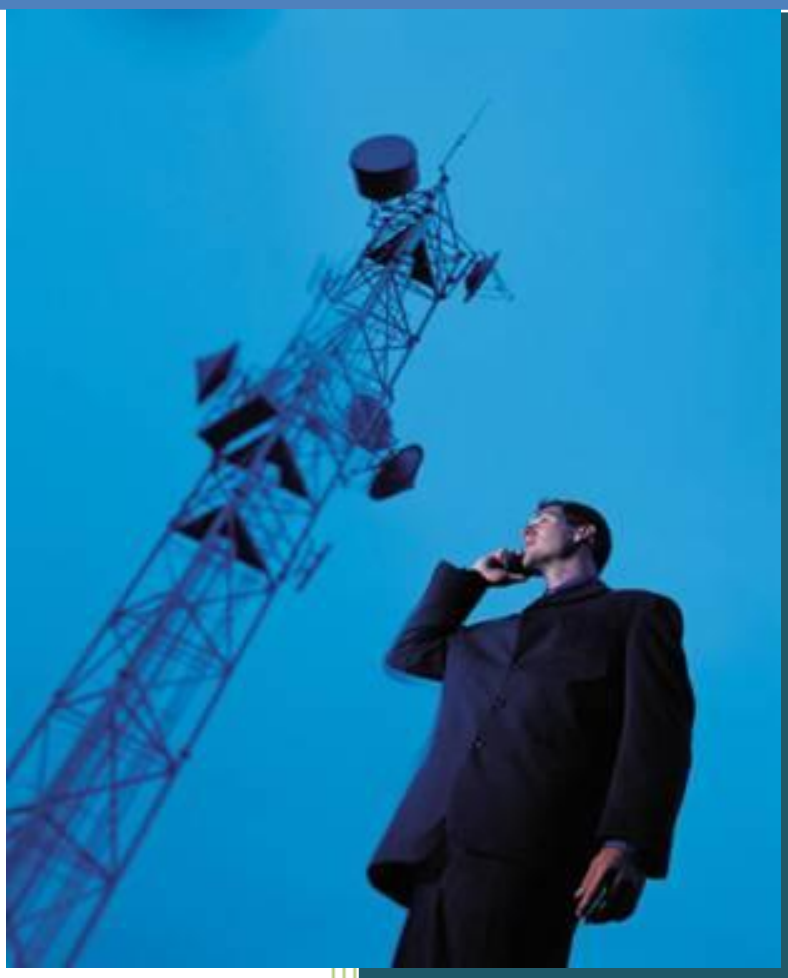
2007

ESTUDIO Y ANÁLISIS DE LOS FACTORES PRINCIPALES PARA EL FUNCIONAMIENTO EFECTIVO DE LA TECNOLOGIA VOIP VIA 802.11



ADRIANA MARCELA ZIPA LLAMAS
ENRILE MARTÍNEZ DIPPE
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
NOVIEMBRE-2007

Contenido

Indice de Figuras

Indice de Tablas

1. INTRODUCCIÓN: CONCEPTOS GENERALES ACERCA DE VO802.11

Para entender las funciones de la PSTN (public switched telephone network) y de por qué puede ser reemplazada, debemos conocer sus tres principales componentes: acceso, conmutación o switching y transporte. El acceso se refiere a cómo el usuario accede a la red. La conmutación o switching se refiere a la manera en que están conectados los enlaces y encontrar el camino directo para la comunicación, y el transporte describe el modo de enviar la información a través de la red dependiendo si es sólo voz, datos o ambos.

1.1. Acceso

Como se mencionó anteriormente, el acceso se refiere a como el usuario entra a la red telefónica. Para la mayoría de los usuarios, el acceso a la red se da mediante el teléfono. La transmisión se da mediante una especie de diafragma en la boquilla del teléfono que convierte la presión del aire producida por la voz en ondas electromagnéticas análogas para la transmisión hasta el switch. El auricular del teléfono hace el proceso contrario.

El aspecto más sofisticado del dispositivo telefónico es su función DTMF (dual-tone multifrequency), la cual permite que se pueda comunicar con el switch mediante tonos. El teléfono es normalmente conectado a la oficina central donde el switch está ubicado par de cobre trenzado, o, si es el caso de instalaciones más recientes, cables de fibra óptica. Todo el cableado y alambrado entre el abonado y la oficina central así como las estructuras y aparatos usados para la conexión se conoce como outside plant o planta externa. Al conjunto de equipos instalados en la Terminal del suscriptor los cuales permiten su conexión con la Central se les denomina CPE (customer-premises equipment) o equipos en las instalaciones del cliente.

El surgimiento de tecnologías emergentes para Internet banda ancha inalámbrico tales como 802.11a/b han hecho que el cobre, el cual ha sido el medio de conexión tradicional entre las locaciones residenciales y pequeñas empresas provista por las compañías telefónicas sea totalmente desplazado

Sin el uso del cobre como medio para alcanzar la conexión a residencias o empresas, los proveedores de servicios se evitan los altos costos de montar una infraestructura cableada así como los enredos con las normas legales para poder desplegar un servicio como éste que pueda competir con la competencia.

Un nuevo mercado ha surgido para las redes de voz: son las tecnologías 802.11a/b. La mayoría de los vendedores de equipos de telecomunicaciones como Motorola, Cisco, y Avaya, ya tiene productos dirigidos a redes de datos y voz inalámbricas. El objetivo de estas industrias es el mercado de empresas con LANs, sin embargo, no estaría demás esperar que estas tecnologías, poco a poco, se tomen el mercado de los proveedores de servicios telefónicos.

1.2. Conmutación

La red PSTN es una red en topología estrella, en el cual los suscriptores están conectados entre sí al menos mediante un hub, si no son mas, los cuales están ubicados en oficinas conocidas como Centrales. En estas oficinas, también hay switches. Hay oficinas locales para servicios de conexión locales y hay oficinas tándem para servicios de conexión de larga distancia. Las oficinas locales, mejor conocidas como Centrales Telefónicas o COs, utilizan switches Clase 5 y las oficinas tándem o centrales tándem usan switches clase 4.

El final de los años 90 se vio marcado por la el surgimiento de VoIP (Voice Over Internet Protocol), que utiliza una tecnología conocida como softswitch para reemplazar los switches clase 4 y 5 el cual no es más que un software implementado en algún servidor conectado a la red IP.

En vez de gastarse 10 millones de dólares en costos de equipos y ocupar un extenso espacio para Centrales Telefónicas (CO, Central Office), un softswitch puede ser implementado casi en cualquier servidor del tamaño de un refrigerador pequeño. Las plataformas para softswitch son equivalentes a una fracción de una de un switch clase 5, otra ventaja además es que con tecnología softswitch no es necesario enrutar el tráfico de voz a través de imponentes switches clase 4 o 5, sino de una manera más simple.

1.3. Transporte

La aparición del Protocolo de Internet IP como tecnología de transporte ocasionó un boom en la construcción de backbones IP, lo cuales tenían una gran ancho de banda, esto es, una sobreabundancia en la capacidad de estas redes. Contrario a las redes tradicionales de telefonía, todos los proveedores de servicios de VoIP prestaban sus servicios de larga distancia mediante una conexión al backbone IP.

1.4. Vo802.11: Desplazando al lazo local (local loop)

La aparición de voice over 802.11 (Vo802.11), mostró la simplicidad del acceso al servicio de voz y movilidad en el uso de éste, si tan solo se reemplaza el cobre de la PSTN. Una vez que el flujo VoIP alcanza la parte cableada de una red (el Access point), este es transportado en una red IP (LAN, IP backbone). Debido a que VoIP está basado en IP, éste puede ser manejado por un switch VoIP específico, correspondiente al softswitch mencionado anteriormente. Aunque la conversación puede ser originada y conmutada por una red IP, es posible también originarla y finalizarla en la PSTN. Este gateway, dependiendo de la dirección del tráfico, empaqueta o desempaqueta el tráfico de voz que viaja entre dos redes diferentes,

En conclusión, ahora es completamente posible desplazar la tradicional PSTN, pues reemplazando los elementos de la PSTN con tecnologías basadas en IP, es posible copiar todas las funciones de la PSTN, y no tan solo eso, sino que también pueden crearse una multitud de nuevas funciones. Los servidores de aplicaciones que operan con softswitches permiten la creación rápida de nuevas

funcionalidades lo cual no hubiera sido posible con la red conmutada de PSTN o realmente si, pero cuesta demasiado dinero lo cual no se justifica.

Una gran cantidad de inconvenientes han surgido en la tecnología Vo802.11. Estos inconvenientes se enfocan en lo que tiene que ver con VoIP y 802.11, ya que el mercado tiene la percepción de que son tecnologías que tienen muchas debilidades y que su nivel de calidad no se compara con el de la PSTN.

De aquí en adelante estudiaremos la tecnología inalámbrica y cuáles son los inconvenientes antes mencionados.

2. INCONVENIENTES DE Vo802.11

Para analizar correctamente las perspectivas para el uso de Vo802.11, es necesario categorizar en que parte de la red están las debilidades o cuáles están expuestas a inconvenientes potenciales. ¿Estas degradaciones potenciales ocurrirían en el segmento 802.11 de la red o en las tecnologías relacionadas con VoIP? Si es así, ¿donde y cómo pueden ser minimizadas o eliminadas esas degradaciones? Aquí nos concentraremos en los posibles inconvenientes de las tecnologías 802.11 y VoIP.

2.1. Inconvenientes relacionados a 802.11

Los censuradores de IEEE 802.11 indican que la tecnología no alcanzará la aceptación popular porque se limita en rango de alcance, seguridad y QoS. Como con cualquier otra tecnología, el mercado se esfuerza constantemente en superar estos inconvenientes con mejoras en el 802.11. La concepción de que las tecnologías wireless sustituirán a la PSTN se enfrenta con un gran número de inconvenientes. Estos inconvenientes se centran principalmente en el QoS, la seguridad de las redes inalámbricas, y las limitaciones en el rango de alcance del servicio.

2.1.1.QoS

Uno de los principales problemas en la entrega de datos por wireless es que, así como en el servicio de Internet por cable, un QoS inadecuado es inevitablemente un factor perjudicial. La interferencia con otros servicios inalámbricos, las pérdidas de paquetes, y las interferencias atmosféricas son inconvenientes constantes del 802.11b y para los protocolos inalámbricos asociados que son una alternativa para las redes PSTN (Figura 2.1) El QoS también está relacionado con la capacidad del proveedor de servicio para entregar servicio de voz de buena calidad en su red. La PSTN no puede ser reemplazada hasta que haya una alternativa lo suficientemente fuerte que pueda competir con su servicio de voz mediante cobre.

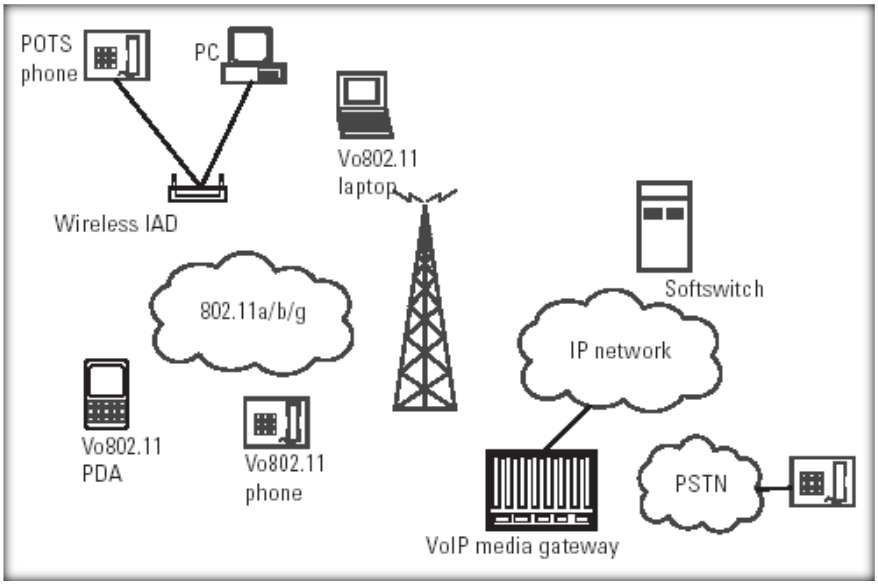


Figura 2. 1 Descripción de una banda ancha inalámbrica, la cual es alternativa para el servicio de PSTN.

2.1.2.Seguridad

La prensa ha sido rápida al divulgar sobre las debilidades que han sido encontradas en las redes inalámbricas. La red 802.11b tiene dos mecanismos básicos de seguridad, los cuales son el SSID (Service Set IDentifier (SSID) y el protocolo WEP (Wired Equivalency Privacy). Estas medidas pueden ser adecuadas para las residencias y pequeñas empresas pero inadecuadas para las empresas que requieren una seguridad más fuerte. Sin embargo un número de medidas adicionales pueden ser agregadas a aquellas redes inalámbricas en que los suscriptores requieran mayor nivel de seguridad

2.1.3.Alcance

En la mayoría de las aplicaciones omnidireccionales, 802.11 ofrece un alcance cercano a los 100m. ¿Entonces cómo esta tecnología ofrecerá un alcance como para competir con la PSTN? El alcance está en función del diseño y de la potencia de la antena utilizada, pero sobre todo del diseño de la antena. Con la antena y la potencia correctas, el alcance de 802.11 se puede prolongar a decenas de millas.

2.2. Inconvenientes relacionados con VoIP

2.2.1.Confiabilidad

La principal preocupación que tienen los proveedores de servicio cuando comparan la competitividad de las tecnología inalámbricas con los switches PSTN's clase 4 y clase 5 es la confiabilidad. Los switches clase 4 y clase 5 tienen una reputación de confiabilidad de categoría "cinco 9s", lo que quiere decir que solo estarán fuera de servicio tan solo 5 minutos en el transcurso de un año.

Crear una solución para la conmutación de voz para alcanzar la categoría cinco 9s' no es posible ni mediante magia negra ni por mandato del cielo en tablas de oro, es simplemente una cuestión de meticulosa ingeniería para crear así una solución consistente en un conjunto de elementos redundantes, y no para solucionar solo un punto de falla, porque se debe planear con NEBS[1] un periodo de inactividad, cuya duración sea máximo de 5 minutos al año. Muchas de las soluciones con softswitch ahora ofrecen categoría de confiabilidad "cinco 9s" o mejor aún.

2.2.2.Escalabilidad

Un segundo punto importante para los proveedores de servicio, es la escalabilidad de un softswitch en relación al de un switch clase 4 o clase 5. Para competir con un switch clase 4 o clase 5, la solución softswitch debe lograr expandirse hasta decenas de miles (líneas telefónicas o puertos) en una zona. Las soluciones con Softswitch, gracias a sus gateways modernos y de alta densidad,

[1] NEBS - Network Equipment Building System : es un estándar para los equipos de telefonía. Se desarrolló en la década de 1970 por los laboratorios Bell (ahora Solutions), muchos fabricantes de equipo debían construir su equipo a las normas NEBS, incluso cuando no tienen la intención de su equipo que se ha colocado en una oficina central)

ahora igualan o exceden 24.000 DS0s en un rack de 7 pies en comparación con los nueve racks que ocupa un switch clase 4 o de la clase 5 para hacer 24.000 DS0[2]s.

Además, las plataformas de softswitch ahora ofrecen potencia en procesamiento de llamadas en términos de millones de BHCAs (busy hour call attempt o número de intentos de llamada en horas pico) en comparación con las cientos de miles ofrecidos por las plataformas tradicionales de conmutación (switching) que usa la PSTN.

Una ventaja significativa de los softswitch sobre los switches clase 4 y de la clase 5 con respecto a la escalabilidad es que ellos pueden reducirse hasta gateways de dos puertos o aún de uno solo en el caso de los teléfonos IP, permitiendo flexibilidad ilimitada. La configuración mínima para un switch clase 4 en cambios es de 480 DSOs.

2.2.3. QoS

Las primeras aplicaciones VoIP dejaron una mala reputación por la mala calidad del servicio que ofrecieron. Las primeras aplicaciones disponibles surgieron en 1995 y se distinguieron porque el uso de este se hacía a través de Internet mediante el uso del PC con micrófono y altavoces. Las llamadas frecuentemente se caían y la calidad de la voz era cuestionable.
Las inmensas mejoras realizadas durante los últimos 7 años a las redes IP, sumadas con los avances en las tecnologías de media gateways, hacen que ahora estas redes discriminadas en el pasado, entreguen una calidad de la voz que iguala o excede la entregada por los switches clase 4 y clase 5 de la PSTN.

2.2.4. Señalización

Un elemento de la PSTN que fue diseñado para entregar una buena QoS y miles de funcionalidades es el SS7. La interconexión de las redes de SS7 y de IP necesaria para procesar llamadas que viajan a través de PSTN y la red IP es un gran desafío. Sin embargo, se ha alcanzado un gran progreso, con la aparición de la nueva tecnología que logra que el SS7 funcione con las redes IP y la cual es conocida como SigTran (for Signaling Transport). Además, la industria VoIP tiene nuevos protocolos tales como SIP que igualan o exceden al SS7 en sus funcionalidades de señalización.

[2] Digital Signal 0 (DS0) es una tasa básica de señalización de 64 Kbps, que corresponden a la capacidad de un canal equivalente a la frecuencia de la voz. Para transportar una conferencia telefónica, el sonido es digitalizado a una tasa de 8 kHz utilizando una modulación de código de pulsos (Pulse Code Modulation: PCM) de 8 bits. Múltiples DS0 son transportados en un enlace de mayor capacidad; 32 DS0s en el caso de un E1. La topología utilizada en nuestra red wan es una combinación de malla y estrella, en una comunicación punto multipunto a través de fibra óptica (E1) en el nodo central y DS0 en los nodos remotos. Donde **E1** es el medio de conducción de señales digitales por fibra óptica a una velocidad de 2.048 Mbps y **DS0** es medio de conducción de señales digitales a una velocidad de 64 Kbps. Además de la diferencia de velocidad en la conducción de señales entre **E1** y **DS0** la diferencia más importante entre uno y otro es que, el DS0 en la conexión final, entre la oficina del proveedor del servicio y el usuario, se lleva atraves de alambre de cobre. A veces no se requiere de un E1 o T1 completo, por lo que los proveedores de servicios ofrecen fracciones de un E1o T1 en múltiplos de 64 Kbps. Un canal de 64 Kbps es conocido comúnmente como un E0 (E cero) en el estándar E1, mientras que un canal de 64 Kbps en el estándar T1, es conocido como DS0.

2.3. Funcionalidades y aplicaciones

Muchos defensores de la PSTN descartan soluciones basadas en VoIP y softswitch pues se interrogan "¿Dónde están las 3.500 funcionalidades de 5ESS?" refiriéndose a los switches clase 5 ESS de Lucent Technologies, el cual se ha informado que tienen aproximadamente 3.500 funcionalidades para llamadas.

Es dudoso que cada una de esas 3.500 características sea necesaria para poder ofrecer un servicio competitivo de voz. Telcos, que requiere nuevas funcionalidades, debe negociar con el fabricante del switch (es Lucent Technologies que tiene el 90% del mercado de los switches clase 5 en Norteamérica) para obtener las nuevas funcionalidades que requiera. La obtención de esas nuevas funcionalidades requiere de no tan solo meses de trabajo sino de años de desarrollo y cientos de miles de dólares de inversión por parte del vendedor del switch que se contrató.

Los Softswitch se basan en estándares abiertos y utilizan a menudo softwares tales como Voice XML (VXML) para crear nuevas funcionalidades. Los proveedores de servicio que usan softswitch a menudo pueden crear sus propias funciones desde casa en cuestión de días.
Dado esta facilidad y economía de desarrollar nuevas características, la pregunta que surge ahora es ¿Por qué limitarte a las famosas 3.500 funcionalidades? ¿Por qué no 3.5000 o más?

Esta facilidad y flexibilidad en desplegar nuevas funcionalidades y servicios en el softswitch proporciona al proveedor de servicio la capacidad de implementar rápidamente dichas funcionalidades equivalentes a un alto margen de ingresos, con la ventaja de que ésta propiedad no la tienen los switches clase 4 o 5. Según cálculos vigentes, una solución basada en softswitch, dado su costo bajo de adquisición y operación junto con la capacidad de generar mayores ingresos, sobrepasa los ingresos generados por un switch clase 4 o 5.

3. Vo802.11: EL ALCANCE ES UNA CUESTIÓN DE INGENIERÍA

Una de las principales malas percepciones en cuanto a 802.11b y otros protocolos inalámbricos es que en cuanto a alcance, está limitado a 100m, lo que lo hace poco práctico como una solución de última milla (1 milla equivale a 1609 metros). La verdad es que con la ingeniería apropiada, 802.11b puede alcanzar más allá de 32Km (20 millas) de un punto a otro. La búsqueda de entrar a la "autopista" PSTN, es uno de los acontecimientos más apasionantes. Direccionando una antena en dirección a la casa del suscriptor, el proveedor de servicios puede entregar servicio banda ancha a un número de casas de casas sin los inconvenientes de PSTN como es canalizar un cable de cobre, romper una calle, o una batalla legal por servidumbre.

¿Cómo puede un proveedor de servicio cubrir un mercado residencial con access points que tienen un alcance máximo de 100m? Tal argumento demostraría un servicio que no sería económicamente viable debido al alcance limitado de la infraestructura 802.11. Si un servicio de Vo802.11 va a ser económicamente viable, su infraestructura debe tener access points (radios y antenas) que tengan un alcance mucho mayor que 100m. Tales productos están saliendo a la venta; de hecho, algunos ahora cubren varias millas cuadradas. Ingeniando una buena infraestructura para conseguir una cobertura mayor, más suscriptores podrían ser atendidos por cada access point, haciendo de esta forma cualquier servicio de Vo802.11 más viable económicamente además de provechoso.

Además, nuevos protocolos inalámbricos para LANs se alistan para la construcción de redes inalámbricas que puedan cubrir ciudades enteras. Redes ad hoc entre iguales incrementan el alcance de una red inalámbrica con un mínimo de inversión. Por otro lado, algunas soluciones de comunicaciones utilizan las líneas de conducción eléctrica para entregar Wi-Fi. Lo más importante en el diseño de una red inalámbrica de banda ancha es la inclusión de un nuevo protocolo, el 802.16, en la implementación de LANs inalámbricas para alimentar las redes 802.11b suburbanas. Otras tecnologías como redes mesh también amplían el alcance de las redes inalámbricas de banda ancha.

En la interconexión de datos, el éxito de 802.11 inexorablemente lo ha logrado conjuntamente con la ingeniería de RF. Mientras una red cableada requiere poco o ningún conocimiento de parte del instalador sobre como viajan datos vía cable Ethernet, las redes inalámbricas requiere un conocimiento fuerte de radios y antenas. Rf ha actuado como complemento de redes cableadas pues ha ayudado a ampliarlas. Se pueden usar componentes diferentes dependiendo de la frecuencia y la distancia que se requiers que lsd señales alcancen, pero todos los sistemas son fundamentalmente los mismos y se componen de un número relativamente pequeño de componentes.

Los tres componentes de RF de interés particular para los usuarios de 802.11 son las antenas, los receptores, los receptores sensores, y los amplificadores. A continuación se proporciona una descripción básica de los sistemas de transmisión inalámbricos, comenzando con las antenas que son de interés particular ya que estas son el rasgo más tangible de un sistema de RF.

3.1. Antenas

Las antenas son el componente más crítico de cualquier sistema RF porque ellas convierten las señales eléctricas que van por cables en ondas de radio y viceversa. El tamaño de la antena que se necesita depende de la frecuencia: entre más alta la frecuencia, más pequeña la antena. La antena más simple y más corta posible en cualquier frecuencia es la que corresponda a la mitad de la longitud de onda. Esta regla básica explica el enorme tamaño de antenas de emisión de radio y el pequeño tamaño de teléfonos móviles. Un estación AM difundiendo a 830kHz tiene una longitud de onda de aproximadamente 360m y tiene en consecuencia una antena de grandes proporciones, pero una interfaz de red 802.11b que funciona en la banda de 2.4 GHz tiene una longitud de onda de tan solo 12.5 cm. Con algunos trucos de ingeniería, una antena es incorporada en una tarjeta de un PC o en un portátil.

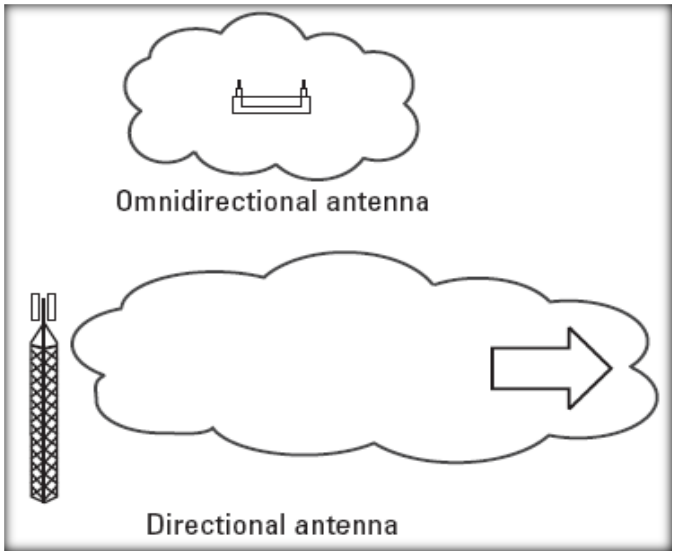


Figura 3. 1 Potencia radiada y alcance de antenas omnidireccionales y direccionales

Las antenas también pueden ser diseñadas con preferencia direccional. Muchas antenas son omnidireccionales, lo que quiere decir que ellas envían y reciben señales de cualquier dirección. Algunas aplicaciones pueden beneficiarse en cambio de antenas direccionales, las cuales irradian y reciben sobre una parte más estrecha del campo. La figura 3.1 compara el poder irradiado de antenas omnidireccionales y direccionales.

Para una cantidad dada de potencia de entrada, una antena direccional puede alcanzar señales claras a un radio más lejano. Esta antena también debe tener una sensibilidad mucho más alta para las señales de radio en la dirección dominante. Cuando se utilizan enlaces inalámbricos para sustituir redes cableadas, las antenas direccionales son usadas a menudo. Los operadores de redes telefónicas móviles también usan antenas direccionales cuando las células son subdivididas. Las redes 802.11 normalmente usan antenas omnidireccionales en ambos extremos de la conexión.

Una línea de transmisión (una especie de cable) entre la antena y el transceptor es también necesaria. Las líneas de transmisión por lo general tienen una impedancia de 50 ohmios. En

términos de antenas prácticas para dispositivos 802.11 en la banda de 2.4 GHz, la tarjeta inalámbrica típica para PC tiene un espacio donde viene incorporada dicha antena.

Todas las tarjetas inalámbricas tienen antenas incorporadas, pero estas antenas, si hablamos de algo en gran escala, son un tanto inadecuadas. Si se planificara cubrir una oficina o un área aún más grande, como un campus, casi seguramente se querrán usar antenas externas para los access points.

3.2. Factores que afectan el rango de alcance

Esto nos hace pensar que usted podría presentar una antena de alta ganancia y un amplificador y así cubrir una enorme cantidad de territorio, lo que economizaría access points y además se serviría a un número grande de usuarios inmediatamente. Esto, sin embargo, no es una idea buena realmente. Entre más grande sea el área a cubrir, más usuarios localizados estarán en aquella área, y por tanto, los access point deberán servir a más usuarios. 20 a 30 usuarios por access point es un límite superior bueno. Un solo access point para cubrir un territorio grande puede parecer una idea buena, y podría aún funcionar bien mientras que el número de usuarios permanezca pequeño.

Pero si una red es exitosa, el número de usuarios crecerá rápidamente, y la red pronto excederá la capacidad de los access point. Una vez que esto pasa, es necesario instalar más access points y dividir la célula original en varias más pequeñas y bajar la salida de potencia en todas las células.

3.2.1. Receptores sensibles

Además de las antenas, el elemento más crítico en un sistema Wi-Fi es el receptor. En especial, es importante buscar una buena sensibilidad del receptor. La sensibilidad de receptor es el nivel más bajo de señal que puede ser descifrado por el receptor. Entre más alta sea la sensibilidad, el alcance será más largo.

3.2.2. Amplificadores

Los amplificadores hacen las señales más amplias. La ganancia es medida en decibeles (dB). Los amplificadores pueden ser clasificados en tres categorías: bajo ruido, alta potencia, y otros. Los amplificadores de bajo ruido (LNAs) por lo general son conectados a una antena para aumentar la señal recibida a un nivel que sea reconocible por los equipos electrónicos a la cual el sistema RF está conectado. Los LNAs también son valorados con un factor de ruido, el cual es la medida de cuanta información extraña el amplificador introduce a la proporción de señal-a-ruido. Un factor de ruido más pequeño permite al receptor oír señales más pequeñas y así obtener un rango de mayor alcance.

Los amplificadores de alta potencia (HPAs) son usados para aumentar la potencia de una señal al máximo posible antes de la transmisión. La potencia de salida es medida en dBm, que es relacionada con vatios. Los amplificadores están sujetos a las leyes de la termodinámica: Ellos emiten calor además de amplificar la señal. El transmisor en una tarjeta de PC 802.11 es necesariamente de baja potencia porque tiene que consumirla de una batería instalada en un

portátil, pero es posible instalar un amplificador externo en access points alimentadores, que pueden estar conectados directamente a la red eléctrica donde la energía es más abundante. Aquí es donde las cosas pueden hacerse difíciles en lo que concierne al cumplimiento de las regulaciones.

Los dispositivos 802.11 están limitados a 1W de salida de poder y 4W de potencia eficaz irradiada (ERP o Effective Radiated Power). ERP multiplica la salida de potencia del transmisor por la ganancia de la antena menos la pérdida en la línea de transmisión. Con un amplificador de 1W, con una antena de 8 dB de ganancia, y 2 dB de pérdida de línea de transmisión, el resultado es una ERP de 4W; la ganancia total del sistema sería de 6 dB, que multiplican la potencia del transmisor por un factor de 4 ($4W = 10^{(6/10)}$).

3.2.3. La red 802.11b de 32 a 132 Kilómetros

Los enlaces punto-a-multipunto superiores a 450 metros con un equipo simple en el lado del cliente son muy posibles. Usando antenas de alta ganancia, receptores sensibles, y amplificadores si fuera necesario, es posible alcanzar velocidades Ethernet en enlaces punto-a-punto de ± 32 kilómetros (Figura 3.2). Un experimento demostró que es teóricamente posible conducir señales 802.11b a más de 32 Km, usando el equipo activo. De hecho, un enlace de 116 kilómetros de San Diego a San Clemente Island ha sido establecido por Hans Werner-Braun con un equipo 802.11 especializado sobre la banda de 2.4 GHz.

Figura 3. 2 El alcance de 802.11b excede los 32 kilómetros

En resumen, 802.11b, por sí mismo, no está limitado a un alcance de 100m. Su alcance máximo es más de 32 Kilómetros. Una comparación es con la central telefónica, donde el máximo alcance de la señal sobre el cable de cobre es 5.4 kilómetros sin un repetidor.

3.2.4. Arquitectura: La solución a redes extensas

Mientras una conexión 802.11b punto-a-punto tenga un alcance de 32 kilómetros, y una conexión punto-a-multipunto sea aún más corta, entonces sería bastante complicado que una red inalámbrica compita con la PSTN. Los temas que giran alrededor del compartimiento del ancho banda y la contención de frecuencia requieren de una estrategia multiescalonada para construir una red de área metropolitana inalámbrica (WMAN) capaz de sustituir la PSTN en una región dada.

El vencimiento de las limitaciones del rango de alcance puede ser logrado mediante una planificación arquitectónica apropiada de la red inalámbrica. Cuatro elementos de arquitectura de red

pueden ser empleados para ampliar el alcance máximo de 802.11b y sus protocolos inalámbricos asociados para cubrir un área entera metropolitana. Primero, un WMAN alimentada de un backbone IP de un ancho de banda alto, digamos, 100 Mbps. Este WMAN funcionaría a una frecuencia autorizada para asegurar una alta calidad de transmisión desprovista de interferencia.

Los suscriptores principales de una WMAN serían los (WISPs o wíreless Internet Service Providers). EL WMAN entonces alimentaría redes menores, las redes de área amplia inalámbricas (WWANs). Las WWANs podrían operar al ancho de banda 802.11 (54 Mbps) a una frecuencia en la banda de 5.8 GHz. Los suscriptores del WWAN incluirían empresas grandes y más pequeños WISPS. EL WWAN, a su turno, alimentaría las WLANS y las WLANs alimentarían residencias y pequeños negocios. Las redes de área personales inalámbricas (WPANs o Wíreless Personal Area Networks) se alimentarían de las WLANS para servir a componentes dentro de una residencia dada (Figura 3.3). Finalmente, una red ad hoc entre iguales, consistente en los dispositivos del suscriptor, access points inteligentes, y enrutadores inalámbricos podrían ampliar la red aún más con pocos costos y cambios en cuanto a infraestructura.

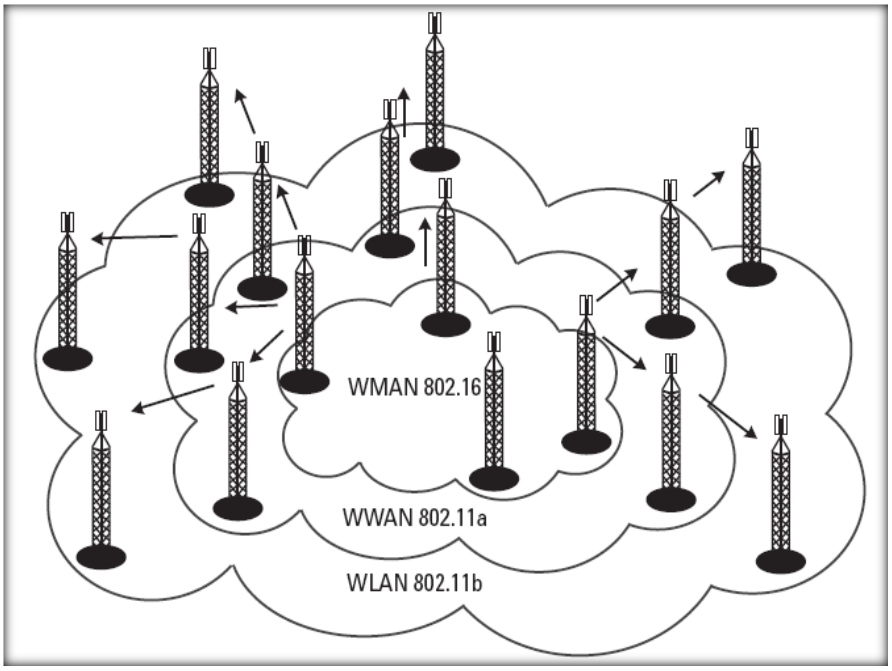


Figura 3. 3 Cubrimiento de un área metropolitana con WMANs, WWANs, WLANs y WPANs.

3.3. MANS

El WMAN abarca un rango de tecnologías de radio y tecnologías a base de láser con el fin de suministrar interacción inalámbrica entre redes a distancias de unos cientos de metros hasta varias millas. La banda ancha inalámbrica, el acceso a banda ancha inalámbrica (BWA, broadband wireless access), el lazo local inalámbrico (WLL, wireless local loop), radio fija y radio cable, todos se refieren a tecnologías para entregar servicios de telecomunicaciones en las últimas millas de la red. La banda ancha inalámbrica y BWA son términos generales que se refieren a sistemas de radio de alta

velocidad conectados a una red. WLL es sacado del término de telefonía local llamado lazo local, que se refiere a la conexión entre un conmutador o switch local telefónico y el suscriptor.

WLL y la radio fija generalmente se refieren a la entrega de servicios de voz y datos entre ubicaciones fijas a través de un medio inalámbrico de alta velocidad. Algunos mercados entrantes ofrecen aplicaciones móviles de esta tecnología. La radio fija incluye el servicio de distribución multipunto local (LMDS, local multipoint distribution service), el servicio de distribución multipunto multicanal (MMDS, multichannel multipoint distribution service), sistemas U-NII, y redes similares. El radio cable por lo general se refiere a sistemas MMDS usados para entregar señales de televisión tal como el servicio de Servicio Fijo de Televisión Educativa (ITFS, Instructional Televisión Fixed Service).

Dos topologías de red básicas son soportadas por estos sistemas. La más simple es un sistema punto-a-punto que proporciona una conexión inalámbrica de alta velocidad entre dos ubicaciones fijas. El ancho de banda no es compartido, pero los enlaces requieren línea de vista[3] entre las dos antenas. La segunda topología es una red punto-multipunto en la cual una señal es difundida sobre un área (llámese célula) y se comunica con las antenas de los suscriptores en la célula. Como el ancho de banda en la célula es limitado y compartido entre todos los usuarios, el funcionamiento puede ser una gran preocupación en células de alta densidad. Los sistemas de diferentes frecuencias pueden ser combinados para cubrir un área donde el terreno u otras obstrucciones obstaculicen la cobertura completa de éste.

Además de la frecuencia, la principal diferencia entre sistemas locales inalámbricos y celulares, WLAN, y las redes WPAN es la movilidad del equipo del suscriptor. Hubo alguna discusión sobre dar más movilidad al equipo del suscriptor en sistemas fijos inalámbricos. Esta movilidad permitiría a estos sistemas BWA funcionar potencialmente como redes celulares de cuarta generación (4G), entregando velocidades al suscriptor de varios megabits. Varias barreras técnicas, reguladoras, y comerciales deben ser vencidas antes de que esto pueda hacerse una realidad, sin embargo empresas tales como Wi-Fi ya han comenzado a examinar productos apuntados a este uso potencial.

3.3.1.802.16, Protocolo para WMANs: WIMAX

Un servicio inalámbrico con 802.16 proporciona un trayecto de comunicaciones entre el sitio de ubicación del suscriptor y una red principal (la red a la cual 802.16 le proporciona el acceso). Ejemplos de una red principal son la red pública telefónica y el Internet. Los estándares IEEE 802.16 están preocupados con la interfaz de aire entre el transceptor de un suscriptor y el transceptor base.

Los protocolos definidos expresamente para la transmisión inalámbrica se enfocan en asuntos relacionados con la transmisión de los bloques de datos a través de la red. Las normas o estándares están organizadas en una arquitectura de tres capas. La capa más baja, es decir, la capa física,

[3] LOS (Line of sight) o línea de vista: Se refiere a un camino (*path*) limpio, sin obstrucciones, entre las antenas transmisoras y receptoras. Para que exista la mejor propagación de las señales RF de alta frecuencia, es necesaria una línea de vista sólida. http://www.wni.com.mx/linea_vista.htmreceptoras. Para que exista la mejor propagación de las señales RF de alta frecuencia, es necesaria una línea de vista sólida. http://www.wni.com.mx/linea_vista.htm

especifica la banda de frecuencia, el esquema de modulación, técnicas de corrección de errores, sincronización entre el transmisor y el receptor, la velocidad de datos, y la estructura de TDM.

IEEE 802.16 aplica los usos "de la primera milla" de tecnología inalámbrica para unir edificios comerciales y edificaciones residenciales para redes principales de alta velocidad y además proporcionan el acceso a aquellas redes. El trabajo del grupo 802.16 ha apuntado principalmente a una topología de punto-a-multipunto con un despliegue celular de estaciones base, cada una enlazada a redes principales y en contacto con estaciones inalámbricas de suscriptor fijas.

Para la transmisión desde suscriptores hasta una estación base, el estándar usa la técnica DAMA-TDMA (*Demand Assignment Multiple Access–Time-Division Multiple Access).* DAMA es una técnica de asignación de capacidad a las estaciones que se adapta dependiendo de como sea necesario, para exigir cambios entre múltiples estaciones. TDMA es la técnica de división de tiempo en un canal en una secuencia de tramas, cada una consistente en un número de ranuras, y asignando una o varias ranuras por trama para formar un canal lógico.

Con DAMA-TDMA, la asignación de ranuras a canales varía dinámicamente. Para la transmisión de una estación base a suscriptores, el estándar especifica dos modo de operación, uno encaminado a manejar un flujo de transmisión continua (el modo A), tal como audio o vídeo, y uno encaminado a manejar un flujo de transmisión ráfaga (el modo B), tal como el tráfico basado en IP. Ambos son esquemas TDM.

3.3.2.Red de Puntos Consecutiva

En una WMAN, la confiabilidad de la red puede ser asegurada implementando una tecnología de red de puntos consecutiva (CPN, consecutive point network) (Figura 3.4).
Como un anillo de fibra SONET, el flujo de datos de la red alrededor del anillo inalámbrico invertiría el flujo en caso de una interrupción en la red. Esto asegura que sólo una parte limitada de la red esté down o sin servicio debido a una interrupción.

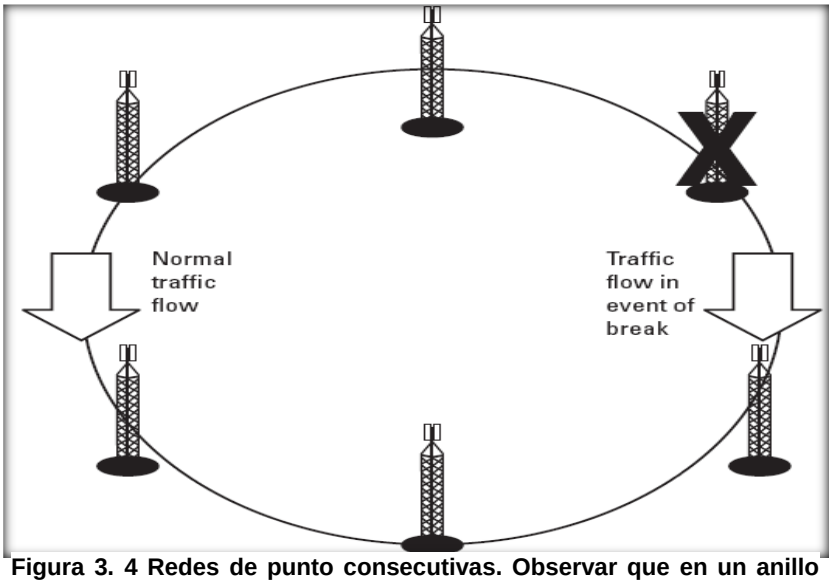


Figura 3. 4 Redes de punto consecutivas. Observar que en un anillo SONET, los flujos de datos se invierten ellos mismos si se da una interrupción o corte en la red.

3.4. Alcance extendido mediante redes Ad-hoc entre pares o peer-to-peer

Las tecnologías Ad-hoc peer-to-peer amplían el alcance máximo de redes Wi-Fi de distancias típicamente moderadas de unos cientos de pies a varias millas (Figura 3.5). El producto añade capacidades peer-to-peer multihopping a las tarjetas 802.11.

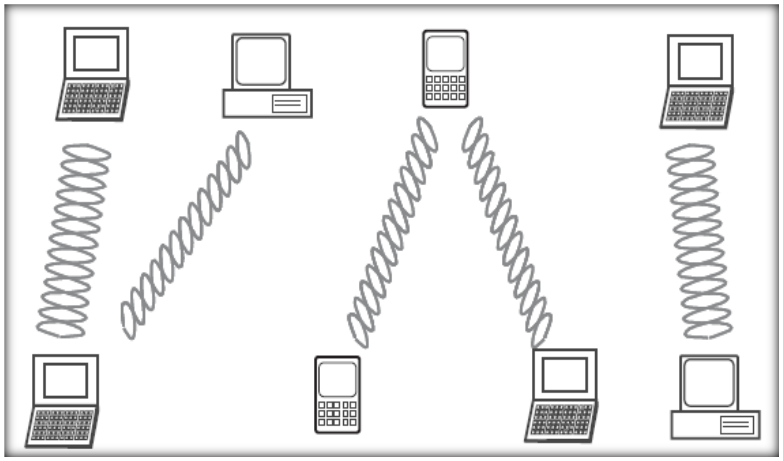


Figura 3. 5 Redes ad-hoc peer-to-peer

Se hace uso de software para convertir tarjetas LAN inalámbricas en enrutadores-repetidores. El resultado es un sistema que permite a los usuarios que están fuera de alcance de access points saltar por uno o varios usuarios cercanos hasta que se conecten a un access point. El software enruta también automáticamente las transmisiones de access points congestionados a otros que no lo estén. En general el funcionamiento de red es mejorado además del aumento dramático del alcance eficaz del enlace. Además, los usuarios dentro del alcance forman una red aunque sin conexión a una red más grande o la Internet.

3.4.1. Ventajas de Redes Ad hoc peer-to-peer.

Las redes ad hoc peer-to-peer ofrecen un gran número de excelentes ventajas para los nuevos mercados o redes municipalmente propias y administradas. Primero, los componentes permanentes, fijos tales como puntos de acceso y enrutadores inalámbricos son pequeños y discretos en relación con las torres de célula que encontramos en las arquitecturas de tercera generación (3G). Esto presenta la ventaja de menores costos de implementación tanto en términos de planta física como cuestiones legales.

Segundo, cuando suficientes dispositivos de suscriptores están presentes en un área dada, el alcance de la red es instantáneo y es económicamente aumentado. Esto, gracias a la utilización que cada suscriptor cuenta con un dispositivo individual como un enrutador o repetidor, así el proveedor de servicio se ahorra el costo de access points y enrutadores inalámbricos.

Además, esta red se establece entre dispositivos de suscriptor cuando no hay ningún IAP (Internet Access Provider) o enrutador inalámbrico en el área para conectarse a Internet o a otras redes.

En una arquitectura ad hoc móvil peer-to-peer, todos los nodos en la red, incluyendo los dispositivos del suscriptor, actúan como enrutadores y repetidores para otros suscriptores en la red. Esto permite a los usuarios saltar entre cualquier número de dispositivos en la red para alcanzar la conexión deseada. Esto aumenta la robustez de la red, reduciendo los gastos de un despliegue de infraestructura. Las redes Ad hoc peer-to-peer hacen fácil para dos personas compartir directamente archivos, correo electrónico, música, vídeo, o llamadas de voz. No es necesaria una infraestructura de red.

Por lo tanto, los usuarios pueden formar redes de voz y datos de alta velocidad en todas partes, en cualquier momento. En vez de operadores inalámbricos que costeen los dispositivos de usuario (handsets, por ejemplo), los usuarios en esta red en realidad costean sus propios equipos y ayudan a desplegar la red para el operador.

3.4.2. Componentes de una Red Ad hoc peer-to-peer

La red está comprendida por los siguientes elementos: dispositivos de suscriptor (incluyendo PDAs, ordenadores portátiles, teléfonos móviles, coches, etcétera), enrutadores) inalámbricos, y Access Points. Los dispositivos de suscriptor pueden ser móviles o fijos, mientras que los elementos restantes son fijos. Los enrutadores inalámbricos y access points pueden ser montados sobre postes, carteleras, edificios, o cualquier otra estructura conveniente. Es importante notar que el transceptor y la tecnología de módem dentro de un dispositivo de suscriptor son idénticos a la tecnología de transceptor en la infraestructura fija. Esto mantiene al suscriptor y los gastos de infraestructura excepcionalmente bajos.

4. SEGURIDAD Y VO802.11

A diferencia de sistemas cableados, los cuales físicamente pueden ser asegurados, las redes inalámbricas no están limitadas a interiores de edificios, y se puede acceder a ellas a 330 metros fuera de los locales con un ordenador portátil y una antena con determinada ganancia. Esto hace las WLANS intrínsecamente vulnerables a las intercepciones. Conociendo esto, el comité de 802.11 añadió una primera línea de defensa llamado WEP (Wíreless Equivalency Protocol) o Protocolo de Equivalencia Inalámbrico. WEP es un protocolo de cifrado que está diseñado para proporcionar el mismo nivel de seguridad que las redes cableadas suministran. El estándar proporciona cifrado tanto de 40bits como 128 bits (realmente sólo 104 bit) en la capa de enlace usando el algoritmo RC4.

Ahora discutiremos la seguridad correspondiente a 802.11 y los problemas sabidos que se han generado. Cuando IEEE 802.11b primero fue definido, la seguridad dependió de dos mecanismos de seguridad básicos: (1) SSID (y 2) WEP. Algunos fabricantes añadieron la filtración de dirección MAC a sus productos.

4.1. Riesgos de seguridad

La seguridad puede ser definida como el impedimento que se le impone a alguien de hacer cosas que usted no quiere que ellos hagan con, sobre, o en sus datos, ordenadores, o dispositivos periféricos. Los riesgos de Seguridad pueden venir de hackers, intrusos criminales, asaltantes corporativos, personas enteradas, contratistas, y empleados disgustados. Los hackers son aficionados típicamente jóvenes. "Script Kiddiez"[4] copian ataques muy bien conocidos de la Internet y los controla. Los hackers más sofisticados entienden los protocolos subyacentes y sus debilidades. Los intrusos criminales pueden estar tras el acceso a los números de tarjetas de crédito y cuentas corrientes. Los asaltantes corporativos están tras la información financiera, planes de negocio, y la propiedad intelectual.

4.2. Modelo de Seguridad de WLAN

Hay cuatro clases principales de ataque a un sistema por intrusos: interceptación, fabricación, modificación, e interrupción .Una quinta clase de ataques – Rechazo- es un ataque contra la responsabilidad de la información. Esto es un ataque desde dentro el sistema por la entidad fuente o por la entidad destino. Cada una de estas clases de ataque puede ser controlado con un mecanismo de seguridad (Ver Tabla 4.1). Juntos, los mecanismos de seguridad forman un cryptosistema

Ataque	Objetivo	Resuelto mediante
Interceptación	Confidencialidad y Privacidad	Encriptación/Decriptación
Fabricación	Autenticidad	Autenticación
Modificación	Integridad	

[4] Es un cracker inexperto que usa programas, scripts, exploits, troyanos, nukes, etc. creados por terceros para romper la seguridad de un sistema. Suele presumir de ser un hacker o cracker cuando en realidad no posee un grado relevante de conocimientos.

Replay	Integridad	
Reacción	Integridad	
Interrupción	Disponibilidad	
Rechazo	No rechazo	

Tabla 4. 1 Clases principales de Ataques de Seguridad

4.2.1. Interceptación

La interceptación es un ataque pasivo sobre la confidencialidad en la cual una entidad intrusa es capaz de leer la información que es enviada de la entidad fuente a la entidad destino. El Sniffing es un ejemplo de un ataque de interceptación.

El intruso intenta aprender o hacer uso de la información del sistema, pero no afecta los recursos de sistema. La identidad de la entidad fuente puede ser interceptada y más tarde usada en un ataque de mascarada,[5] o el intruso puede estar interesado en el contenido de mensaje de liberación como la información de autenticación, contraseñas, números de la tarjeta de crédito, propiedad intelectual, u otra información confidencial. El intruso también puede estar interesado en el análisis de tráfico del sistema para sacar o deducir la información de las características del tráfico. Algunos ejemplos de Interceptación son *Eavesdropping y Sniffing.*

4.2.2. Fabricación

La fabricación es un ataque activo a la autenticación donde el intruso pretende ser la entidad fuente. Los paquetes y los correos electrónicos imitados o falsos son ejemplos de un ataque de fabricación. Algunos ejemplos de Fabricación son *Ataques Man-in-the Middle, Spoofing, Ataques de Inserción, Ataques por fuerza bruta, Invasión y Robo de recursos.*

4.2.3. Modificación

La modificación es un ataque activo sobre la integridad en la cual una entidad intrusa cambia la información que es enviada de la entidad fuente a la entidad destino. La inserción de un programa Troyano o virus es un ejemplo de un ataque de modificación. Unos ejemplos de ataques de modificación son *Pérdida de equipos e Infección por Virus.*

4.2.4. Repetición (Replay)

Replay es un ataque activo sobre la integridad en cual un tercero o mejor dicho intruso, reenvía la información que es enviada de la entidad fuente a la entidad de destino.

[5] El ataque denominado de *masquerading* o mascarada consiste simplemente en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno; esta suplantación puede realizarse electrónicamente - un usuario utiliza para acceder a una máquina un *login* y *password* que no le pertenecen - o en persona. El *masquerading* es más habitual en entornos donde existen controles de acceso físico, y donde un intruso puede `engañar' al dispositivo - o persona - que realiza el control, por ejemplo con una tarjeta de identificación robada que un lector acepta o con un carné falsificado que un guardia de seguridad da por bueno.

Si estudiamos el método WEP encontramos que la idea de éste es proporcionar a las redes inalámbricas la "privacidad de un cable". El algoritmo WEP se basa en el RC4 y utiliza una clave que deben conocer tanto los clientes como los puntos de acceso (habitualmente se utiliza más de una clave), junto con un vector de iniciación (IV) generado de forma pseudoaleatoria para realizar la encriptación de los datos. Una vez cifrado el texto, además de éste hay que enviar el IV y el checksum, este último independiente de la clave. Para dificultar los ataques al protocolo, el IV se cambia periódicamente. Pero como Como WEP envía los IV sin cifrar junto con el mensaje cifrado, es posible usar métodos estadísticos y otros métodos para crackear la clave WEP. Tanto las implementaciones de 64-bits como las de 128bits tienen el mismo defecto

Es aquí donde la seguridad se ve afectada pues 802.11 básico no tiene ninguna protección contra Replay ya que no contiene números de secuencia o sellos de tiempo. Como los IVs y las claves pueden ser reutilizados, es posible volver a repetir mensajes almacenados con los mismos IV sin se detectados para insertar mensajes falsos en el sistema. Los paquetes individuales deben ser autenticados, no solamente cifrados. Los paquetes deben tener números de secuencia o sellos de tiempo. Un ejemplo de Replay es *Redirección de Tráfico, Reacción e Interrupción.*

4.2.4.1. Reacción

La reacción es un ataque activo donde los paquetes son enviados por el intruso al destino. La reacción es supervisada por el intruso. La información adicional puede ser aprendida desde este nuevo lado del canal.

4.2.4.2. Interrupción

Interrupción es un ataque activo sobre la disponibilidad de la información pues una entidad intrusa bloquea la información enviada de la entidad fuente a la entidad de destino. Ejemplos de esto son ataques de denegación-de-servicios (DoS) e inundaciones de red.

4.2.5.Rechazo

Un ataque de rechazo es un ataque activo al no rechazo ya sea a la fuente o al destino en el cual cualquier entidad fuente se niega enviar un mensaje, o la entidad de destino se niega recibirlo. La seguridad 802.11 no protege el no rechazo. Sin el no rechazo, la entidad fuente puede negar el envío de mensajes y la entidad destino puede negar recibir mensajes.

4.3. MOVILIDAD Y SEGURIDAD

Si se desea poner en práctica la solución de movilidad, ésta debe ser segura durante los handoff[6]. Los Handoffs exponen la red a ataques de redirección. Si la red no es correctamente asegurada, el intruso puede asumir la comunicación con la entidad destino después del handoff.

[6] El handoff es el proceso de pasar una llamada de un canal de voz en una celda a un nuevo canal en otra celda o en la misma, a medida que el usuario se mueve a través de la red. El manejo de estas transiciones es un factor vital para garantizar la continuidad de las comunicaciones tanto de voz como de imágenes y datos, caso en el que es muy crítica la pérdida de información. http://www.monografias.com/trabajos3/pcscolombia/pcscolombia.shtml

4.3.1. Seguridad: Un rango de opciones

Para construir un sistema de seguridad, es indispensable tener claro dos necesidades. La primera necesidad es saber que está siendo protegido. Estos podrían ser dispositivos como servidores, enrutadores, y modems e información como el correo electrónico, propiedad intelectual, secretos de fabricación, listas de clientes, planes de negocio, y expedientes médicos. A veces, la información tiene que ser protegida por ley.

Otra de las necesidades es tener una idea de: ¿de quién este material está siendo protegido? Pueden ser hackers, clientes, personas enteradas (empleados y contratistas), competidores. A partir de ésto puede hacer un análisis simple de riesgos para determinar que está riesgo – datos o la red - y el nivel de contramedidas requeridas para solucionar el problema. En la gestión de riesgos uno no puede ignorar, aceptar, defender, o dejar pasar un problema. Lamentablemente, no hay ninguna política de seguridad estándar que se pueda obtener y hacer uso de ella. Cada negocio tiene sus propias exigencias y determinará que solución implementará. La tabla 4.2 muestra los diferentes niveles de seguridad, la configuración, lo que es asegurado por la configuración, y en lo que usos tal configuración podría ser usada.

		Configuración	Entidad Asegurada	Aplicaciones
0	Sin Seguridad	Red Lista para usar; no configuración; no Wep.	Ninguna	¿?
1	Acceso Público	Autenticación de Usuario; el usuario debe tener una VPN a través de Internet con la empresa.	Acceso a la Red	Hot Spots, Bibliotecas, coffee shops, hoteles, aeropuertos, y otros que ofrezcan movilidad
2	Seguridad Limitada	WEP de 40 o 128 bits; Lista para control de Acceso por MAC; no hay broadcast	Acceso a alguna red; privacidad en algunos datos	Hogares y SOHO[7] con movilidad
3	Seguridad Básica	Acceso Wi-Fi protegido; Luego 802.11i	Acceso a la red y privacidad de datos	Hogares, SOHO, y pequeñas empresas con movilidad
4	Seguridad Avanzada	802.1x/EAP-x, RADIUS	Acceso a la red y privacidad de datos	Empresas con movilidad
5	Seguridad de Terminal a Terminal	VPNs tales como PPTP, PPTPv2, L2TP. Kerberos e IPSEC.	Acceso a la red y privacidad de datos	Aplicaciones especiales, ejecutivos viajeros, telecommuting[8], y más; empresas con usuarios externos.

Tabla 4. 2 Rango de opciones de seguridad para redes inalámbricas

[7] Se suele hablar de entornos SoHo para referirse a entornos domésticos o de pequeña empresa, en los que se puedan necesitar equipos de una potencia relativamente baja (Small Office - Home Office). usuarios.lycos.es/Resve/diccioninform.htm

[8] Trabajo a Distancia. Tanto para las empresas grandes como las pequeñas, mover a parte de su fuerza laboral a oficinas en casa para todo o parte del tiempo de trabajo a la semana puede significar la reducción de costos por menor espacio en edificios del requerido para las operaciones regulares

4.4. Medidas de Seguridad de 802.11 más allá de WEP

4.4.1. Acceso Protegido a Wi-Fi

En noviembre de 2002, la Alianza Wi-Fi anunció el estándar de seguridad de Acceso Protegido a Wi-Fi (WPA). Esto reemplazó el estándar débil WEP antes ofrecido para los equipo Wi-Fi.

WPA usa el Protocolo de Integridad Temporal Clave (TKIP, temporal Key Integrity Protocol), un esquema de cifrado más implacable que el usado en WEP. TKIP usa la clave hashing (KeyMix) y una comprobación de integridad de mensaje no lineal (MIC, message integrity check). TKIP también usa una nuevo protocolo rápido de reasignación de clave (ReKey) que cambia la llave de cifrado cada 10,000 paquetes. Sin embargo, TKIP no elimina defectos fundamentales en la seguridad Wi-Fi. Si uno puede hackear TKIP, no solo se rompería la confidencialidad, sino que también se tendría control al acceso y la autenticación.
WPA trabajará de dos modos diferentes, dependiendo del tipo de red. En casas y pequeñas oficinas que carecen de servidores de autenticación, la tecnología trabajará en un modo llamado clave "precompartida". Los usuarios simplemente entran en la clave de red para ganar el acceso.

En el modo administrado, WPA trabajará con servidores de autenticación y requerirá el apoyo de 802.1x y EAP. La combinación 802.1x/EAP permite a un adaptador de red de cliente negociar vía un Acess Point con un servidor de autenticación usando transmisiones cifradas para cambiar las claves de sesión.

Otrss medidas de seguridad se pueden tomar con 802.1x, EAP y RADIUS..

4.4.1.1. RADIUS

El RADIUS es de hecho el estándar para la autenticación remota. Este es un protocolo extensamente desplegado para acceso a la red, autenticación, autorización, y contabilidad (AAA, authentication, authorization, and accounting) tanto en sistemas nuevos como en los tradicionales. Aunque este tiene pocos temas de seguridad y transporte asociadas con el, es muy probable que el RADIUS seguirá siendo extensamente usado en los años que están por venir. Tarde o temprano, RADIUS será reemplazado por un nuevo protocolo llamado DIÁMETER. RADIUS es simple, eficiente, y fácil de poner en práctica lo que hace posible implementarlo también en dispositivos integrados más económicos.

5 INTERFERENCIA Y QoS EN UNA RED Vo802.11

Si las redes Vo802.11 desean superar a la red PSTN, deben entregar al suscriptor una experiencia en lo referente a servicios de voz igual o mejor que la que ofrece PSTN. Las compañías de telecomunicaciones más reconocidas brindan con orgullo servicios de voz de una gran calidad mediante sus redes tradicionales que son relativamente confiables.

La preocupación que la mayoría de la gente tiene con el reemplazo del cobre y cables de fibra óptica de la PSTN por las ondas electromagnéticas de 802.11 es que, dichas ondas, dado que no son controlables o predecibles como el cobre y la fibra óptica, entreguen un QoS inferior al deseado o que sean susceptibles a interferencias debido a otros emisores del espectro electromagnético.

La voz es un medio exigente que se entrega mediante paquetes conmutados en la red por tanto la QoS en redes VoIP inalámbricas se convierte en un tema de discusión interminable. Los administradores de redes se esfuerzan en reducir los milisegundos que toma entregar los paquetes de voz en las redes IP. Dada la importancia y el énfasis de la QoS en redes cableadas, el principal inconveniente con las redes Vo802.11 es que ésta no pueda suministrar el QoS necesario para adquirir una buena calidad de voz, sin embargo este problema puede solucionarse con una buena ingeniería que pueda lograr los objetivos: entregar una calidad de voz igual o mejor que la PSTN.

¿Qué factor atraerá a los clientes empresariales y residenciales para que renuncie al servicio de PSTN tradicional que han venido usando y prueben el de Vo802.11? La principal atracción puede ser que ofrece un considerable mayor ancho de banda (11Mbps vs. 56Kbps) el cual permite entregar servicios de datos que con la PSTN no podía tener como son video en tiempo real, video por demanda, videoconferencia, compartimiento de archivos y servicios telefónicos de local y larga distancia; y además que tendría una mejor relación costos/beneficios que tener servicios de telefonía, TV Cable y acceso a internet por separado.

Quizá el principal inconveniente a Vo802.11 es la percepción que se tiene de que la señal sufrirá interferencias por parte de fuentes externas a la red, como controles para la operación de puertas de garajes, hornos microondas, teléfonos inalámbricos, y muchos más.

Otro inconveniente común que va más allá de fuentes externas es que el suscriptor deba tener una línea de vista directa desde el transmisor del proveedor de servicios. Este anterior obstáculo influye en el primero, el cual es el referente al QoS. Sin embargo hay que tener en cuenta que la transmisión de paquetes IP a través de cable tiene su propia serie de retos así como interferencias.

Como se muestra en la Figura 5.1, QoS debe ser equitativo en toda la red, es decir, debe acoger toda la red tanto la parte cableada como las partes inalámbricas.

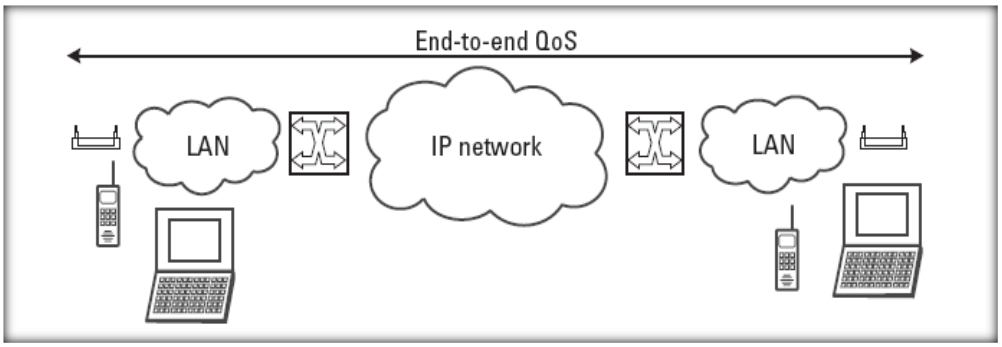


Figura 5. 1 El QoS está presente entre terminal y terminal, tanto en la parte cableada como la inalámbrica de la red.

5.1 Interferencia

Lo que la mayoría de la gente realmente piensa cuando nos referimos al QoS en redes inalámbricas es en la interferencia que puede existir por parte de otras fuentes de transmisión. Un inconveniente inmediato visible es la abundancia de aplicaciones inalámbricas en la vida diaria, como son los controles de operación de puerta de garajes, hornos microondas y teléfonos inalámbricos. La verdad es que muchas de estas aplicaciones hogareñas no operan en la misma frecuencia que 802.11, además que la potencia de sus emisiones es muy baja o distante como para interferir con el tráfico 802.11.

Otra variedad de dispositivos (escáneres de códigos de barras, iluminación industrial, calentadores industriales y hornos microondas) usan las mismas frecuencias pero a causa de que estas LANs (y otros dispositivos en la banda ISM) operan con niveles de potencia bastante bajos, el riesgo de interferencia es relativamente nulo, pero aún así existe. Claro que con la acogida que han tenido estas WLAN, estas situaciones deben solucionarse o al menos mejorarse.

5.1.1 Fuentes Externas de Interferencia

Las interferencias pueden ser categorizadad según la fuente de origen en externas e internas. Las fuentes externas son las que no están relacionadas con la red 802.11 misma, como teléfonos inalámbricos, monitores de bebés, y otros. Y las fuentes internas pertenecen a la red 802.11

5.1.1.1 Rectificación de los mitos de la interferencia externa

Los controles para operar la puerta de los garajes se han asumido como una fuente de interferencia para las LAN's 802.11 sin ser cierto, por tanto podemos decir que es un mito (Ver Tabla 5.1).

Un control para la operación de puertas de garaje opera en la banda de 286 a 390 MHz, por tanto ellos no interfieren con 802.11.

Los teléfonos inalámbricos de 900MHz operan en la banda ISM de los 802 a 829 MHz y por tanto tampoco interfieren con 802.11. Sin embargo, los teléfonos inalámbricos de 2.4 GHz operan en la misma banda que 802.11 y si pueden causar interferencia.

Entonces, ¿Cómo se manejan las interferencias? Los Access Point inalámbricos 802.11 tienen licencia para operar bajo clase B, en la banda ISM 2.4GHz.

Fuente de Interferencia	Factor que la descarta como fuente o solución a la interferencia
Dispositivo para apertura de puerta de Garaje	Frecuencia equivocada
Horno Microondas	Los microondas industriales pueden interferir con una WLAN debido a la que la potencia que maneja es suficiente para lograrlo pero los hornos residenciales no tienen la potencia suficiente para interferir.
Teléfono Inalámbrico	Muy baja potencia como para producir interferencia más allá de la oficina o residencia donde se encuentre. Si el teléfono inalámbrico del suscriptor está interfiriendo con su propia red WLAN, debe reemplazar el teléfono de 2.4GHz por uno que trabjae a 900MHz. Además, por qué una residencia con teléfono celular y servicio VoIP 802.11 aún utilizaría un teléfono inalámbrico PSTN? Es insensato.

Tabla 5. 1 Fuentes Externas Potenciales de Interferencia para redes Vo802.11

Las regulaciones establecen que cualquier dispositivo licenciado no debe interferir con otro ni interrumpir la operación de otros dispositivos licenciados que estén en el mismo espectro. Es decir, los dispositivos sin la licencia son los de menor prioridad, luego, los servicios licenciados del gobierno federal y los dispositivos licenciados (únicamente dispositivos de transmisión) para servicios tales como telemetría, radiolocación y calentamiento e iluminación con RF, y por último la parte 97 (amateur radio). Hay que tener en cuenta que si dispositivos se encuentran sin licencia y además están bajo las condiciones equivocadas, muy posiblemente interferirán con la red tales como los teléfonos inalámbricos de 2.4GHz, aplicaciones Bluetooth, hornos microondas y monitores de bebé de 2.4GHz.

5.1.1.2 Pautas para minimizar las interferencias externas en WLANs

Cinco son los parámetros que los planificadores o diseñadores de la red deben tener totalmente controlados para poder minimizar las interferencias por fuentes externas:

- El canal/banda que se esté usando.
- La distancia hasta la fuente de interferencia (entre más larga, mejor)
- Los niveles de potencia de la interferencia (entre más baja, mejor)
- El ancho del lóbulo la antena.
- El protocolo usado.

5.1.1.2.1 Cambio de canales

Algunas veces lo más fácil de hacer para evitar la interferencia es cambiarse a un canal menos concurrido o usado. Las especificaciones para 802.11a y 802.11 estipulan varios canales y frecuencias. Si una interferencia es encontrada a una frecuencia dada, entonces sería bueno optar por cambiarse a una canal que no tenga este problema. La especificación 802.11b proporciona 11

canales traslapados para Norte América (Ver Tabla 5.2), cada canal tiene un ancho de 22MHz y es centrado en intervalos de 5MHz comenzando en 2.412 GHz y terminando en 2.462 GHz). Esto quiere decir que solo hay tres canales que no se traslapan (1,6 y 11).

Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Tabla 5. 2 Los 11 canales traslapados de 802.11b

La especificación 802.11a proporciona 12 canales, cada uno con 20 MHz de ancho de banda y centrado en intervalos de 20 MHz (comenzando en 5.180GHz y terminando en 5.320 GHz para las bandas UNII inferior e intermedia, y comenzando en 5.745 GHz y terminando en 5.805GHZ para la banda UNII superior). Es importante notar que estos canales no se traslapan.

La mejora de este problema yace en el despliegue de los estándares 802.11a y 802.11g. La banda de UNII 5GHz es la más lejos de estar congestionada, y WIFi tiene la mayor cantidad del espectro aquí. Son permitidos más canales, y los estándares trabajan con protocolos que permiten que múltiples Access Points negocien entre ellos mismos por la asignación de las frecuencias.

El estándar 802.11g usa OFDM en 2.4GHz, la cual es la banda menos susceptible a interferencias y tiene más canales disponibles. Sin embargo, la velocidad de operaciones de 802.11g y 802.11a es adecuada para grandes escenarios.

Una vez una fuente de interferencia ha sido definida, una práctica común entre WISPs (Wireless Internet Service Provider) es negociar entre ellos (los WISPs) quiénes transmitirán y en cual frecuencia van a hacerlo. Si tal arreglo no puede ser totalmente concretado, hay múltiples canales a los que se puede cambiar con tal de evitar las interferencias.

5.1.1.2.2 Distancia a la fuente interferente

En el cálculo de un enlace, la entrega de una señal inteligible es una función tanto de la potencia de la señal como de la distancia entre el transmisor y el receptor. Una señal que esté en la misma

frecuencia que una WLAN 802.11, por ejemplo, no interferirá si la fuente de origen de esa interferencia está distante. Esto es debido a que la señal interferente se vuelve muy débil como para representar algún tipo de interferencia para la WLAN.
Por otro lado, si la distancia entre el AP y el dispositivo suscriptor es mayor que la recomendada, la señal deseada se atenúa a través de la distancia y se vuelve muy susceptible a interferencias ya que la señal interferente puede tener mayor potencia que ésta.

Cuando 802.11 es usado como una solución de última milla en la distribución de servicios a residencias o pequeñas empresas, las fuentes potenciales de interferencia deben ser consideradas.

Si fuentes de interferencia (teléfonos inalámbricos u hornos microondas) pueden ser eliminados dentro de la residencia o la pequeña empresa, es una buena opción, sien embargo habría entonces que colocar inmediata atención a las posibles fuentes externas de interferencia que puedan existir.

La capacidad de estas fuentes de interferencia es limitada por la distancia a la red del suscriptor y el nivel de potencia de esa interferencia. Los electrodomésticos como hornos microondas y teléfonos inalámbricos generan una potencia muy pequeña como para producir interferencia más allá de la edificación en donde estén localizados, a menos que el dispositivo sea defectuoso.

5.1.1.2.3 Niveles de potencia

Los niveles de potencia de la señal primaria y la interferente deben ser registrados. Si el nivel de potencia de la señal interferente es cercano al nivel de potencia de la señal primaria de la WLAN 802.11 u otra señal WLAN, entonces definitivamente habrá interferencia. Lo importante aquí es que el proveedor de servicio no debe interferir con otros operadores que estén en el mismo espectro.
La otra solución es que el nivel de potencia de la señal interferente se reduzca. Sin embargo, es importante entender que si se incrementa la potencia de la señal primaria se podría causar interferencia a usuarios de la misma banda, y además hay que tener en cuenta limitaciones en la potencia de salida las cuales están publicadas en las regulaciones correspondientes.

5.1.1.2.4 Ancho del lóbulo de la Antena

Otra forma de eliminar la interferencia es teniendo sumo cuidado con el uso de las antenas. Un lóbulo estrecho puede incrementar efectivamente la potencia hacia el receptor y también incrementar la fuerza de la señal que va a ser recibida. Otra cosa que debe tenerse en cuenta es el QoS, por tanto debe utilizarse antenas con alta tecnología.

En cuanto a cómo debe dirigirse la antena, debe tenerse en cuenta que con esto se debe lograr: mejorar el SNR, que depende de la forma del lóbulo, reducir la interferencia hasta el canal de reuso y atenuar la interferencia en ambientes donde pueda existir multipath[9]. Muchas de estas tecnologías usan MIMO (Múltiple-in, multiple-out).

[9] El efecto multipath o multitrayecto es causado principalmente por múltiples reflexiones de la señal emitida en superficies cercanas al receptor. Estas señales reflejadas (en edificios, vehículos, árboles, etc.), que se superponen a la señal directa son siempre más largas, ya que tienen un tiempo de propagación más largo y pueden distorsionar significativamente la amplitud y forma de la onda. http://www.isa.cie.uva.es/gps/GPSerrores.html

Vivato, basado en San Francisco está comercializando su WiFi de una manera nunca vista. Los switches de WiFi entregan la potencia de la red conmutando con radio antenas phased-array[10]. Estos switch Wi-Fi usan radio antenas phased-array para crear lóbulos altamente dirigidos en las transmisiones WIFi. Los lóbulos WiFi son creados mediante la tecnología Packet Steering.

A diferencia de la difusión que se da en las actuales LAN inalámbricas, la transmisión conmutada de Vivato es enfocada en un patrón totalmente controlado y dirigido exactamente al dispositivo del cliente deseado.

Estos lóbulos estrechos en WiFi habilitan transmisiones simultáneas para diferentes dispositivos en diferentes direcciones, lo cual permite operaciones paralelas a muchos usuarios, lo cual es la esencia del WiFi switching. Estos lóbulos estrechos también reducen la interferencia entre canales, porque se activan únicamente cuando se necesitan.

5.1.1.2.5 Protocolo

Mediante 802.11g en vez de 802.11b, puede tomarse ventaja de OFDM, el cual es menos susceptible a las interferencias y al multipath.

5.1.1.2.6 Otras opciones para el control de la interferencia externa

Otras medidas que pueden tomarse para controlar la interferencia externa, son las siguientes:

(1) Controlar el ambiente o entorno ya que la interferencia ya está limitada en parte por el control que tienen los dispositivos usados.

(**2)**. Escoger la banda correcta para cada aplicación Un ISP de Wireless puede considerar usar 802.11a así su WLAN no interfiere con alguna posible WLAN.

5.1.2 Fuentes internas de interferencia

Dentro de una red inalámbrica existen muchos retos en cuanto a interferencia y la naturaleza de las transmisiones. Las fuentes internas de interferencia incluyen multipath y ruido en el canal.

5.1.2.1 Multipath y Fade Margin

La interferencia por multipath ocurre cuando las ondas emitidas por el transmisor viajan a través de diferentes trayectos e interfieren destructivamente con las ondas que viajan en trayectoria de línea en vista directa. (Ver Figura 5.2)

[10] También llamada sistemas en fase. Este tipo de antena permite orientar el haz del radar sin desplazar mecánicamente la antena.

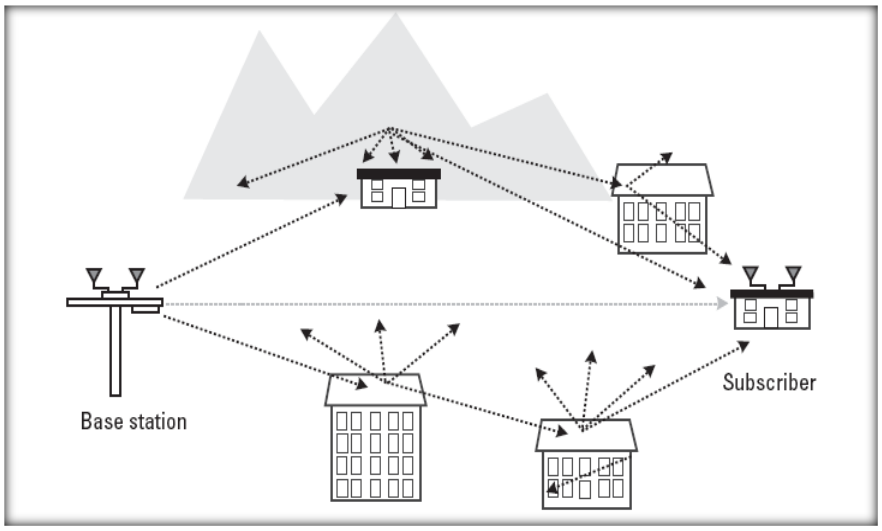


Figura 5. 2 Interferencia por multipath

Esto muchas veces es referido como un signal fading, o atenuación de la señal. Este fenómeno ocurre porque las ondas viajan por diferentes trayectorias lo que causa un desfase al momento de alcanzar la antena, lo que implica la cancelación entre ellas mismas.

Un método para superar este problema es transmitir las señales con más energía. En un ambiente indoor, las multipath están siempre presentes y tienden a ser dinámicas (Varían constantemente). Muchas atenuaciones se producen por multipath, a más de 30 dB. Por esto es esencial tener un margen adecuado en el enlace para eliminar éstas pérdidas cuando se esté diseñando la red inalámbrica.

La cantidad extra de RF radiado para soportar este fenómeno es referido como fade margin o margen de atenuación. La cantidad exacta que el fade margin requiere depende de la confiabilidad deseada en el enlace, pero debe tenerse en cuenta una buena regla para los protocolos 802.11 y es que esté en un rango de 15 a 20 dB para lograr una confiabilidad del 95%.

Un método para disminuir los efectos de multipath es implementando diversas antenas. Como la cancelación de las ondas de radio depende de la geometría, puede hacerse uso de dos o más antenas separadas por al menos media longitud de onda para mitigar este problema.

Cuando se adquiere la señal, el receptor verifica cada antena y simplemente detecta la antena que tenga la señal de mejor calidad. Este método reduce pero no elimina el problema, y el fade margin requerido en el enlace podría ser necesitado por un sistema que no usa diversidad de antenas.
El inconveniente es que esta propuesta requiere más antenas y un diseño más complicado para la parte de recepción.

Otro método para evitar el multipath es usando un ecualizador adaptativo de canal. La ecualización adaptativa puede implementarse con o sin diversidad de antenas. Después de que la señal es recibida y digitalizada, es aprovisionada por una serie de fases retardantes, que son totalizadas mediante ciclos de retroalimentación.

Esta técnica es particularmente efectiva en ambientes lentamente cambiantes tal como transmisiones sobre líneas telefónicas, pero es más difícil de implementar en entornos que cambian rápidamente como en pisos de fábricas, oficinas y hogares donde los transmisores y los receptores se mueven uno con respecto al otro. El principal inconveniente es el impacto en la complejidad y costos del sistema. Los ecualizadores adaptativos pueden ser costosos de implementar para enlaces de datos en banda ancha.

Los sistemas con el espectro expandido son bastante robustos ante la presencia de multipath. Los sistemas basados en DSSS rechazan las señales reflejadas que están significativamente retardadas con relación al trayecto directo que deben seguir o con relación a una señal más fuerte. Esta propiedad de espectro expandido es la que permite que múltiples usuarios compartan el mismo ancho de banda en sistemas CDMA. Sin embargo, DSSS de 802.11 no presenta suficiente ganancia en procesamiento y OFDM si.

FHSS[11] también exhibe algunos grados de inmunidad a multipath. Debido a que el transmisor FHSS está continuamente cambiando de frecuencia, el siempre elige algunas frecuencias que tengan poca o ninguna pérdida por multipath. En ambientes atenuados de forma severa, la tasa de transferencia de un sistema FHSS es reducida, es poco probable que el enlace se pierda completamente. En sistemas OFDM tales como 802.11 y 802.11g se transmiten en múltiples subcarriers en diferentes frecuencias al mismo tiempo. El efecto multipath está limitado en su mayoría de la misma manera que está limitado un sistema FHSS. Además, OFDM especifica una tasa de símbolos más lenta para reducir cualquier de que una señal invada la señal siguiente, minimizando así la interferencia por multipath.

5.1.2.2 Ruido del canal

Cuando se evalúa un enlace inalámbrico, hay tres preguntas que deben responderse:
1. ¿Cuánta potencia RF está disponible?
2. ¿Cuánto ancho de banda está disponible?
3. ¿Cuál es la confiabilidad requerida definida mediante bit error rate (BER)?

En general, la potencia RF y el ancho de banda son efectivamente la parte esencial en la capacidad de comunicación del enlace. El límite superior en términos de velocidad de datos está dado por el teorema de capacidad del canal de Shannon:

$$C = B \times \log 2(1 + S/N)$$

Donde:
C = capacidad del canal (bps);
B = ancho de banda (Hz);
S = fuerza de la señal (W);
N = ruido de la señal (W).

[11] El espectro ensanchado por salto de frecuencia (del inglés frequency hopping o FHSS) es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia síncronamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits.

Observemos que esta ecuación está dada para un sistema ideal, el BER se aproximará a cero si la velocidad de transmisión de los datos está debajo de la capacidad del canal. En el mundo real, el grado en que un sistema puede alcanzar este límite de BER aproximado a cero depende de la técnica de modulación y del ruido en el receptor.

Para todos los sistemas de comunicaciones, el ruido de una canal está íntimamente vinculado al ancho de banda de éste, y además todos los objetos que emiten calor también emiten energía RF en forma de ruido aleatorio (gaussiano). La cantidad de radiación emitida puede ser calculada mediante:

$$N[\text{watts}] = kT\ B$$

Donde:
k = constante de Boltzmann (1.38 x 10^{-23} J/K)
T = Temperatura del sistema (K), se asume normalmente en 290K;
B = ancho de banda del canal (Hz), predetectado.

Este es el más bajo nivel de ruido posible en un sistema con una temperatura física dada. Para la mayoría de las aplicaciones, la temperatura es asumida normalmente como la temperatura del lugar o ambiente en (290K). Las anteriores dos ecuaciones demuestran que si desea alcanzar un dado nivel de funcionamiento (como el definido mediante BER), puede comenzarse por sacrificar la potencia RF y el ancho de banda. Esto implica que usando una velocidad de datos menor que ocupe un ancho de banda menor brindará un mejor rango de funcionamiento.

5.2 Línea de Vista, Proximidad de Línea de Vista y Sin línea de Vista

Otro impedimento que se observa en las redes 802.11 es la percepción de que el suscriptor debe tener una línea de vista directa con el transmisor. Los detractores que piensan esto, temen que parta poder tener una WLAN necesitan un antiestético bosque de antenas en el techo, no diferentes de las antenas de TV de 1950 y 1960.

Dada la amenaza a la esteticidad de algunos buenos barrios, algunas comisiones de las zonas podrían intentar prohibir las antenas para redes inalámbricas. Otros se inquietan porque muchos electrodomésticos no beneficiarían los servicios de banda ancha inalámbrica porque sus casas no tienen línea de vista directa con el trasmisor del proveedor de servicios.

A pesar de esto, estas no son consideraciones insignificantes, a continuación se dan algunas pautas sobre factores que deben tener en cuenta los proveedores de servicio con sus trasmisores para que puedan entregar sus servicios al máximo número de suscriptores que pueda alcanzar.

5.2.1 Consideraciones de Zona Fresnel y Línea de Vista

La línea de vista en microondas incluye el área alrededor del trayecto, a la cual se llama Zona de Fresnel. Esta zona es un área elíptica inmediatamente alrededor del trayecto visual al transmisor.

Esta zona depende de la longitud del trayecto de la señal y de su frecuencia. La zona Fresnel (Figura A puede ser calculada, y debe ser tomada en cuenta cuando se diseña un enlace inalámbrico. Algunos objetos que estén dentro de la zona Fresnel atenuarán el trayecto de transmisión entre los dos puntos (transmisor y receptor).

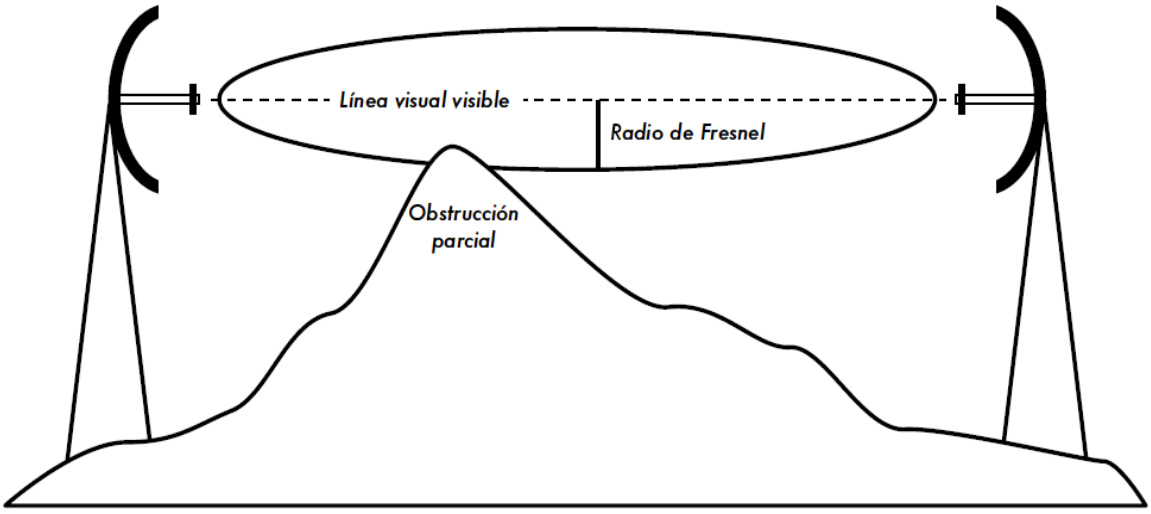


Figura A 1 La zona de Fresnel es bloqueada parcialmente en este enlace, aunque la línea visual no está obstruida.

La teoría exacta de las zonas de Fresnel es algo complicada. Sin embargo el concepto es fácilmente entendible: sabemos por el principio de Huygens que por cada punto de un frente de onda comienzan nuevas ondas circulares. Sabemos que los haces de microondas se ensanchan. También sabemos que las ondas de una frecuencia pueden interferir unas con otras. La teoría de zona de Fresnel simplemente examina a la línea desde A hasta B y luego al espacio alrededor de esa línea que contribuye a lo que está llegando al punto B. Algunas ondas viajan directamente desde A hasta B, mientras que otras lo hacen en trayectorias indirectas.

Consecuentemente, su camino es más largo, introduciendo un desplazamiento de fase entre los rayos directos e indirectos. Siempre que el desplazamiento de fase es de una longitud de onda completa, se obtiene una interferencia constructiva: las señales se suman óptimamente. Tomando este enfoque, y haciendo los cálculos, nos encontramos con que hay zonas anulares alrededor de la línea directa de A a B que contribuyen a que la señal llegue al punto B.

Tenga en cuenta que existen muchas zonas de Fresnel, pero a nosotros nos interesa principalmente la zona 1. Si ésta fuera bloqueada por un obstáculo, por ej. un árbol o un edificio, la señal que llegue al destino lejano será atenuada. Entonces, cuando planeamos enlaces inalámbricos, debemos asegurarnos de que esta zona va a estar libre de obstáculos. En la práctica en redes inalámbricas nos conformamos con que al menos el 60% de la primera zona de Fresnel esté libre.

La fórmula para el cálculo de dicho radio es:

$$R = 548\sqrt{\frac{d_1 d_2}{f.d}}$$

$d_1, d_{2,}, d$ en Km

f en MHz., R en metros.

Línea de Vista o Línea Visual (LOS, line of sight) se refiere a una situación en la cual hay un trayecto directo e inosbtaculizado del transmisor al receptor. Esto quiere decir en cualquier red inalámbrica, la transmisión sufrirá más degradación si hay un objeto que obstruya el trayecto. LOS es la mejor configuración posible para transmisión en redes 802.11.

Sin línea de Vista (NLOS, nonline of sight) se refiera a situaciones en donde el radio del enlace se encuentra bloqueado. Sin embargo, con ingeniería apropiada, es posible recibir servicios 802.11 sin tener un LOS directo hasta los transmisores de los proveedores de servicios. Éste término aplica usualmente donde el proveedor de servicio ha implementado sus tranceivers en una célula de la red donde hay un backbone en vez de células de servicio individuales. Si un suscriptor está en una ubicación que se caracteriza por ser NLOS, no será entonces atendido por el WISP (Wireless Internet service provider). Para alcanzar estos posibles clientes, el proveedor de servicio tendría que desplegar una nueva y costosa estación base.

Una alternativa de estación base nueva podría ser una tecnología "punto-multipunto" o una red ad hoc "peer to peer"[12]. (Ver figura 5.3)

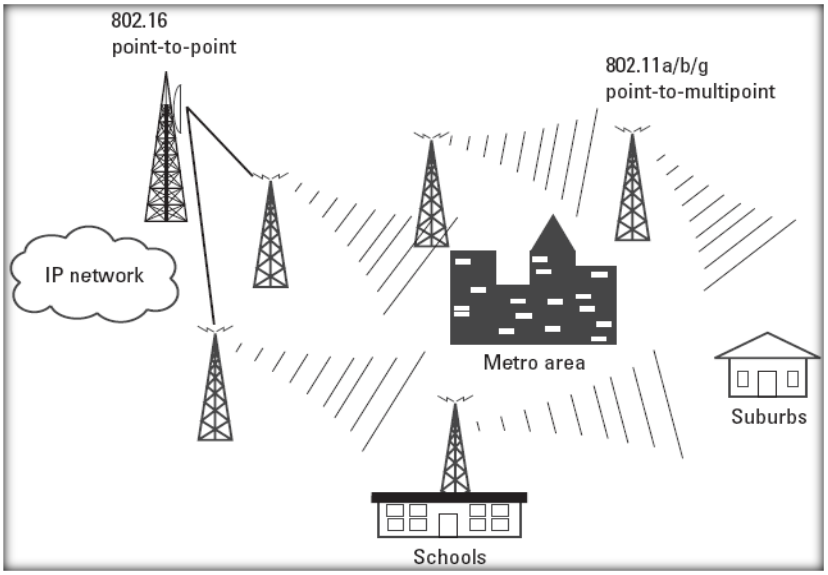


Figura 5. 3 Tecnología "cualquier punto-multipunto" usada para alcanzar un suscriptor NLOS

[12] Sistema de red en el que los archivos se reparten en diferentes computadoras, los usuarios accesan a éste de uno a otro en vez de por un servidor central.

Si, por ejemplo, la ubicación 5 está dentro de la LOS de la ubicación 2, el nodo 2 empezará a funcionar como un repetidor simplemente si se le instala una antena de enfoque amplio en su puerto B. En el sitio del nuevo suscriptor (locación 5) se instala entonces un tranceiver con una antena direccional apuntando a la locación 2.

Los sistemas ad-hoc peer-to-peer, también conocidos como mesh networks, pueden también proveer unos medios costosos pero efectivos para proveer servicios a locaciones NLOS. Los enlaces de radio extensos son reemplazados con varios enlaces cortos que son menos susceptibles al ruido y el multipath. En una red ad-hoc peer-to-peer, algo tan simple como un dispositivo de un suscriptor (PDA de mano, teléfonos celulares, laptop, y otros) puede ser usado como repetidor para alcanzar el access point de la estación base.

El inconveniente es que los adaptadores del cliente existente deben usar un nuevo software para controlar el enrutamiento del dispositivo del cliente y además cambiar su infraestructura existente a una ad-hoc como se necesite. El costo de los Access Points y la tecnología de las estaciones base así como los routers inalámbricos se están haciendo más económicos a medida que pasa el tiempo. Por tanto, la capacidad del proveedor del servicio para alcanzar mayor número de suscriptores se incrementa con el tiempo. Lo mismo para suscriptores potenciales si ellos mismos desean proveer los equipos para recibir el servicio de banda ancha inalámbrico. Aún si no se tiene LOS con una estación base o un Access Point, esto no quiere decir que no se puedan recibir los beneficios de la banda ancha inalámbrica.

Si es el caso de una red con topología “cualquier punto-multipunto”, cualquier nodo que ya esté en la red puede ser usado como punto de retransmisión para alcanzar el sitio.

5.3 Importancia del QoS en las redes 802.11

Cuando se presentó la posibilidad de que las redes 802.11 y protocolos asociados podrían reemplazar la PSTN, la idea era proveer una alternativa al servicio primario para el que la PSTN fue construida: la voz. La Voz sobre redes de datos requiere muchísima atención a los detalles de ingeniería de la red que la va a proveer. La principal objeción para transmitir voz sobre IP (Internet Protocol), es que el QoS de una red IP es inadecuado para entregar un servicio perceptible y adecuado al suscriptor. Las limitaciones de una red IP para entregar un adecuado QoS para voz y video incluyen problemas de latencia, jitter[13] y pérdidas de paquetes.

[13] El jitter se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto. En general, es un problema frecuente en enlaces lentos o congestionados. Se espera que el aumento de mecanismos de QoS (calidad del servicio) como prioridad en las colas, reserva de ancho de banda o enlaces de mayor velocidad (100Mb Ethernet, E3/T3, SDH) puedan reducir los problemas del jitter en el futuro aunque seguirá siendo un problema por bastante tiempo. Los valores recomendados de jitter entre el punto inicial y final de la comunicación debiera ser inferior a 100 ms. Si el valor es menor a 100 ms el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado. POSIBLES SOLUCIONES: La solución más ampliamente adoptada es la utilización del jitter buffer. El jitter buffer consiste básicamente en asignar una pequeña cola o almacén para ir recibiendo los paquetes y sirviéndolos con un pequeño retraso. Si alguno paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea necesario se descarta. Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más pérdida de paquetes.

Mediante la entrega de un adecuado QoS con el servicio de voz, 802.11 se presenta como una alternativa al servicio de voz PSTN. Suministrando un buen QoS en servicio de video, la red 802.11 se presenta como alternativa al servicio de TV cable o TV satelital.

5.4 Necesidades para el QoS en Redes Inalámbricas

Para entregar un servicio de voz de calidad que se compare con el servicio ofrecido por la PSTN, el operador de red debe minimizar la latencia, jitter y las pérdidas de paquetes en una red Vo802.11.
Un requerimiento de red adicional debe ser soportado si se quiere que la experiencia del usuario con banda ancha inalámbrico sea similar a la experiencia del usuario en ancho de banda con cable (acceso por T1). La IEEE ha estado tratando de resolver los problemas de QoS en las redes inalámbricas y recientemente aprobó 802.11e, el cual es compatible con versiones anteriores de 802.11, lo que quiere decir que las mejoras que contiene el 802.11 pueden aplicarse a 802.11 o 802.11a.

A continuación, se resumen los mecanismos requeridos para asegurar que la QoS está contenida en 802.11 y 802.11e.

5.4.1 Desafíos en el QoS de una Red Inalámbrica

Muchos intentos previos en la mejora de la QoS de las WLAN, muestran que estrategias que trabajan bien en redes cableadas no quiere decir que lo hagan también en las WLANs.

Esto es debido a que la velocidad de los paquetes de error pueden estar en un rango del 10% al 20%; la velocidad de los bits varia de acuerdo a las condiciones del canal; y los administradores del ancho de banda se enfrentan al problema de “rubber pipe“, que se refiere a cuando los administradores no saben cuando ancho de banda tienen que manejar, debido a que posibles vecinos sin relación con el administrador del ancho de banda pueden hacer uso de alguna parte del ancho de banda.

Además, si una red inalámbrica va a reemplazar a la PSTN, debe ser capaz de dar prioridad a los paquetes de voz y video que a los de datos.

5.4.2 Latencia en las redes inalámbricas

Como se ha venido comentando, la principal amenaza para una red IP es la latencia, o el retardo en la entrega de los paquetes a través de la red. Latencia se define como el tiempo que le toma a la red responder a comandos del usuario.

Si la latencia es alta, causa notables retardos en descargar una página Web por ejemplo, entonces la experiencia sería confusa pues no parecería estar haciéndose uso de la tecnología banda ancha, a pesar de toda la velocidad que ésta pueda manejar. Una baja latencia (menos de 50ms) es un requerimiento que debe manejarse si los servicios y dispositivos inalámbricos pretenden consolidarse exitosamente en el mercado.

La latencia experimentada por el usuario se debe a varias fuentes como son el procesamiento del enlace por el aire, la propagación, el procesamiento y transporte de la red, el servidor remoto (si aplica), la aplicación que está siendo usada y el dispositivo del usuario. La suma de todas estas latencias debe minimizarse para asegurar una experiencia positiva en la Terminal del usuario. (Ver Tabla 5.3).

Retardo	Definición
Procesamiento del enlace aéreo	Tiempo necesario para convertir los datos de usuario en paquetes aéreos (codificación, modulación y estructura e los datos) y la transmisión de éstos.
Propagación	Tiempo necesario para que una señal viaje entre la estación base y el dispositivo del suscriptor y viceversa.
Transmisión en la red	Tiempo necesario para enviar el paquete a través del entorno de red y el backbone de las redes, incluyendo el retardo por enrutamiento y procesamiento de protocolos, además del tiempo de transmisión.
Procesamiento en terminal remoto	Tiempo requerido para el procesamiento mediante servidores remotos u otros dispositivos.

Tabla 5. 3 Tipos de retardos encontrados en una red 802.11

El retardo de procesamiento conduce a otra muy exclusiva desventaja en sistemas que no están completamente basados en IP. Muchas redes no pueden transmitir paquetes IP propios y requieren "Asistencia IP" a través de algún protocolo o mediante la adición de equipos en la red para simular la ejecución IP. Estas medidas introducen complejidad y retardos en los paquetes, influyendo en la latencia del sistema e incrementando los costos.

La tasa de transferencia y la latencia son dos puntos esenciales para el funcionamiento de la red. Ambos definen la velocidad de la red.
Mientras que la tasa de transmisión es la cantidad de datos que pueden pasar de la fuente al destino en un tiempo especifico, la latencia (tanto de recepción como al transmitir) es el tiempo que le toma a una sola transmisión de datos en concretarse (por ejemplo, el tiempo entre la solicitación de determinados datos y la recepción de éstos) La latencia se ha adoptado como el tiempo en que toma mandar los datos de una terminal y la recuperación de éstos en otra terminal.

La latencia es crucial en el uso de banda ancha ya que el Internet está basado en TCP, y éste requiere paquetes ACK que confirmen las llegadas de los paquetes. Si el remitente no recibe un acuse de recibo cada cierto periodo de tiempo (milisegundos), entonces TCP asume que la conexión está congestionada y disminuye la velocidad con que está enviando los paquetes. TCP es muy efectivo manejando las congestiones de las redes cableadas.

La capacidad de un sistema de consolidarse entre la gran cantidad de de usuarios depende significativamente en su habilidad de manejar muchos mensajes pequeños TCP/IP por unidad de tiempo, y además multiplexar todos esos datos dentro de una celda determinada. De ahí, que altas latencias es sinónimo de un sistema de baja capacidad para el servicios de datos, lo que es equivalente a costos más altos para adecuar la red y eliminar las latencias. La red móvil de datos ideal soporta tanta velocidad de datos pico (3Mbps) como baja latencia de paquetes (2ms), y solo un mecanismo es necesitado para lograr hacer la transmisión: Wireless.

5.4.3 QoS en 802.11

El consenso en la industria es que 802.11 por ella misma no ofrece adecuados QoS. La IEEE ha adelantado un nuevo protocolo diseñado para mejorar el QoS en la MAC 802.11 original mediante el aumento del soporte para aplicaciones sensibles al QoS como VoIP, videoconferencia y video streaming.

El MAC 802.11 original incluía dos modos de operación, DCF y PCF. El 802.11e hizo un borrador de especificaciones que introducen dos nuevos modos de operación, DCF avanzado o enhanced DCF (EDCF) y función híbrida de coordinación o hybrid coordination function (HCF). Así como el MAC 802.11 original, las mejoras del 802.11e son diseñadas para trabajar con todas las capas físicas de 802.11 (802.11 original, 802.11, 802.11a y 802.11g).

A continuación se describirán las fortalezas de QoS en 802.11 y los mecanismos en 802.11e que se diseñaron para mejorar el QoS en las redes inalámbricas.

5.4.4 MAC 802.11 tradicional

Para entender la evolución de 802.11e como un mecanismo. de QoS, es necesario que primero analicemos el MAC 802.11 tradicional. La MAC 802.11 tradicional incluye soporte para dos mecanismos de acceso, el DCF y el PCF. (Ver figura 5.4)

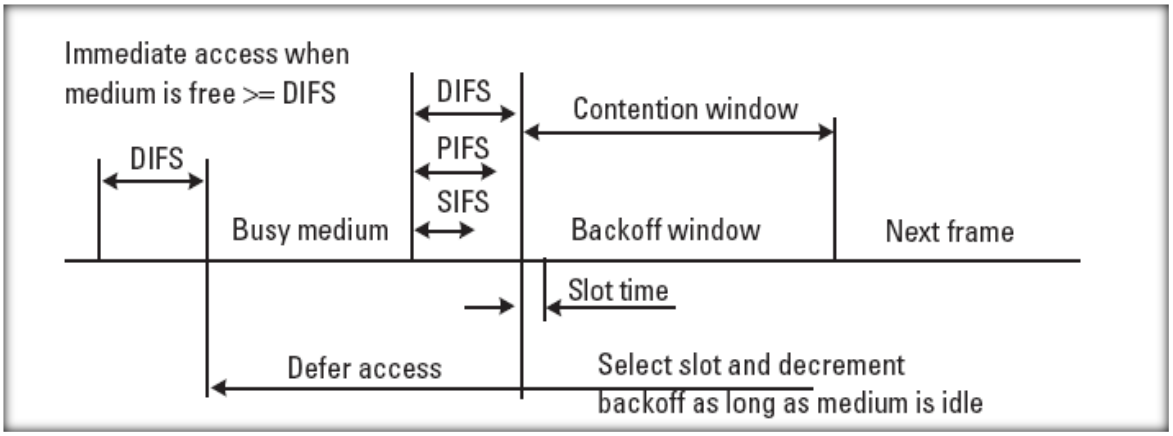


Figura 5. 4 Método básico de acceso en DCF y PCF

En la práctica, casi todas las implementaciones comerciales, si es que no son todas usan DCF son exclusivas.

5.4.5 DCF

El protocolo básico de MAC 802.11 es el Distribuited Coordination Function (DCF) o Función de Coordinación Distribuida. Está basado en CSMA/CA, es decir, si un nodo desea transmitir, antes debe escuchar el canal. CSMA/CD es muy parecido al Ethernet CSMA/CD, sin embargo, si se implementa en un transceiver inalámbrico, no es posible la detección de colisiones.

En CSMD/CA, las estaciones escuchan al medio para determinar cuando está libre. Una vez una estación detecta que el medio esta libre comienza a reducir su contador back-off[14]. Cada estación mantiene una Containt Window o Ventana de Contención (CW) que es usada para determinar el número de time slots que tiene que esperar antes de transmitir. Esta ventana depende de la historia de las retransmisiones del paquete actual. El back-off counter se decrementa en uno (1) después de que el medio ha estado libre por un período DIFS (Distributed Interframe Space) o Espacio Intertramas Distribuido. Cuando contador back-off llega a cero y el medio está todavía libre, la estación comienza a transmitir. El hecho que el canal esté libre en el DIFS no evita que dos o más estaciones intenten transmitir simultáneamente (luego del DIFS), por lo que existe la posibilidad de que se produzcan colisiones. Por cada transmisión exitosa de una trama cada estación recibe reconocimientos positivos (ACK). Si una transmisión falla (no se recibe un ACK) y la CW aumenta

Las colisiones (y otros problemas de transmisión) son detectados por la falta de dicho ACK que debe provenir del receptor. Después de la detección de una colisión, la estación escoge alternativamente un nuevo período de back-off (espera, suspensión) de su CW (la CW aumenta de forma exponencial binaria similar a Ethernet)) para luego ganar control del medio nuevamente. Además de las colisiones y el mecanismo binario de back-off, no hay garantía de transmisión con DCF. Una representación gráfica del mecanismo de acceso DCF se incluye en la figura 5.4.

5.4.5.1 Mecanismos de evasión de colisiones (CA, Collision Avoidance)

Para evitar colisiones, DCF usa mecanismos para sensar si el medio está en uso antes de comenzar a transmitir. Si el medio está en uso, la estación esperará según un algoritmo predeterminado antes de intentar transmitir. El DCF soporta mecanismos de portadoras físicas y virtuales.

Debido a que cada medio tiene diferentes características, la acción de sensar físicamente el medio es llamado clear channel assesment o evaluación de canal libre (CCA). Por ejemplo, una secuencia de radio directa de la PHY (Physical Layer, Capa Física) es utilizada para informar mediante tres condiciones de qué manera el medio está en uso. La primera condición informa que está en uso si detecta en el medio algún tipo de energía por encima de la umbral. La segunda condición informa que está en uso si detecta algún tipo de señal DSSS. Por último, la tercera condición informa que el medio está en uso si detecta una señal DSSS por encima del umbral. El sensado físico es muy eficiente pero es susceptible a nodos ocultos (ya que no puede saber cual está fuera del rango que debe sensar).

En el proceso de sensado con portadora virtual, no se sensa el medio de ninguna manera física. La información sobre el uso del medio es intercambiada mediante el uso de tramas de control. A lo contrario que el sensado físico, éste reduce notablemente la probabilidad de colisiones entre nodos ocultos y la red. También reduce la tasa de transferencia total, debido a que las tramas de control adicionales también deben ser intercambiadas. A causa de que éste overhead es fijo, entre más

[14] Este backoff es un periodo de tiempo aleatorio y es determinado como un múltiplo del tiempo que dura el slot. Es parte del mecanismo de evasión de colisiones. Este periodo de tiempo es un procedimiento de back-off (contienda) que se da antes de comenzar a transmitir.

pequeñas son las tramas de datos enviadas, mayor cantidad de porcentaje de overhead es añadido. En redes con grandes cantidades de pequeños paquetes o bajas colisiones, es mejor usar el sensado físico. Por esta razón, el sensado virtual con DCF es opcional.

Una solución para reducir el problema estaciones ocultas, es el mecanismo RTS/CTS (Request-To-Send:RTS / Clear-To-Send:CTS) que puede ser usado opcionalmente, los cuales corresponden a mensajes de control de sensado con portadora virtual. El tamaño umbral de una trama RTS puede ser configurado de manera que habilite un procedimiento de sensado con portadora virtual solo para paquetes mayor que un tamaño especificado.

Los procedimientos con RTS/CTS no usan tramas para broadcast o multicast (tramas individuales con múltiples destinos) porque esto podría generar múltiples conflictos en las respuestas CTS. El mecanismo de sensado de portadora virtual también ayuda a evitar las colisiones cuando dos BSSs traslapadas utilizan el mismo canal de radio para la transmisión.

Cuando el nodo A quiere enviar datos, envía una trama RTS al AP con la información de direccionamiento y duración. Este envía la dirección del nodo RA (receiver address) que recibirá las tramas de datos, su propia dirección TA (transmitter address), y la duración de la transmisión, cuyo cálculo tiene varios elementos.

Un AP recibe una trama RTS respondiendo con una trama CTS, la cual puede ser escuchada por todos los nodos dentro del rango del AP. El AP copia el TA del RTS dentro del RA de la trama CTS. También copia el campo de duración de la transmisión dentro del CTS después de hacer el ajuste para la transmisión actual de la CTS.

La recepción del CTS hace que el receptor guarde el campo de duración como network allocation vector o vector de asignación de red (NAV). El NAV es un temporizador que indica la cantidad de tiempo que queda antes de que el medio pueda ser usado. Ese valor se comienza a decrementar, y cuando llega a cero, indica que el medio está libre. Este, es actualizado siempre que un RTS o CTS con valor extenso es recibido. Mediante la combinación del sensado físico con el procedimiento RTS/CTS, se logra que un nodo oculto no pueda recibir datos del nodo originario para evitar colisiones con los datos de transmisión.

Entre dos paquetes consecutivos en la secuencia RTS, CTS, datos y ACKs, que indica que el canal está libre, existe un tiempo llamado Espacio Inter-Tramas Pequeño (Short Inter-Frame Space: SIFS), con el cual el resto de las estaciones actualiza su Vector de Asignación de Red (Network Allocation Vector: NAV), que contiene la información de control para transmisión y provee un mecanismo CSMA Virtual. A través de este mecanismo las colisiones se producen sólo entre los paquetes de coordinación RTS, lo que mejora el desempeño de la red en condiciones de alta carga.

Además de las tramas de control RTS y CTS, el procedimiento DCF CSMA/CA requiere que una trama acknowledgment (ACK) sea enviada para indicar una recepción exitosa de las tramas. No hay negative acknoeledgment (NACK), solo un temporizador que indica cuando debe esperarse el ACK antes de asumir que la transmisión fue errónea.

El DCF también suministra temporizadores intermedios para las tramas basados en valores específicos PHY. Estos temporizadores intermedios representan el tiempo que una estación debe sensar que el medio esté inactivo antes de darle inicio a la transmisión.

Hay dos intervalos PHY específicos que sirven de base para otros temporizadores intermedios de trama: slot time y SIFS. El slot time para un DSSS PHY (20us) se define como la suma de el tiempo de respuesta del receptor tras la llegada y el tiempo de detección de energía, también incluye el retardo por propagación.

El SIFS es el más corto de los intervalos entre las tramas y es usado para permitir la ejecución completa de una transmisión en progreso. El SIFS para DSSS PHY es de 10us y para FHSS PHY es de 28us.

El slot time y los SIFS son utilizados como componentes en otros tres intervalos de tramas. Estos son DIFS, EIFS (extended interframe space), y el PIFS (PCF interframe space). El DIFS es usado para habilitar la transmisión de datos y administración de MPDUs. El EIFS es usado para habilitar el procesamiento de tramas erróneas las cuales son informadas por la capa PHY. El PIFS habilita a una estación para que tenga prioridad de acceso al medio si está operando en el modo libre PCF.

Otro temporizador usado en el DCF virtual con habilidad CSMA/CA es el intervalo back-off. Si una estación que quiere transmitir detecta que una transmisión está en progreso, esperará antes de intentar nuevamente la transmisión.

El tiempo que esperará es determinado por un algoritmo back-off, el cual consiste en una progresión exponencial entre el mínimo y máximo de los valores. El valor de inicio para esta progresión se calcula multiplicando un número al azar entre el mínimo y máximo valor de back-off con el slot tome de la PHY.

El tiempo back-off es calculado entonces como una secuencia ascendente de potencias enteras de 2, menos 1. Por ejemplo, si el número al azar es 3 y el slot time es 10us, la estación esperara 7 o (2^3 -1) x 10us lo cual es igual a 70us. Los reintentos entonces continuarían con 15 o (2^4 -1) y luego con 31 (2^5 – 1) hasta el máximo valor permitido de reintentos. Debido que se usa un número al azar, dos estaciones que entran a una secuencia de transmisión no llegarán en el mismo intervalo back-off.

Eso previene que dos estaciones colisionen repetidamente porque sus secuencias se volverían sincrónicas. La estación también tiene un contador de reintentos que puede limitarse con un valor de reintentos permitidos. La figura 5.5 ilustra el protocolo de sensado virtual.

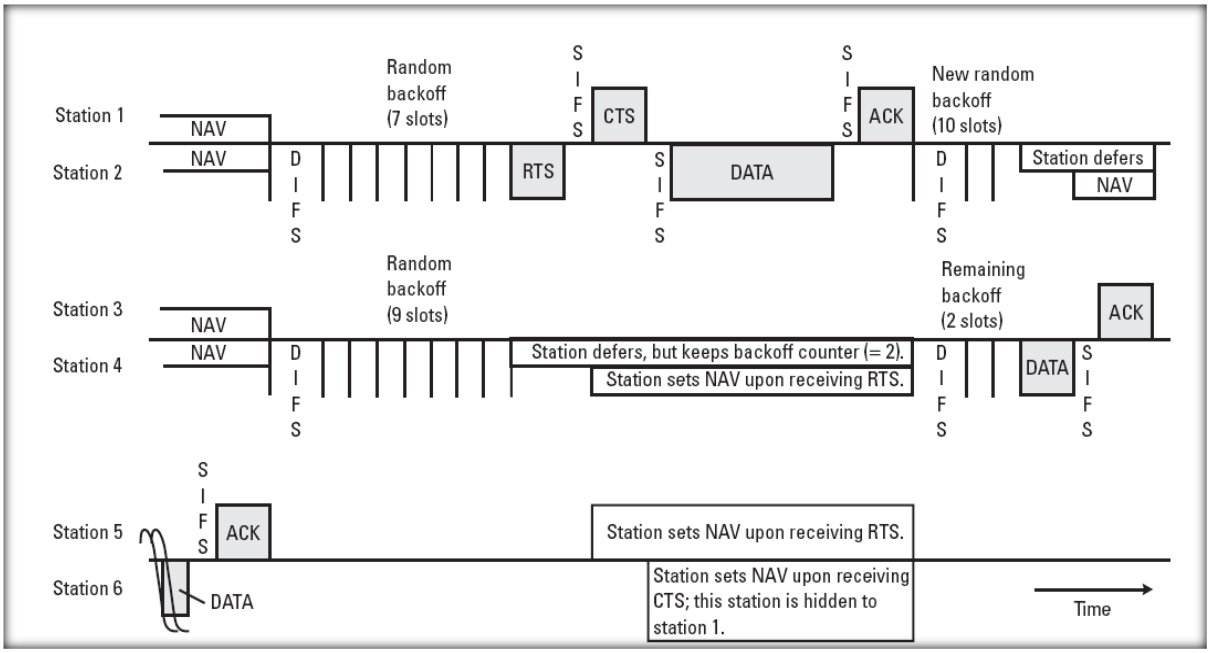


Figura 5. 5 Protocolo de sensado con portadora virtual

El protocolo de sensado con portador DCF es un método robusto para soportar los retos de velocidad de transmisión de datos entre los que comparten una red. La administración de tráfico centralizado lo hacen los AP.

5.4.5.2 Fragmentación de datos

Una transmisión que tome mucho tiempo, está bajo la posibilidad de ser afectada por interferencia. Permitir la transmisión de tramas más pequeñas para reducir la probabilidad de interferencia, fue analizada por la IEEE MAC 802.11 la cual especificó un método que consiste en dividir el contenido de la transmisión en unidades más pequeñas. Esto es llamado fragmentación. Un valor llamado umbral de fragmentación o fragmentation threshold especifica que las tramas por encima de un tamaño determinado deben ser divididas en múltiples transmisiones.

El encabezado de la trama contiene un campo de control de secuencia que muestra el orden de los segmentos. Los fragmentos que constituyen una trama son transmitidos inmediatamente uno tras otro sin ninguna contención del medio.

Cada fragmento tiene su propio CRC[15] y un ACK individual es transmitido por cada fragmento. Los fragmentos de transmisión son separados en intervalos apropiados y la transmisión de una secuencia de estos es llamada frame burst o ráfaga de tramas. Si ocurre un error con un fragmento, los fragmentos siguientes no serán transmitidos hasta que el fragmento erróneo sea conocido.

[15] CRC o Código de redundancia cíclica es un código de comprobación que se suele añadir a los datos transmitidos en muchas comunicaciones, y que permiten detectar (hasta cierto punto) si se ha producido algún error en la transmisión.

La retransmisión y reglas de back-off aplican a la retransmisión de tramas fragmentadas. La información de duración de los fragmentos y las tramas ACK establecen la NAV. Las tramas Broadcast y Multicast no son fragmentadas aún si su tamaño excede el umbral de fragmentación.

Mediante el uso de CSMA/CA y la definición de reglas para peer-to-peer, así como la administración de la transferencia de datos centralizados, la capa MAC proporciona estructuras de acceso confiable a la capa PHY.

5.4.6 PCF

En un intento de soportar la QoS, 802.11 también definió la Función de Punto de Coordinación o Pont Coordination Function, que encuesta a los nodos si desean o no transmitir. PCF es un mecanismo de acceso al medio centralizado, basado en encuestas, que requiere la presencia de una estación base que actúe como nodo coordinador (point coordinator, PC). Si existe PCF coexisten ambos esquemas, PCF y DCF. El modo PCF tiene prioridad más alta que DCF, ya que puede comenzar a transmitir después de un tiempo más corto que DIFS, este tiempo es llamado Espacio Inter-Tramas de la Función de Coordinación Puntual (PCF Inter-Frame Space: PIFS)..

El tiempo con PCF se divide en periodos repetidos llamados supertramas (superframes), donde se alternan Periodos Libres de Contención (Contention Free Period: CFP) y Periodos de Contención (Contention Period: CP). Un CFP seguido de un CP es una super-trama. Durante el CFP, el punto coordinador permite que las estaciones tengan prioridad de acceso al medio organizando las estaciones mediante round-robin.[16] , y se usa la PCF para accesar el medio mientras que durante el CP se usa la DCF. Un super-frame comienza con una trama de alerta (beacon), independientemente si la PCF está o no activa.

El “beacon” es un paquete de administración que sirve para sincronizar los relojes locales en las estaciones. Para que las estaciones accesen el medio compartido, el PC genera mensajes de “beacon” a intervalos regulares, las cuales informan a las estaciones bases que un nuevo CFP ha comenzado. El PC pregunta a una estación si desea transmitir. En caso de no obtener respuesta después de un PIFS, pregunta a otra estación o da por terminado el CFP. A partir de lo anterior es claro que durante un CFP el canal no permanece desocupado por un periodo mayor a PIFS. El PC continúa preguntando a las otras estaciones hasta que el CFP expire.
En esta forma de operación no se puede evitar totalmente que se produzcan colisiones, ya que, por ejemplo, si una estación escondida pierde la señal de alerta, y supone que aún se está transmitiendo en modo DCF, transmitirá durante un periodo que no le corresponde. Otro problema es que una estación se puede apropiar del canal injustamente, lo que va en detrimento de las otras estaciones.

[16] Es un método para seleccionar todos los elementos en un grupo de manera equitativa y en un orden racional, normalmente comenzando por el primer elemento de la lista hasta llegar al último y empezando de nuevo desde el primer elemento. Una forma sencilla de entender el round robbin es imaginar una secuencia para "tomar turnos". Es un método para ejecutar diferentes procesos de manera concurrente, para la utilización equitativa de los recursos del equipo, es limitando cada proceso a un pequeño periodo de tiempo (quantum), y luego suspendiendo éste proceso para dar oportunidad a otro proceso y así sucesivamente. A esto se le denomina comúnmente como Planificación Round-Robin.

En el punto coordinador de PCF no hay conocimiento de la carga ofrecida a cada estación. El punto coordinador simplemente mediante "round- robin" organiza todas las estaciones que han indicado el deseo de transmitir durante el período de contención libre. Cualquiera de las estaciones puede solicitar ser incluida dentro de la secuencia organizada de estaciones mediante un intercambio especial de tramas durante el período de contención.

EDCF define ocho tipos de tráfico. El acceso al medio que se da es parecido a DCF, adicionándole un AIFS (arbitration interframe space). Una estación no puede comenzar a decrementar su temporizador back-off hasta que se cumpla el AIFS ((Arbitration Interframe Space). Dentro del nodo, cada clase de tráfico debe hacer cola. Las colas de tráfico compiten por tener acceso al canal virtual. Las tramas que ganan el acceso al canal virtual, luego compiten por el acceso al medio.
HCF es análogo a PCF excepto porque permite un coordinador híbrido para mantener el estado de los nodos y destina las oportunidades de transmitir en el período de contención libre inteligentemente. El coordinador híbrido usa la carga ofrecida por cada clase de tráfico en cada estación para planificar el orden de las estaciones.

5.4.6.1 Mejoras de 802.11 MAC

Para mantener el QoS, se han discutido muchos esquemas. Las mejoras que definen la IEEE 802.11m Task Group E al 802.11 MAC, anteriormente mencionado, se convierte entonces en 802.11e. Estas mejoras o avances introducen dos mejoras a la MAC: EDCF y HCF. Ambos protocolos QoS-enhanced para MAC soportan más de 8 niveles de prioridad de tráfico, lo cual nos lleva directamente al protocolo RSVP y otro protocolo de prioridad de niveles

5.4.6.2 EDCF

El mayor avance por parte de EDCF versus DCF es la introducción de 8 clases de tráfico. Aparte de esto, EDCF, como su nombre lo dice, trabaja con un estilo similar a DCF MAC, excepto que algunos elementos de MAC son parametrizados según la clase. En la figura 5.6 se muestra el funcionamiento de EDCF:

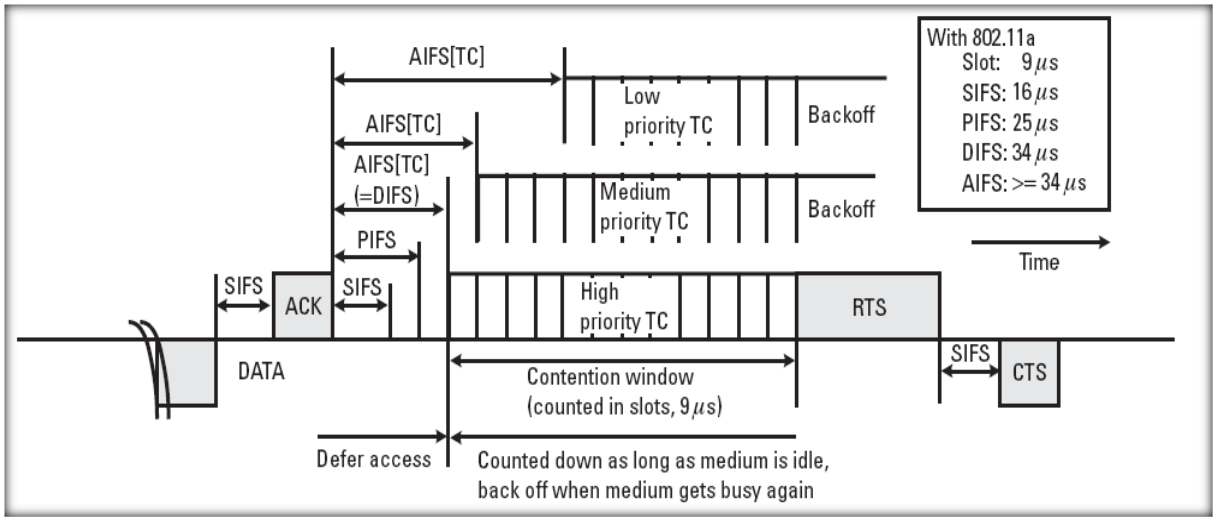


Figura 5. 6 IEEE 802.11e

Aquí, cada traffic class (TC) o categoría de tráfico da inicio a una back-off después de detectar que el canal está inactivo mediante un AIFS. El AIFS es al menos tan largo como el DIFS y puede ser escogido individualmente para cada TC. Este es el primer parámetro MAC por clase añadido en EDCF.

El mínimo valor de la CW para cada clase de tráfico, denotado como CWMin, puede ser seleccionado en base a la TC. En DCF una constante CWMin global es usada para inicializar todos los valores posteriores de la CW.

Cuando se detecta una colisión y la CW tiene que incrementarse, el valor de la CW es aumentado por un factor de persistencia o persistence factor (PF), el cual es también determinado en base a la TC.

Si el valor de la PF es 1, da como resultado una CW que permanece constante aún si hubiera caso de colisiones; si es 2 (default) da como resultado un tiempo back-off exponencial idéntico al de DCF.

El valor CWMax establece el máximo valor posible que puede tomar la CW basada en TC; sin embargo, la CWMax normalmente pretende permanecer igual para todas las clases de tráfico (al valor predeterminado usado en DCF).

Dentro de una estación, las 8 TCs tienen colas de transmisión independientes. Si los contador back-off de dos o más TCs en una estación llegan a cero al mismo tiempo, un programador o scheduler dentro de la estación toma este evento como posible una colisión virtual y la evita. La oportunidad de transmisión o transmit opportunity (TXOP) está dada a al TC con la más alta prioridad de las TCs colisionantes, los otros esperan como si una colisión hubiera ocurrido.

Los parámetros QoS, los cuales son suministrados en base al TC, puede ser adaptados a través del tiempo sin ningún problema. La estación base hace esto dándolos a conocer periódicamente mediante los beacon, los cuales son transmitidos al inicio de cada supertrama.

5.4.6.3 HCF

HCF (Hybrid coordination function) es una extensión de la idea de sondeo o encuesta (polling) que vimos en PCF. Así como en PCF, bajo HCF, la supertrama es dividida en dos períodos: el de contención libre (CFP) que inicia con cada beacon, y el periodo de contención (CP). Durante el CP, el acceso es gobernado por el EDCF, aunque el coordinador híbrido (HC, generalmente colocado en el AP) puede iniciar acceso con HCF en cualquier momento. (Debido a que tiene la prioridad más alta, puede empezar a transmitir antes de la expiración de los DIFS)

Durante el CFP, el HC distribuye una CF-Poll QoS a una estación particular para darle una TXOP. El HC especifica el tiempo de inicio y la máxima duración de la transmisión como parte de la trama CF-Poll. Durante el CFP, ninguna estación intenta ganar acceso al medio, pero luego cuando una CF-Poll es recibida, entonces asumen que tienen una TXOP y transmiten los datos que tengan. La CFP finaliza después del tiempo comunicado por el beacon o por la trama CF-End.

Si a una estación se le da dado una CF-Poll, se espera que responda luego dentro de un periodo SIFS. Si no lo hace, el HC puede hacerse cargo del medio después de un periodo PIFS, y delegar otro CF-Poll a otra estación. Esto permite un uso eficiente del medio durante la CFP.

El campo de control de QoS que ha sido agregado a la definición de trama MAC permite a las estaciones implementar 802.11e enviar colas por TC al HC.

5.4.6.4 Programación (Scheduling)

La MAC define protocolos y mecanismos para ejecutar HCF y EDCF. Sin embargo, hay un par de oportunidades para tomar decisiones por programación o scheduling, donde no hay participación de ningún número al azar como se vio en DCF.

5.4.6.5 Programación HCF

El HC tiene disponible permanentemente una vista instantánea de información sobre la longitud de las colas de cada TC por cada estación, incluyendo el AP mismo. Con esto, debe decidirse a quien darle una TXOP durante el CFP. Para esto hay que tener en cuenta al menos las siguientes consideraciones:

- Prioridad de el TC;
- QoS requerido por el TC (bajo jitter, gran ancho de banda, latencia baja, etc);
- Longitud de las colas por TC;
- Longitud de las colas por estación;
- QoS anterior experimentado por el TC.

El scheduling implementa un esquema para calcular un promedio de longitud de colas por estación y destinar el máximo TXOP disponible dentro del CFP a la estación con el promedio más largo.

5.4.6.6 Terminal programada con TXOP

Cuando una estación inalámbrica obtiene una TXOP mediante polling del HC, el HC no especifica un TC particular para el TXOP. Este le deja esa decisión a la estación inalámbrica. Esta decisión depende de los mismos factores que el HC scheduler, excepto por las celdas de múltiple-estación agregadas que el HC scheduler no tiene.

5.4.6.7 EDCF y HCF: QoS en redes 802.11

EDCF provee unas mejoras muy significativas para el tráfico de alta prioridad de QoS, sin embargo, estas mejoras sacrifican el procesamiento del tráfico de baja prioridad También parece que los parámetros EDCF pueden requerir una sintonización efectiva para conseguir los objetivos en cuanto a funcionamiento del sistema. A pesar de estos problemas, se encuentra a EDCF atractiva por su simplicidad, así como HCF.

HCF, tal como su antecesor PCF, provee mayor eficiencia en cuanto al uso del medio cuando este esta bastante ocupado. A diferencia de PCF, HCF hace una buena utilización del canal aún cuando

el canal está operando debajo de su capacidad. Debido a la reducción de overead, HCF puede proporcionar mejor soporte QoS a flujos de alta prioridad y también puede decidir que ancho de banda disponer para esta clase de flujos y también para los de baja prioridad.

Ambas funciones de coordinación son compatibles con DCF y PCF, lo cual significa que EDCF y HCF serán una adaptación que estará presente en las dominantes tecnologías de LAN inalámbricas.

6 Ingeniería de redes 802.11 para un máximo QoS

En el capítulo anterior tratamos con la ingeniería de redes 802.11 que alcanzarían el mejor QoS posible para la entrega de paquetes inalámbricamente. Este capítulo explica las medidas particulares que hay que tener en cuenta con la voz para entregar la mejor calidad de ésta en una red Vo802.11.

6.1 QoS en redes Vo802.11

A pesar del hecho de que las empresas telefónicas pierden miles de líneas por mes en los Estados Unidos debido a proveedores de servicio de telefonía móvil, muchos perciben que la voz sobre una conexión de telefonía móvil entrega una calidad de voz inferior y, por consiguiente, no correspondería a una alternativa viable frente al cableado de cobre de la PSTN. Como ya vimos, un gran número de nuevas medidas (principalmente 802.11e) mejoran el QoS sobre 802.11.

¿Pero en cuanto a voz qué? Los proveedores de servicio cableado y administradores de red han encontrado, que la voz es el servicio más difícil para aprovisionar sobre una red de IP. Nuevos acontecimientos en la industria Vo802.11 indican algunos desarrollos apasionantes que vencen la objeción principal a Vo802.11. Antes de que hablemos de estos acontecimientos, primero debemos determinar que métrica usar en la comparación de la calidad de voz de Vo802.11 con la de la PSTN.

6.1.1 Medición de la Calidad de Voz en Vo802.11

¿Cómo se mide la diferencia en la calidad de voz entre una red Vo802.11 y la PSTN? Tanto como la industria VoIP madura, nuevas formas de medir la calidad de voz salen al mercado. Actualmente, dos pruebas están disponibles que proveen una forma de medir la calidad de voz. El primero es un método de evaluación de la industria de los circuitos conmutados de voz conocido como MOS (*mean opinión score,* calificación promedio de opinión*)*. El otro ha surgido con el aumento de la popularidad de VoIP y se conoce como PSQM (perceptual speech quality measure, medición de la calidad perceptual del habla).

6.1.1.1 MOS

¿Puede expresarse la calidad de voz como una función de QoS al ser medido científicamente? La industria telefónica emplea un sistema de calificación subjetivo conocido como MOS *mean opinión score,* calificación promedio de opinión*)* para medir la calidad de sus conexiones telefónicas. Las técnicas de medida son definidas en la ITU-T P.800 y están basadas en las opiniones de muchos voluntarios de pruebas que escuchan una muestra de tráfico de voz y califican la calidad de aquella transmisión. Los voluntarios escuchan una variedad de muestras de voz y se les pide considerar factores como pérdidas, el ruido de circuito, el tono de retorno[17], eco del hablador, distorsión, delay[18], y otros problemas de transmisión. Los voluntarios entonces califican las muestras de voz de

[17] Señal de transmisión en la línea de recepción. http://ar.geocities.com/jedelectronica/electronica/manos_libres.pdf
[18] Retardo.

1 a 5 con 5 siendo "excelentes" y 1 ser "malo". Entonces a partir de dichas muestras se promedia el "MOS". Un MOS de 4 es considerado “toll quality o voz de calidad” que es igual al de la PSTN.

Note aquí que la calidad de voz de las aplicaciones VoIP está hecha para ser tan buena o mejor que la de la PSTN. Una investigación reciente realizada por el Instituto de Ciencias de Telecomunicaciones en la Boulder, Colorado, comparó la calidad de voz de tráfico enrutado por gateways VoIP con la de la PSTN. Los investigadores experimentaron con una variedad de muestras de voz y pidieron determinar si la muestra provenía de la PSTN o o de un gateway VoIP. El resultado de la prueba era que la calidad de voz del tráfico enrutado por el gateway VoIP era "indistinguible del de la PSTN". Téngase en cuenta que la red de IP usada en esta prueba era una red cerrada y no la Internet pública u otra red de IP de larga distancia.

Este resultado indica que los media gateways pueden entregar calidad de voz al mismo nivel que la PSTN. El desafío entonces cambia a lo siguiente: asegurar que la red IP pueda entregar un QoS similar para certificar una buena calidad de voz en transmisión. A continuación explicaremos qué tipo de medidas pueden tomarse en una red inalámbrica para asegurar que la calidad de voz sea igual al de la PSTN.

6.1.1.2 PSQM

Otra manera de de probar la calidad de voz en redes de Vo802.11 es la PSQM (perceptual speech quality measure, medición de la calidad perceptual del habla). Está basado en la Recomendación P.861 de la ITU-T, que especifica un modelo para mapear señales reales de audio a representaciones equivalentes de éstas dentro de lo que es el cerebro humano. La calidad de voz consiste en una mezcla de partes objetivas y partes subjetivas y varía extensamente entre los diferentes esquemas de codificación y tipos de topología de red usadas para el transporte.

En PSQM, las medidas de procesamiento (compresión, codificación, etcétera) de las señales sacadas de una muestra de voz son recogidas y se les realiza un análisis objetivo para comparar la voz original con la versión procesada de ella. (Figura 6.1).

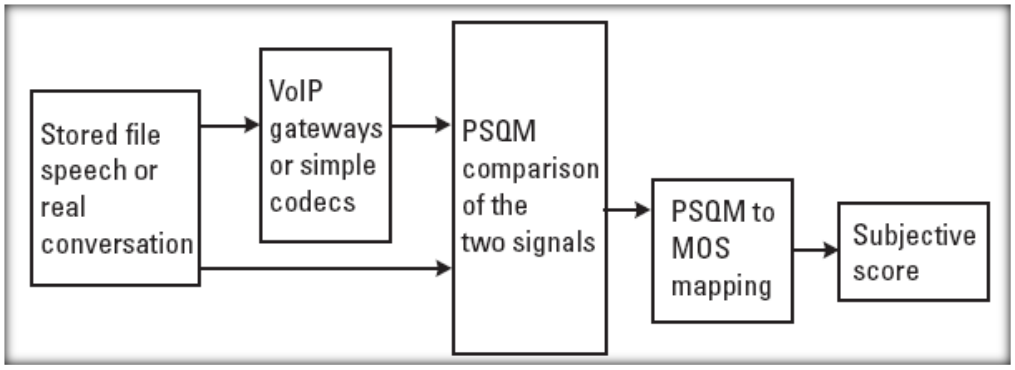


Figura 6. 1 Proceso de evaluación con PSQM

De aquí, se llega a una opinión resultado en cuanto a la calidad de las funciones de procesamiento de la señal que es procesada. A diferencia de las calificaciones de MOS, las de PSQM producen un

número absoluto, no una comparación relativa entre las dos señales. Los proveedores de servicio entonces pueden hacer al menos su decisión de compra basados en los scores de PSQM de la plataforma Vo802.11.

6.1.2 Detractores de la Calidad de Voz en redes Vo802.11

¿Qué detracta específicamente una buena calidad de voz en un ambiente 802.11? La latencia, el jitter, la pérdida de paquetes, y el eco perjudican la buena calidad de la voz en una red 802.11. Con la ingeniería apropiada, el impacto de estos factores sobre la calidad de voz puede ser reducido al mínimo y la calidad de voz de redes 802.11 puede llegar a ser igual a o mejor que el de la PSTN.

6.1.2.1 Contrarrestando la latencia en redes 802.11

La voz como una aplicación IP inalámbrica presenta desafíos únicos para redes 802.11. El primero entre estos es la calidad aceptable de audio que es resultado de la reducción al mínimo de la latencia de red (también conocida como delay) en un ambiente mixto de voz datos. Ethernet, cableada o inalámbrica, no fue diseñada para medios de comunicación que se ejecutan en tiempo real o para una entrega de paquetes garantizada. La congestión en la red inalámbrica, sin la diferenciación de tráfico, rápidamente puede dejar la voz inutilizable. Deben tomarse medidas en cuanto al QoS para asegurar que el paquete de voz se retrase menos que 100 ms.

El procesamiento de la señal de voz en el envío y la recepción, incluye el tiempo requerido para codificar o descifrar la señal de voz de forma análoga o digital en el esquema de cifrado de voz seleccionado para la llamada y viceversa, y añade delay. La compresión de la señal de voz también aumentará el delay. Entre mayor sea la compresión mayor será el delay. Ahora, si el consumo de ancho de banda no es una preocupación, el proveedor de servicio puede utilizar G 711, que es la voz sin comprimir (64 Kbps), y que impone un mínimo de delay debido a la carencia de compresión.

Sobre el lado de transmisión, el delay de empaquetamiento es otro factor que debe ser considerado en los cálculos. El delay de empaquetamiento es el tiempo que toma formar un paquete de datos. Entre más grande el paquete más tiempo requiere.
La utilización de tamaños de paquete más cortos puede acortar este delay, pero aumentará el overead porque más paquetes van a tener que ser enviados, todos tienen información similar en el header o encabezado. El equilibrio de la calidad de voz, el delay de empaquetamiento, y la eficacia de uso del ancho de banda es muy importante para el proveedor de servicio.

¿Cuándo el delay es demasiado extenso? De todos los factores que degradan Vo802.11, la latencia (o el delay) es el mayor. Pruebas recientes realizadas por Laboratorios Mier ofrecen una forma de medida referente a cuanta cantidad de latencia es aceptable o cuanta es comparable a "toll quality" (p. ej., la calidad de voz ofrecida por el PSTN). La latencia de menos de 100 ms no afecta la calidad de voz "toll-quality". Sin embargo, latencias mayores que 120 ms son perceptibles a la mayor parte de los llamantes, y las de 150 ms perjudican la calidad de voz muy notoriamente, degradando la calidad “toll-quality”. El desafío para los proveedores de servicios Vo802.11 y sus vendedores es conseguir que la latencia de cualquier conversación sobre su red no exceda los 100 ms.

La gente es intolerante con los delays de voz de más de aproximadamente 200 ms. Como se mencionó antes, la G.114 de ITU-T especifica que el delay no debe exceder los 150 ms de ida o 300 ms de ida y vuelta. El dilema es que mientras aplicaciones elásticas[19] (el correo electrónico por ejemplo) pueden tolerar una cantidad justa de delay, ellos por lo general tratan de consumir cada bit de la red que pueda. Al contrario, las aplicaciones de voz necesitan sólo pequeñas cantidades de la red, pero ésta pequeña cantidad tiene que estar disponible inmediatamente.

El delay experimentado en una llamada ocurre sobre el lado de transmisión, en la red, y sobre el lado de encubrimiento. La mayor parte del delay sobre el lado de transmisión es debido al delay de codec (empaquetamiento) y el delay de procesamiento de la señal. En la red, la mayor parte del delay se deriva a partir del tiempo de transmisión (serialización y propagación) y la cola en el enrutamiento. Finalmente, la profundidad del jitter buffer, el procesamiento y, en algunas implementaciones, los intervalos de sondeo, añaden delay sobre el lado de recepción.

El delay introducido por el codificador de voz puede ser dividido en delay algorítmico y delay de procesamiento. El delay algorítmico ocurre debido a la formación de tramas para el procesamiento de bloques, ya que el codificador produce un juego de bits que representan un bloque de muestras de voz. Además, muchos codificadores que usan bloques de procesamiento también tienen una función de visión posterior para proteger futuras muestras de voz antes de que un bloque sea codificado. Esto es el delay algorítmico. El delay de procesamiento es la cantidad de tiempo que toma codificar y descifrar un bloque de muestras de voz.

6.1.2.2 Paquetes caídos

En redes Vo802.11, un porcentaje de los paquetes puede perderse o retrasarse, sobre todo durante los períodos de congestión. También, algunos paquetes son desechados debido a los errores que ocurrieron durante la transmisión. Los paquetes perdidos, retrasados, y dañados causan una deterioración sustancial de calidad de voz. En técnicas de corrección de error convencionales usadas en otros protocolos, los bloques entrantes de datos que contienen errores son desechados, y el computador que recibe solicita la nueva transmisión del paquete. Así, el mensaje que finalmente es entregado al usuario es exactamente igual que el mensaje que lo originó. Debido a que los sistemas Vo802.11 son sensibles al tiempo y no pueden esperar por retransmisión, se usan sistemas de detección de errores más sofisticados para crear sonidos que llenen los huecos o agujeros que se hayan generado en la transmisión.

La mayor parte de las pérdidas de paquete ocurren en los enrutadores debido a la alta carga de enrutamiento o la alta carga del enlace. En ambas situaciones, paquetes en cola podrían caerse. Otra fuente de pérdida de paquetes son los errores en los enlaces de transmisión, causando errores CRC para el paquete. Los errores de configuración y colisiones también podrían causar pérdidas de paquetes. En aplicaciones que no son en tiempo real, las pérdidas de paquete son solucionadas en

[19] Aplicaciones elásticas: pueden hacer uso de tanto o tan poco ancho de banda como tengan a su disposición. Ejemplo: correo electrónico. No tienen restricciones de tiempo, a a diferencia de las aplicaciones en tiempo real que son bastante estrictas en cuanto a los tiempos de transmisión extremo a extremo. Ejemplo: aplicaciones multimedia.

la capa de protocolo por re transmisión (TCP). Para la telefonía esto no es una solución viable ya que los paquetes retransmitidos llegarían muy tarde y serían inútiles.

Quizás el desafío principal para Vo802.11 es que, en comparación con las redes cableadas, los paquetes se caen a una gran velocidad (más del 30 %). Esto puede conducir a la distorsión de la voz por lo que la conversación sería ininteligible. En gateways de VoIP diseñados para redes cableadas, una solución es usar un jitter buffer con un "cubo de bits " La solución en la industria VoIP cableada ha sido simplemente eliminar ("dejar caer") los paquetes de voz que llegan tardíos y averiados. Esto es aceptable si el porcentaje de paquetes tardíos y averiados es pequeño (es decir, menos del 10%). Cuando la pérdida de paquetes crece debido a muchas pretensiones de las transmisiones inalámbricas, la calidad de voz disminuye precipitadamente.

6.1.2.3 Jitter

Jitter ocurre porque los paquetes tienen tiempos de transmisión variables. Esto es causado por tiempos diferentes de cola en los enrutadores y posiblemente por trayectos de enrutamiento diferentes. Jitter causa un tiempo desigual de espaciado entre los paquetes que llegan y requiere un jitter buffer para asegurar la repetición uniforme y contínua del flujo de voz).

En VoIP, el jitter es la variación del tiempo entre la llegada de distintos paquetes. Estas variaciones son debidas a la saturación de la red, la falta de sincronismo o los cambios dinámicos en las rutas.

En redes con grandes cambios de velocidad se puede usar un “jitter buffer” para mejorar la calidad de la conversación. Un buffer es un espacio intermedio donde se almacenan los paquetes hasta su procesamiento. La idea básica del “jitter buffer” es retrasar deliberadamente la reproducción del sonido para garantizar que los paquetes más “lentos” hayan llegado. Los paquetes se almacenan en el buffer, se reordenan si es necesario y se reproducen a una velocidad constante. La calidad de voz mejora al incrementar la latencia total.

Muchos equipos de VoIP te dejan ajustar el tamaño del “jitter buffer.” El buffer es esa área donde los paquetes se almacenan para luego ser enviados al procesador de voz en intervalos constantes. El tamaño del buffer se mide en milisegundos. Si el buffer es de 200 ms significa que introducimos un delay de ese tiempo antes de reproducir la voz.

Existen dos tipos de jitter buffers: estático y dinámico. Un buffer estático está implementado como parte del equipo y configurado de manera fija por el fabricante. El dinámico se configura usando un programa y lo puede cambiar el usuario. Un valor común del jitter buffer es de 100 ms. Al incrementar el buffer vamos a mejorar la calidad de la conversación pero no olvidemos que lo que estamos haciendo es incrementar el delay total (latencia). Debemos buscar un valor de compromiso. Hay que tener en cuenta que un delay total muy por encima de 300 ms hace muy difícil tener una conversación. [20]

[20] Tomado de http://wiki.it46.se/doku.php?id=voip4d:capitulo_3:calidad_servicio

6.1.3 Factores que afectan el QoS en redes Vo802.11

Los cuatro parámetros de red más importantes para el transporte eficaz de tráfico Vo802.11 son el ancho de banda, delay, jitter, el eco, y la pérdida de paquetes (Tabla 6.1).

Factor	Descripción
Delay (Retardo)	Latencia entre la transmisión del paquete IP y el momento de su recepción en el destino.
Jitter	Variación entre los tiempos de llegada entre paquetes continuos desde un punto A hasta un punto B; causado por cambios en el enrutamiento de los paquetes, congestión y delays de procesamiento.
Ancho de Banda	Un gran ancho de banda entrega mejor calidad de voz.
Pérdida de Paquetes	Porcentaje de paquetes que nunca fueron recibido en el destino

Tabla 6. 1 Factores que afectan la calidad de voz en Vo802.11

La calidad de voz y vídeo son cosas sumamente subjetivas de medir. Esto presenta un desafío para los diseñadores de red ya que primero deben enfocarse en estos puntos para entregar el mejor QoS posible. En esta sección exploraremos las soluciones disponibles para los proveedores de servicio para entregar el mejor QoS posible.

Es necesario investigar la red en búsqueda de cualquier elemento que podría inducir delay, jitter, la pérdida de paquetes, o eco. Esto incluye elementos de hardware como enrutadores y media gateways y también estudiaremos los protocolos de enrutamiento que le dan prioridad a los paquetes de voz sobre todos los otros tipos de tráfico en la red IP.

6.1.4 Mejora del QoS en Routers y Gateways IP

El delay end-to-end es el tiempo requerido para que una señal generada desde la boca del llamante pueda alcanzar el oído del oyente. El delay es el principal factor de deterioro que recibe la mayor parte de atención en la industria de los media gateways. Puede ser corregido mediante funciones contenidas en los enrutadores de redes IP, los gateways VOIP, y en la ingeniería de red IP. Entre más corto el delay end-to-end, se percibe una mejor calidad de voz y además mejor experiencia para el usuario.

6.1.4.1 Fuentes de Delay: IP Routers

El delay de paquetes es principalmente determinado por el retardo de los IP routers en buffering, tráfico en cola, y conmutación o enrutamiento. El delay en la captura de paquetes es el tiempo requerido para recibir el paquete entero antes de procesarlo y reenviarlo a través del router.
Este delay es determinado por la longitud de paquete, los parámetros de operación de la capa de enlace, y la velocidad de transmisión. El uso de paquetes pequeños sobre redes de alta velocidad puede fácilmente disminuir el delay. Las redes Vo802.11 usan la velocidad de empaquetamiento para equilibrar la eficacia del ancho de banda de la conexión y el delay de paquetes.

6.1.5 Medidas necesarias para la entrega de un óptimo QoS en redes Vo802.11

QoS requiere la cooperación de todas las capas lógicas en la red IP – desde aplicaciones hasta el medio físico.-- y de todos los elementos de red, de un extremo al otro. Claramente, optimizar el desempeño del QoS en todos los tipos de tráfico sobre una red Vo802.11 representa un gran desafío. Para superar este desafío muy lentamente, varios grupos IETF han estado trabajando en propuestas estandarizados de tecnologías de QoS basadas en IP. Las propuestas del IETF podemos clasificarlas en las categorías siguientes:

- Organización mediante el uso del protocolo RSVP (Protocolo de Reserva de Recursos, Resource Reservation Protocol) y servicios diferenciados (DiffServ)[21];
- Conmutación de Etiqueta usando el protocolo MPLS (Multiprotocolo de conmutación de etiquetas, Multiprotocol Label Switching);
- Administración del ancho de banda usando el administrador de ancho de banda de subredes.

Para simplificar enormemente la discusión de que la calidad de voz de VoIP no es igual al de la PSTN, la red ha sido diseñada muy ingeniosamente para disminuir el delay y el jitter estableciendo RSVP, DiffServ, y/o MPLS en la red.

6.1.5.1 RSVP

Un punto clave en esta industria es diseñar redes Vo802.11 que le den prioridad a los paquetes de voz sobre los paquetes de datos. Una de las iniciativas más tempranas, Servicios Integrados (Integrated Services, int-serv), desarrollado por el IETF, se caracteriza por la reserva de recursos de red antes de la transmisión de cualquier paquete. El RSVP, definido en RFC 2205, es el protocolo de señalización que es usado para reservar ancho de banda en un trayecto de transmisión específico. RSVP es diseñado para operar con los protocolos de enruitamiento OSPF y BGP. El modelo de int-serv es significa para RSVP: una rutina de control de admisión, que determina la disponibilidad de los recursos de red; un clasificador, que pone paquetes en colas específicas; y un planificador de paquetes, que programa paquetes para analizar los requerimientos de QoS. El último desarrollo en RSVP fue el RSVP-TE (Protocolo de Reserva de Recursos–Ingeniería de Tráfico, Resource Reservation Protocol–Traffic Engineering*)*, es un protocolo de control/señalización que puede ser usado para establecer un trayecto para el tráfico por la red a través del router de la red especial para tráfico de alta prioridad. Este trayecto para el tráfico funciona independientemente de las otras clases de tráfico.

---

[21] Se han desarrollado y estandarizado los dos mecanismos de QoS, reserva y prioridad:

- ✓ IntServ (Integrated Services) y protocolo RSVP. El usuario solicita de antemano los recursos que necesita; cada router del trayecto ha de tomar nota y efectuar la reserva solicitada.
- ✓ DiffServ (Differentiated Services). El usuario marca los paquetes con un determinado nivel de prioridad; los routers van agregando las demandas de los usuarios y propagándolas por el trayecto. Esto le da al usuario una confianza razonable de conseguir la QoS solicitada. Es el más interesante actualmente. ... Ambos son compatibles y pueden coexistir.

Tomado de http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

RSVP actualmente ofrece dos niveles de servicio. El primer nivel es el garantizado, para aplicaciones de tiempo real que necesitan garantías cuantitativas firmes de QoS; garantiza un caudal mínimo y un retardo máximo. Cada router del trayecto debe ofrecer las garantías solicitadas, aunque a veces esto no es posible por las características del medio físico.
El segundo nivel es el de carga controlada, para aplicaciones elásticas, incluso de tiempo real, como las que se han diseñado para Internet actual, que son relativamente tolerantes a retardos pero muy sensitivas a congestión. El servicio es cualitativamente "bueno" (pérdidas y delays bajos) pero no se dan garantías cuantitativas

La tabla 6.2 listas los mecanismos disponibles en los sistemas convencionales de reenvío de paquetes que pueden manejar tráfico sincrónico.

Reserva, Asignación y Vigilancia	
RSVP	Protocolo de reservación de recursos, un protocolo de control de la red que permite que las aplicaciones que van a trabajar en Internet puedan obtener la calidad de servicio que sus flujos de datos puedan requerir.[22] Provee la señalización para reservar recursos en la red, típicamente utilizado para flujos simples, aún cuando es posible utilizarlo para flujos agregados. El host, en donde se ejecuta la aplicación que genera el tráfico en la red, inicia una sesión con el router con capacidad RSVP, especificando la dirección de destino, el identificador de protocolo y puerto a utilizar. Si recibe respuesta, obtiene un identificador de sesión que marcará el camino que seguirán los paquetes que genere el programa. Cuando se activa la sesión, cuando los paquetes son enviados, el router recibirá, junto a ellos, mensajes RSVP en donde se especifican la reserva de recursos que ha de realizar a lo largo de toda la trayectoria.[23]
RTP	Ofrece otro modo de priorizar el tráfico de voz. Los paquetes de voz por lo general dependen del protocolo de datagrama de usuario con encabezados RTP. RTP considera una gama de puertos UDP estricta prioridad.
Velocidad de Acceso Comprometida (CAR, Commited Access Rate)	CAR, que limita la tasa máxima de tráfico transmitido o recibido, y también puede marcar la Precedencia IP de los paquetes. Los dispositivos del interior de la red pueden usar la precedencia IP para determinar cómo se trata el tráfico para entregar la calidad de servicio requerida. Es un mecanismo que vigila tráfico, destina anchos de banda comprometidos y limita fuentes de tráfico y destino especificando políticas para manejar el tráfico que excede el ancho de banda asignado.

Tabla 6. 2 Mecanismos de Reserva, Asignación y Vigilancia disponibles en sistemas de Reenvío de paquetes que pueden diferenciar y manejar apropiadamente Tráfico Isocrónico.

RSVP trabaja así: un remitente envía primero un mensaje PATH a la lejanía a través de un número de enrutadores. El mensaje PATH contiene una especificación de tráfico (Tspec) que proporciona detalles sobre el tamaño del paquete de datos. Cada enrutador con RSVP habilitado a lo largo del camino establece un trayecto que incluye la dirección de la fuente del mensaje PATH. El receptor del mensaje PATH responde con una petición de reserva (RESV) que incluye una especificación de flujo (flowspec). El flowspec incluye un Tspec y la información sobre el tipo de servicio de reserva solicitado, tal como el servicio de carga controlada o el servicio garantizado.

[22] Tomado de http://www.mincomunicaciones.gov.co/minintranet/src/user_docs/conocimiento/desarrollosector/STVA(ProtocoloInternet62002)306.pdf
[23] Tomado de http://www.danysoft.info/free/reservarecursos.pdf.

El mensaje RESV viaja hacia el remitente a lo largo de la misma ruta que el mensaje PATH viajó. (Al revés). En cada enrutador los recursos solicitados son asignados, asumiendo que están disponibles y que el receptor tiene la autoridad para hacer la petición. Finalmente, el mensaje RESV alcanza al remitente con una confirmación de que los recursos han sido reservados.

El delay es una función de dos componentes. El primero es un retraso fijo debido al procesamiento dentro de los nodos individuales y es sólo una función del trayecto tomado. El segundo componente del delay es el retraso de cola dentro de varios nodos. La formación de una cola de espera es un mecanismo de QoS basado en IP que está disponible en sistemas convencionales de reenvío de paquetes y puede distinguir y de manera apropiada manejar el tráfico isócrono para entregar un QoS óptimo sobre redes de Vo802.11. Numerosos mecanismos toman lugar para lograr hacer la formación de una cola de espera lo más eficiente posible, éstos se describen en la tabla 6.3.

Mecanismo de Cola	Descripción
FIFO (First In, First Out; primero en entrar, primero en salir)	También conocido como una clase de servicio best effort, el FIFO simplemente expide paquetes según el orden de llegada. Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. Es adecuado para interfaces de alta velocidad, sin embargo, no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes. Hoy en día se necesitan algoritmos más sofisticados, que permiten diferenciar entre distintos tipos de paquete, por lo que este método está cayendo en desuso.
Priority queuing (PQ)	El Encolamiento de Prioridad (PQ:**Priority** Queueing) consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. En el mecanismo PQ, cada uno de los paquetes debe de ser colocado en una de las cuatro posibles colas (alta, media, normal, baja prioridad), servidas en riguroso orden de prioridad, lo cual puede crear inanición. Las prioridades se definen por filtros en los routers. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad y así. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. La prioridad de los paquetes puede diferenciarse por diversos medios, como: el protocolo de red, el interfaz del router por el que llegue el paquete, el tamaño del paquete y la dirección de origen o destino. Los paquetes que no se puedan clasificar serán asignados a la cola de prioridad normal. Este método es estático y no se adapta a los requerimientos de la red. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad (starvation).
Custom queuing (CQ)	Para evadir la rigidez de PQ, se opta por utilizar Encolamiento Personalizado (CQ: Custom Queueing). CQ fue diseñado para permitir que varias aplicaciones compartieran la red, y que además tuvieran asignado un ancho de banda mínimo garantizado, y unas garantías aceptables en cuanto a los retrasos. Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo Round-Robin. CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles
Weighted fair queuing (WFQ)	Es adaptativo a los cambios en la red. Es un método automatizado que provee una justa asignación de ancho de banda para todo el tráfico de la red, utilizado habitualmente para

	enlaces de velocidades menores a 2048 [Mbps]. WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Por ejemplo, para una conversación TCP/IP, se utiliza como filtro el protocolo IP, dirección IP fuente, dirección IP destino, puerto de origen, etc. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola. WFQ es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generen altas y bajas cargas en la red, ya que WFQ se adapta a las condiciones cambiantes del tráfico en ésta. Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable, al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas.
Class-based weighted fair queuing (CBWFQ)	WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta; colapsa debido a la cantidad numerosa de flujos que analizar. CBWFQ fue desarrollada para evitar estas limitaciones, tomando el algoritmo de WFQ y expandiéndolo, permitiendo la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación del ancho de banda. Algunas veces es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ, pero sí con CBWFQ. Las clases que son posibles implementar con CBWFQ pueden ser determinadas según protocolo ACL, valor DSCP, o interfaz de ingreso. Cada clase posee una cola separada, y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se pueden configurar específicamente el ancho de banda y límite de paquetes máximos (o profundidad de cola) para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase.
Low-latency queuing (LLQ)	El Encolamiento de Baja Latencia (LLQ: Low-Latency Queueing) es una mezcla entre **Priority** Queueing y Class-Based Weighted-Fair Queueing. Es actualmente el método de encolamiento recomendado para Voz sobre IP (VoIP) y Telefonía IP, que también trabajará apropiadamente con tráfico de videoconferencias. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene referencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas. La cola de prioridad que posee LLQ provee de un máximo retardo garantizado para los paquetes entrantes en esta cola, el cual es calculado como el tamaño del MTU dividido por la velocidad de enlace.

Tabla 6. 3 Mecanismos de Manejo de Tráfico Isocrónico[24]

El servicio de carga controlado (verRFC 2211) es una aproximación cercana del QoS que una aplicación recibiría si los datos estuvieran siendo transmitidos sobre una red que fue cargada ligeramente. Un alto porcentaje de paquetes será entregado satisfactoriamente y el retraso experimentado por un alto porcentaje de los paquetes no excederá el retraso mínimo experimentado por algún paquete que haya sido satisfactoriamente entregado.

[24]Tomado de http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf y http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

6.1.5.2 DiffServ

Una continuación de la inicial IETF son los Servicios Diferenciados (diff-serv; mirar RFC 2474). DiffServ clasifica los paquetes que requieren servicios de red diferentes en clases diferentes. Los paquetes son clasificados en el nodo de ingreso de red según los SLAs (Service Level Agreements o Acuerdos de nivel de servicio). DiffServ es un juego de tecnologías propuesto por el IETF para permitir a Internet y otros proveedores de servicio de red de basadas en IP para ofrecer niveles de servicio diferenciados a clientes individuales y sus flujos de información.
Sobre la base de un marcador DSCP (punto de código de DiffServ, DIffServ code point) en la cabecera de cada paquete IP, los enrutadores de red aplicarían los grados diferenciados de servicio a varios flujos de paquetes, expidiéndolos según diferentes PHBs (Per-hop Behaviors, comportamientos por salto). El GoS (grade of service, grado de servicio) preferencial, que sólo puede ser intentado pero no garantizado, incluye un nivel inferior de latencia de paquetes debido a que el avance de aquellos paquetes preferidos a la cabeza de una cola de paquetes haría sufrir congestión a la red.

La idea básica de DiffServ consiste en que cada paquete lleva escrito un código que indica a que clase pertenece; se supone que los routers saben el tratamiento que han de dar a cada una de las clases posibles, por lo que no han de mantener ninguna información sobre conexiones o flujos concretos; el número de clases posibles es limitado e independiente del número de hosts o de flujos que pasan por los routers, por lo que la arquitectura DiffServ es escalable.

DiffServ mejora el QoS sobre redes de Vo802.11 mediante el aprovechamiento del campo ToS (Type of service, tipo de servicio) de la versión 4 de IP y el equivalente al campo de clase de tráfico de la versión 6 de IP. La parte del campo de clase ToS/traffic que DiffServ emplea se conoce como el campo DS. Este campo es usado de modos específicos para marcar un flujo dado como el requerir un tipo particular de reenvío. El tipo de reenvío para ser aplicado es conocido como el comportamiento por salto o per-hop behavior, del cual DiffServ define dos tipos: EF (Expedited Forwarding o reenvío apresurado) y AF (Assured Forwarding o reenvío seguro)

PHB es el tratamiento que un router DiffServ aplica a un paquete con un valor DSCP dado. Un router trata con múltiples flujos de muchas fuentes a muchos destinos. Muchos de los flujos pueden tener paquetes marcados con un valor de DSCP que indica cierto PHB. El conjunto de flujos desde un nodo al siguiente que comparte el mismo DSCP codepoint es conocido como *aggregate (conjunto)*. De una perspectiva DiffServ, un router funciona sobre paquetes que pertenecen a aggregates específicos. Cuando un enrutador es configurado para soportar un PHB dado, entonces la configuración es establecida conforme más bien a conjuntos o aggregates que a flujos específicos de una fuente específica a un destino específico.

EF (RFC 2598) es un servicio en el cual un flujo de tráfico dado es asignado una velocidad mínima de salida de un nodo dado, una mayor que la velocidad de llegada en el mismo nodo. Este servicio es el de mayor calidad. Se supone que debe ofrecer un servicio equivalente a una línea dedicada virtual, o a un circuito ATM CBR o VBR-rt. Debe garantizar un caudal mínimo, una tasa máxima de pérdida de paquetes, un retardo medio máximo y un jitter máximo. El valor del subcampo DSCP

relacionado con este servicio es '101110'. Este es un servicio extremo a extremo de bajas pérdidas. Los aggregates o agregados no deben encontrar colas a su llegada a los routers.

El componente de servicios integrados, RSVP, proporciona un servicio de ancho de banda garantizado. Aplicaciones como la voz sobre IP, video, y programas online requieren este servicio robusto. EF PHB, elemento clave de DiffServ, proporciona este servicio a través de una pérdida baja, una baja latencia y un bajo jitter, asi como un servicio asegurado de ancho de banda. EF puede implementarse usando PQ. Cuando se implementa en una red DiffServ, EF PHB proporciona una linea virtual, o un servicio premium. Sin embargo, para una eficiencia óptima, EF debe ser reservado para únicamente las aplicaciones más críticas, puesto que en situaciones de congestión de tráfico, no es factible tratar todo o gran parte del tráfico con alta prioridad.[25]

El PHB Assured Forwarding (AF) PHB define un método por el cual los BAs pueden darse con diferentes garantías de envío hacia delante. Por ejemplo, el tráfico de red puede dividirse en las siguientes clases:

· Oro: El tráfico de esta categoría dispone del 50 % del ancho de banda.
· Plata: reserva el 30% del ancho de banda.
· Bronce: con el 20% del ancho de banda.

Además, este PHB define cuatro clases: AF1, AF2, AF3, y AF4. Cada clase se asigna a una cantidad específica del espacio del buffer y ancho de banda de la interfaz, de acuerdo con la política establecida. En cada clase AF, se pueden especificar tres valores de precedencia: 1, 2 y 3.

EL AF PHB permite a un proveedor ofrecer los niveles diferentes de reenvío asegurado para paquetes recibidos de un cliente. El AF PHB permite a los paquetes ser marcados con diferentes clases de AF y dentro de cada clase puede ser marcado con valores de preferencia de "caída" diferentes. Dentro de un router, los recursos son asignados según las diferentes clases de AF. Si los recursos asignados a una clase dada se congestionan, entonces los paquetes deben ser dejados, es decir, se caen. Los paquetes para abandonar son aquellos que tienen valores de preferencia de "caída" más altos. El objetivo es proporcionar un servicio que asegura que paquetes prioritarios son reenviados con un grado mayor de fiabilidad que los paquetes de una prioridad inferior.

En una red DiffServ, la implementación de AF debe detectar y responder a largas congestiones dejando caer los paquetes y respondiendo a congestiones de corto plazo, suavizando de esta manera las congestiones a largo plazo. Cuando el nivel de congestión suavizado está debajo de un umbral particular, entonces ningún paquete deberá ser dejado caer. Si el nivel de congestión suavizado está entre un primer y segundo nivel de umbral, entonces los paquetes con el nivel de preferencia de "caída" más alto deberían ser dejados caer. Tanto como suba el nivel de congestión, entonces más de los paquetes de alta preferencia de "caída" deberán ser dejados caer hasta que un segundo umbral de congestión sea alcanzado. A éste punto, todos los paquetes de alta preferencia de "caída" son dejados caer. Si la congestión sigue elevándose, entonces los paquetes del nivel de preferencia medio de "caída" también comenzarán a ser dejados caer.

[25] http://www.dsi.uclm.es/asignaturas/42650/PDFs/practica5.pdf

6.1.5.3 Bit Rate en redes Vo802.11

El bit rate (o velocidad de compresión) es el número de bits por segundo entregado por el codificador de voz; por lo tanto, esto determina la carga de ancho de banda en la red. Es importante notar que los encabezados de paquete (IP, UDP, RTP) también añaden carga al ancho de banda. La calidad de voz generalmente aumenta con el bit rate. En resumidas cuentas, a mayor ancho de banda, mayor es la calidad de voz.

6.1.6 Codecs de voz diseñados para redes Vo802.11

Muchos de los detractores de la buena calidad de la voz en Vo802.11 pueden ser callados mediante la implementación de codecs de voz tanto en la tecnología de circuitos conmutados como en la tecnología de conmutación de paquetes. Las subdivisiones siguientes describen la codificación de voz y como esto se aplica a la calidad de voz, pero primero miraremos la solución QoS:

> Solución QoS: Codecs de circuitos conmutados fijos en un circuito de conmutación de paquetes.

6.1.6.1 Codificación de voz de circuitos conmutados en Telefonía IP

Los codecs más comúnmente usados hoy en día para la telefonía IP son G 711, G 729, y G 723.1 (a 6.3 Kbps). Todos estos codecs fueron diseñados para la telefonía de circuitos conmutados (PSTN). La telefonía móvil ha sido el motivo principal para el desarrollo de tecnologías de codificación de voz en años recientes.

Estos codecs están diseñados para el empleo en redes de circuitos conmutados y no trabajan bien en redes de conmutación de paquetes, porque su diseño se enfoca en el manejo de errores de bit más que en las pérdidas de paquete.

Los puntos importantes en cuanto a la G 711 como un codec Vo802.11 son que (1) el coder fue diseñado para la telefonía de circuitos conmutados y (2) además no incluye ningún medio para manejar la pérdida de paquetes. La inserción de ceros comúnmente es usada cuando ocurre una pérdida de paquetes, conduciendo a una interrupción del flujo de voz y la degradación de la calidad con la creciente pérdidas de paquetes.

Es posible ocultar los errores extrapolando e interpolando segmentos de voz recibidos, mejorando de esta manera la calidad en comparación con el relleno con ceros. Un ejemplo es el nuevo Anexo I a la G 711 llamada G 711 PLC, que no siempre trabaja bien y no garantiza la operación robusta.

Los códecs G.729 y G.723.1 pertenecen a una clase diferente de coders comparados a G 711. Los puntos más importantes en cuanto a G 729 y G 723.1, son así: (1) el paradigma de codificación usado en estos coders fue desarrollado para la telefonía de circuitos conmutados y telefonía móvil; (2) la calidad de discurso básica es peor que la calidad PSTN, es decir tienen la calidad de telefonía móvil; (3) el proceso de codificación está basado en dependencias de intertrama que conducen a dependencias de interpaquete; (4) el funcionamiento de la pérdida de paquetes es muy pobre debido

a la propagación de errores que son resultado de dependencias de interpaquetes, así la calidad de discurso se degrada rápidamente con la creciente pérdidas de paquetes; (5) los coders tiene métodos de ocultamiento de errores montados en métodos heurísticos y también sufren de dependencias de intertrama y (6) los coders producen un flujo de bits inflexible y el tamaño de paquete es restringido a un número entero de tramas, lo que reduce la flexibilidad.

6.1.6.2 Modificación de codecs de voz para mejorar el QoS en redes Vo802.11

Uno de los primeros procesos en la transmisión de una llamada telefónica es la conversión de la señal analógica (la onda correspondiente a voz que entra en el teléfono) en una señal digital. Este proceso es llamado modulación por impulsos codificados o PCM. Esto es un proceso de cuatro pasos que consiste en el muestreo PAM, companding, cuantización, y la codificación. La codificación es un proceso crítico en Vo802.11. Los codecs de voz usado en VoIP (conmutación de paquetes) son tomados directamente de tecnologías PSTN (conmutación de circuitos).
Las tecnologías de teléfono móvil usan los codecs de voz de PSTN Nuevos softwares en la industria Vo802.11 modifican los codecs PSTN para entregar una calidad de voz comparable con el de la PSTN.

Hay un mercado emergente de voz de software de procesamiento y realzamiento de la calidad de voz que corrige los defectos de los codecs tradicional de voz, que fueron hace décadas diseñados para los circuitos conmutados de PSTN. Estos acontecimientos recientes en el software Vo802.11b proporcionan soluciones de mejora del QoS para la telefonía IP con una muy alta calidad de voz aún con degradaciones de red severas causadas por la pérdida de paquete y jitter.

Estas mejoras en el QoS de Vo802.11b deben proporcionar una calidad de voz Vo802.11b comparable con el de PSTN. También, la calidad de voz debe degradarse gradualmente tanto como sean los aumentos de la pérdida de paquetse. Los porcentajes de pérdida de paquete moderados deben ser inaudibles.

6.1.6.3 Software de procesamiento de mejora de voz

Los nuevos algoritmos de procesamiento de voz aseguran la pluralidad, es decir, que un segmento de voz entero no se pierde cuando un paquete es perdido. La pluralidad es alcanzada reorganizando la representación de la señal de voz Esta reorganización no añade redundancia, es decir, no envía la misma información dos veces. Por lo tanto, existe un ancho de banda eficiente y asegura que las pérdidas de paquetes conduzcan a una degradación gradual e imperceptible de calidad de voz.

Los softwares de procesamiento de mejora de voz incluyen un tratamiento de señal avanzado para reducir al mínimo el retraso. Por lo tanto, el retraso total es mantenido en aproximadamente el mismo nivel que sería sin la pluralidad. Además, la calidad básica (sin pérdida de paquete) es equivalente a o mejor que la de PSTN (usando la G 711).

Los softwares de procesamiento de mejora de voz son construidos para mejorar las normas existentes usadas en telefonía IP. Este software permite la alta calidad de voz sobre una red cargada con jitter, altas pérdidas de paquetes, y delays.

6.1.6.3.1 Ejemplos de productos de procesamiento de mejora de voz:

Algunos productos de procesamiento de mejora han sido diseñados:

- Jitter buffer adaptativo. El empleo de un Jitter buffer adaptativo optimiza la calidad del sonido mediante el uso de un Jitter buffer adaptativo combinado con un algoritmo de ocultación de error. Esto trabaja con cualquier codec como G 711, G 729, y G 723.1. Este arreglo mejora la calidad del sonido considerablemente sin cualquier problema de interoperabilidad. Esta solución se adapta rápidamente a las condiciones de red dinámicas de redes de paquetes conmutados. Esto asegura la alta calidad de voz con ahorros de latencia significativos comparados con la tecnología convencional de Jitter Buffer.

- G 711 Mejorado. El G 711 mejorado consiste en el códec G 711 combinado con unas mejoras para proporcionar una robustez superior de pérdida de paquetes. Durante una llamada, el sistema determina si el receptor usa también el G 711 Mejorado, si es así, entonces la llamada seguirá usando G 711 Mejorado; si no hay correspondencia, la llamada continuará utilizando G.711 entre ambos terminales. El G 711 Mejorado en combinación con un Jitter buffer adaptativo proporciona un nivel de calidad de voz PSTN.

- Robustez de pérdida de paquetes. Usar un codec de bajo bit-rate es un método de robustez de pérdida de paquete creciente: los codecs de bajo bit-rate usan menos ancho de banda, proporcionando un empleo más eficiente del ancho de banda disponible. La calidad de voz básica de un códec de bajo bit-rate ofrece mejor calidad de voz que G 729 y G 723.1 y funciona a una velocidad de 13.3 Kbps.

- Cancelación de eco acústico. El eco es a menudo frecuente cuando se usan teléfonos IP o un computador personal. La cancelación de eco acústico está contenida en el software de procesamiento de mejora de voz para contrarrestar el eco.

7 ESCALABILIDAD EN REDES VoIP INALÁMBRICAS

Si Vo802.11 pretende reemplazar las tradicionales redes de voz TDM, debe ser capaz de extenderse al mismo nivel que tiene la red a la que está reemplazando. A diferencia de la tradicional red cableada, no solo debe considerar la capacidad de conmutación sino que debe tener en cuenta otros factores como el ancho de banda y el espectro asignado. A continuación estudiaremos algunos asuntos importantes que los diseñadores de redes deben tener en cuenta cuando tienen pensado implementar una aplicación Vo802.11. (Ver figura 7.1)

7.1 Consideraciones de Ancho de Banda para VoIP Inalámbrico

La especificación IEEE para 802.11b demanda un máximo de 11Mbps de ancho de banda. El estándar G.711 para tráfico de voz exige 64Kbps. Dicho de una manera más simple, esto indicaría que podrían efectuarse más de 170 conversaciones G.711 simultáneas con tan solo un Access Point. Sin embargo, VoIP añade cuantiosos overhead[26] por conversación, por lo que el ancho de banda usado en una conversación VoIP sin comprimir es mucho mas de 64Kbps, dependiendo de que información es incluida en los encabezados de los paquetes de voz (podría exceder los 10 Kbps). Además, el uso del 802.11b no garantiza los 11Mbps de ancho de banda. Mejor dicho, por ejemplo en el caso de hotspots[27], el ancho de banda proviene de un sistema T1 (1.54Mbps) suministrado por la compañía telefónica local. Esto indicaría que más de 20 conversaciones simultáneas podrían ser posibles si se basan en stream de 64Kbps para la conversación VoIP, sin incluir el overhead de VoIP.

El uso de otras variantes de 802.11, a saber, 802.11a, que tiene un máximo de ancho de bando de 54Mbps, indicaría que existe la posibilidad de más de 800 conversaciones simultáneas, sin figurar el overhead de VoIP. Comprimiendo el flujo de voz a 8Kbps (G.729) podría incrementarse el número de conversaciones simultáneas por Access Point (AP).

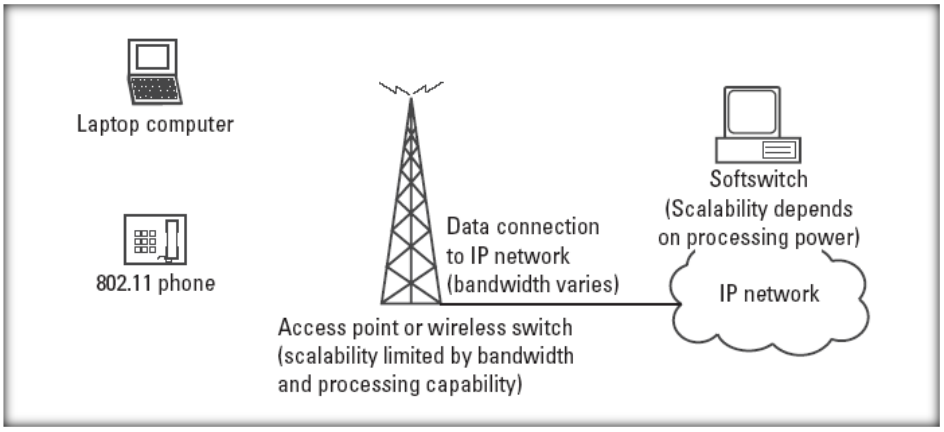


Figura 7. 1 Consideraciones de escalabilidad en redes VoIP inalámbricas

[26] **Overhead** se refiere a la proporción de datos de control, encabezados, etc que se adhieren a los datos de usuario y que implican mayor consumo de ancho de banda. http://www.ice.go.cr/esp/serv/hogar/tele/internet/anchobanda.htm

[27] **Hot- Spots**: consiste en la colocación de puntos de conexión en zonas públicas como aeropuertos, hoteles, cafés, restaurantes, etcétera, dando la posibilidad al usuario que disponga de dispositivo con tarjeta de conexión WIFI cuya compatibilidad no cause problemas (el nivel de estandarización es elevado por lo que no los suele haber). Tomado de http://www.microsoft.com/spain/empresas/tecnologia/hotspot.mspx

7.2 Importancia del ancho de banda para la escalabilidad

El ancho de banda de un AP, el cual es determinante en el número máximo de conversaciones simultáneas que pueden ser soportadas, no es infinito a través del espacio. Más bien, el ancho de banda disminuye de acuerdo a la distancia a la que se encuentre el Access Point. Factores como árboles, edificaciones y el clima pueden degradar la capacidad de penetración de 802.11 por el espacio. Esto es llamado pérdidas por propagación[28], que luego serán descritas. La Figura 7.2[29] muestra las pérdidas por propagación o degradación de la velocidad del enlace de datos contra las diferentes variantes del 802.11 a través del espacio.

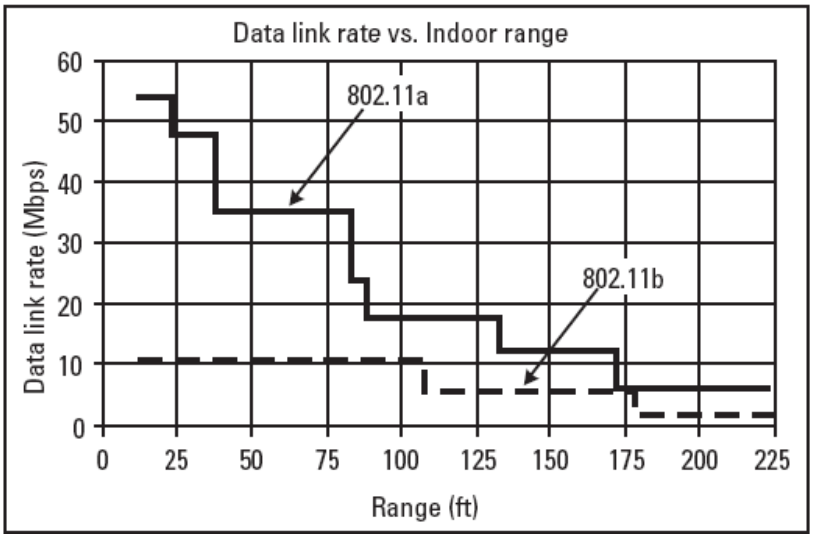


Figura 7. 2 Entre mayor sea la distancia al Access Point, mayor es la degradación del ancho de banda, lo cual limita el número de llamadas simultáneas en el Access Point

7.3 Protocolos para Vo802.11

Cuatro protocolos primordiales todavía se encuentran disponibles: 802.11, 802.11b, 802.11a y 802.11g. A continuación haremos un breve repaso para examinar las fortalezas y debilidades de Vo802.11 con cada uno de los protocolos 802.11.

Las características que pueden influir en estos protocolos incluyen ancho de banda, frecuencia, alcance y penetración.

7.3.1 802.11b

Es el protocolo estándar más utilizado, requiere tecnología DSSS, definiendo una velocidad máxima de datos a través del aire de 11Mbps y un método para las reducir las velocidades de datos más altas que no puedan ser sostenidas.

---

[28] Path Loss.

[29] Tomada de The FCC Web site, http://www.fcc.gov, tiene mucho material. La Part 15completa puede ser encontrada en http://www.access.gpo.gov/nara/cfr/waisidx_01/47cfr15_01.html.

La tecnología DSS (Direct Sequence Spread Spectrum)[30] es una técnica de expansión del espectro donde el ancho de banda de las señales transmitidas es mucho mayor que el mínimo necesario para transportar la información Se basa en la multiplicación de la secuencia de bits original por una secuencia digital (llamada chip) de velocidad mucho mayor.

El código de expansión expande la señal por una gran banda de frecuencias, dicha expansión es proporcional al número de bits usados. Con DSS se combina la información digital (Data Input A) de la secuencia de bits con los bits de la secuencia de expansión (PN), usando OR exclusivo (XOR). Esto se observa en la figura D.1.

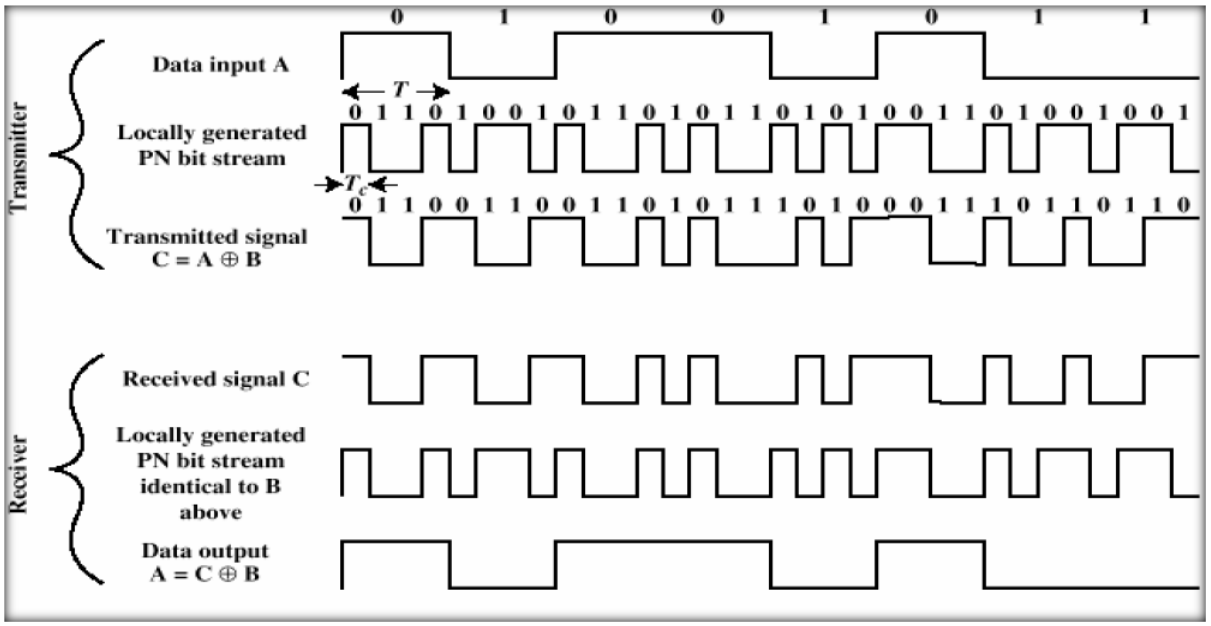


Figura D. 1 Ejemplo transmisión y recepción con DSS

El protocolo 802.11 soporta velocidades de datos de 5.5, 2, y 1Mbps a través del aire además de 11Mbps si se usa DSSS y CCK. Éste estándar adopta CCK[31] como método de modulación para lograr conseguir una velocidad de datos de 5 a 11 Mbps.

La especificación 802.11b permite la transmisión inalámbrica de datos sin procesar o en bruto a aproximadamente 11Mbps en espacios indoor de alrededor de 300 pies de distancia, y outdoor de alrededor de 20 millas en aplicaciones punto-a-punto en la banda de 2.4GHz. La distancia depende de los obstáculos, materiales y LOS[32].

[30] Tomado de http://www.info-ab.uclm.es/asignaturas/42638/pdf/cap2.pdf
[31] CCK: Complementary Code Keying o Modulación por Cambios de Código Complementarios
[32] LOS (Line of sight) o línea de vista: Se refiere a un camino (*path*) limpio, sin obstrucciones, entre las antenas transmisoras y receptoras. Para que exista la mejor propagación de las señales RF de alta frecuencia, es necesaria una línea de vista sólida. http://www.wni.com.mx/linea_vista.htm

7.3.2 802.11a

La banda de 5.1 GHz está especificada solo para usos indoor, la de 5.2GHz para usos tanto indoor como outdoor, y la de 5.7GHz solo para usos outdoor. Las interferencias por RF son muchísimo menores debido a que la banda de 5GHz es la menos concurrida o usada. Cada una de las bandas de 5GHz tiene por separado cuatro canales nonoverlapping[33]. El estándar 802.11 especifica OFDM[34] el cual genera 52 subportadoras para evitar las interferencias por propagación y efectos multipath[35], y soporta una velocidad máxima de datos de 54Mbps usando 64QAM, y velocidades menores de 6, 12, y 24 Mbps.

7.3.3 802.11g

La variante 802.11g es una extensión de la 802.11b y opera en la banda de 2.4GHz. Esta variante del estándar incrementa la velocidad de los datos a 54Mbps usando la tecnología OFDM, la cual es usada también en 802.11a. El alcance a 54Mbps es menor que el existente en los AP 802.11b, que operan a 11Mbps. Como resultado a esto, si una celda 802.11b es actualizada a 802.11g, los datos de mayor velocidad no podrán estar disponibles en todas las áreas.

A pesar de ésto, 802.11g ofrece velocidad de datos más altas y mayor tolerancia a multipath o interferencias por propagación que 802.11b. Aunque hay más interferencia en la banda de 2.4GHZ, 802.11g permite la elección del protocolo para lograr mejor alcance y ancho de banda y además es compatible con equipos con 802.11b.

7.4 Importancia de las bandas de frecuencia

Las tecnologías 802.11 pueden ser utilizadas en cuatro bandas de frecuencia sin licencia que se encuentran en dos bandas llamadas ISM y U-UNII. La banda ISM 2.4GHz tiene una señal intrínseca fuerte con un largo alcance y puede viajar a través de muros o paredes mejor que las bandas U-NII 5GHz.

Sin embargo, la banda U-NII permite que estén mayor número de usuarios en el mismo canal simultáneamente. La banda ISM 2.4GHz tiene un máximo de tres canales nonoverlapping (sin traslaparse) de 22MHz, mientras que la banda de 5GHz tiene 4 de 20 MHz en cada una de las bandas U-NII.

---

[33] Canales que no se traslapan o superponen.

[34] OFDM (*orthogonal frequency-division multiplexing):* técnica que permite la transmisión de diferentes flujos de información sobre un mismo canal de comunicación, es decir, la multiplexación. Divide el ancho de banda disponible en 52 partes llamadas portadoras o subportadoras, 48 de las cuales son usadas para datos y 4 para la portadora piloto que alinea la frecuencia en los receptores, y hace que cada una de estas subportadoras estén disponibles como distintos canales para la transmisión de datos. Ohrtman Frank, *Voice Over 802.11.* Artech House, Inc*, 2004*

[35] El efecto multipath o multitrayecto es causado principalmente por múltiples reflexiones de la señal emitida en superficies cercanas al receptor. Estas señales reflejadas (en edificios, vehículos, árboles, etc.), que se superponen a la señal directa son siempre más largas, ya que tienen un tiempo de propagación más largo y pueden distorsionar significativamente la amplitud y forma de la onda. http://www.isa.cie.uva.es/gps/GPSerrores.html

7.4.1 Explicación de las pérdidas por propagación

La parte más difícil de calcular un enlace tiene que ver con las pérdidas de propagación. En exteriores, las pérdidas en espacio libre son más faciles de enteder. La ecuación para pérdidas de propagación en exteriores puede ser expresada de la siguiente manera:
Pérdidas por propagación en espacio libre:

$$20 \log(d\,[\mathrm{m}]) + 20 \log(f[\mathrm{MHz}]) + 36.6\ \mathrm{dB}$$

En 2.4GHz, la fórmula se reduce a:

Pérdidas por propagación en espacio libre = $20 \log(d\,[\mathrm{m}]) + 40\ \mathrm{dB}$

Ésta fórmula se mantiene cierta tanto como se mantenga la línea de vista entre el receptor y el transmisor y se tenga el área suficiente alrededor del trayecto de propagación entre los dos puntos a interconectar, esta área es llamada Zona Fresnel[36].

Para espacios indoors, ésta fórmula es más complicada y depende de factores tales como los materiales de los cuales está hecho la edificación, los muebles, y también depende de los ocupantes. A 2.4GHz, se realizó una estimación la cual es expresada en la siguiente fórmula:

$$\text{Indoor path loss (2.4 GHz)} = 55\ \mathrm{dB} + 0.3\ \mathrm{dB}/d\,[\mathrm{m}]$$

A 5.7GHz, la fórmula es:

$$\text{Indoor path loss (5.7 GHz)} = 63\ \mathrm{dB} + 0.3\ \mathrm{dB}/d\,[\mathrm{m}]$$

7.4.2 Ganancia de la Antena Receptora

La ganancia de la antena receptora se añade al cálculo del enlace así como la de la antena transmisora, con esto se tiene una ganancia balanceada.

7.4.3 Margen del enlace

El margen de atenuación (Fade Margin) es la diferencia, en decibeles, entre la magnitud de la señal recibida a la entrada del receptor y el nivel mínimo o umbral de señal requerido para operaciones confiables. Entre más alto sea el margen de atenuación, más confiable será el enlace. El valor exacto del margen de atenuación requerido depende de la confiabilidad deseada en el enlace, pero debe tenerse en cuenta una buena regla general que sugiere que sea de 20 a 30dB. El margen de

[36] La propagación de las ondas de radio entre los dos puntos (Tx y Rx) no se propaga en línea recta, sino que debido a consideraciones de dispersión, la propagación se realiza en un área elíptica por encima y debajo de la línea recta del pasaje visual entre los dos puntos a interconectar. Esta zona elíptica se llama la Zona Fresnel. http://www.icamericas.net/Cases_Reports/Wi-FiBriefs/WiFi3_Spanish.pdf

atenuación es frecuentemente referido a SOM (System Operating Margin o Sistema Marginal de Operación)[37].

7.4.4 Pérdidas por difracción

La difracción ocurre cuando el radio del trayecto entre el transmisor y el receptor es obstruido por una superficie con irregularidades o bordes agudos. Las ondas resultantes de ésta obstrucción se presentan detrás del obstáculo. Cuando hay obstáculos en una situación LOS, las pérdidas por difracción pueden ser tan pequeñas como 6dB. Cuando hay obstáculos en situaciones NLOS[38], las pérdidas por difracción puede ir de 20 a 40dB.

7.4.5 Pérdidas por cableado y conectores

Las pérdidas por cableados están en función del tipo de cable que se esté usando, el grosor y la longitud de éste. Generalmente, el más grueso y mejor construido, tiene las menores pérdidas (y mayores costos).

Las pérdidas por coaxial son casi prohibidas en las bandas de 2.4 a 5.8 GHz. La mejor opción es usar la menor cantidad de cable coaxial que se pueda y ubicar el transceptor microondas lo más cerca posible de la antena preferiblemente en un ambiente cerrado. Las pérdidas por conectores se estima en aproximadamente en 0.5dB por conexión.

Un planificador de redes al calcular la capacidad de una red Vo802.11 debe tomar en cuenta las pérdidas por propagación usando las formulas que se dieron anteriormente. Conociendo la relación directa entre el ancho de banda y el número máximo de conversaciones simultáneas, puede determinarse el máximo número de usuarios Vo802.11 en un determinado AP.

7.5 Planes de reutilización de frecuencia para redes Vo802.11

Otro factor determinante en la escalabilidad de una red Vo802.11 es la reutilización de la frecuencia en un área de servicio dada. Si un proveedor o una empresa usan la misma frecuencia sobre un área extensa, habrá inevitablemente interferencias, que podrían limitar el número máximo de usuarios en la red Vo802.11 dada.

La implementación de la reutilización de la frecuencia es un factor importante en la determinación de la capacidad de la red Vo802.11. Los proveedores de telefonía móvil o celular han usado técnicas por años.

---

[37] SOM correlaciona la potencia del transmisor, el tipo de antena, la longitud de los cables coaxiales y la distancia. Así, podemos asegurar si nuestro sistema tiene un margen de potencia suficiente para alcanzar dicha distancia.

[38] NLOS (Nonline of sight): se refiere a situaciones en la que el radioenlace está obstruido.

7.5.1 Reutilización de frecuencia a 2.4GHZ

La banda de 2.5GHz tiene 11 canales amplios de 22MHz definidos desde 2.412GHz, incrementándose sucesivamente en 5MHz, hasta 2.462GHz. Tres canales nonoverlapping están disponibles – 1, 6 y 11- como se muestra en la figura 7.3.

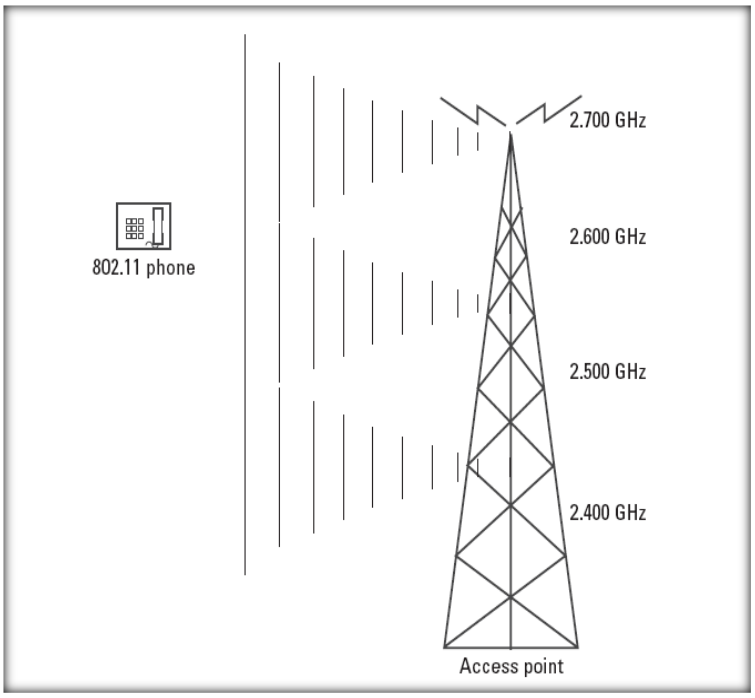


Figura 7. 3 La banda de 2.4GHz tiene tres canales nonoverlapping.

Estos tres canales nonoverlapping pueden ser utilizados en un patrón de reutilización 3 a 1 como se muestra en la figura 7.4**(39)**.

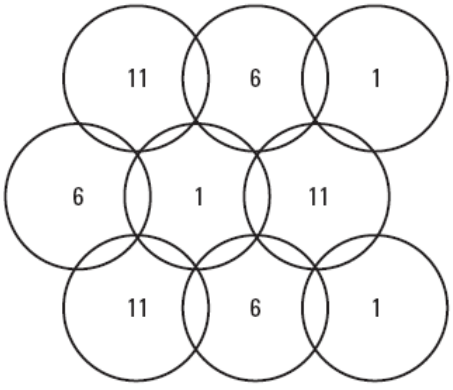


Figura 7. 4 Patrón de Reutilización 3 a 1.

[39] Tomado de Prasad, N., and A. Prasad, (eds.), *WLAN Systems and Wireless IP for Next Generation Communications,*Norwood, MA: Artech House, 2002

7.5.2 Reutilización de frecuencia a 5GHz

Las frecuencias centrales de los canales de operación están definidas en cada múltiplo de 5 MHz hasta 5GHz. Los canales válidos de operación son 36, 40, 44, 48, 52, 56, 60, 64,149, 153, 157 y 161. Las sub-bandas inferiores e intermedias de 802.11 acomodan 8 canales en un ancho de banda de 200 MHz y la banda superior acomoda 4 canales en uno de 100 MHz. Los centros de los canales extremos están a 30 MHz de los bordes de las bandas, esto para las bandas inferiores y medias de 802.11, y 20 MHz para la banda superior U-NII. Ver Figura 7.5.

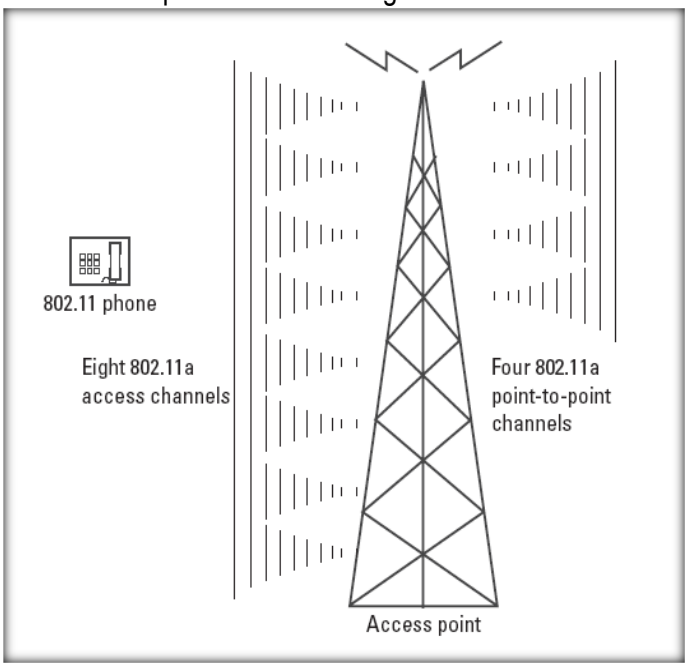


Figura 7. 5 Canales de operación válidos a 5 GHz

Los enlaces punto-a-punto operan en los cuatro canales: 149, 153, 157 y 161. Esto permite que cuatro canales sean usados en la misma área. Los AP de 802.11 y las tarjetas adaptadoras del cliente operan en los otros 8 canales: 36, 40, 44, 48, 52, 56, 60 y 64. Esto permite utilizar dos patrones de reutilización 4 a 1 como se muestra en la figura 7.6.

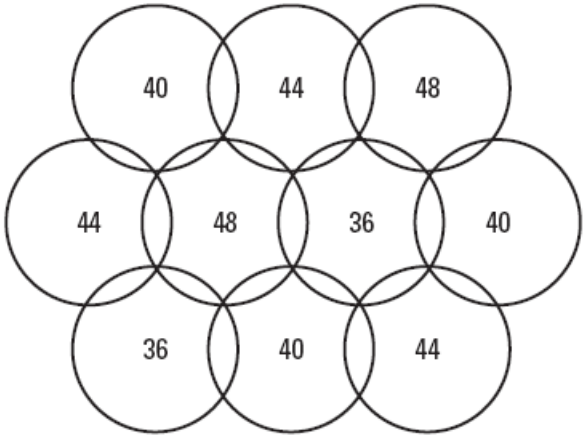


Figura 7. 6 Patrón de reutilización 4 a 1.

Con los rangos de baja y media frecuencia, puede tomarse ventaja usando el patrón de reutilización 7 a 1 donde quedaría un canal de sobra, como se observa en la figura 7.7. Este canal de sobra puede ser añadido luego como complemento para extender la cobertura o agregar capacidad en áreas que lo necesiten tales como salones de conferencias.

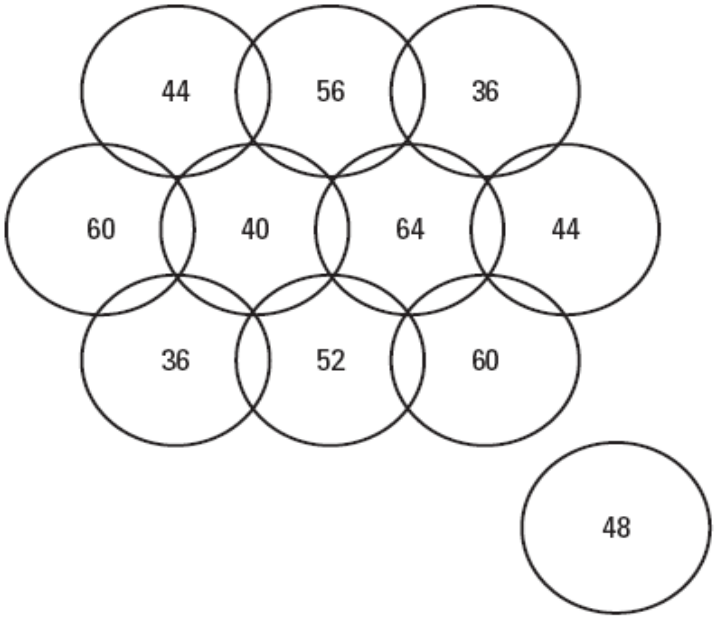


Figura 7. 7 El patrón de reutilización 7 a 1 y un canal libre.

7.5.3 Asignación de frecuencia

Para un proyecto sencillo con uno o dos APs, simplemente se asignan las frecuencias menos usadas en el sitio inspeccionado. Por otro lado, para proyectos más complejos que involucren tres o más APs, debe elegirse un patrón de reutilización de frecuencia para las frecuencias que se usaran en el proyecto, pero antes debe comenzarse con la parte más complicada del sitio inspeccionado y asignar las frecuencias. Debe evitarse el traslapamiento de canales si es posible. Si hay un área que tiene que tener un traslape, debe tomarse como un área que naturalmente requerirá la mayor capacidad.

7.6 Regulaciones del Ministerio de Comunicaciones

En cuanto a las regulaciones que rigen para el espectro en Colombia podemos mencionar que estas se encuentran consigandas en la **RESOLUCION NUMERO 000689 DE 2004 del Ministerio de Comunicaciones,** en el TITULO II: Disposiciones Técnicas, donde encontramos las condiciones operativas para las bandas de frecuencia, la potencia de transmisión y otros asepctos significativos que hay que tener en cuenta en caso de que se desee diseñar una red inalámbrica.

7.7 Limitaciones en AP

Actualmente, la mayor parte de la industria está enfocada en las aplicaciones empresariales donde aplicaciones Vo802.11 permitan al empleador recorrer el establecimiento y tener acceso a la red LAN inalámbrica con un teléfono 802.11, un portátil o un PDA. La pregunta entonces es ¿Cuántos usuarios VoIP inalámbricos pueden acceder al Access Point en un tiempo dado? Ante esto deben tenerse en cuenta las limitaciones en cuanto a escalabilidad que son dos: el ancho de banda disponible y la capacidad del Access Point para procesar las sesiones simultáneas.
Como resultado de estos dos factores, los vendedores de plataformas Vo802.11 incluyen APs adicionales que fueron diseñados específicamente para manejar voz, independientemente de los otros APs que corresponden a la red de datos. Algunos de estos APs especiales para voz pueden procesar de 10 a 12 conversaciones simultáneas. Una vez que a la empresa le parezca que la demanda de es mayor a 12 conversaciones simultáneas por AP, entonces puede añadir otro AP para cubrir aquella área que lo necesita (Salón de descanso, salón de conferencias, y otros).

7.8 Escalabilidad en VoIP Switching

En el lado cableado de la arquitectura Vo802.11, el próximo obstáculo con respecto a la escalabilidad es el ancho de banda de la conexión a los AP o switch inalámbrico. En la mayoría de los casos la restricción ocurrirá en los AP. Sin embargo, si, por ejemplo, un switch inalámbrico capaz de procesar sesiones simultáneas inalámbricas es conectado a un T1 (1.54Mbps), entonces no habrá suficiente ancho de banda para transportar las sesiones de voz y datos desde ese switch inalámbrico a la red IP.

La restricción más relevante en el lado cableado de las redes inalámbricas VoIP es la capacidad de procesamiento de llamadas del softswitch VoIP. Algunos vendedores de Vo802.11 ofrecen solo una interface a la tradicional PBX de TDM. En este caso, la escalabilidad es una función del bloqueo en la PBX de TDM. Otros vendedores (Cisco y Vocera, por ejemplo) ofrecen un IP-PBX que ejecuta y finaliza llamadas. El Call-Manager de Cisco, por ejemplo, puede manipular 512 llamadas simultáneas.

Si un proveedor de servicios contempla ofrecer 802.11 a un mercado masivo, ellos necesitarían un softswitch tipo "*carrier grade*"[40] o un IP Centrex con la habilidad de procesar millones de BHCAs[41]. Esto también puede expresarse en llamadas por segundo (CPS, calls per second). La principal limitación en el procesamiento de una llamada es la potencia de procesamiento de datos del servidor donde el softswitch está ubicado. El más importante de los switches Clase 5, para softswtiches, es el Lucent #5ESS, que puede procesar 800.000 BHCAs. Los nuevos softswitches en el mercado exceden los 5 millones de BHCAs. Por tanto, puede sostenerse desde la perspectiva de swtiching o conmutación, que VoIP inalámbrico es mucho más escalable que la tecnología de conmutación TDM usada en PSTN.

[40] Un sofswitch Carrier-Grade se refiere a un softswitch con características de un operador tradicional, como son con alta calidad, es decir, sin eco perceptible, retardos considerables, ni ruido en la línea; alta confiabilidad, para que al momento de descolgar el teléfono se escuche el tono de marcado y garantía en alcanzar el número deseado siempre que se haya marcado un número telefónico; y escalabilidad. http://www.cinit.org.mx/articulo.php?idArticulo=3
[41] BHCA (Busy Hour Call Attempts): Se refiere a la cantidad de llamadas en horas pico.

Lo que nos queda por decir en esta discusión es el hecho de que un Access Point 802.11 de una empresa puede manejar normalmente aplicaciones de datos y además sesiones VoIP inalámbricas. La mayoría de los AP fueron diseñados para manejar no más de 12 sesiones simultáneas. La principal limitación es la capacidad de procesamiento de los AP, que es una función de su potencia de procesamiento y los stack de TCP/IP asociado.

8 FUNCIONALIDADES Y APLICACIONES DE VO802.11

Imaginemos instalar una aplicación Vo802.11 en una WLAN corporativa. ¿Cómo hace el cliente para escuchar sus mensajes de voz, tener servicio de desvío de llamadas, conferencia telefónica, remarcado al último número y otros servicios típicos de una llamada? ¿Una red Vo802.11 es equivalente a un Walkie-Talkie?

Utilizar una red Vo802.11 para exclusivamente prestar servicios de voz no es comercialmente viable en la economía de las industrias. Si una red Vo802.11 se dispone a reemplazar una PBX de una empresa o la PSTN, debe ofrecer al menos características similares de la red a la cual va reemplazar.

Un inconveniente frecuente es tener la idea de que ninguna alternativa diferente a PSTN o una PBX empresarial puede ejecutar E911 o CALEA, términos que explicaremos posteriormente y que son esenciales en el país potencia mundial Estados Unidos, sin embargo los productos Vo802.11 que en este momento se encuentran en el mercado ya están realizando estas funciones. Los recursos de estas redes VoIP inalámbricas son capaces de brindar todas esas funcionalidades y servicios de la red de las redes tradicionales.

Las empresas que piensan implementar VoIP inalámbrico deben considerar también que servicios necesitará el personal de la empresa y de que forma serán proporcionados estos servicios. ¿La empresa continuará usando su PBC TDM existente o se actualizará a un IP-PBX o utilizará un IP Centrex para la conmutación y funciones asociadas mediante outsourcing?

Un impedimento que muchos proveedores de servicios y abonados han presumido con las tecnologías Vo802.11 es la percepción de que éstas no brindan las 3500 características que ofrece un switch Clase 5, o las 21 o muchas otras funciones disponibles con un PBX o un servicio Centrex.

La arquitectura descrita en este trabajo se aplica tanto para empresas como para aplicaciones "*carrier grade*"[42]. Un softswitch en una red Vo802.11 que esté reemplazando a un switch clase 5 o una PBX, utiliza servidores de aplicaciones y media servers[43] que hacen posible efectuar las mismas funciones que ofrece el swtich clase 5 o la PBX. Además, también brinda importantes funciones y servicios que no se encuentran en un switch clase 5, y que aún este switch no podría ofrecer. Estas nuevas características de Vo802.11 se basan en lenguajes de texto propios de estándares abiertos.

Es posible que, dada la flexibilidad que manejan éstos estándares para poder crear nuevas funciones y servicios en los softswitches, más adelante éstos puedan ofrecer más de las 3.500 funciones que ofrecería un switch clase 5. A continuación se dará un vistazo a como esas funciones y características son entregadas mediante una red Vo802.11 con softswitch.

[42] Aplicaciones con características de un operador tradicional, como son con alta calidad, es decir, sin eco perceptible, retardos considerables, ni ruido en la línea; alta confiabilidad, para que al momento de descolgar el teléfono se escuche el tono de marcado y garantía en alcanzar el número deseado siempre que se haya marcado un número telefónico; y escalabilidad.
[43] Servidores de medios.

8.1 Funcionalidades de la tradicional PSTN

Las funcionalidades de CLASS[44] (*Custom Local-Area Signaling Service, Servicio de señalización de área local personalizado)* son los servicios básicos disponibles en cada LATA[45] (*Local Access and Transport Area, Área de transporte y acceso local*).

Las funcionalidades y los servicios que proveen son una función de los switches clase 5 y las redes SS7, y por ser de alto margen producen a los proveedores del servicio fuertes ingresos.

Los servicios ofrecidos por un switch CLASS podemos clasificarlos en 2 portafolios: los servicios básicos y los servicios avanzados. El portafolio de servicios básicos incluye llamadas a 1+800/900, llamadas mediante Travel Cards, PINs, acceso a operadora, marcado rápido, línea de atención al cliente[46], identificador automático de llamadas, VPN's, llamadas mediante tarjetas de llamada y grabación de los detalles de llamadas (número origen, destino, duración, etc) o CDR (Call Detail Recording).

Por otro lado, el portafolio de servicios avanzados ofrece servicio de base de datos (servicio de números NXX, códigos de autorización, autorización tarjetas de llamadas, llamadas mediante tarjetas débito/prepago), enrutamiento y servicios de monitoreo (que incluye enrutamiento CIC[47], hora del día, identificador de llamadas, clase de servicio de monitoreo), redes empresariales, servicios de voz y datos (acceso a línea dedicadas, servicio ISDN PRI[48], servicios de Wideband[49], servicios conmutado de 56Kbps) y múltiples planes para realizar llamadas (enrutamiento con 10 dígitos, enrutamiento VPN con 7 + dígitos, marcaciones internaciones con 150 + dígitos, marcación rápida y línea de atención al cliente). La mayoría de los servicios mencionados han estado en los switches clase 5 desde hace muchos años.

La larga lista de funcionalidades mencionadas que ofrece PSTN es un indicio de la gran importancia que ya tiene dentro del mercado tradicional, además los proveedores de este servicio no renunciarán a dichas funcionalidades pues son de gran rendimiento ni además a los ingresos que les representa este rendimiento.

Una solución basada en softswitch se enfatiza en los estándares abiertos los cuales se oponen a los switches clase 4/5 que se caracterizan por ofrecer uno patentado y limitado. Los vendedores de softswitches hacen énfasis en que sus estándares abiertos están apuntando a independizar a los

---

[44] Grupo de opciones avanzadas que ofrecen las operadoras a sus suscriptores telefónicos como: desvío de llamadas, devolución automática de llamadas, identificación del llamante, timbrado diferenciado, rechazo de llamadas, etc. http://213.96.121.150/glosario.htm

[45] Es el área geográfica en que puede operar una compañía telefónica de telecomunicaciones, de acuerdo con los términos de su licencia. Área geográfica de discado telefónico atendida por una única compañía telefónica local. Las llamadas dentro de LATAs se denominan "llamadas locales". http://www.telsolutions.com.ar/glosarioim.htm, http://www.gratisweb.com/gulle79/glosario/l.htm

[46] Hotline: línea de servicio al cliente.

[47] CIC: Carrier Identification Code, Código de identificación del operador.

[48] PRI (Primary Rate Interface): Acceso primario Tipo de servicio de RSDI contratado normalmente por empresas de gran demanda, ya que soporta desde 23 canales B de 64Kbps y uno de D de 64Kbps. Para usuarios individuales está el tipo BRI (Basic Rate Interface o acceso básico que proporciona tan solo dos canales.

[49] Wideband: La banda intermedia permite generalmente una velocidad de entre 64 y 1.544 Mbps. Banda ancha es de 1.544Mbps en adelante.

proveedores de servicios de los vendedores y de la extensa y costosa manufactura de los switches tradicionales.

8.2 Funcionalidades y Señalización

Los servicios ofrecidos están en función de los switches clase 5 y la red SS7. A partir de esto surge la pregunta: ¿Cómo son transferidas las funcionalidades de una PSTN a una red basada en softswitches y switches clase 4/5? Primero que todo, la información generada en la PSTN debe ser transportada de forma transparente para el usuario a través de la red IP.
Es necesario tener en cuenta que es necesario el uso de estrategias que faciliten al proveedor de servicios extender sus novedades en productos rápidamente, pues el mercado se irá con el que le brinde las funcionalidades manera más pronta.

Los softswitch permiten que un proveedor de servicios entregar funcionalidades de su portafolio de servicios directamente al PC del cliente o en su teléfono IP. Los PC ofrecen mayor flexibilidad que un teléfono debido a la velocidad de la comunicación entre el suscriptor y el switch. Por ejemplo, *11 o alguna otra entrada al teléfono, es relativamente limitada si comparamos lo que puede ofrecernos una página Web. En teoría, si las 3500 funcionalidades de un switch clase 5 fueran catalogadas en un sitio Web y se hicieran más obvias y convenientes para usar por el suscriptor, entonces el proveedor de servicios podría sacar mejor provecho de sus servicios. Sin embargo, hasta la fecha, los switches clase 4/5 ofrecen solo un teléfono como interface entre el usuario y los servicios.

El SCE[50] (*service creation environment)* del softswitch es casi ilimitado y tiene el potencial para desplazar muchos de los switches presentes en el mercado. Un softswich tiene la capacidad de ofrecer los servicios existentes de los switches clase 5 y las redes SS7. Además, puede ofrecer una variedad de nuevas funciones potentes que superan el número de funcionalidades que puede brindar un switch clase 5.

8.2.1 SCE

El simple transporte de voz (Vo802.11, VoIP, TDM) se ha convertido en un producto de consumo masivo y ofrece márgenes de ingreso bajos a los proveedores del servicio. Sin todas las funcionalidades de los softswitches en una red Vo802.11, ésta no estaría en capacidad de generar los ingresos referentes a voz, que actualmente representan el 80% de los ingresos totales de un proveedor de servicio. La clave para tener altos ingresos en el mercado es la facilidad para la rápida creación de nuevos servicios. Los proveedores de servicios pueden diferenciarse de su competencia mediante servicios exclusivos lo que lograría el posicionamiento en el mercado y además excelentes entradas económicas. En el mercado tradicional, el ofrecimiento de esta clase servicios fue idea de los vendedores de switch (no más de 2 o 3 en el mercado norteamericano). Los vendedores de switch incentivaron a sus clientes expandiendo nuevos servicios de una manera rápida y flexible. Ahora, Sofswitch les cambia el escenario.

[50] SCE (*Entorno de Creación de Servicios):* Sistema de desarrollo software que permite la creación de nuevos servicios que luego van a ser desplegados en la red y la personalización de los ya existentes.

Gracias a sus interfaces de estándar abierto, softswitch permite a los proveedores de servicio la creación de nuevos servicios. La estructura de la arquitectura de softswitch hace posible a los proveedores de servicios integrar aplicaciones de sus vendedores de sofswitch o terceros vendedores o aún desarrollar sus propias aplicaciones. La opción de incluir API[51]s (*application program interface*) personalizadas en los softswitch permite al proveedor de servicio copiar solo los APIs de aquellos clientes a los que se les debe proveer un servicio dado en una ubicación dada. Además de la interoperabilidad entre gateways y sofswitches, los APIs están ajustados para permitir la creación por terceros de cualquier aplicación en el softswitch.

La creación de nuevos servicios significa el desarrollo de nuevos bloques de servicios y la implementación de estos nuevos servicios, se hace mediante herramientas comunes como un IDE[52] (*integrated development environment).* Lo más importante en esto, es la modularidad, es decir, que la aplicación pueda integrarse luego con las demás aplicaciones, más exactamente lo que esto significa es que un proveedor de servicio pueda combinar y juntar componentes de su red sin importar sin son de vendedores diferentes. Por ejemplo, si la plataforma de buzón de voz de un proveedor de servicio 802.11 no está trabajando al nivel que el proveedor de servicio desea, esta podría ser reemplazada por la plataforma de voz de la competencia. También, por ejemplo, los servicios de una red Vo802.11 podrían implementarse improvisadamente en una modalidad plug-and-play, reduciendo de manera drástica el tiempo y el esfuerzo que hubiera implicado desarrollar nuevos servicios, en caso de que no se hubiera cumplido la modularidad.

8.2.2 APIs

Las funcionalidades se ubican en la capa de aplicación de la arquitectura Vo802.11 de los sofswitch. La interface entre la capa de control de llamadas y aplicaciones específicas es la interfaz del programa de la aplicación. La creación de una aplicación y su interfaz en la arquitectura softswitch ocurre en el SCE. Los estándares abiertos mencionados incluyen APIs como Parlay, Jain, CORBA y XML. La figura 8.1 detalla la relación de APIs en el SCE.

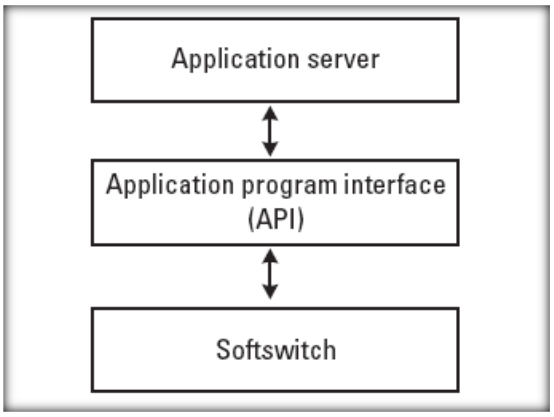


Figura 8. 1 Relación de APIs en el SCE

[51] API: se encarga de mantener el diálogo con la base de datos, para poder llevar a cabo el acceso y manipulación de los datos. La función que tienen las API's, es la de ser una interfaz entre las aplicaciones y las bases de datos, llevando ésta tarea unas veces a través de los clientes y otros a través del servidor de base de datos.

[52] IDE: Aplicación compuesta por un conjunto de herramientas útiles para un programador. Un entorno IDE puede ser exclusivo para un lenguaje de programación o bien, poder utilizarse para varios. Suele consistir de un editor de código, un compilador, un debugger y un constructor de interfaz gráfica GUI

8.2.3 API y los Servicios

Los estándares abiertos propios de estos APIs permiten que los servicios sean creados, administrados y desplegados sin requerir de infraestructuras nuevas o de la actualización de las existentes. Una de las mayores ventajas del uso de softswitch Vo802.11 es el hecho de que el protocolo de transporte (IP) también es usado para otra variedad de servicios como acceso Web, e-mail y mensajería instantánea. Los servicios avanzados de las redes Vo802.11 tendrán disponibles también estos servicios, brindando así simultáneamente telefonía y servicio de Internet.

Los servidores de aplicaciones son requeridos para interactuar con los protocolos no telefónicos y APIs para lograr ésta interacción. Debido a la complejidad y al overhead[53], los servicios de los APIs radican en el servidor de aplicaciones para realizar el procesamiento de los servicios avanzados.

El modelo del servidor de aplicaciones provee una arquitectura para servicios avanzados dentro una red Vo802.11 y bajo el dominio del proveedor de red. Por otro lado, los APIS como Parlay, JAIN y CORBA se ubican en redes híbridas y brindan servicios tanto adentro como fuera de la red y de la tecnología planteada por el proveedor.

8.2.4 XML

XML (Extensible Markup Language) corresponde a la nueva generación de HTML, es visto hasta ahora como el estándar mediante el cual se podrá intercambiar información entre entornos que no comparten una misma plataforma. XML 1.0 fue publicada en Febrero de 1998.

La administración de redes basadas en XML usa el Consorcio World Wide Web (W3C`s) XML para codificar los datos, el cual es un excelente mecanismo para la transmisión de datos complejos, utilizados para administrar las conexiones de redes. Establecer un API en una RPC (Remote Procedure Call) basada en XML, representa una manera simple de intercambiar este tipo de datos con algún dispositivo.

La recepción de datos en XML tiene una variedad de opciones para el manejo de los datos, como con el uso de herramientas basadas en estándares. XML es ampliamente aceptado en otros campos, y están emergiendo con gran rapidez herramientas comerciales para su manipulación.

8.3 SIP: Arquitectura para los servicios avanzados en Softswitched Vo802.11

En una red Softsiwtched 802.11 existen dos componentes, el servidor de aplicaciones y el media server. Estos proporcionan soporte para el servicio lógico avanzado, funciones de gestión y recursos especializados. Ver Figura 8.2.

[53] **Overhead** se refiere a la proporción de datos de control, encabezados, etc que se adhieren a los datos de usuario y que implican mayor consumo de ancho de banda. http://www.ice.go.cr/esp/serv/hogar/tele/internet/anchobanda.htm

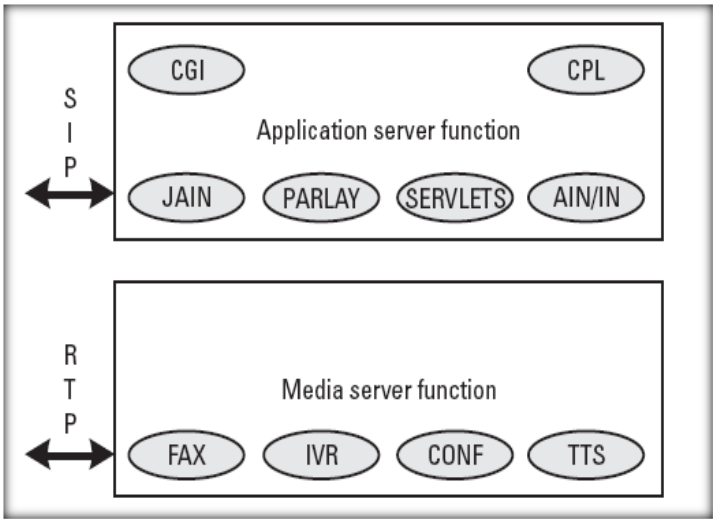


Figura 8. 2 Funciones del servidor de aplicaciones y el servidor de medios (media server)

Los servidores de aplicaciones proporcionan a los host variedad de servicios avanzados, y además brinda una estructura útil para la ejecución y administración de dichos servicios. Estos servicios hacen uso de las funciones de control de llamada mediante la infraestructura de la capa fundamental (subyacente) y también permite la integración de funciones como mensajería, asistencia y facsímil.

8.3.1 Servidores de Medios (Media Servers)

Un servidor de medios brinda recursos especializados tales como servicio de IVR (Interactive Voice Response), conferencias y facsímile. Los servidores de medios y de aplicaciones son independientes y pueden ser implementados en plataformas físicas separadas o en la misma plataforma. Un servidor de aplicaciones puede utilizar recursos en un servidor de medios para la ejecución de servicios avanzados, lo cual requeriría un acceso al media stream[54].

8.3.2 Servidores de Aplicaciones

Los APIs, como se describieron anteriormente, están localizados en el servidor de aplicaciones y proporcionan el acceso a los servicios fundamentales y a las funciones de conmutación. Mediante el uso de estos APIs, los servicios pueden ser fácilmente desarrollados para luego ser comercializados.

Al mismo tiempo, los modelos de llamadas de la telefonía tradicional y los protocolos TCAP/INAP pueden localizarse en este servidor, proporcionando así acceso a los servicios de telefonía del

[54] Un media stream (flujo de datos multimedia o simplemente flujo multimedia) consiste en datos multimedia obtenidos de un fichero local o adquiridos a través de la red, puede ser identificado por su localización y el protocolo utilizado para acceder a él. http://www.lcc.uma.es/~pinilla/JMFbnx2.pdf

estándar AIN/IN. Las entidades de control de llamadas de una red Vo802.11, tales como gateways, softswitches y teléfonos IP, sirven de agentes usuarios SIP. Los servidores de aplicaciones pueden actuar como entidades SIP, es decir, como agente de usuario, servidor de redirección, servidor proxy o controladores de llamada externos (agentes de usuario consecutivos). Todas las entidades SIP pueden comunicarse directamente o a través de servidores proxy.

Un servidor de aplicaciones requieren de un mecanismo de registro para poder informar a una entidad de control de llamada acerca de su disponibilidad. Alternativamente, una entidad de control puede estar configurada de forma estática con la dirección de un servidor de aplicaciones.

8.3.3 Arquitectura

Una vista funcional de la arquitectura Vo802.11 del softswitch se muestra en la figura 8.3, y en la tabla 8.1 se describen la función de cada una de las entidades.

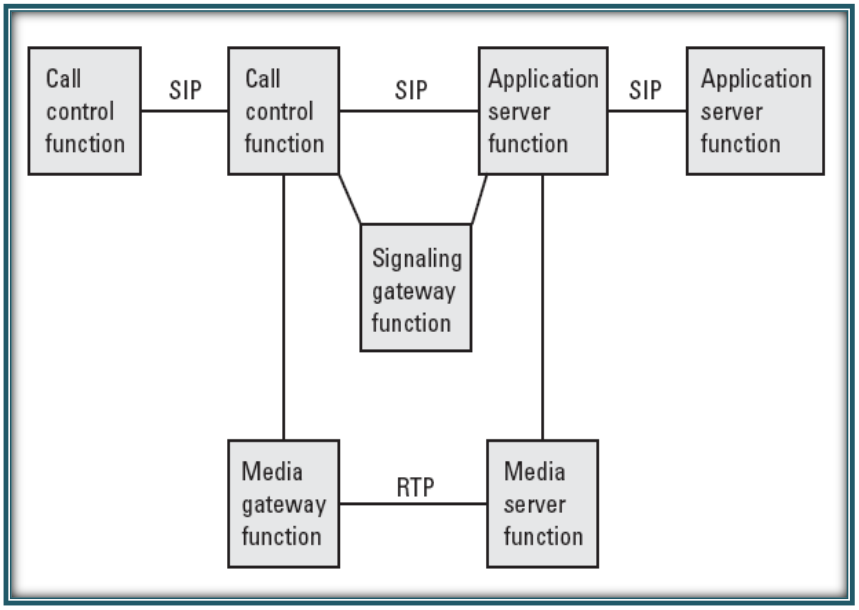


Figura 8. 3 Arquitectura de un softswitch con servicio avanzado

La introducción de un servidor de aplicaciones en una red Vo802.11 brinda servicios avanzados a las plataformas específicamente diseñadas. Mediante el uso de SIP como interface de aplicación entre la entidad de control de llamadas (softswitch) y el servidor de aplicaciones, cualquier protocolo estándar común puede ser usado para la comunicación entre todas las llamadas de control y las entidades de servicio de ejecución.

Estos nuevos servicios pueden ser implementados rápidamente con un mínimo impacto o si es posible sin ninguno en las redes más recientes.

Función	Descripción
Función de control de llamada	Puede proveer control de conexión, traslados y enrutamiento, administración del Gateway, control de llamada, administración del ancho de banda, señalización, aprovisionamiento, seguridad y genera la grabación de detalles de llamadas.
Función de media gateway	Proporcionar conversión entre recursos de circuitos conmutados (líneas, trunks) y la red de paquetes (IP, ATM), también realiza funciones de comprensión de voz, fax relay, cancelación de eco y detección de dígitos.
Función de señalización de gateway	Permite la conversión entre redes con señalización SS7 (enlaces SS7) y la red de paquetes, incluyendo protocolos como ISUP y TCAP.
Función de servidor de aplicaciones	Permite la ejecución y administración de servicios avanzados, se encarga de la interface de señalización de la función de control de llamada. También provee APIs para la creación de servicios.
Función de servidor de medios	Provee recursos multimedia especializados (IVR, conferencia, facsímil, anuncios, reconocimiento de voz, y se encarga de la interfaz efectiva de una función de media Gateway.

Tabla 8. 1 Funciones de las entidades de la arquitectura de servicios avanzados

Un servidor de aplicación utiliza una interface SIP, que proporciona acceso a la señalización de una llamada, mientras que un servidor de medios usa una interface RTP, la cual proporciona acceso al flujo multimedia. Los servicios en los servidores de aplicaciones hacen uso de los recursos de los servidores de medios. Con un servidor de aplicaciones y un servidor de medios, aquellos servicios que requieren acceso tanto a la señalización como al flujo multimedia pueden ser ejecutados.

8.3.4 Interface entre la entidad de control de llamadas y el Servidor de Aplicaciones

SIP sirve de interface entre las entidades de control (softswitch) y los servidores de aplicaciones por sus características de disponibilidad y capacidad de establecer, finalizar y administrar las sesiones entre 2 puntos terminales. Dentro de esto contexto, una entidad de control de llamadas tiene la capacidad de establecer y deshacer la ruta de señalización de llamadas a un servidor de aplicaciones, y viceversa.

Esto también incluye la habilidad de transmitir la información del usuario que hace la llamada y también del que la recibe, mantener y reanudar conexiones, transferir sesiones y establecer conexiones múltiples grupos. SIP es usado únicamente para señalización mientras que RTP es usado para transportar la multimedia. SIP retransmite la información necesaria para establecer una comunicación entre dos puntos terminales.

8.3.5 Interacciones que ejecuta el servidor de aplicaciones

Además de usar SIP como interface entre las entidades de control de llamadas y los servidores de aplicaciones, éste también sirve de interface entre los servidores de aplicaciones. Esto permite que los servidores de aplicaciones interactúen, es decir, que dos o más servicios avanzados que pertenezcan al mismo servidor o de diferentes, se relacionen e interactúen. Ante la habilidad del servidor de aplicaciones de delegar control a otro servidor de aplicaciones, puede introducirse un mecanismo para administrar de la interacción de determinadas funcionalidades. Hay que advertir

que esto comienza a ponerse crítico a medida que más servicios avanzados son introducidos dentro de la red.

La implementación de aplicaciones dentro de las redes Vo802.11 es un medio para lograr el despliegue de los servicios avanzados. Utilizando un protocolo estándar entre las entidades de control de llamadas y los servidores de aplicaciones, los servicios avanzados pueden ser rápidamente introducidos en los servidores de aplicaciones mediante expertos en dichas aplicaciones.

Los servidores de medios pueden ser usados para suministrar recursos especializados requeridos por muchos servicios avanzados. El servicio estandarizado de APIs y los modelos de llamadas AIN/IN, que se localizan en el servidor de aplicaciones, pueden ser usados para permitir que los promotores del servicio accedan a las funciones fundamentales de la red telefónica. Además, los servidores de aplicaciones pueden utilizar también los protocolos de Internet y los APIs para proporcionar servicios realmente convergentes.

8.4 Redes Vo802.11 y Requerimiento E911 y CALEA

8.4.1 E911

Un obstáculo para la implementación amplia de 802.11 en sus inicios en Estados Unidos que fue donde se originó, fue la de acoger las necesidades del servicio E9111 (Enhanced 911). Aunque los servicios 911 permiten la conexión rápida con el personal de emergencia, E911 tiene un paso adelante pues mediante el uso de ANI proporciona información sobre la locación desde la que se esté llamando al 911 y así determina que tipo de PSAP (service answering point) debe responder a la llamada.

En el entorno de una empresa, para E911 no solo es importante dirigir los servicios de emergencia a esa edificación en particular, sino indicar desde que parte de la edificación se originó la llamada. Típicamente, cuando alguien marca el 911 desde un escritorio, la información que llega por ANI (Automatic Number Identification) al PSAP (Public Safety Answering Point, que es donde está ubicado el operador 911) está basada en la compañía en general, un número de 7 dígitos que recibe es asociado a la PBX, sin embargo, no a la extensión del usuario que realiza la llamada. En una circunstancia de vida o muerte, puede tener consecuencias perjudiciales debido al retardo en la llegada al lugar exacto donde está la emergencia. Por esto, algunos gobiernos locales y de estado hacen que la incorporación de E911 sea obligatoria. Ante esto, muchos vendedores de sistemas de telefonía privada incorporan métodos mediante los cuales las PBXs satisfacen el anterior requerimiento.

Diferentes vendedores ofrecen diferentes estrategias para logara satisfacer las demandas de E911. La manera más sencilla es relacionar las terminales del circuito telefónico a un número o extensión. Esto lo hacen las PBX, donde cada jack de cada teléfono está asociado con una extensión en particular. Cuando una llamada al 911 es realizada desde una locación en particular, la PBX envía un número de 7 dígitos asociados con la extensión al router central de la oficina, que puede

entonces usar ANI para enrutar la llamada al correcto PSAP. El PSAP puede entonces enviar el personal de emergencia con la información obtenida del número que se registró.

Sin embargo, esto es un problema en una red Vo802.11, pues los circuitos conmutados de E911 no soportan el protocolo SIP y ningún otro protocolo VoIP. Esto es debido a que los teléfonos y dispositivos que funcionan con SIP u otro protocolo VoIP son aplicaciones flotantes que pueden asociarse con cualquier punto, su ubicación no es fija. Como un laptop, un teléfono SIP puede conectarse desde cualquier lado en una red empresarial, todo lo que necesita es una dirección IP válida.

Por tanto, como el teléfono puede estar en cualquier lado, entonces ¿Cómo podría la red E911 de la compañía telefónica obtener la información necesaria para poder atender la emergencia?

Varias propuestas con el fin de solucionar este problema han sido presentadas dentro de la comunidad SIP:

- Instalar chipsets GPS en los dispositivos terminales de usuario que puedan proporcionar la ubicación geográfica del usuario.
- Triangular la fuente de la llamada mediante Access Point Vo802.11.
- Que el usuario deba iniciar sesión en su dispositivo si se esté trasladando de una locación a otra.
- Que una implementación de SIP, haga uso de una red de voz cableada preexistente para crear otra: una red de únicamente VoIP, la IP PBX puede relacionar las terminales de los circuitos a líneas DID (direct inward delivery) de la misma manera que una PBX conmutada.

Cualquiera de las anteriores soluciones, "reparadoras" del problema del E911 tiene que ser estandarizada en los productos SIP de todos los vendedores, ya que E911 se volvió un requerimiento.

8.4.2 CALEA

¿Qué es CALEA? CALEA (*Communications Assistance for Law Enforcement Act)* es la Comisión de Acreditación para las Agencias que Aplican la Ley.

Esta es una ley de USA instaurada para la intervención de líneas telefónicas e intercepción de información desde una red de telecomunicaciones. CALEA data desde 1990 y no es un requerimiento de la PSTN. Otro concepto relacionado con CALEA es la intercepción legal, que sucede cuando un juez ha emitido una orden judicial que permita la intervención de un número telefónico dado. La orden de la corte es adjudicada a una agencia de fuerza policial que sucesivamente ejecuta la acción ordenada por la corte mediante el proveedor del servicio de telecomunicaciones. Seguramente hay muchas órdenes de la corte para diferentes agencias de fuerza policial para interferir un número telefónico dado.

La intervención telefónica se divide en dos categorías: intervención de detalles de llamada e intervención del contenido de la llamada. En el caso de intervención de detalles de llamada, el intervenidor o wiretap del teléfono graba los números de las llamadas entrantes y salientes, la fecha, la hora y la duración de cada llamada. Por otro lado, en el caso de intervenciones del contenido de llamada, el wiretap graba la llamada misma revelando el contenido de ésta. El sospechoso no debe detectar el wiretap. La intervención debe realizarse entonces dentro de la red y no en el Gateway del subscriptor. La intervención no debe ser detectable por ningún cambio en el ritmo de la llamada, funcionalidades u operación.
En la PSTN, las intervenciones legales se hacen en los switches clase 5 porque éste evita tener cualquier tipo de contacto con el Gateway del suscriptor. En lo concerniente a la industria, no es fácil instalar wiretaps en una red VoIP pues no usa switches clase 5.

Sin embargo, si es posible ejecutar intervenciones legales en una red VoIP. Las redes VoIP tienen separados los agentes de llamadas y los media gateways. El agente de llamada es responsable de todo el control de la llamada y es el elemento que recolecta todos los detalles requeridos en caso de una intervención telefónica. De ahí, que un softswitch podría ser una solución para una intervención de detalles de una llamada. El agente de llamada no ve el contenido, el cual está en el media stream RTP, por tanto si se necesitara una intervención del contenido de la llamada entonces la intervención debe hacerse en otra parte de la red.

CALEA se aplica a aquellos proveedores de servicios que ofrecen sus servicios como línea primaria. CALEA no aplica a proveedores de servicios que ofrecen servicios de voz como línea secundaria. Esto aplica a proveedores de servicios dentro de los Estados Unidos. No todos los mercados del mundo tienen estos requerimientos, un ejemplo es Colombia.

8.5 Aplicaciones Vo802.11 que se hicieron posibles con las funcionalidades de Softswitch

8.5.1 Web Provisioning

La disponibilidad WEB permite a los clientes aprovisionarse del servicio Vo802.11 vía Web. Los clientes pueden elegir sus propios productos y cuándo los servicios pueden iniciarse o cuando deben ser apagados.

Otras funciones disponibles en las redes Vo802.11 con softswitch son buzón de voz a email, e-mail de voz, calendario de voz (en el cual una llamada alerta sobre algún evento próximo), marcación por voz, enrutamiento de llamadas basada en eventos externos, marcarción desde el PC (en el cual el teléfono timbra y se establece la llamada), control remoto de llamadas (mediante el cual se puede desviar el teléfono incluyendo sus funcionalidades vía WEB), y control Web telefónico. Dentro de poco, programando mediante VoiceXML, se podrán crear nuevas funcionalidades en muy poco tiempo (de 20 minutos a algunos días).

8.5.2 Interface Web de Activación por Voz

Muchos proveedores de servicio celular ya proporcionar un servicio de marcación por voz, en el cual la voz del suscriptor interactúa con una base de datos de números telefónicos y selecciona uno para

ser marcado. La misma aplicación puede realizarse en las redes Vo802.11. EL vendedor de Vo802.11Vocera ofrece esta función. No hay teclado de marcado en los handsets de Vocera, sino que el marcado se hace mediante el comando de voz, conocido como marcación por voz.
Esta tecnología, dentro de poco introducirá al mercado lo que es la interacción con la Web mediante la voz. En vez de necesitar de un computador para interactuar con los sitios Web o revisar el e-mail, un suscriptor podría acceder a estos recursos mediante la interface de activación por voz. Muy pronto, un suscriptor podría obtener instrucciones de manejo mediante vía celular u obtener información sobre las acciones, las últimas noticias, reportes del clima, tal como los recibe en su e-mail.

9 Conclusión: Vo802.11 es el futuro de las comunicaciones de voz

El objetivo de este trabajo es vencer todas objeciones que han surgido frente al uso de 802.11 como un medio de transmisión de voz sobre el Protocolo De Internet. Primero, este trabajo expone la tesis de que Vo802.11 puede sustituir los elementos de la PSTN: acceso, conmutación, y transporte. Mediante el uso de 802.11 como un medio de acceso, pueden evitar los cables de cobre de la PSTN (pero no substituido a corto plazo). Mediante el uso de VoIP y un softswitch, pueden evitarse los switches Clase 4 y Clase 5 de la PSTN. Los IP backbones reemplazan las redes de larga distancia de la PSTN para evitar la infraestructura PSTN en sitios lejanos. La PSTN puede físicamente ser desplazada y reemplazada, el debate entonces cambia a tratar con las objeciones relacionadas con 802.11 y VoIP. Para que el uso de las aplicaciones Vo802.11 alcance una aceptación comercial generalizada, tendrá que estar claro para los fabricantes que la tecnología es sana y que las objeciones formuladas contra la tecnología pueden ser superadas fácilmente.

La común mala percepción sobre 802.11b era que su alcance máximo estaba limitado a 100m. Con la ingeniería apropiada esto pueden alcanzar una distancia de 32 Km de punto a punto. La puesta en marcha del protocolo 802.16 permite la extensión de 802.11b y protocolos asociados inalámbricos sobre una amplia área geográfica. Descendiendo desde una MAN hasta redes con ancho de banda más bajo, las redes inalámbricas pueden llegar a mercados residenciales y a otros de baja densidad. Las redes ad hoc peer-to-peer, debido a que no requieren una infraestructura costosa, son quizás el medio más rentable de ampliar una red inalámbrica. Estas tienen el potencial de ampliar la red aún más lejos. Aquí, los suscriptores son la red en sí.

Los sistemas Wi-Fi actúan como pequeños enrutadores, con cada nodo retransmitiendo a sus vecinos más cercanos. Se dan saltos de mensajes, en un modo peer-to-peer mediante su conexión banda ancha. Esto produce un sistema de telecomunicaciones banda ancha, que aunque es construido por separado, independiente, sirve para que los proveedores de servicios se interconecten el uno con el otro para un bien común. Dos cosas hacen que esta estructura peer-to-peer sea tan interesante. Primero, su aparición y el crecimiento son virales. Las telecomunicaciones virales son un fenómeno realmente nuevo. Segundo, su funcionamiento aumenta con el número de nodos. La ley de Metcalf declara que el valor de una red aumenta exponencialmente con la adición de cada nuevo nodo. En esta topología, más cantidad de nodos es igual a un mejor servicio. Además, autorizando a los suscriptores para "ser" la red, se reducen drásticamente los costos a los proveedores de servicio. La red también podría ser colectivamente adquirida.

Ahora en cuanto a seguridad, a finales de los años 90, hubo mucha cobertura en la prensa en cuanto a agujeros potenciales en las medidas de seguridad en 802.11. En muchos casos en aquellas historias, los gerentes de redes 802.11 fallaron al permitir solo las medidas básicas de 802.11. Esto es el equivalente de dejar la puerta abierta a alguien y tiene poco que ver con la seguridad de 802.11. Cualquier planificación de seguridad debería comenzar con una ecuación que incluyera lo que se desea asegurar (por ejemplo registros bancarios, inteligencia militar, bromas de la Tía Nancy, etcétera) y cuales serían los posibles amenazantes (servicios de inteligencia extranjeros, ladrones cibernéticos bancarios, el hacker ocasional, un vecino practicante de eavesdropping). La especificación 802.11 tiene un número de medidas, incluyendo WEP, para proteger una red de amenazas externas. Si el gerente de red no siente que WEP es adecuado para

proteger la red basado en la susodicha ecuación, otras medidas pueden ser añadidas a la red para aumentar el nivel de seguridad. Debería declararse que ninguna red es absolutamente segura. Con la adición de medidas de seguridad externas, las redes 802.11 pueden ser tan seguras como la mayoría de las redes cableadas. Asegurando la red 802.11, las probabilidades de que una conversación Vo802.11 sea escuchada o interceptada o se cometa algún fraude mediante alguna forma de intrusión de red se hacen bastante remotas. La seguridad deja una preocupación superior para los proveedores de servicio y vendedores de 802.11 por igual.

La especificación 802.11e está basada en más de una década de experiencia en el diseño de protocolos WLAN y fue construida para condiciones inalámbricas reales. Además, 802.11e es compatible con versiones anteriores de 802.11; los que significa que terminales que no son 802.11e pueden recibir flujos de aplicaciones con el QoS habilitado. Se describieron métodos para mejorar el QoS en redes 802.11 como la reducción de la latencia y de la pérdida de paquetes, lo cual arruina la calidad de la voz. Estas redes inalámbricas son potencialmente capaces de entregar QoS y calidad de voz comparable a las de la PSTN. Comentamos que RBOCs estaban perdiendo líneas telefónicas por los ofrecimientos de proveedores de servicio de telefonía celular en una cifra alarmante en el 2002. El servicio de telefonía celular se ha admitido que es de calidad inferior que el de la PSTN, sin embargo, los consumidores han preferido su servicio de telefonía celular que telefonía fija de la PSTN, debido a que ésta no ofrece facilidades de movilidad ni ventajas en el precio. El punto aquí es que últimamente, la QoS de la PSTN no el requerimiento principal de los clientes.

La PSTN tiene todas las de perder si debe competir con 802.11 en donde por ejemplo 802.11e entrega potencialmente QoS alto en cuanto a voz y datos ofreciendo una velocidad de 11Mbps (comparado con los planes DSL de 256Kbps de la PSTN). Dado que los consumidores sacrificarían QoS por precio y conveniencia, su línea de teléfono fija, no es difícil imaginar que cambiarían los servicios de la PSTN por servicios de 802.11e más eficientes debido al mayor ancho de banda, lo cual significa una mayor y mejor variedad de servicios (video por demanda, videoconferencia, etc). El QoS sobre una red de Vo802.11 ahora puede ser configurado para ser superior al de PSTN. Como con cualquier cuestión de ingeniería, vencer lo defectos es simplemente un asunto de buena ingeniería. Una buena ingeniería incluiría medidas como RSVP, Diff- Serv, y codecs modificados para Vo802.11. Con una correcta mezcla de los factores mencionados, las redes Vo802.11 pueden entregar una calidad de voz tan buena o mejor que la de la PSTN.

También se trabajó en el tema de la escalabilidad en aplicaciones VoIp inalámbricas. Existen limitaciones importantes en cuanto al ancho de banda, la asignación del espectro, la capacidad de los AP o switches inalámbricos de procesar y soportar múltiples sesiones, y finalmente, en la capacidad de procesar llamadas de los softswitch. Para que Vo802.11 reemplace a PSTN o TDM, debe estar en capacidad de ofrecer el mismo conjunto de funcionalidades disponibles en la PSTN o en la PBX de una empresa. Esto es posible mediante la arquitectura softswitch y lenguajes de programación como VoiceXML.

Dada la relativa flexibilidad en los switches clase 5 y 4, una red Vo802.11 debe ofrecer al menos las funcionalidades que los conmutadores de la PSTN ofrecen. Debido a la facilidad de crear y desplegar nuevas funciones en relación con las redes tradicionales, es posible que las soluciones

potentes de softswitch ofrezcan aún más que las 3.500 funciones disponibles en un switch clase 5. La facilidad de implementar estas nuevas funcionalidades facilita a los proveedores de servicios Vo802.11 buscar competir con los de la PSTN.

En resumidas cuentas pudimos observar cómo Vo802.11 interrumpirá la industria de la telefonía tradicional debido a que, primero, es más económica, gracias a su virtud de ser más barato para comprar y funcionar, una red de Vo802.11 marca una disminución significativa en cuanto a barreras para la entrada al mercado. Ya no es solo un servicio de voz de dominio exclusivo de un monopolio protegido por siglos. Esta disminución de las barreras de entrada permitirá que múltiples tipos de proveedores de servicio puedan ofrecer servicios de voz como competencia directa al monopolio de la telefonía tradicional. Esta lista de proveedores de servicio podría WISPs, ISPs, compañías de energía, municipios, empresas de televisión por cable, y nuevos principiantes del mercado.

Segundo, es más simple**,** considerando su evolución de 100 años, la PSTN es supremamente más compleja. Las COs son, en muchos casos, museos de historias de conmutación debido a que los operadores raras veces desechan los equipos de conmutación que todavía funcionan (y así disfruta de un muy generoso horario). Los proveedores de servicio Vo802.11 no cargarán con ese pasado. Más bien un Vo802.11 está basado en IP, lo que quiere decir que es mucho más eficiente para funcionar. La clave aquí está en sus normas abiertas a diferencia de los sistemas cerrados de la PSTN tradicional. Las normas abiertas permiten a un proveedor de servicio " mezclarse y combinar " los componentes de la red. Una red de voz sofswitch verdadera es dependiente de software, el cual puede ser actualizado fácilmente y con frecuencia.

Tercero, es más pequeña, pues una red de Vo802.11 puede ser fácilmente desplegada como un sistema modular aún por los proveedores de servicio más pequeños en economías en vías de desarrollo o rurales. Esto también aplica a campus universitarios o corporativos, o unidades múltiples en una empresa. Considerando que las operaciones de softswitch son geográficamente independientes del suscriptor, un proveedor de servicio puede proporcionar conmutación para suscriptores extensamente dispersados. La huella de un softswitch es menos del 10 % del de un switch Clase 5 manejando la misma carga de tráfico o aún mayor y no tiene que ser almacenado en una CO telco. Los Access Points praa el reemplazo de la PSTN por redes Vo802.11 son pequeños (no más que un metro cuadrado) y delgados. Esto hace que el despliegue sea rápido y barato.

Y por último, son más convenientes de usar. La PSTN puede ser condenada por la razón para la cual fue creada: voz. El negocio y mercados residenciales ahora exigen un acceso conveniente a servicios de datos de banda ancha. La PSTN no ofrece esta función de manera eficiente. Una red Vo802.11 ofrece servicios de datos fácilmente desplegables y manejados con banda ancha. Las redes Vo802.11, debido a la flexibilidad de su infraestructura softswitch, ofrecen mayor conveniencia debido a la serie extensa de funcionalidades y servicios que ofrece el sofswitch. Esto marca un nivel alto de conveniencia para el proveedor de servicio también. En vez de esperar años y gastar millones de dólares para ofrecer una nueva funcionalidad a un grupo de suscriptores, los proveedores de servicio a menudo pueden crear sus propias funcionalidades internamente y desplegarlos en asuntos de días.

10 BIBLIOGRAFIA

- **OHRTMAN**, **Frank**. VOICE OVER 802.11. Artech House, Inc. 2004.

Sitios Web.

- **Modelos de negocio y tecnología. Hot spot: aquí hay negocio.**
  http://www.microsoft.com/spain/empresas/tecnologia/hotspot.mspx
- **RSVP**
  http://www.danysoft.info/free/reservarecursos.pdf
- **API**
  http://es.wikipedia.org/wiki/Application_Programming_Interface
- **Proyecto Extremadura Wireless**
  http://wifiepcc.unex.es/modules.php?op=modload&name=Textos&file=index&serid=39.
- **Ataque Smurf**
  http://es.wikipedia.org/wiki/Smurf_ataque
- **PCS en Colombia**
  http://www.monografias.com/trabajos3/pcscolombia/pcscolombia.shtml
- **Diccionario Informático**
  http://usuarios.lycos.es/Resve/diccioninform.htm
- **Blackhaul**
  http://es.wikipedia.org/wiki/Backhaul
- **Redes Virtuales. Tipos VPN.**
  http://www.textoscientificos.com/redes/redes-virtuales/tipos-vpn
- **TLS**
  http://es.wikipedia.org/wiki/Transport_Layer_Security
- **Instituto Tecnológico Metropolitano Institución Universitaria. CCNA4 – Tecnologías WAN v3.1**
  http://www.itm.edu.co/doc/cisco/CCNA4%20Cisco.doc
- **Fuentes de Error en GPS. Efecto Multipath.**
  http://www.isa.cie.uva.es/gps/GPSerrores.html

- **QoS en VoIP**
  http://wiki.it46.se/doku.php?id=voip4d:capitulo_3:calidad_servicio

- **Doctorado QoS y Servicios. Evaluación de mecanismos de calidad de servicio en los routers para servicios multimedia.**
  http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

- **QoS. RSVP. DiffServ. MPLS.**
  http://www.mincomunicaciones.gov.co/minintranet/src/user_docs/conocimiento/desarrollosector/STVA(ProtocoloInternet62002)306.pdf

- **Estudio y configuración de la Calidad del Servicio.**
  http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf

- **Calidad de Servicio. QoS.**
  http://www.dsi.uclm.es/asignaturas/42650/PDFs/practica5.pdf

- **Federal Communications Commissionn Home Page**
  http://www.fcc.gov

- **Zona Fresnel**
  http://wndw.org/pdf/chapter2-es.pdf

- **Transmisión y Control de Errores. DHSS. FHSS. CRC. Otros.**
  http://www.info-ab.uclm.es/asignaturas/42638/pdf/cap2.pdf

- **WNI México. Soporte. Línea de vista.**
  http://www.wni.com.mx/linea_vista.htm

- **WiFi.**
  http://www.icamericas.net/Cases_Reports/Wi-FiBriefs/WiFi3_Spanish.pdf

- **Chapter i--federal communications commission. Part 15--radio frequency devices.**
  http://www.access.gpo.gov/nara/cfr/waisidx_01/47cfr15_01.html.

- **VoIP: Una nueva alternativa en Telefonía.**
  http://www.cinit.org.mx/articulo.php?idArticulo=3

- **Glosario de términos de telecomunicaciones.**
  http://213.96.121.150/glosario.htm

- **Glosario de términos de telecomunicaciones.**
  http://www.telsolutions.com.ar/glosarioim.htm

- **Glosario de términos de telecomunicaciones.**
  http://www.gratisweb.com/gulle79/glosario/l.htm

- **QoS. Calidad de Servicio DiffServ. MPLS.**
  http://telematica.cicese.mx/i2/presentaciones/Primavera_2k1_CUDI_parte_2_files/frame.htm

- **El ABC de las redes inalámbricas [WLANs]**
  http://www.eveliux.com/articulos/wlans.html

- **Redes Locales Inalámbricas**
  http://www.unincca.edu.co/boletin/indice.htm

- **Seguridad en Redes 802.11x**
  http://www.atc.uniovi.es/inf_med_gijon/3iccp/2006/trabajos/wifi/

- **NEBS**
  http://www.tech-faq.com/lang/es/nebs.shtml

- **DSO**
  http://cofetel.gob.mx/cofetel/html/4_tar/bestphone/5209.pdf
  http://isc.mx.tripod.com/tecnologiasdecom.htm
  http://www.todoexpertos.com/categorias/tecnologia-e-internet/redes-de-computadores/respuestas/37245/direccion-mac
  http://www.com.uvigo.es/asignaturas/scvs/trabajos/curso9900/tdm/Contenido.html
  http://html.rincondelvago.com/red-de-telecomunicaciones-banobras.html
  http://www.eveliux.com/mx/index.php?option=content&task=view&id=178

- **Aplicaciones Elásticas**
  http://ants.dif.um.es/~humberto/asignaturas/02ct/temas/tema1.pdf

- **RESOLUCION NUMERO 000689 DE 2004 (de Colombia).**
  http://www.mincomunicaciones.gov.co/mincom/src/user_docs/Archivos/normatividad/2004/Resolucion/R00689d2004.pdf