UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS

FACULTAD INGENIERÍA ELÉCTRICA

DEPARTAMENTO DE ELECTRÓNICA Y TELECOMUNICACIONES

Calidad de servicio en redes VoWLAN con interoperabilidad a redes móviles

Tesis presentada en opción al Título Académico de Máster en Telemática

Maestría en Telemática

Autor: *Ing. Roberto Vázquez Sánchez*

Tutor: *Dr. C. Félix F. Álvarez Paliza*

Consultante: Dr. C. Vitalio Alfonso Reguera

Santa Clara, 2016

Hago constar que la presente Tesis en Opción al Título Académico de Máster en Ciencias Telemáticas fue realizada en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de Maestría en Telemática, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____ _____

Ing. Roberto Vázquez Sánchez Fecha
Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Ing. Roberto Vázquez Sánchez Fecha
Autor

_____ _____

Dr. C. Vitalio Alfonso Reguera Fecha
Jefe del Departamento

_____ _____

Dr. C. Félix F. Álvarez Paliza Fecha
Coordinador de la Maestría en Telemática

PENSAMIENTO

"…la grandeza del hombre está precisamente en querer mejorar lo que es (…) Por ello, agobiado de penas y de tareas, hermoso dentro de su miseria, capaz de amar en medio de las plagas, el hombre sólo puede hallar su grandeza, su máxima medida en el Reino de este Mundo."

Alejo Carpentier, 1949.

DEDICATORIA

A mis padres, por su ejemplo y ayuda incondicional.

A mi esposa, por su apoyo y por todo lo que compartimos juntos.

A mi hija, por entender, a pesar de su corta edad.

AGRADECIMIENTOS

Primeramente, agradecer a mi familia y en especial a mis padres y a mi esposa, por el gran apoyo durante todo este tiempo en el que fui universitario de nuevo, y me vi forzado a desatender algunos asuntos domésticos, en aras de culminar exitosamente la maestría.

Hago extensivo este agradecimiento a esos amigos (algunos muy recientes, otros no tanto), que de forma directa o no, contribuyeron a la realización de este trabajo.

Finalmente, agradezco por su preocupación y profesionalidad, al claustro de profesores de la Maestría de Telemática de la Universidad Central "Marta Abreu" de Las Villas, y en especial a mi tutor y coordinador de la maestría Dr. C. Félix F. Álvarez Paliza, a mi consultante Dr. C. Vitalio Alfonso Reguera, y a mi profesora de toda la vida Dr. C. Ileana Moreno Campdesuñer.

RESUMEN

La Calidad de Servicio (QoS) es el requerimiento más importante a la hora de dar soporte a aplicaciones exigentes como la voz, debido a sus características de tiempo real. Las nuevas tecnologías de *Wireless* LAN que han ido surgiendo en los últimos años han ido incorporando mecanismos para dar soporte a este y otros tipos de tráfico como el video, este es el caso de las nuevas extensiones de WiFi enfocadas a la calidad de servicio (QoS), la seguridad, la movilidad, e incluso la interoperabilidad con otros tipos de redes. A esto se añade el amplio despliegue que están teniendo las redes WiFi tanto en el sector empresarial, como en el sector público y doméstico, y la prevalencia de *smartphones* y *tablets* como terminales de acceso, los cuales tienen la capacidad de conectarse prácticamente a cualquier red inalámbrica. En este trabajo se definen cuáles son los parámetros que influyen de manera determinante en la QoS, al soportar servicios VoIP en las redes WiFi, además se demuestra que es posible lograr la convergencia e interoperabilidad entre estas y las redes móviles.

Palabras Clave: Voz sobre redes inalámbricas (VoWLAN), Voz sobre IP (VoIP), Calidad de servicio (QoS), Interoperabilidad, EAP-SIM/AKA.

ÍNDICE

Contenido

GLOSARIO DE TÉRMINOS

3GPP	*Third Generation Partnership Project*
AAA	*Authentication, Authorization and Accounting*
AC	*Access Category / Access Controller*
ACK	*Acknowledgement*
AES	*Advanced Encryption Standard*
AIFS	*Arbitration InterFrame Space*
AKA	*Authentication and Key Agreement*
AP	*Access Point*
BRAS	*Broadband Remote Access Server*
CAC	*Call Admission Control*
CAP	*Controlled Access Phase*
CAP-WAP	*Control and Provisioning of Wireless Access Points*
CCKM	*Cisco Centralized Key Management*
CCMP	*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*
CFP	*Content Free Period*
CP	*Content Period*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
CW	*Contention Window*
DAC	*Dynamic Admission Control*
DCF	*Distributed Coordination Function*
DHCP	*Dynamic Host Configuration Protocol*
DIFS	*DCF InterFrame Space*
DSSS	*Direct Sequence Spread Spectrum*
EAP	*Extensible Authentication Protocol*
EAP	*Extensible Authentication Protocol*
EAPOL	*Extensible Authentication Protocol over LAN*
EDCA	*Enhanced Distributed Channel Access*
EDCF	*Enhanced Distribution Coordination Function*
GSM	*Global System for Mobile communications*
HC	*Hybrid Coordinator*
HCCA	*HCF Controlled Channel Access*
HCF	*Hybrid Coordination Function*
HEMM	*HCCA-EDCA Mixed Mode*
HLR	*Home Location Register*
HSDPA	*High Speed Downlink Packet Access*
HSPA	*High Speed Packet Access*
HSS	*Home Subscriber Servers*
HSUPA	*High Speed Uplink Packet Access*
IBSS	*Independent Base Service Set*
IEEE	*Institute of Electrical and Electronics Engineers*

IMSI	*International Mobile Subscriber Identifier*
IP	*Internet Protocol*
KPI	*Key Performance Indicators*
LAN	*Local Area Network*
LTE	*Long Term Evolution*
MAC	*Media Access Control*
NMS	*Network Management System*
nQSTA	*non Quality of Service aware Station*
OFDM	*Orthogonal Frequency Division Multiplexing*
PC	*Point Coordinator*
PCF	*Point Coordination Function*
PE	*Provider Edge*
PMK	*Pairwise Master Key*
PoE	*Power over Ethernet*
QoE	*Quality of Experience*
QoS	*Quality of Service*
QSTA	*Quality of Service aware Station*
RADIUS	*Remote Authentication Dial-In User Service*
RF	*Radio Frequency*
RRM	*Radio Resource Measurement*
SIFS	*Short Interframe Space*
SIM	*Subscriber Identity Module*
SIP	*Session Initiation Protocol*
SNR	*Signal to Noise Ratio*
SSID	*Service Set Identifier*
TDM	*Time Division Multiplexing*
TID	*Traffic ID*
TKIP	*Temporal Key Integrity Protocol*
TLS	*Transport Layer Security*
TS	*Traffic Stream*
TXOP	*Transmision Opportunity*
USIM	*Universal Subscriber Identity Module*
VoIP	*Voice over IP*
VoLTE	*Voice over LTE*
VoWiFi	*Voice over Wi-Fi*
VoWLAN	*Voice over Wireless LAN*
WiMax	*Worldwide Interoperability for Microwave Access*
WLAN	*Wireless Local Area Network*
WMM	*Wi-Fi Multimedia*
WPA	*WiFi Protected Access*
WPA2	*WiFi Protected Access 2*

INTRODUCCIÓN

La Calidad de Servicio (*Quality of Service*, QoS) en redes de telecomunicaciones suele implementarse por medio de mecanismos para dar un tratamiento preferente a unas clases de tráfico frente a otras, sobre todo a la hora de tratar con tráfico multimedia, el cual presenta requisitos de ancho de banda y tiempo real, en el caso de redes basadas en la conmutación de paquetes como es el caso de las redes IP se hace necesario velar por otros parámetros como son la latencia o retardo, la perdida de paquetes y el *jitter*, que afectarían no tanto el ancho de banda, pero si los requerimientos de tiempo real, imprescindibles en el caso de la voz.

Aunque aún subsisten muchas aplicaciones basadas en tecnología TDM, el mundo actual de las telecomunicaciones está evolucionando a un transporte y acceso basado completamente en redes IP, y dentro de estas, las redes de acceso inalámbricas le están ganando terreno a las cableadas, debido a su movilidad, versatilidad, fácil instalación y bajo costo con respecto a las soluciones cableadas. Por otra parte, mientras los dispositivos de acceso cableados continúan siendo rígidos y diseñados para una tecnología de acceso específica, su contrapartida móvil (*smartphones* y *tablets*), presentan diseños atractivos para el cliente, *software* de alto nivel que permite implementar diferentes servicios y prestaciones, portabilidad y movilidad, e incluso interoperabilidad, ya que son capaces de conectarse a prácticamente cualquier tecnología de red inalámbrica.

Para las modernas redes de acceso inalámbrico el ancho de banda ya no es una limitante, las tecnologías de telefonía celular de tercera generación haciendo uso de HSPA logra velocidades de acceso de 14,4 Mbps en el *downlink* y 5.7 Mbps en el *uplink*, mientras que las redes de cuarta generación que están en pleno desarrollo, haciendo uso de LTE, soportan anchos de banda de hasta 150 Mbps en bajada y de 50 Mbps en subida, además de menores latencias (de unos 10-20 ms), mejorando notablemente la experiencia de usuario para todo tipo de servicios. Este tipo de redes fueron diseñadas teniendo en cuenta los requerimientos que exigía soportar la voz, heredando la calidad de servicio de su predecesor, las redes de segunda generación (GSM), la cual fue creada solamente para soportar voz con calidad comparable a la telefonía fija. En cambio, las redes de área local inalámbricas (*Wireless* LAN), y particularmente las redes WiFi (IEEE 802.11), fueron diseñadas para proveer intercambio de datos entre usuarios cercanos y acceso a internet, pero no para soportar servicios de voz (VoIP). Sin embargo, el gran éxito que ha tenido este tipo de redes ha provocado su desarrollo y evolución a nuevos estándares que dotan a WiFi de mayores anchos de banda, densidad de usuarios, seguridad de acceso, interoperabilidad, y por supuesto, calidad de servicio [1].

Este trabajo describe las referencias teóricas para dotar de calidad de servicio a las redes WiFi, y más específicamente, los mecanismos necesarios para soportar tráfico de voz. Además se propone una topología, usando el *Core* de la Red Móvil, para la implementación de este servicio, detallando en particular como sería el proceso de autenticación de los usuarios. Las técnicas adoptadas para garantizar la calidad de servicio en el resto de la red de telecomunicaciones, así como la implementación de los servicios de voz sobre IP, no

serán tratados en este trabajo. Para ello se plantea el siguiente **problema científico**: *¿Cómo lograr calidad de servicio (QoS) sobre redes WiFi, para poder soportar servicios de voz sobre IP (VoIP), e interoperabilidad con redes móviles públicas?* Lo que nos lleva a que el **objeto de investigación** sea las redes WiFi, y el **campo de acción** la calidad de servicio en redes WiFi. Para dar solución al problema planteado, el **objetivo general** de la investigación es: *Proponer un diseño que garantice calidad de servicio (QoS) para soportar Voz sobre IP en redes WIFi, que posibilite la interoperabilidad con redes móviles*. Para alcanzar este objetivo general, se deben completar los siguientes objetivos específicos:

1. Establecer los referentes teóricos sobre la calidad de servicio en las redes WiFi.
2. Diseñar propuestas de red VoWLAN empleando criterios para lograr QoS.
3. Evaluar el desempeño de redes VoWLAN con interoperabilidad a redes móviles.

Con vistas a organizar la investigación, se plantean las siguientes **tareas científicas**:

1. Análisis de la bibliografía para fundamentar las bases teóricas de la calidad de servicio en las redes WiFi.
2. Determinación de los parámetros de QoS en redes WiFi.
3. Selección de escenarios de redes WiFi con calidad de servicio.
4. Evaluación de distintas arquitecturas.
5. Valoración de distintas redes con el objetivo de medir el desempeño de la QoS.

Este trabajo contribuye, en el orden teórico, metodológico y práctico, a la sistematización de los conocimientos sobre redes WiFi y en particular, de las aplicaciones basadas en la voz sobre IP, al describir los criterios de diseño que garantizan calidad de servicio (QoS) para soportar Voz sobre IP en redes WiFi; esto posibilitará la implementación de aplicaciones VoWLAN y su interoperabilidad con redes móviles públicas, lo cual favorece a operadores como ETECSA, al permitirles brindar sus servicios a un mayor número de clientes, con el consiguiente beneficio económico y social.

La investigación se desarrolló utilizando los siguientes métodos científicos:

El histórico lógico el cual permite contextualizar el problema de investigación, sus antecedentes y desarrollo.

El analítico-sintético ya que es necesario trabajar cada estándar y sus relaciones y luego lograr la integración de las partes constitutivas del objeto de investigación para lograr el objetivo planteado.

El Inductivo-Deductivo que posibilitó establecer los parámetros con respecto al diseño de experimentos que permitieron la evaluación de aplicaciones de voz sobre IP en escenarios concretos.

La modelación mediante la cual se crean abstracciones con vistas a explicar la realidad. El modelo como sustituto del objeto de investigación. Opera en forma práctica o teórica con un objeto, no en forma directa, sino utilizando cierto sistema intermedio, auxiliar, natural o artificial, en este caso, la simulación.

El informe está formado por la introducción, el desarrollo, las conclusiones, seguido de las recomendaciones, y las referencias bibliográficas y anexos. El desarrollo está estructurado en tres capítulos, en el primero se describen los diferentes estándares involucrados, sus características, factibilidad de su uso para el cumplimiento del objetivo general, además se realiza un estudio del estado de la tecnología WiFi en el mundo, y su implementación y perspectivas en Cuba.

En el capítulo dos, se definen los mejores criterios de diseño para la implementación de redes Wifi con QoS para soportar VoIP, en espacios cerrados y en espacios abiertos, haciendo particular énfasis en los escenarios públicos; también se hace un análisis crítico de la implementación de las zonas de acceso WiFi desplegadas por ETECSA.

En el tercer y último capítulo se realiza la simulación de escenarios VoWLAN, empleando las técnicas de QoS propuestas en el capítulo 2, y se hace una propuesta de implementación de redes VoWLAN en un escenario real, con interoperabilidad a la red móvil.

CAPÍTULO 1. Caracterización de las tecnologías de redes VoWLAN

1.1 Calidad de servicio en redes WiFi

Para soportar servicios de voz sobre IP (VoIP) usando como red de acceso *Wireless* LAN del tipo IEEE 802.11, más conocidas como WiFi, es necesario dotar a estas de Calidad de Servicio (QoS). Para ello, Wi-Fi Alliance, publicó en el 2004 un certificado para soportar aplicaciones multimedia con calidad de servicio en redes WiFi o WMM [2] (Wi-Fi Multimedia), esto sirvió como anticipo al estándar IEEE 802.11e [3], aprobado en el 2005 por el LAN/MAN *Standards Committee* de la *IEEE Computer Society*, el cual define los mecanismos para lograr calidad de servicio en este tipo de redes, además de introducir enmiendas a numerosas evoluciones del estándar original. El estándar IEEE 802.11n [4] sale a luz en el 2009, siendo el más utilizado en la actualidad, y este ya incluye los requerimientos para QoS que habían sido especificados en 802.11e.

El entorno inalámbrico es particularmente agresivo para aplicaciones multimedia y en especial para la voz, debido a su variabilidad con el tiempo, por lo que satisfacer la QoS resulta imposible en todos los casos, esto obliga a la implementación de restricciones de máximo retardo o latencia y máxima varianza en el retardo o *jitter*. La pérdida de paquetes resulta prácticamente inadmisible, ya que las condiciones de tiempo real exigen que los paquetes perdidos sean descartados, ya que sería inútil retransmitirlos. En cuanto al ancho de banda, si bien es cierto que es fundamental en aplicaciones multimedia como el video, en el caso de la voz esto no es una exigencia, ya que en la actualidad existen numerosos códecs que garantizan calidad en la voz, reduciendo notablemente el ancho de banda necesario; por otra parte los estándares de WiFi usados en la actualidad (IEEE 802.11a/b/g/n) han mejorado la velocidad de acceso a 11, 54 y hasta 100 Mbps.

1.1.1 Parámetros de calidad de servicio

En las redes basadas en tecnología IP, ocurren diferentes problemas que repercuten en la calidad de servicio. Algunos de ellos se mencionan a continuación:

Retardos o Latencia: Tiempo que tarda un paquete en llegar desde la fuente al destino. Puede ocurrir que los paquetes tomen un largo período en alcanzar su destino, debido a que pueden permanecer en largas colas o tomen una ruta menos directa para prevenir la congestión de la red. Un retardo excesivo puede inutilizar aplicaciones VoIP.

Paquetes sueltos: Los *routers* pueden fallar en liberar algunos paquetes si ellos llegan cuando los buffers ya están llenos. Algunos, ninguno o todos los paquetes pueden quedar sueltos dependiendo del estado de la red, y es imposible determinar qué pasará de antemano. La aplicación del receptor puede preguntar por la información que será retransmitida posiblemente causando largos retardos a lo largo de la transmisión.

Jitter: Los paquetes del transmisor pueden llegar a su destino con diferentes retardos. Un retardo de un paquete varía impredeciblemente con su posición en las colas de los *routers* a

lo largo del camino entre el emisor y el destino. Esta variación en el retardo se conoce como *jitter* y puede afectar seriamente la calidad de la voz y el vídeo.

Errores: En ocasiones, los paquetes son mal dirigidos, combinados entre sí o corrompidos cuando se encaminan. El receptor tiene que detectarlos y cuando el paquete es descartado, pregunta al transmisor para repetirlo.

Pérdida de Paquetes: Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían. La Pérdida de Paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor, por lo que los eventos vistos anteriormente pueden desencadenarla, en adición, en las redes inalámbricas puede estar causada por pobre nivel de señal, limitaciones de rango e interferencias provocadas por otros dispositivos compartiendo el mismo rango de frecuencias. Debido al uso de códecs en las aplicaciones VoIP, la pérdida de paquetes afecta sensiblemente la inteligibilidad de la voz.

1.1.2 Requerimientos de los servicios según su naturaleza

La transmisión de datos, como pueden ser ficheros de un servidor, correo electrónico o páginas web, es un tráfico poco exigente. El servicio demanda la mayor velocidad de transmisión y la menor pérdida de paquetes que sea posible, una degradación de estos parámetros producto de alguna interferencia externa, o simple colisión entre clientes, provocaría alguna pérdida. El usuario lo que apreciará es disminución en la velocidad de acceso a los datos, pero a no ser que esta se reduzca por debajo de un cierto umbral que la haga inaceptable, no habrá una mayor exigencia.

El tráfico de video añade requerimientos extra, los cuales están motivados porque el video ha de ser mostrado en el instante que corresponde. El hecho de que los datos lleguen más despacio, en una página web influye en que tarde menos o más en bajar, pero los fotogramas del video se han de mostrar secuencialmente, o el video no será reproducido de forma correcta, apreciándose cuadros, sonido deficiente (cortes o chasquidos), aceleraciones del vídeo, pausas, etc. Además de una velocidad de transmisión mínima, dependiendo de la codificación y la calidad de la imagen, para poder transmitir el video con fiabilidad, y una ausencia de pérdida de paquetes, hará falta un cumplimiento estricto de otros parámetros como el *jitter*, la latencia, la duplicación y reordenación de paquetes y la emisión en ráfagas.

Las necesidades del tráfico de voz son análogas a la del video, puesto que se trata de un servicio que no permite pérdida de información y que precisa de una temporización muy estricta. Sin embargo, existen diferencias con respecto al servicio de video. La primera es que aunque es necesario que se garantice un ancho de banda y que este dependerá del sistema de codificación de la voz que utilice el sistema, esta velocidad de transmisión será mucho menor que en caso del video. Otra diferencia a tener en cuenta es que la latencia es un parámetro importante para la voz, si esta es alta, la red no será apta para conversaciones de voz, pues un retraso mínimo es percibido muy negativamente por los usuarios. De manera general, mientras en el video podemos convivir con un umbral bajo de tasa de

perdida de paquetes, sin que se pierda sensiblemente la información que se recibe aunque se afecte la calidad de la imagen, en el caso de la voz la harían inteligible, y por tanto la comunicación sería imposible.

1.1.3 Requerimientos de la voz sobre IP

Normalmente, los servicios de datos pueden tolerar perdida de la conexión o altas tasas de pérdidas de paquetes. La voz como aplicación tiene requerimientos muy estrictos:

- **Tasa de paquetes erróneos** (PER) <= 1%
- ***Jitter*** < 100ms (tan pequeño como sea posible)
- **Latencia** (retardo extremo-a-extremo) < 150ms
- **Retransmisión de paquetes** < 20%
- **Eco**: es tolerable cuando su retardo con la señal original es menor de 65 ms y tiene una atenuación de 25 a 30 dB.

En adición a estos problemas, las aplicaciones VoIP son sensibles a alta ocupación o compartición de la red con otro tipo de servicios cuando no existen mecanismos de QoS. Los usuarios no aceptaran que se entrecorte o que se escuche en una sola dirección, por lo que siempre será preferible que no se efectúe la comunicación, a que tenga lugar en un medio congestionado. [5]

1.1.4 Mecanismos de QoS en WiFi

Como ha sido explicado, la naturaleza de la voz hace que sea difícil de implementar servicios VoIP, incluso en redes cableadas de banda ancha, sin soluciones de control de la QoS, y por las características del medio inalámbrico, imposible en las *Wireless* LAN. Es por ello que los mecanismos de control de la calidad de servicio en redes inalámbricas no pueden estar enfocados solamente en otorgar diferentes prioridades según el tipo de tráfico, como ocurre en redes cableadas, es necesario además establecer mecanismos de acceso al medio, ya que en este además de estar compartido por otros usuarios del mismo sistema, conviven otros sistemas y equipos que operan en el mismo rango de frecuencias, por lo que además de colisiones y congestión, habrá interferencias provocadas por cusas disímiles.

El estándar IEEE 802.11 define dos funciones de acceso al medio a nivel MAC. La primera de ellas recibe el nombre de DCF (*Distributed Coordination Function*) y utiliza un mecanismo de acceso al medio distribuido basado en CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). La segunda de las funciones recibe el nombre de PCF (*Point Coordination Function*), y utiliza la anterior como base para su funcionamiento. PCF es opcional y usa un mecanismo de *polling* que requiere de un nodo central llamado PC (*Point Coordinator*) que lo coordine [6].

Cuando DCF es usado, cualquier estación que tenga datos para transmitir debe determinar el estado del canal de transmisión. Si el canal permanece libre durante un intervalo de tiempo DIFS (*DCF InterFrame Space*) la estación obtiene los derechos para comenzar a transmitir. En caso contrario, la estación deberá ejecutar un algoritmo de *backoff*, que

asignará un número aleatorio de slots de espera El valor de ese contador de *backoff* será decrementado en una unidad cada vez que el canal permanezca libre por un tiempo *aSlotTime*. Si en un instante cualquiera la estación detecta actividad en el canal, detendrá el decremento del contador, hasta que el canal este inactivo durante un intervalo DIFS. Después de este tiempo de espera, el contador reiniciará su cuenta atrás hasta llegar a 0, instante en el que comenzará la transmisión de la trama. El envío de una trama necesita la confirmación, por parte de la estación destino de que ha llegado correctamente. Si no es así, el emisor debe retransmitir la trama duplicando el tamaño de la ventana. Si por el contrario la estación emisora recibe el ACK de la receptora, actualizará el valor de CW (*Contention Window*) a CWmin.

DCF es un mecanismo simple, en el cual todas las estaciones que intentan acceder al canal lo hacen utilizando los mismos tiempos de espera, por lo que DCF no proporciona ningún soporte de QoS.

Cuando se activa PCF, el tiempo que existe entre dos paquetes (*beacon*) enviados por el punto de acceso se divide en dos periodos: CFP (*Content Free Period*) y CP (*Content Period*). Durante el periodo CFP el funcionamiento de la red es como se ha explicado hasta el momento, mientras que durante el CP los clientes no emitirán por iniciativa propia, sino que el punto de acceso le enviará un paquete a cada host por turnos, dándoles la oportunidad de emitir. El cliente aprovechará la oportunidad para emitir o si no tiene datos para enviar responderá con un paquete indicándolo. Con este método se pretende evitar que un cliente se apodere del canal, permitiendo a todos la emisión de datos con una frecuencia aceptable.

Sin embargo, PCF no es capaz de diferenciar los tipos de tráfico, solo diferencia a los hosts, y dará el mismo tratamiento a un cliente que va a transmitir datos, como al que espera transmitir video o voz. Por otra parte, PCF es un mecanismo que solo es funcional en redes de tipo infraestructura, nunca en redes ad-hoc, pues será el punto de acceso (AP) el encargado de realizar el control de acceso al medio.

Para proporcionar soporte QoS, en IEEE 802.11e se introduce una tercera función de coordinación, llamada HCF (*Hybrid Coordination Function*), que incorpora dos nuevos mecanismos de acceso al canal: EDCA (*Enhanced Distributed Channel Access*) y HCCA (*HCF Controlled Channel Access*), como se muestra en la Figura 1.1, además, se hace una distinción entre aquellas estaciones que no utilizan los servicios QoS, que se denominan nQSTA, y aquellas que si los utilizan, llamadas QSTA.

La principal característica de HCF es la definición de cuatro categorías de acceso (AC) y de ocho *traffic stream* (TS) a nivel MAC [7]. Cuando un paquete procedente de las capas superiores llega a la capa MAC, es etiquetado con un identificador de prioridad de usuario (TID) acorde con sus necesidades de QoS. Este identificador puede tomar valores de 0 a 15. Si el TID del paquete tiene valores de 0 a 7, es mapeado con respecto a las cuatro AC, usando el método EDCA para acceder al canal. Si por el contrario el identificador TID tiene valores de 8 a 15, usará la función HCCA para acceder al medio, quedando almacenado el paquete en la cola de TS correspondiente a su TID. Otra característica incluida en este

nuevo estándar es el concepto de TXOP (*Transmision Opportunity*), que es un intervalo de tiempo en el cual la estación que lo posee tiene permiso para enviar sus tramas.

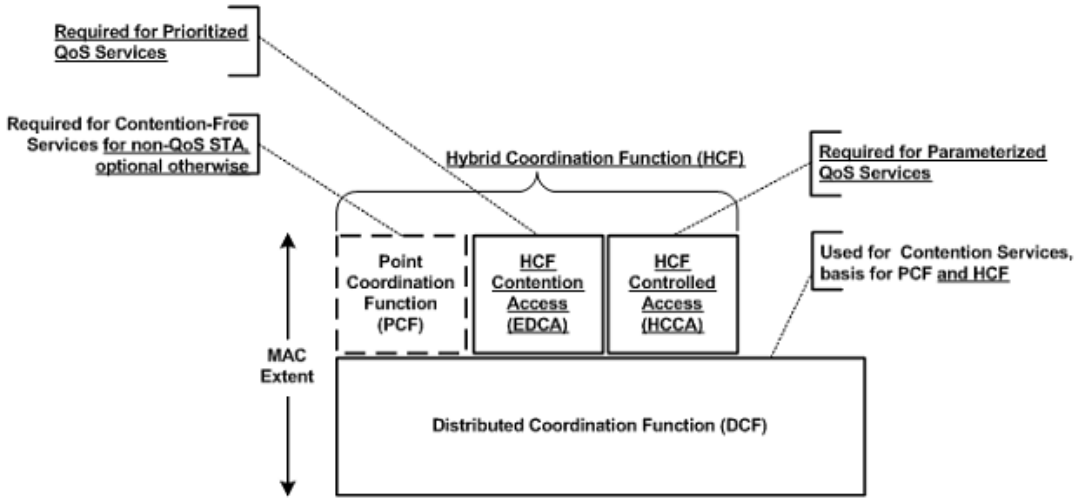


Figura 1.1 Funciones de Coordinación, Arquitectura MAC. Fuente [3], p. 71.

Las categorías de acceso, ordenadas de la más la menos prioritaria son:

- **Voz** (AC_VO): A esta categoría pertenecerá el tráfico de Voz.
- **Video** (AC_VI): Categoría en la que se encuadrará el tráfico de video que necesite prioridad.
- ***Best Effort*** (AC_BE): Tráfico que deberá transmitirse tan pronto como sea posible, tras atender a aquel que sea más prioritario. El tráfico de este tipo podría ser una sesión Telnet o de control remoto de un equipo, tráfico que aunque no sea tan crítico como los anteriores si será sensible a lentitud y pérdidas, dando sensación al usuario de falta de respuesta.
- ***Background*** (AC_BK): Es el tráfico que no entra en ninguna de las otras categorías. Es el tráfico de fondo o de relleno, de aquellas aplicaciones que no necesitan un tratamiento especial, como puede ser correo electrónico, la trasferencia de ficheros o el acceso a páginas web.
- ***Legacy DCF***: Esta no es realmente una categoría de acceso, es un grupo de tráfico que recibe un tratamiento diferente. Engloba a todo el tráfico normalmente gestionado por equipos que no cumplen con la norma 802.11e y por tanto no se engloba en ninguna de las categorías que la norma prevé. Por esta razón, al no tener indicación de la prioridad con que ha de ser tratado, será el menos prioritario de todos.

El método de acceso al medio EDCA [8], mejora el funcionamiento de DCF (por lo que también es conocido como *Enhanced Distribution Coordination Function*, EDCF), tratando de forma preferencial a las aplicaciones con restricciones en el tiempo. Para realizar esta diferenciación, EDCA introduce dos métodos, el primero de ellos es asignar distintos IFS a cada categoría de acceso. Para ello, el estándar introduce un nuevo tiempo de espera llamado AIFS (*Arbitration InterFrame Space*). El valor de AIFS es: AIFS[AC] = AIFSN[AC] x

aSlotTime + SIFS, donde AIFSN (*Arbitration InterFrame Space Number*), es utilizado para la diferenciación entre las distintas AC. El segundo método utilizado es asignar distintos tamaños de ventana CW para cada AC. Con este segundo método, el estándar pretende asignar menores tiempos de espera a las estaciones más prioritarias cuando estas tengan que efectuar el mecanismo de *backoff*. Estos tamaños se obtendrán mediante la asignación de distintos tamaños límite de ventana CWmin y CWmax. Otro factor utilizado para la distinción en EDCA, es la duración del TXOP (TXOPLimit). Este parámetro limita el tiempo en el que una estación tiene los derechos para transmitir, sin que el resto de estaciones le disputen el canal. El estándar IEEE 802.11e además recomienda diferentes valores de AIFS, CWmin, CWmax y TXOPLimit para las diferentes categorías de acceso, los cuales se muestran a continuación.

Tabla 1.1 Valores EDCA recomendados por Cisco. Fuente [9].

AC	AIFSN	CWmin	CWmax	TLimit
VO	2	7	15	3 ms
VI	2	15	31	6 ms
BE	3	31	1023	-
BK	7	31	1023	-

El método HCCA [10] pretende mejorar el funcionamiento de PCF, incorpora un mayor control del tráfico que EDCA, este mecanismo permite a las QSTA la reservación de *transmission opportunities* (TXOPs) con el *Hybrid Coordinator* (HC), el cual radica en el punto de acceso (QAP). El HC además, realiza gestión del ancho de banda y opera durante ambos períodos de contención: CFP (*Content Free Period*) y CP (Content Period), a diferencia del PC (*Point Coordinator*) en PCF. El HC puede tomar el control del medio inalámbrico, asignándose a sí mismo la mayor prioridad y menor TXOP, para transmitir tráfico con QoS cuando se necesite, esperando tiempos entre transmisiones más cortos que si se usara EDCA; y puede funcionar como PC para estaciones que no soporten esta función (nQSTA) [11].

HCCA es compatible y puede convivir con todos los métodos de acceso anteriores, basa su funcionamiento en el manejo y planificación de TXOP por parte del HC, según las necesidades del tráfico que se va a transmitir, ya que este conoce de antemano la cantidad de trafico pendiente y los requerimientos de QoS de cada *traffic stream* (TS), de esta forma, provee un tiempo limitado para la emisión de tráfico con QoS durante el *controlled access phase* (CAP), que no es más que el período de tiempo durante el cual el HC mantiene el control del medio inalámbrico, después de haber ganado acceso al medio detectando cuando el canal está libre durante el espacio entre tramas PCF, como se observa en la Figura 1.2.

HCF también define el método de acceso HEMM, que se refiere a EDCA y HCCA trabajando en modo mixto.

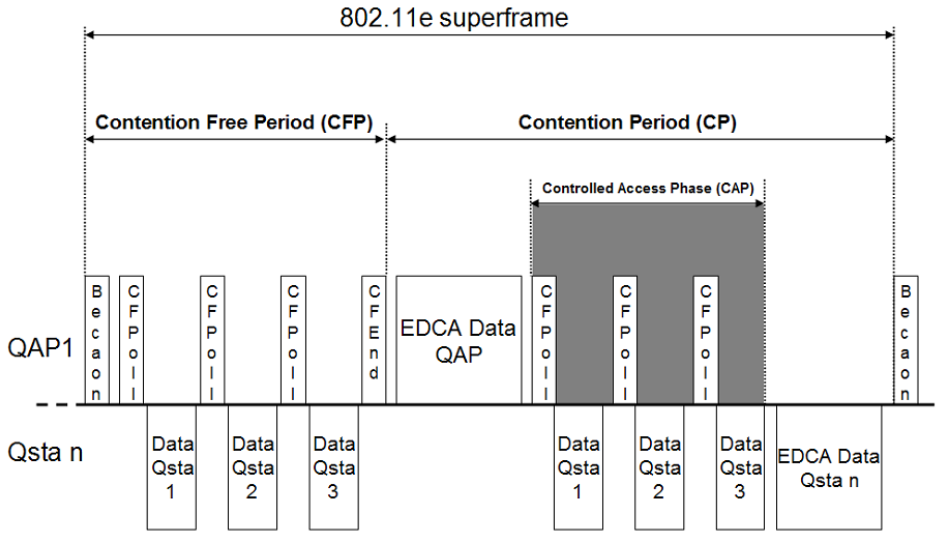


Figura 1.2 Supertrama 802.11e, CAP. Fuente [8], p. 4.

De manera general, HCCA realiza un control más estricto de la QoS y es el más adecuado para el tráfico de video y voz, dado que EDCA no implementa ningún mecanismo para proveerle las garantías al tráfico de tiempo real y no es posible asignarle ancho de banda a las aplicaciones, aunque esto no es importante en el caso de la voz; por otra parte, EDCA provee servicio diferenciado a categorías diferentes de tráfico y su uso está más extendido que HCCA, el cual solo funciona en redes del tipo infraestructura, ya que es necesario implementar el *Hybrid Coordinator* (HC) en el AP [12]. Cualquiera que sea el método de acceso empleado, las implementaciones prácticas y numerosos estudios demuestran que utilizando *Hybrid Coordination Function* (HCF), se garantiza calidad de servicio para aplicaciones en tiempo real como VoIP en redes WiFi.

1.2 Voz sobre IP en redes WiFi

La convergencia de dos áreas: voz sobre IP (VoIP) y redes inalámbricas (*Wireless* LAN), dentro de las que se enmarcan las redes WiFi, ha creado el término VoWLAN (*Voice over Wireless LAN*), aunque actualmente muchos proveedores manejan el término VoWiFi (*Voice over Wi-Fi*), para referirse a los servicios de voz usando como acceso las redes WiFi; por otra parte, los operadores de telecomunicaciones venden este servicio como *Wi-Fi Calling*. La idea de VoWLAN es utilizar la tecnología inalámbrica existente para que redes computacionales transporten tráfico de voz, el principal problema a resolver es implementar calidad de servicio en estas redes para soportar tráfico de voz, como ya ha sido discutido en este trabajo; pero esta no es la única problemática a la hora de implementar este tipo de servicio. La movilidad y la seguridad se convierten en un problema mayor, en adición, implementar un servicio de VoIP sobre redes públicas, usando como acceso redes WiFi, es más complicado que implementar soluciones VoIP en una red empresarial o privada. Un escenario VoWLAN que se comporte de forma eficiente en un ambiente empresarial, donde el tráfico es predecible y la cantidad de usuarios está controlada, podría colapsar en un entorno público.

1.2.1 Seguridad y autenticación

Para la voz sobre IP, en un entorno de red pública, la seguridad ya es un problema grave, y más aún cuando el protocolo SIP, que es uno de los más usados comúnmente, tiene sus propias vulnerabilidades. En adición, los problemas de seguridad de las redes inalámbricas, cuyas transmisiones van por el aire en lugar de cables, por la que son más fáciles de interceptar. Por todo esto, cualquier red WiFi que soporte VoIP tiene que ser segura, y este tráfico debe ser protegido por autenticación y encriptación.

El estándar IEEE 802.11i-2004 (*Enhanced Security*) [13] resuelve este problema, dotando a las redes WiFi de esta necesaria funcionalidad, a través de dos protocolos: TKIP (*Temporal Key Integrity Protocol*) y CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*).

TKIP conocido como WPA (*WiFi Protected Access*) es un primer paso en mejorar la seguridad en las redes WiFi, comienza con una clave temporal de 128 bits que es compartida entre los clientes y los puntos de acceso. Combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que cifrará los datos. Este procedimiento asegura que cada estación utilice diferentes *streams* claves para cifrar los datos. Utiliza el algoritmo RC4 para realizar el cifrado, y cambia las claves temporales cada 10.000 paquetes.

CCMP comúnmente conocido como WPA2 (*WiFi Protected Access 2*) aunque su funcionamiento es similar, es más seguro y robusto que TKIP, ya que utiliza AES (*Advanced Encryption Standard*), que es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Incluye como mejoras Preautenticación (*Extensible Authentication Protocol over LAN, EAPOL*), negociación del cifrado entre clientes y APs, y autenticación *peer-to-peer* para redes ad-hoc (*Independent Base Service Set, IBSS*).

Estos dos mecanismos proveen seguridad a nivel MAC, pero para soportar VoIP, es necesario que el usuario tenga movilidad, equipar a la arquitectura de seguridad con un servidor centralizado para autenticación a nivel de usuario, satisface este requerimiento, permitiendo al cliente autentificarse independientemente de su punto de acceso a la red. Esto pudiera lograrse a través de un servidor RADIUS (*Remote Authentication Dial-In User Service*), usando EAP (*Extensible Authentication Protocol*) que es el procedimiento estándar de autenticación. Este mecanismo brinda integridad y confidencialidad al proceso de autenticación, pero la re-autenticación durante el *hand-off* usando RADIUS pudiera tardar demasiado (500 milisegundos o más) lo que causaría interrupción de la voz, para mejorar esto se han implementado varias soluciones, por ejemplo Cisco recomienda el uso de *Cisco Centralized Key Management* (CCKM), el cual reduce a menos de 100 ms el tiempo de *hand-off* [14], otros fabricantes como Ruckus o Huawei recomiendan el uso de otras técnicas: *Pairwise Master Key (PMK) Caching*, y *Opportunistic PMK Caching*; todas estas técnicas se basan en incorporar un mecanismo centralizado de llaves que permita negociar una llave para toda la sesión, evitando tener que volver al servidor a autenticarse durante el *roaming*.

Existe otro método de autenticación, basado en la distribución de claves de sesión, conocido como EAP-SIM/AKA [15], [16] (*Extensible Authentication Protocol - Subscriber Identity Module/Authentication and Key Agreement*), el cual hace uso de las credenciales almacenadas en la SIM/USIM del usuario de la red GSM/UMTS/LTE), y las encapsula usando EAP para enviarlas al AAA (*Authentication, Authorization and Accounting*) y este realiza la autenticación de usuario con el HLR (*Home Location Register*) o HSS (*Home Subscriber Servers*) de la red móvil [17]. En la figura 1.3 se aprecia el mecanismo de autenticación EAP-SIM; como se observa, este reemplaza la necesidad de una contraseña pre-establecida entre el cliente y el servidor AAA, proporcionando autenticación mutua entre el cliente y la red.

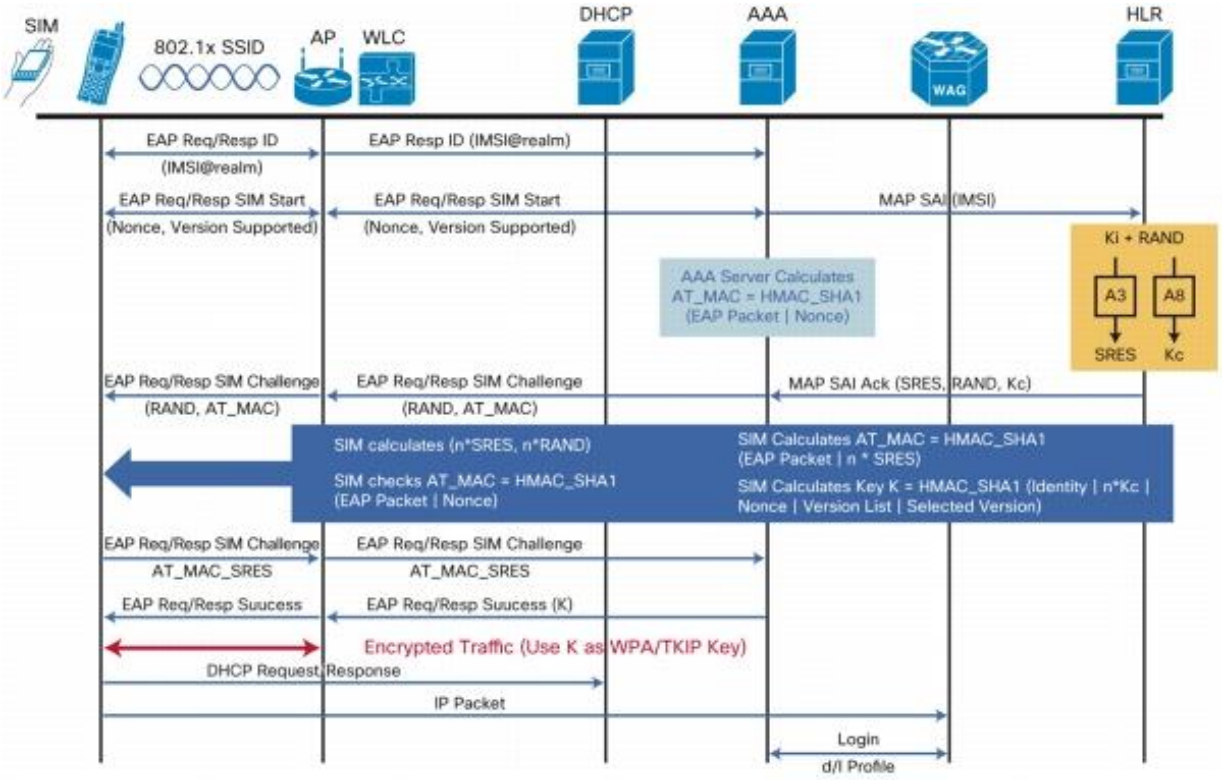


Figura 1.3 Autenticación EAP-SIM. Fuente [18]

1.2.2 Movilidad

Las aplicaciones como la Voz, necesitan la habilidad de continuar la comunicación cuando el usuario se mueve de un área a otra, en un escenario VoWLAN, un terminal en movimiento requerirá conmutar de un AP (*Access Point*) a otro, para ello necesitará negociar la conexión con el AP destino, y una vez que conmute, liberarse del AP de origen. El estándar IEEE 802.11r (*Fast Roaming*) [19], permite a los usuarios hacer *hand-off* de forma rápida, y negociar la configuración de seguridad y calidad de servicio antes de desasociarse del AP actual. Esto permite al usuario móvil mantener el servicio aunque cambie de Access Point, ya que la transición de un AP a otro demora menos de 50 milisegundos, un lapso de tiempo

lo suficientemente corto como para mantener una comunicación VoIP sin que haya cortes perceptibles [20].

Además del estándar 802.11r, para minimizar la pérdida de ráfagas de paquetes controlando el tiempo de *roaming*, se desarrolló el IEEE 802.11k (*Radio Resource Measurement, RRM*) [21], el cual permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WiFi, mejorando así su gestión. Ambos estándares fueron publicados en el 2008, y junto con el 802.11i, están contenidos dentro del IEEE 802.11n-2009.

1.3 Códecs y protocolos para VoWLAN

Esta sección no pretende hacer un estudio pormenorizado de los códecs y protocolos usados para dar servicios de VoIP, sino que se limita a mencionar los recomendados por la mayoría de las bibliografías consultadas, lo que se reduce a *Session Initiation Protocol* (SIP), para el establecimiento, modificación y terminación de conexiones; con respecto a los códecs se puede usar el clásico G.711(64 Kbit/s) usado en telefonía, pero es más recomendable usar G.729A que reduce la carga útil a 8 Kbit/s en tramas de 10 ms [22]. También podría utilizarse el propio códec GSM (13 Kbit/s en tramas de 20 ms).

1.4 Interoperabilidad

Al implementar servicios VoIP en redes inalámbricas, la interoperabilidad no es un requisito. Perfectamente se puede brindar un servicio que aunque converja con redes públicas, el acceso necesariamente tenga que ser desde una red de datos. Ahora bien, si tenemos en cuenta que un gran número de los terminales son dispositivos que pueden conectarse tanto a redes WiFi como a redes móviles, y que cada año los líderes en el mercado de los *smartphones* incorporan a estos los últimos y más actualizados estándares, es de esperar que los operadores no rechacen la idea de lograr interoperabilidad entre ambas redes, permitiendo a los usuarios mantener la comunicación al hacer *roaming* de una red a otra.

Muchos son los escenarios de implementación propuestos para lograr Interoperabilidad, pero generalmente se requiere que la red celular tenga un *Core* IP, ya sea con acceso HSPA o LTE, aunque en GSM también pueden implementarse soluciones; en cuanto a los terminales móviles, deben cumplir con el estándar IEEE 802.21-2008, el cual define mecanismos, independientes del método o modo de acceso, que posibilita la optimización del *handover* ya sea entre redes del mismo tipo, de las distintas redes 802 o entre redes móviles [23].

En el caso de las redes WiFi, estas deben cumplir el estándar IEEE 802.11u (*Interworking with External Networks*) [24], el cual fue publicado en el 2011 y establece mecanismos para *interworking* con redes que no sean del tipo 802, como es el caso de las redes celulares.

1.5 Implementación de Zonas WiFi en Cuba

En el planeamiento realizado para la implementación de las zonas de acceso público WiFi de ETECSA (figura 1.4), se tuvo en cuenta que este es un servicio brindado por un operador de

telecomunicaciones y que estaría expuesto a condiciones de operación exigentes, en la implementación se usó equipamiento *Carrier Class* de tecnología Huawei.

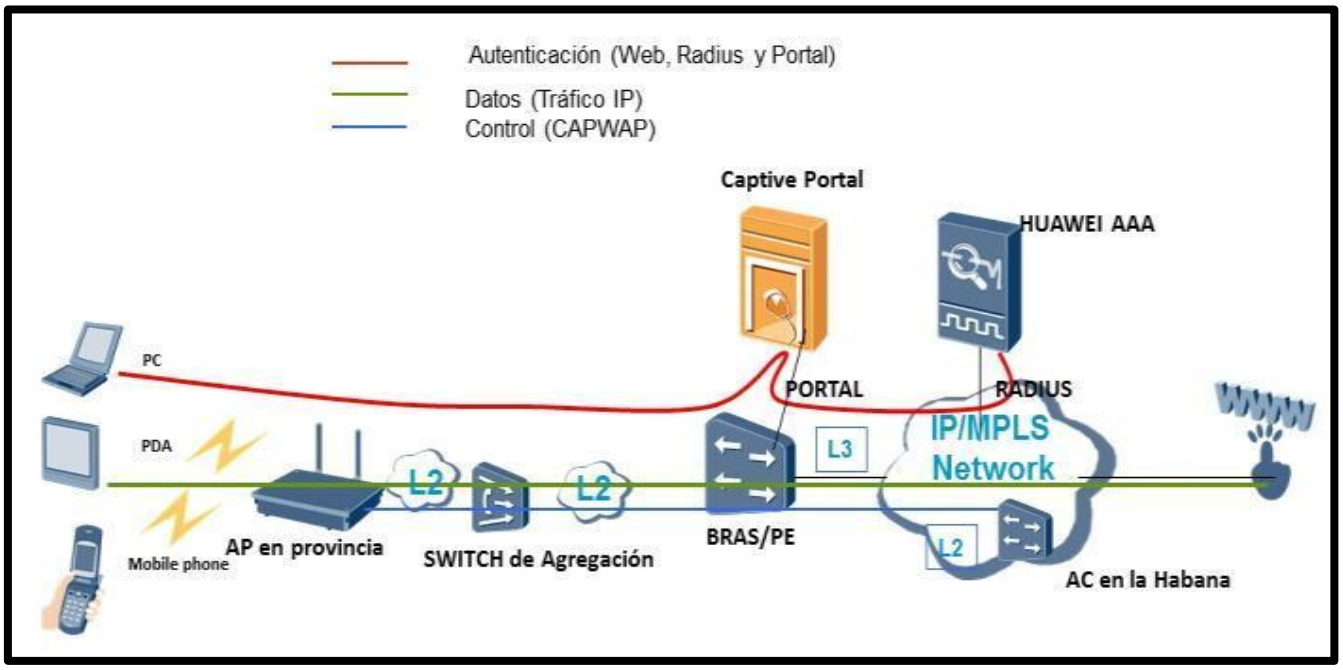


Figura 1.4: Implementación de Zonas WiFi. Fuente [25]

La configuración y gestión de los APs es centralizada con un AC (*Access Controller*), usando un túnel CAP-WAP (*Control and Provisioning of Wireless Access Points*) [26] para proteger todo el intercambio de información que se genera entre estos; mientras que la autenticación de los usuarios es a través de un Portal Captivo y un servidor AAA RADIUS, el cual soporta la funcionalidad AAA 3gpp [27], lo que permitiría en un futuro para los usuarios móviles autenticarse por su IMSI (*International Mobile Subscriber Identifier*) en el HLR correspondiente; todo integrado en el Sistema de Gestión propietario iManager U2000. La movilidad de los usuarios está contemplada en las actuales zonas de acceso WiFi, siempre que estos no salgan de la misma. Los AP Huawei utilizados trabajan con el estándar IEEE802.11n y en ambas bandas (2.4 y 5 GHz), que como se ha descrito en este capítulo, garantiza movilidad, seguridad, y calidad de servicio suficiente para soportar tráfico de VoIP.

1.6 Consideraciones finales del capítulo 1

En este capítulo se describen los estándares que garantizan calidad de servicio para soportar Voz sobre IP en redes WiFi, lo que posibilita la implementación de aplicaciones VoWLAN y su futura interoperabilidad con redes públicas, aprovechando las ventajas que brindan los *smartphones* y *tablets*.

Se hace particular énfasis en los mecanismos de control de acceso al medio introducidos por el estándar IEEE802.11e, EDCA y HCCA, los cuales están contenidos dentro de la función de coordinación HCF, la cual está encargada de proveer QoS a nivel MAC en las redes WiFi.

También se refieren otros estándares encargados de dar seguridad y movilidad a los usuarios, dos temas fundamentales a la hora de dar soporte a la voz en redes inalámbricas, que son tratados en este documento por estar estrechamente ligados a la calidad de servicio en redes VoWLAN, ya que no se concibe un servicio de voz inalámbrico que tenga que comportarse de forma estática. El cliente debe poder moverse de un AP a otro sin percibir afectación del servicio, por tanto, el *hand-off* en este tipo de redes debe ser rápido, pero sin comprometer la seguridad. El estándar IEEE 802.11n, incluye todas las enmiendas y especificaciones mencionadas en este trabajo.

CAPÍTULO 2. Diseño de redes VoWLAN con calidad de servicio

El servicio de voz sobre WiFi (VoWiFi), también llamado *Wi-Fi Calling*, permite a los usuarios usar *smartphones* que soporten esta funcionalidad, para marcar números e iniciar llamadas de voz o video-llamadas, cuando esté disponible una conexión WiFi, en lugar de usar la red móvil conmutada o los datos móviles. Para que esto sea posible no basta con implementar una arquitectura de red (o usar una ya existente como es el caso de las redes que soportan VoLTE, cuya infraestructura puede ser aprovechada para dar servicios VoWiFi), que permita la autenticación, seguridad, movilidad, conectividad e interoperabilidad de los usuarios de la red de acceso WiFi; además es necesario que estas últimas cuenten con un diseño que garantice la calidad del servicio de voz.

Esta sección define criterios de diseño para la implementación de redes WiFi con QoS para soportar VoIP, que si bien es cierto que son aplicables a cualquier arquitectura Wireless LAN, son indispensables en el caso de escenarios VoWLAN.

2.1 Etapas para el desarrollo de redes WLAN

Sin importar el tipo de arquitectura de red inalámbrica que se desee implementar, si se quiere garantizar el buen desempeño de estas, es necesario tener en cuenta cada uno de los siguientes pasos para su desarrollo, estos adquieren mayor relevancia cuando se trata de redes inalámbricas para alta densidad de usuarios:

- **Planeamiento**: Determina los requerimientos de aplicaciones y dispositivos, en cuanto a ancho de banda, protocolos, frecuencias, servicios, etc.
- **Diseño**: Determina densidad y dimensionamiento de celdas, tipos de antena, cobertura, *survey* de los sitios, diseño de la infraestructura de red. Usualmente la etapa de diseño incluye simulación del escenario.
- **Implementación**: Instalación (montaje), pruebas, ajustes iniciales.
- **Optimización**: Monitoreo, reportes, ajustes, revisión de lo planificado.
- **Operación**: Herramientas de gestión, *troubleshooting*, monitoreo de alarmas y eventos, capacidad, tráfico, etc.

2.1.1 Planeamiento

En el **planeamiento** se establecen las condiciones iniciales del diseño, esto es establecer el tipo de escenario: si es en interiores o exteriores, si es empresarial o público (parques, anfiteatros, etc.), para pocos usuarios o para alta densidad de usuarios, y el tipo de servicios que se va a brindar, con vistas a tener claro los requerimientos de ancho de banda (diseño de capacidad) y calidad de servicio. Todo esto conlleva a tener una idea aproximada de la cantidad de *Access Points* (AP) a utilizar, el balance de usuarios por AP, la separación entre estos y los canales y bandas que se deben utilizar, de manera que se minimice la interferencia entre canales vecinos y se cubra toda el área con buen nivel de señal. Una vez que se conoce el escenario WLAN se debe definir la arquitectura de red que se va a utilizar, la forma en que se autenticaran los usuarios, y la variante de seguridad a emplear [28].

Con estos datos se debe seleccionar el equipamiento apropiado; en la práctica ocurre que un proveedor vende toda la arquitectura de la red, pero aun así, siempre va estar en manos del planificador la selección del equipamiento, ya que cualquier fabricante siempre va a ofertar varias gamas de equipos con diferentes prestaciones y costes, lo que permite escoger un equipamiento que satisfaga las condiciones iniciales sin elevar demasiado el costo de la inversión, pero siempre se debe tener cuidado que nuestra red sea escalable, si cambiaran las condiciones iniciales en cuanto al tipo de tráfico, cantidad de usuarios, y servicios soportados. Por ejemplo, podemos seleccionar el uso de *Fat* AP, que son puntos de acceso autónomos con grandes prestaciones, pero también elevados costos, o usar *Fit* AP con un *Access Controler* (AC), que son puntos de acceso de menor costo con pocas prestaciones y que dependen del AC para implementar servicios de red (como DHCP, *management*, autenticación, ruteo, seguridad, y QoS) [29].

El planeamiento también debe considerar el tipo de dispositivos que se conectaran a la red, ya que no todos los terminales soportan todos los estándares existentes, en redes públicas esto es un gran problema, pues debe tenerse en cuenta la compatibilidad a cualquier dispositivo [30]. A menudo, para garantizar la calidad de un servicio determinado, este se restringe a terminales que cumplan determinados requerimientos. Por ejemplo: Las redes de alta densidad requieren que los clientes transmitan tramas en velocidades lo más elevadas posibles, el uso de mayores velocidades permite la transmisión de datos del cliente más rápido, reduce el uso de tiempo al aire del cliente y proporciona una mayor capacidad y rendimiento de la red; por tanto, la desactivación de las velocidades de datos más bajas asegura que los clientes sólo puedan conectarse utilizando velocidades de datos elevadas y ayuda a evitar situaciones de clientes que pueden reducir la capacidad global de la red. Otro caso es cuando se ofrecen servicios de tiempo real como la voz o el video, que requieren el uso de técnicas de QoS, para no afectar la calidad percibida por el usuario, podría decidirse que equipos que no soporten WMM no puedan acceder a estos [31]; lo mismo ocurre en el caso de servicios con determinados requerimientos de seguridad, si el terminal no es capaz de establecer una conexión segura, no debe poder acceder al servicio en cuestión, pues esto sería una vulnerabilidad. Si bien es cierto que estas soluciones pueden parecer drásticas, en realidad quedan muy pocos dispositivos en funcionamiento, que no cumplan con estos requerimientos.

2.1.2 Diseño

El **diseño** de la red está estrechamente ligado al planeamiento y consiste en la síntesis de las necesidades identificadas en una arquitectura de red que cumpla con los requisitos de rendimiento establecidos. Esto se logra al realizar los siguientes pasos: En primer lugar, identificar las capacidades del cliente y los requisitos de rendimiento de las aplicaciones. En segundo lugar, determinar los *Access Points* y las capacidades de radio necesarias para apoyar las necesidades de los clientes y de las aplicaciones identificadas. En tercer lugar, determinar el tipo y la cantidad apropiada de *Access Points*, así como los accesorios que necesarios y su ubicación en el sitio para obtener una cobertura óptima basada en las características de las instalaciones. La realización de estudios de campo (*survey*) para

recolectar la información necesaria y verificar las decisiones de diseño, son fundamentales para la creación del diseño exitoso de una red WiFi.

Existen diferencias significativas entre las capacidades de las redes WiFi diseñadas orientadas a la cobertura, frente a las diseñadas enfocadas en el desempeño. Los matices entre estos dos enfoques a menudo no son bien entendidos por el usuario final; por ejemplo, el uso de las barras de señal inalámbrica como una representación de la viabilidad de la red, es un indicador muy pobre sobre el éxito de la red, ya que en realidad representa intensidad de señal y no calidad de esta, al no tener en cuenta otros parámetros como la relación señal-ruido (*signal to noise ratio, SNR*) [32]. Un diseño de orientado a la cobertura a menudo no tiene en cuenta otras variables críticas necesarias para satisfacer las necesidades de rendimiento y obtener una experiencia satisfactoria para el usuario, como las siguientes:

- Reducción al mínimo de la interferencia de canales vecinos.
- Maximización de la capacidad espectral por medio de la localización de diferentes frecuencias.
- Optimización del ancho de banda para hacer un mejor uso de la capacidad espectral disponible.
- Equilibrio en el número de clientes por Access Point.
- Diseño basado en calidad de servicio.

Escoger el tipo de antenas es otro factor importante del diseño. En redes inalámbricas de alta densidad de usuarios, puede ser necesario ubicar múltiples puntos de acceso en un solo espacio físico para proporcionar la capacidad requerida, el uso de antenas semi-direccionales (sectoriales) con potencia de transmisión baja para limitar el área de cobertura de los AP's, en lugar de antenas omnidireccionales, es una estrategia eficiente para disminuir la interferencia co-canal, sobre todo en la banda de 2.4 GHz, habiendo sólo tres canales que no se superponen [33].

Otra estrategia podría ser utilizar solamente la banda de 5 GHz, al estar conformada por cuatro bandas de frecuencias únicas y un total de 23 canales de 20 MHz que no se superponen, se logra una mayor separación entre los puntos de acceso que operan en el mismo canal y permite un mejor plan de reutilización de frecuencias. La capacidad espectral disponible también está influenciada por el ancho del canal operativo, la banda de 5 GHz permite usar canales con anchos de banda mayores para aumentar la capacidad de la celda, 802.11n introduce 12 canales de 40 MHz para aumentar el ancho de banda máximo y el rendimiento dentro de una sola celda WiFi, y 802.11ac introduce aún mayores anchos de banda (80 MHz y 160 MHz), lo que con menor número de canales [34].

En general, la banda de 5 GHz ofrece mucha más capacidad que la banda de 2.4 GHz. Sin embargo, los diseñadores de redes deben todavía ser conscientes del impacto que la desactivación de la banda de 2.4 GHz traería consigo, ya que la mayoría de los dispositivos que están hoy en el mercado aún no soportan la banda de 5 GHz, por lo que se recomienda en los diseños de redes de gran capacidad que estas soporten ambas bandas. De manera general, lo usual es que se diseñen redes compatibles a casi todas las normas existentes (802.11 a/b/g/n), percibiendo mejor desempeño los usuarios con mejores terminales y en especial los que logran conectarse a 5 GHz [35].

Parte del diseño lo es también la arquitectura de la red, el dimensionamiento de esta, la forma en que se autenticaran los usuarios, la configuración y forma de conexión del *Access Controler* (en caso de ser utilizado), que incluye las especificaciones de seguridad, *roaming*, QoS, balance de carga, entre otros parámetros. Esta sección no pretende hacer un análisis pormenorizado de las diferentes formas de interconectar los elementos de red (*networking*), por no ser objetivo de este trabajo, el cual se centra en el diseño de red inalámbrica.

Por último, en el diseño se debe utilizar una herramienta de simulación, que permita modelar el escenario inalámbrico teniendo en cuenta las mediciones que se realizaron en los sitios, los materiales utilizados en la construcción de edificios, los árboles en caso de espacios abiertos, y cualquier otro objeto que pueda tener un impacto significativo en la propagación y atenuación de la señal RF; esto permitirá realizar ajustes de potencia, orientación de las antenas, posición de los AP, y frecuencias a utilizar, antes de la fase de implementación.

2.1.3 Implementación, optimización y operación

La **implementación**, como su nombre lo indica, consiste en el montaje del equipamiento según lo proyectado, incluye la revisión y ajuste, mediante nuevas mediciones y pruebas en el sitio, de los parámetros previamente definidos en las fases anteriores.

Los escenarios inalámbricos son muy cambiantes con el tiempo, sobre todo porque el medio es compartido por todos los usuarios, incluso por usuarios no registrados en la red propia, pero que también son causantes de interferencias, en redes públicas es particularmente difícil predecir la cantidad de usuarios y el tipo de servicios que estos demandan [36]. Es por ello que se hace necesaria la **optimización**, usualmente se establece un período de pruebas durante el cual se revisan y re-ajustan constantemente los parámetros de la red, pasado este tiempo, los parámetros de desempeño de la red (KPI) se chequean de forma más espaciada. Para su solución, los problemas detectados por las mediciones realizadas en esta fase, vuelven a pasar por el planeamiento y re-diseño de la red.

Aunque la **operación** no es parte como tal del proceso de desarrollo de redes, el ajuste de parámetros planificados (optimización) en el caso de las redes inalámbricas no es una tarea de una vez, sino que requiere un trabajo profiláctico de análisis de las mediciones de desempeño de estas, con vistas a detectar cualquier variación de los parámetros deseados y ante esta situación, es necesario reajustar lo planificado para las condiciones iniciales; la operación cuenta con las herramientas para detectar y corregir de forma inmediata cualquier falla o evento que pueda perjudicar el desempeño de la red.

2.2 Caracterización de las zonas WiFi desplegadas por ETECSA

Como fue explicado en el epígrafe anterior, el planeamiento y diseño, juegan un papel fundamental cuando se trata de redes WLAN de alta densidad. También es importante garantizar que el equipamiento que se adquiera sea capaz de ofrecer, tanto un alto rendimiento, como funciones de optimización para un espectro limitado.

Esta sección pretende hacer un análisis de la situación actual de las zonas de acceso WiFi, desplegadas por ETECSA, para el servicio de acceso público a internet usando la plataforma

nauta, en cuanto a los factores en su diseño e implementación que afectan la calidad del servicio, y que repercutirían de negativamente de implementarse sobre estas un servicio de voz sobre IP.

Para el despliegue de las zonas de acceso WiFi, ETECSA licitó la oferta del proveedor Huawei Technologies Co., Ltd. [37], consistente en un modelo de AP *indoor* y un modelo de AP *outdoor* (ver anexos). A continuación mostramos algunas características de ambos:

Figura 2.1 WA201DK-NE, indoor AP. Fuente [38]

Figura 2.2 WA251DK-NE, outdoor AP. Fuente [39]

- Tipo: *Enterprise/Service Provider Access Point*.
- Cumple con IEEE 802.11 a/b/g/n (Wi-Fi CERTIFIED™).
- Usa módulos RF *dual-band* y 3x3 MIMO con antenas integradas (*built-in*).
- Soporta 2.4GHz y 5GHz conmutable, hasta 450 Mbit/s por cada módulo de radio.
- AP indoor, antenas omnidireccionales; AP outdoor, antenas sectoriales.
- Cumple con 802.3af/at *Power over Ethernet*, para facilitar su instalación.
- Soporta seguridad WPA2™, EAP-TLS, EAP-SIM, EAP-AKA, entre otras.
- Soporta WMM®-*Power Save* (*WLAN Multimedia profile*).
- Puede trabajar como *Fat-AP*, o como *Fit-AP* integrado a *Access Controller* (AC) y *Network Management System* (NMS) para implementar monitoreo en tiempo real, análisis de espectro, detección de interferencia, balance de carga, *beamforming, roaming*, y control de acceso flexible.

A cada zona WiFi se le garantiza un *backhaul* que soporte con buena eficiencia espectral y baja latencia, todo el tráfico desde y hacia estas, los AP se conectan a través de un *switch* de acceso PoE. Los AC utilizados (MAG9811, Huawei) tienen redundancia y pueden

gestionar hasta 4096 APs y hasta 96 mil usuarios, con una capacidad de tráfico de hasta 40Gb/s en cada una de sus tres ranuras, la capacidad total de conmutación es de 1Tb/s; estas capacidades están en dependencia de los servicios que soporten, el modo de trabajo y la carga elaborativa de los procesadores [40]. Todo el acceso se gestiona mediante el *Network Management System* (NMS) U2000. La funcionalidad de BRAS (*Broadband Remote Access Server*), así como la de *router Provider Edge* (PE), la desempeña el Quidway ME60, que es un potente *Multiservice Control Gateway* de Huawei. La autenticación de los usuarios es a través de un servidor AAA y portal cautivo, también de Huawei.

Como se puede apreciar, el equipamiento adquirido, así como la arquitectura de red implementada, cumple con todos los estándares necesarios para lograr calidad del servicio. El autor considera además, que el planeamiento de la red fue adecuado, los problemas fundamentales encontrados en esta investigación están en el diseño e implementación de las zonas de acceso, así como en la carencia de un proceso de optimización de estas.

Para llegar a estas conclusiones se hicieron mediciones en los sitios empleando diferentes técnicas, a modo de ejemplo, en la figura 2.3 se muestra un *survey* realizado en el "Parque Ignacio Agramonte" de la ciudad de Camagüey, empleando el software "*WiFi Analyzer and Surveyor* v1.21" sobre sistema Android 4.2.2.

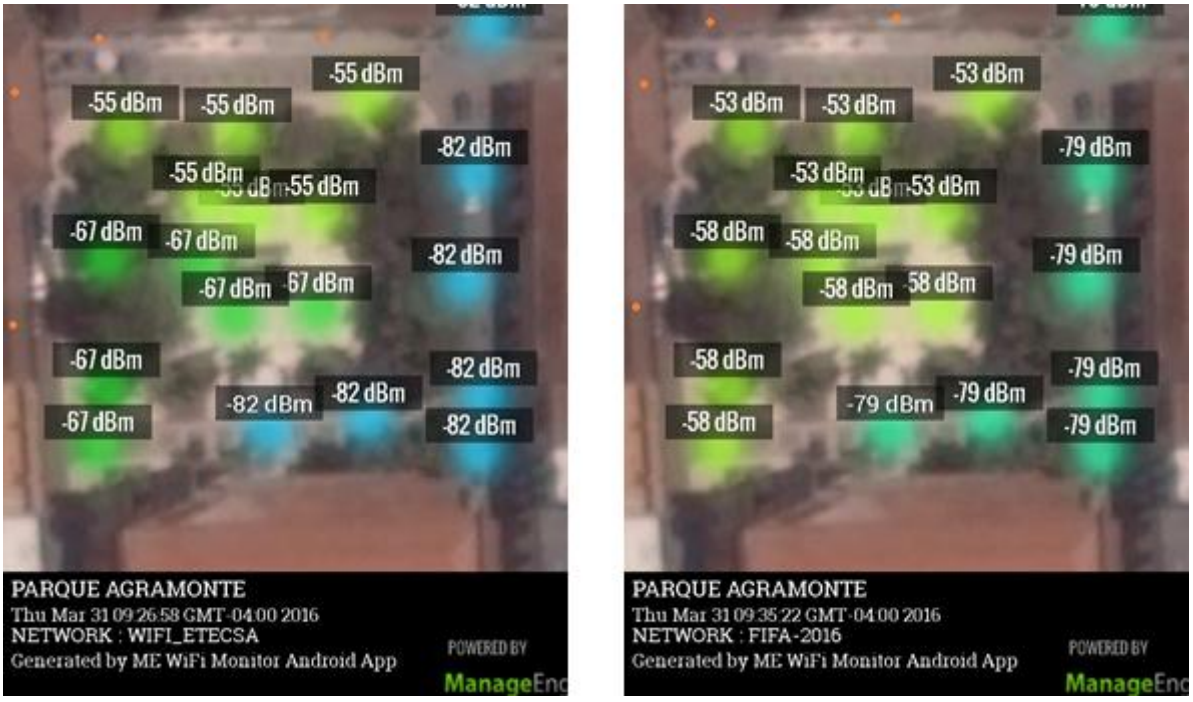


Figura 2.3: *Survey* Parque Agramonte, *outdoor* AP. Fuente elaboración propia.

Los puntos en rojo representan la posición aproximada de los AP, la imagen de la izquierda corresponde a la WIFI_ETECSA, mientras que la de la derecha es una red privada que tiene el SSID: FIFA-2016. Se puede apreciar como en el caso de la WIFI_ETECSA la señal se desvanece de tal forma que en toda la parte este del parque, y en gran parte del sur, la intensidad de la señal es muy baja (-82 dBm, en azul); la causa de que esto ocurra, es que el follaje de los árboles del parque atenúa la señal, sin embargo esto no afecta en igual medida

la intensidad de la señal en el centro del parque, por lo que se puede concluir que la posición de los AP no es la idónea. De haberse ubicado los AP de forma tal que cubrieran todo el parque (por ejemplo, uno en cada esquina), las mediciones hubieran dado un resultado diferente, obteniéndose intensidades de entre -55 dBm y -67 dBm en toda el área. Otro aspecto a tener en consideración es que en la banda de 2.4 GHz necesariamente se repite una portadora (recuérdese que en esta banda solo hay 3 portadoras sin solapamiento: 1, 6, y 11) y en este diseño los AP están muy juntos, por lo que al menos dos de ellos tienen interferencia co-canal, esto también pudo evitarse con un mejor posicionamiento de los AP, y aprovechando la direccionalidad de las antenas, se podían orientar de tal forma que los efectos de la interferencia co-canal fueran mínimos. Desde el punto de vista del desempeño de la red, se pudo observar mediante mediciones realizadas con el NMS U2000, que en este sitio existe desbalance de carga entre los cuatro AP, y que en horas de alto tráfico las retransmisiones de paquetes, así como la taza de paquetes erróneos, es mayor que los umbrales establecidos para lograr calidad de servicio en aplicaciones como la voz y el video.

En la imagen de la derecha de la figura 2.3 se observa una red privada, cuyo equipamiento se desconoce, pero que se propaga con patrón muy semejante al de la WIFI_ETECSA e incluso con niveles de señal superiores, es de esperarse que los efectos en cuanto a interferencia que provoca, resulten muy perjudiciales para la calidad de servicio percibida por los usuarios. Desgraciadamente, el autor de este trabajo no cuenta con las herramientas para medir el impacto real sobre la calidad del servicio de estas redes no licenciadas.

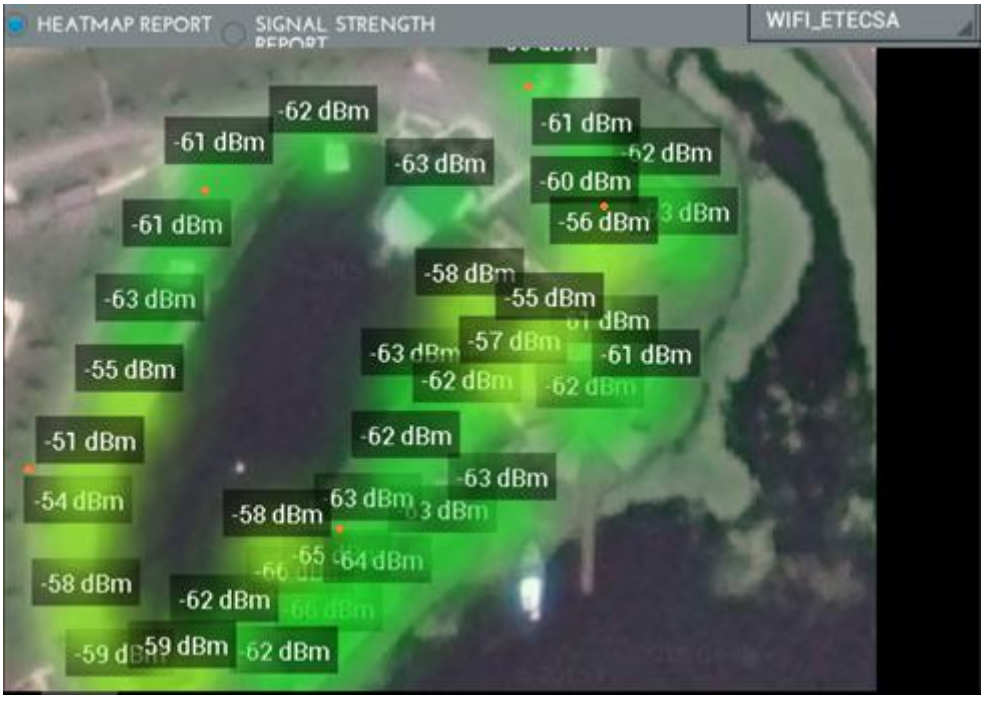


Figura 2.4: *Survey* Lago de los sueños, *outdoor* AP. Fuente elaboración propia.

La figura 2.4 muestra un ejemplo de buen diseño. Se trata de un *survey* realizado en el "Lago de los sueños", un área mucho más extensa en la que se ubicaron cinco AP *outdoor* y dos AP *indoor* (en la figura solo se muestran los *outdoor*), los AP están distribuidos para lograr niveles de señal altos en cualquier parte del sitio (por encima de -64dBm), las antenas

están orientadas de tal forma que la interferencia co-canal es insignificante. Los valores medidos mediante el U2000, reflejan una taza de paquetes erróneos y retransmisiones de paquetes, por debajo de los umbrales establecidos para garantizar calidad de servicio.

2.3 Otros factores que afectan la calidad percibida del servicio WiFi

Otro aspecto que da al traste con la calidad del servicio percibida por el usuario (QoE), es la autenticación por Portal Cautivo, si bien es cierto que el uso de esta forma de autenticación brinda gran información al usuario, además de permitir autenticarse con la cuenta nauta, que ya existía antes de la aparición de las zonas de acceso público, también es cierto que esta ha prestado vulnerabilidades como el robo de cuentas y la suplantación de usuarios; por otra parte, para la cantidad de usuarios concurrentes que existe actualmente, el portal presenta dificultades cuando recibe demasiadas peticiones simultaneas, rechazando las que no puede atender, el usuario que no puede conectarse vuelve a realizar otro intento de autenticación, lo que aumenta aún más el número de peticiones. Además de todo esto, el proceso de autenticación por portal cautivo es sumamente lento, ya que requiere que el cliente entre su usuario y contraseña, y en ocasiones, un código de validación.

Para implementar servicio de voz sobre IP empleando la infraestructura descrita en el epígrafe anterior (VoWiFi), sería necesario implementar otra forma de autenticación para no afectar la calidad del servicio, por ejemplo, la introducción de la autenticación basada en EAP-SIM/AKA, tema que ya fue tratado en el capítulo anterior. La introducción de esta forma de autenticación, operando de conjunto con la autenticación por portal, reduce la utilización de tarjetas nauta y la necesidad de contratación de cuentas permanentes, por lo que se reducirían las colas en las oficinas comerciales de ETECSA. Otras ventajas que trae consigo este método es que elimina las brechas de seguridad de la autenticación por portal cautivo; funciona más rápido y elimina la demora que provoca el propio cliente, al no tener que introducir su usuario y contraseña; al usar para el acceso WiFi las mismas credenciales del usuario móvil, permite la tarificación unificada de ambos servicios y sienta las bases para una futura interoperabilidad entre la red WiFi y la red móvil.

Entre las quejas de los clientes, también está el cobro por tiempo de conexión y no por volumen, este último le permitiría a usuarios que no intercambian gran volumen de información estar conectados más tiempo, mientras que para usuarios que hacen grandes transferencias de datos es más conveniente el cobro por tiempo.

2.4 Criterios de diseño para implementar redes WiFi con QoS

Es muy común en este tipo de redes que los usuarios finales, entusiasmados por el boom que últimamente las WLANS han alcanzado, compren e instalen equipos sin un previo planeamiento y diseño, trayendo como resultado un deficiente desempeño. La instalación y configuración de una WLAN pueden ser un proceso muy sencillo, pero precisamente esto las hace ser un blanco fácil para ataques externos e interferencias. En esta sección se describe cómo planear y diseñar una red WLAN con el propósito de optimizar su desempeño para garantizar calidad de servicio, logrando además que sean seguras.

Independientemente de cual sea el escenario en el que se va a implementar una red WLAN, siempre se debe orientar su diseño velando por los siguientes tres factores:

- Proporcionar señal de alta calidad a todas las áreas de cobertura.
- Minimizar la interferencia co-canal entre AP's.
- Adaptar el diseño a las características de las instalaciones.

Para lograr esto, primeramente, es necesario posicionar correctamente los AP, seleccionar las frecuencias de trabajo de estos, y orientar bien las antenas. La figura 2.5 muestra un ejemplo en el caso de que se usen tres AP con antenas omnidireccionales.

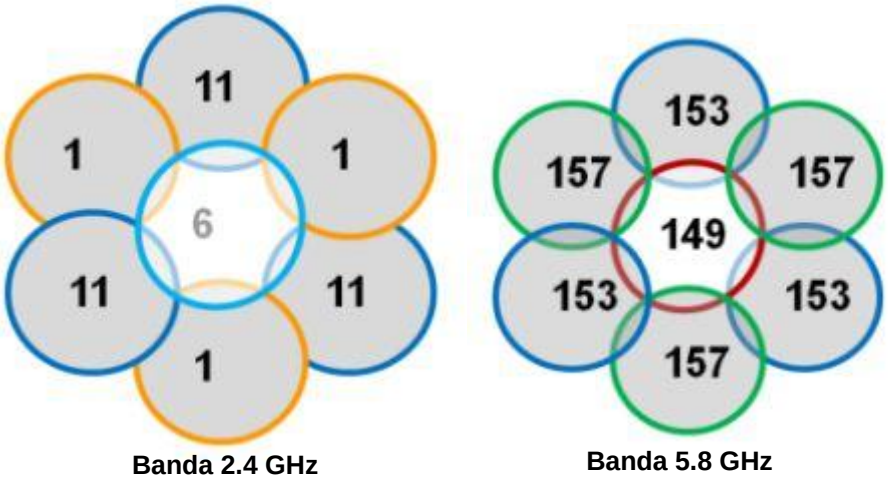


Figura 2.5: Distribución de celdas para antenas omnidireccionales. Fuente [41], pag. 906.

Este tipo de distribución es más frecuente en el caso de usar AP *indoor*, la imagen de la izquierda muestra la distribución de los tres canales de 20 MHz sin solapamiento en la banda de 2.4 GHz, mientras que la derecha muestra un ejemplo usando la banda alta de 5.8 GHz, pero en este caso hay otras opciones, ya que la banda de 5 GHz está dividida en tres sub-bandas (baja, media y alta) y en cada una de ellas pueden usarse cuatro canales de 20 MHz sin solapamiento (y hasta cinco en 5.8 GHz), como se ve en la tabla 2.1 [28].

Tabla 2.1 Bandas y frecuencias usadas para WiFi. Fuente elaboración propia.

2.4 GHz			**5 GHz**		
Ch ID		**Center Freq. (MHz)**	**Ch ID**	**Freq. Band**	**Center Freq. (MHz)**
1	América y resto del mundo	2412	36	Low Band 5.15 - 5.25 GHz	5180
2		2417	40		5200
3		2422	44		5220
4		2427	48		5240
5	América y resto del mundo	2432	52	Middle band 5.25 – 5.35 GHz	5260
6		2437	56		5280
7		2442	60		5300
8		2447	64		5320

9	América y resto del mundo	2452	149	High band 5.725 - 5.825 GHz	5745
10		2457	153		5765
11		2462	157		5785
12	Europa, China, Japón y Australia	2467	161		5805
13		2472	165	5.825 - 5.850	5825

En algunas regiones, la banda de 2.4 GHz se extiende hasta el canal 13, en estos casos, distribuyendo adecuadamente las antenas, se puede usar una combinación de cuatro frecuencias prácticamente sin solapamiento: 1, 5, 9, y 13. La banda media de 5 GHz, ha sido extendida en algunos países con 11 nuevos canales de 20 MHz: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, y 140 (de 5500 MHz a 5700 MHz), no siempre se usan todos, ya que en presencia de radares meteorológicos cercanos solo se pueden usar 8 canales, pues tres de ellos quedan interferidos (120, 124, y 128).

En cuanto al dimensionamiento de las celdas, el radio de estas debe ser de -67 dBm en el área primaria y de más de -75 dBm en la secundaria; la separación mínima entre celdas con el mismo canal es de 19 dbm (a -86 dbm del centro de la celda), en la figura 2.6 se muestra esto con más claridad.

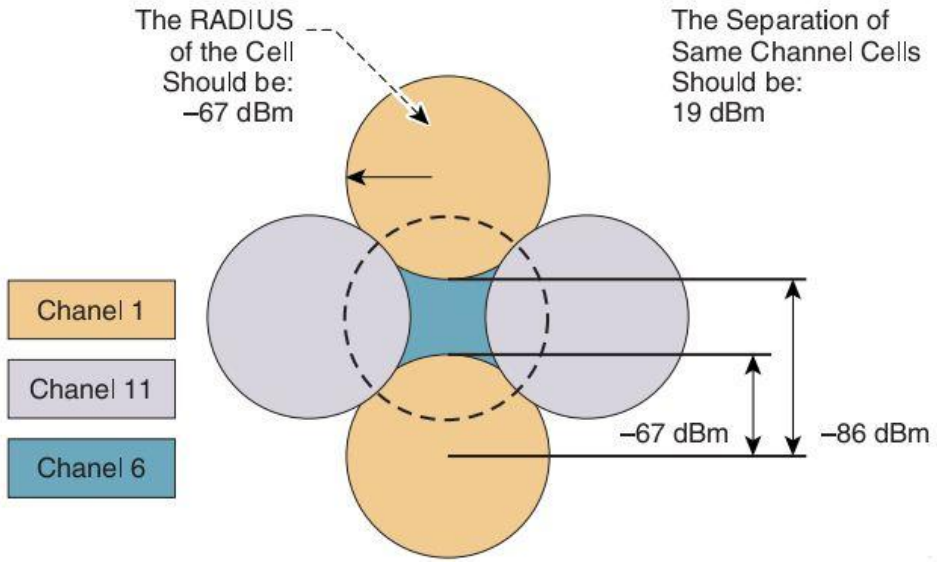


Figura 2.6: Radio de celdas, y separación de celdas con el mismo canal. Fuente [14], fig. 9-12.

El solapamiento entre celdas para escenarios con una densidad media debe ser de 20%, pero para escenarios con muy alta densidad de usuarios el solapamiento puede ser de hasta 50%; en el caso de escenarios con baja densidad de usuarios se prefiere que las celdas cubran la mayor área posible, teniendo siempre en cuenta que para lograr el *roaming* entre AP's vecinos, el solapamiento entre celdas debe ser 15% como mínimo [42].

Cuando se utilizan antenas semi-direccionales, como es el caso de los AP *outdoor* utilizados por ETECSA para el despliegue de las zonas WiFi, el posicionamiento de los AP se vuelve

un poco más crítico, debido precisamente a que el patrón de radiación no es circular y es necesario orientar las antenas; no obstante, de manera general, las reglas son las mismas:

- Minimizar los obstáculos que la señal debe atravesar, atendiendo a la atenuación que estos ofrecen.
- Asegurarse de que los AP "miran" directamente a su área de cobertura, no ponerlos detrás de columnas.
- Posicionar los AP lejos de fuentes de interferencia (cámaras y teléfonos inalámbricos, hornos de microonda, dispositivos Bluetooth, AP de otras WLAN, etc.).
- Seleccionar las frecuencias de los AP, basándose en la dirección de las antenas, para evitar la interferencia co-canal en cada área de cobertura.

La figura 2.7 muestra algunas de las formas recomendadas para la instalación de AP con antenas semi-direccionales o sectoriales, nótese que la forma recomendada de instalar varios AP es de un punto hacia afuera cubriendo toda el área, de esta forma se minimiza la interferencia co-canal y se garantiza un apropiado solapamiento de celdas.

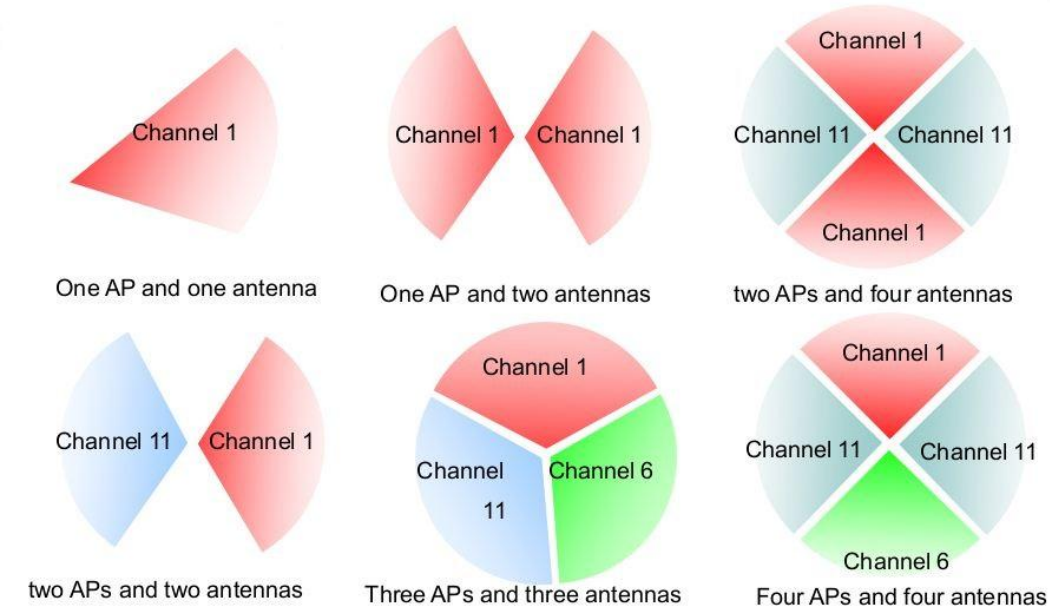
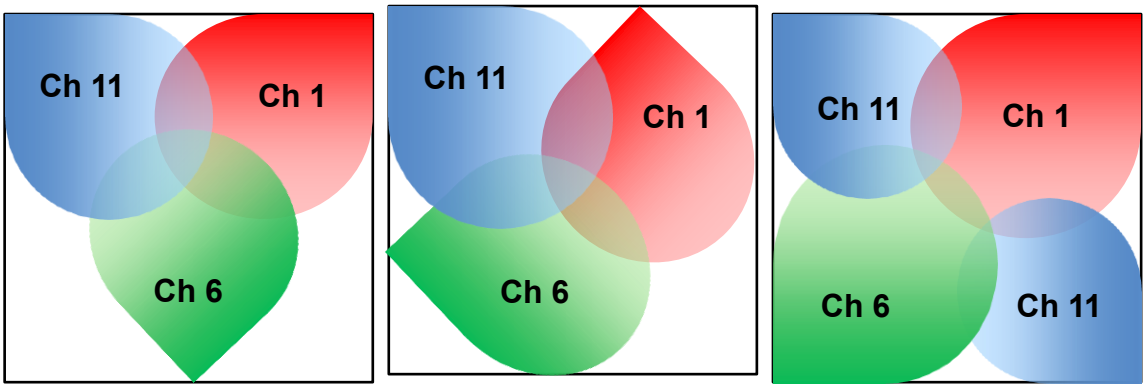


Figura 2.7: Distribución correcta de celdas con antenas sectoriales. Fuente [43], pag. 32.

En escenarios reales, las características del terreno no siempre permiten este tipo de distribución, sobre todo en espacios abiertos como parques, donde la presencia de equipamiento puede dar al traste con la estética del lugar, además que es necesario poner cables hacia los equipos para su alimentación y enlace. En la figura 2.8 se muestran variantes alternativas para estos casos, siempre cuidando no usar cables Ethernet mayores de 80 m, si queremos alimentar los AP usando PoE.

En el escenario de la imagen de la izquierda, se usan tres APs, por lo que no existirá interferencia co-canal en la banda de 2.4 GHz, al menos dentro de la propia red; esta distribución tiene el inconveniente que en las esquinas de la zona "sur" el nivel de señal será pobre, por lo que los AP deben situarse y orientarse atendiendo al interés de cobertura dentro del área, como se muestra en la imagen del centro.



Tres AP con tres antenas (a) **Tres AP con tres antenas (b)** **Cuatro AP con cuatro antenas**

Figura 2.8: Distribución de celdas con antenas sectoriales. Fuente elaboración propia.

La imagen de la derecha representa un escenario con cuatro APs, por lo que en la banda de 2.4 GHz existirá interferencia co-canal entre dos de ellos, en los cuales debe cuidarse no usar el canal 1, por ser el que está más expuesto a interferencias externas; también es necesario ajustar la potencia en estos AP (representados en la figura por el canal 11) de forma que estas dos celdas no se solapen, con vistas a minimizar la interferencia co-canal; otra forma de lograr esto es orientar convenientemente las antenas, de manera que no se miren directamente. Cualquiera que sea la distribución de los AP, siempre debe cuidarse que estén separados un mínimo de 6 m entre ellos.

2.4.1 Diseño de *throughput*

El diseño de *throughput* consiste en determinar el ancho de banda requerido por cada usuario y el número de usuarios concurrentes, con el fin de determinar la cantidad de AP y bandas de trabajo necesarios. En este análisis es necesario tener en cuenta que con el aumento de los usuarios concurrentes disminuye el ancho de banda disponible para cada uno de ellos.

La experiencia práctica simplifica notablemente este cálculo, un AP trabajando en una banda de frecuencias puede soportar 20 usuarios con un *throughput* de 1 Mb/s en el *uplink* y 2 Mb/s en el *downlink*, si trabaja en dos bandas simultáneamente, puede soportar potencialmente 40 usuarios. En diseños para alta densidad de usuarios esto se puede considerar como un buen *throughput* y una concurrencia de usuarios elevada. En la práctica siempre será mayor el número de usuarios conectados en la banda de 2.4 GHz que en la banda de 5 GHz, por estar más difundido el uso de la primera y porque aún muchos dispositivos no soportan la segunda. También se puede sacrificar un poco el *throughput*, en aras de lograr mayor concurrencia de usuarios por AP, por ejemplo, con 512 Kb/s en el *uplink* y 1.5 Mb/s en el *downlink*, se logran hasta unos 50 en las dos bandas [41].

En un escenario con cuatro APs funcionando en ambas bandas, en donde se ha diseñado cuidadosamente el área de cobertura de cada celda, las antenas están correctamente orientadas, se ha evitado el sobre solapamiento de celdas y la interferencia co-canal, es usual poder alcanzar 150 usuarios concurrentes sin comprometer el *throughput.*

2.4.2 Diseño de cobertura

Por diseño de cobertura se entiende determinar el tamaño de las celdas, o lo que es lo mismo, su área de cobertura, esto va depender en primera instancia del tipo de escenario: en interiores o exteriores; para baja o alta densidad de usuarios; obstáculos que pueden atenuar la señal como paredes, vigas y columnas (en el caso de interiores) o árboles, vallas y edificaciones (para exteriores). En espacios abiertos, el radio de cobertura recomendado para un solo AP es de 20 m [43].

Cuando se cuenta con herramientas de simulación, el diseño de cobertura cosiste en "construir" virtualmente un escenario lo más parecido posible al real, y el software hace todo el trabajo. Huawei recomienda el uso de "*WLAN Planner",* Cisco por su parte utiliza "*WCS Deployment Planning Tool*", ambas son herramientas propietarias para el planeamiento y diseño de redes WLAN; otros proveedores como HP (*Aruba Networks*) recomienda el uso de "*Aruba's VisualRF Plan*", que es una herramienta que permite hacer *survey* virtuales [44].

Después de la implementación de la red inalámbrica, es necesario hacer nuevamente un *survey* en el sitio, para comprobar en la práctica el diseño de cobertura. Para ello, se pueden usar herramientas sencillas como *inSSIDer* (recomendada por Huawei, disponible gratis para Windows y Android), pero es más recomendable usar otras más profesionales como *AirMagnet Survey*, *Ekahau Site Survey*, o *VisiWave Site Survey*. Es recomendable usar siempre la misma herramienta en todos los *survey,* pues las diferencias entre estas pueden introducir errores [42].

Las herramientas profesionales son caras, incluso cuando una empresa decide invertir en ellas, normalmente vienen amarradas a licencias de hardware o a licencias de software por utilización, lo que provoca que estas aplicaciones solo funcionen en las máquinas por las que se pagó. Muchas son las aplicaciones no profesionales que podemos encontrar para hacer *survey* en los sitios, pero esto no ocurre con las herramientas para simulación de redes inalámbricas. Afortunadamente, existe un método relativamente sencillo que permite hacer un cálculo aproximado del área de cobertura de celdas WLAN, atendiendo a la estimación del enlace (*Link Budget*) el cual exponemos a continuación [41].

En enlaces inalámbricos el *Link Budget* puede calcularse con la siguiente ecuación:

$$Pr = Pt + Gt + Gr - PL - Ls \quad (2.1)$$

Donde:

- **Pr**: Nivel de recepción (dB, dBm, W, o mW)
- **Pt**: Potencia de transmisión (dB, dBm, W, o mW)
- **Gt**: Ganancia de la antena de transmisión (dBi)
- **Gr**: Ganancia de la antena de recepción (dBi)
- **PL**: Pérdidas de trayecto (*Path Loss*) (dB)
- **Ls**: Pérdidas en cables y componentes (dB)

Para hacer una estimación de cobertura, no interesa conocer el nivel de señal en el receptor, pues esto dependerá de las características de cada dispositivo, sino la intensidad de señal (*signal strength*) en las fronteras de la celda, por lo que la ecuación queda así:

$$Ss = Pt + Gt - Ta - Sa - Ls \quad (2.2)$$

Dónde:

$$PL = Ta + Sa \quad (2.3)$$

- **Ss**: Intensidad de señal (*signal strength*) (dBm)
- **Sa**: Atenuación de la señal debido a obstáculos (dBm)
- **Ta**: Atenuación de la Transmisión (dBm)

En la ecuación 2.2 se asume nula la ganancia de la antena de recepción (**Gr = 0**), se sustituye el nivel de recepción (**Pr**) por intensidad de señal (**Ss**), y se descompone la pérdida de trayecto (**PL**) en atenuación de la señal transmitida en espacio abierto (**Ta**) y Atenuación de la señal debido a obstáculos (**Sa**).

En el caso de AP con antenas *built-in*, las pérdidas en cables y componentes son despreciables por lo que **Ls = 0**.

En espacios abiertos sin obstáculos **Sa = 0**, de existir obstáculos se puede estimar la atenuación que estos producen según la tabla 2.2.

Tabla 2.2 Atenuación producida por objetos. Fuente [41] pag. 499.

Obstáculos	**Pérdidas por penetración (dB)**	
	2.4 GHz	**5 GHz**
Materiales sintéticos	**2**	**3**
Asbesto	**3**	**4**
Puerta de Madera	**3**	**4**
Ventana de Cristal (5 mm)	**4**	**7**
Vegetación (follaje)	**7**	**10**
Cristal coloreado grueso (8 mm)	**8**	**10**
Ladrillo (12 cm de espesor)	**10**	**20**
Ladrillo (24 cm de espesor)	**15**	**25**
Hormigón	**25**	**30**
Metal	**30**	**35**

La atenuación de la señal transmitida (**Ta**) se puede estimar por la relación que esta tiene con la distancia y la frecuencia, según la tabla 2.3.

Tabla 2.3 Relación entre señal transmitida y distancia. Fuente [41] pag. 498.

Distancia	**1 m**	**2 m**	**5 m**	**10 m**	**20 m**	**40 m**	**80 m**	**100 m**
2.4 GHz	46.0 dB	53.8 dB	64.2 dB	72.0 dB	79.8 dB	87.6 dB	95.5 dB	98.0 dB
5 GHz	56.0 dB	63.8 dB	74.2 dB	82.0 dB	89.8 dB	97.6 dB	105.5 dB	108 dB

Si se quiere obtener la distancia, partiendo de una intensidad de señal deseada (**Ss**), se calcula la atenuación de la señal transmitida (**Ta**) de la ecuación 2.2, si se asume que no hay obstáculos nos queda la siguiente ecuación:

$$Ta = Pt + Gt - Ss \quad (2.4)$$

Por ejemplo, si se usan AP *indoor* configurados con Pt = 20 dBm, y se quiere que las celdas sean de 20 m de radio, según la tabla 2.3, Ta = 89.8 para la banda de 5 GHz, la ganancia de las antenas se obtiene del manual del AP [38], que en este caso es 3 dBi, usando la ecuación 2.2, obtenemos que en la frontera de la celda la intensidad de señal es -66.8 dBm. Este valor coincide con lo recomendado, como se mostró en la figura 2.6.

Se ilustrará con otro ejemplo, ahora se determinará el alcance en línea recta sin obstáculos de un AP *outdoor* con antenas direccionales, configurado a 20 dBm en la banda de 2.4 GHz, para celdas con intensidad de señal en su frontera de -66 dBm (Ss), del manual del AP se obtiene la ganancia de las antenas [39], que es 12 dBi para 2.4 GHz (14.5 dBi para 5 GHz). Usando la ecuación 2.4 se calcula Ta = 98 dBm, de acuerdo a la tabla 2.3 esto corresponde a una distancia de 100 m.

Los datos usados en el último ejemplo no se escogieron al azar, de hecho, en las zonas WiFi de ETECSA, los AP están configurados a 20 dBm en la banda de 2.4 GHz y a 23 dBm en la banda de 5 GHz, 3 dB por encima (Huawei, Cisco, y Aruba Networks recomiendan que sea 6 dB por encima). Si bien es cierto que cien metros de radio pueden parecer exagerados, recuérdese que para este cálculo no se tuvo en cuenta el follaje de los árboles y otros obstáculos que casi siempre están presentes en la práctica, lo cual reduce notablemente esta distancia.

Como las antenas son direccionales, se debe tener en cuenta este dato, junto con el ancho vertical del haz, para escoger la altura y *downtilt* de los AP, evitando reflexiones en el terreno, para lo cual nos podemos auxiliar de la siguiente ecuación:

$$Adt = tan^{-1} \boldsymbol{((Ht - Hr) / D)} \quad (2.5)$$

Donde:

- **Adt**: Ángulo de *downtilt* con respecto a la horizontal (deg)
- **Ht**: Altura de la antena transmisora (m)
- **Hr**: Altura de la antena receptora (m)
- **D**: Distancia entre transmisor y receptor (m)

En esta ecuación supone que el transmisor y el receptor se están “mirando” directamente, por lo que D es una distancia media entre el radio de ataque interior y exterior. Para estos AP, el ancho del haz en sentido vertical es de 28° para 2.4 GHz y de 15° para 5 GHz. Si tomamos D como radio exterior de la celda, para calcular el ángulo de *downtilt*, hay que sumarle 14° o 7.5° (según sea el caso) al resultado de la ecuación 2.5. Si despejamos D, y le sumamos nuevamente al ángulo de *downtilt* la mitad del ángulo de ancho de haz vertical, podemos obtener el radio interior de la celda:

$$R_{(interior,\ exterior)} = \boldsymbol{(Ht - Hr) / tan(}Adt \pm Abw/2\boldsymbol{)} \quad (2.6)$$

Donde:

- **Abw**: Ángulo de ancho de haz (*beamwidth*) vertical (deg)
- **$R_{(interior,\ exterior)}$**: Radio interior o exterior de la celda. (m)

Siguiendo con el ejemplo anterior, tomando como altura del receptor el nivel del piso **Hr = 0**, asumiendo que los AP estén a 3 m de altura, y se quiere que las celdas no sean mayores de 100 m en la banda de 2.4 GHz, de la expresión 2.5 se obtiene un *downtilt* de 15.7°; luego, aplicando 2.6 se pude conocer que el radio interior de la celda será 5.25 m, en este punto la intensidad de señal obtenida según expresión 2.2 será de -32 dBm.

Este resultado se calculó al nivel del suelo, a una altura del receptor de 1 m (una persona parada con un terminal en la mano), tendrá señal directa desde una distancia de 3.5 m, hasta 67m.

En la práctica, la distancia es lo que se conoce, y a partir de esta se calcula el ángulo de *downtilt* y la potencia de transmisión, que es lo único que se puede ajustar por separado, cuando se trabaja en ambas bandas simultáneamente; hay que hacer los cálculos para ambas frecuencias, ya que incluso dentro de la propia banda de 5 GHz hay diferencias por la separación que existe entre sub-bandas. Para encontrar el ángulo de *downtilt*, se establece una relación de compromiso atendiendo a que los *beamwidth* también son diferentes. Las pérdidas por propagación de la banda de 5 GHz son notablemente mayores que a 2.4 GHz, por lo que siempre las celdas a esta frecuencia serán menores y deberán ser compensadas con una potencia mayor, teniendo en cuenta que este aumento está condicionado por la potencia máxima de trabajo del AP en cuestión.

2.5 Parámetros recomendados para garantizar QoS en redes VoWLAN

La voz, como cualquier otra información, viaja en paquetes sobre las redes IP con una capacidad máxima fija. La principal diferencia entre el tráfico de voz y el de datos, es el hecho de que los paquetes de datos pueden ser reenviados si se pierden, mientras que con la voz no tiene sentido hacerlo, ya que es un *stream* continuo de paquetes. Como el reenvío de paquetes de voz no es una opción, los parámetros para garantizar el tráfico de voz deben ser configurados con cuidado.

Generalmente los paquetes de voz necesitan más ancho de banda que los datos, y ese ancho de banda necesita ser protegido para que se mantenga constante, por esta razón, el tráfico de voz funciona mejor cuando el *Service profile* de la WLAN (SSID) y el *Radio profile* usados, están dedicados y diseñados para la voz. Se recomienda que el tráfico de voz y datos estén separados por SSID, también debe asegurarse una cobertura con un nivel adecuado de -60 dBm a -70 dBm y capacidad para la carga de tráfico de voz esperada. Debe considerarse el uso de *Call Admission Control* (CAC), en el *Service profile* destinado a la voz, para limitar el número de usuarios concurrentes por AP [45].

El tráfico de voz debe usar "*seamless roaming"* para que ninguna llamada sea interrumpida durante este, para ello, el *roaming* debe ocurrir dentro de 50 ms y el solapamiento entre *access points* debe ser de al menos el 20%. En caso de usar los APs como *bridge* para soportar *backhaul*, el número de saltos debe ser minimizado [46].

Todo equipamiento usado para soportar tráfico de voz debe soportar Calidad se Servicio (QoS), debe asegurarse que los *switches* y *routers* usados para la infraestructura de la red, soporten y preserven la prioridad de paquetes de voz; de igual forma, Los *access points*, así como los terminales VoIP deben soportar *Wi-Fi Multimedia* (WMM) [47].

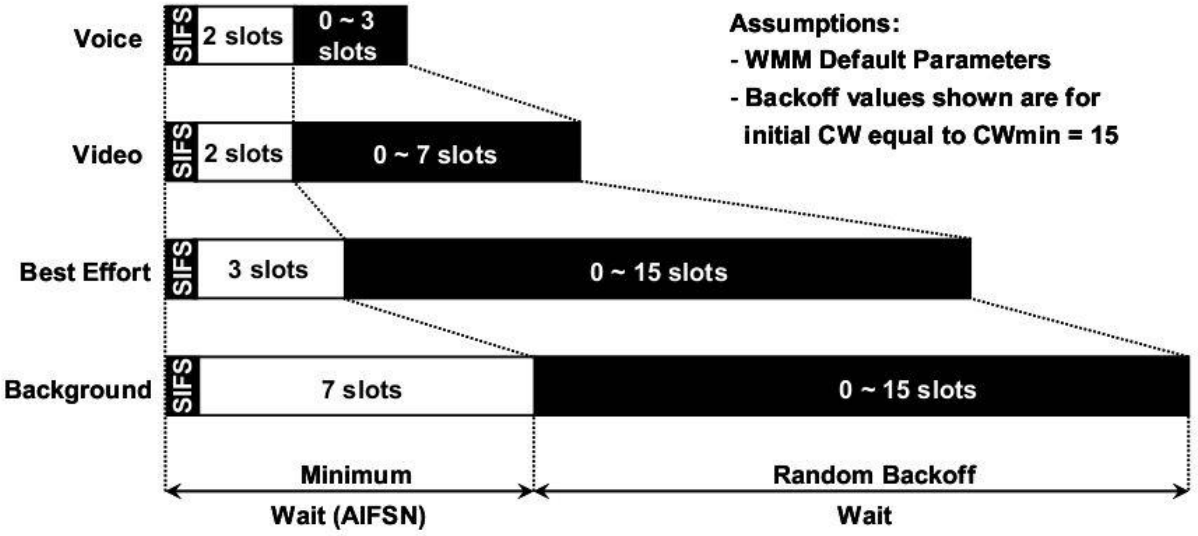


Figura 2.9: Valores por defecto de AIFSN y *Backoff* (CWmin). Fuente [2], pag. 8.

Para garantizar que se priorice el tráfico de voz en el medio inalámbrico, no basta con que los APs implementen el *subset* WMM del estándar IEEE802.11e, también se precisa que los parámetros que definen su comportamiento ante cada tipo de tráfico estén bien ajustados. En el Capítulo 1, tabla 1.1, se definen los valores recomendados por Cisco de *AIFS, CWmin, CWmax y TXOPLimit* para las diferentes categorías de acceso, a modo de comparación, en la tabla 2.4 se muestran los valores recomendados por Huawei, y la figura 2.9 muestra dos de los valores por defecto (*AIFS y CWmin*), según el estándar IEEE802.11e.

Tabla 2.4 Valores EDCA recomendados por Huawei. Fuente [28] pag. 613.

AC	***AIFSN***	***CWmin***	***CWmax***	***TXOPLimit***
VO	*2*	*15*	*30*	*1.5 ms*
VI	*2*	*30*	*60*	*3 ms*
BE	*3*	*60*	*max*	*0*
BK	*7*	*60*	*max*	*0*

Del análisis de ambas tablas, Huawei propone una ventana de contención (*CWmin, CWmax*) mayor, mientras que reduce el tiempo de *transmission opportunities* (TXOPLimit). Por los resultados de experimentos realizados, el autor de este trabajo se inclina más por los valores recomendados por Cisco.

2.6 Consideraciones finales del capítulo 2

El enlace inalámbrico entre un cliente y un *Access Point* es compartido entre todos los clientes que se encuentren dentro del rango de alcance de una frecuencia en particular; por lo tanto, la intensidad de señal no es en realidad una indicación de calidad del enlace, como sucede en una conexión por cable. En el caso de las redes WiFi, la capacidad de la red debe ser determinada por la demanda de clientes; por lo tanto esta debe estar diseñada para distribuir la carga de manera efectiva en todo el espectro disponible. Otros factores como la capacidad espectral, la utilización de canales, la interferencia, la reutilización de frecuencias y los requisitos reglamentarios se convierten en variables de diseño críticas, además de la cobertura y la intensidad de la señal. Esto requiere un análisis detallado de las capacidades del cliente, los requisitos de aplicación, las características de las instalaciones y el uso apropiado de *Access Points* suficientes. El objetivo es segmentar al máximo los dominios de los clientes utilizando radios diferentes para aumentar al máximo la capacidad espectral disponible.

CAPÍTULO 3. Evaluación del desempeño de redes WiFi con QoS

Los indicadores clave de desempeño (*Key Performance Indicators, KPI*) importantes para VoIP, son dependientes de la arquitectura de la red. Los únicos tres problemas que afectan la calidad de la voz son: la latencia, el *jitter*, y la pérdida de paquetes. Además, el tráfico de voz puede tener problemas de *roaming* porque las personas son propensas a pasear con los teléfonos [48].

La **latencia** o demora, es la cantidad de tiempo que toma al sonido de la voz alcanzar el oído de la otra persona. La máxima latencia permitida para VoIP es de 150 ms a 200 ms, dependiendo de los requerimientos de calidad del usuario.

El ***jitter*** es la variación en la demora entre paquetes. El *jitter buffer* retiene los paquetes, de forma que sean recibidos a intervalos coherentes. Un *jitter* significante puede causar que el *jitter buffer* se incremente a tal punto que la latencia alcance valores inaceptables. Para aplicaciones en tiempo real, es recomendable que el *Jitter* no supere los 30 ms.

La **pérdida de paquetes** ocurre cuando la demora máxima especificada en el *jitter buffer* es excedida, una pérdida de paquetes por encima del 5% es considerada inaceptable cuando se usa el códec G.711, pero si se usan otros códecs más eficientes como el G729, la pérdida de paquetes no debe superar el 1%.

Los resultados de los experimentos que serán mostrados en este capítulo, están enfocados en evaluar escenarios WLAN en cuanto a estos indicadores de desempeño, demostrando la eficacia del uso de técnicas de calidad de servicio en dichas redes.

3.1 Descripción de escenarios de simulación

Para evaluar el desempeño de redes VoWLAN de alta densidad de usuarios, se utilizó el software “OPNET Modeler 14.5 – Educational Version”, el cual brinda las herramientas necesarias para la simulación de escenarios inalámbricos [49].

En la construcción de los escenarios se usaron algunas aproximaciones, la versión de Opnet utilizada no trae el estándar IEEE802.11n, pero como en la red de ETECSA esta norma se utiliza en compatibilidad con los estándar anteriores IEEE802.11a/b/g, que si están en los modelos de redes inalámbricas del Opnet 14.5, podemos asumir que para escenarios con alta densidad de usuarios, el estándar “n” tendrá un comportamiento similar al “g” en la banda de 2.4 GHz y al “a” en la banda de 5 GHz. La diferencia entre estos estándares, para el modo de trabajo configurado, está en que el “n” logra velocidades de hasta 65 Mb/s, mientras que “a” y “g” alcanzan 54 Mb/s; al estar limitado a 1 Mb/s la velocidad de conexión por usuario en las zonas WiFi de ETECSA, esto solo afectaría la cantidad de usuarios concurrentes por AP.

De acuerdo con lo planificado usualmente en las zonas de acceso WiFi, los AP se situaron a 3 m de altura, a una potencia de 20 dBm para la banda de 2.4 GHz y de 23 dBm para 5 GHz, y con antenas omnidireccionales, ya que por limitaciones del simulador no se pueden usar antenas direccionales.

La figura 3.1muestra el primer escenario, compuesto por 3 *Access Points* y 30 usuarios, los cuales se situaron a diferentes alturas, posiciones aleatorias, y algunos de ellos en movimiento, dentro de un área de 2500 m^2 (50 m x 50 m). Para generar un tráfico en la red que nos permita evaluar los KPI determinantes para la QoS, se configuró trafico *best effort* a la mitad de los usuarios, y tráfico de voz a la mitad restante. No se pudo generar un tráfico *backgroud* en la red, ya que esta funcionalidad no es compatible con el modelo de redes inalámbricas del Opnet 14.5.

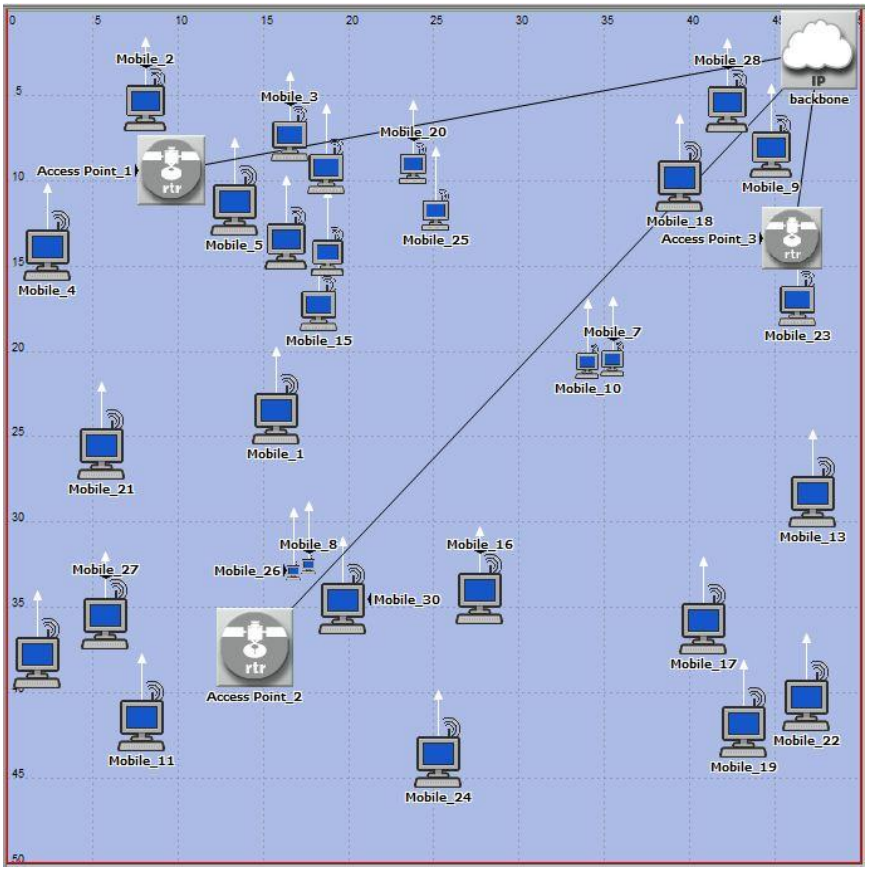


Figura 3.1: Escenario 1, WLAN, 3 AP, 30 usuarios. Fuente elaboración propia.

Sobre este escenario se realizaron experimentos usando la banda de 2.4 GHz con norma “b” y “g”, y la banda de 5 GHz con la norma “a”; esto permitió comparar el estándar “b” (modulación DSSS, velocidad de conexión máxima: 11 Mb/s), muy usado antiguamente y aún en explotación, con los estándares “a”, “g”, y “n” (modulación OFDM); además, se comparan las dos bandas usadas (2.4 GHz y 5 GHz).

Luego, sobre este mismo escenario se aplicaron las enmiendas que introduce IEEE802.11e, dotando a la WLAN de calidad del servicio para aplicaciones en tiempo real, y se realizan los experimentos pertinentes que demuestran la influencia de estas mejoras en el desempeño de la red [50].

A modo de comparación, se construye un nuevo escenario con características similares, solo que en este se ponen 4 APs en lugar de tres, uno en cada esquina. Se repiten todos los experimentos anteriores sobre este nuevo escenario, que se muestra en la figura 3.2.

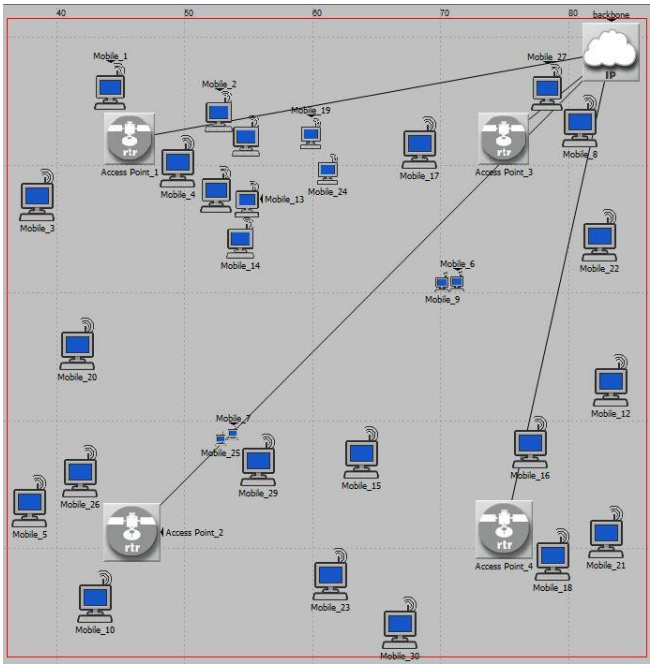


Figura 3.2: Escenario 2, WLAN, 4 AP, 30 usuarios. Fuente elaboración propia.

Las pruebas realizadas arrojaron que 30 usuarios no representan una carga elevada para para los escenarios evaluados, por lo que se construyó un tercer escenario con 3 AP y 100 usuarios que se muestra en la figura 3.3; en esta ocasión, solo se realizaron los experimentos en la banda de 2.4 GHz, primero sin aplicar técnicas de QoS, para evaluar el impacto sobre la red del aumento de usuarios y tráfico, luego se configuraron los parámetros de calidad de servicio, para demostrar que estos garantizan el buen desempeño de redes VoWLAN de alta densidad de usuarios.

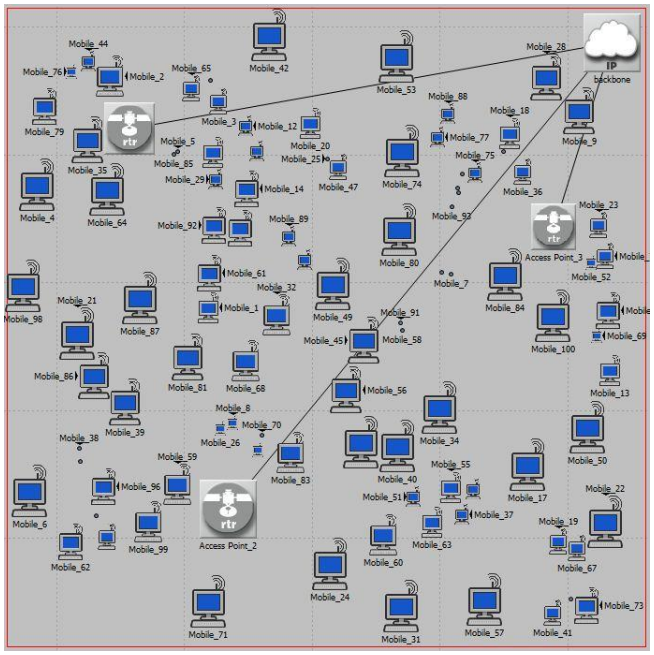


Figura 3.3: Escenario 3, WLAN, 3 AP, 100 usuarios. Fuente elaboración propia.

3.2 Análisis del resultado de los experimentos

Al evaluar los resultados de las simulaciones se tendrá en cuenta los KPI que afectan la calidad de servicio (QoS) para soportar servicios de VoIP, es decir, latencia, *jitter*, tasa de paquetes erróneos, y retransmisión de paquetes.

Como no es posible evaluar la demora de extremo a extremo en toda la arquitectura de red, ya que los escenarios solo comprenden la parte de la red de acceso inalámbrica, además de que esto sería contraproducente, pues el otro extremo de la comunicación de voz tendrá retardos muy variables, en dependencia del tipo de red (fija, móvil, internacional, etc.); para evaluar la latencia se utilizará el retardo o *delay* que se produce en la propia red inalámbrica. Al no existir un consenso en cual debe ser el valor del retardo en una WLAN para soportar servicios VoIP, se tomará como paradigma la demora que logran otras redes inalámbricas que si han sido creadas para estos fines, como es el caso de las redes LTE y WiMax; por lo que se evaluará la **latencia** a partir de un ***delay*** menor o igual a 10 ms.

El ***jitter*** se define como la varianza del retardo, en las mediciones que permite hacer el Opnet no se toma en cuenta este parámetro, pero se puede calcular como la diferencia entre el *delay* máximo y el mínimo. Al evaluar el ***jitter***, se considera como adecuado para aplicaciones de voz, siempre que sea menor de 20 ms.

Aunque es posible medir la **tasa de paquetes erróneos**, en los experimentos realizados no se observó *overflow* en los *jitter buffer*, ni en las colas, por lo que este parámetro no será evaluado; en su lugar, se observará el comportamiento de las colas (***queue size***) y de los intentos de retransmisión de paquetes (***retransmission attempts***), ya que para el tráfico de voz los paquetes no se retransmiten, sino que son descartados, de igual manera que los paquetes que por estar en colas muy largas llegan fuera de tiempo.

Por último, la **retransmisión de paquetes**, tampoco puede ser medida directamente, es necesario calcularla a partir del total de paquetes transmitidos y los intentos de retransmisión de paquetes. Aunque este parámetro no afecta la calidad del servicio para tráfico de voz, sobre todo cuando se aplican técnicas para garantizar la QoS, es recomendable que en redes que soportan VoIP, no supere el 20%.

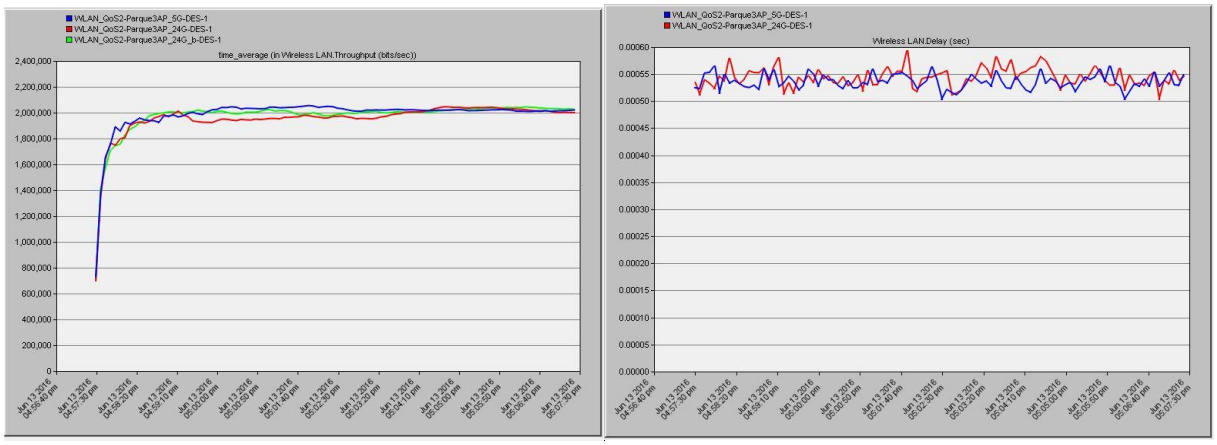
3.2.1 Primer experimento, comparación entre estándares WiFi

Descripción:

Usando el escenario 1, se evaluarán los estándares IEEE802.11 a/b/g en cuanto a los parámetros que afectan la QoS. No ha sido configurada la funcionalidad HCF (descrita en el epígrafe 1.1.4), por lo que el tráfico de voz no tendrá ninguna prioridad sobre el tráfico de datos. El *throughput* de la red es el mismo en las tres simulaciones, como se aprecia en la figura 3.4-a, donde el azul corresponde al estándar “a”, el rojo al “g”, y el verde al “b”.

Análisis de los resultados:

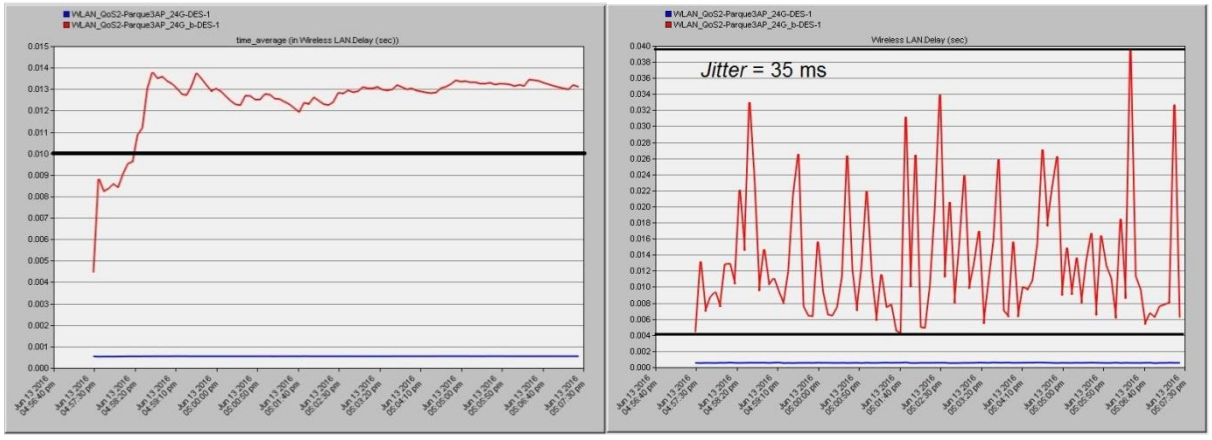
La figura 3.4-b muestra el comportamiento del *delay* y el *jitter*, para las normas “g” y “a”, se puede observar que estos dos parámetros se comportan de manera similar para ambas normas y que se mantienen muy bajos, *delay* = 0.55 ms, y *jitter* = 0.1 ms.



(a) (b)

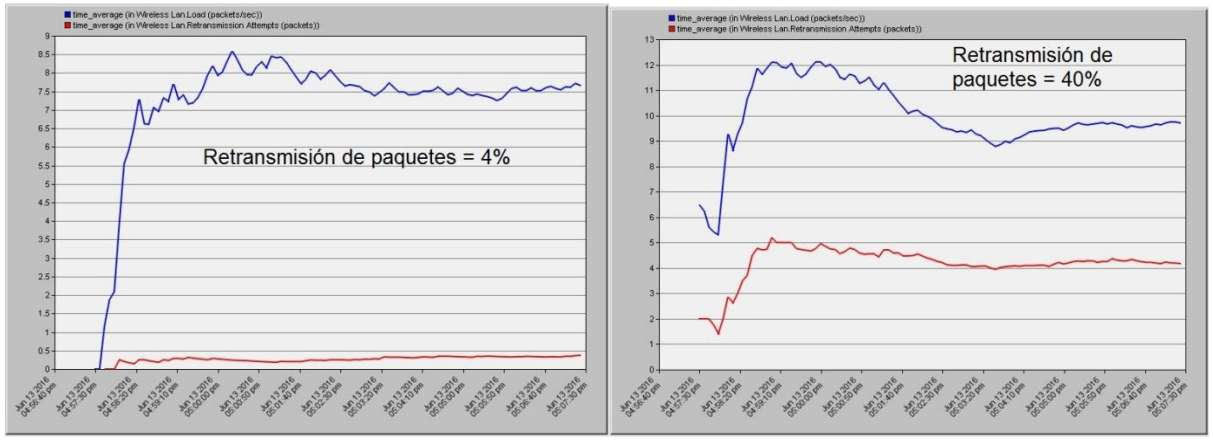
Figura 3.4: Experimento 1, (a) *throughput* IEEE802.11a/b/g, (b) *delay* & *jitter* IEEE802.11a/g.

En cambio, la figura 3.5 muestra el comportamiento del estándar “b” (rojo) con respecto a los estándares “a” y “g” (azul) en cuanto al *delay* (a), que supera los 10 ms, y al *jitter* (b), que supera los 30 ms.



(a) (b)

Figura 3.5: Experimento 1, (a) *delay*, (b) *jitter*, IEEE802.11a/b/g.



(a) (b)

Figura 3.6: Experimento 1, Retransmisión de paquetes (a) IEEE802.11a, (b) IEEE802.11b.

En la figura 3.6 se puede comparar el comportamiento de la retransmisión de paquetes, en el caso del estándar “a” es de aproximadamente un 4% (a) y en el estándar “g” alcanza el 5% (se muestra más adelante en la figura 3.9-a), mientras que para el estándar “b” es del 40%, el doble de lo permisible para la voz, que es 20%.

En conclusión, el estándar IEEE802.11b no es apropiado para soportar servicios de voz, además que tampoco tendría un buen desempeño en una red con alta densidad de usuarios. En cuanto a los estándares IEEE802.11a/g, y por supuesto el IEEE802.11n, hasta el momento tienen un buen desempeño, claro que 30 usuarios para 3 AP no es una densidad considerable.

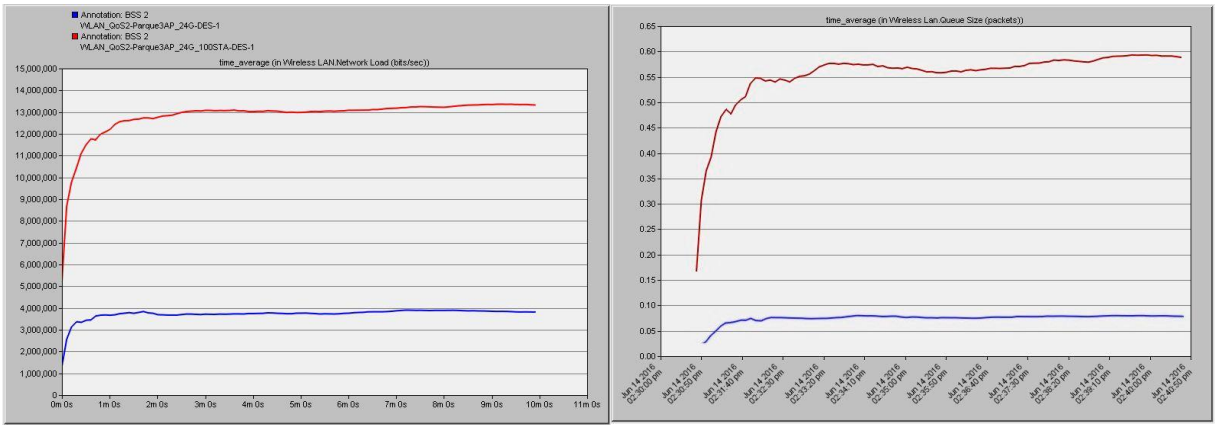
3.2.2 Segundo experimento, comportamiento con alta densidad

Descripción:

Por medio de los escenarios 1 y 3, en la banda d 2.4 GHz (estándar IEEE802.11g) se evaluará el comportamiento de los parámetros que afectan la QoS. Aún no ha sido configurada la funcionalidad HCF, básicamente, la única diferencia entre ambos escenarios es la cantidad de usuarios, que de 30 en el primer escenario, se eleva a 100.

Análisis de los resultados:

Con el aumento a 100 usuarios (gráfica en rojo), el tráfico total de la red aumenta de 4 Mb/s a 13 Mb/s, según muestra la figura 3.7-a; y el tamaño de las colas es 6 veces mayor que con 30 usuarios (gráfica en azul), como se observa en la figura 3.7-b, aunque no alcanza valor alarmantes, nótese que el aumento de las colas no es lineal, sino exponencial.

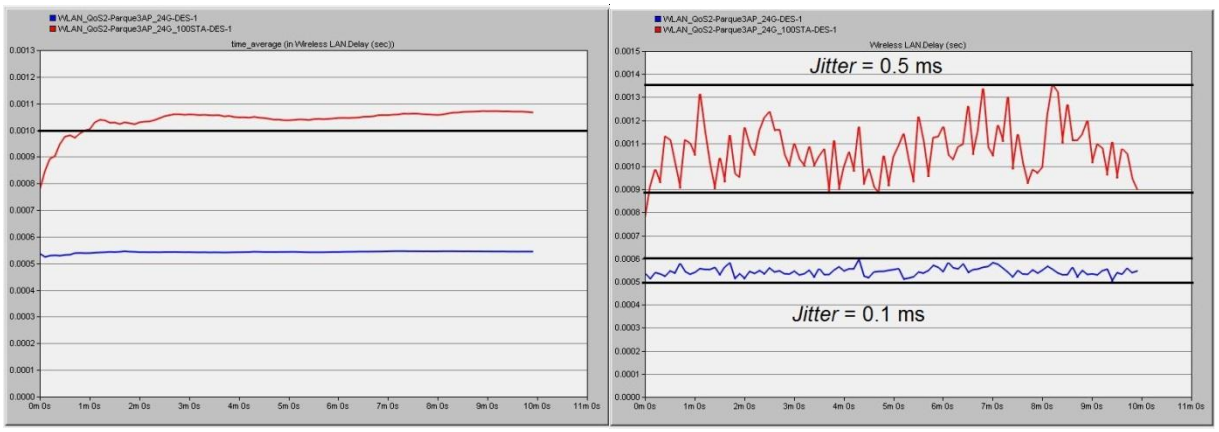


(a) (b)

Figura 3.7: Experimento 2, 30 usuarios vs 100 usuarios, (a) carga de la red, (b) tamaño de colas.

La demora en la red inalámbrica (figura 3.8-a) tampoco sube alarmantemente, mientras el comportamiento del *jitter* (figura 3.8-b), se mantiene muy por debajo de los 20 ms, pero aumenta 5 veces con respecto a la medición realizada en el experimento anterior.

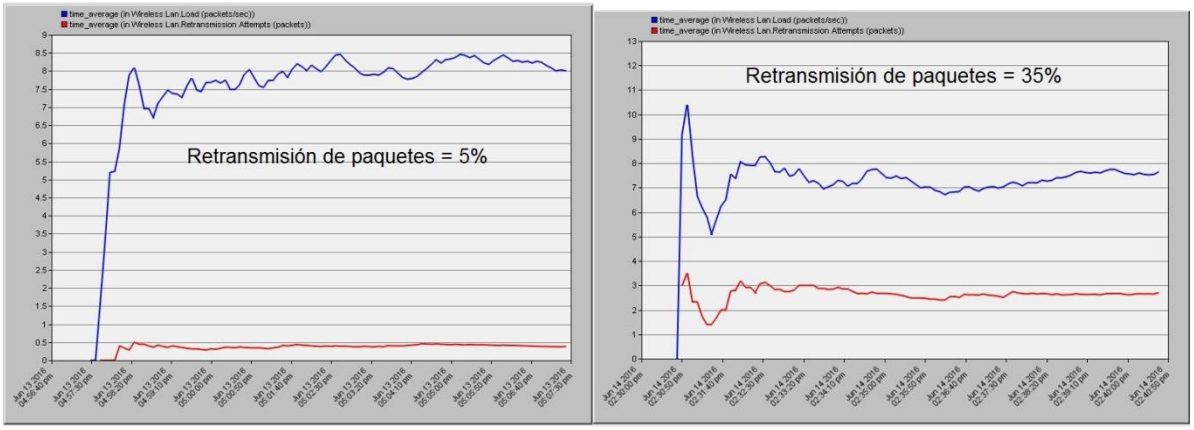
Si bien es cierto que los resultados vistos hasta ahora para un escenario de alta densidad de ususarios, no son suficientes como para interpretar un desempeño ineficiente de la WLAN, si se observa un aumento en los KPI que pueden afectar sensiblemente a la voz.



(a) (b)

Figura 3.8: Experimento 2, 30 usuarios vs 100 usuarios (a) *delay*, (b) *jitter*.

La figura 3.9 muestra la comparación entre ambos escenarios para la retransmisión de paquetes, este indicador sí alcanza valores totalmente fuera de lo recomendado para servicios en tiempo real, como se puede apreciar en la figura 3.9-b, para 100 usuarios hay un 35% de retransmisiones, muy por encima del 20% que es el umbral permisible.



(a) (b)

Figura 3.9: Experimento 2, Retransmisión de paquetes, (a) 30 usuarios, (b) 100 usuarios.

Concluyendo, para una WLAN con una alta densidad de usuarios, sin aplicar técnicas de QoS, no se garantiza un buen desempeño para tráfico de voz y en general, para cualquier tipo de tráfico en tiempo real.

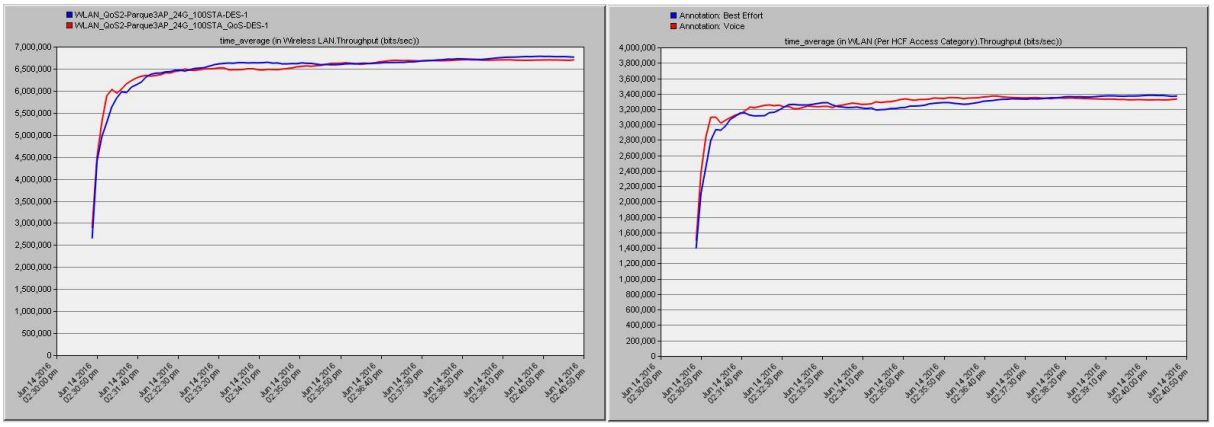
3.2.3 Tercer experimento, evaluación de calidad de servicio

Descripción:

Se configura en el escenario 3 la función HCF (*Hybrid Coordination Function*), introducida por la enmienda del estándar IEEE802.11e, y enfocada a mejorar el control de acceso al medio en redes WiFi, para proveerlas de calidad de servicio. Los resultados de la simulación serán comparados los resultados del segundo experimento, con el objetivo de demostrar que usando técnicas de QoS, las WLAN pueden cumplir con los requerimientos para soportar tráfico de voz, aún en escenarios con alta densidad de usuarios.

Análisis de los resultados:

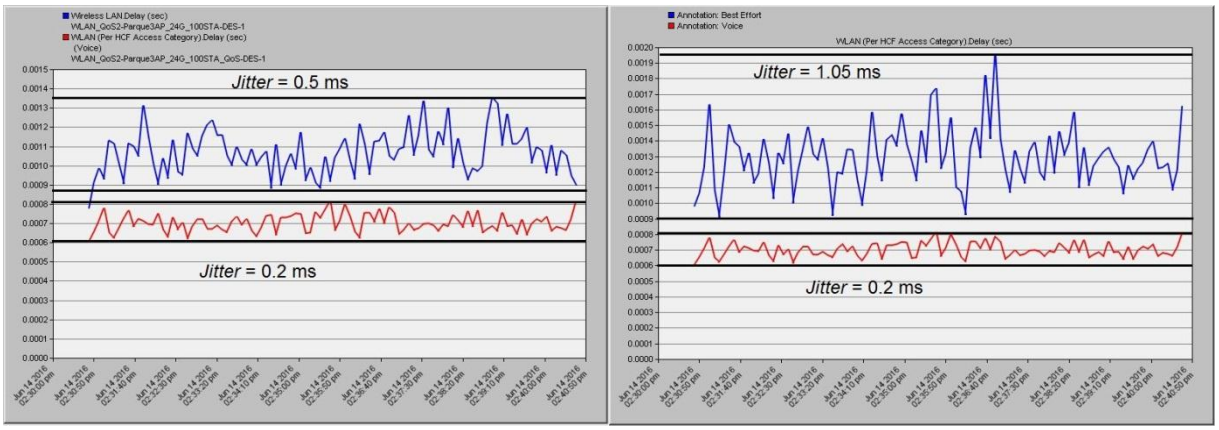
Como es de esperar, el hecho de activar la función HCF, no influye en el *throughput* de la red (figura 3.10-a), sin embargo, separa el tráfico por categorías; con el propósito de poder comparar el comportamiento de la red ante diferentes tipos de tráfico, se configuró la misma carga para tráfico *best effort*, que para tráfico de voz (figura 3.10-b).



(a) (b)

Figura 3.10: Experimento 3, *Throughput*, (a) Sin QoS vs QoS, (b) Tráfico *Best Effort* vs voz.

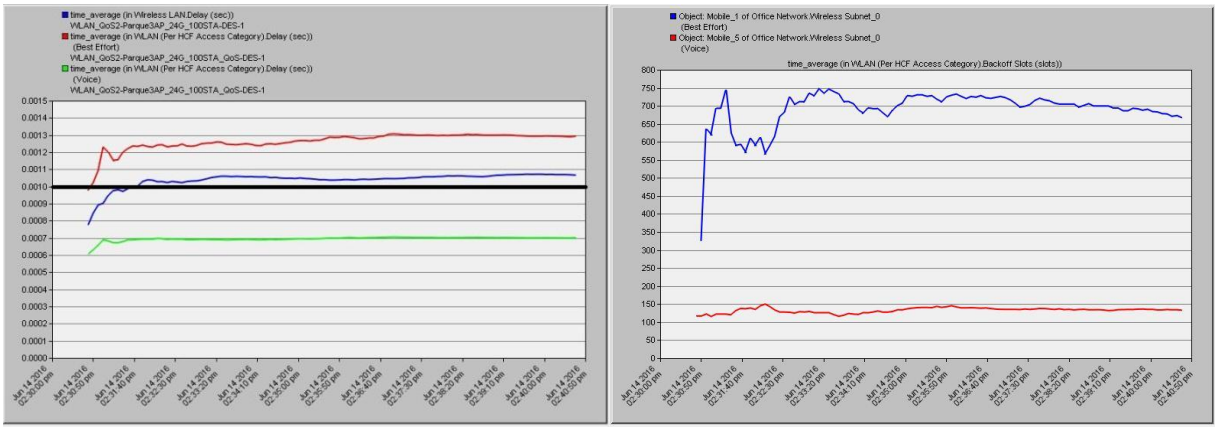
En la figura 3.11 se observa el comportamiento del *jitter* (varianza de la demora), que para el tráfico de voz mejora al punto de ser comparable con el valor obtenido en el primer experimento, al aplicar técnicas de QoS (figura 3.11-a), claro que esta mejora tiene un costo, y es que se eleva para tráfico *best effort* (figura 3.11-b), en donde no es un parámetro importante, aunque sigue estando en valores bajos.



(a) (b)

Figura 3.11: Experimento 3, *Jitter*, (a) Tráfico sin QoS vs voz, (b) Tráfico *Best Effort* vs voz.

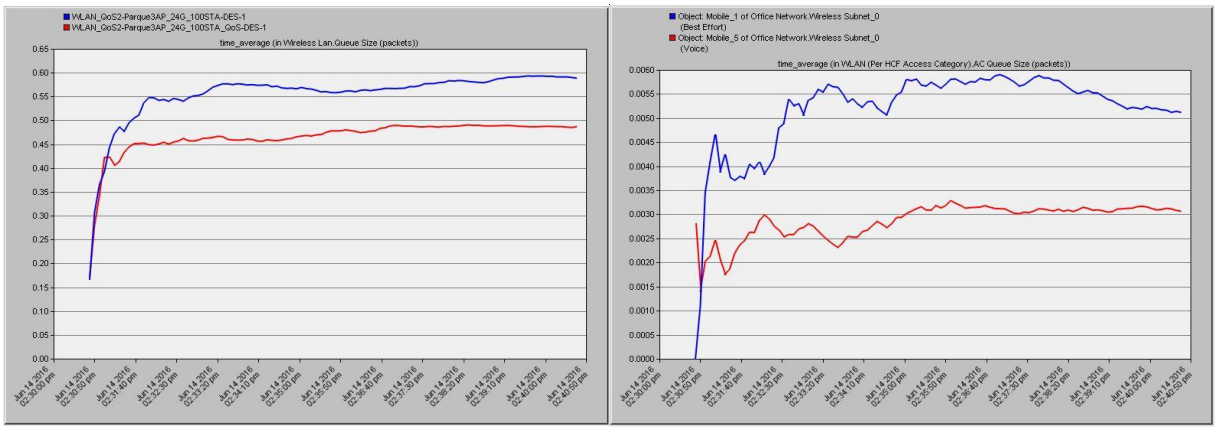
Para apreciar mejor la demora, en la figura 3.12-a se muestran estas tres mediciones usando el valor medio. El tráfico sin aplicar técnicas de QoS se representa en azul, el rojo para tráfico *best effort* y el verde la voz; nótese como el tráfico de voz es priorizado disminuyendo su demora con respecto a otros tipos de tráfico. La figura 3.12-b muestra como los *backoff slots* asignados son menores para el tráfico de voz, representado en rojo, que para el tráfico *best effort*, representado en azul.



(a) (b)

Figura 3.12: Experimento 3, (a) *Delay* sin QoS vs voz y *Best Effort*, (b) *Backoff Best Effort* vs voz.

El hecho de que el mecanismo de acceso al medio HCF, dé prioridad al tráfico de voz, también repercute en el tamaño de las colas de paquetes, en la figura 3.13-a se muestra en azul las colas para un tráfico sin aplicar técnicas de QoS, y en rojo aplicando HCF, mientras que en la figura 3.13-b se comparan las colas de paquetes para el tráfico *best effort* (azul) y de voz (rojo).



(a) (b)

Figura 3.13: Experimento 3, Tamaño de colas, (a) Sin QoS vs QoS, (b) Tráfico *Best Effort* vs voz.

De manera general, las mejoras introducidas por la función de acceso al medio HCF, no solo mejoran los KPI relativos al tráfico en tiempo real, sino que al optimizar el funcionamiento de la capa MAC, mejoran el desempeño de toda la red.

3.2.4 Cuarto experimento, balance de carga

Descripción:

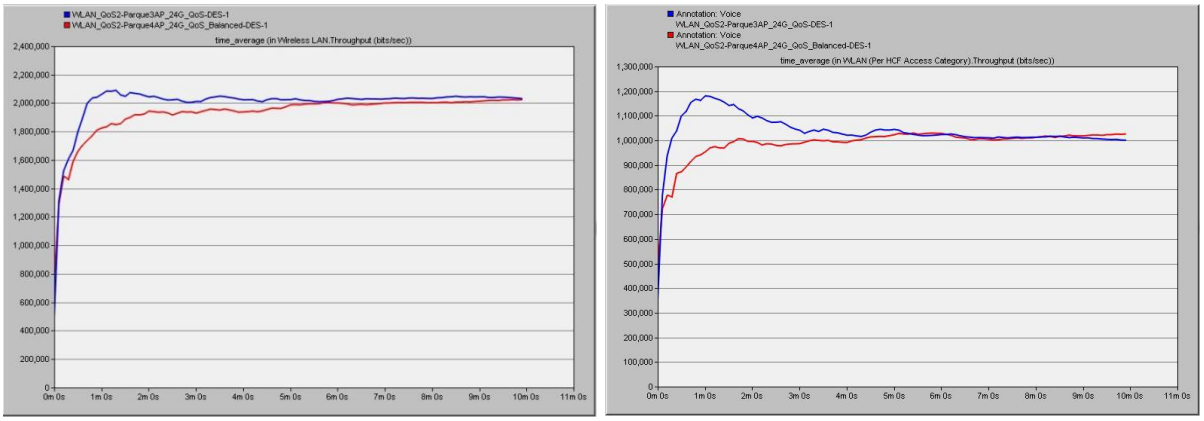
La funcionalidad de balance de carga, permite que dentro de la WLAN, la cantidad de usuarios que maneja cada AP esté siempre balanceada, independientemente de que los usuarios se muevan de lugar y hagan *hand-off* hacia otro AP.

En este experimento se usan los escenarios 1 y 2, ambos con 30 usuarios trabajando en la banda de 2.4 GHz, con la función HCF activada. En el primer escenario los tres AP tienen

una carga de usuarios aleatoria, esto en la práctica ocurre cuando no está activada la funcionalidad de balance de carga y muchos usuarios se acercan a un AP, en busca de sombra o comodidad. El segundo escenario tiene un correcto balance de carga entre sus cuatro AP, para lograr esto en la simulación, se configuró en cada AP un número fijo de usuarios, a los que no se les permite movilidad [51].

Análisis de los resultados:

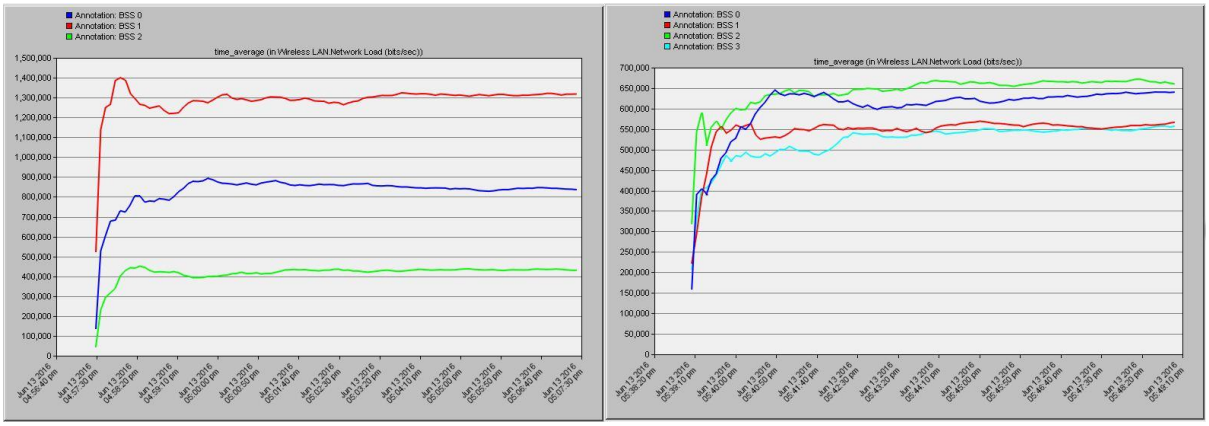
La carga de tráfico en ambos escenarios es la misma, por eso el hecho de usar 3 o 4 APs no afecta *el throughput* de la red, sin embargo, en la figura 3.14 se puede apreciar cómo en el caso de usar balance de carga (graficas rojas), el comportamiento del tráfico es más estable que cuando no se usa (graficas azules).



(a) (b)

Figura 3.14: Experimento 4, *Throughput*, 3 AP vs 4 AP, (a) Tráfico total, (b) Tráfico de voz.

La figura 3.15 muestra la carga de tráfico para cada AP, se puede observar el desbalance en el caso del escenario 1, y como para el escenario 2 la carga de los 4 APs es similar.

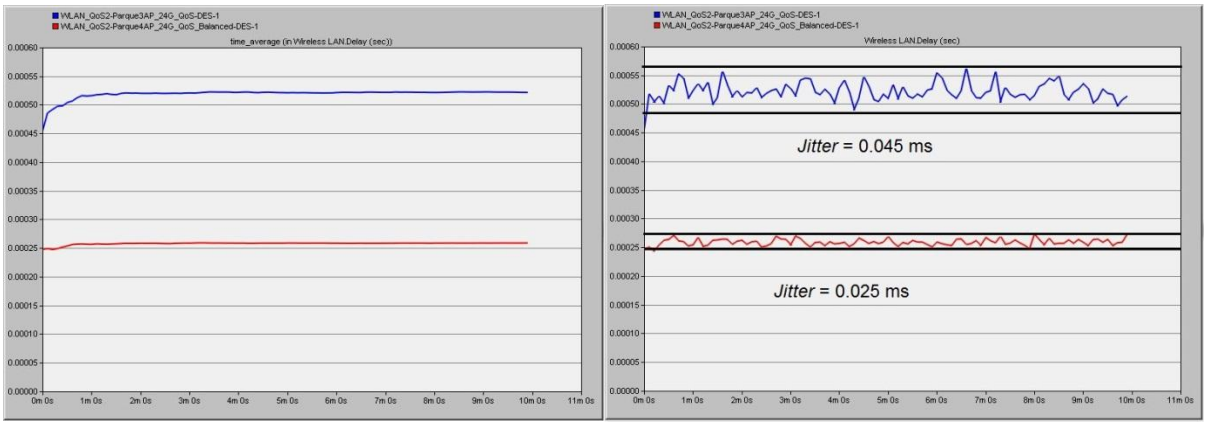


(a) (b)

Figura 3.15: Experimento 4, Balance de carga entre APs, (a) Escenario 1, (b) Escenario 2.

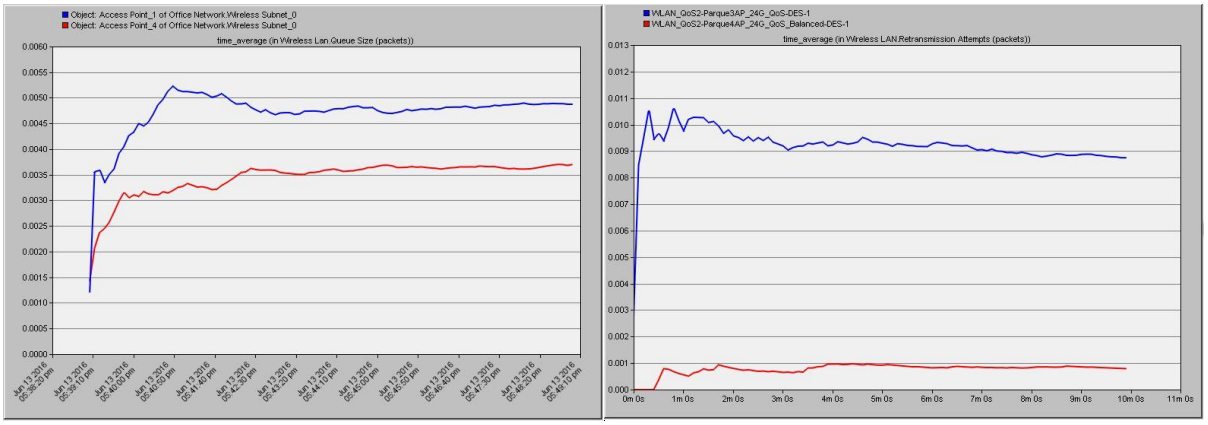
Estos resultados coinciden con los esperados cuando se diseñó el experimento, ahora se verá el impacto del balance de carga en los parámetros determinantes para la calidad de servicio para tráfico de voz.

En la figura 3.16 se compara el comportamiento de la demora (a) y el *Jitter* (b) para ambos escenarios, claramente se aprecia cómo ambos indicadores se reducen a la mitad cuando se emplea balance de carga. Un comportamiento similar presenta el tamaño de las colas, como muestra la figura 3.17-a, estas mejoras en el desempeño de la red tienen su mayor repercusión en la retransmisión de paquetes, que se reduce casi diez veces, como se observa en la figura 3.17-b.



(a) (b)

Figura 3.16: Experimento 4, Balance de carga 3 AP vs 4 AP, (a) *delay*, (b) *jitter*.



(a) (b)

Figura 3.17: Experimento 4, Balance de carga, (a) Tamaño de colas, (b) Retransmisión de paquetes.

Ninguno de los dos escenarios está funcionando en condiciones de alta densidad de tráfico o de usuarios, en cuyo caso el escenario 2 estaría en ventaja por tener mayor capacidad, el hecho de usar 3 o 4 AP no debe influir notablemente en estos resultados, por lo que se atribuye la mejora en los KPI al uso del balance de carga.

3.2.5 Quinto experimento, ajuste de parámetros EDCA

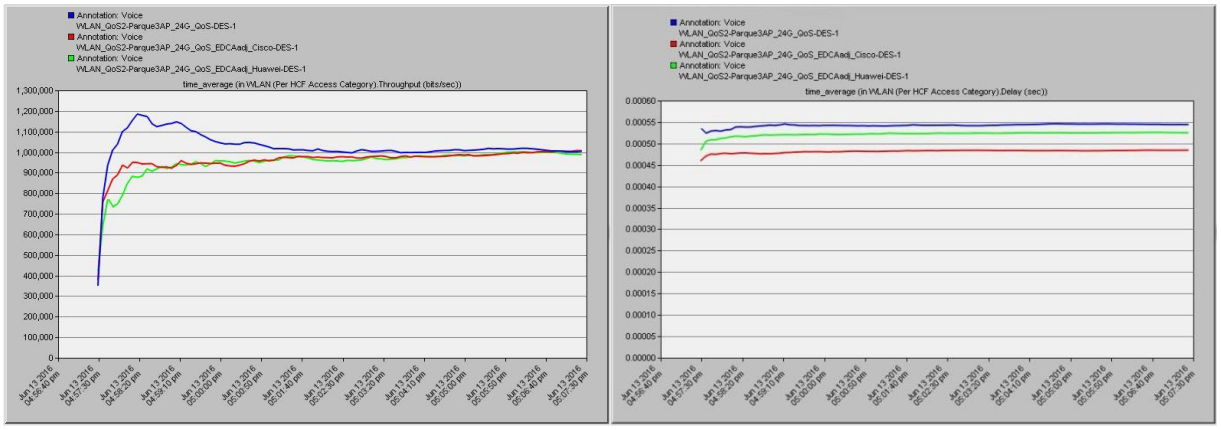
Descripción:

Cuando se activa la funcionalidad HCF, los parámetros de trabajo (*AIFS, CWmin, CWmax y TXOPLimit*), que condicionan el funcionamiento del método de acceso al medio EDCA (*Enhanced Distributed Channel Access*), traen una configuración por defecto.

En este experimento se ajustarán estos parámetros, según lo recomendado por los proveedores Huawei (tabla 2.4) y Cisco (tabla 1.1), y se evaluará el comportamiento de los KPI determinantes en la voz, comparando ambos. Para ello, se trabajará una vez más sobre el escenario 1, simulando por separado el desempeño de la red para los parámetros EDCA por defecto, los recomendados por Cisco, y por último lo que recomienda Huawei.

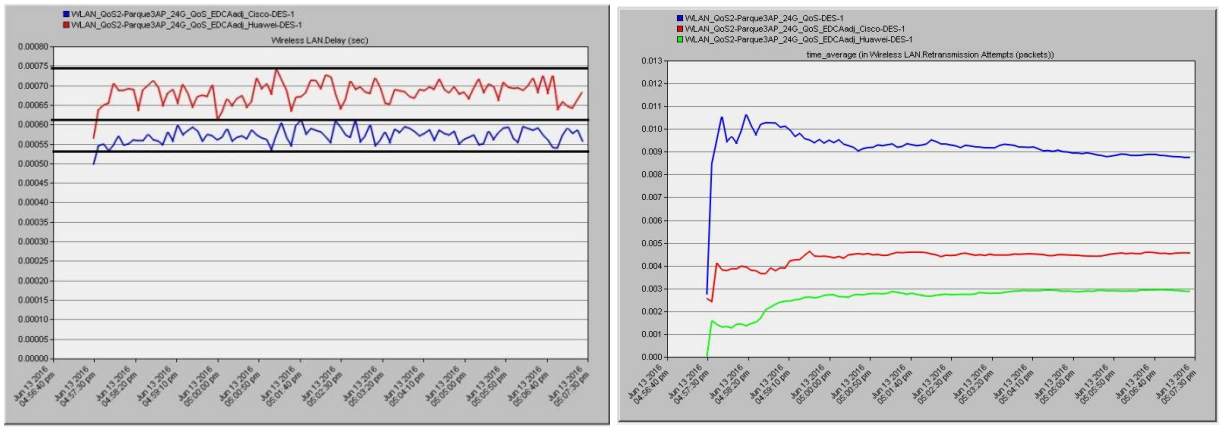
Análisis de los resultados:

De antemano se conoce que la carga de la red en los tres casos es la misma, es por ello que en la figura 3.18-a se muestra solo el comportamiento del tráfico de voz, la gráfica azul corresponde al resultado para los parámetros EDCA por defecto, la roja representa los ajustes recomendados por Cisco, y la verde los que recomienda Huawei. Aunque en los tres casos el *throughput* es el mismo, se observa un comportamiento más estable en el tiempo cuando los parámetros están ajustados a valores recomendados. La figura 3.18-b muestra el retardo para el tráfico de voz, observándose una ligera mejoría después de realizar los ajustes, que es un poco más notable en el caso de Cisco. Este resultado se evidencia un poco mejor en la figura 3.19-a, nótese que no solo el retardo es menor para Cisco (azul), sino que además presenta una variabilidad (*jitter*) ligeramente menor que Huawei (rojo).



(a) (b)

Figura 3.18: Experimento 5, ajuste EDCA, (a) *Throughput* de voz, (b) Retardo de la voz.



(a) (b)

Figura 3.19: Experimento 5, ajuste EDCA, Cisco vs Huawei, (a) *Jitter*, (b) Retransmisión de paquetes.

En la figura 3.19-b se muestra el comportamiento de la retransmisión de paquetes, en este caso el impacto de los ajustes es un poco mayor, y al contrario de la demora y el *jitter*, presenta su valor más bajo para los parámetros EDCA recomendados por Huawei.

Este experimento no pretende demostrar la superioridad de una u otra recomendación, más aún cuando este resultado tendría que ser evaluado más a fondo, usando varios escenarios de prueba con características diferentes que posibiliten comparar desempeño de uno u otro ante situaciones diversas. El objetivo del experimento persigue demostrar que es necesario ajustar los parámetros EDCA, con el fin de optimizar el desempeño de las WLAN que soportan calidad de servicio para aplicaciones en tiempo real.

3.3 Propuesta de escenario VoWLAN con interoperabilidad

En los dos capítulos anteriores fue discutida la arquitectura de red usada para soportar el despliegue de zonas de acceso WiFi en Cuba. Para culminar este trabajo, se hará una propuesta que aprovecha las potencialidades del equipamiento que ya está en explotación, en aras de implementar un servicio de VoIP sobre la red WiFi de ETECSA, que sea capaz en una primera etapa de converger con la red celular móvil de segunda generación que actualmente da cobertura a los más de 3.3 millones de usuarios móviles de ETECSA; y en una segunda etapa pueda evolucionar hacia la interoperabilidad entre ambas redes inalámbricas, una vez que quede en explotación la red celular móvil de tercera generación.

Según el *Gartner Magic Quadrant* para infraestructura de acceso LAN y *Wireless* LAN del 2015 [52], los proveedores líderes del sector son: *Cisco*, *Hewlett Packard Enterprise* (*Aruba Networks*), y *Huawei*, aunque también se mencionan otros vendedores referenciados en este trabajo como *Juniper Networks* y *Ruckus Wireless*. Para hacer esta propuesta se analizaron las arquitecturas de Cisco [53], Aruba Networks [54], y Huawei [55].

Básicamente el cambió fundamental que sería necesario implementar, en la arquitectura actual de la red para zonas de acceso WiFi de ETECSA, para brindar un servicio VoWiFi, es el mecanismo de autenticación. En la figura 3.20 se muestra el escenario actual.

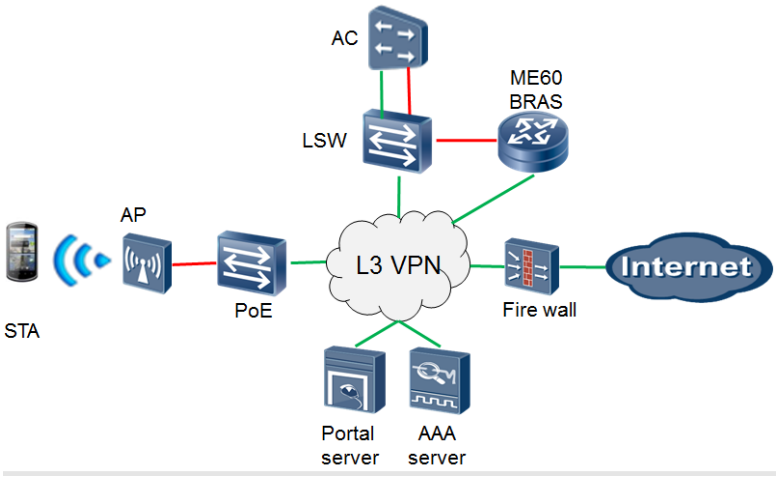


Figura 3.20: Escenario actual, autenticación por Portal Cautivo y AAA. Fuente elaboración propia.

En escenario propuesto, la autenticación de los usuarios se realizaría a través del protocolo EAP-SIM (descrito en el epígrafe 1.2.1), esto no varía mucho del escenario que actualmente usan las zonas WiFi, de hecho, mantiene funcionando en paralelo el mecanismo actual, solo que en lugar de autenticarse con la cuenta “nauta” en un servidor RADIUS, los usuarios de este servicio, lo harían con su mismo IMSI *(International Mobile Subscriber Identifier*), contenido en la SIM, en el HLR correspondiente, gracias a que el servidor AAA para el actual servicio de navegación, soporta la funcionalidad AAA 3gpp; este esquema de autenticación se muestra en la figura 3.21.

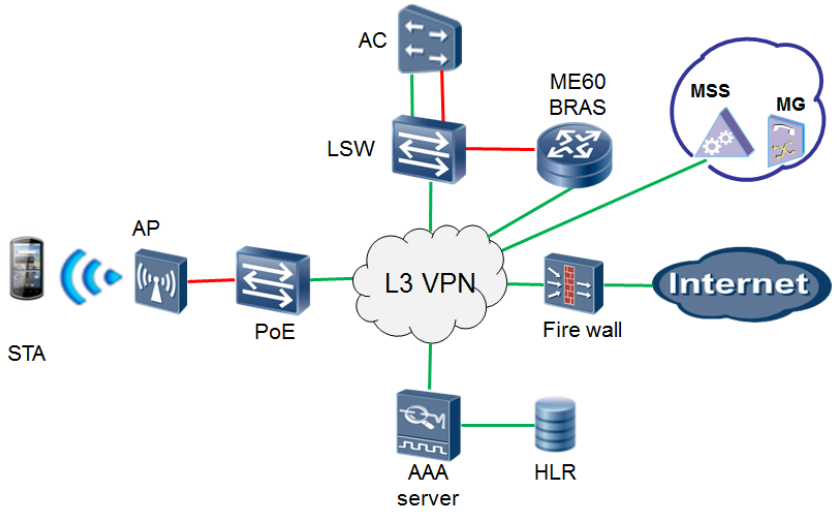


Figura 3.21: Propuesta de autenticación EAP-SIM. Fuente elaboración propia.

En esta propuesta, la función de “*Call Gateway*” la realizarían los *SoftSwitch* del *core* de la red móvil, aprovechando que estos ya cuentan con esta funcionalidad, y porque además de esta manera no es necesario implementar un nuevo número para el cliente, sino que se usa el mismo número móvil, almacenado en los HLR. Si se usa el códec G.711 no será necesario hacer modificaciones en el *core*, aunque podría considerarse el uso de otros códecs más eficientes como el G.729a, siempre que se adquieran las licencias correspondientes y se hagan los *upgrade* de software necesarios.

La movilidad no es un problema, pues está contemplada en las actuales zonas de acceso WiFi. Los AP Huawei utilizados trabajan con el estándar IEEE802.11n y en ambas bandas (2.4 GHz y 5.8 GHz), que como se ha descrito en este trabajo, garantiza movilidad, seguridad, y calidad de servicio suficiente para soportar tráfico de VoIP. Se deberá crear un nuevo SSID en la red de acceso, específicamente para soportar este servicio, el autor aconseja el uso de *Dynamic Admission Control* (DAC) en este perfil de red, para proteger la calidad del tráfico de voz.

En cuanto a los terminales (*smartphones* en su mayoría, aunque muchos *tablets* soportan tarjeta SIM), en caso de no tener implementada la funcionalidad “*WiFi Calling*”, pueden usar aplicaciones para *softphone* como el *Sipdroid* o el *ZoiPer*, este último disponible para *Android*, iOS (*iPhone*), y *Windows Phone 8*.

La “segunda etapa” de esta propuesta, contempla la interoperabilidad con la red 3G, una vez que esta entre en explotación, esto no solo permitiría el *roaming* de voz entre ambas redes, sino además permitiría hacer *roaming* de datos; para lograr esto habría que implementar la autenticación EAP-AKA, la arquitectura de la red se muestra en la figura 3.22, aunque en la imagen no se detallan todos los elementos del *core* móvil.

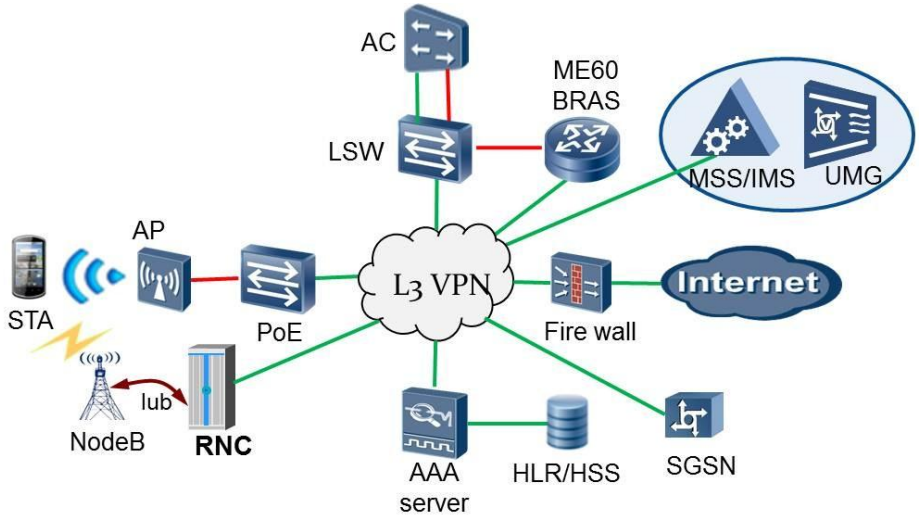


Figura 3.22: Propuesta de interoperabilidad y autenticación EAP-AKA. Fuente elaboración propia.

Con estas propuestas se persigue lograr mayor satisfacción del cliente, al permitirle con un único usuario, acceder a varios servicios, y poder pagarlos con una cuenta única (en el epígrafe 2.3 se comentan otras ventajas); en la medida que aumente la informatización de la sociedad cubana, es importante contar con métodos de autenticación seguros y confiables, pero que además resulten sencillos para el cliente [56].

3.4 Consideraciones finales del capítulo 3

En este capítulo se evaluó el comportamiento de redes WLAN en cuanto a los indicadores de desempeño que pueden afectar al tráfico de voz, se realizó un análisis de las mejoras introducidas por estándar IEEE 802.11e para ofrecer Calidad del Servicio (QoS) en redes WLAN; para ello, se modelaron tres escenarios, usando la herramienta *Opnet Modeler* 14.5, que permitieron mediante la simulación, demostrar la eficacia de las prestaciones que ofrece el mecanismo de acceso al medio EDCA y evaluar su impacto en el desempeño de redes VoWLAN para alta densidad de usuarios.

Finalmente, se hace una propuesta para mejorar el mecanismo de autenticación de los usuarios de la red WiFi de ETECSA, que posibilite implementar servicios VoIP con interoperabilidad a la red móvil, garantizando la calidad del servicio.

CONCLUSIONES

En este trabajo se describieron los estándares que garantizan calidad de servicio para soportar Voz sobre IP en redes WiFi, se hizo particular énfasis en los mecanismos de control de acceso al medio introducidos por el estándar IEEE802.11e, encargados de proveer QoS a nivel MAC en las redes WiFi. También se refieren otros estándares encargados de dar seguridad, movilidad, e interoperabilidad a los usuarios, temas fundamentales a la hora de dar soporte a la voz en redes inalámbricas, y que están estrechamente ligados a la calidad de servicio en redes WiFi. Todo esto posibilita la implementación de aplicaciones VoWLAN y su futura interoperabilidad con redes públicas, aprovechando las ventajas que brindan los *smartphones* y *tablets* y las bondades del equipamiento instalado por ETECSA como parte del despliegue de zonas de acceso WiFi.

Se evaluaron por medio de la simulación y mediciones en zonas de acceso WiFi el desempeño de estas en cuanto a la calidad de servicio, y se describen métodos de diseño que garanticen calidad de servicio en el desarrollo de redes WLAN, tanto en interiores como en exteriores, estableciendo criterios concretos para el dimensionamiento de celdas, que no deben superar los – 67 dBm, y para el solapamiento de estas, que no debe ser mayor del 20%, ni menor del 15%; si se desea implementar redes WiFi para alta densidad de usuarios, con un balance de carga adecuado, y la posibilidad de que sus usuarios realicen *hand-off* entre los *Access points*.

Además, se demostró, por medio de la simulación, la eficacia de las mejoras introducidas por el estándar IEEE802.11e, lográndose demoras en la red de acceso inalámbrica por debajo de los 10 ms para el tráfico de voz, con una varianza en la demora por debajo de 1 ms, tasa de paquetes erróneos prácticamente nula, y retransmisiones de paquetes del orden del 5%, lo que garantiza calidad de servicio para aplicaciones en tiempo real como la voz, en redes WLAN de alta densidad de usuarios. También se evaluó la importancia de ajustar los parámetros que trae por defecto este estándar, demostrándose que es aconsejable elevar la ventana de contención mínima (*CWmin*) de 3 ms para tráfico de voz, 7 ms para tráfico de video y 15 ms para tráfico *best effort* y *background*, a 7 ms, 15 ms, y 31 ms, respectivamente, y en correspondencia con esto, elevar la ventana de contención máxima (*CWmax*) a 15 ms y 31 ms para la voz y el video, y para el caso de tráfico *best effort* y *background* al valor máximo, según el período de *backoff.*

Por último, se propuso una topología que permite a los usuarios de la red GSM autenticarse de forma segura, sin necesidad de usar usuario y contraseña, usando para ello el *Core* de la Red Móvil, lo que les permitiría hacer llamadas VoIP a través de este, usando como acceso las zonas WiFi y manteniendo su número móvil. Poner en práctica el método de autenticación propuesto, sentaría las bases para una futura interoperabilidad entre ambas redes, tanto para servicios de voz, como para datos.

RECOMENDACIONES

Que ETECSA realice un estudio de mercado determinando factibilidad económica de un servicio de voz sobre IP para la red de acceso WiFi, usuarios potenciales (actualmente existen 1 400 000 cuentas nauta permanentes, de ellas 1 300 000 acceden por el móvil), tarifas y forma de pago (por tiempo o por volumen).

Que se realicen pruebas de campo VoIP en zonas de acceso WiFi, con el fin de garantizar que se cumple con los estándares de QoS para un servicio brindado por un operador. Para lograr esto, se deberá usar un SSID diferente y aplicar control de admisión, con el fin de que los terminales que solo funcionan con estándar IEEE802.11b, no puedan conectarse a este servicio, para no afectar al resto.

BIBLIOGRAFIA

[1] J. Ghetie, *Fixed-Mobile Wireless Networks Convergence*: Cambridge University Press, 2008.

[2] W.-F. Alliance, "Wi-Fi CERTIFIED™ for WMM™ - Support for Multimedia Applications with Quality of Service in Wi-Fi® Networks ", ed: Wi-Fi Alliance, 2004, p. 15.

[3] IEEE Computer Society, "IEEE Std 802.11e," in *Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*, ed. IEEE-SA Standards Board: LAN/MAN Standards Committee, 2005, p. 211.

[4] IEEE Computer Society, "IEEE Std 802.11n," in *Amendment 5: Enhancements for Higher Throughput*, ed. IEEE-SA Standards Board: LAN/MAN Standards Committee, 2009, p. 536.

[5] F. Richard. (2012), Voice over WiFi – Deployment recommendations and best practices. 62.

[6] A. S. Tanenbaum and D. J. Wetherall, "Computer Networks - 5th edition," 5th ed: PRENTICE HALL, 2011, pp. 299-312.

[7] D. Gu and J. Zhang. (2003), QoS Enhancement in IEEE802.11 Wireless Local Area Networks. 9.

[8] H. Yoon, J. Kim, and D. Shin. (2006, Dynamic Admission Control in IEEE 802.11e EDCA-based Wireless Home Network. 5.

[9] J. Villalón_Millán, P. Cuenca_Castillo, and L. Orozco_Barbosa. (2005), Estudio de QoS en WLANs IEEE 802.11e. 8.

[10] L. Yang. (2006), P-HCCA: A New Scheme for Real-time Traffic with QoS in IEEE 802.11e Based Networks 7.

[11] J. M. Hernando_Rábanos, E. Álvarez_González, and S. Molins_Riera, "CALIDAD DE SERVICIO DE LA VOZ SOBRE IP EN REDES 802.11e " presented at the XXV Simposium Nacional. UNIÓN CIENTÍFICA INTERNACIONAL DE RADIO, Bilbao, 2010.

[12] L. L. Bello, E. Toscano, and S. Vittorio. (2010), A perspective on the IEEE 802.11e Protocol for the Factory Floor. 25.

[13] H. Chaouchi and M. Laurent-Maknavicius, *Wireless and Mobile Networks Security*: Wiley, 2009.

[14] Cisco, "VoWLAN Design Recommendations," in *Enterprise Mobility 4.1 Design Guide*, ed: Cisco Systems, Inc., 2013, p. 16.

[15] IETF, "RFC4186 - Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Mod-ules (EAP-SIM)," ed, 2006, p. 92.

[16] IETF, "RFC4187 - Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," ed, 2006, p. 79.

[17] O. S. Consultants. (2016), Radiator EAP-SIM, EAP-AKA and EAP-AKA' Support. 17.

[18] H. Kattema. (2014, 18-10-2015). *EAP-SIM and EAP-AKA*. Available: https://supportforums.cisco.com/document/12088681/eap-sim-and-eap-aka#

[19] K.-H. CHI, C.-C. TSENG, and Y.-H. TSAI, "Fast Handoff among IEEE 802.11r Mobility Domains," *JOURNAL OF INFORMATION SCIENCE AND ENGINEERING,* vol. 26, p. 18, 2010.

[20] K. Dridi, N. Javaid, K. Djouani, and B. Daachi. (2009, Performance Study of IEEE802.11e QoS in EDCF-Contention-based Static and Dynamic Scenarios 4.

[21] Cisco Systems. (2014). *802.11-r-k-w Deployment Guide, Cisco IOS-XE Release 3.3*.

[22] Cisco, "Voice Over Wireless LAN (VoWLAN) Troubleshooting Guide," ed: Cisco Systems, Inc., 2010, p. 102.

[23] M. H. Miraz, S. A. Molvi, M. Ali, M. A. Ganie, and A. H. Hussein, "Analysis of QoS of VoIP Traffic through WiFi-UMTS Networks " presented at the World Congress on Engineering, London, UK, 2014.

[24] Y. Liu, S. Li, J. Xie, and X. Xu. (2012, Security Analysis and Improvements of IEEE802.11u. 10.

[25] E. Samada_Granda, "Propuesta de facturación por volumen para nuevo servicio WiFi de áreas públicas," presented at the XVI CONVENTION OF ELECTRICAL ENGINEERING, CIE-2015, Facultad de Ingeniería Eléctrica. Univ. Central “Marta Abreu” de Las Villas, 2015.
[26] IETF, "RFC5415 - Control and Provisioning of Wireless Access Points (CAPWAP)," ed, 2009, p. 153.
[27] M. Sauter. (2015), Deep Inside the Network: Wifi Authentication with EAP-SIM.
[28] Huawei. (2014), HCNA-WLAN v1.6 Training Materials. 828.
[29] Huawei Technologies. (2014, HUAWEI WLAN Products Portfolio. 106.
[30] Cisco. (2007), Design Principles for Voice over WLAN. 16.
[31] Aruba Networks. (2011), Bringing QoS Over Wireless LAN into Focus. 14.
[32] J. Florwick, J. Whiteaker, A. C. Amrod, and J. Woodhams. (2013), Wireless LAN Design Guide for High Density Client Environments in Higher Education. 41.
[33] Tektronix. (2013), Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. 44.
[34] Aruba Networks. (2014), Aruba 802.11ac In-Depth. 37.
[35] Motorola. (2009), Preparing your WLAN infrastructure for voice. 16.
[36] Spectralink. (2014), The challenges of ensuring excellent voice. 4.
[37] Huawei Technologies. (2016, 18-05-2016). Technical Analysis on Huawei VoWiFi Solution. Available: http://carrier.huawei.com/en/technical-topics/core-network/
[38] Huawei. (2014). *WA201DK-NE Product Description*. Available: http://www.huawei.com
[39] Huawei. (2014). *WA251DK-NE Product Description*. Available: http://www.huawei.com
[40] Huawei. (2015). *MAG9811 Product Description(V100R006C00_02)*. Available: http://www.huawei.com
[41] Huawei. (2014), HCS Field WLAN V1.0 Training Materials. 1009.
[42] M. Jordy, "Real-time Traffic Applications and Service over WLAN," *BRKCOL,* vol. 2275, p. 85, 2015.
[43] Y. Xiangwei. (2012, 2-06-2016). *WLAN Basic Network Planning (V1.0 ed.)*. Available: www.huawei.com
[44] Aruba Networks. (2015, Aruba 802.11ac Networks Validated Reference Design. 43.
[45] Juniper Networks. (2013, 23-04-2016). Understanding Voice Clients and Voice Traffic. Available: http://www.juniper.net/documentation/
[46] O3b Networks. (2015), What is Network Latencyband Why Does It Matter. 13. Available: www.o3bnetworks.com/wp-content/
[47] Ruckus Wirelless. (2014), Clear Voice Over Wi-Fi in the Enterprise. 6.
[48] K. Gierłowski, A. Kostuch, J. Woźniak, and K. Nowicki. (2010, 23-04-2016). Testbed analysis of video and VoIP transmission performance in IEEE 802.11 b/g/n networks. Available: https://www.researchgate.net/publication/
[49] N. I. Sarkar, "Performance Modeling of IEEE 802.11 WLAN using OPNET: A Tutorial," in *Handbook of Research on Discrete Event Simulation Environments: Technologies and Applications: Technologies and Applications*, I. Global, Ed., ed. www.igi-global.com/chapter/performance-modeling-ieee-802-wlan/38271: AUT University, New Zealand, 2010, p. 20.
[50] A. Mukhopadhyay, T. Chakraborty, S. Bhunia, I. S. Misra, and S. K. Sanyal. (2011, Study of Enhanced VoIP Performance under Congested Wireless Network Scenarios. 7.
[51] R. Krishan and D. V. Laxmi, "IEEE 802.11 WLAN Load Balancing for Network Performance Enhancement," presented at the 3rd International Conference on Recent Trends in Computing 2015, University, Talwandi Sabo, INDIA, 2015.

[52] T. Zimmerman, B. Menezes, and A. Lerner. (2015), Magic Quadrant for the Wired and Wireless LAN Access Infrastructure. 26.
[53] S. Ghosh, "Design and Deployment of Enterprise WLANs," p. 114, 2010.
[54] T. Cappalli. (2015), Aruba WLANS 101 and Desing Fundamentals. 69.
[55] Huawei Technologies Cloud Core Network Documentation Department. (2016), Cloud Core Network Technical Series V1.0. 68.
[56] Huawei, "Building a Better Connected World," p. 38, 2014-11-12 2014.

ANEXOS

WA201DK-NE Indoor AP, Product Description.

WA201DK-NE is an indoor AP working in 3x3 MIMO mode. It is a fit AP supporting the 2.4 GHz and 5 GHz frequency bands and complying with IEEE 802.11a/b/g/n standards. WA201DK-NE can be powered by a PoE-supporting switch or PoE power converted from alternating current (AC) power.

With powerful functions and high transmission rates, WA201DK-NE provides operators, Internet service providers (ISPs), and enterprises with ideal solutions. In addition, WA201DK-NE is characterized by:

- High reliability and security
- Easy deployment
- Automatic AC discovery and configuration
- Real-time management and maintenance

It can be installed in areas that have a simple architecture with a high user density and large traffic requirements, such as hotels, airports, schools, and small- and medium-sized enterprises.

WA201DK-NE on a wireless local area network (WLAN) has the following advantages:

- **High security**
  - The WA201DK-NE supports a variety of authentication and encryption modes:
  - WEP authentication and encryption are applied.
  - WPA/WPA2 authentication and encryption are applied.
  - The Wireless Intrusion Detection System (WIDS), rogue AP identification, wireless flood attack detection and defense, and wireless spoofing attack detection prevent user access to rogue APs and service interruption when the device is attacked, thereby improving user experience.
  - User isolation prevents STAs associated with the same AP from forwarding Layer 2 packets between each other, thereby blocking direct communication between STAs.
  - Anti-DoS attack enables the system to blacklist users who initiate DoS attacks and protect networks from attacks to ensure stable and secure services for users.
- **Easy device management and maintenance**

The WA201DK-NE is a fit AP managed by an AC. After being powered on, the AP automatically discovers the AC and loads configurations from it. Authentication, AP management, security protocol configuration, and routing are performed by the AC, and the AP status is monitored in real time by the OSS. This simplifies AP management and maintenance. In addition, the WA201DK-NE provides automatic channel and frequency adjustment and in-service fast roaming.

Hardware Specifications

The following illustrates the appearance of the WA201DK-NE and describes the ports and buttons of the WA201DK-NE.

Equipment lock port: Lock slot for connecting to the chain of the lock. Anti-theft locks are not delivered, and they must be prepared by customers if required.

ETH/PoE: Adaptive to 10/100/1000 Mbit/s connections and supports PoE/PoE+.

Reset button To reset the AP, press and hold down the button for less than 3 seconds. To restore the factory settings, press and hold down the button for longer than 10 seconds.

Functions and Features

- **WLAN features**
  - Compliance with IEEE 802.11a/b/g/n
  - Channel rate adjustment
    - IEEE 802.11a-compliant rates: 54, 48, 36, 24, 18, 12, 9, or 6 Mbit/s
    - IEEE 802.11b-compliant rates: 11, 5.5, 2, or 1 Mbit/s
    - IEEE 802.11g-compliant rates: 54, 48, 36, 24, 18, 12, 9, or 6 Mbit/s
    - IEEE 802.11b- and IEEE 802.11g-compliant rates: 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, or 1 Mbit/s
    - Adjustable IEEE 802.11n-compliant rates:
      20 MHz (HT20): mcs0-23
      40 MHz (HT40): mcs0-23
  - Automatic channel scanning
  - The WA201DK-NE automatically scans channels and selects the optimum channel.
  - Power-saving mode for STAs
  - Service set identifier (SSID) hiding
  - Control and Provisioning of Wireless Access Points (CAPWAP)

- Automatic AC discovery
- Spectrum analysis and interference detection
- Low rate user suppression
- Intelligent frequency band navigation
- Intelligent load balancing
- Compliance with mesh networks

- **Network features**
  - Virtual local area network (VLAN) assignment based on SSIDs
  - STA isolation in the same VLAN on a virtual access point (VAP)
  - Support for 4093 VLAN IDs (1–4093) and 32 VLANs (16 on either RF band)
  - Support for the DHCP client to obtain IP addresses through DHCP
  - Support Hotspot 2.0
- **QoS features**
  - Priority mapping according to the WLAN multimedia (WMM) profile, implementing priority-based data processing and forwarding
  - WMM parameter management for each radio frequency
  - WMM power saving
  - Priority mapping for upstream and downstream packets
  - Queue mapping and scheduling
  - Rate limiting for STAs on the VAP
- **Security features**
  - Open system authentication
  - WEP authentication and encryption
  - WPA/WPA2 authentication and encryption
  - Link integrity check (The AP stops sending radio signals when the tunnel between the AP and AC is terminated.)
  - Wireless Intrusion Detection System (WIDS)
  - User isolation
  - DoS Attack Prevention
- **Ethernet features**
  - Compliance with IEEE 802.3z
  - Auto-negotiation of rates and duplex mode
  - Automatic switchover between the Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X)
- **Maintenance features**
  - AP management and maintenance on an AC
  - AP management and maintenance using the command line interface (CLI)
  - AP maintenance using Secure Shell (SSH)

- Upgrade using the CLI on the AC
- Factory setting recovery using software
- Alarm monitoring using the OSS

Technical Specifications

- **Power specifications**
  - Power less than 15 W
  - Input of the PoE switch or PoE power supply: 42 V DC to 57 V DC
  - Compliance with AC/OSS power supply through the CAPWAP tunnel
  - Support for the 802.3at and 802.3af PoE power standards (The 802.3af PoE power standard lowers the transmit power.)
- **Operating environment specifications**
  - Operating temperature: –10°C to +50°C
  - Storage temperature: –40°C to +70°C
  - Operating relative humidity: 5% RH to 95% RH (non-condensing)
  - Storage relative humidity: 10% RH to 100% RH (non-condensing)
  - Protection rating: IP41
- **Physical specifications**
  - Dimensions (H x W x D): 40 mm x 200 mm x 200 mm
  - Weight: 0.6 kg (without installation accessories)
  - Installation mode: on a wall, on a ceiling, or on a keel
  - Mean time between failures (MTBF): 100,000 hours
- **WLAN specifications**
  - Antenna type: integrated dual-band 3x3 antenna array (supports MIMO)
  - Antenna gain: 2G:3dBi

    5G: 3dBi
  - Adjustment step: 1 dB
  - Transmit power: 2.4 G: 3 Antenna Port*20dBm/(3*100mW)

    - High band@5.725GHz-5.825GHz：3AntennaPorts*20dBm/(3*100mW)

    - Middle band@5.470GHz-5.7250GHz：3Antenna Ports*19dbm/(3*80mW)

    - Low band@5.150GHz-5.350GHz：3Antenna Ports*18dBm/(3*60mW)

Issue: 03

Date: 2014-05-28

WA251DK-NE Outdoor AP, Product Description.

The WA251DK-NE is an outdoor high-performance AP complying with IEEE 802.11a/b/g/n standards. Using integrated smart antennas, the AP supports 3x3 MIMO-OFDM and two frequency bands: 2.4 GHz and 5 GHz. The AP also supports PoE+ switches and DC/PoE+ adapters. The WA251DK-NE is designed to help operators, Internet service providers (ISPs), and enterprises build a high performance network giving them a competitive edge.

The WA251DK-NE on a wireless local area network (WLAN) has the following advantages:

- **High security**

The WA251DK-NE supports a variety of authentication and encryption modes:

- WEP authentication and encryption
- WPA/WPA2 authentication and encryption

- **Superb environment adaptability**

The WA251DK-NE meets IP66 requirements and ensures normal transmission of radio signals in an outdoor environment.

- **Easy device management and maintenance**

The WA251DK-NE is a fit AP managed by an AC. After being powered on, the AP automatically discovers the AC and loads necessary configurations from it. Authentication, AP management, security protocol configuration, and routing are performed by the AC, while the AP status is monitored in real time by the NMS. This simplifies AP management and maintenance. In addition, the WA251DK-NE automatically manages channel and frequency adjustment and supports in-service fast roaming.

Hardware Specifications

The following illustrates the body of the WA251DK-NE and describes its ports

ETH/PoE: A 10/100/1000 Mbit/s adaptive Ethernet port supporting PoE+

Functions and Features

- **WLAN features**
  - Complies with IEEE 802.11a/b/g/n standards
  - Channel rate adjustment
    - IEEE 802.11a-compliant rates: 54, 48, 36, 24, 18, 12, 9, or 6 Mbit/s
    - IEEE 802.11b-compliant rates: 11, 5.5, 2, or 1 Mbit/s
    - IEEE 802.11g-compliant rates: 54, 48, 36, 24, 18, 12, 9, or 6 Mbit/s
    - IEEE 802.11b- and IEEE 802.11g-compliant rates: 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, or 1 Mbit/s
    - Adjustable IEEE 802.11n-compliant rates
      20 MHz (HT20): mcs0-23
      40 MHz (HT40): mcs0-23
  - Automatic channel scanning

    The WA251DK-NE automatically scans and selects the optimum channel.
  - Power-saving mode for STAs
  - Service set identifier (SSID) hiding
  - Control and Provisioning of Wireless Access Points (CAPWAP)
  - Automatic AC discovery
  - Spectrum Analysis and Interference Detection
  - Low Rate User Suppression
  - Intelligent Frequency Band Navigation
  - Intelligent Load Balancing
- **Network features**
  - Virtual local area network (VLAN) assignment based on SSIDs
  - STA isolation within a VLAN on a virtual access point (VAP)
  - Tunnel forwarding and direct forwarding
  - Support for 4093 VLAN IDs (1–4093) and 32 VLANs (16 on either RF band)
  - Support for IP addresses assignment through DHCP
  - Support for Hotspot2.0
- **QoS features**
  - Priority mapping according to WLAN multimedia (WMM) profile, implementing priority-based data processing and forwarding
  - WMM parameter management for each radio frequency
  - WMM power saving
  - Priority mapping for upstream and downstream packets
  - Queue mapping and scheduling
  - Rate limiting for STAs on a VAP
- **Security features**

- Open system authentication
- WEP authentication and encryption
- WPA/WPA2 authentication and encryption
- Link integrity checks (The AP stops sending radio signals when the tunnel between the AP and AC is terminated.)
- Wireless Intrusion Detection System (WIDS)
- User Isolation
- DoS Attack Prevention

- **Ethernet features**
  - Compliance with IEEE 802.3u
  - Auto-negotiation of rates and duplex mode
  - Automatic switchover between the Media Dependent Interface (MDI) and Media Dependent Interface Crossover (MDI-X)
- **Maintenance features**
  - AP management and maintenance on an AC
  - AP management and maintenance through the command line interface (CLI) AP maintenance through Secure Shell (SSH)
  - Upgrades through the CLI on the AC
  - Factory default recovery through software
  - Alarm monitoring using the NMS

Technical Specifications

- **Power specifications**
  - Maximum power consumption: 24 W
  - Input of the PoE switch or PoE power supply: 42 V DC to 57 V DC
  - Compliance with AC/NMS power supply through the CAPWAP tunnel
  - Compliance with the 802.3at PoE power standard
- **Operating environment specifications**
  - Operating temperature: –40°C to +55°C
  - Storage temperature: –40°C to +70°C
  - Operating relative humidity: 5% to 100% (non-condensing)
  - Storage relative humidity：10% to 100% (non-condensing)
  - Protection rating: IP66
- **Physical specifications**
  - Dimensions (H x W x D): 320 mm x 320 mm x 81 mm
  - Weight: 3 kg (without installation brackets)
  - Installation mode: on a pole or wall
  - Mean time between failures (MTBF): 100,000 hours

- **WLAN specifications**
  - Antenna type: integrated high-gain antenna array (supports MIMO)
  - Antenna Horizontal Beamwidth: 2.4 GHz: 60° ±10° (horizontal polarization)

    80° ±10° (vertical polarization)

    5 GHz: 65° ±20°
  - Antenna Vertical Beamwidth: 2.4 GHz: 28° ±3°

    5 GHz: 15° ±3°
  - Antenna gain: 12 dBi (2.4 GHz) or 14.5 dBi (5 GHz)
  - Transmit power adjustment step: 1 dB
  - Transmit power: 2.4 G: 3 Antenna Port*24dBm/(3*250mW)

    5G： - High band@5.725GHz-5.825GHz：3AntennaPorts*24dBm/(3*250mW)

    - Middle band@5.470GHz-5.7250GHz：3Antenna Ports*23dbm/(3*200mW)

    - Low band@5.150GHz-5.350GHz：3Antenna Ports*22dBm/(3*160mW)

Issue: 03

Date: 2014-04-02