PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR



FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

TEMA:

"IMPLEMENTACIÓN DE CALIDAD DE SERVICIO EN REDES INALÁMBRICAS DE ÁREA LOCAL, PARA LA OPTIMIZACIÓN DEL SERVICIO DE TELEFONÍA IP EN SMART PHONES CON CLIENTE SIP"

Chauca Chicaiza Jose Luis

Quito, Febrero 2016

AUTORÍA

Yo, Jose Luis Chauca Chicaiza, portador de la cédula de ciudadanía No.0603602269, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

Jose Luis Chauca Chicaiza

Dedicado a mis dos amores, Lo y Paquito.

Gracias a Dios por permitirme disfrutar de mi trabajo diario en el apasionante mundo de las Telecomunicaciones, a los profesores que me han guiado en el desarrollo de este trabajo, a mis familiares por su apoyo incondicional.

ÍNDICE DE CONTENIDO.

ÍNDICE DE CONTENIDO. v
ÍNDICE DE GRÁFICOS. ix
ÍNDICE DE TABLAS. xi
1. Introducción. 1
2. Justificación. 2
3. Antecedentes. 3
3.1. Planteamiento del problema. 3
3.2. Alcance del proyecto. 4
4. Objetivos. 5
5. Desarrollo del Caso de Estudio. 6
5.1. Ambientes comunes de redes de datos empresariales. 6
5.2. Descripción del trabajo a desarrollar 7
6. Redes Inalámbricas 9
6.1. Fundamentos de redes inalámbricas de área local 9
6.1.1. Elementos de una red inalámbrica. 9
6.1.2. Modos de funcionamiento de los Puntos de Acceso. 10
6.1.3. Principios básicos de RF (radiofrecuencia) 12
6.1.4. Bandas y canales 802.11 15
6.2. Estándares de redes inalámbricas IEEE 802.11 17
6.2.1. 802.11b 17
6.2.2. 802.11g 17
6.2.3. 802.11a 18
6.2.4. 802.11n 18
6.2.5. 802.11ac 19
6.3. Tipos de redes inalámbricas 20
6.4. Modo de operación de las redes inalámbricas de área local. 21
6.4.1. Modo Ad-hoc. 21
6.4.2. Modo Infraestructura. 22
6.5. Capa física de la redes IEEE 802.11. 23
6.5.1. FHSS (Frequency Hop Spread Spectrum) – Espectro Ensanchado por Salto de Frecuencia. 24
6.5.2. DSSS (Direct Sequence Spread Spectrum) - Espectro ensanchado por Secuencia Directa. 24

6.5.3. CCK (Complementary Code Keying) – Codificación de Código Complementario. 25
6.5.4. OFDM (Orthogonal Frequency Division Multiplexing). 26
6.6. Capa de enlace de datos IEEE 802.11 28
6.6.1 Tramas 802.11 30
6.7 Disponibilidad de QoS en redes WLAN 32
6.8. Necesidades de QoS en servicios de telefonía IP sobre WLAN 33
7. Telefonía IP 37
7.1. Fundamentos de telefonía IP 37
7.1.1. Digitalización de la voz, teorema de Nyquist y codificación. 38
7.2. Elementos de una red de telefonía IP 39
7.3. Protocolos y señalización de telefonía IP 40
7.3.1. Protocolo RTP 42
7.3.2. Protocolo RTCP 43
7.3.3. Protocolo UDP 43
7.3.4. Protocolo IP 44
7.3.5. Protocolo SIP 44
7.3.6. Señalización SIP. 45
7.4. Códecs de telefonía IP 54
7.5 Telefonía IP en redes best-effort 56
7.6 Telefonía IP en redes inalámbricas 57
7.7 Requerimientos de Calidad de Servicio 58
7.7.1 Jitter 58
7.7.2 Latencia 59
7.7.3 Pérdida de paquetes 60
7.8 Retos de una red de VoIP para garantizar la QoS 61
8. Calidad de Servicio en Redes Inalámbricas. 62
8.1. Requerimientos de servicio para aplicaciones de video, voz y datos 62
8.1.1. QoS en tecnologías WIMAX 63
8.1.2. QoS en redes WIFI 64
8.2. Fundamentos de calidad de servicio. 65
8.2.1. Objetivos de la aplicación de QoS. 65
8.2.2 Arquitectura de la Calidad de Servicio 67
8.3. Identificación y marcado QoS (Clasificación) 68
8.3.1. Aplicación de políticas QoS con PBR (policy-based Routing). 68

8.3.2. CAR: Establecimiento del campo “IP Precdendence”. 68
8.3.3. Prioridad IP (IP Precedence): QoS Diferenciado..... 69
8.4. QoS dentro de un elemento de red único. 70
8.4.1. Administración de congestión. 70
8.4.2. Administración de colas 74
8.5. Eficiencia de enlace. 76
8.5.1. Fragmentación e intercalado de paquetes LFI (Link Fragmentation Interleaving) 76
8.5.2. Compresión de encabezado RTP 77
8.6. Herramientas de conformación de tráfico (Traffic Shaping & Policing) 77
8.6.1. Tasa de acceso acordada, CAR (Committed Access Rate) 78
8.6.2. GTS (Generic Traffic Shaping) 78
8.7. Modelos de QoS extremo a extremo. 78
8.8. Parámetros de QoS 80
8.9. Tecnologías para la aplicación de calidad de servicio en redes inalámbricas 81
8.9.1. Modelos de calidad de servicio en redes inalámbricas 81
8.9.2. Calidad de servicio para redes inalámbricas con el protocolo IEEE 802.11e 81
8.9.3. Distribution Coordination Function (DCF) 83
8.9.4 Point Coordination Function (PCF) 83
8.9.5. Enhanced Distributed Channel Access (EDCA) 84
8.9.6. HCF Controlled Channel Access (HCCA) 88
9. Implementación de Prototipo..... 90
9.1. Definición del problema 90
9.2. Enfoque del ciclo de vida de los procesos. 91
9.3. Definición del modelo de red a implementar. 93
9.4. Elementos del sistema..... 94
9.4.1. Central telefónica IP. 95
9.4.2. Access Point con soporte 802.11e..... 96
9.5. Consideraciones de diseño. 97
9.6. Impacto de QoS en una red inalámbrica 97
9.7. El softphone. 98
9.7.1 Bria Android Edition..... 99
9.7.2. Zoiper IAX & SIP 100
9.7.3. CSIP Simple..... 100

9.8. Análisis de pruebas y resultados. 101
9.8.1. Configuración de la red 101
9.8.2. Tamaño de muestra y tráfico en la red. 104
9.8.3. Resultados obtenidos. 109
9.8.4. Intervalos de confianza de las pruebas realizadas. 117
9.9. Costo Total de Propiedad 119
10. CONCLUSIONES Y RECOMENDACIONES. 121
10.1. Conclusiones 121
10.2. Recomendaciones 122
11. BIBLIOGRAFÍA 124
12. ACRÓNIMOS. 128
13. ANEXOS 133
13.1. Configuración de QoS en AP. 133
13.2 Captura de paquetes en entornos inalámbricos. 135
13.3. Archivo de configuración del AP utilizado en el proyecto. 138

ÍNDICE DE GRÁFICOS.

Figura 1. Diagrama AP en modo repetidor (Jerome, 2013) 10
Figura 2. Diagrama AP en modo WGB universal (Jerome, 2013)..... 11
Figura 3. Diagrama AP en modo puente (Jerome, 2013). 11
Figura 4. Diagrama AP en modo malla (Jerome, 2013). 12
Figura 5. Parámetros de una señal RF (longitud de onda y amplitud de señal), (Jerome, 2013). 12
Figura 6. Zona de Fresnel (Ramos, 2015). 14
Figura 7. Fenómenos RF (Carroll, 2008). 15
Figura 8. Canales para la frecuencia de 2.4GHz (Donovan, 2013)..... 16
Figura 9. Canales para la frecuencia 5GHz (UNII-1 y UNII-2), (Bakin, 2007). 16
Figura 10. Diagrama de una red Ad-Hoc o IBSS (Jerome, 2013). 22
Figura 11. Conceptos de una red inalámbrica en modo Infraestructura (Jerome, 2013). 23
Figura 12. DSSS, codificación “Barker 11” (Info Tech plus, n.d.). 24
Figura 13. Representación del símbolo CCK (Bakin, 2007). 25
Figura 14. Representación de técnica de modulación BPSK (Jerome, 2013). 26
Figura 15. Representación de técnica de modulación QPSK (Jerome, 2013). 27
Figura 16. Representación de técnica de modulación 16 QAM (Jerome, 2013). 27
Figura 17. Acceso al medio 802.11 (Rajesh, 2006). 30
Figura 18. Trama 802.11 (Yang R. , 2012). 31
Figura 19. Diagrama de una red telefónica tradicional, (Landivar, 2008). 38
Figura 20. Datagrama de voz sobre IP (Nóvoa, 2012). 42
Figura 21. Estructura de un datagrama RTP (Nóvoa, 2012). 42
Figura 22. Estructura de un datagrama UDP (Nóvoa, 2012). 43
Figura 23. Ejemplo de resolución de direcciones. (Kuthan & Sisalem, 2007) 50
Figura 24. Establecimiento de sesión. (Kuthan & Sisalem, 2007)..... 51
Figura 25. Modificación de la sesión. (Kuthan & Sisalem, 2007). 52
Figura 26. Terminación de la sesión. (Kuthan & Sisalem, 2007) 52
Figura 27. Cancelación de sesión. (Kuthan & Sisalem, 2007). 53
Figura 28. Control de llamada. (Kuthan & Sisalem, 2007)..... 53
Figura 29. Contenido del paquete INVITE y OK (Elastixtech, 2013). 54
Figura 30. Arquitectura básica de QoS. (Cisco Systems, 2012). 68
Figura 31. Esquema de campo ToS en datagrama IPv4 (Cisco Systems, 2012). 69
Figura 32. Esquema de funcionamiento “Priority Queuing” (Cisco Systems, 2012)..... 71
Figura 33. Esquema de funcionamiento “Custom Queuing” (Cisco Systems, 2012)..... 72
Figura 34. Esquema de funcionamiento WFQ (Cisco Systems, 2012). 73
Figura 35. Esquema de funcionamiento CBWFQ (Cisco Systems, 2012). 74
Figura 36. Esquema de funcionamiento LLQ. (Pham, 2012). 74
Figura 37. Diagrama de funcionamiento WRED (Cisco Systems, 2012)..... 75

Figura 38. Esquema de funcionamiento LFI (Cisco Systems, 2012) 76
Figura 39. Ejemplo de compresión de encabezado sobre red Ethernet (Cisco Systems, 2012). 77
Figura 40. Niveles de QoS extremo a extremo (Cisco Systems, 2012). 79
Figura 41. Capa de enlace de datos 802.11 (Carroll, 2008). 82
Figura 42. Diagrama de tiempo de las Categorías de Acceso (AC) (Cisco Systems, 2010). 86
Figura 43. Esquema de funcionamiento AC en EDCA (Cisco Systems, 2010). 86
Figura 44. Proceso de funcionamiento EDCA (Cisco Systems, 2010). 87
Figura 45. Esquema de funcionamiento HCCA (Simsek & Wolter, 2006). 88
Figura 46. Ejemplo de super-trama 802.11e (Simsek & Wolter, 2006). 89
Figura 47. Metodología del ciclo de vida de los servicios (Cisco Systems, 2010). 92
Figura 48. Topología de red a implementar. (Autor: José Chauca). 94
Figura 49. Sentido de flujo de tráfico de red. (Nayanajith, My CCIE Wireless Journey, 2013) 98
Figura 50. Capturas de pantalla del Softhphone BRIA ANDROID EDITION (COUNTERPATH, 2016). 99
Figura 51. Capturas de pantalla de softphone ZOIPER para Android (ZOIPER, 2015). 100
Figura 52. Capturas de pantalla de softphone CSIP SIMPLE para Android (CSipSimple, 2015) 101
Figura 53. Registro de llamadas de la central telefónica IP. (Autor: José Chauca). 105
Figura 54. Reporte de clientes conectados al AP sin QoS. (Autor: José Chauca) 107
Figura 55. Reporte de clientes conectados a la red de datos y a la red de telefonía, AP con QoS. (Autor: José Chauca). 107
Figura 56. Tráfico inalámbrico, red sin QoS. (Autor: José Chauca). 108
Figura 57. Resultado de Wifi Analizer, SSID Autelcom2 trabajando en canal 1. (Autor: José Chauca). 109
Figura 58. Trama 802.11 sin QoS. (Autor: José Chauca) 110
Figura 59. Paquete marcado en campo DSCP con valor EF. (Autor: José Chauca). 110
Figura 60. Estadísticas durante una llamada sin QoS, softphone BRIA. 111
Figura 61. Trama 802.11 con QoS para voz. (Autor: José Chauca) 114
Figura 62. Estadísticas con softphone BRIA (pruebas con QoS), (Autor: José Chauca) 115
Figura 63. Estadísticas en softphone ZOIPER, (Autor: José Chauca) 117
Figura 64. Seleccionar la opción “Capture Settings”. 135
Figura 65. Seleccionar el adaptador inalámbrico. (Captura realizada por José Chauca) 136
Figura 66. Propiedades del adaptador de red. (Captura realizada por José Chauca) 136
Figura 67. Selección del canal de operación de la red inalámbrica. (Captura realizada por José Chauca) 137
Figura 68. Datos capturados. (Captura realizada por José Chauca) 137

ÍNDICE DE TABLAS.

Tabla 1. Clasificación del tipo de empresas según la cantidad de empleados. 6
Tabla 2. Resumen de las técnicas de modulación utilizadas en 802.11. 28
Tabla 3. Parámetros básicos para el cálculo del backoff timer. 29
Tabla 4. Ventajas y desventajas de la telefonía IP. 37
Tabla 5. Campos del protocolo SDP. (RFC 2327). 49
Tabla 6. Ancho de banda de los principales códec de voz y su calidad. 55
Tabla 7. Ancho de banda requerido por códec. 57
Tabla 8. Valores de retardo en una comunicación. (ITU-T G.114) 59
Tabla 9. Retardos de codificación para códecs de voz. 59
Tabla 10. Retardo de paquetización para Códecs de voz. 60
Tabla 11. Requerimientos de calidad de servicio de las aplicaciones 67
Tabla 12. Valores IP Precendence del campo ToS. 70
Tabla 13. Clasificación de categorías de acceso con relación a clasificación 802.1D, ... 85
Tabla 14. Ventana de contención EDCA, para QSTA AIFS = DIFS, para QAP < DIFS. 85
Tabla 15. Distribución de usuarios y equipos. 91
Tabla 16. Detalle de elementos del sistema. 95
Tabla 17. Sub direccionamiento IP 101
Tabla 18. Direccionamiento IP de equipos de telecomunicaciones. 102
Tabla 19. Parámetros QoS para Asterisk 103
Tabla 20. Parámetros QoS Access Point. 103
Tabla 21. Intervalos de confianza. 104
Tabla 22. Datos para cálculo de tamaño de muestra, red sin QoS. 105
Tabla 23. Datos para el cálculo del tamaño de muestra, red con QoS. 106
Tabla 24. Datos obtenidos con el software BRIA en la red sin QoS. 112
Tabla 25. Comparación valores obtenidos con QoS vs límite. 115
Tabla 26. Precio de equipos involucrados en la solución. 119
Tabla 27. Valores por defecto Categorías de Acceso QoS inalámbrico. 134

1. Introducción

En la actualidad las redes de comunicaciones tienden a converger en una misma infraestructura permitiendo disponer de diversos servicios como transmisión de datos, exploración de la web, acceso a bases de datos, comunicaciones unificadas, transmisión de video entre otros. Pudiendo los clientes acceder a ellos por la red cableada o a través de puntos de acceso inalámbrico (Carroll, 2008). Este último sea por su facilidad de implementación y bajo costo a la hora de ponerlo en marcha, así como al auge de nuevos dispositivos con capacidades de acceso inalámbrico han permitido el desarrollo vertiginoso de la tecnología inalámbrica permitiendo velocidades de transferencia en el rango de los Gbps (Cisco Systems, 2013) con los nuevos estándares.

Una de las aplicaciones que es imprescindible en las PyMes es la telefonía, en la mayoría de empresas es uno de los pilares fundamentales sobre los cuales se levanta el negocio, el desarrollo tecnológico ha permitido que la telefonía evolucione a tal punto de ser parte de una red convergente, donde los datos, el video y la voz coexisten en una misma infraestructura; la voz dentro de una conversación telefónica, al ser transportada dentro de la misma red, presenta mayor o menor degradación en la calidad de la comunicación en función del número de usuarios que acceden a los recursos de la red, esto hace necesaria la implementación de algún mecanismo que garantice una buena calidad de las llamadas sin dejar de lado la “calidad de servicio” de los otros recursos de la red.

Hoy en día la mayor parte de los empleados de un negocio grande o pequeño cuentan con un Smart-phone, que permite disponer de la mayoría de aplicaciones corporativas, siendo una de ellas la telefonía IP que da la posibilidad al dispositivo de contar con una extensión telefónica de la red corporativa sin la necesidad de disponer un equipo final exclusivo para este propósito, situación que ha permitido mejorar la productividad por cuanto el trabajador puede recibir llamadas de su extensión fija en su teléfono móvil sin hacer uso de la red telefónica pública dentro de su empresa en un entorno inalámbrico haciéndose necesario garantizar una comunicación eficiente (Ubeda & Wikipedia, 2014).

La aplicación práctica de este proyecto consistirá en implementar una red tipo de una empresa comercial donde se dispone de la infraestructura básica de acceso a la red y el servicio de telefonía IP en marcha, donde se aplicarán las políticas de calidad de servicio basadas en el estándar 802.11e (IEEE, 2005) para la parte inalámbrica a fin de optimizar el acceso de los usuarios y garantizar una comunicación eficiente.

2. Justificación.

Con el presente trabajo se pretende incorporar mecanismos de calidad de servicio especialmente en microempresas que están avanzando a la convergencia de sus servicios, y los recursos de TI se puedan alinear a los objetivos del negocio de la mano de los avances tecnológicos.

La tendencia BYOD ha generado mayor demanda de recursos en las redes, debido a que cada vez se incrementa el número de usuarios que disponen de un equipo móvil, más los equipos inalámbricos tradicionales que en conjunto generan gran cantidad de tráfico, donde cada uno de ellos compite por acceder al medio sin importar el tipo de contenido que están transmitiendo.

El disponer de la extensión telefónica corporativa en el dispositivo móvil de cada empleado permite aprovechar también la red inalámbrica, pero no todo es color de rosa, como se comentó, en la actualidad, diversos equipos acceden de esta manera y resulta difícil garantizar que la comunicación será eficiente. En tal virtud una solución a este grave inconveniente es la aplicación de mecanismos de calidad de servicio provistos en el estándar IEEE 802.11e (Cruz & Martinez, 2013).

Y con la aplicación de algún mecanismo de calidad de servicio lo que se busca es mantener el retardo, el jitter y las pérdidas de paquetes para los tipos de tráfico de tiempo real (en especial telefonía IP) dentro de límites aceptables, teniendo en cuenta sus conceptos:

- Retardo (Latencia): cantidad de tiempo que le toma a un paquete alcanzar al receptor luego de ser enviado por el transmisor. También se conoce como retardo de extremo a extremo (Robles, 2008)

- Jitter: diferencia en el retardo de extremo a extremo entre varios paquetes (Robles, 2008).

- Pérdida de paquetes: medida comparativa de los paquetes transmitidos y recibidos exitosamente con respecto al total de paquetes transmitidos (Robles, 2008).

3. Antecedentes.

Las pequeñas y medianas empresas, en especial las dedicadas al sector comercial, han innovado sus redes de datos a tal punto que mantienen redes convergentes de datos y telefonía sobre la misma infraestructura, la telefonía por ser un servicio que se debe brindar en tiempo real es sensible a los retardos (máximo 150ms) (Méndez & Gaviria, 2006), en una red cableada se pueden minimizar aplicando políticas de calidad de servicio adecuadas. Ahora el problema radica cuando el acceso se realiza por redes inalámbricas debido al método de acceso al medio que emplean los dispositivos.

El crecimiento exponencial de los dispositivos móviles inteligentes con capacidades de acceso a la red corporativa de manera inalámbrica ha dado lugar a la tendencia tecnológica "Lleve su propio dispositivo" (BYOD: Bring Your Own Device) (Cisco Systems, 2014) donde el usuario puede hacer uso del dispositivo con el que se sienta cómodo para realizar su trabajo, pudiendo acceder a todos los recursos de la red en base a las políticas de seguridad de la empresa. Uno de estos recursos a los que tiene acceso un equipo móvil es a la telefonía IP, que como ya se menciona anteriormente es muy sensible a los retardos, y dada la naturaleza de las redes inalámbricas el método de acceso a diferencia de una red cableada no cuenta con mecanismos de QoS y no existe forma de garantizar los recursos ni retardos para la información de los usuarios, (Jerome, 2013).

La principal desventaja de no disponer de mecanismos de calidad de servicio en redes inalámbricas, cuando la red cuenta con clientes (SIP) de telefonía IP (Landivar, 2008) sobre dispositivos móviles inteligentes, o bien sobre equipos adecuados para telefonía IP es la degradación de la calidad de la conversación, llegando a ser completamente improductiva debido a que el tráfico de los datos no es exclusivo para la VoIP sino también para diferentes aplicativos como bases de datos, video bajo demanda, navegación web y otros.

El tráfico de voz sobre una red sin calidad de servicio es tratado de la misma manera que cualquier otro tipo de tráfico de datos de usuario, situación que está fuera de la realidad para conseguir una conversación telefónica aceptable Por esta razón es muy importante definir prioridades de acuerdo al tipo de información sobre la red, lo que nos conlleva a implementar mecanismos de aplicación de calidad de servicio en redes WLAN basados en estándares como el IEEE 802.11e (IEEE, 2005) con el objetivo principal de que el usuario se sienta satisfecho del servicio que recibe.

3.1. Planteamiento del problema.

Por la naturaleza de las redes inalámbricas (CSMA/CA (Jerome, 2013): detección de portadora y acceso múltiple / evitar colisiones) el acceso de las estaciones a la red se da en una contienda entre dispositivos donde no importa el tipo de estación ni el tipo de tráfico que se transmita, representando un problema para aplicaciones que requieren transmisión en tiempo real como la telefonía (voz sobre IP) (Carroll, 2008)

Los requerimientos que se deben cumplir cuando se trabaja con voz sobre IP indistinto del medio de acceso que se utilice son:

- Retardo máximo en un sentido no mayor de 150 ms (de acuerdo con la recomendación ITU-T G.114) (Méndez & Gaviria, 2006).

- Pérdida de paquetes mínima, en vista de que la VoIP no es tolerante a las pérdidas de paquetes, aun con un 1% de paquetes perdidos se puede degradar enormemente una comunicación de voz así se esté utilizando el códec G.711, en caso de utilizar códecs con mayor tasa de compresión la pérdida es prácticamente intolerable (Méndez & Gaviria, 2006).

- El jitter promedio no debe ser mayor que 30 ms (Méndez & Gaviria, 2006).

Considerando que en la mayoría de empresas del tipo PyMe no dispone de un departamento de tecnología y por consiguiente la adopción de equipos para el acceso inalámbrico no se hace en base a un criterio técnico surge el siguiente problema:

Calidad de servicio deficiente en redes inalámbricas locales para aplicaciones de voz sobre IP (telefonía)

3.2. Alcance del proyecto.

Con el presente proyecto se implementará la calidad de servicio (QoS) en una red inalámbrica de área local (WLAN) perteneciente a la empresa AUTELCOM de la ciudad de Cuenca a fin de que se pueda disponer de una extensión telefónica (clientes SIP) en los teléfonos móviles de los empleados que dispongan de Smart-phones con aplicaciones para telefonía IP.

La red prototipo a implementar dispondrá de un servidor de telefonía IP basado en software libre (Elastix), dos puntos de acceso autónomos marca Cisco, switch de acceso, equipos terminales como PCs o teléfonos IP, smarth-phones con software Android y clientes SIP instalados.

4. Objetivos.

Objetivo general:

- Implementar calidad de servicio (QoS) en redes inalámbricas de área local para optimizar el servicio de telefonía IP (protocolo SIP) en Smart-phones dentro de una PyMe

Objetivos específicos:

1. Describir el estándar IEEE 802.11e, como uno de los principales mecanismos para la aplicación de calidad de servicio en redes inalámbricas de área local (WLAN).

2. Describir las políticas de calidad de servicio aplicables a las redes inalámbricas

3. Implementación de una red de prototipo para una PyMe donde se utilizará telefonía IP en dispositivos móviles

4. Realizar las pruebas de la aplicación de calidad de servicio en redes WLAN para optimizar el servicio de telefonía IP con clientes SIP instalados en Smart-phones con acceso local.

5. Realización de un artículo referente a la implementación de Calidad de Servicio en redes inalámbricas de área local para optimizar el servicio de telefonía IP

5. Desarrollo del Caso de Estudio.

5.1. Ambientes comunes de redes de datos empresariales.

Al referirnos a una red de datos empresarial, hablamos de la red de comunicaciones que sirve de infraestructura a una empresa que provee bienes o servicios; de acuerdo a la cantidad de empleados estará dentro de la clasificación de pequeña y mediana empresa PyMe inclusive las microempresas (o SOHO, acrónimo de Small Office Home Office) cuyo número de empleados es menor a 200 o una empresa grande con mayor cantidad de trabajadores. En la tabla 1, encontraremos la clasificación de las empresas en Ecuador[1] en función del número de empleados, que será de utilidad para determinar a qué sector enfocar la solución.

Tabla 1. Clasificación del tipo de empresas según la cantidad de empleados.

Tipo	Cantidad de empleados
Microempresas	Hasta 9
Pequeña empresa	Hasta 49
Mediana empresa	De 50 a 199
Grande empresa	Mayor a 200

Fuente: Directorio de empresas INEC al 2014

El enfoque a las redes de las pequeñas y medianas empresas se efectúa, desde el punto de vista comercial, motivados por ser un potencial nicho de mercado para la implementación de tecnologías de información y comunicación TICs que sean útiles para la consecución de los objetivos de mercado de cada una de ellas, dado que en el país tenemos que un 90.4% de las empresas están dentro del rango de Micro Pequeñas y Medianas Empresas. Pero no todas las empresas van a requerir el uso de TICs, ya sea por la actividad que realice y/o el número de trabajadores con que cuente, de esta manera los potenciales nichos de mercado se enfocarían a actividades económicas de comercio, servicio profesionales, científicos y técnicos, y de información y comunicación que representa el 43.3% de las empresas existentes de acuerdo a la última estadística obtenida del Directorio de Empresas 2014 (INEC, 2015)

[1] Las empresas en el Ecuador se clasifican en base a dos parámetros, el primero el volumen de ventas anual y el segundo el número de empleados de acuerdo a información del Directorio de Empresas del INEC, (INEC, 2015).

El ambiente de la red de comunicaciones en una empresa PyMe es básico, aquí encontramos una red de cableado estructurado con switches de acceso para permitir conectividad y el enrutador del proveedor de servicios que lo conecta a la Internet, al mismo tiempo en la mayoría de casos se dispone de cableado adicional para el servicio de telefonía, manteniéndose aún la telefonía analógica. Es común hoy en día también encontrar sistemas de video vigilancia que están funcionando de manera aislada.

5.2. Descripción del trabajo a desarrollar

El auge en el desarrollo y comercialización de los teléfonos inteligentes los ha hecho cada vez más asequibles al público en general, estos nuevos dispositivos muy atrás dejaron sus funcionalidades básicas que permitían solo realizar llamadas de voz y/o menajes de texto a través de la red celular y hoy por hoy con una mayor cantidad de funcionalidades permiten ejecutar un sin número de aplicaciones de entretenimiento y productividad. En el ámbito de productividad ha permitido el surgimiento del concepto de llevar su propio dispositivo (al trabajo) BYOD (Bring Your Own Device) (Cisco Systems, 2014), que entre otras cosas ha elevado los requerimientos de seguridad de la red para evitar todo tipo de incidentes que afecte a la confidencialidad, integridad y disponibilidad de la información.

El interés y la demanda de las aplicaciones multimedia en redes inalámbricas han crecido rápidamente, estimulado por los nuevos dispositivos y en especial por el deseo de los usuarios inalámbricos de extender la funcionalidad de la red cableada.

En redes empresariales, el soporte de servicios como telefonía IP (VoIP), streaming de audio y video en tiempo real, hace necesario que el administrador de la red esté en la capacidad de gestionar el tráfico en la red inalámbrica para que pueda ofrecer estos servicios dentro de niveles aceptables.

Con lo expuesto anteriormente tenemos suficientes razones para querer mejorar las condiciones de la telefonía IP en una empresa del grupo de pequeñas y medianas. Para alcanzar este objetivo haremos un repaso teórico por los distintos temas involucrados en el proyecto como son:

- Conocimiento básico del funcionamiento de las redes inalámbricas
- Conocimiento básico del funcionamiento del protocolo SIP para telefonía IP.
- Funcionamiento de los mecanismos de calidad de servicio (QoS)

Una vez que se haya definido la teoría de los componentes del proyecto, se procederá con la implementación de una solución real que permitirá proveer QoS a teléfonos inteligentes de usuarios para poder aprovechar el servicio de telefonía IP corporativo en el entorno inalámbrico, que por lo general se provee mediante la red cableada.

Para la ejecución se hará uso de la infraestructura del cableado existente en la red, pero mejorando los dispositivos instalados, de ser necesario; poniendo mayor énfasis en el Access Point, de tal manera que los nuevos equipos permitan el desarrollo de las funcionalidades definidas en la certificación WMM[2] del WIFI Alliance.

[2] WMM (Wi-Fi Multimedia) es la certificación que provee la Wi-Fi Alliance a los equipos inalámbricos que tiene la capacidad de soportar aplicaciones multimedia con QoS. WMM se basa en el mecanismo de acceso EDCA (Enhanced Distributed Channel Acces) definido en la enmienda 802.11e para proveer QoS a la comunicación. 802.11e incluye también características adicionales que se pueden agregar a WMM como módulos adicionales, entre estas funcionalidades están el acceso programado, establecimiento de enlace directo (DLS), bloqueo de acuse de recibo (ACK) y ahorro de energía (Jerome, 2013).

6. Redes Inalámbricas

6.1. Fundamentos de redes inalámbricas de área local

Las redes de área local son un conjunto de dispositivos electrónicos que se comunican entre sí y/o a través de un servidor con el propósito de compartir algún tipo de información, en entornos empresariales estos equipos se conectan a un dispositivo central conocido como *switch* (conmutador) y el medio físico que se utiliza para la comunicación es el cobre (cable de par trenzado) comúnmente conocido como UTP (Unshielded Twisted Pair). Cuando no se utiliza el par trenzado como medio de transmisión, como alternativa se puede utilizar un haz de luz o alguna porción del espectro de RF (radiofrecuencia), en los dos casos estamos hablando de una comunicación inalámbrica. Por las diversas ventajas que presenta, en las redes de área local se ha desarrollado el uso del espectro RF como medio inalámbrico regido por el conjunto de estándares y enmiendas a partir del primer estándar IEEE 802.11. El uso del espectro ha sido establecido a nivel internacional a través de acuerdos que han permitido utilizar porciones de espectro sin licenciamiento para propósitos Industriales, Científicos y Médicos (ISM, Industrial, Scientific, Medical), al mismo tiempo se crearon regulaciones locales para prohibir que más porciones de espectro sean utilizados de manera privada. En 1997 el IEEE con el estándar IEEE 802.11 describió de qué manera las señales deben ser enviadas sobre la banda ISM de 2.4Ghz como portadora de información digital (Carroll, 2008).

A partir del primer estándar las comunicaciones inalámbricas han evolucionado considerablemente, como se puede notar con el surgimiento de las diversas enmiendas, pero los conceptos fundamentales están aún presentes.

6.1.1. Elementos de una red inalámbrica.

De acuerdo a (Carroll, 2008), para establecer la conexión entre dispositivos en una red inalámbrica son necesarios dos elementos, el primero de ellos la estación cliente (considerado como “STA, station” por el estándar 802.11) y el equipo central que coordina la comunicación llamado también Punto de Acceso (base-station).

- Estación cliente, es cualquier dispositivo que tenga instalado un adaptador inalámbrico o conocido también como tarjeta de red inalámbrica, que le permite conectarse a la red inalámbrica bien sea en modo ad-hoc o en modo infraestructura.

- Punto de Acceso (AP), es el dispositivo central en una red inalámbrica, se encarga de concentrar las conexiones (a manera de hub ethernet pero con funciones avanzadas) de las estaciones, inalámbricamente; también tiene la función de puente que se encarga de la comunicación con la red cableada (DS, distribution system) realizando las conversiones de trama pertinentes.

6.1.2. Modos de funcionamiento de los Puntos de Acceso.

De acuerdo a las condiciones de espacio físico y ubicación presentes en la implementación de una red de datos (nos referimos a la red cableada), pueden surgir problemas que limitan su despliegue; para solucionar estos inconvenientes los AP pueden ser muy útiles con el firmware adecuado permitiéndole operar en los modos que a continuación se indican (Carroll, 2008):

Modo Repetidor, un AP es configurado para repetir la señal de otro AP, y es muy útil para cubrir inalámbricamente áreas donde el primero no cubre (como se puede apreciar en la figura 1). Los repetidores incrementan el rango de cobertura de una celda pero al mismo tiempo se reduce el "throughput" o rendimiento porque el repetidor debe repetir la señal del AP para cada cliente. En algunos casos un repetidor tiene dos radios, uno para la comunicación con los clientes y otro para el AP, estos repetidores se los conoce como "repetidor full-duplex"

Modo Puente de Grupo de Trabajo WGB (Workgroup Bridge), es un AP utilizado para conectar uno o varios dispositivos no-inalámbricos a la red inalámbrica. En la infraestructura inalámbrica un WGB es visto como un cliente normal y soporta un solo cliente no-inalámbrico, a este modo se conoce como "universal WGB", también puede ser visto como un cliente especial que soporta varios clientes no-inalámbricos, a este modo se llama WGB y es propietario de Cisco. En la figura 2, se presenta el diagrama del modo WGB universal.

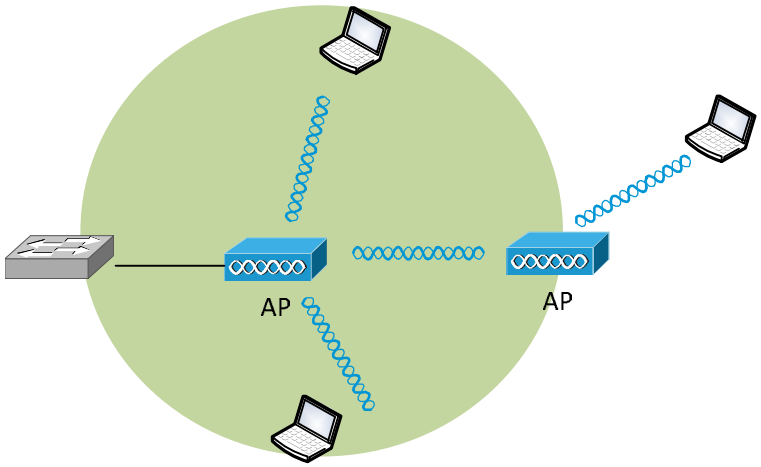


Figura 1. Diagrama AP en modo repetidor (Jerome, 2013)

Modo Bridge (puente), este modo es utilizado para conectar dos redes Ethernet, como por ejemplo las que están en dos edificios en un campus, en este modo un AP transmite el tráfico que ingresa por su puerto Ethernet hasta otro AP a través de un enlace de radiofrecuencia, y viceversa, un ejemplo de este modo de operación lo podemos apreciar en la figura 3.

Modo Mesh (malla) (Carroll, 2008)**,** en grandes implementaciones que cuentan con múltiples APs, por lo general algunos APs no se conectan directamente a la red cableada, en su lugar lo hacen a través de sus radios, y con la ayuda de protocolos específicos estos APs buscan la mejor ruta hacia la red cableada en respuesta a condiciones como la carga, condiciones de radio, o priorización de tráfico, actualizándose dinámicamente. En el ejemplo de la figura 4 que representa una red Mesh, tenemos que entre los APs se conectan inalámbricamente por una ruta principal, manteniendo como ruta de respaldo el enlace a otro dispositivo inalámbrico para el caso que la ruta principal falle se mantenga la conectividad.

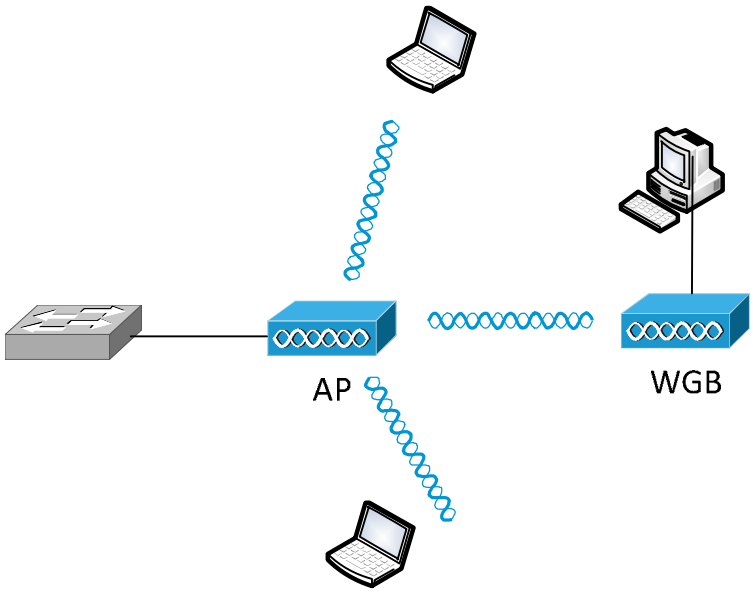


Figura 2. Diagrama AP en modo WGB universal (Jerome, 2013).

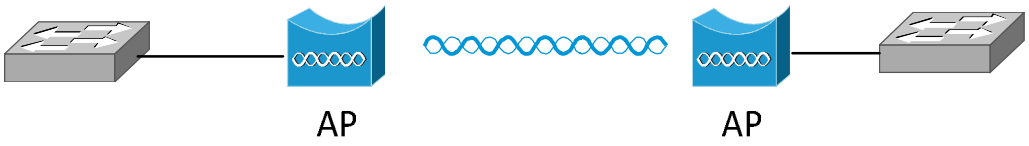


Figura 3. Diagrama AP en modo puente (Jerome, 2013).

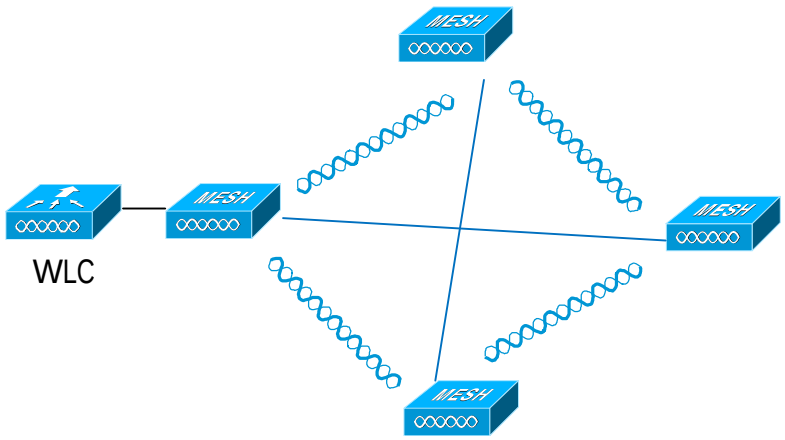


Figura 4. Diagrama AP en modo malla (Jerome, 2013).

6.1.3. Principios básicos de RF (radiofrecuencia)

Una onda de radio es un campo eléctrico y magnético utilizado para transportar información, las ondas tienen diferentes tamaños que se expresan en metros (Carroll, 2008), o también en Hertz que indica el número de veces que se repite un ciclo de onda en un segundo. Las redes inalámbricas operan sobre las bandas de 2.4 GHz y 5 GHz. Las ondas de radio dependiendo de la frecuencia (banda) de transmisión pueden ser afectadas por la interferencia, mientras más baja es la frecuencia es menos susceptible a interferencias y obstáculos y puede alcanzar rangos de cobertura más grandes.

En radiofrecuencia es importante tener presente los parámetros relacionados a una onda de radio; uno de los parámetros es la longitud de onda, que es la distancia desde un punto del ciclo al mismo punto en el siguiente ciclo, se representa por el símbolo griego lambda (λ), el siguiente parámetro es la amplitud de la señal, que es la distancia entre los picos más alto y más bajo de un ciclo. En la figura 5 se representan los parámetros antes indicados.

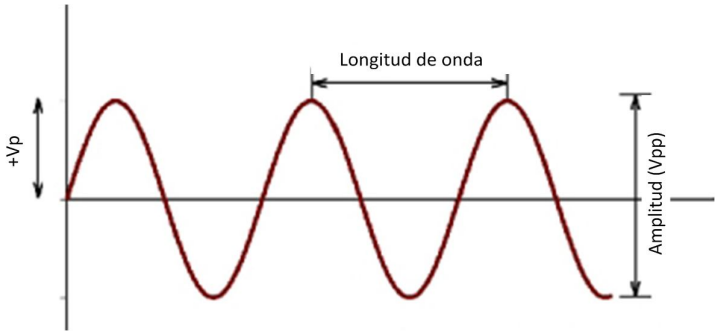


Figura 5. Parámetros de una señal RF (longitud de onda y amplitud de señal), (Jerome, 2013).

Cuando una onda viaja hasta su destino pueden ocurrir cambios en ella dependiendo de las condiciones del medio y obstáculos en su paso, como por ejemplo:

ATENUACIÓN

La atenuación se produce cuando una onda de radio choca con un obstáculo, parte de la energía es absorbida por el material y una pequeña cantidad de energía con menos amplitud y manteniendo la misma frecuencia continuará su camino al otro lado del obstáculo. La atenuación no solo puede ser provocada por obstáculos, sino también por el hecho de que la onda viaja desde su origen hasta el destino y en el trayecto va perdiendo energía. La atenuación relacionada a la distancia desde el emisor se la conoce como "free path loss"

El Free path loss se toma en cuenta para calcular la potencia necesaria del transmisor para que la señal llegue al receptor en buenas condiciones, a este cálculo se llama presupuesto de enlace (Link Budget). Un concepto que surge al hablar de enlaces o conexiones directas entre el emisor y receptor se conoce como línea de vista de RF (line-of-sigtht) que a diferencia de una "línea de vista visual", donde la presencia de un obstáculo no permite visualizar el receptor (desde el transmisor), la suficiente energía del transmisor hará posible que la onda atraviese el obstáculo.

Se asegura que existe línea de vista RF entre dos puntos, en base a los cálculos realizados en las zonas alrededor de la línea de vista, por el físico Augustin-Jean Fressnel, donde teóricamente define un infinito número de zonas, pero donde la zona que necesita de nuestra preocupación es la primera zona (Ramos, 2015); la figura 6 representa la forma de elipse de la primera zona de Fresnel, en esta zona, alguna obstrucción podría ser aceptable pero al menos el 60% de la zona[3] debería estar libre de cualquier obstáculo para permitir un señal de calidad aceptable, (Carroll, 2008). En enlaces de gran distancia (superiores a los 15kms) es importante considerar la curvatura de la tierra, lo que hará necesario elevar las antenas.

En una red inalámbrica es importante conocer el nivel de señal que se recibe en el receptor, este valor es indicado por el RSSI (Receiver Signal Strenght Indicator) que se expresa en dBm, es un valor negativo cuyo menor valor absoluto representa una mejor calidad de señal, por ejemplo -30dBm es mejor que -60 dBm. En un receptor debemos tomar en cuenta también que le están llegando señales innecesarias conocidas como ruido, que se expresa en dB y con valor negativo, el mayor valor absoluto representa un mejor ambiente (menos ruido) por ejemplo -100dB de ruido es mejor que -10dB. La relación entre la señal recibida y el ruido (SNR) es importante también que su valor es el más bajo posible.

REFRACCIÓN

Es un fenómeno poco común en redes inalámbricas interiores, y generalmente sucede cuando la señal pasa de un medio a otro (como del aire al agua) provocando que la onda cambie de dirección.

[3] El radio para la primera zona de fresnel R1, en un punto cualquiera del enlace puede calcularse a partir de la siguiente expresión: $R1 = \sqrt{\lambda \frac{d1*d2}{d1+d2}}$, para enlaces menores a 15km (Ramos, 2015).

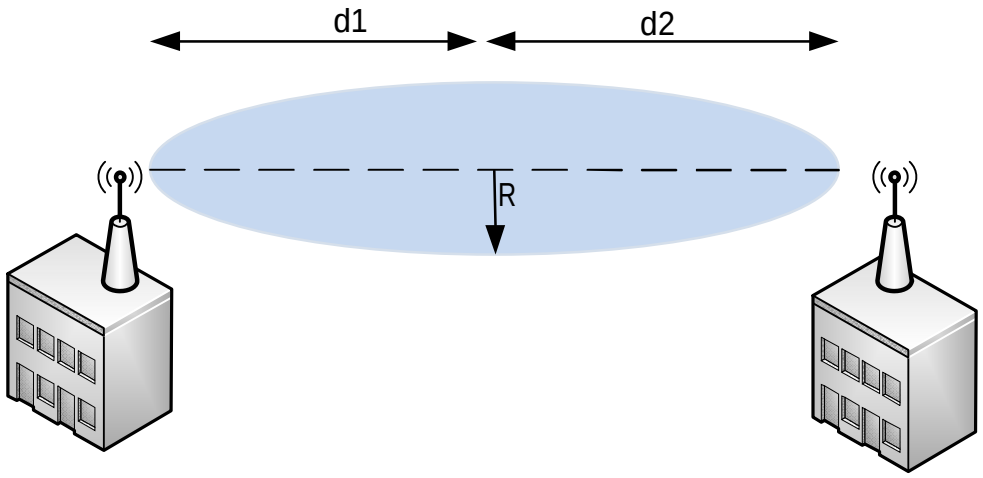


Figura 6. Zona de Fresnel (Ramos, 2015).

REFLEXIÓN

La reflexión se produce cuando la onda choca con el obstáculo a un pequeño ángulo de incidencia, esto provoca que toda la onda o parte de ella rebote. Dependiendo de la frecuencia de operación, un obstáculo puede ser o no ser fuente de reflexión de una onda, este fenómeno depende del material del obstáculo, la frecuencia de la señal y el ángulo de incidencia.

MULTIPATH

Mutipath (multi-camino), es un fenómeno producto de la reflexión que se da en la mayoría de casos en ambientes *"indoor"* donde la señal se refleja en paredes, techo, piso, entre otros, el fenómeno consiste en que la estación ha recibido la señal, y micro-segundos después recibe copias de la misma señal producto de la reflexión, (Jerome, 2013). El fenómeno de multipath es destructivo cuando las "señales copia" están fuera de fase, un caso inusual puede ser que las señales lleguen en fase, en este caso las amplitudes de cada onda se suma obteniéndose una señal de mayor potencia; un caso extremo es cuando las ondas se recibe desfasadas 180 grados, como resultado tenemos que las señales se cancelan, y no tenemos señal en el receptor; pero las ondas se pueden desfasar entre 0 y 180 grados y por la refracción vamos a tener en el receptor varias copias de la señal generando un grave problema.

Para mitigar el problema generado por multipath, la mayoría de equipos cuentan con dos antenas conectadas al mismo circuito de radio, a este concepto se lo conoce como diversidad, (Jerome, 2013). Un dispositivo con diversidad de antenas, cuando detecta una trama, evalúa la señal de cada antena y utiliza la que ofrece mejor señal y responde por la misma antena por la que recibió. La decisión de que antena utilizar para recibir y transmitir se realiza por cada trama, pero nunca se utilizan las dos antenas al mismo tiempo. Es importante considerar que las antenas deben encontrarse en la misma área y sobre todo deben ser del mismo tipo.

El concepto de diversidad no se debe confundir con el concepto de MIMO, que son totalmente diferentes, con diversidad se utilizan dos antenas pero conectadas al mismo circuito de radio mientras que con MIMO se utilizan las mismas dos antenas (para el caso de esta comparación, ya que pueden ser más) pero conectadas a radios diferentes cada una.

En la figura 7 podemos apreciar gráficamente los conceptos de los fenómenos RF que se han descrito recientemente.

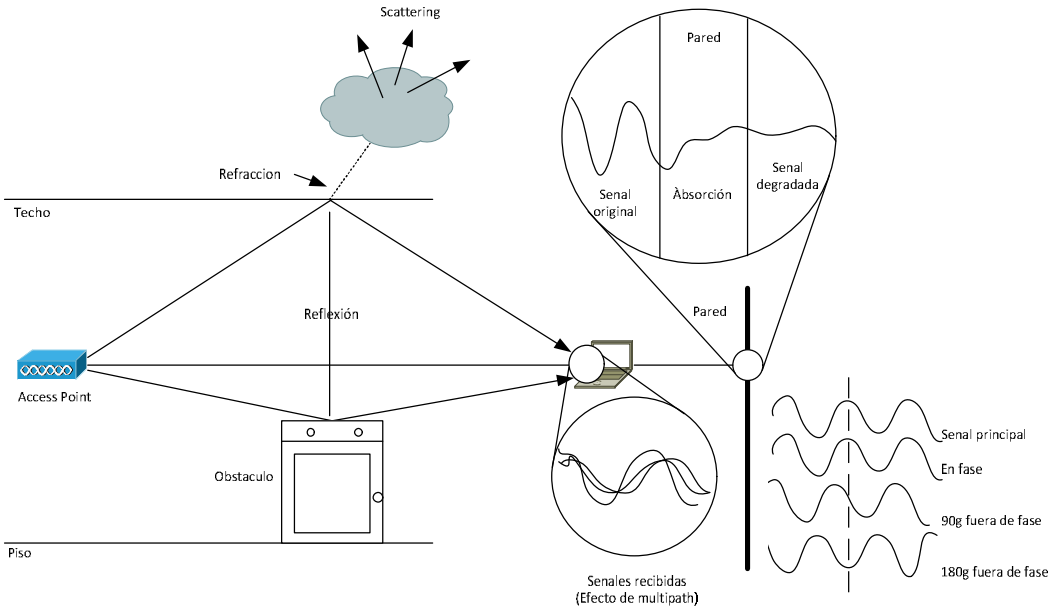


Figura 7. Fenómenos RF (Carroll, 2008).

6.1.4. Bandas y canales 802.11

Las redes WLAN pueden operar en dos bandas: 2.4 GHz y 5 GHz. La banda de 2.4 GHz comprende las frecuencias entre 2.400 GHz y 2.4835 GHz, y fue declarada por el ITU como banda no licenciada para equipos Industriales, Científicos y Médicos (ISM, Industrial, Scientific, Medical). Esta banda está dividida en canales con una separación de 5MHz entre ellos, pero en WLAN se requiere un ancho de canal de 20-22 Mhz (ver figura 8), esto hace que el uso de uno de los canales solapen a cuatro canales contiguos por ende será impráctico utilizarlos en la misma área (si utilizamos el canal 1, los canales 2,3,4,5 no se pueden utilizar), los canales 1 y 6 no se solapan y se consideran canales adyacentes, en la banda de 2.4 GHz existen solamente tres canales que no se solapan, el 1,6 y 11, que se pueden utilizar al mismo tiempo en un locación.

La banda de 5GHz está divida en cuatro sub-bandas, pero solo una de ellas es considerada como ISM (UNII-3) (Cisco Systems, n.d.), no existe un acuerdo en el mundo sobre el uso de estas bandas lo que ha hecho que en ciertos países se permita todos los canales (Jerome, 2013), en otros ciertas sub-bandas y en casos extremos el uso en WLAN no está permitido con esta banda.

- Banda 1 (UNII-1, Unlicensed National Information Infraestructure -1 en Estados Unidos) abarca el espectro desde 5.15 a 5.25 GHz, se pueden utilizar cuatro canales que están separados 20 MHz (canales 36, 40, 44 y 48)

- Banda 2 (UNII-2) se extiende desde 5.25 a 5.35 GHz, permite el uso de cuatro canales separados 20 MHz (52, 56, 60 y 64). En la figura 9 se muestra la distribución del espectro para las bandas 1 y2.

- Banda 3 (UNII-2 extendido) se extiende desde 5.47 hasta 5.725 GHz y contiene 11 canales con 20MHz de separación (canales desde 100 hasta 140)

- Banda 4 (UNII-3) se extiende desde 5.725 hasta 5.825 GHz, contiene cuatro canales separados 20MHz (149, 153, 157, 161), esta es una banda ISM.

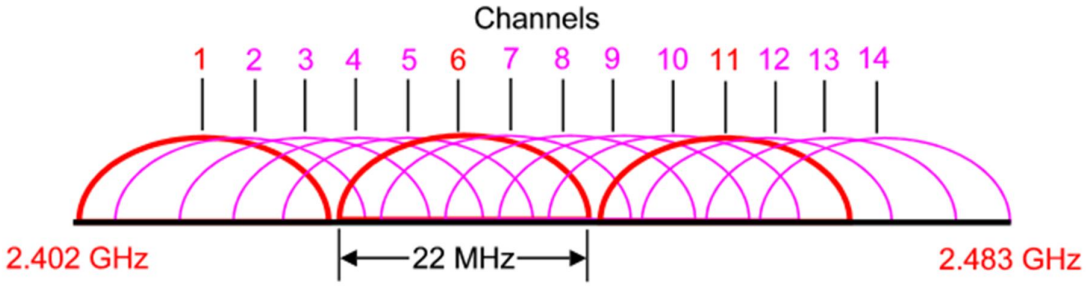


Figura 8. Canales para la frecuencia de 2.4GHz (Donovan, 2013)

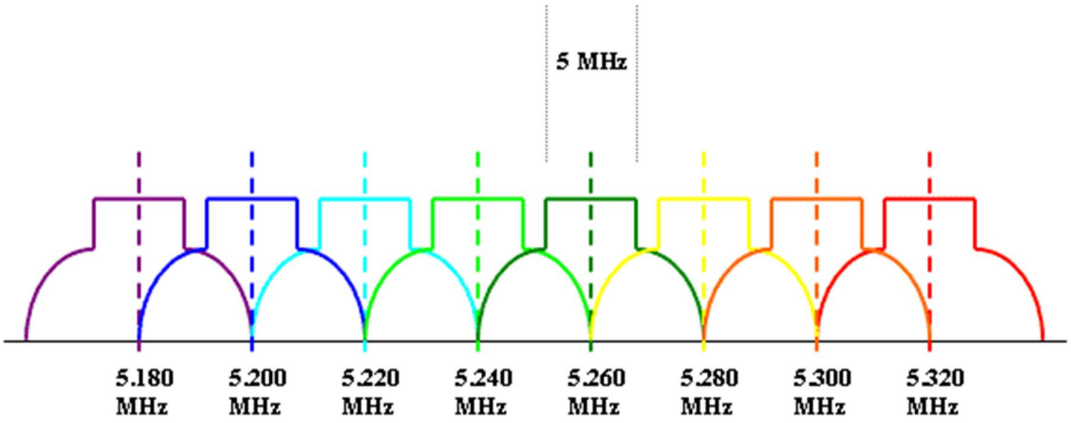


Figura 9. Canales para la frecuencia 5GHz (UNII-1 y UNII-2), (Bakin, 2007).

6.2. Estándares de redes inalámbricas IEEE 802.11

La primera versión del estándar 802.11 que se publicó en 1997 describe la utilización de tecnologías de modulación de Espectro Ensanchado por Salto de Frecuencia FHSS (Frequecy Hop Spread Spectrum) a 1 Mbps y la utilización del Espectro Ensanchado de Secuencia Directa DSSS (Direct Sequence Spread Spectrum) a 1Mbps y 2Mbps utilizando el espectro de 2.4HGz dividido en 14 canales separados 5MHz entre cada uno de ellos. En el transcurso del tiempo se han agregado varias enmiendas, cada enmienda contiene la palabra 802.11 más un carácter alfabético. El estándar en su conjunto fue revisado en el año 2007 para integrar todas las enmiendas publicadas en los años anteriores, esta revisión se llamó 802.11-2007 e integra las enmiendas 802.11a, b, d, e, g, h, i, j , (Jerome, 2013).

Una nueva revisión se llevó a cabo en 2011, ésta integraba las publicadas entre 2007 y 2011 (802.11k , r, y, w, n,p,z, v, u, s) y se llamó 802.11-2012.

6.2.1. 802.11b

802.11b fue publicado en 1999, utiliza el mismo método de acceso al medio (CSMA/CA) definido en el estándar original, 802.11b es una extensión de la tecnología DSSS, técnicamente utiliza un código de claves complementaria CCK (Complementary Code Keying), gracias al incremento drástico del throughput hasta 11Mbps y la reducción de costos de desarrollo lo llevaron rápidamente a ser adoptado como el estándar definitivo para la “Wireless LAN” (Carroll, 2008). Los dispositivos que utilizaban 802.11b experimentaron interferencias de otros dispositivos que operan en la misma banda de 2.4Gz como hornos de microondas, buethoots, teléfonos inalámbricos entre otros.

6.2.2. 802.11g

La enmienda publicada en 2003 introdujo la Multiplexación por División de Frecuencias Ortogonales OFDM (Orthogonal Frequency Division Multiplexing) a la banda de 2.4GHz, permitiendo tasas de hasta 54Mbps con su hardware compatible completamente con 802.11b.

802.11g así como mejora la velocidad a 2.4GHz también presenta importantes desafíos:

- La potencia máxima descrita para equipos OFDM en la banda de 2.4GHz en 802.11g es diferente a la descrita en 802.11 y 802.11b. Un cliente Wireless puede usar 20dBm para DSSS, pero solo 15dBm para para OFDM, situación que crea problemas en el diseño de celdas.

- 802.11g soporta estaciones 802.11b, pero no viceversa: las estaciones 802.11b no entienden por tanto ignoran las señales enviadas por una estación 802.11g. Para prevenir que una estación 802.11b transmita sus datos mientras una estación 802.11g está enviando o recibiendo, 802.11g implementa un mecanismo de protección. Cuando se detecta una estación 802.11b dentro de la celda, el AP informa su presencia a todas las estaciones mediante su información en modo broadcast. Este broadcast contiene dos bits puestos a 1: “nonERP_present (no-802.11g presente)” y

"use protection". En cuanto una estación 802.11b es detectada en la celda, las estaciones 802.11g usan el mecanismo de protección RTS/CTS (Request to Send/ Clear to Send) mediante el cual la estación 802.11g informa, a la velocidad de 802.11b, su intención de comunicar y la duración de esa comunicación, forzando a la estación 802.11b a permanecer escuchando. La desventaja de este mecanismo de protección es que divide el throughput total de la celda para 3 (Jerome, 2013), y aun peor, un AP vecino que escucha el mensaje de broadcast de un AP con elementos 802.11b a menudo decide implementar el mecanismo de protección en su celda.

6.2.3. 802.11a

A más de los problemas relacionados con el mecanismo de protección de clientes 802.11b están los inconvenientes relacionados con las interferencias en la banda de 2.4 GHz generados por dispositivos no-802.11 por el hecho de ser una banda ISM. Este problema surgió tan pronto el primer estándar 802.11 fue publicado. Con el propósito de remediar esta incómoda situación la enmienda 802.11A fue publicada en 1999.

802.11a hace uso únicamente de la modulación OFDM que permite manejar tasas de bits de 6Mbps hasta 54 Mbps. El principal cambio de 802.11a es que utiliza una banda dedicada a WLAN en el espectro de 5GHz que a diferencia de la banda 2.4 GHz, dispone de un espectro más amplio, permitiendo al estándar ofrecer hasta 23 canales no sobrepuestos. Los canales están separados 20 MHz lo cual es suficiente para un canal OFDM de 20 MHz requerido por el estándar, aun así la recomendación es dejar al menos un canal de separación cuando se usan dos canales en el mismo espacio físico, por ejemplo al utilizar los calanes 36 y 44 estamos dejando el canal 40 de separación. Como la banda de 5GHz es casi utilizada solo para WLAN esta sufre menos interferencia (Carroll, 2008).

6.2.4. 802.11n

Fue publicado en 2009 con el propósito de incrementar la velocidad más allá de los 54Mbps con la descripción de tres conjuntos de técnicas.

- **Agregación de canales**. 802.11n permite la unión de dos canales de 20MHz separados para formar un canal de 40Mhz (por ejemplo 36 y 40 en 5GHz o 1 y 5 en 2.4 GHz). Con este canal más grande, las sub-portadoras pueden ser utilizadas para la transmisión de datos, creando un canal con una tasa de datos de 119 Mbps. La agregación de canales no se recomienda en la banda de 2.4 GHz debido a que muy pocos canales están disponibles para la unión. Utilizar un canal de 40MHz también consume más energía que un canal de 20MHz, por esta razón los dispositivos portátiles (teléfonos, tablets) no soportan esta técnica (Jerome, 2013).

- **Mecanismo de eficiencia MAC.** Por ejemplo las estaciones pueden enviar ráfagas de tramas que son confirmadas con una sola trama de acuse de recibo después de la ráfaga, reduciendo la sobrecarga de tramas sin datos (non-data overhead). Otro mecanismo es utilizar un intervalo de guarda más corto (el silencio entre símbolos en una onda) 400ns en lugar de 800ns. Este proceso incrementa la velocidad en un 11%, pero también incrementa el riesgo de colisiones en un ambiente ruidoso.

- **MIMO (multiple input, multiple output).** Es el mecanismo que más se publicita. Una estación 802.11n puede tener varios radios en el mismo canal y usarlos al mismo tiempo permitiendo varias mejoras como:

    - **Transmit Beamforming (TxBF)** El emisor puede enviar la misma señal por varias antenas. Con una coordinación cuidadosa en base a la retroalimentación que transmite la estación receptora 802.11n, el emisor apunta a que la señal sea recibida en fase por lo tanto incrementa su nivel de potencia en el receptor permitiendo un mayor rango de cobertura o un throughput muy alto.

    - **Multiplexación espacial**. El emisor puede también enviar diferentes señales simultáneas por diferentes radios, el receptor 802.11n recibirá estas señales en todos sus radios, cada uno de los radios receptores decodifica la señal independientemente, y cada señal recibida es combinada con la señal de otros radios dando como resultado throuhput adicional.

    - **Multi Ratio Combining (MRC)**. Como consecuencia de "multipath" la señal viaja por diferentes rutas antes de llegar al receptor, con MRC, el receptor puede combinar las señales recibidas en cada antena y radio resultando una señal recibida más fuerte dando como resultado el incremento de la cobertura o velocidad.

Estas técnicas permiten a los dispositivos 802.11n alcanzar tasas de datos de hasta 144Mbps cuando se utilizan dos "streams", intervalo corto de guarda con canales de 20MHz, y 300Mbps utilizando dos streams, intervalo corto de guarda con canales de 40MHz.

6.2.5. 802.11ac

802.11ac es una evolución del estándar 802.11n, donde uno de los objetivos es disponer de niveles muy altos de rendimiento comparables con las redes Gigabit Ethernet, experimentando una transferencia de datos instantánea. Esto permite a usuarios domésticos la distribución de contenido en múltiples canales de alta definición (HD, High Definition) en todas las áreas de la casa; mientras que para una empresa, los desafíos consisten en la distribución de la red con velocidad y latencia de clase-empresarial, ambientes de alta densidad de clientes por AP para el despliegue eficiente de la tendencia BYOD donde un usuario puede conectar hasta tres dispositivos inalámbricos a la red, y el incremento de la adopción del video streaming (Cisco Systems, 2013).

De acuerdo a como se describe en (Cisco Systems, 2013), 802.11ac obtiene el incremento en la velocidad bruta enfocándose en los siguientes tres parámetros:

- Uniendo más canales, se incrementa de un máximo de 40 MHz en 802.11n hasta 80 o aún 160 GHz (que representa un incremento en la velocidad del 177 o 333 por ciento, respectivamente)

- Modulación más densa, utilizando modulación 256 QAM (Quadrature Amplitude Modulation) de 64QAM usado con 802.11n (representa un incremento del 33 por ciento de velocidad)

- MIMO, mientras en 802.11n se utiliza hasta 4 secuencias espaciales (spatial streams), 802.11ac va más allá con el uso de 8 “spatial streams” para un incremento del 100% de la velocidad.

802.11ac es una tecnología que funciona únicamente en 5GHz, pero los APs de doble banda continuaran utilizando 802.11n a 2.4GHz, sin embargo los clientes 802.11ac operaran en la banda menos congestionada de 5GHz.

Los productos 802.11ac se los puede clasificar en dos grupos: de primera fase y de segunda fase; los de primera fase, construidos sobre canales de 80 MHz reparten en la capa física hasta 433 Mbps (gama baja), 867 Mbps (gama media) y 1300 Mbps (gama alta); mientras que los dispositivos de segunda fase pueden prometer aun mayor unión de canales y “spatial streams” que configurados adecuadamente operaria hasta 3.47 Gbps.

Los equipos de segunda fase podrían incorporar una nueva tecnología, MIMO multiusuario MU-MIMO. Mientras que 802.11n es comparable con un hub Ethernet donde solo puede transmitir una trama a la vez en todos sus puertos, MU-MIMO permite a un AP enviar múltiples tramas a múltiples clientes al mismo tiempo sobre el mismo espectro de frecuencia pero utilizando múltiples antenas haciendo que el AP se comporte como un switch inalámbrico.

6.3. Tipos de redes inalámbricas

Las redes inalámbricas hacen uso de diferentes tecnologías dependiendo de la distancia que se quiere alcanzar, el número de dispositivos a conectar y la cantidad de información a transmitir. Las tecnologías incluyen:

- Redes Inalámbricas De Área Personal, WPAN (Wireless Personal Area Network), tienen un rango de cobertura corto, hasta unos 7 o 10 metros. Este tipo de redes se basa en el conjunto de especificaciones de los estándares 802.15[4] para conectar dos o más dispositivos con bajo consumo de potencia, un ejemplo de tecnología de este tipo de red es bluetooth.

- Redes Inalámbricas De Área Local, WLAN (Wireless Local Area Network), los dispositivos consumen mayor cantidad de potencia, pero extienden su cobertura hasta unos 100 metros o más según las nuevas enmiendas como 802.11n, 802.11ac

[4] El IEEE 802.15 es un grupo de trabajo dentro del IEEE 802 que define las redes inalámbricas de área personal WPAN o redes inalámbricas de corta distancia. La evolución constante de la tecnología ha llevado a que se desarrollen varias revisiones al estándar desde el estándar original basado en Bluetooth (802.15.1) para la interconexión de dispositivos a no más de 10m, pasando por la revisión 802.15.2 que permite la coexistencia de WPAN con otros dispositivos que utilizan frecuencias ISM como WLAN, 802.15.3 que define parámetros de WPAN de alta velocidad, 802.15.4 para redes WPAN de baja velocidad, 802.15.5 para la definición de redes tipo malla interoperables, estables y escalables, 802.15.6 donde se optimiza el consumo de energía de dispositivos BAN (Body Area Network) que se utilizan en el cuerpo humano tal es el caso de los sensores y 802.15.7 que define el uso de luz visible para la comunicación de corto alcance. Los principales objetivos que se pretenden conseguir son principalmente: facilitar la comunicación entre dispositivos móviles, eliminar cables y conectores, crear redes inalámbricas pequeñas que faciliten la sincronización de datos entre los equipos personales. (Rodriguez, 2015).

- Redes Inalámbricas Metropolitanas, WMAN (Wireless Metropolitan Area Network), extiende su cobertura a lo largo de una área geográfica extensa, como una ciudad por ejemplo, para alcanzar la cobertura deseada se utilizan enlaces punto-punto o punto-multipunto, Las redes WMAN utiliza frecuencias de espectro licenciado, aunque también utiliza bandas ISM; WiMAx[5] es una tecnología muy utilizada para WMAN.

- Redes Inalámbricas De Área Extensa, WWAN (Wireless Wide Area Network), este tipo de redes proveen una cobertura geográfica mucho mayor que las redes WMAN, ejemplos de este tipo de redes son las redes de telefonía móvil y los servicios de portadores de datos. Utilizan bandas licenciadas.

6.4. Modo de operación de las redes inalámbricas de área local.

El estándar 802.11 define dos modos de operación, el modo Ad-hoc o independiente y el modo de infraestructura, (Jerome, 2013).

6.4.1. Modo Ad-hoc.

Dos dispositivos inalámbricos, conocidos como estaciones en el estándar 802.11, que se encuentren dentro del mismo rango al compartir simples parámetros en común como la frecuencia, nombre de conexión, entre otros, están en capacidad de comunicarse y formar una WLAN. La primera estación define los parámetros de radio y el nombre de la conexión; las otras estaciones detectan la conexión y ajustan sus parámetros para conectarse a la primera estación y a los demás que se conecten. Es decir en este modo de operación la información viaja directamente entre la estación que transmite y la estación que recibe sin pasar por ningún otro equipo y se grafica en la figura 10.

En cuanto las estaciones están conectadas entre sí, se forma un “Conjunto Básico de Servicios” o BSS (Basic Service Set), las redes ad-hoc no dependen de ningún otro dispositivo más que de las estaciones mismas que la forman, por lo que también se conoce como Conjunto Básico de Servicios Independientes o IBSS (Independent BSS), esta falta de un dispositivo central que defina reglas en común como parámetros de radio, prioridades, rango, entre otros hacen que su funcionalidad sea limitada.

Para permitir el acceso de los elementos de esta red inalámbrica a la red cableada es necesario conectar una de las estaciones, la misma que actuará como enrutador.

[5] WiMax es el estándar de acceso inalámbrico para redes metropolitanas ratificado por el IEEE a través del grupo de trabajo IEEE 802.16. el objetivo de WiMax es proporcionar acceso a Internet de alta velocidad que en teoría va hasta los 70Mbps en un rango de 50Km. El principio de operación de WiMAx se basa en el término “enlace punto a multipunto”, donde el principal elemento es el transceptor de la estación base (BTS) que se comunica con las antenas de los abonados, sin que sea necesario tener línea de vista directa entre el abonado y la estación (NLoS, No Line of Sight). El estándar tiene dos revisiones, IEEE 802.16d (802.16-2004) o WiMAx fijo determina las conexiones a los abonados en puntos fijos a través de una antena, funciona en las bandas licenciadas de 2.5 GHz y 3.5 GHz y no licenciada de 5.8 GHz; IEEE 802.16e o WiMax móvil que permite la movilidad de los abonados dentro del área de cobertura de la BTS. (CCM Benchmark, 2015)

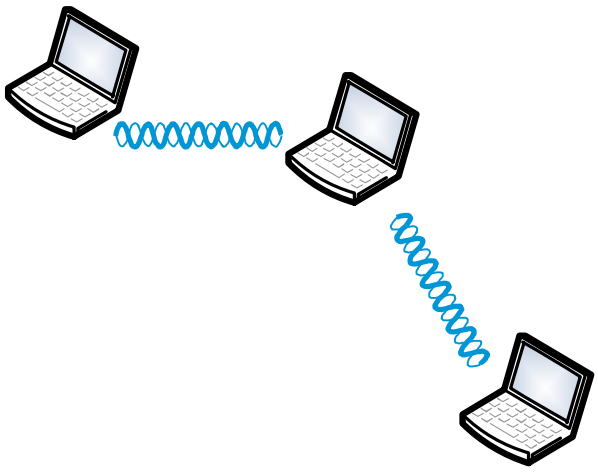


Figura 10. Diagrama de una red Ad-Hoc o IBSS (Jerome, 2013).

El modo ad-hoc fue descrito en el protocolo original 802.11 y la enmienda 802.11b, este modo no es muy escalable y no se describió en las posteriores enmiendas como 802.11a u 802.11g. Si se configura una red ad-hoc con equipos certificados WIFI la red se limita a trabajar en 2.4GHz con una tasa de bits máximo de 11Mbps (valor máximo en la enmienda 802.11b) sin autenticación y sin encriptación o seguridad de clave compartida WEP[6].

6.4.2. Modo Infraestructura.

A diferencia del modo ad-hoc, en el modo infraestructura se utiliza un dispositivo central llamado Punto de Acceso (AP, Access Point) que define un conjunto de parámetros en común. Los dispositivos inalámbricos envían su señal hasta un AP, el cual retransmite la señal a la estación inalámbrica de destino o a la red cableada.

Un AP es un dispositivo con un concepto similar a un hub Ethernet donde todas las estaciones comparten la misma frecuencia y sólo una estación puede transmitir en un tiempo determinado formando una red half-duplex. El AP ofrece un BSS como en una red ad-hoc, pero no un IBSS porque del AP depende la conexión de las estaciones.

Para comprender mejor los conceptos referentes al modo infraestructura la gráfica de la figura 11 será de gran utilidad.

[6] WEP (Wired Equivalent Privacy), Privacidad Equivalente a Cableado, definido en el estándar IEEE 802.11 inicial, podía ser utilizado como mecanismo de autenticación y/o encriptación con un mecanismo desafío – respuesta. WEP utiliza claves de 40 bits y 104 bits. Para asegurar que le mismo contenido de datos enviado varias veces no resulta en el mismo valor encriptado, WEP agrega un Vector de Iniciación (IV) aleatorio de 24 bits a cada nuevo paquete que se envíe. Los datos son encriptados usando el algoritmo RC4 y con la combinación de la clave WEP y IV. A partir del 2004 ya no es considerado como mecanismo de seguridad para redes Wi-Fi. (Jerome, 2013).

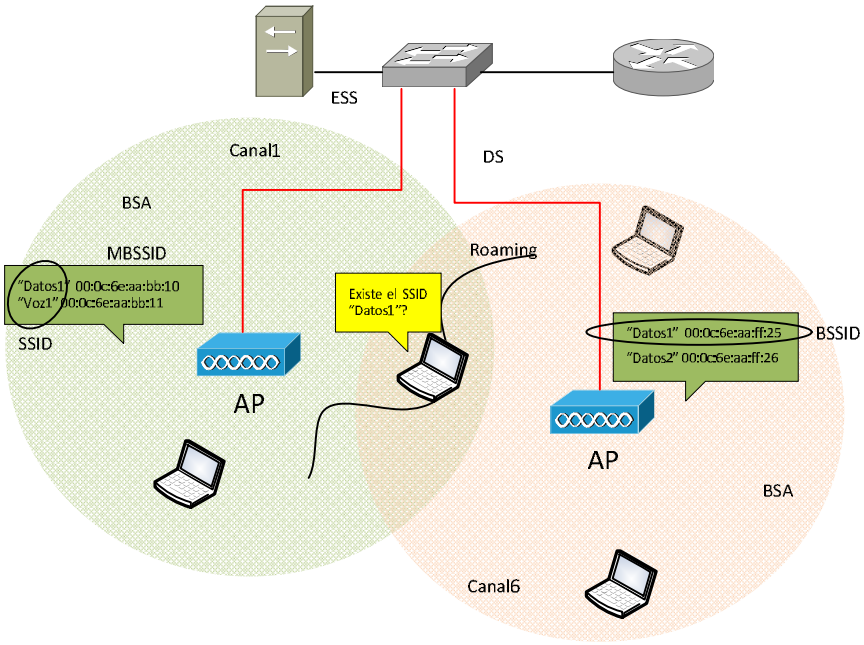


Figura 11. Conceptos de una red inalámbrica en modo Infraestructura (Jerome, 2013).

El área que cubre un AP se llama Área de Servicios Básicos o BSA (Basic Services Area) comúnmente conocido también como celda. La sección cableada que se puede alcanzar a través del AP, desde la perspectiva inalámbrica, se conoce como Sistema de Distribución (DS, Distribution System). Cuando el DS une dos APs, o dos celdas, el grupo se llama Conjunto de Servicios Extendidos (ESS, Extended Service Set). Un ESS puede ser alcanzado solo a través de un AP BSS, no a través de un cliente IBSS conectado a la red cableada. Si una estación deja el área de cobertura del AP al que se conectó originalmente y pasa al BSA de otro AP, se dice que la estación esta itinerando (roaming) entre celdas. Para evitar interferencias, las celdas vecinas están en diferentes canales. La detección de celdas vecinas es transparente desde el punto de vista de la estación, para esto el AP al que se conecta y el anterior ofrece el mismo conjunto de parámetros y tipo de conexión, usa el mismo nombre o identificador de conjunto de servicios SSID (Service Set IDentifier) definido con un conjunto de caracteres ASCII que dan nombre a la conexión.

Cada AP se identifica a si mismo asociando la dirección MAC de su radio con el SSID, esta asociación se conoce como Identificador de Conjunto de Servicios Básico (BSSID) y permite conocer a las estaciones que AP ofrece que SSID. Cuando un AP tiene la capacidad de difundir más de un SSID tenemos un Multiple BSSID (MBSSID).

6.5. Capa física de la redes IEEE 802.11

El estándar IEEE 802.11 define las capas física y de acceso del modelo OSI para las comunicaciones inalámbricas, la capa física es la encargada de controlar todos los parámetros del medio de transmisión, en esta capa tenemos las definiciones que hacen referencia al espectro ensanchado (spread spectrum) que es la forma como se modula y señaliza la señal para transmitirse en el medio (Jerome, 2013).

6.5.1. FHSS (Frequency Hop Spread Spectrum) – Espectro Ensanchado por Salto de Frecuencia.

Con el objetivo de evitar interferencias, se utiliza la técnica de salto de frecuencias, donde la banda de 2.4GHz se divide en muchos canales más pequeños (79 canales en Estados Unidos, FCC), el transmisor selecciona e informa al receptor de los canales seleccionados y la secuencia de saltos, y emite la señal mientras salta de un canal a otro canal cada 300 a 400 ms, con esto si la interferencia en el medio provoca la pérdida de la señal de un canal solo se perderían 300 o 400ms de información, (Jerome, 2013).

Esta técnica fue descrita por el estándar original 802.11 y en enmiendas posteriores ya no es utilizado, esto por dos razones principalmente, la primera que no es muy escalable, por ejemplo si se dispone de diez transmisores y receptores los diferentes saltos de frecuencia colisionaran y cada uno sufrirá la interferencia de los saltos de frecuencia de los otros; la segunda razón es porque la cantidad de información que se envía por canal es limitada dado que los canales son de 1MHz. La técnica de modulación que se emplea es FSK (Frequecy Shift Keying) que permite alcanza una velocidad de 1Mbps ampliable a 2 Mbps.

6.5.2. DSSS (Direct Sequence Spread Spectrum) - Espectro ensanchado por Secuencia Directa.

A diferencia del método FHSS, con este método la información se envía por un canal mucho más ancho, de 22 MHz para ser más precisos, y sin saltos entre los canales, sobre estos canales varios bits de información se envían en paralelo, (Jerome, 2013).

DSSS genera un código para representar cada 0 o 1 que se vaya a transmitir, este código también se llama símbolo o chip y puede ser una secuencia de hasta 11 bits, esta secuencia se llama código “Barker 11” (en la figura 12 tenemos la representación de la codificación Barker 11), estos bits son enviados en paralelo en el canal de 22MHz, y para poder recuperar la señal con dos de estos bit sería suficiente.

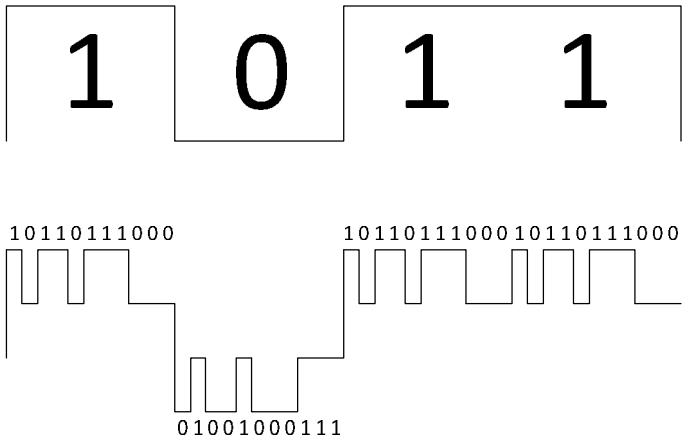


Figura 12. DSSS, codificación “Barker 11” (Info Tech plus, n.d.).

La manera como son representados los 1 o 0 en RF se conoce como modulación, que no es otra cosa que cambiar la onda para representar alguna señal, una vez que la información se ha codificado se puede utilizar dos técnicas de modulación, la primera opción es DPSK (Differential Phase Shift Keying) cuya condición dice: cuando el siguiente valor a enviar es un 0 , no hace nada especial, simplemente la onda se envía continuamente, cuando el siguiente valor a enviar es 1, la dirección de la onda cambia; el resultado es una comunicación de 1Mbps.

La segunda opción de técnica de modulación es DQPS (Differential Quadrature Phase Keying), que agrupa los bits en pares (00, 01, 10, 11) y debe cumplir la siguiente condición: si los bits a transmitir son 00 no hace nada, la onda se envía continuamente, si se va a transmitir un 01 la onda se desfasa 90 grados, para trasmitir un 10 se debe desfasar 270 grados y para transmitir un 11 debe existir un desfase de 180 grados, con esta técnica se envían dos bits en la misma onda doblando la tasa de bits hasta 2 Mbps para la transmisión.

6.5.3. CCK (Complementary Code Keying) – Codificación de Código Complementario.

Cada grupo de 4 bits se codifica en un símbolo de 6 bits en lugar de los 11 bits de Barker 11, obteniéndose 64 símbolos diferentes, cada uno de los cuales representa a un único chip de 6 bits (ver figura 13). A cada chip de 6 bits se agregan dos bits, para representar la orientación del inicio de símbolo y ayudar a regenerar la señal si parte del símbolo no se recibe, (Jerome, 2013).

La onda se envía sobre un canal de 22MHz a una velocidad de 1.375 millones de símbolos de código por segundo que representa 4 bits dando como resultado un throughput de 5.5 Mbps. Posteriormente los dos bits de orientación se utilizaron para representar dos símbolos diferentes en lugar de solo la orientación del símbolo, consiguiendo doblar la tasa de bits a 11Mbps.

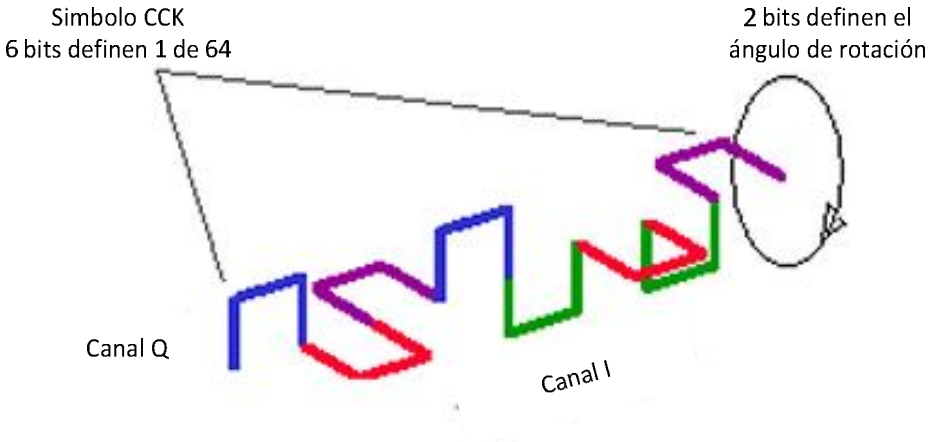


Figura 13. Representación del símbolo CCK (Bakin, 2007).

6.5.4. OFDM (Orthogonal Frequency Division Multiplexing).

La técnica de modulación OFDM reduce el tamaño de canal de 22MHz empleado en DSSS a un canal de 20MHz y este a su vez es subdividido en 52 sub canales o sub portadoras con una separación de 312.5 kHz. 48 sub-portadoras se utilizan para llevar los datos y las 4 restantes para control de la comunicación. Cada sub-portadora utiliza BPSK o QPSK, la representación de estas dos técnicas de modulación las podemos apreciar en las figuras 14 y 15 respectivamente. Estas sub-portadoras no necesitan ser muy veloces, la velocidad se da por el gran número de sub-canales que se disponen, permitiendo alcanzar hasta 18 Mbps. (Jerome, 2013).

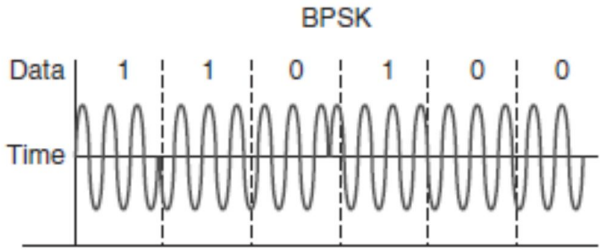


Figura 14. Representación de técnica de modulación BPSK (Jerome, 2013).

Con el propósito de alcanzar mayor tasa de bits en la transmisión también se hace uso de la técnica de modulación QAM (Quadrature Amplitude Modulation), esta técnica cambia la amplitud o la dirección o fase para representar el siguiente grupo de bits. Para cuatro cambios de dirección o fase de QPSK, QAM agrega cuatro cambios en la amplitud, creando 16 combinaciones para poder representar 16 símbolos, de aquí el nombre de la primera variante, 16-QAM, representada en la figura 16. Con esta variante 4 bits son codificados por símbolo y 500kbps por portadora; para mejorar la resistencia del sistema cada símbolo se repite dos veces (16-QAM 1/2, de todos los símbolos enviados la mitad corresponde a la información original) permitiendo un throughput total de 24 Mbps; esta velocidad se puede incrementar si solo se repite ¼ de los símbolos (16-QAM ¾) hasta 36 Mbps. OFDM puede usar también 64-QAM donde ahora se transmite 64 símbolos y 8 bits se codifican en cada símbolo. Si se utiliza 1/3 de los símbolos para redundancia se puede alcanzar una tasa de bits de 48Mbps con sub-portadoras de 1Mbps (64-QAM 2/3). Si se reducen los símbolos de redundancia a ¼ la velocidad puede incrementar hasta 54Mbps (64-QAM ¾) transmitiendo 1.125 Mbps por canal.

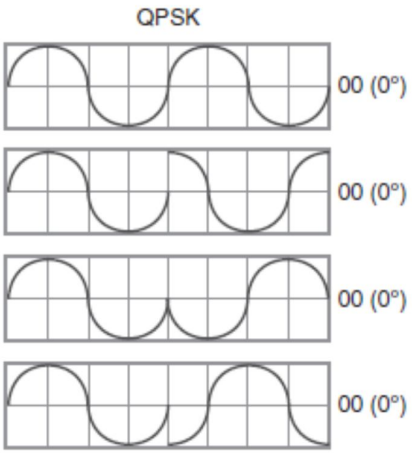


Figura 15. Representación de técnica de modulación QPSK (Jerome, 2013)

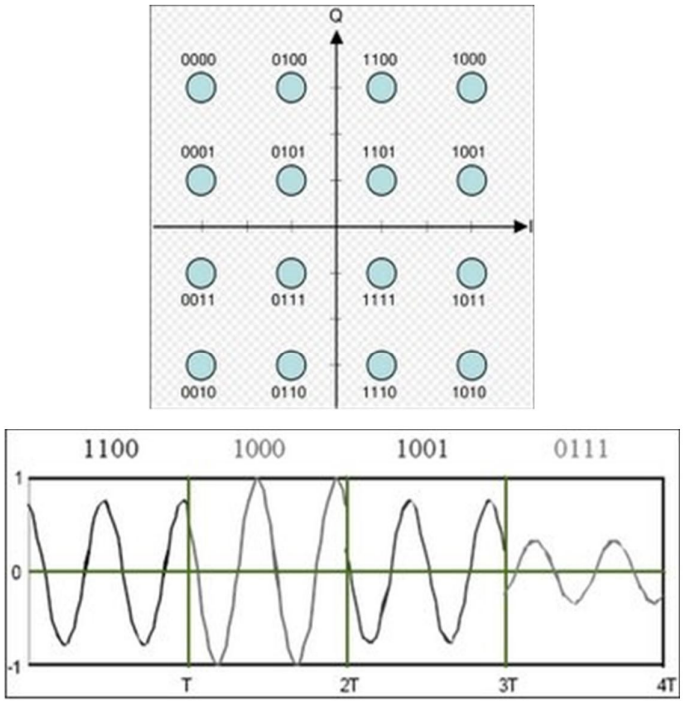


Figura 16. Representación de técnica de modulación 16 QAM (Jerome, 2013).

En la tabla 2, se presenta un resumen de las técnicas de modulación que se encuentra en el estándar 802.11 y su correspondiente tasa de transmisión de datos "data rate" para una mejor comprensión de la evolución de los estándares (Jerome, 2013).

*Tabla **2**. Resumen de las técnicas de modulación utilizadas en 802.11.*

Técnica de modulación	Data rate (mbps)
BPSK	1
QPSK	2
CCK	5.5
OFDM (BPSK ½)	6
OFDM (BPSK ¾)	9
CCK	11
OFDM (QPSK ½)	12
OFDM (BPSK ¾)	18
OFDM (16-QAM ½)	24
OFDM (16-QAM ¾)	36
OFDM (16-QAM 2/3)	48
OFDM (16-QAM 3/4)	54

Fuente. (Jerome, 2013)**.**

6.6. Capa de enlace de datos IEEE 802.11

La capa de enlace de datos del estándar IEEE 802.11 es la encargada del control de acceso al medio, indistinto de la versión del protocolo con la que se trabaje, el objetivo de todo dispositivo inalámbrico es evitar las colisiones durante la comunicación, las colisiones ocurren cuando dos equipos transmiten al mismo tiempo, y se evitan utilizando mecanismos de contención. Cuando no tenemos un dispositivo central que decida que trama transmitir primero y en su lugar cada dispositivo se preocupa de aquello, estamos dentro del concepto de un método de acceso no centralizado. El método de acceso no centralizado también es llamado como Función de Coordinación Distribuida (DCF, Distributed Coordination Function) donde las estaciones siempre escuchan el medio y se abstienen de enviar si la señal de otra estación es detectada. Después de que la señal se envía por completo hay un silencio o espacio de tiempo sin transmisión hasta que las señales multipath desaparezcan. La longitud del silencio es determinada por la prioridad de la trama (Jerome, 2013):

- Espacio corto entre-tramas SIFS (Short Interframe Space) es el tiempo que una estación debe esperar si la trama tiene prioridad alta.

- Espacio entre-tramas Distribuido DIFS (Distributed Interframe Space) , es el periodo utilizado para transmitir tramas estándar, este es el temporizador normal en las rede DCF

- Espacio entre-tramas reducido RIFS (Reduced Interframe Space), se utiliza en las redes 802.11n entre cada segmento de una ráfaga.

Para evitar colisiones, los dispositivos dentro de una celda utilizan el mecanismo de Acceso Múltiple con Detección de Portadora y Evitar Colisiones CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance). Cuando el dispositivo necesita enviar una trama en primer lugar toma un número aleatorio entre 0 y 31 y empieza el conteo regresivo desde ese número, a este espacio de tiempo se lo conoce como temporizador de retardo (backoff timer). La velocidad a la que ocurre el conteo regresivo se llama ranura de tiempo (slot time) y depende del protocolo. En la tabla 3 tenemos los valores comunes del slot time para las diferentes versiones del estándar 802.11 (Yang R. , 2012).

Tabla 3. Parámetros básicos para el cálculo del backoff timer.

	802.11b	**802.11a**	**802.11g**
Slot Time	20 us	9 us	20 us (red mixta) 9 us (solo g)
CWmin	31 slots	15 slots	15 slots
SIFS	10 us	16 us	10 us
DIFS = 2xSlot + SIFS	50 us	34 us	50 us (red mixta) 28 us (solo g)

Fuente: (Yang R. , 2012).

Cuando una estación detecta que una trama está siendo transmitida durante el conteo regresivo, la estación detiene su conteo, y la reanuda una vez que la trama ha sido transmitida completamente. El encabezado de la trama, contiene la duración de la trama o vector de asignación de red NAV (Network Allocation Vector) y la estación que la detecta puede sumar el NAV a su contador y continuar con el conteo regresivo desde el nuevo total. Cuando el conteo llega a cero la estación transmite asumiendo que el medio está libre. Al tiempo total que una estación espera para transmitir, es decir a la sumatoria del tiempo de backoff mas la espera por la transmisión de otra estación se llama ventana de contención (Contention window).

El desarrollo del intercambio de tramas en el medio entre dos estaciones lo podemos apreciar en la figura 2.17 (Rajesh, 2006).

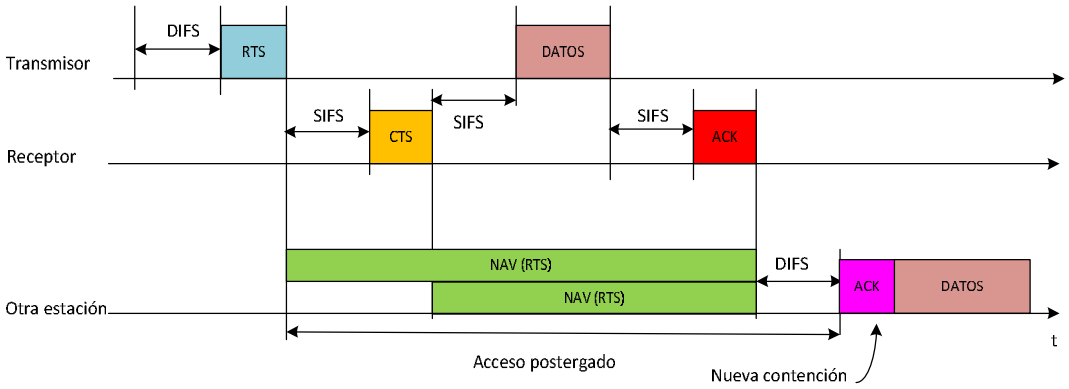


Figura 17. Acceso al medio 802.11 (Rajesh, 2006).

Las redes WLAN trabajan en modo half-duplex, esto provoca un inconveniente, que es, que la estación no puede recibir mientras transmite, por esta razón la estación no sabe si la trama llegó a su destino o se dañó en el medio. Para solucionar este inconveniente todas las tramas unicast solamente reciben un mensaje de acuse de recibo ACK (acknowledge) desde la estación de destino. El receptor, posterior a la recepción del paquete espera SIFS y envía el mensaje de acuse de recibo a la estación que transmitió la trama.

Si la transmisión de la trama falló, la estación toma un número que es el doble del original para el temporizador de retardo, espera DIFS y empieza el conteo regresivo desde el nuevo número. Para cada transmisión fallida incrementa en el doble del número anterior hasta un máximo de 1023.

6.6.1 Tramas 802.11

Las tramas correspondientes a todos los estándares tienen la estructura similar, y están compuestos por los siguientes campos (ver figura 18):

- Preámbulo: 72 o 144 bits de longitud
- Control de trama (“frame control”)
- Duración: 16 bits
- Direcciones MAC: 48 bits cada uno.
- Opcional (QoS o información 802.11n)
- Cuerpo de la trama: por defecto 2304 bytes máximo, se puede extender con 802.11n.
- Secuencia de control de trama FCS (Frame Control Sequence): 4 bytes.

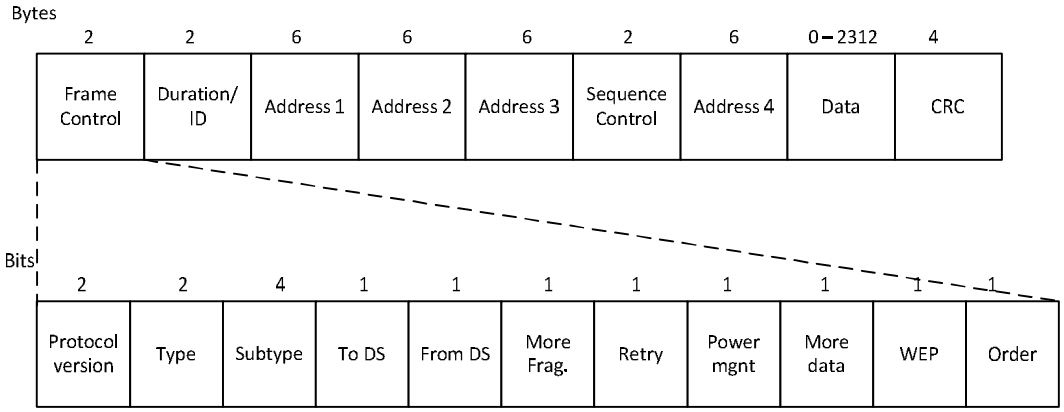


Figura 18. Trama 802.11 (Yang R. , 2012).

La longitud total de la trama es por defecto de 2346 bytes máximo. El contenido del cuerpo depende del tipo de trama y su propósito, existen tres tipos de tramas: de datos, de administración y de control. (Jerome, 2013).

2.6.1.1. Tramas de Datos.

Este tipo de tramas lleva información, el encabezado contiene tres o cuatro direcciones MAC cuyo orden depende del emisor, sea estación o AP, entre los tipos de direcciones MAC que podemos encontrar están (Jerome, 2013):

- Dirección Fuente SA (Source Address), es la dirección del equipo que generó la trama original.
- Dirección de Receptor RA (Receiver Address), corresponde al radio receptor.
- Dirección del Transmisor TA (Transmiter Address), corresponde al radio transmisor.
- Dirección de Destino DA (Destination Address), es el destino final de la trama.

De los tipos de direcciones indicadas anteriormente, tres direcciones MAC están siempre presente en la trama, la cuarta es utilizada solo para comunicación AP – AP; las direcciones fuente y destino (SA, DA) están presente cuando la trama es reenviada por uno o varios APs.

2.6.1.2. Tramas de Administración.

Contiene información del Área Básica de Servicios (BSA) o los parámetros de comunicación que ayudan a la administración de la celda (Jerome, 2013).

- **Beacons:** son enviados mediante broadcast por el AP a la tasa de tramas mandatorio "mandatory frame rate" más baja cada 102.4 (100 TU) ms por defecto. Los beacons contienen información relacionada a la red como el SSID que es el nombre que identifica a la red, la tasa de bits permitida en la ceda.

- **Probe request, Probe response**, los dispositivos pueden enviar tramas de sonda de solicitud (probe request) a la dirección de broadcast o la dirección MAC del AP preguntando por características de la red inalámbrica, el AP responde mediante tramas de sonda de respuesta (probe response) con información similar a la contenida en las tramas beacon.

- **Authentication:** Cuando una estación decide unirse a la celda, envía una trama de solicitud de autenticación (authentication request) y recibe un respuesta de autenticación (authentication response) desde el AP, pudiendo esta respuesta ser directamente un mensaje de autenticación exitosa en el caso de utilizar autenticación abierta, o el inicio de la fase de desafío cuando se utiliza otro método de autenticación como WEP.

- **Association:** Una vez completada la fase de autenticación, el cliente envía una solicitud de asociación (association request) y recibe del AP una trama de respuesta (association response) con un número único que identifica a la estación en la celda.

- **Deassociation, reassociation, deauthentication**: en cualquier momento el cliente puede dejar la celda o el AP puede desconectar al cliente utilizando las tramas "deassociation" o "deauthentication"; el cliente que salió de la celda momentáneamente o se cambia de AP (roaming) puede unirse nuevamente a la red enviando una trama de solicitud de re-asociación y el AP envía la respuesta correspondiente.

2.6.1.3 Tramas de control.

Son tramas especiales que se utilizan en la celda para mejorar la eficiencia de la conexión, así tenemos las tramas ACK o acuse de recibo de tramas unicast, que indica que la trama fue recibida en el otro dispositivo con éxito. También tenemos las tramas RTS/CTS como protección contra colisiones en dos casos:

- Cuando existen clientes 802.11b en una red 802.11g, la estación 802.11g envía un mensaje de solicitud para enviar, RTS (Request to Send), a la velocidad de 802.11b y el receptor responde con un mensaje indicando que el medio está libre para transmitir, CTS (Clear to Send) a la velocidad de 802.11b. La estación 802.11b permanecerá en silencio mientras la comunicación ocurre a una tasa de bits 802.11g.

- Nodo oculto, se conoce como nodo oculto cuando dos estaciones están en lados opuestos de la celda, donde puede escuchar al AP pero no se escuchan entre sí, y si transmiten al mismo tiempo se producirá una colisión. Con el mecanismo RTS/CTS, cada estación escucha el CTS del AP y permanece en silencio mientras se produce la transmisión de tramas de la otra estación.

6.7 Disponibilidad de QoS en redes WLAN

Las redes inalámbricas por factores característicos de su funcionamiento no ofrecen calidad de servicio QoS, razón por la cual en 2005 el IEEE publicó la enmienda 802.11e donde se diseñan mecanismos de Calidad de Servicio (QoS) y priorización del tráfico.

Con la enmienda 802.11e crea cuatro colas: AC_VO para tráfico prioritario como la voz en tiempo real, Platino (Platinum); AC_VI para tráfico menos urgente como el video, Dorado (Gold); AC_BE con prioridad estándar, Plata (Silver) y AC_BK para tráfico que no es urgente, Bronce (Bronze). Los nombres que se indican entre paréntesis hacen referencia a la nomenclatura de los perfiles que utilizan los equipos Cisco (Jerome, 2013).

Una estación usa internamente las cuatro colas en paralelo, y selecciona aleatoriamente el temporizador de retardo de un rango mucho más corto para el tráfico urgente, de tal forma que se maximice la oportunidad de que el tráfico urgente alcance primero el valor cero y sea transmitido. Cuando se utiliza una estación con QoS no se utiliza DIFS, en su lugar se emplea un Espacio de inter-tramas de Arbitraje AIFS (Arbitration Interframe Space) el cual es mucho más corto para el tráfico urgente que DIFS.

802.11e ofrece estas características a través de dos esquemas de QoS principales, los mismo que se desarrollarán en el capítulo dedicado a este tema: El más simple se llama Acceso de Canal Distribuido Mejorado EDCA (Enhanced Distributed Channel Access) y el más complejo el Acceso de Canal Controlado por Coordinador de Función Hibrido, HCCCA (Hybrid Coordinated Function Controlled Channel Access). La organización Wi-Fi Alliance publicó la certificación WIFI Multi Media (WMM) para las estaciones que implementan las funciones en EDCA.

6.8. Necesidades de QoS en servicios de telefonía IP sobre WLAN

La tecnología de voz sobre IP (VoIP) sobre la cual se levanta el servicio de telefonía IP, ha expandido el rango de los servicios de voz y dispositivos para que los usuarios puedan elegir. Los servicios de voz no solamente están restringidos a las redes cableadas por conmutación de circuitos o redes celulares que tradicionalmente se diseñaron para transportar el tráfico de voz (Wi-Fi Alliance, 2008). En la actualidad virtualmente cualquier conexión de banda ancha basada en IP puede soportar voz, pero la calidad de la llamada se ve afectada por las características de rendimiento de la red.

La VoIP es una aplicación que tiene requerimientos únicos debido a su alta sensibilidad a los retardos en la red. Particularmente las llamadas de voz son extremadamente sensibles a la latencia o retardo, jitter y pérdida de paquetes durante la transmisión como se verá en los capítulos siguientes. Al comparar aplicaciones como la descarga de un archivo muy grande o la navegación a internet que típicamente requieren más ancho de banda, pero tienen mayor flexibilidad en el manejo de valores altos de latencia, jitter y pérdida de paquetes, que nos dan una percepción de degradación del rendimiento como la descarga o navegación lenta. En contraste con una llamada de voz que simplemente no puede continuar si estos valores son demasiado altos volviendo a la conversación muy distorsionada o inaudible.

Dentro de una pequeña empresa u hogar inclusive, la voz sobre WIFI típicamente es utilizada dentro de una red compartida donde múltiples flujos o “streams” compiten por la disponibilidad de los recursos de red. Para optimizar el rendimiento de la red mientras se provee soporte consistente para aplicaciones de voz, la voz tiene que ser priorizada sobre el tráfico de datos, audio o video con la aplicación de técnicas de calidad de servicio QoS en redes inalámbricas definidas en la certificación WMM del WIFI Alliance, o su similar el estándar 802.11e.

Para ayudar a asegurar la buena calidad de la voz en equipos “WIFI Certified”, la WIFI Alliance ha desarrollado un programa opcional llamado “WIFI Certified Voice-Personal” que no ha tenido el despliegue esperado por cuanto la cantidad de dispositivos cliente que cuentan con esta certificación es muy baja[7]. El programa dirige los requerimientos específicos de las aplicaciones de voz en ambientes de empresas pequeñas y domesticas (SOHO Small Office Home Office) requiriendo de los dispositivos de cliente y Access Points satisfacer los niveles apropiados de rendimiento para la pérdida de paquetes, latencia y jitter y de esta manera asegurar una buena calidad de la voz.

Disponer de calidad de servicio (QoS) en redes que brindan el servicio de VoIP para aplicaciones como la telefonía por ejemplo, se hace necesario por cuanto la voz es una aplicación interesante e importante para muchos usuarios de redes WIFI de oficinas pequeñas o domésticas por varias razones, entre las cuales podemos indicar las siguientes.

- Dispositivos de capacidades de manejo de voz. La tecnología WIFI ofrece al usuario un amplio abanico de dispositivos para soporte de aplicaciones de voz que incluye teléfonos móviles. El número de teléfonos en modo simple y dual (WIFI y celular) está creciendo rápidamente, ofreciendo a los usuarios, VoIP sin cables.

- Conveniencia. Las aplicaciones de voz sobre WIFI como la telefonía IP, operan dentro de una red asequible y confiable que los usuarios saben cómo administrar.

- Buena calidad de voz. Los Access Points y dispositivos clientes soportan la distribución de buena calidad de voz dentro de una red inalámbrica que es compartida por múltiples dispositivos.

- Ahorro en costos, el uso de voz sobre WIFI amplía la selección de servicios disponibles para los usuarios a través de los proveedores de servicios, y reduce la inversión en adquisición de nuevos terminales fijos.

El ambiente típico de una red para el despliegue de la VoIP sobre redes WIFI incluye los siguientes elementos:

- Un solo Access Point que sirve a múltiples clientes.

- Soporte de al menos cuatro llamadas simultaneas desde cuatro dispositivos conectados al AP.

- Transporte de tráfico de datos y video adicional al tráfico de voz.

- Asignación de prioridades a la voz sobre cualquier otro tipo de tráfico.

- Acceso seguro a través del uso de WPA2 - Personal[8].

---

[7] En la página web oficial de Wi-Fi Alliance se realizó la búsqueda de los dispositivos como teléfonos y tablets que cumplen con la certificación “Wi-Fi Alliance Certified Voice-Personal” http://www.wi-fi.org/product-finder-results?sort_by=default&sort_order=desc&categories=4,5&capabilities=6&certifications=48

[8] Con la enmienda 802.11i, ratificada en 2004 por el Wi-Fi Alliance se publicó la actualización a WPA llamada WPA2 (Wi-Fi Protected Access). El principal cambio es que ya no se usa el algoritmo RC4 para

De la correcta aplicación de la QoS se debería obtener como rendimiento de la red los siguientes valores:

- Pérdida de paquetes inferior al 1% sin pérdidas de paquetes consecutivos.
- Latencia menor a 50ms.
- Máximo jitter menor a 50ms

A partir del año 2009 la Wi-Fi Alliance empezó el desarrollo del programa de certificación de dispositivos "Wi-Fi Voice – Enterprise" que comprende el mejoramiento de la calidad de las llamadas de VoIP pero en ambientes empresariales, donde la carga del tráfico de datos es alta así como la cantidad de usuarios conectados y los Access Points (Wi-fi Alliance, 2012).

Dentro de una red WIFI empresarial se presentan tres modelos de uso de aplicaciones de VoIP:

1. Trabajadores móviles de ubicación múltiple: este tipo de trabajadores por lo general hace uso de teléfonos inteligentes de modo dual (WIFI/ Celular), de tal forma que mientras están conectados a la red inalámbrica de la empresa tienen acceso a todos los servicios de voz y comunicaciones unificas y cuando salen de la cobertura inalámbrica pueden hacer uso de la red celular.

2. Trabajador móvil ubicación única: sus actividades las realizan dentro del mismo sitio, pero no están atados a un escritorio. Y hace uso del dispositivo con capacidades de voz para acceder a la red empresarial para disponer de los recursos TI que le son permitidos.

3. Trabajadores no móviles: ya sea por facilidad de instalación y un poco de ahorro (no necesita cableado) los trabajadores tienen acceso a la red de voz a través de sus PCs / laptops de manera inalámbrica instalando un softphone por lo que permanecerán en un puesto fijo.

En un entorno empresarial, adicional a los elementos del ambiente personal la red debe disponer de las siguientes características:

- Administración del ancho de banda utilizando WMM Admisión Control.
- Transición transparente a través de toda la red WIFI para que la llamada se mantenga mientras el usuario se mueve dentro del área de cobertura de la red WIFII compuesta de varios Puntos de Acceso.
- Ahorro de energía en el Punto de acceso, opcional en el cliente.

encriptación nunca más, en su lugar se usa el algoritmo AES (Advanced Encription Estándar) al cual se agregó un mecanismo de seguridad adicional CCMP (Counter Mode with CBC-MAC Protocol). Este algoritmo es más fuerte que RC4 y requiere un upgrade de hardware. Wi-Fi Alliance llama a la versión de clave compartida WPA2-Personal y como WPA2-Enterprise cuando se utiliza autenticación 802.1x/EAP

Las métricas que determinan la calidad de la voz al igual están determinadas por los siguientes valores:

- Latencia menor al 50ms en un sentido.
- Jitter menor a 50ms
- Pérdida de paquetes menor al 1%
- Pérdida de paquetes consecutivos no más de tres.

Tanto para redes domésticas como de clase empresarial la optimización de una llamada de VoIP se consigue con la asignación de prioridades a determinados tipos de tráfico más sensibles sobre otros que lo son menos, la forma como se prioriza el tráfico en redes WIFI se define con el estándar 802.11e del IEEE o su similar WMM de WIFI Alliance.

7. Telefonía IP

7.1. Fundamentos de telefonía IP

En la actualidad el protocolo predominante en las redes de datos a nivel global es el protocolo IP ubicado en la capa de Internet del modelo TCP/IP o en la capa de red (Capa 3) del modelo OSI, entonces telefonía IP es el poder realizar llamadas de voz utilizando la red de datos, con esto seguimos avanzando hacia la convergencia de las telecomunicaciones y evitamos disponer de una infraestructura distinta para diversos servicios que se pueden desarrollar en un edificio o empresa en particular (Landivar, 2008).

Tabla 4. Ventajas y desventajas de la telefonía IP.

Ventajas	Desventajas
Reducción de costos de llamadas, cuando la matriz de una empresa y sus sucursales están enlazadas.	La calidad de servicio se ve afectado por retardos en la transmisión, jitter, o pérdidas de paquetes
Reducción de ROI, con la optimización de recursos al utilizar la red de datos existente en lugar de emplazar una nueva para telefonía convencional	
Nuevas funcionalidades, como correo de voz al e-mail, integración con correo electrónico, fax hacia o desde correo electrónico, multi-conferencia. También conocido como Comunicaciones Unificadas.	
Evolución continua, hoy en día se puede realizar llamadas de voz y video integrado	Seguridad, la telefonía IP puede ser susceptible a ataques y fraude en las llamadas
Movilidad de usuarios, con funcionalidades como “follow-me” el usuario puede ser alcanzado en su extensión o en su teléfono fijo doméstico o móvil.	

Fuente: (Landivar, 2008)

El que la telefonía IP haga uso de la red de datos implica varias ventajas, como la que se indicó anteriormente, pero también ciertas desventajas para el servicio en sí, una de las principales es que una red de datos es una basada en el mejor esfuerzo (el tráfico que atraviesa la red no tiene prioridades) y una llamada telefónica es sensible a retardos y pérdidas de sus paquetes que en gran medida pueden ser controlados en una red cableada con los equipos de red adecuados pero dentro de una red inalámbrica es un reto bastante grande, en la tabla 4 podemos apreciar las principales ventajas y desventajas de utilizar telefonía IP.

Antes de proseguir con lo relacionado a la telefonía IP es importante tener claro algunos aspectos de su antecesor la telefonía tradicional o analógica. La idea principal con la que nació la telefonía (del latín tele: distancia, y fonos: sonido) es hacer audible la voz a grandes distancias. Una red telefónica tradicional a nivel macro está compuesta por el abonado y su enlace (última milla) a una Oficina Central (OC) y la Oficina Central local, representados en la figura 19; esta OC para poder interconectar usuarios en diferentes localidades se conecta con otras OC. La comunicación entre la OC y el abonado es en banda base, es decir la voz de una persona se pone directamente en el enlace a la OC sin modulación. La OC se encarga de digitalizar la voz a una señal PCM (Pulse Code Modulation) de 64kbps.

7.1.1. Digitalización de la voz, teorema de Nyquist y codificación.

Para que la voz atraviese la red telefónica es necesario que esta sea digitalizada y pueda ser tratada por los equipos de conmutación de la OC. Debemos tomar en cuenta el oído humano puede captar un rango de frecuencias comprendido entre 20Hz y 20 kHz (Landivar, 2008) pero llevar a cabo una conversación telefónica normal requiere un rango de frecuencias entre 400Hz y 4kHz.

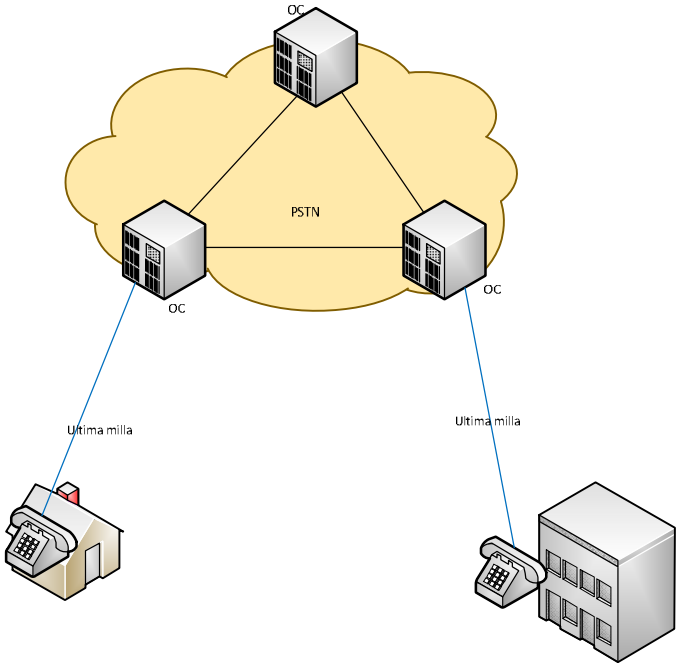


Figura 19. Diagrama de una red telefónica tradicional, (Landivar, 2008).

La digitalización de una señal está compuesta por dos fases:

- El muestreo, que consiste en el proceso de conversión de señales continuas a señales discretas en el tiempo, en este proceso se realizan mediciones de la señal en instantes periódicos de tiempo. La frecuencia con que se realizan estas mediciones se definen con ayuda del Teorema de Nyquist.

- La cuantificación, que consiste en convertir una sucesión de muestras de amplitud continua en una sucesión de valores discretos prestablecidos según el código utilizado.

Con ayuda del teorema de Nyquist, que demuestra que: "la reconstrucción exacta de una señal periódica continua en banda base a partir de sus muestras, es matemáticamente posible si la señal está limitada en banda y la tasa de muestreo es superior al doble de su ancho de banda" (Mérida, 2012), se define la ecuación que determina la frecuencia de muestreo:

$$\mathbf{Fs \geq 2Fmax}$$

Donde, **Fs**: es la frecuencia de muestreo, expresada en Hertz, y **Fmax**: es la frecuencia más alta contenida en una señal analógica expresada también en Hertz.

Esto quiere decir, para el caso de la telefonía, que la tasa de muestreo, se debe realizar al menos al doble de la frecuencia de la voz que el oído humano puede captar y entender de manera adecuada que es 4kHz. Considerando que la frecuencia máxima que queremos muestrear es de 4000Hz, la frecuencia de muestreo será 8000 Hz. (Landivar, 2008).

Las muestras discretas de una señal son valores exactos que aún no han sufrido redondeo o truncamiento sobre una precisión determinada, es decir, aún no han sido cuantificadas.

Durante el proceso de cuantificación se mide el nivel de cada una de las muestras, obtenidas en el proceso de muestreo, y se le atribuye un valor discreto de amplitud, seleccionado por aproximación dentro de un margen de niveles previamente fijado

Para dar valores a los diferentes niveles de muestra de la señal analógica, en el caso de la voz, donde se ha definido que la frecuencia de muestreo es de 8kHz, se utiliza el proceso de codificación con 8bits que permite dar valor a 256 niveles de muestra, lo que nos da como resultado 64kbps que representa la voz digitalizada sin compresión (Códec g.711). (Landivar, 2008)

7.2. Elementos de una red de telefonía IP

La arquitectura de una red de telefonía IP está formada por tres elementos fundamentales de acuerdo a (Nefta, 2013) y (Nóvoa, 2012) que comparte el mismo criterio:

Terminales: son los elementos que originan y establecen una llamada telefónica, estos pueden ser hardware como teléfonos IP y los adaptadores ATAs (Analog Telephony Adapter) que permiten mantener teléfonos analógicos en la red IP; y software como los

Softphones (teléfonos IP basados en software que se instalan en PCs, teléfonos inteligentes o tabletas)

Gatekeepers: Son el centro de una red de Telefonía IP, proveen administración y control centralizados de ancho de banda para todos los dispositivos de una determinada zona. Proporciona el servicio de Control de Admisión de Llamadas o "Call Admision Control" para evitar la sobresuscripción y se encarga además de la traducción de nombres o números a direcciones IP para el enrutamiento de llamadas.

Gateways: Es el elemento encargado de la interconexión de la red de telefonía IP con los elementos de la telefonía tradicional, actuado de manera transparente para el usuario. Puede proveer interfaces que conectan a la Oficina Central de tipo FXO (Foreing eXchange Office) y/o tipo BRI/PRI mediante líneas digitales, e interfaces que conectan a los aparatos telefónicos de suscriptor FXS (Foreing eXchange Subscriber)

En una implementación de telefonía IP también podemos encontrar los siguientes elementos opcionales dependiendo de los servicios adicionales que proveerá la solución:

Unidades de Control Multipunto MCU (Multipoint Control Unit): es un dispositivo necesario para la gestión de conferencias, los participantes envían los datos al MCU y este los reenvía a todos los participantes.

Servidores de aplicaciones: proporcionan servicios a los teléfonos IP basados en XML.

Terminales de video: añaden funcionalidades de video a la voz incorporando elementos para la captura y emisión de video y voz.

7.3. Protocolos y señalización de telefonía IP

Existen un sinnúmero de protocolos involucrados en la transmisión de datos dentro de una red IP, dentro de estos están incluidos protocolos inherentes a la transmisión y señalización de la telefonía IP a los que se les ha clasificado en tres grupos principales (Landivar, 2008):

- **Protocolos de señalización:**
    - Cumplen funciones similares a su homólogos en la telefonía tradicional, es decir a las tareas de establecimiento de sesión entre terminales, control de progreso de llamadas, entre otras.
    - Existen estándares desarrollados por organismos como IETF[9] así como propietarios desarrollados por fabricantes de tecnología.

[9] IETF (Internet Engineering Task Force) o Fuerza de Trabajo de Ingeniería de Internet, es un grupo de personas con una organización informal que contribuye a la ingeniería y evolución de las tecnologías de Internet que tiene como misión "Hacer que el Internet funcione mejor, desde el punto de vista de la ingeniería evitando las cuestiones políticas y comerciales tanto como sea posible". Es la entidad que regula las propuestas y los estándares de Internet también conocidos como RFC. (http://www.ietf.org/tao-translated-es.html)

- Entre los protocolos existentes tenemos:
  - SIP
  - IAX
  - H.323
  - MGCP
  - SCCP

- **Protocolos de transporte de voz:**
  - Son protocolos que transportan la voz propiamente dicha de extremo a extremo.
  - Entre los protocolos tenemos:
    - RTP (Real –Time Transport Protocol)
    - RTCP (RTP Control Protocol)

- **Protocolos base:**
  - Son el conjunto de protocolos de una red de datos.
  - Su funcionamiento es el mismo si el tráfico es voz, video o simplemente datos.
  - En el modelo TCP/IP corresponden a las capas de Acceso al medio, internet y transporte como por ejemplo: Ethernet, PPP, IP, TCP, UDP.

El flujo que sigue un mensaje de voz para ser puesto dentro la red se muestra en la figura 20, es en la capa de aplicación (modelo TCP/IP) donde la voz es muestreada con el códec de voz adecuado y se agrega el encabezado RTP para flujos de tiempo real, en la capa de transporte se utiliza el protocolo UDP para aplicaciones que hacen uso de señalización SIP, otro tipo de aplicaciones como Microsoft Lynk utilizan el protocolo TCP; en la capa de internet se agrega el encabezado del protocolo IP, mientras que en la capa de enlace de datos se puede hacer uso de cualquier tecnología como Ethernet, punto a punto PPP/HDLC o Frame Relay. Un paquete VoIP sobre Ethernet tiene la estructura de la figura 20.

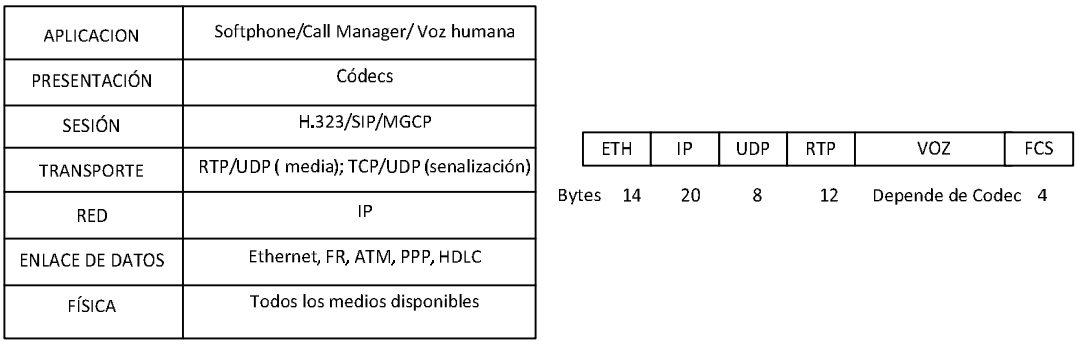


Figura 20. Datagrama de voz sobre IP (Nóvoa, 2012).

7.3.1. Protocolo RTP

El Protocolo de Transporte en Tiempo-Real, fue desarrollado por el grupo de transporte de audio y video del IETF en 1996 y actualizado en 2003 [RFC3550].

RTP opera en la capa de sesión sobre el protocolo UDP, este último no tiene control sobre el orden en que los paquetes son recibidos en el terminal tampoco sobre el tiempo que les toma en llegar, puntos críticos para el desarrollo de una conversación aceptable, UDP se encarga de la multiplexación de conexiones en base a un número de puerto y a la comprobación de cabeceras.

RTP resuelve el inconveniente del desorden en la recepción de paquetes a través de la asignación de números de secuencia que facilitan el re-ordenamiento de los datagramas, y mediante un pequeño buffer que elimina el efecto jitter o retraso en la llegada de los paquetes, la estructura de una datagrama RTP se muestra en la figura 21.

Cuando un dispositivo intenta establecer una sesión, RTP elige un puerto aleatorio entre 16384 y 32726 para cada flujo RTP. Los flujos RTP son simplex, es decir la transmisión de la información es en un solo sentido; una comunicación bidireccional hace uso de dos flujos RTP, uno en cada sentido. Los números de puertos se mantienen durante toda la sesión.

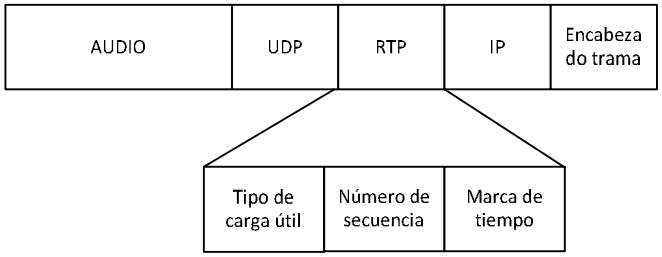


Figura 21. Estructura de un datagrama RTP (Nóvoa, 2012).

7.3.2. Protocolo RTCP

RTCP, desarrollado por el IETF como complemento del protocolo RTP es definido en el RFC3605, proporciona información de control que está asociado con un flujo de datos para una aplicación multimedia (RTP). LA función principal de RTCP es informar acerca de la calidad de servicio proporcionado por RTP con información estadística de numero de paquetes, retardo, pérdida de paquetes, jitter.

Este protocolo proporciona información útil, pero no es crítico para el normal desarrollo de una comunicación, intercambia información cada 5 segundos.

7.3.3. Protocolo UDP

UDP (User Datagram Protocol) es un protocolo liviano de la capa de transporte, definido en el RFC 768 del IETF. Permite el envío de datagramas sin que previamente se haya establecido una conexión (no orientado a conexión), tampoco dispone de información de control de flujo ni de confirmación de entrega o recepción, por lo que el terminal que envía la información no tiene conocimiento si el paquete llego o no a su destino, y el destino no conoce el orden en que los paquetes deben ser presentados, simplemente entrega el paquete UDP a la red y acepta datagramas de entrada; en la figura 22 se muestra la estructura del datagrama UDP.

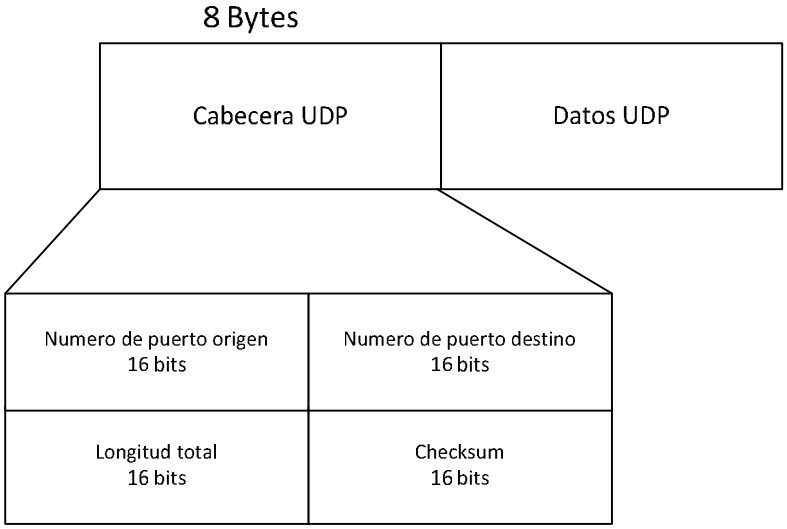


Figura 22. Estructura de un datagrama UDP (Nóvoa, 2012).

Este protocolo es muy útil para aplicaciones en tiempo real como la transmisión de audio y / o video donde la realización de retransmisiones afectarían a la calidad de la comunicación por los retardos que esto implica. Para suplir esta carencia en la capa superior se emplea el protocolo RTP.

7.3.4. Protocolo IP

IP (Internet Protocol) es un protocolo ubicado en la capa de red, definido en el RFC791, provee un servicio de envío de datagramas no fiable o también conocido como "best effort" (mejor esfuerzo) esto quiere decir que buscará la mejor ruta para la entrega de un datagrama pero no garantiza su entrega, no provee ningún mecanismo para determinar si un paquete alcanza o no a su destino (similar a UDP).

7.3.5. Protocolo SIP

SIP (Session Initiation Protocol) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Fue desarrollado inicialmente en el grupo de trabajo IETF MMUSIC (Multiparty Multimedia Session Control) y, a partir de septiembre de 1999, pasó al grupo de trabajo IETF SIP.

SIP especifica los comandos y respuestas necesarios para establecer, modificar y finalizar llamadas, proporcionando servicios de seguridad, proxy y transporte. Es un protocolo de señalización extremo a extremo, considera a cada conexión como un par y se encarga de negociar las capacidades entre ellos (Nóvoa, 2012). Tiene una sintaxis simple, similar a HTTP o SMTP, y posee un sistema de autenticación de pregunta/respuesta. Para agregar capacidades de seguridad utiliza un mecanismo seguro de transporte mediante TLS. Como desventaja se puede mencionar que no tiene un adecuado direccionamiento de información para el funcionamiento con NAT.

Antes de entrar en detalles del principal protocolo se señalización utilizado veremos las características principales de protocolos de señalización también utilizados en las redes de telefonía IP

IAX (Inter Asterisk eXchange) es un protocolo abierto, por lo que se puede descargar y desarrollar libremente pero aún no es un estándar (Nefta, 2013). Es un protocolo de transporte, que utiliza el puerto UDP 4569 tanto para señalización de canal como para RTP, puede empaquetar múltiples sesiones dentro de un flujo de datos, así requiere de menos ancho de banda y permite mayor número de canales entre terminales.

H.323. Es un protocolo estándar creado por el ITU (International Telecomunications Union) para realizar conferencias multimedia en entornos no orientados a conexión. En la actualidad es un conjunto de estándares que definen todos los aspectos de la sincronización de voz, video y datos.

SCCP. Acrónimo de "Skinny Client Control Protocol". Es un protocolo propietario de Cisco. Es el protocolo por defecto para terminales con el servidor Cisco Call Manager PBX que es el similar a Asterisk PBX. El cliente Skinny usa TCP/IP para transmitir y recibir llamadas. Para el audio utiliza RTP, UDP e IP. Los mensajes Skinny son transmitidos sobre TCP y usa el puerto 2000.

7.3.6. Señalización SIP.

El protocolo de inicio de sesión SIP, es un protocolo de la capa de aplicación para la señalización en telefonía IP, fue desarrollado por el IETF con el propósito de ser el estándar para la iniciación, modificación y finalización de las sesiones interactivas entre dos o más usuarios donde intervienen elementos multimedia, fue aceptado como protocolo de señalización de 3GPP, (TUTORIAL TELECOM, 2014).

Al igual de lo que sucede en la telefonía analógica o telefonía RDSI, el protocolo SIP se encarga únicamente de la señalización, no del transporte de voz. El protocolo que en realidad se encarga del transporte de la voz y video es el RTP. SIP puede utilizar el puerto 5060 de TCP o UDP en la capa de transporte, en la mayoría de implementaciones se emplea UDP, que es un protocolo no orientado a la conexión, por lo que la propia aplicación es la encargada verificar que el paquete sea recibido de manera correcta.

SIP es un protocolo punto a punto (peer to peer), lo que quiere decir es que cada elemento que interviene en la sesión puede hacer las veces de cliente o servidor dependiendo de quién inicie la sesión. En la práctica es necesario el uso de los denominados SIP Proxy, que se encargan de registrar y actualizar cuando sea necesario la localización de un terminal SIP en redes con gran cantidad de dispositivos. SIP es un protocolo ligero basado en texto por lo que un solo SIP Proxy puede atender sin mayor dificultad la señalización de miles de llamadas por segundo.

SIP comparte algunos principios de diseño de los protocolos HTTP, empelado en la construcción de páginas web y SMTP muy común en los servidores de correo electrónico. Una llamada SIP se realiza desde (FROM) alguien hasta (TO) alguien, como enviar un correo electrónico, y por otro lado se utilizan códigos de estado como en HTTP.

Un datagrama SIP contiene la siguiente información de encabezado (Nefta, 2013):

- **Via:** Indica el protocolo de transporte usado para el envío e identifica la ruta de la solicitud.
- **From:** Indica la dirección del origen de la petición.
- **To:** Indica la dirección del destinatario de la petición.
- **Call-Id:** Identificador único para cada llamada y contiene la dirección del host. Debe ser igual para todos los mensajes dentro de una transacción.
- **Cseq:** Se inicia con un número aleatorio e identifica de forma secuencial cada petición.
- **Contact:** Contiene una dirección que pueden ser usada para contactar con el usuario.
- **User Agent:** Contiene el cliente agente que realiza la comunicación.

3.3.6.1. Elementos del protocolo SIP

- **Agente de Usuario (UA, User-Agents):** Son los terminales físicos: dispositivos con aspecto de teléfono tradicional pero utilizan los protocolos SIP y RTP para la comunicación, estos pueden ser teléfonos IP, ATAs o softphones. Cuando un UA realiza una petición actúa como cliente, y cuando la recibe actúa como servidor.

- **Servidor de registro (SIP Registrar):** cuando un usuario inicializa su dispositivo (teléfono o softphone) envía una petición con el método REGISTER a un servidor de registro indicando a que ubicación física (depende en donde el usuario está conectado, se relaciona con la dirección IP) debe asociarse la dirección lógica (usuario@sipserver) del usuario. La asociación debe ser renovada trascurrido un determinado tiempo. La dirección lógica de usuario no cambia con respecto a su ubicación física. De acuerdo a la definición del RFC 2396 el valor del parámetro SIP Server de una URI (Uniform Resource Identifier) que identifica al usuario este puede representar un dominio, el nombre del host o la dirección IP del servidor.

- **Servidor proxy y de redirección (SIP Proxy y Redirect):** Un servidor proxy dirige una petición entre un UA cliente a un UA servidor. Un proxy puede actuar de dos maneras:

    - Proxy: Encamina el mensaje al destino

    - Redirector: Genera una respuesta que indica al origen la dirección destino o de otro servidor que lo acerque al destino

Un mismo equipo puede actuar como servidor de registro, proxy y redirección, en la mayoría de los casos, dependiendo del tamaño de la implementación.

3.3.6.2. Mensajes SIP

SIP define la comunicación a través de dos tipos de mensajes: las solicitudes o métodos y las respuestas o códigos de estado (Elastixtech, 2013).

Métodos SIP

SIP originalmente desarrolló seis tipos de mensajes para las diferentes fases de señalización, pero con las revisiones se han creado extensiones a los mensajes, entre las funcionalidades de los mensajes originales tenemos:

- INVITE: Utilizado en la iniciación de un “diálogo de sesión”. Típicamente una llamada telefónica.

- ACK: Utilizado para confirmación de respuestas.

- BYE: Utilizado para la finalización de una sesión previamente establecida.

- CANCEL: Utilizado para cancelar una petición que aún no ha sido atendida.

- OPTIONS: Utilizado por un cliente SIP para consultar a otro cliente SIP sobre su capacidades en cuanto a códecs soportados, extensiones, métodos y otros.

- REGISTER: Utilizado para registrar un cliente SIP en un Servidor SIP Registrar.

Los métodos SIP se caracterizan por la línea inicial del mensaje, llamada Request-line, que contiene el nombre del método, el identificador del destinatario de la petición, y la versión del protocolo SIP. A continuación un ejemplo de método REGISTER.

```
REGISTER sip:sip.linphone.org SIP/2.0
Via: SIP/2.0/UDP 25.52.14.213:5060;branch=z9hG4bK53440
Max-Forwards: 70
To: <sip:ursula74@sip.linphone.org>
From: <sip:ursula74@sip.linphone.org>;tag=796
Call-ID: 1396960671-3440-MEGA@25.52.14.213
CSeq: 3 REGISTER
Contact: <sip:ursula74@25.52.14.213:5060>;expires=3600;q=0.90
Authorization: Digest username="ursula74",realm=...
Content-Length: 0
```

Métodos de extensión SIP

- INFO: Monitoreo de la llamada (RFC2976).

- COMET: Notificación de Precondiciones.

- PRACK: Reconocimiento provisional de las respuestas.

- SUBSCRIBE: Requerir notificación de evento.

- UNSUCRIBE: Cancelar notificación de evento.

- NOTIFY: Mensajería Instantánea.

- MESSAGE: Mensajería Instantánea.

- REFER: Transferencia a otra URL (extensiones).

Mensajes de Respuesta SIP.

Después de la recepción e interpretación del mensaje SIP, el receptor bien sea el proxy o un User-Agent devuelve un mensaje de respuesta o código de estado compuesto por tres dígitos donde el primero identifica a la clase de la respuesta. Es así que tenemos las siguientes clases principales:

1xx – Información provisional, requerimiento en progreso pero no terminado.

2xx - Mensaje de éxito

3xx - Redirección

4xx - Error de Cliente (error en la petición).

5xx - Error del Servidor.

6xx - Fallo global

A diferencia de un método, una respuesta empieza con un status-line que contiene la versión del protocolo SIP, el código de estado y una pequeña descripción, como en el ejemplo siguiente:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 25.52.14.213:5060;branch=z9hG4bK53440;received=78.115.131.19
From: <sip:ursula74@sip.linphone.org>;tag=796
To: <sip:ursula74@sip.linphone.org>;tag=tmKH496Hp2N3j
Call-ID: 1396960671-3440-MEGA@25.52.14.213
CSeq: 3 REGISTER
Contact: <sip:ursula74@78.115.131.19:5060>;expires=3600
        Server: Flexisip/0.7.0 (sofia-sip-nta/2.0)
Content-Length: 0
```

3.3.6.3. Protocolo SDP.

El protocolo SDP (Session Description Protocol) definido en el RFC 2327 describe el contenido multimedia de la sesión, por ejemplo que direcciones IP, puertos, y códec se emplearán durante la comunicación.

Como SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos como SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos HTTP. Un mensaje SDP está codificado en modo texto, y está compuesto por campos que se definen uno en cada línea, los nombres de los campos son abreviados con una sola letra, y están dispuestos en un orden que simplifica el análisis.

SDP no fue diseñado para ser fácilmente extensible pero la única manera de agregar nuevas funcionalidades es definir un nuevo atributo. A continuación en la tabla 5 se indican los principales campos del protocolo SDP.

Tabla 5. Campos del protocolo SDP. (RFC 2327).

Campo	Nombre
V	Versión del protocolo (obligatorio)
o	Identificador (obligatorio)
S	Nombre de sesión (obligatorio)
I	Información de la sesión (obligatorio)
U	URI de la descripción
e	Dirección de correo
p	Número de teléfono
C	Información de conexión
b	Ancho de banda
Z	Tiempo de corrección
K	Clave de encriptación
a	Atributos
T	Tiempo de sesión (Start y stop) (obligatorio)
R	Tiempo de repetición
m	Información del protocolo de transporte(media) (obligatorio)

3.3.6.4. Funciones de SIP.

El protocolo SIP cumple con las siguientes funciones:

- **Resolución de direcciones:**

  Es una de las principales funciones de SIP, y es realizada por agentes o servidores generalmente el proxy. La resolución de direcciones no siempre implica la traslación a IP. En la figura 23 se presenta un ejemplo de la resolución de direcciones.

- **Funciones de Sesión:**

  - Establecimiento.

    A continuación graficamos el proceso de intercambio de PDUs para establecer una llamada (sesión) en dos escenarios (figura 24), en el primero se muestra el proceso entre dos dispositivos SIP directamente o peer-to-peer; en el segundo caso existe un tercer elemento (proxy) que coordina la comunicación entre los dos terminales SIP.

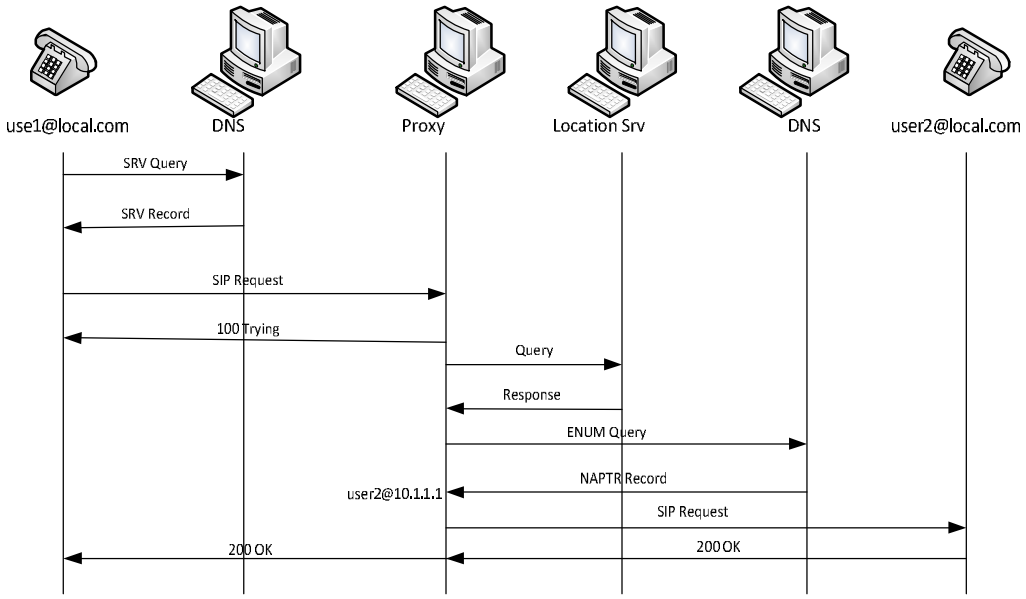


Figura 23. Ejemplo de resolución de direcciones. (Kuthan & Sisalem, 2007)

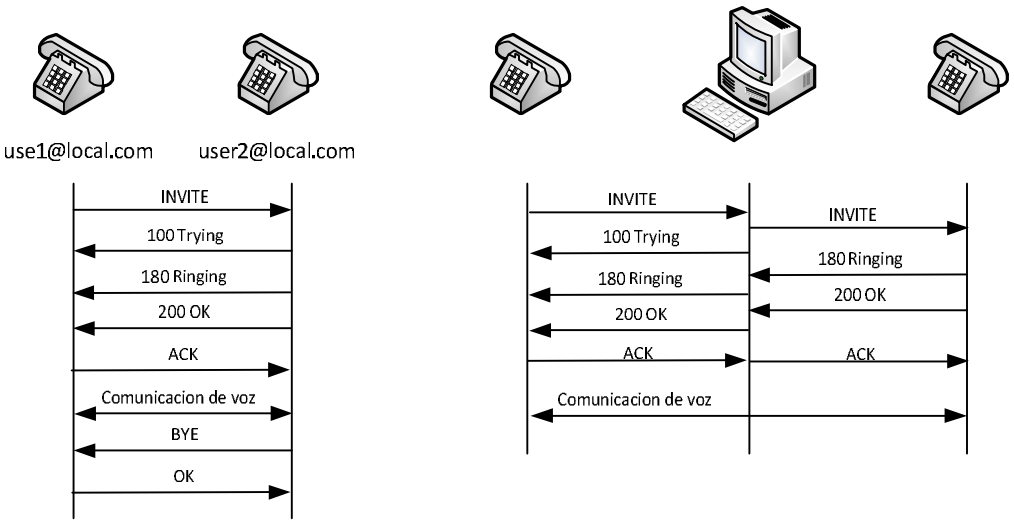


Figura 24. Establecimiento de sesión. (Kuthan & Sisalem, 2007).

- Negociación de medios.

  La negociación es parte del mensaje INVITE, y SIP por sí solo no la soporta por lo que se vale del protocolo SDP el cual viaja dentro del cuerpo del mensaje SIP, se basa en modo ofrecimiento y respuesta, la respuesta se envía dentro del ACK.

- Modificación.

  Solo se puede modificar después del primer establecimiento de sesión. La nueva sesión puede cambiar cualquier característica de la sesión incluyendo el tipo, códec utilizado, dirección IP, y puerto. Mientras se negocia los medios se continúa con la sesión anterior como se aprecia en la figura 25.

- Terminación.

  Una sesión llega a su término cuando cualquiera de los dos Agentes que participan en la sesión decide finalizar la comunicación de voz enviando en mensaje BYE, un ejemplo tenemos en la figura 26.

- Cancelación.

  La sesión se cancela en respuesta al mensaje CANCEL enviado por el agente que origina la llamada, antes que la comunicación de voz se establezca (ver figura 27).

- Control de llamada.

  En la figura 28 se grafica un ejemplo del proceso del control de llamadas, en este caso se describe la transferencia de la llamada con la utilización del mensaje REFER.

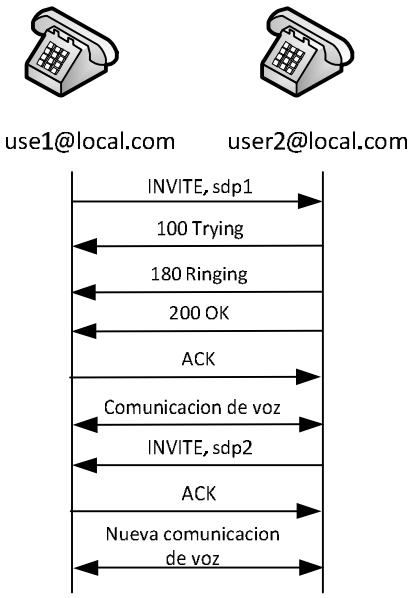


Figura 25. Modificación de la sesión. (Kuthan & Sisalem, 2007).

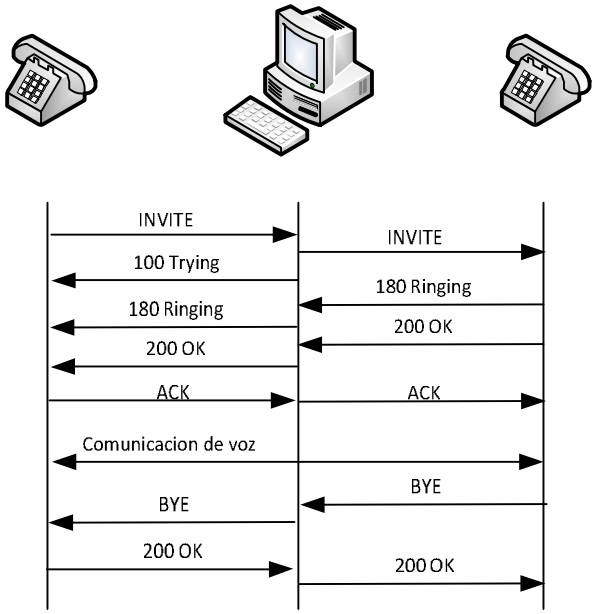


Figura 26. Terminación de la sesión. (Kuthan & Sisalem, 2007)

- **No relacionadas a la sesión:**

Adicional a las funciones básicas que se han descrito anteriormente, SIP permite la implementación de funciones no relacionadas al establecimiento de sesiones, como por ejemplo:

- Movilidad.
- Transporte de mensajes.

- Suscripción de eventos.
- Autenticación.

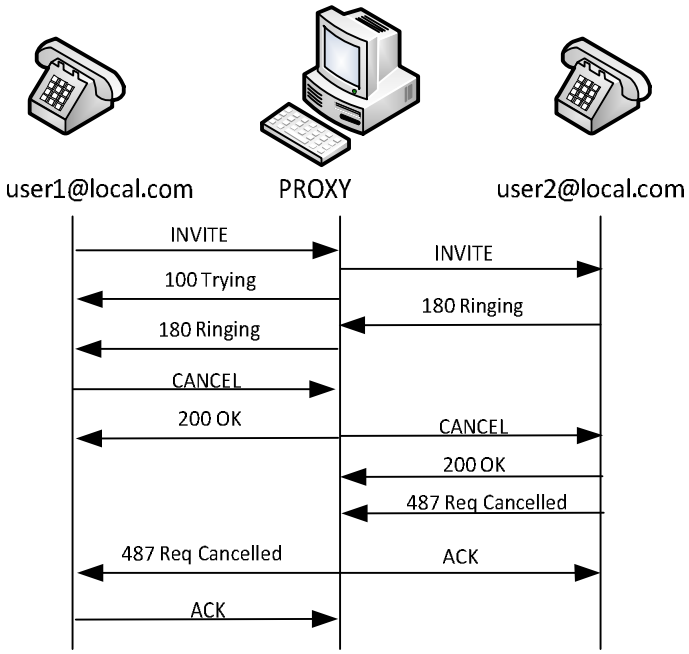


Figura 27. Cancelación de sesión. (Kuthan & Sisalem, 2007).

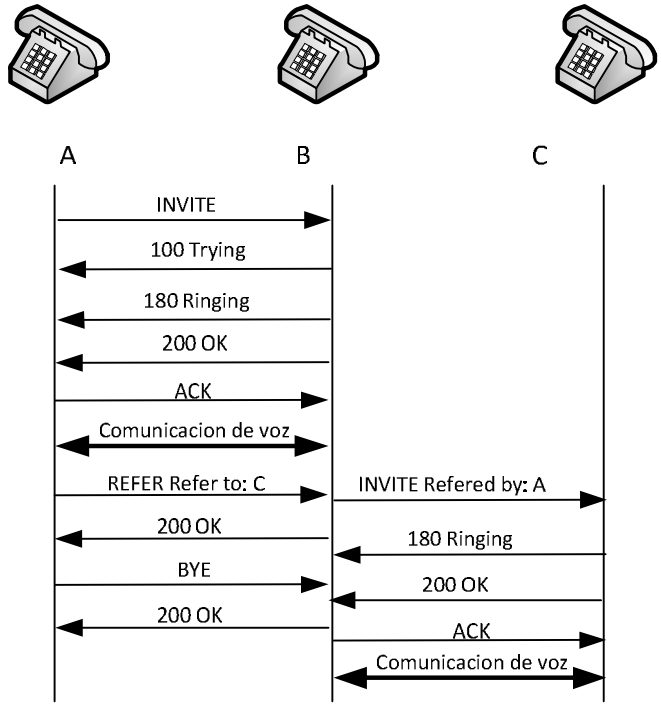


Figura 28. Control de llamada*. (Kuthan & Sisalem, 2007)*

A continuación en la figura 29 disponemos de ejemplo de estructura y contenido que podemos encontrar en un datagrama SIP, para nuestro ejemplo la solicitud a través del mensaje INVITE, y la respuesta con el mensaje OK, de este intercambio de mensajes podemos resaltar la información SDP como la dirección IP de quien realiza la invitación: 100.101.102.103, el códec a utilizar es G.711 (PCMU/8000) y el puerto que utilizará para recibir el audio RTP es 49172.

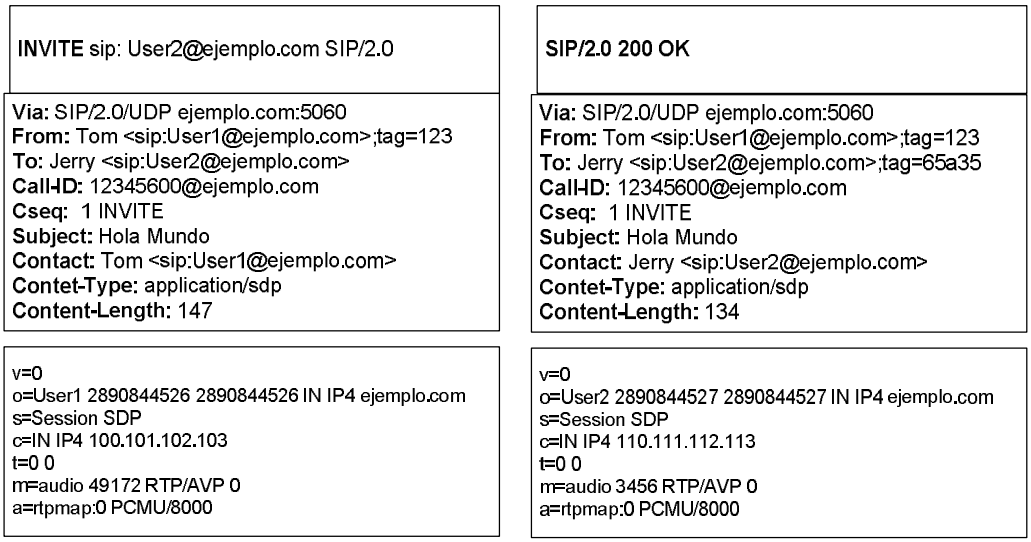


Figura 29. Contenido del paquete INVITE y OK (Elastixtech, 2013).

7.4. Códecs de telefonía IP

La palabra códec proviene de abreviar las palabras CODificación y DECodificación, un códec incluye un conjunto de algoritmos implementados en hardware o software o una combinación de ambos, que permiten **codificar y decodificar** los datos auditivos en el caso de un códec de voz, esto significa reducir la cantidad de bits que ocupa un fichero (compresión) de modo que se utilice menos ancho de banda para su transmisión y la descompresión para reproducirlos o manipularlos en un formato más apropiado.

Los códec más utilizados, en Voz sobre IP, especificados por la ITU-T están G.711, G.729, y G723.1. Para medir la calidad de la voz al emplear códecs, se utiliza una medida subjetiva denominada MOS (Mean Opinion Score) que se emplea una escala de 0 a 5 en base a las opiniones subjetivas de los usuarios (Landivar, 2008). En la tabla 6 se muestra un resumen de los principales códecs de voz con su ancho de banda y calificación en escala MOS.

Tabla 6. Ancho de banda de los principales códec de voz y su calidad.

Códec	Ancho de banda de codificación.	MOS
G.711	64kbps	4.1
ILBC	15.2 kbps	4.1
G.729	13 kbps	3.92
G.726	32kbps	3.85
G.729ª	8 kbps	3.7
G.728	16 kbps	3.61

Fuente: (Landivar, 2008)

Hay que tener presente que el ancho de banda del códec no quiere decir que es el ancho de banda de transmisión por cuanto hay que sumar los encabezados que se agregan en cada capa (del modelo OSI)

G.711

Este códec ha sido especificado como estándar de la ITU-T liberado en 1972. Lo podemos encontrar en dos versiones: u-law utilizado en los Estados Unidos y Japón; y a-law que se utiliza en Europa y el resto del mundo.

Una de las características principales es la alta calidad de la voz debido a que casi no la comprime, hace uso de la codificación PCM de 8 bits con muestreo de 8 kHz y su uso ideal es dentro de las redes LAN.

G.729

Es un estándar de la ITU-T, su uso está permitido bajo la adquisición de una licencia por canal, la ventaja de su utilización radica en su alta compresión por consiguiente bajo consumo de ancho de banda lo que lo hace muy eficaz en redes de baja velocidad como Internet.

G.729 codifica las señales PCM a 8kbps utilizando el algoritmo CS-ACELP que se fundamenta en el modelo CELP que no mantiene una estructura de onda sino que codifica el audio en base a características del oído y de la voz humana, trabajando con ventanas de audio de 10ms que equivale a 80 muestras u 80 bits

G.726

El estándar G.726 de la ITU-T codifica señales PCM, genera entre 16-40 kbit/s y se basa en tecnología ADPCM. El modo más utilizado frecuentemente es 32 kbit/s, ya que es

la mitad de la velocidad del G.711 pero mantiene los datos de voz generados y aumenta la capacidad de utilización de la red en un 100%. ITU estandarizó G.726 por primera vez en 1984.

G.723.1

El estándar G.723.1 fue desarrollado por la ITU, este codifica señales PCM a 6.4 kbit/s o 5.3 kbit/s utilizando ventanas de audio de 30 ms. Para la codificación a 6.4 kbps se utiliza el algoritmo MPC-MLQ, generando 24 bytes por cada ventana de 30 ms. Para la codificación a 5.3 kbps se utiliza ACELP, generando 20 bytes por cada ventana de 30 ms.

7.5 Telefonía IP en redes best-effort

Las redes IP son redes del tipo best-effort y por tanto no ofrecen garantía de Calidad de Servicio, pero las aplicaciones de telefonía necesitan algún tipo de garantía para minimizar el impacto del retardo, jitter, y pérdida de paquetes.

Debemos tener en cuenta que el tráfico generado por la telefonía IP no es muy grande por lo que el impacto de los parámetros como retardo, jitter, pérdida de paquetes, se hace considerable en redes donde el ancho de banda es limitado como en la red de redes, internet, donde el recurso que dispone el proveedor de servicios ISP (Internet Service Provider) se comparte con sus clientes. Como podemos ver en la tabla 7, para el caso de una red LAN o Ethernet, el ancho de banda requerido para una comunicación IP por códec, no supera los 10Mbps de Ethernet, peor aún los 100Mbps de Fastethernet; en este tipo de redes no representaría mayor problema disponer del mecanismo best-effort.

Dentro de la red de Internet, una red completamente best-effort, los enrutadores ofrecen la mejor ruta hacia el destino, que por lo general para cada paquete es diferente, esto hace que los paquetes no lleguen a tiempo, lleguen en desorden, o simplemente no lleguen. El protocolo IP deja la responsabilidad de implementar mecanismo de solución a las capas superiores como TCP, que implementará ventanas deslizantes para no congestionar el enlace, o solicitudes de reenvío de paquetes perdidos; para tráfico en tiempo real como la voz estos mecanismos simplemente son inaplicables, por lo que surge la necesidad de implementar mecanismos de QoS eficientes que provean a la telefonía la misma calidad que la telefonía tradicional.

Tabla 7. Ancho de banda requerido por códec.

Información de códec				Cálculos de ancho de banda			
Velocidad de bits y códec (kbps)	**Ejemplo de tamaño del códec (bytes)**	**Ejm. de intervalo del códec (ms)**	**Mean Opinion Score (MOS)**	**Tamaño de la carga útil de voz (bytes)**	**Tamaño de la carga útil de voz (ms)**	**Paquetes por segundo (PPS)**	**Ancho de banda Ethernet (kbps)**
G.711 (64 kbps)	80 bytes	10 ms	4,1	160 bytes	20 ms	50	87,2 kbps
G.729 (8 kbps)	10 bytes	10 ms	3,92	20 bytes	20 ms	50	31,2 kbps
G.723.1 (6.3 kbps)	24 bytes	30 ms	3,9	24 bytes	30 ms	34	21,9 kbps
G.723.1 (5.3 kbps)	20 bytes	30 ms	3,8	20 bytes	30 ms	34	20,8 kbps
G.726 (32 kbps)	20 bytes	5 ms	3,85	80 bytes	20 ms	50	55,2 kbps
G.726 (24 kbps)	15 bytes	5 ms		60 bytes	20 ms	50	47,2 kbps
G.728 (16 kbps)	10 bytes	5 ms	3,61	60 bytes	30 ms	34	31,5 kbps

Fuente: (Cisco Systems, 2008)

7.6 Telefonía IP en redes inalámbricas.

Las tecnologías de acceso a redes inalámbricas ha evolucionado en gran medida desde el surgimiento de la primera versión del estándar 802.11 que permitía una tasa de datos en el medio de 1Mbps, hasta hoy en día disponer de tecnologías que permiten tasas de datos de hasta 600Mbps con el estándar 802.11n, y mejor aún alcanzar hasta tasas de bits que bordean el Gbps con el estándar 802.11ac, (Cisco Systems, 2013), que aún está en desarrollo. La posibilidad de contar con movilidad y este asombros avance ha hecho que los recursos de TI piensen en la posibilidad de disponer los servicios de una red cableada en el entorno inalámbrico.

La voz sobre IP (VoIP) ha llegado a ser la principal tecnología que los usuarios esperan disponer en una red WLAN. Múltiples factores han impulsado la adopción de aplicaciones de voz sobre redes WIFI, entre ellas:

- Proliferación de dispositivos de doble funcionalidad y capacidades de voz, como los teléfonos inteligentes que incorporan una radio para redes celulares y un radio para redes WIFI.

- Extensión de las capacidades de voz a dispositivos que se consideraban netamente de datos como laptops y PCs de escritorio.

- Incremento del uso de Telefonía IP y comunicaciones unificadas, permitiendo la transición a dispositivos móviles totalmente transparente en cuanto a funcionalidad y características.

- Optimización del ancho de banda en redes con dispositivos "Wi-Fi Certified" 802.11n, permitiendo a un gran número de dispositivos compartir la red.

La telefonía IP sobre redes inalámbricas trae nuevas oportunidades y desafíos, como la necesidad de soporte de VoIP sobre WIFI en la diversidad de dispositivos de cliente, para integrarlos a la red corporativa, que cumplan con los requerimientos de rendimiento y seguridad de clase empresarial. Los empleados necesitan también la flexibilidad de usar la mayoría de sus dispositivos WIFI para aplicaciones de voz sin importar el lugar donde se encuentren, en la oficina, en sus casas o en la calle.

7.7 Requerimientos de Calidad de Servicio

En una red telefónica tradicional la comunicación fluye en tiempo real a diferencia de una red de telefonía IP donde desafortunadamente el modelo TCP/IP no puede garantizar este hecho; la comunicación depende de varios factores como la codificación que se emplea (códecs) equipos de red como switches o router por los que tiene que atravesar la comunicación, dispositivos finales de usuario como teléfonos IP y/o softphones; cada uno de los equipos indicados toma su tiempo en procesar la información que recibe por lo tanto que en una llamada telefónica sobre IP intervengan varios dispositivos resultaría crítico para una comunicación aceptable.

La Calidad de Servicio es el rendimiento de extremo a extremo de los servicios electrónicos tal como lo percibe el usuario final. Los principales parámetros que una red con calidad de servicio debe vigilar que no lleguen a degradar la comunicación son el jitter, el retardo y la pérdida de paquetes a fin de garantizar cierto nivel de calidad.

7.7.1 Jitter

El jitter o fluctuación de retardo no es otra cosa que la variación en los retardos en la llegada de los paquetes entre su origen y el destino, usualmente producido por la congestión de tráfico en algún punto de la red, o diferencia en el tránsito de paquetes cuando estos viajan por diferentes rutas

La solución usual es utilizar un buffer que almacene los paquetes antes de entregárselos al destino, asegurándose que lleguen al destino en orden.

7.7.2 Latencia

Se define como latencia a la suma de los retardos en la red, o para ser más conciso como el retardo entre el envío de un paquete y su recepción. La ITU-T en el estándar G.114 define los límites de los retardos en una comunicación telefónica, estos límites se muestran en la tabla 8; cabe recalcar que para garantizar una comunicación de calidad el retardo deberá estar dentro del primer rango.

Tabla 8. Valores de retardo en una comunicación. (ITU-T G.114)

Rango (ms)	Descripción
0 – 150	Aceptable para las aplicaciones más comunes (llamada de voz por ejemplo)
150 – 400	Aceptable para ciertas aplicaciones, se requiere cuidado para garantizar la satisfacción del usuario
Sobre 400	Inaceptable para la mayoría de aplicaciones

Fuentes de retardo:

- **Retardo por codificación.** Es el tiempo que tarda el DSP en comprimir un bloque de muestras PCM, este retardo varía dependiendo del codificador de voz, de la velocidad y carga del procesador. En la tabla 9 se observa los valores de retardo de codificación para los principales códec de voz.

Tabla 9. Retardos de codificación para códecs de voz.

Codificador	Rate	Tamaño de muestra requerida	Mejor Opción	Peor Opción
ADPCM, G.726	32 Kbps	10 ms	2.5 ms	10 ms
CS-ACELP, G.729	8.0 Kbps	10 ms	2.5 ms	10 ms
MP-MLQ, G.723.1	6.3 Kbps	30 ms	5 ms	20 ms
MP-ACELP, G.723.1	5.3 Kbps	30 ms	5 ms	20 ms

Fuente: (Andrade, 2012)

- **Retardo por paquetización.** Es el retardo para completar un paquete de información con carga útil (conversación codificada y comprimida). Este retardo es función del tamaño de bloque requerido por el codificador de voz y el número de bloques encapsulados en una sola trama. Ejemplos de este tipo de retardo podemos ver en la tabla 10.

Tabla 10. Retardo de paquetización para Códecs de voz.

Codificador	Payload (bytes)	Retardo paquetización	Payload	Retardo paquetización
PCM, G.711	160	20 ms	240	30 ms
ADPCM, G.726	80	20 ms	120	30 ms
CS-ACELP, G.729	40	20 ms	30	30 ms
MP-MLQ, G.723.1	24	24 ms	60	48 ms
MP-ACELP, G.723.1	40	30 ms	60	60 ms

Fuente: (Andrade, 2012)

- **Retardo por conmutación de la red**. Los enlaces en las redes WAN son las causantes de grandes retardos como consecuencia del procesamiento en los nodos para el manejo de enrutamiento.

7.7.3 Pérdida de paquetes

La pérdida de paquetes es medida por el porcentaje de paquetes que no llegan a su destino, lo cual es un gran problema en las redes porque los errores de transmisión pueden dañar los bits y retardar la transmisión. Esta pérdida puede producirse por errores en alguno de los equipos que proveen conectividad a la red o por sobrepasar la capacidad de algún buffer de algún equipo o aplicación en momentos de congestión.

En aplicaciones que no funcionan en tiempo real la pérdida de paquetes sería un problema manejable con el empleo de protocolos de capa 4 (del modelo OSI) como TCP que permite la retransmisión de paquetes perdidos y la confirmación de su llegada al destino mediante acuses de recibo (ACK). Pero en aplicaciones como telefonía donde el trafico funciona en tiempo real la retransmisión de un paquete perdido no tendría sentido, es por esto que se utiliza el protocolo UDP a nivel de transporte. Para reducir el porcentaje de paquetes perdidos una de las opciones es utilizar mecanismos de calidad de servicio que prioricen la información a transmitir de acuerdo a su tipo.

7.8 Retos de una red de VoIP para garantizar la QoS

La internet, red sobre la cual hoy en dia se implementan diversas aplicaciones, cuyo origen data de los anos 1960s con la puesta en marcha de la red ARPANET por parte del Departamento de Defensa de los Estados Unidos fue concebida como una red con servicio "best effort" o mejor esfuerzo mediante la formalización del protocolo TCP/IP por el año 1982.

Este tipo de redes no prestan ninguna garantía a aplicaciones con tráfico sensible a retardo, jitter o pérdida de paquetes por lo que ha surgido la necesidad de disponer de algún tipo de mecanismo que mejore la calidad de una llamada de voz por internet donde existen limitantes de recursos o tecnológicos. Por ejemplo podemos hablar de limitante de recursos en redes WAN donde el recurso ancho de banda es escaso y obtener una mayor cantidad se traduce en costos, en cambio un limitante tecnológico se presenta en redes inalámbricas donde un Access Point funciona en modo half-duplex, en ambos casos como consecuencia vamos a tener que los valores de las métricas sobre las que se determina la calidad de una llamada van a estar por encima de los valores recomendados.

En los últimos años las aplicaciones de VoIP como la telefonía, gracias a las ventajas que presenta han tenido un auge importante dentro de redes de todo tipo de empresa, sin embargo las limitantes antes indicadas, en conjunto con el diseño e implementación deficiente hacen que el rendimiento no sea el adecuado generando resistencia en ciertos gerentes de TI para la adopción completa de soluciones convergentes que podrían fácilmente alinearse a los objetivos de negocio de la empresa.

Dentro de una red VoIP, el reto más importante, para el éxito en el diseño e implementación de la infraestructura va estrechamente ligado con la capacidad de proveer una red con calidad de servicio (QoS) que minimice el impacto de las limitantes tecnológicas o de recursos. El cumplimiento de este reto se consigue con la aplicación adecuada de mecanismos de QoS que garanticen que los valores de los parámetros que definen la calidad del tráfico de voz permanezcan dentro los límites con mínimo impacto para el resto de tráfico.

Las actividades que se deben llevar a cabo para la aplicación QoS:

- Identificación del tráfico sensible, en este caso VoIP.
- Asignación de prioridades adecuadas al tipo de tráfico.
- Uso de mecanismos de colas adecuado.

Cabe indicar que la selección del hardware adecuado que soporte la implementación va a influir de manera directa en el éxito o fracaso de la solución por cuanto no todos los dispositivos tienen el soporte de las funcionalidades requeridas principalmente cuando de entornos inalámbricos hablamos.

8. Calidad de Servicio en Redes Inalámbricas.

8.1. Requerimientos de servicio para aplicaciones de video, voz y datos

En la actualidad se transmite a través de las redes de datos todo tipo de tráfico tales como datos, video y voz teniendo como ventaja principal la formación de una red convergente. La transmisión de video y voz a través de una red IP convencional presenta una serie de retos, debido a las necesidades específicas de estos tipos de tráfico, haciendo necesario que los elementos de red deban poseer ciertas características necesarias para el buen funcionamiento del servicio tanto en redes cableadas, y mucho más en redes WIFI, puesto que en el último caso, el medio es compartido, no solo con interferencias y elementos externos, si no con el resto de los clientes (Cruz & Martinez, 2013).

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 posible. En las redes inalámbricas estos dos parámetros no son tan fácil de optimizar como en las redes cableadas, pues las velocidades de transmisión son menores y siempre existe alguna interferencia externa, o simple colisión entre clientes, lo que provocará alguna pérdida.

El tráfico de video es más exigente. Con respecto a la transmisión de datos, este tipo de tráfico 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 cuando corresponden, o el video no será visionado de forma correcta, apreciándose defectos como sonido deficiente, aceleraciones del vídeo, pausas, entre otros.

En general, a parte de una velocidad de transmisión mínima para poder transmitir en video con fiabilidad, y una falta de pérdida de paquetes, hará falta un cumplimiento de otros parámetros como el jitter, latencia, duplicación y reordenación de paquetes y emisión en ráfagas.

El video, dependiendo de la codificación y la calidad de la imagen, demandará un ancho de banda mínimo, que deberá ser soportado por la red inalámbrica para proporcionar un buen servicio. En caso de que la red no sea capaz de proporcionar esta velocidad, se perderá información al no poder ser enviada por la red, provocando pérdida de paquetes.

La pérdida de paquetes, ya sea por causa de un tráfico excesivo para la red, por interferencias o cualquier otra causa, provocará video de calidad deficiente, mostrándose los típicos cuadros o pixelado, cortes de sonido.

La duplicación y reordenación de paquetes es un fenómeno que sucede en las redes más habitualmente de lo que se cree, y en video es importante, pues si se produce y no se detecta, gracias a la inclusión de algún protocolo junto con los algoritmos pertinentes en los clientes, dará como resultado que se muestre información que no corresponde con el instante y fotograma en curso, con la consecuente degradación en la calidad de la imagen y sonido. Las ráfagas son algo habitual en sistemas de comunicación que adolecen de congestión. (Cruz & Martinez, 2013).

Las necesidades del tráfico de voz, en este caso voz sobre IP (VoIP), 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 dos diferencias con respecto al servicio de video. La primera es que 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.

La segunda 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.

Una vez analizados los parámetros de QoS y los requerimientos de cada uno de los servicios, se revisará brevemente las diferentes tecnologías inalámbricas con respecto a la forma de implementar QoS.

8.1.1. QoS en tecnologías WIMAX

El estándar 802.16, integra QoS en la capa MAC. La capa MAC, es la que coordina la comunicación sobre el medio inalámbrico compartido.

El protocolo MAC 802.16, es un protocolo orientado a conexión. Cuando una estación suscriptora (SS) ingresa a la red, éste crea una o más conexiones por donde sus datos son transmitidos desde y hacia la estación base (BS). Cada conexión es un flujo de MSDU's (unidad de servicio de datos MAC), que son provistos de ciertos parámetros de QoS. Los parámetros de calidad de servicio son definidos por los denominados flujos de servicio (Cruz & Martinez, 2013).

Un flujo de servicio es un envío MAC que provee un transporte unidireccional de paquetes, ya sea para el enlace de subida (uplink) los paquetes transmitidos por la estación suscriptora (SS) o para el enlace de bajada (downlink) los paquetes transmitidos por la estación base (BS). Un flujo de servicio, es caracterizado por la forma como maneja los parámetros como la latencia, jitter y políticas de priorización de tráfico (Cruz & Martinez, 2013).

El flujo en el cual se transmite un paquete, se basa en el contenido del campo de cabecera IP, permitiendo a cada aplicación recibir un flujo de servicio diferente. La estación suscriptora (SS) y la estación base (BS), negociarán los parámetros de QoS. La calidad de servicio en IEEE 802.16, se logra por medio de un mecanismo de programación de servicio en la estación base (BS). Esta programación es diseñada para mejorar la eficiencia de acceso al medio.

Mediante un servicio programado y los parámetros asociados de QoS, la estación base podrá anticiparse a las necesidades del rendimiento, jitter u otro parámetro del tráfico de subida y además proveer de los métodos adecuados de sondeo y peticiones de concesión de ancho de banda en tiempos apropiados. (Cruz & Martinez, 2013).

8.1.2. QoS en redes WIFI

Las redes WIFI, al ser redes inalámbricas de canal compartido entre todos los clientes de una celda, implementan controles de acceso al medio, necesarios para evitar colisiones e interferencias en caso de que más de un usuario transmita al mismo tiempo. Estos mecanismos son el CSMA/CA y el RTS/CTS que se engloban dentro del mecanismo DCF.

Sin embargo este sistema de control de acceso al medio no previene que un cliente pueda monopolizar el medio en mayor medida que el resto, afectando al servicio en la celda e imposibilitando su utilización con algunas aplicaciones sensibles al retardo y el jitter.

Una primera solución a este problema viene dada por un sistema de control que recibe el nombre de PCF (del inglés, Point Coordination Function). Dicho mecanismo solo es funcional en redes de tipo infraestructura, nunca en redes ad-hoc, pues será el punto de acceso el encargado de realizar dicho control. Cuando se activa el PCF, el tiempo que existe entre dos paquetes "beacon" (aquellos que usa el punto de acceso para anunciar su presencia y las características de la red) enviados por el punto de acceso se divide en dos periodos: CFP (Periodo Libre de Contención) y CP (Periodo de Contención) (Cruz & Martinez, 2013).

Durante el periodo CFP el funcionamiento de la red es como se ha explicado hasta el momento a lo largo del documento, mientras que durante el CP, los clientes no emitirán por iniciativa propia, sino que el punto de acceso le enviará un paquete a cada usuario 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 permite evitar que un cliente se apodere del canal, permitiendo a todos la emisión de datos con una frecuencia aceptable.

El sistema antes mencionado no es capaz de diferenciar los tipos de tráfico, solo diferencia a los clientes, y tratará igual tanto a un cliente que deba transmitir video, como al que espere emitir datos o voz. Puesto que cada servicio, cada tipo de tráfico tiene unas necesidades diferentes, es preciso diferenciarlo y aplicarle un tratamiento individual acorde a sus requerimientos.

La enmienda 802.11e, define estaciones de trabajo y puntos de acceso mejorados con QoS, las cuales las define como QSTA y QAP respectivamente. Y se crearon dos principales funciones que definen calidad de servicio en 802.11, las cuales son: EDCF y HCF.

Este protocolo permite clasificar el tráfico en cuatro categorías, dependiendo las necesidades y características del tráfico. Estas categorías ordenadas de la más prioritaria a 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 le sea más prioritario. 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.

Esta norma amplía los sistemas de control existentes hasta el momento, DCF y PCF, con un nuevo esquema denominado HCF (Hybrid Coordination Function) que define dos métodos de acceso al canal para la emisión de datos, priorizando aquellos que sean más sensibles: Enhanced Distributed Channel Access y HCF Controlled Channel Access.

Ambos métodos tienen una base común, siendo el EDCA el más extendido y obligatorio para los sistemas certificados WIFI y que soporten WMM. El método HCCA incorpora un mayor control del tráfico, pero su cumplimiento es opcional, está menos extendido y es soportado por un número muy reducido de sistemas.

8.2. Fundamentos de calidad de servicio.

La calidad de servicio comúnmente abreviado como QoS (Quality of Service) se puede definir como la capacidad de una red para servir a determinada aplicación eficientemente, sin afectar su función o rendimiento (Pham, 2012), es decir proveen un mejor servicio a cierto tráfico seleccionado. Cabe recalcar que dar prioridad a uno o más flujos de datos no hace que los otros flujos sin prioridad se pierdan.

QoS permite proveer mejor servicio a ciertos flujos asignado prioridades dependiendo de los requerimientos del flujo de información. Cuando se utilizan herramientas de control de congestión el objetivo es dar mayor prioridad al flujo creando colas y dando servicio a las colas en diferentes maneras. La herramienta de administración de colas usada para evitar congestión sube la prioridad y descarta los flujos con prioridad más baja antes que los flujos con más alta prioridad. La aplicación de políticas de regulación/supervisión “policing” y formación “shaping” provee prioridad a un flujo limitando el “throughput” de otros. Las herramientas de eficiencia de enlace limitan los flujos grandes para dar preferencia a flujos pequeños.

8.2.1. Objetivos de la aplicación de QoS.

El objetivo principal de QoS es proveer prioridades incluyendo ancho de banda dedicado, control de jitter y latencia, parámetros muy importantes en redes con tráfico en tiempo real como la telefonía; y mejora de pérdidas características.

La utilización de QoS provee los siguientes beneficios:

- Permite a los administradores de red establecer acuerdos de nivel de servicio, LSA (Level Service Agreements) con los usuarios de la red

- Control de los recursos: se dispone de control sobre cualquiera de los recursos, como ancho de banda, equipos, enlaces, entre otros están siendo utilizados.

- Uso más eficiente de los recursos: conocimiento del para qué está siendo utilizada la red y poder dar mejor servicio al tráfico más importante de acuerdo al giro del negocio.

- Servicios a medida: el control y la visibilidad de QoS provee la capacidad que el ISP (Internet Service Provider) pueda ofrecer servicios diferenciados a medida y requerimiento de cada cliente.

- Coexistencia de aplicaciones de misión crítica: asegurar el ancho de banda y retardos mínimos es muy importante en aplicaciones multimedia y de voz pero al mismo tiempo permite servicio justo a otras aplicaciones si interferirse entre sí.

Con QoS, el ancho de banda puede ser utilizado de manera más eficiente a través de redes LAN, WLAN y WAN. QoS provee una red mejorada y confiable al realizar las siguientes acciones:

- Soportar ancho de banda dedicado para usuarios y aplicaciones críticas.

- Control de jitter y retardo (requerimiento para aplicaciones de tiempo real)

- Manejo y minimización de congestión en la red.

- Conformación “shaping” del tráfico de la red para tener un flujo fluido.

- Establecer prioridades al tráfico de la red.

Los requerimientos de QoS de las aplicaciones en función de los parámetros más importantes que definen la calidad del servicio las podemos resumir en la tabla 11, la fiabilidad hace referencia a la sensibilidad de la aplicación a la pérdida de paquetes. Para nuestro caso en particular, la telefonía, podemos concluir que la información que se debe transmitir debe tener una fiabilidad media, es decir se tolera cierto valor de pérdida de paquetes, los valores de retardo y jitter deben ser lo más bajo posibles, y el ancho de banda requerido es bajo (Felici, 2010).

Tabla 11. Requerimientos de calidad de servicio de las aplicaciones

Aplicación	Fiabilidad	Retardo	Jitter	Ancho de banda
Correo electrónico	Alta *	Alto	Alto	Bajo
Transferencia de archivos	Alta *	Alto	Alto	Medio
Acceso web	Alta *	Medio	Alto	Medio
Login remoto	Alta *	Medio	Medio	Bajo
Audio bajo demanda	Media	Alto	Medio	Medio
Video bajo demanda	Media	Alto	Medio	Alto
Telefonía	Media	Bajo	Bajo	Bajo
Video conferencia	Media	Bajo	Bajo	Alto

*Nota: * La fiabilidad de estas aplicaciones se consigue al utilizar el protocolo TCP. Fuente:* (Felici, 2010).

8.2.2 Arquitectura de la Calidad de Servicio

La arquitectura básica introduce tres elementos fundamentales para la implementación de QoS (Cisco Systems, 2012):

- **Clasificación de paquetes:** son técnicas QoS de identificación y marcado de paquetes para garantizar la calidad de extremo a extremo entre los elementos de la red.

- **Control de admisión**: QoS dentro de un elemento de red único como por ejemplo colas (queuing) planificación (scheduling) y herramientas de formación de tráfico.

- **Administración de la configuración**: son funciones de políticas QoS, administración, y contabilidad para administrar y controlar el tráfico extremo a extremo a través de la red.

La arquitectura básica de QoS se puede resumir gráficamente en la figura 30 y estos elementos se describirán en las siguientes páginas.

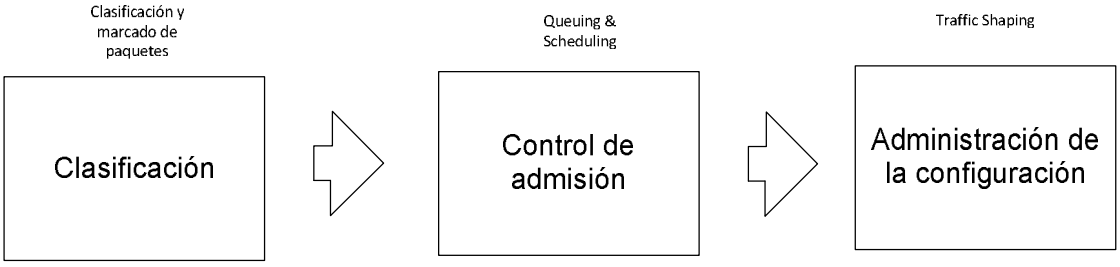


Figura 30. Arquitectura básica de QoS. (Cisco Systems, 2012).

8.3. Identificación y marcado QoS (Clasificación)

La identificación y marcado de paquetes se logra a través de la clasificación y reservación. Para proveer servicio preferencial a un tipo de tráfico, este primero debe ser identificado y luego el paquete puede o no ser marcado, a estas dos actividades se las conoce como clasificación (Cisco Systems, 2012). Cuando un paquete es identificado pero no marcado se dice que es una clasificación por salto "per-hop basis" y la clasificación pertenece solo al equipo que la realiza, cuando el paquete es marcado para su uso a lo largo de la red se fijan los bits prioridad "IP Precedence".

Los métodos comunes para la clasificación incluyen listas de control de acceso ACL (Access Control List), enrutamiento basado en políticas PBR (policy-based routing), tasa de acceso comprometido CAR (Commited Access Rate).

8.3.1. Aplicación de políticas QoS con PBR (policy-based Routing).

La función principal de PBR es enrutar paquetes en base a las políticas que se hayan configurado para este propósito. Por ejemplo podemos identificar el tráfico de cierta aplicación prioritaria y enviar hacia el destino por una ruta de mayor ancho de banda, y para el tráfico restante se enviará por una ruta de menor ancho de banda.

PBR permite clasificar el tráfico en base a listas de control de acceso extendidas, establecer los bits de prioridad del campo "IP Precedence", e incluso enrutar el tráfico de acuerdo a prioridades por vías que permitan una mejor calidad de servicio. Utilizando PBR los mapas de rutas son hechos emparejando los criterios de flujo y estableciendo los bits de prioridad (Cisco Systems, 2012).

8.3.2. CAR: Establecimiento del campo "IP Precdendence".

En cierto modo similar a PBR, la característica de CAR es permitir la clasificación del tráfico en una interface entrante. Esto permite especificar políticas para manejar el tráfico que excede el ancho de banda asignado. CAR mira el tráfico entrante en una interface o un subconjunto de ese tráfico seleccionado por un criterio de lista de control de acceso, lo

compara con el configurado en un “token bucket” y toma una decisión basado en el resultado, por ejemplo descartar o re-escribir la prioridad (IP Precendence). (Cisco Systems, 2012)

CAR es utilizado para supervisar (policing) que el tráfico fluya a una tasa de bit acordada (Commited Access Rate). CAR lo hace con una “cubeta de testigos” (token bucket) que es un contenedor con tokens que representan bytes (1 token = 1 byte). La cubeta está llena de testigos a una tasa de bits configurada por el usuario. En cuanto los paquetes llegan son repartidos, el sistema revisa los token de la cubeta, si hay suficientes de acuerdo al tamaño del paquete, los tokens son removidos y estos paquetes pasan (paquete de acuerdo), si no hay suficientes se descarta (paquete excede).

Cuando se establecen los bits de Ip Precedence en un host o cliente de la red, este establecimiento se puede usar de manera opcional, sin embargo, esto puede ser anulado por la política dentro de la red. “IP Precedence” permite que las clases de servicio sean establecidas utilizando los mecanismos de cola existentes en la red como WFQ o WRED sin cambios en las aplicaciones existentes o complicados requerimientos de la red. (Cisco Systems, 2012).

8.3.3. Prioridad IP (IP Precedence): QoS Diferenciado.

El mecanismo de prioridad IP utiliza los tres bits de prioridad del campo Tipo de Servicio, ToS (Type of service) que es parte del encabezado de un paquete IP V4 (en la figura 31. se puede observar el formato del datagrama IPv4 con el campo ToS), el cual especifica la clase de servicio para cada paquete, el tráfico se puede dividir en hasta 6 clases de servicio con los bits de prioridad, los otros dos están reservados para uso interno de la red. Las tecnologías de colas a través de la red puede entonces utilizar esta señal para proveer el manejo rápido apropiado. (Cisco Systems, 2012).

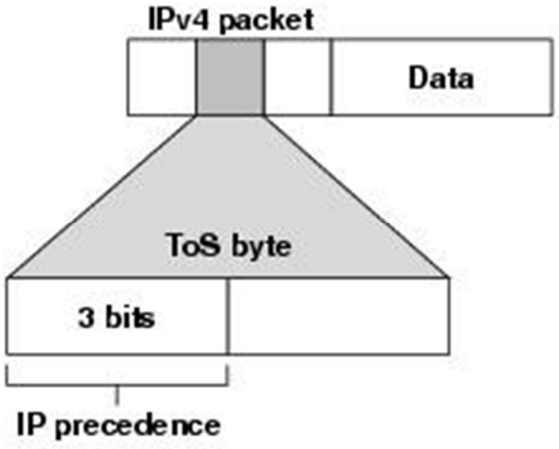


Figura 31. Esquema de campo ToS en datagrama IPv4 (Cisco Systems, 2012).

Los tres bits más significativos del campo ToS constituyen la prioridad IP, el RFC 2457 extiende estos tres bits a seis. Los 6 bits más significativos serán usados para la configuración de la prioridad (conocidos como puntos de código DS) y los restantes 2 menos

significativos están reservados para uso futuro. En la tabla 12 tenemos la descripción de los valores posibles al utilizar “IP Precendence”.

Tabla 12. Valores IP Precendence del campo ToS.

Valor	Descripción
000 (0)	Routine or Best Effort
001 (1)	Priority
010 (2)	Immediate
011 (3)	Flash (mainly used for voice signaling or for video)
100 (4)	Flash Override
101 (5)	Critical (mainly used for voice RTP)
110 (6)	Internet
111 (7)	Network

Fuente: (Cisco Systems, 2012).

8.4. QoS dentro de un elemento de red único.

8.4.1. Administración de congestión.

Debido a la naturaleza de transmisión por ráfagas del tráfico de video, voz o datos, a veces la cantidad de tráfico excede la capacidad del enlace. Una manera que los elementos de la red manejan el desbordamiento o congestión de tráfico es el uso de algoritmos de colas para ordenar el tráfico y entonces determinar algún método para dar prioridad al tráfico sobre el enlace de salida. (Cisco Systems, 2012).

Cada algoritmo de colas fue diseñado para resolver un problema de tráfico en la red específico y tiene un efecto particular en el rendimiento de la red:

- Colas FIFO (First In, First out), primero en entrar, primero en salir.
- Colas de prioridad PQ (Priority Queuing)
- Colas personalizadas CQ (Custom Queuing)

- Cola equitativa ponderada basada en flujo WFQ (Flow-based Weighted Fair Queuing)

- Cola equitativa ponderada basada en clase CBWFQ (Class-based Weighted Fair Queuing)

Los algoritmos de colas tienen efecto cuando existe congestión en la red, si no existe congestión no hay necesidad de poner los paquetes en una cola y los paquetes son puestos directamente en la interface.

4.4.1.1. Colas FIFO

Con las colas FIFO los paquetes son almacenados cuando la red esta congestionada y se reenvían en el mismo orden de llegada cuando la red está menos congestionada. FIFO es el mecanismo de cola por defecto en la mayoría de casos, y presenta algunas deficiencias, la más importante es que no toma decisiones con respecto a la prioridad de paquetes (Cisco Systems, 2012). No brinda protección contra el "mal comportamiento" de ciertas aplicaciones. Cuando la cola está llena provoca que los últimos paquetes sean descartados (tail drop).

4.4.1.2. Priority Queuing (PQ)

PQ asegura que el tráfico importante sea atendido más rápido en cada punto donde es utilizado. Fue diseñado para dar estricta prioridad al tráfico importante. PQ puede dar prioridades de manera flexible de acuerdo al protocolo, interface de entrada, tamaño de paquete, origen y destino, entre otros. En PQ cada paquete es colocado en una de cuatro colas: alta, media, normal y baja según la prioridad asignada. Los paquetes que no son asignados con esta lista de prioridades entran a la cola de tráfico normal. Durante la transmisión, el algoritmo da a las colas de más alta prioridad absoluto trato preferencial sobre las colas de prioridad más baja. Con la figura 32 se ilustra el funcionamiento de PQ. (Cisco Systems, 2012).

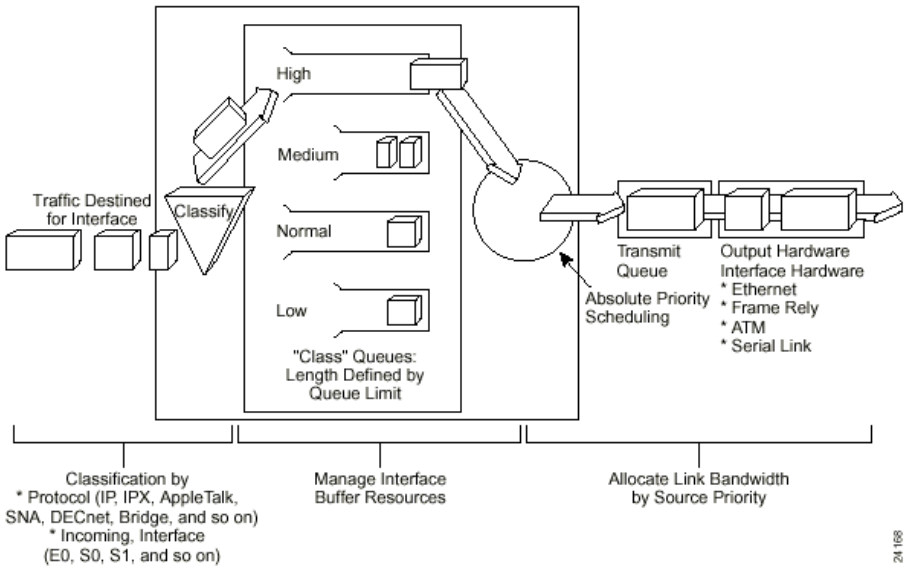


Figura 32. Esquema de funcionamiento "Priority Queuing" (Cisco Systems, 2012)

El inconveniente que presenta este método es que es estático y no se adapta a los requerimientos de la red, además, puede crear inanición, es decir dejar fuera de servicio al tráfico menos prioritario.

4.4.1.3. CUSTOM QUEUING (CQ).

CQ fue designado para permitir a varias aplicaciones compartir la red entre aplicaciones con requerimientos específicos de mínimo ancho de banda y latencia. En este ambiente el ancho de banda debe ser compartido proporcionalmente entre aplicaciones y usuarios. CQ provee un ancho de banda garantizado en un potencial punto de congestión, asegurando al tráfico especificado una porción fija del ancho de banda disponible y dejando el resto de ancho de banda para otro tráfico, (Cisco Systems, 2012), el funcionamiento se ilustra en la figura 33.

Este algoritmo utiliza 17 colas, la cola 0 contiene los mensajes del sistema, y se vacía de acuerdo a la ponderación de la prioridad. El router va sirviendo a las colas desde la 1 hasta la 16 por turnos (round-robin), saca de la cola la cantidad de bytes configurados desde cada cola en cada ciclo. Esto logra que ninguna aplicación obtenga más que la proporción predeterminada de la capacidad total cuando el enlace está siendo usado a su máxima capacidad.

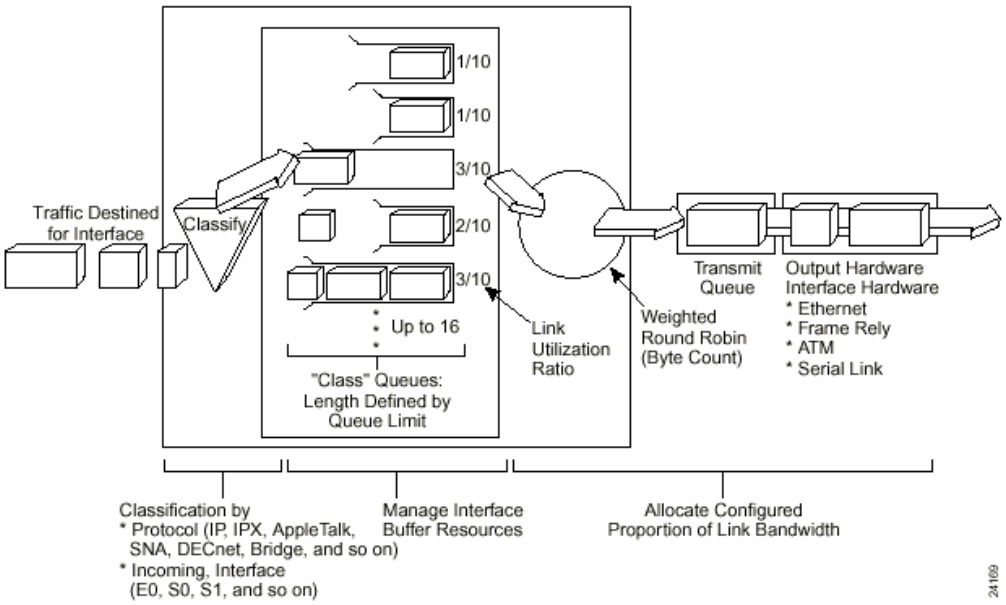


Figura 33. Esquema de funcionamiento "Custom Queuing" (Cisco Systems, 2012).

4.4.1.4. WFQ Basado en flujo.

El algoritmo de colas basado en flujos crea una equidad bit-a-bit, permitiendo que cada cola sea servida de manera equitativa en términos de conteo de bytes. Por ejemplo si la cola 1 tiene paquetes de 100 bytes y la cola 2 tiene paquetes de 50 bytes, el algoritmo WFQ tomará dos paquetes de la cola 2 por cada paquete de la cola 1. Esto hace que el servicio sea equitativo para cada cola. (Cisco Systems, 2012).

WFQ automáticamente se adapta a las condiciones cambiantes del tráfico de la red. Crea flujos basados en un conjunto de características (direcciones de origen y destino, números de socket e identificadores de sesiones) en un paquete. Cada flujo tiene su propia cola para almacenamiento si el enlace experimenta congestión (figura 34).

La porción ponderada de WFQ viene del uso de los bits de prioridad IP para proveer mayor servicio a ciertas colas. Utilizando valores del 0 al 5, WFQ utiliza su algoritmo para determinar cuánto servicio debe proveer a una cola.

WFQ es eficiente en el uso de cualquier ancho de banda disponible para renviar tráfico desde flujos de baja prioridad sin tráfico y desde flujos de alta prioridad si el tráfico está presente. Esta es la diferencia con el esquema estricto de TDM (Time Division Multiplexing) donde el ancho de banda no es usado si no hay tráfico presente par un tipo de tráfico en particular.

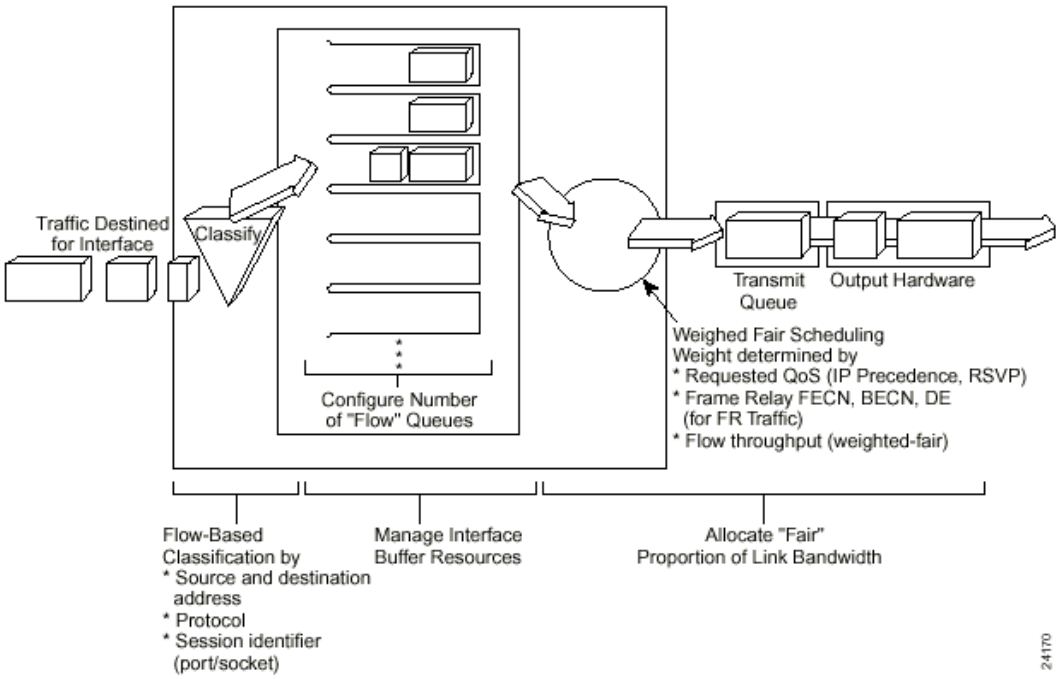


Figura 34. Esquema de funcionamiento WFQ (Cisco Systems, 2012).

4.4.1.5. WFQ BASADO EN CLASES, CBWFQ.

CBWFQ permite al administrador de la red crear clases con ancho de banda mínimo garantizado, en lugar de proveer una cola para cada tráfico individual. Una clase está compuesta de uno o más flujos. Cada clase puede tener garantizado una cantidad mínima de ancho de banda. Un ejemplo en el que se puede aplicar CBWFQ es para prevenir que múltiples flujos de baja prioridad inunden un solo flujo de alta prioridad. El administrador de la red define la clase e indica al enrutador proveer un ancho de banda determinado para la clase. Una clase por defecto es usada para el tráfico restante que utiliza el esquema de WFQ para la asignación del ancho de banda restante. (Cisco Systems, 2012). Su funcionamiento lo podemos resumir en la figura 35.

4.4.1.6. LLQ Colas de Baja latencia

Este tipo de cola surge de la combinación de dos mecanismos de colas básicos PQ y CBWFQ, para crear un mecanismo de cola mucho más versátil, la cola PQ es utilizada para el tráfico en tiempo real. LLQ garantiza a las clases con alta prioridad baja latencia en la propagación de paquetes y ancho de banda. Las clases de alta prioridad también son vigiladas cuando la congestión ocurre para que no excedan de su ancho de banda garantizado. (Pham, 2012). El tráfico de baja prioridad utiliza el mecanismo CBWFQ como se puede ver en la figura 36.

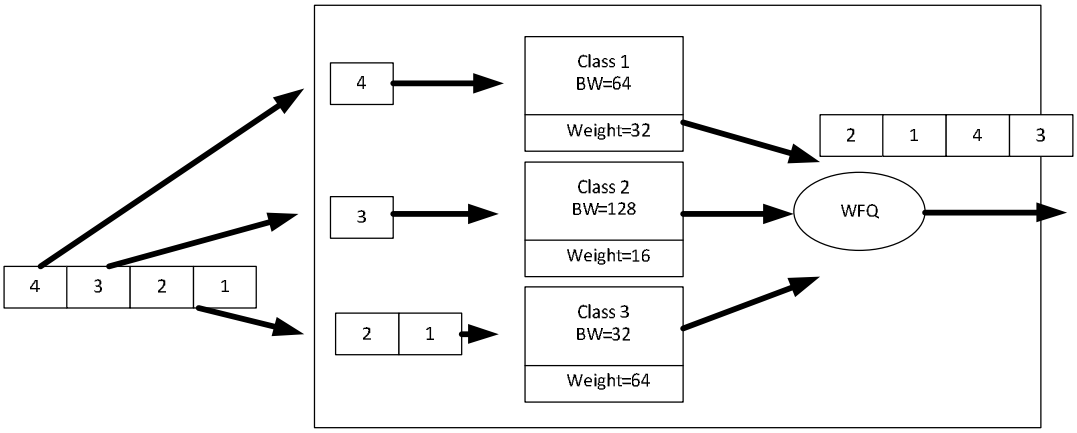


Figura 35. Esquema de funcionamiento CBWFQ (Cisco Systems, 2012).

8.4.2. Administración de colas

Las colas no son de tamaño infinito, por lo que se pueden llenar y desbordar. Cuando la cola está llena ningún paquete adicional puede ingresar y el paquete será descartado, a esto se conoce como descartar la cola, en este caso la palabra cola hace referencia a los últimos paquetes (tail drop). El problema de descartar la cola es que el router no puede prevenir que el paquete sea descartado aun considerando que tiene una alta prioridad. (Cisco Systems, 2012).

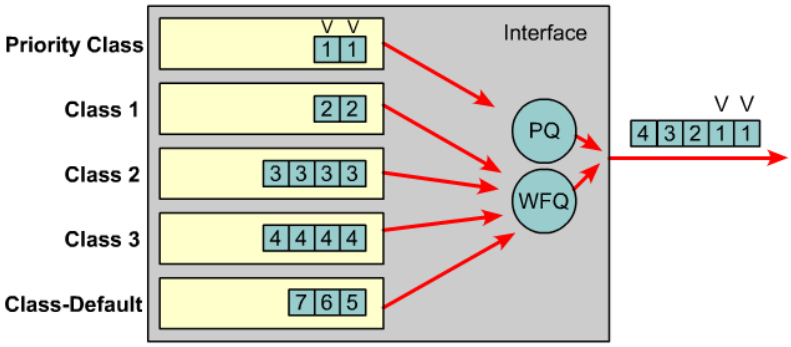


Figura 36. Esquema de funcionamiento LLQ. (Pham, 2012).

Para minimizar los efectos del “tail drop” se utiliza la técnica de detección temprana aleatoria ponderada WRED (Weighted Random Early Detect) que utiliza dos mecanismos:

- Tratar de asegurar que la cola (queue) no se llene, y utilizar una clase de memoria para los paquetes de alta prioridad.

- Utilizar una especie de criterio para descartar los paquetes con baja prioridad antes que descartar los paquetes de alta prioridad.

4.4.2.1. WRED

Los algoritmos de detección temprana aleatoria RED (random early detection) son diseñadas para evitar congestión entre redes antes que estas lleguen a ser un problema. RED trabaja monitoreando la carga del tráfico en puntos de la red, y estocásticamente descarta paquetes si la congestión empieza a incrementar. Como resultado de descartar paquetes el origen detecta el tráfico descartado y hace su transmisión lenta. RED fue diseñando en principio para trabajar con TCP en una red IP. (Cisco Systems, 2012). Su funcionamiento se describe en la figura 37.

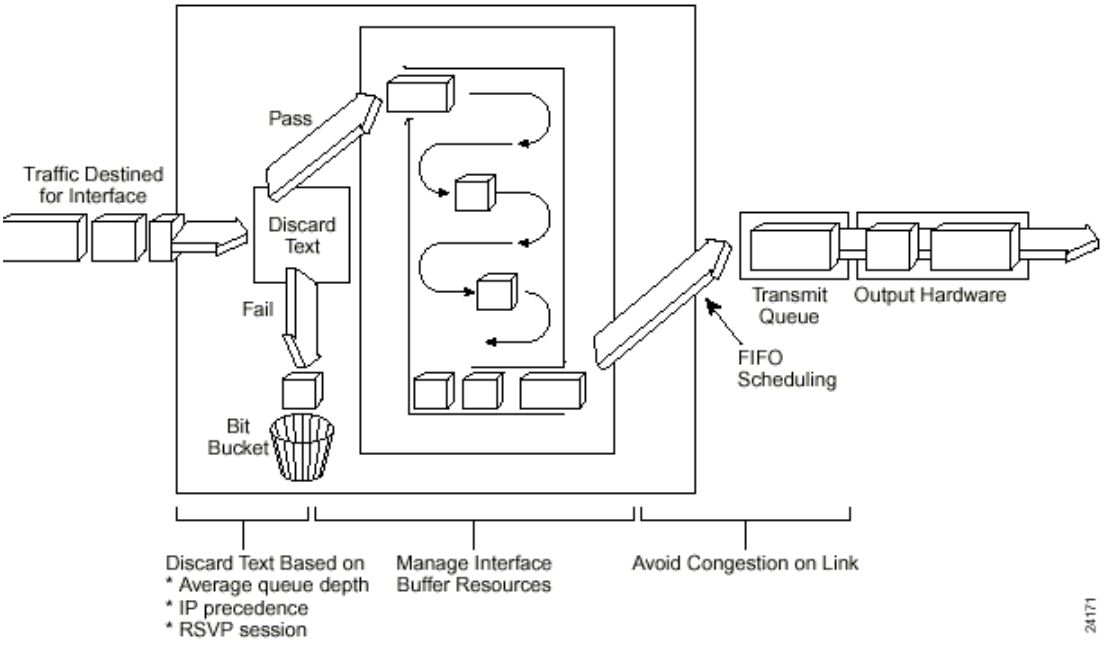


Figura 37. Diagrama de funcionamiento WRED (Cisco Systems, 2012).

WRED combina las características de RED con los bits de prioridad “IP Precedence”. Esto provee un trato preferencial al tráfico de mayor prioridad que puede selectivamente descartar tráfico de baja prioridad cuando la interface empieza a congestionarse y puede proveer características de rendimiento diferenciado para diferentes clases de servicio.

Cada cola tiene la capacidad de almacenar un numero finito de paquetes, que la cola este llena provocará que los últimos paquetes sean descartados (tail drop), sin importar su prioridad; pero si la cola no está llena, el enrutador mira la prioridad del paquete que llega y lo descarta si tienen baja prioridad. Manejando la profundidad de la cola o (número de paquetes de la cola) para descartar paquetes el enrutador asegura que la cola no se llene y que los paquetes no sean descartados. Esto permite al enrutador tomar la decisión de que paquetes serán descartados cuando la cola se vaya llenando. WRED utiliza un umbral mínimo para cada nivel de prioridad IP para determinar cuándo un paquete puede ser descartado.

8.5. Eficiencia de enlace.

Los enlaces de baja velocidad representan un problema para los paquetes pequeños. Para minimizar estos problemas se utilizan dos mecanismos que ayudan a reducir el retardo y jitter en enlaces de baja velocidad, que en conjunto con el mecanismo de encolamiento (queuing) y formación de tráfico (shaping) mejoran la eficiencia y la predicción de la aplicación de niveles de servicio. (Cisco Systems, 2012).

8.5.1. Fragmentación e intercalado de paquetes LFI (Link Fragmentation Interleaving)

Un paquete grande producen un retardo de serialización (retardo producido por poner los bits en el medio de transmisión), si por la capacidad del enlace el retardo es superior al mínimo requerido para una comunicación aceptable, un paquete grande necesita ser fragmentado en paquetes más pequeños, esto como se espera tomará tiempo de procesamiento, sí al mismo tiempo estamos transmitiendo voz, este paquete tendrá mayor retardo que el permitido como para mantener una conversación normal, para que la fragmentación del paquete grande no afecte el retardo al paquete de voz (más pequeño) se va intercalando con los paquetes fragmentados. (Cisco Systems, 2012). Su funcionamiento se puede ver en la figura 38.

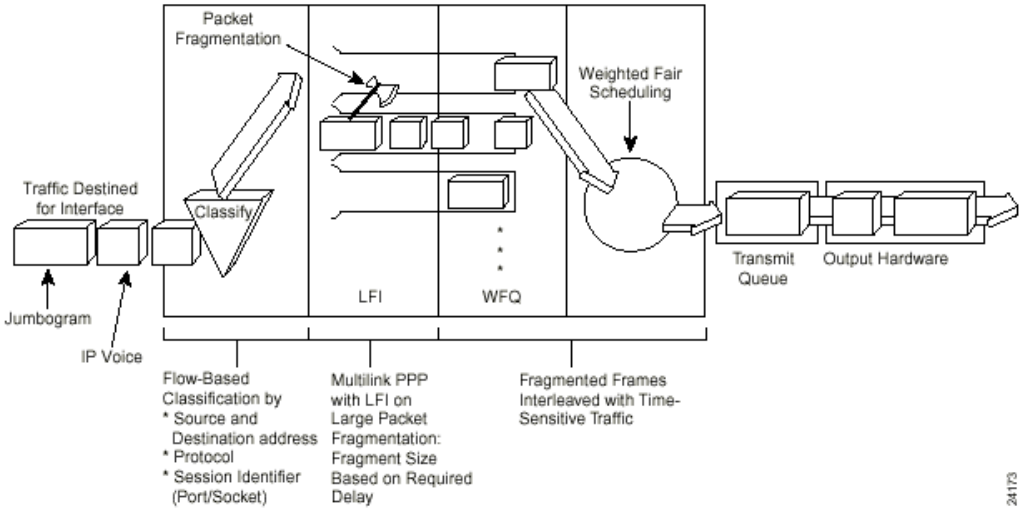


Figura 38. Esquema de funcionamiento LFI (Cisco Systems, 2012)

8.5.2. Compresión de encabezado RTP

Otra manera de hacer un enlace más eficiente es eliminar los bits de cabecera innecesarios por ejemplo utilizar el protocolo RTP para transporte de voz. El protocolo de transporte en tiempo real es un protocolo host a host utilizado para llevar trafico multimedia, incluyendo audio y video en paquetes sobre una red IP. (Cisco Systems, 2012).

Para aplicaciones de audio con carga útil comprimida, el paquete RTP tiene un encabezado de 40 bytes y típicamente de 20 a 150 bytes de carga útil. Con el tamaño combinado de los encabezados IP/UDP y RTP resulta ineficiente para transmitir sobre enlaces de baja velocidad. La compresión de los encabezados RTP/UDP/IP reduce el tamaño del encabezado de 40 bytes a uno de 2 a 5 bytes, reduciendo el retardo significativamente. Este ejemplo se grafica en la figura 39.

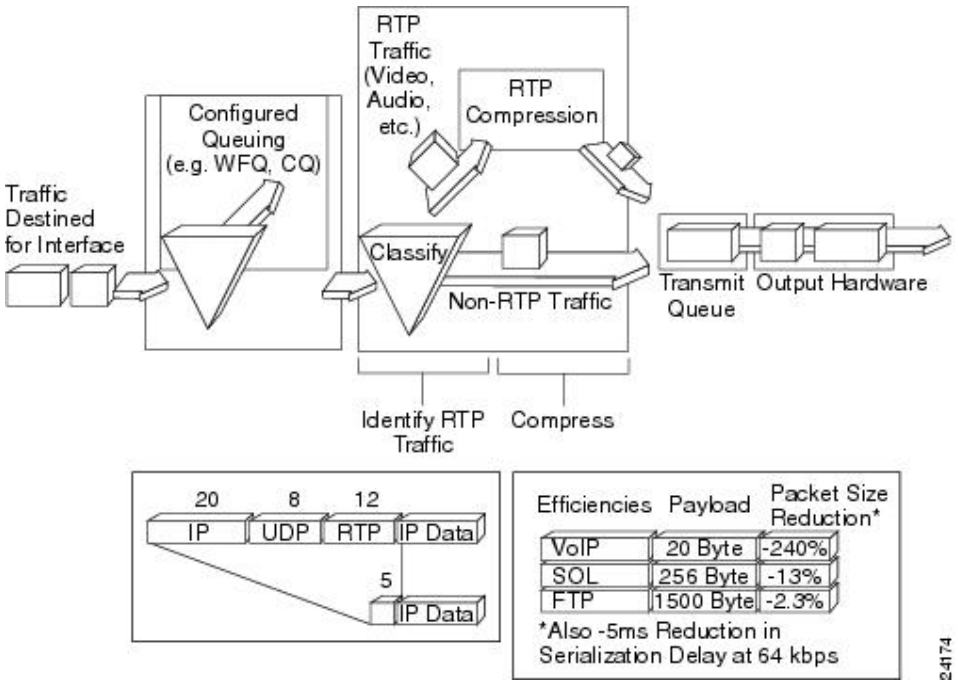


Figura 39. Ejemplo de compresión de encabezado sobre red Ethernet (Cisco Systems, 2012).

8.6. Herramientas de conformación de tráfico (Traffic Shaping & Policing)

La conformación de tráfico o “Shaping” es utilizado para crear flujos de tráfico que limitan el potencial ancho de banda total del flujo, se utiliza para prevenir el problema de desbordamiento. El tráfico por encima del límite establecido es almacenado en un buffer para su posterior transmisión y de esta manera mantener la tasa de datos configurada (Cisco Systems, 2012).

"Policing" es similar al "shaping" con la diferencia de que el tráfico que excede el límite establecido no se almacena en un buffer y normalmente es descartado.

Como herramientas de formación de tráfico tenemos dos herramientas: formador de Tráfico Genérico, GTS (Generic Traffic Shapping) y Formador de Tráfico Frame-Relay FRTS (Frame Relay Traffic Shaping). En cuanto a herramientas de vigilancia o policing tenemos la tasa de acceso confirmado, CAR (Committed Access Rate) que también realiza funciones de clasificación. (Cisco Systems, 2012).

8.6.1. Tasa de acceso acordada, CAR (Committed Access Rate)

CAR es utilizado para limitar el ancho de banda de flujo para favorecer a otro. Con la implementación de CAR un número de acciones puede ser realizado. Estas acciones consisten en transmitir, descartar, ajustar los bits de Prioridad IP "IP Precedence" y ejecutar acciones CAR en cascada. (Cisco Systems, 2012). Esta flexibilidad permite actuar de varias maneras sobre el tráfico, como en los siguientes escenarios:

- El tráfico conforme puede ser clasificado con prioridad IP de 5, y el tráfico excedente puede ser descartado.
- El tráfico conforme puede ser transmitido con la prioridad IP ajustada a 5, mientras que el tráfico en exceso puede ser transmitido, pero con prioridad IP ajustada a 1.
- El tráfico conforme puede ser transmitido, y el tráfico en exceso puede ser reclasificado con un valor de prioridad IP más bajo y entonces enviar al a siguiente sentencia CAR para condiciones adicionales.

8.6.2. GTS (Generic Traffic Shaping)

GTS provee un mecanismo para controlar el flujo de tráfico en una interface particular, reduciendo el flujo de tráfico saliente para evitar congestión restringiendo un tipo de tráfico específico a un bit rate particular mientras la cola se llena de ráfagas del tráfico especificado, de esta manera el tráfico por encima del "rate" establecido va a una cola; a diferencia de CAR donde los paquetes no son encolados. Así, el tráfico que se adhiere a un perfil en particular puede ser formado para conocer los requerimientos descendientes, eliminando cuellos de botella en topologías con data-rates diferentes. (Cisco Systems, 2012).

8.7. Modelos de QoS extremo a extremo.

El nivel de servicio se refiere a la actual capacidad de QoS, esto es la capacidad de una red de distribuir servicios que necesita un tráfico de red específico de extremo a extremo o borde a borde. Los servicios se diferencian por su nivel de QoS estrictamente, el cual describe cuan firmemente el servicio está ligado al ancho de banda especifico, retardo, jitter o pérdidas. (Cisco Systems, 2012).

En una red se pueden ofrecer tres modelos de servicio extremo a extremo, también conocidos como modelos de QoS definidos por el IETF, (Cisco Systems, 2012), en la figura 40 se resumen graficamente:

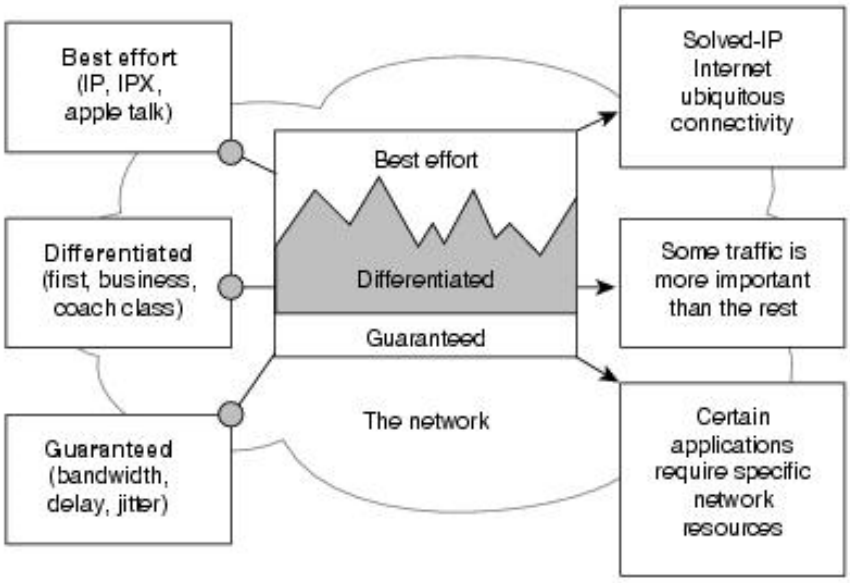


Figura 40. Niveles de QoS extremo a extremo (Cisco Systems, 2012).

- **Servicio best effort**, es básicamente la conexión sin garantías. La mejor caracterización son las colas FIFO (First Input Firts Oputput) que no diferencias entre flujos; donde el paquete sale en el mismo orden en el que llegó. (Cisco Systems, 2012).

- **Servicio diferenciado (Differentiated Service).** Algún tipo de tráfico se trata de mejor manera que el resto en cuanto al manejo más rápido, mayor promedio de ancho de banda, muy bajo promedio de pérdidas. Es provisto por la clasificación del tráfico y utiliza herramientas de QoS como PQ, CQ, WFQ, WRED. Lo que hace el modelo es identificar los paquetes a través del campo de cabecera DSCP (Diffserv Code Point) y según el valor de este campo se aplican los servicios al paquete. En este modelo es el administrador de la red quien configura en cada equipo las condiciones que deben cumplir los paquetes para disponer del servicio respectivo. (Cisco Systems, 2012).

- **Servicio garantizado o integrado (Integrated Service).** Provee una absoluta garantía de los recursos para cierto tipo de tráfico. Para garantizar el servicio se utilizan herramientas QoS como RSVP o CBWFQ. Este modelo identifica los servicios por flujos y aplica los servicios para cada uno de los flujos. La red reserva recursos para cada uno de los flujos, independiente de que el flujo esté transmitiendo o no, la red tiene reservados esos recursos. El modelo de servicios integrados utiliza el protocolo RSPV (RFC 1633) para identificar los flujos e informar a la red que necesita reservar recursos. (Cisco Systems, 2012).

Cada uno de estos niveles puede ser apropiado para ciertas aplicaciones, dependiendo de la aplicación o problema que se desee resolver.

8.8. Parámetros de QoS

Tres son los parámetros que se deben considerar para que la comunicación sea considerada de calidad para aplicaciones en tiempo real, en este caso la telefonía IP; el exceder los límites de cualquiera de estos parámetros acarrea consecuencias que simplemente se traducen en la degradación de la comunicación. Estos parámetros se vieron con mayor grado de detalle en el apartado 3.7 Requerimientos de calidad de servicio.

Latencia.

También conocida como retardo, técnicamente se define "como el tiempo que tarda un paquete en llegar desde la fuente hasta el destino" (VoIP Foro, 2012) y está presente en todo tipo de red de comunicaciones.

De acuerdo a la recomendación ITU-T G.114, el valor de retardo recomendable para que una conversación de voz sea fundamentalmente transparente, debe ser menor a 150 ms. Y dentro de este tiempo está incluido el tiempo de procesamiento de codificación y decodificación de la voz. (Cisco Systems, 2008). El retardo depende de los equipos por los que se debe atravesar y para que no llegue a afectar la comunicación en redes congestionadas se pueden utilizar técnicas como reservación de ancho de banda y priorización de paquetes con el campo ToS del datagrama IP para indicar que se trata de tráfico en tiempo real.

Jitter.

La definición técnica del jitter dice que "es la variación en el tiempo en la llegada de los paquetes, causadas por congestión de la red, perdida de sincronización, o por las diferentes rutas que sigue el paquete para llegar al destino" (VoIP foro, 2012), y a diferencia de la latencia el jitter es un efecto de las redes de datos no orientadas a conexión que se basan en la conmutación de paquetes como internet.

EL valor recomendado del jitter debería ser inferior a 100 ms, (VOIP-info.org, 2011), de este modo puede ser compensado de mejor manera, con la utilización del buffer de jitter, que no es otra cosa que una cola que recibe los paquetes y los reenvía con un pequeño retardo controlado, para que sea menos perceptible por el usuario.

Pérdida de paquetes.

La pérdida de paquetes es medido por el porcentaje de paquetes que no llegan a su destino, las comunicaciones en tiempo real hacen uso del protocolo UDP en la capa de transporte, que es un protocolo no orientado a conexión, donde a diferencia del protocolo TCP, si un paquete se pierde no se vuelve a reenviar (VoIP foro, 2012).

La pérdida de paquetes máxima admitida para que una comunicación no se degrade debe ser inferior al 1%, (VOIP-info.org, 2011), aunque este parámetro también es relativo al códec utilizado, puesto que cuanto mayor es la compresión del códec utilizado más notorio es el efecto de la pérdida. Por consiguiente una pérdida de 1% degrada más una comunicación que utiliza G729 en lugar de G711.

Como medida para minimizar la deficiencia en los parámetros antes indicados tenemos las herramientas de QoS.

8.9. Tecnologías para la aplicación de calidad de servicio en redes inalámbricas

8.9.1. Modelos de calidad de servicio en redes inalámbricas

En el tema anterior se conocieron los modelos de calidad de servicio aplicable a una red de datos, de allí conocimos que tenemos el modelo de servicios integrados y el modelo de servicios diferenciados. Dada la premura de contar con QoS en la redes inalámbricas el WI-FI Alliance introdujo (en 2003) la especificación WMM (Wireless Multi Media) alineada con el estándar IEEE 802.11e un poco antes de que este último sea publicado oficialmente como estándar (Smith & Group, 2008). WMM por ende IEEE 802.11e, se basa en la arquitectura DiffServ del IETF, la cual ha sido bien ajustada para proveer QoS en tecnologías de medio compartido como lo es WIFI, habilitando de manera efectiva la priorización de tráfico sin imponer gran cantidad de encabezado en las tramas. Los paquetes individuales son marcados con encabezados IETF DSCP o etiquetas IEEE 802.1d

WMM se basa en el mecanismo de acceso EDCA (Enhanced Distributed Channel Acces) definido en la enmienda 802.11e para proveer QoS a la comunicación. 802.11e incluye también características adicionales que se pueden agregar a WMM como módulos adicionales, entre estas funcionalidades están el acceso programado, establecimiento de enlace directo (DLS), bloqueo de acuse de recibo (ACK) y ahorro de energía (Jerome, 2013).

Una de las primeras funcionalidades en adoptarse es la de acceso programado, que permite a las aplicaciones reservar los recursos de la red en base a sus características de tráfico mediante el envío de una solicitud de parte de la estación al AP. Este soporta acceso planificado y parametrizado, corresponde al Acceso Controlado al Canal HCF, HCCA, (HCF Controlled Channel Access) del 802.11e. Gracias a que el impacto del retardo de backoff es muy bajo, el acceso programado puede reducir en promedio la latencia de la red al utilizar un mecanismo de control de programación centralizado.

8.9.2. Calidad de servicio para redes inalámbricas con el protocolo IEEE 802.11e

El estándar que ha definido el WIFI Alliance para la aplicación de calidad de servicio en redes inalámbricas de área local es el WMM (Wireless Multi Media) que se basa en la enmienda 802.11e del IEEE. 802.11e se implementa en la sub capa de Control de Acceso al Medio MAC de la capa de enlace de datos. En la figura 41 se presenta la estructura de la capa de enlace de datos del estándar 802.11 con la relación entre cada uno de los elementos que lo constituyen.

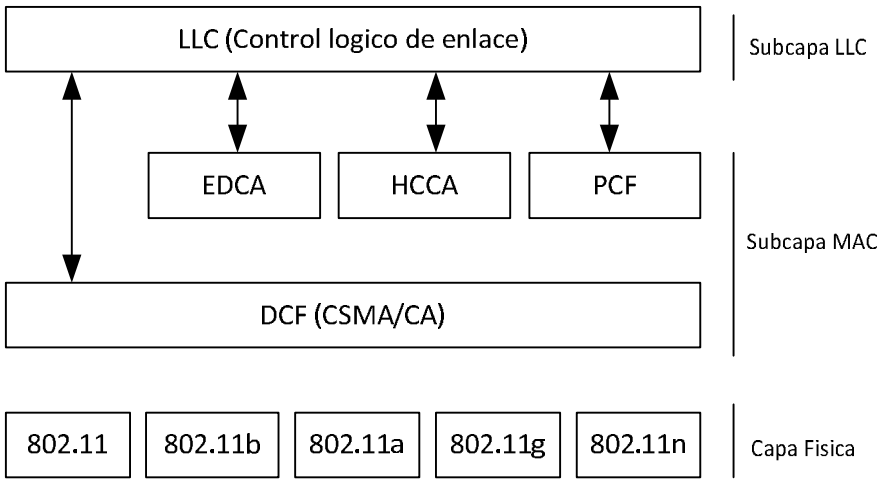


Figura 41. Capa de enlace de datos 802.11 (Carroll, 2008).

802.11e surge por las limitaciones en cuanto a calidad de servicio QoS del estándar 802.11 pese a la existencia de dos mecanismos de control de acceso al medio como son DCF y PCF, como limitaciones de cada uno de estos mecanismos de acuerdo a (Yang M.-H. , 2006) tenemos:

- **DCF (Función de Coordinación Distribuida)**
  - Solo soporta servicios best-effort.
  - No provee garantías en cuanto a ancho de banda, retardo de paquetes y jitter.
  - Presenta degradación del throughput cuando la carga de la red se vuelve pesada.
- **PCF (Función de Coordinación Puntual)**
  - Esquema de consultas centralizado ineficiente.
  - Retardos de la trama BEACON impredecibles debido a la cooperación incompatible entre los modos de contención y libre de contención.
  - El tiempo de transmisión de una estación consultada es difícil de controlar.

802.11e define cuatro categorías de acceso (AC, Access Category) o clases de tráfico de acuerdo a la prioridad con que deben ser transmitidos:

- Background, tráfico no importante.
- Best effort, tráfico de datos normal.
- Voice, tráfico de voz en tiempo real como la telefonía.
- Video, tráfico de video en tiempo real como la videoconferencia.

802.11 soporta 8 valores para prioridades de usuario (UP, User Priority) idénticas a las prioridades de 802.1D, se debe tener en cuenta que un UP pertenece a un AC, cada AC puede contener más de un UP y el tráfico del UP más alto será transmitido primero en un AC.

8.9.3. Distribution Coordination Function (DCF)

DCF es el protocolo básico de la subcapa MAC 802.11, su funcionamiento como se detalló en el capítulo 2, se basa en escuchar el medio y si este está libre transmite, con el esquema CSMA (Acceso Múltiple con Detección de portadora), como una transmisión inalámbrica está compuesta por numerosos dispositivos varios de ellos pueden transmitir al mismo tiempo provocando lo que se conoce como colisión, (Robles, 2008), DCF maneja las colisiones antes de que éstas se produzcan evitándolas con el empleo del mecanismo CA (Collision Avoidance) que utiliza un temporizador de backoff que mejora el rendimiento del sistema a diferencia de tener que detectar la colisión. DCF también implementa el mecanismo RTS/CTS para evitar el problema de nodo oculto que se presenta en redes con más de dos estaciones. Una de las ventajas de utilizar RTS/CTS es que al transmitir varias tramas el AP puede confirmar su recepción con solo un mensaje ACK, a diferencia de no utilizar este mecanismo donde por cada trama recibida tenemos un ACK como respuesta.

En cuanto a la calidad de servicio, el protocolo DCF, considera a todas las estaciones y el tráfico que estas generan, iguales, sin distinción alguna, considerándose un sistema de mejor esfuerzo (best-effort) donde todos los dispositivos tiene la misma probabilidad de acceder medio. En vista de que no hay forma de priorizar un tipo de tráfico de otro, se puede decir que es un protocolo sin calidad de Servicio.

8.9.4 Point Coordination Function (PCF)

Para soportar aplicaciones de tiempo limitado el estándar define la Función de Punto de Coordinación PCF (Point Coordination Function) para permitir que las estaciones tengan acceso prioritario al medio inalámbrico, coordinado por una estación llamada Punto Coordinador (PC, Point Coordinator). PCF tiene más alta prioridad que DCF, porque puede iniciar la transmisión después de un periodo más corto que DIFS, este espacio de tiempo se conoce como PIFS (PCF Interframe Space). Con PCF un periodo sin contención (CFP, Contention Free Period) y un periodo de contención CP, (Contention Period) alternan en el tiempo, donde un CFP y CP adyacente forman una super-trama “superframe”. Durante el CFP, el mecanismo PCF se utiliza para acceder al medio, mientras que DCF, es utilizado durante CP. Es obligatorio que una super-trama incluya un CP de longitud mínima que permita al menos una MSDU (MAC Service Data Unit) ser transmitida durante DCF. (Robles, 2008).

Una super-trama inicia con una trama indicadora “beacon frame” sin importar si PCF está activo o no. La “beacon frame” es una trama de administración que mantiene la sincronización de los temporizadores locales en las estaciones y distribuye parámetros relacionados al protocolo. El punto coordinador PC, que está colocado en el AP genera las tramas “beacon” a intervalos regulares, de este modo todas las estaciones saben cuándo llegara el próximo “beacon frame”; a este tiempo se lo llama tiempo de transición de indicador objetivo (TBTT, Target Beacon Transition Time) y se anuncia en cada “beacon frame”. La trama de “beacon” es requerida en DCF puro, aun si hay tráfico en contienda.

No hay contención entre estaciones, en su lugar, las estaciones son consultadas o sondeadas. El PC sondea a la estación preguntando por tramas pendientes. Debido a que el PC tiene datos pendientes para esta estación utiliza una trama combinada de datos y consulta, donde lleva a cuestas la trama CF-Poll en la trama de datos.

Al ser sondeada la estación durante la trama de datos, esta sabe del éxito de la transmisión. Si el PC no recibe respuesta de la estación consultada después de esperar PIFS, este consulta a la siguiente estación o termina el periodo CFP de esta forma durante el CFP no ocurre inactividad más allá de un periodo PIFS; El PC continúa sondeado a otras estaciones hasta que el periodo CFP expira, y esto se da a conocer con la trama de control CF-End.

El uso de PCF también presenta problemas, que afectan a la calidad de servicio de la red, como por ejemplo, retardos de “beacon” impredecibles y tiempos de duración de la transmisión desconocido en las estaciones consultadas, (Robles, 2008) .

8.9.5. Enhanced Distributed Channel Access (EDCA)

EDCF es en efecto DCF con 4 categorías de acceso AC (Access Category) de acuerdo al tipo de tráfico, que están relacionadas con 8 prioridades de usuario UP (User Prority) definidas en el esquema de clasificación IEEE 802.1p (Parte de la especificación 802.1d). En la tabla 13 (Cisco Systems, 2010) se muestra la relación entre categorías de acceso prioridades UP.

- Tráfico de segundo plano (Background): AC-BK
- Tráfico de mejor esfuerzo (sin prioridades): AC_BE
- Tráfico de video: AC_VI
- Tráfico de voz: AC_VO

Cada AC tiene una cola de transmisión diferente y cada cola tiene una espacio inter-tramas diferente, AIFS (Arbitrary Interframe Space) el cual está definido por los parámetros mínimo y máximo de la ventana de contención CW (Contention Window) propios de cada AC empleados en la asignación del valor aleatorio para ejecutar el algoritmo de backoff. El valor mínimo de AIFS indica la mayor prioridad del AC, esto quiere decir que cuando el valor de AIFS es mínimo el AC tiene mayor probabilidad de acceder al medio.

Tabla 13. Clasificación de categorías de acceso con relación a clasificación 802.1D,

Prioridad	Prioridad de usuario UP (802.1D)	Designación 802.1D	Categoría de Acceso (AC)	Designación WMM
Más baja.	1	BK	AC_BK	Background
	2	-	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Excellent Effort
	4	CL	AC_VI	Controlled Load
	5	VI	AC_VI	Video
Más alta.	6	VO	AC_VO	Voice
	7	NC	AC_VO	Network Control

Fuente: (Cisco Systems, 2010)

El valor mínimo de AIFS utilizado en EDCA es igual al valor de DIFS usado en DCF, sin embargo la ventana de contención para EDCA es decidido por el HQ (Hybrid Controller) / QAP (Access Point QoS) y esto hace significativamente más pequeños que el de DCF, ver tabla 14.

Tabla 14. Ventana de contención EDCA, para QSTA AIFS = DIFS, para QAP < DIFS.

AC	CW_{MIN}	CW_{MAX}	AIFS QSTA	AIFS QAP
AC_BK	CW_{min}	CW_{max}	7	7
AC_BE	CW_{min}	CW_{max}	3	3
AC_VI	$[(CW_{min} + 1)/2] -1$	CW_{min}	2	1
AC_VO	$[(CW_{min} + 1)/4] -1$	$[(CW_{min} + 1)/2] -1$	2	1

Fuente: (Cisco Systems, 2010).

Para clarificar lo expuesto, en la figura 42 se muestra el principio detrás de EDCF donde los valores correspondientes al espaciado intertramas (IFS) y Cwmin y Cwmax son aplicados de acuerdo a la clasificación del tráfico. Los diferentes tipos de tráfico pueden esperar diferentes IFS antes de empezar con el conteo de su backoff aleatorio, y el valor de CW utilizado para generar el backoff aleatorio también depende de la clasificación del tráfico. Por ejemplo el Cwmin [3] para voz es 2^3-1 mientras que el Cwmin [5] para tráfico común es 2^5-1.

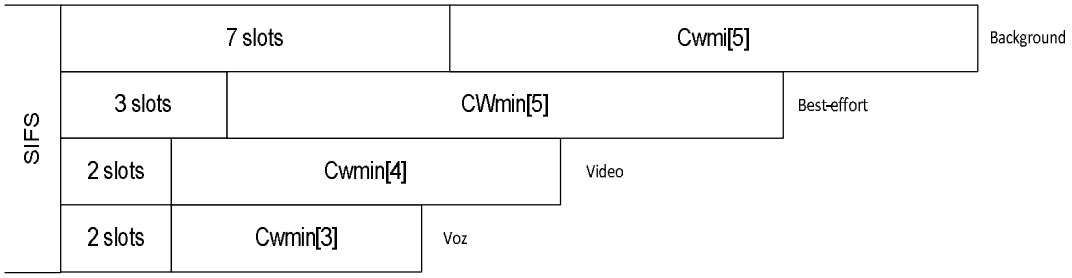


Figura 42. Diagrama de tiempo de las Categorías de Acceso (AC) (Cisco Systems, 2010).

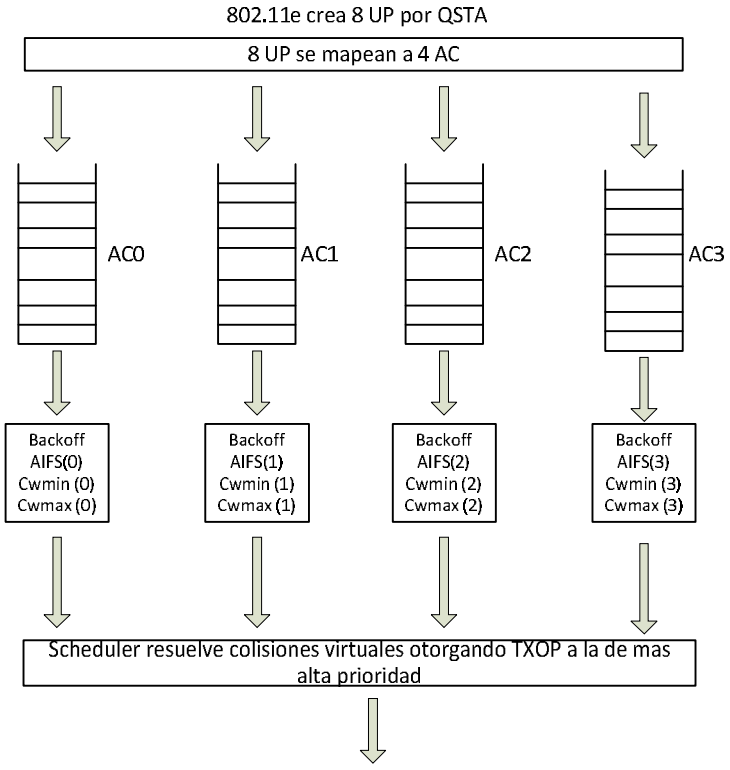


Figura 43. Esquema de funcionamiento AC en EDCA (Cisco Systems, 2010).

Cada una de estas AC se comporta como una estación virtual dentro de la estación física, si los temporizadores de dos o más AC llegan a cero al mismo tiempo, el planificador "scheduler" dentro de la estación trata el evento como una colisión virtual sin afectar al medio, en la figura 43 podemos ver el esquema de funcionamiento. La oportunidad de transmitir TXOP (Transmit Opportunity) se da a la AC (de las que colisionaron) con la más alta prioridad, mientras que los otros continúan con el proceso de backoff como si hubiese existido una colisión en el medio, con un nuevo valor de backoff; pero el tamaño de CW no se dobla.

El periodo de tiempo que un QSTA puede mantener el acceso al canal es EDCA-TXOP, implementado usando el temporizador de ocupación del medio. Durante el tiempo de TXOP la estación mantiene el control sin interrupciones del medio, y puede transmitir múltiples tramas (incluido el ACK) pertenecientes a la misma AC. El EDCA-TXOP para cada AC es definido en el HC/QAP y anunciada a través de los "beacons"y "probe responses". La ausencia de la respuesta esperada para una trama transmitida da como resultado la pérdida del EDCA-TXOP por lo tanto un nuevo proceso de backoff se genera.

El proceso EDCA se puede resumir en la figura 44 y los pasos que esto implica se describen a continuación:

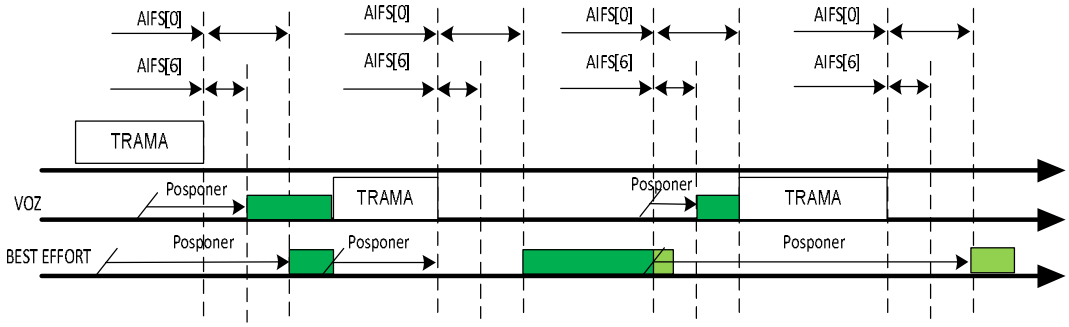


Figura 44. Proceso de funcionamiento EDCA (Cisco Systems, 2010).

1. Mientras una estación X está transmitiendo su trama, otras tres estaciones determinan que también deben enviar una trama. Estas estaciones aplazan la transmisión porque una trama ya se está trasmitiendo y cada estación genera su valor de backoff aleatorio.

2. Debido a que la estación de voz tiene la clasificación de tráfico para voz, su espacio arbitrado inter-tramas (AIFS) de 2 y usa un valor inicial de CWmin igual a 3, por lo tanto, debe posponer el conteo regresivo del valor aleatorio de backoff por 2 ranuras de tiempo y un corto valor aleatorio de backoff.

3. "Best – effort" tiene un AIFS de 3 y un valor aleatorio de backoff más grande porque su CWmin es de 5.

4. La voz tiene el valor aleatorio de backoff más corto y empieza a transmitir primero. Cuando la voz se empieza a transmitir, las otras estaciones esperan.

5. Después que la voz ha terminado su transmisión, todas las estaciones esperan su AIFS y empiezan a disminuir nuevamente el contador de backoff.

6. Cuando best-effort termina su contador de backoff empieza a transmitir. Todas las otras estaciones quedan en espera. Esto puede suceder a pesar der que podría haber una estación de voz a la espera de transmitir. Esto demuestra que el tráfico best-effort no se interrumpe por el tráfico de voz, gracias a que el proceso de decremento de backoff finalmente lleva al valor de backoff de mejor esfuerzo a tamaños similares a los de alta prioridad.

7. El proceso continúa a medida que el resto del tráfico entra al sistema.

8.9.6. HCF Controlled Channel Access (HCCA)

El Acceso Controlado al Canal de la función de Coordinación Hibrida, HCCA, es una extensión del mecanismo de "polling" de PCF. Al igual que en PCF, HCF divide la super-trama en dos periodos, el periodo libre de contienda CFP que se inicia con cada "beacon", y el periodo de contienda PC (ver figura 45). Durante el periodo de contienda el acceso se lleva a cabo utilizando el mecanismo EDCA, aunque el HC puede iniciar el acceso HCF en cualquier instante. (Simsek & Wolter, 2006).

Básicamente HCCA es un planificador en tiempo real asíncrono, para los casos donde existen restricciones específicas para el retardo y perdidas, la estación informa al punto de acceso que debe ser incluido en el planificador HCCA, para ello las estaciones proveen, dentro de una trama de administración llamada TSPEC (Traffic Especification), información detallada acerca del flujo de tráfico. La trama TSPEC incluye información como el tamaño nominal MSDU, tasa de datos promedio, intervalo de suspensión, retardo, asignación de ancho de banda excedente e intervalo máximo de servicio.

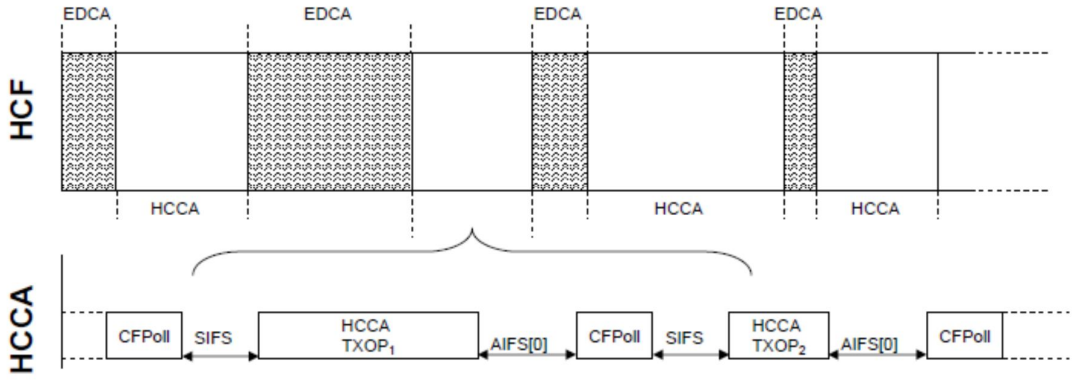


Figura 45. Esquema de funcionamiento HCCA (Simsek & Wolter, 2006).

En la figura 46 podemos apreciar cómo se intercala el periodo de contienda con EDCA y el periodo libre de contienda HCCA para la función HCF. Durante el periodo CFP, el HC (típicamente reside en el AP) emite una trama QoS CF-Poll a una estación en particular, para darle una oportunidad de transmitir TXOP especificando el tiempo de inicio y la duración máxima; para diferenciar la TXOP en HCCA de EDCA lo llamaremos HCCA-TXOP. Ninguna estación intenta acceder al medio durante este tiempo, la estación que recibió el CF-Poll asume el HCCA-TXOP y transmite cualquier dato que disponga. El periodo CFP termina después del tiempo anunciado por la trama "beacon" o en su defecto por la trama CF-End.

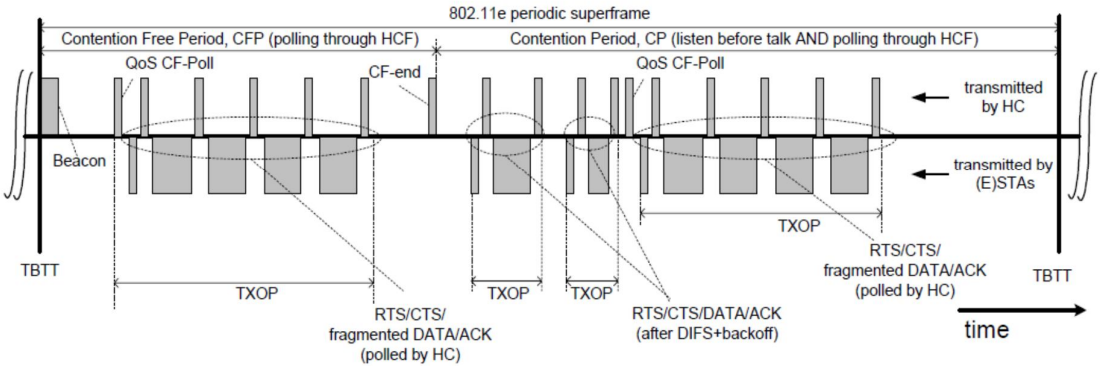


Figura 46. Ejemplo de super-trama 802.11e (Simsek & Wolter, 2006).

Si a una estación se ha dado un CF-Poll, se espera que empiece a responder con datos dentro de un periodo SIFS (Short Inter-Frame Space). Si esto no sucede el HC puede adueñarse del medio luego de un periodo PIFS, y asignar un CF-Poll a otra estación.

HCF permite a una estación base o punto de acceso iniciar una transmisión en base a CF-Polls dentro de un periodo CP, si así lo desea.

9. Implementación de Prototipo

9.1. Definición del problema

Una empresa se crea con el firme propósito de generar rentabilidad económica, para lo cual debe hacer uso de varios recursos, los mismos deben estar en alineados con los objetivos de negocio de la empresa, entre los recursos tenemos:

- Recursos materiales.
- Recursos humanos.
- Recursos financieros.
- Recursos técnicos.

Dentro de los recursos técnicos podemos encontrar a las Tecnologías de Información y Comunicación TICs, que muchas veces se ve relegada de un desarrollo pleno al interior de una empresa y que así pueda servir como pilar para el óptimo desempeño de las actividades sean estas comerciales o productivas.

En el ámbito empresarial, con relación a las TICs, hoy en día nos encontramos que por lo general las instituciones disponen de redes separas para los servicios tecnológicos como son una red de datos, una red para telefonía, una red para el circuito de CCTV, cada una independiente de la otra, situación que complican la administración eficiente de este entorno.

El avance de las redes de comunicación nos han llevado a la convergencia de los sistemas de tal manera que podamos integrar por ejemplo la red de datos, telefónica y de CCTV, en una sola infraestructura, que si bien nos permite simplificar la gestión, exige también el uso de equipamiento adecuado, para que la convergencia se adapte de manera eficaz a los objetivos de la empresa y no se convierta en un dolor de cabeza.

Las redes actuales, en su mayoría disponen de acceso inalámbrico para los empleados y colaboradores como también para usuarios invitados, permitiendo que puedan acceder a recursos a los que estén autorizados desde cualquier dispositivo y desde cualquier lugar que esté dentro del área de cobertura del entorno inalámbrico.

En una empresa dedicada al ámbito comercial es común que sus actividades se desarrollen con el soporte de los servicios de telefonía como para compras, ventas, contactar clientes, entre otras, integrando en una misma infraestructura de comunicaciones convergente al sistema de telefonía IP, es decir que la comunicación de voz es llevada por la misma red de datos.

El problema que se plantea resolver es la posibilidad de hacer uso del sistema telefónico a través de la red inalámbrica accediendo a través de teléfonos inteligentes, con el objetivo de permitir el desplazamiento a los empleados y colaboradores dentro de las instalaciones de la empresa mientras realizan una llamada telefónica con una calidad muy cercana a una comunicación vía cable.

Con la implementación de la solución al problema planteado también podremos de manera subjetiva incrementar la productividad de los trabajadores que se basan en el uso del servicio telefónico, inclusive se podría reducir el costo de propiedad (TCO) de la infraestructura de telecomunicaciones.

En este caso en particular tenemos el siguiente desafío, una red empresarial con 12 empleados en oficina, distribuidos de acuerdo a la tabla 15, los empleados están dedicados a funciones de compras, ventas, y servicio al cliente.

La necesidad de plantear este proyecto surge a raíz de que el personal de ventas debe coordinar con el personal de bodega el stock de productos, inclusive el mismo personal de ventas debe desplazarse a hasta bodega, y en el lugar se requiere el desplazamiento por los estantes. Labores que es muy común realizar con el cliente en la línea telefónica para ofrecer una atención más oportuna.

Tabla 15. Distribución de usuarios y equipos.

ITEM	CANTIDAD
USUARIOS ESCRITORIO	6
USUARIOS LAPTOP	6
TELÉFONOS IP FIJOS	7

Nota: (Autor: José Chauca)

9.2. Enfoque del ciclo de vida de los procesos.

A la hora de llevar a cabo la implementación de un proyecto de tecnologías, y éste no es la excepción, es necesario disponer de una guía que nos lleve al éxito del proyecto. Esto se puede conseguir con un enfoque en el “Ciclo de Vida de los Servicios”; basado en la metodología de Cisco el ciclo de vida define un conjunto mínimo de actividades necesarias de acuerdo a la tecnología y complejidad de la red para ayudar al éxito en el desarrollo y operación de la solución (Cisco Systems, 2010).

El la figura 47 se ilustra la metodología general del ciclo de vida de los servicios. Este ciclo de vida se basa en proveer una metodología para la planificación, diseño, implementación, operación y optimización del rendimiento de las soluciones de tecnológicas. Esto crea un marco de referencia para la definición de servicios independiente de quien realiza las actividades. A continuación describiremos brevemente lo que implica cada fase.

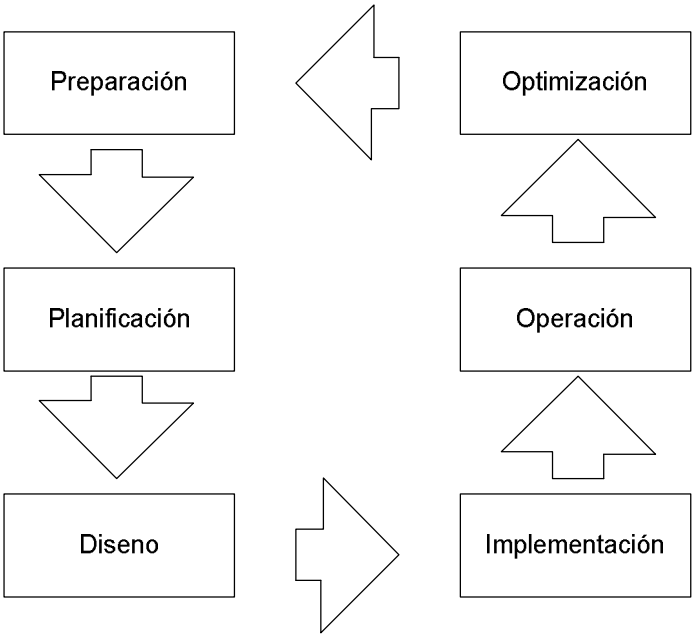


Figura 47. Metodología del ciclo de vida de los servicios (Cisco Systems, 2010).

Fase de preparación.

En esta fase la compañía determina la solución que puede ayudar a satisfacer las necesidades del negocio que además sea financieramente viable, y se anticipe a poder suplir las necesidades futuras. En esta fase se realizan las siguientes actividades:

- Evaluación y documentación de los requerimientos de negocio para usuarios finales del servicio de telefonía IP sobre la red WLAN por ejemplo.
- Análisis técnico de los requerimientos.
- Desarrollo conceptual de la solución a alto nivel

Fase de planificación.

El éxito en el desarrollo de la solución depende de una precisa evaluación de la red de la empresa con todo lo relacionado a soportar la solución propuesta para determinar si la implementación de la solución requerirá mejorar la infraestructura o será capaz de albergar la nueva implementación sin mayor impacto en los servicios que ya están funcionando.

Fase de diseño.

Desarrollar un diseño detallado es esencial para reducir el riesgo, retardos y el costo total del desarrollo de la solución. El diseño alineado con los objetivos del negocio y los requerimientos técnicos puede mejor el rendimiento de la red mientras soporta alta disponibilidad, confiabilidad, seguridad y escalabilidad.

Fase de implementación.

En la fase de implementación, una compañía trabaja para integrar los dispositivos y nuevas funcionalidades en concordancia con el diseño sin comprometer la disponibilidad de la red ni su rendimiento. Después de identificar y resolver los problemas potenciales, la compañía puede mejorar el retorno de la inversión con una migración eficiente e implementación exitosa. Debemos tener en cuenta que una red es esencial en una organización exitosa, y esta debe repartir servicios vitales sin interrupción.

Fase de operación.

La operación de la red representa una porción considerable del presupuesto de TI, por esto es importante estar en la capacidad de reducir los gastos de operación mientras continuamente se mejora el rendimiento. En esta fase, una compañía monitorea proactivamente la "salud y signos vitales" de la red para mejorar la calidad, reducir perturbaciones, mitigar cortes y mantener alta disponibilidad, confiabilidad y seguridad.

Fase de Optimización.

La optimización consiste en la búsqueda continua de los medios para alcanzar la excelencia operacional a través de la mejora del rendimiento, expansión de servicios y evaluaciones periódicas de los valores ligados a la red. Un buen negocio nunca se detiene en la búsqueda de una ventaja competitiva. En esta fase se debe evaluar si los objetivos del negocio o requerimientos técnicos han cambiado, o quizá existe una nueva funcionalidad o recomendación de mejora del rendimiento.

9.3. Definición del modelo de red a implementar.

En el diagrama de la figura 48 se muestra el modelo de red básico sobre el cual se implementará la solución de telefonía IP a través de red inalámbrica para los dispositivos móviles.

Los elementos básicos para la implementación son:

- Switch LAN, que permite las conexiones de los terminales cableados como PCs e impresoras.
- Servidor de aplicaciones, propio de la institución; alberga las aplicaciones relacionadas con el giro de negocio.
- IP-PBX, es el servidor de telefonía IP. Conecta a la PST a través de puertos analógicos
- Access Point, que cumpla con la certificación Wi-Fi Alliance WMM (Wireless Multi Media)
- Los terminales de usuarios inalámbricos, pueden ser los smartphones, tablets y PC portátiles.

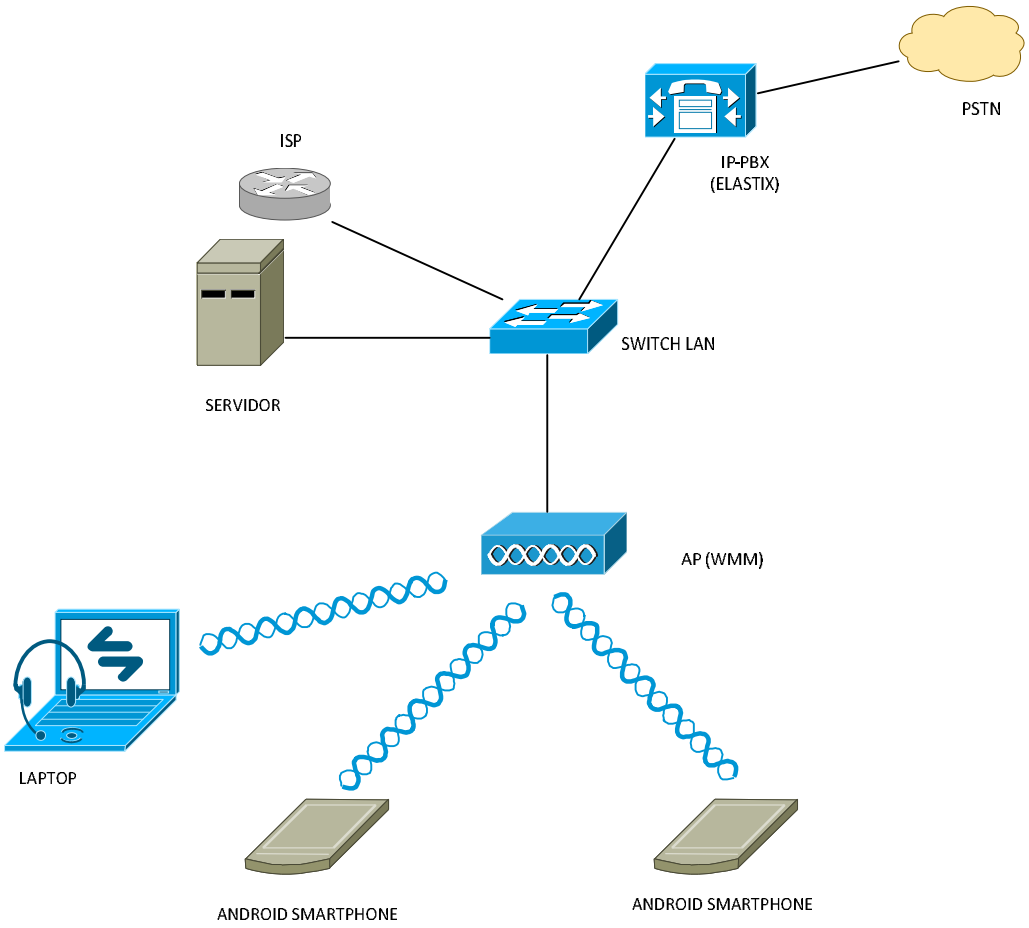


Figura 48. Topología de red a implementar. (Autor: José Chauca).

Este modelo de red es adecuado para pequeñas empresas donde la cantidad de usuarios inalámbricos será inferior a 32 dispositivos, y el área de cobertura no sea muy extensa.

Los cambios en las configuraciones se realizarán principalmente en el Access Point.

9.4. Elementos del sistema.

Para el desarrollo de la solución, los equipos específicos utilizados son los que se detallan en la tabla 16, estos se implementaran como se muestra en la figura 48.

Tabla 16. Detalle de elementos del sistema.

Elemento	Modelo	Versión	Aplicación SIP
IP-PBX	ELASTIX	2.4 64bits	
SWITCH-LAN	SG200-24		
AP	SAP1602I	15.2(2)JB2	
ANDROID TELEFONO 1	DELL VENUE 7 (3730)	4.4.2	CSIPSimple 1.02.00
ANDROID TELEFONO 2	SAMSUNG S4 MINI	4.2.2	Zoiper 1.19.5
LAPTOP	HP probook 4530	Win 7 SP2 64bist	

Nota: (Autor: José Chauca)

9.4.1. Central telefónica IP.

Para el desarrollo de este proyecto en particular se utiliza la funcionalidad de central telefónica del Servidor de Comunicaciones Unificadas Elastix, el cual es un software de código abierto para el establecimiento de comunicaciones unificas que incorpora en una única solución todos los medios y alternativas de comunicación existentes en el ámbito empresarial (Elastix, 2015). Cabe recalcar que Elastix no es una aplicación que hace de central telefónica únicamente, sino que también integra otros medios de comunicación muy útiles para mejorar la productividad en el entorno empresarial.

Los servicios que Elastix incorpora para ser considerado un Servidor de Comunicaciones Unificadas son los siguientes:

- Voz sobre IP (telefonía)
- Mensajería Instantánea.
- Servidor de Fax.
- Video conferencia
- Servidor de correo electrónico.

Para la elección de la plataforma de comunicaciones basada en una distribución de código abierto sobre una solución propietaria se tomaron en cuenta los siguientes parámetros:

- **Precio**, uno de los puntos más importantes a la hora de la toma de decisiones sobre el desembolso para la adquisición de soluciones tecnológicas es su costo, la solución escogida tiene un valor de USD $0.00 en su licenciamiento para la adición de usuarios así como de sus funcionalidades. Esto no implica que la solución será gratuita, puesto que habrá que invertir en el hardware adecuado acorde a las necesidades particulares de cada cliente y en la puesta en marcha del sistema.

- **Funcionalidades**, para un gerente o tomador de decisiones de una organización mientras más funcionalidades puede obtener a menor costo siempre será lo mejor, Elastix incorpora las funciones de Comunicaciones Unificadas antes descritas sin costo de licenciamiento.

- **Robustez tecnológica**, Elastix es una plataforma que está en constante desarrollo para incrementar nuevas características y funcionalidades que ayuden a incrementar la productividad con el uso de comunicaciones unificadas.

- **Soporte Técnico**, Lo que hasta hace poco no existía para aplicaciones de código abierto, en la actualidad se puede disponer de soporte directamente del fabricante que garantiza la continuidad de negocio.

Es importante indicar también, que a la hora de implementar la solución se debe tener en cuenta ciertas diferencias con respecto a una solución propietaria:

Seguridad, el hecho de que sea una plataforma de código abierto lo hace más vulnerable a ataques cuando se identifiquen sus vulnerabilidades, por lo que es importante revisar constantemente la solución que ofrece el fabricante o las comunidades de soporte.

Capacidad y rendimiento, las soluciones propietarias han sido desarrolladas sobre hardware dedicado a Comunicaciones Unificadas, por lo que tienen un rendimiento elevado, en una solución de código abierto el rendimiento va a depender de los recursos que se le asignen al sistema y el tamaño de la implementación.

9.4.2. Access Point con soporte 802.11e

Haciendo un balance entre costo y funcionalidad se ha optado por el Access Point de Cisco Aironet 1602I con antenas integradas, en la web del fabricante nos da a conocer que es un Access Point de clase empresarial, diseñado para atender las necesidades de conectividad inalámbrica de redes de empresas pequeñas y medianas (Cisco Systems, 2015).

Este modelo de Access Point provee al menos 6 veces más el throughput de las redes existentes 802.11a/g e incluye la tecnología MIMO 3x3 para redes 802.11n con dos flujos espaciales y funciona en las bandas de 2.4 GHz y 5GHz en canales de 20 y 40 MHz, entre otras características propias del fabricante, un parámetro muy importante para el desarrollo de este proyecto es el cumplimiento de la normativa WMM (Wi-Fi Multimedia) que nos permitirá la implementación de QoS para tráfico de voz con el uso del estándar 802.11e.

9.5. Consideraciones de diseño.

Al configurar QoS en los equipos de acceso inalámbrico lo que se hace es proveer un tratamiento preferencial a cierto tipo de tráfico. Sin QoS el AP simplemente ofrece un servicio “best-effort” a cada paquete sin importar su contenido o tamaño, se envían los paquetes sin ninguna garantía de fiabilidad, límites de retardo o rendimiento.

Recapitulando, las redes típicamente operan basadas en un esquema de distribución del “mejor esfuerzo” lo que significa que todo el tráfico tiene igual prioridad e igual oportunidad de ser entregado oportunamente. Pero, cuando ocurre congestión, todo el tráfico tiene igual oportunidad de ser descartado.

Cuando se configura QoS en un Access Point, se puede seleccionar un tráfico de red especifico, priorizarlo, y usar técnicas de manejo de congestión y prevención de congestión para proveer trato preferencial haciendo más efectivo el uso del ancho de banda.

Al momento de configurar QoS se crean políticas de QoS y se aplican a las VLAN configuradas en el AP.

La implementación de QoS para redes LAN inalámbricas difiere de la implementación en redes cableadas. Cuando el QoS está habilitado en un AP Cisco, este realiza las siguientes actividades, (Nayanajith, My CCIE Wireless Journey, 2013):

- Los AP NO clasifican los paquetes, ellos priorizan el paquete en base al valor de DSCP, tipo de cliente, o el valor de prioridad de las etiquetas 802.1q o 802.1p.
- No construyen valores internos de DSCP, solo soportan mapeo asignando los valores de IP DSCP, Precedencia o Protocolo a valores de CoS de capa 2.
- Llevan a cabo EDCF como colas solo en el puerto de salida del radio.
- Realizan solo encolamiento FIFO en el puerto de salida Ethernet.
- Soportan solo paquetes etiquetados 802.1q/p.
- Soportan solo MQC como policy-map.

9.6. Impacto de QoS en una red inalámbrica

Las características de QoS en redes inalámbricas son un subconjunto de propuestas en el draft 802.11e, QoS en redes LAN Inalámbricas provee priorización del tráfico desde el Punto de Acceso sobre la red inalámbrica basada en la clasificación del tráfico. Al igual que en otros medios de comunicación, puede ser que no sea notorio los efectos de aplicar QoS en una red inalámbrica con poca carga de tráfico, Los benéficos de aplicar QoS en la red inalámbrica se hacen más obvios y notorios a medida que el tráfico en la red se incrementa, manteniéndose los parámetros fundamentales como latencia, jitter y pérdida de paquetes dentro de rangos aceptables.

QoS en las redes inalámbricas se enfoca en la priorización descendente desde el punto de acceso, para tener una mejor idea del sentido del tráfico nos guiaremos en la figura 49:

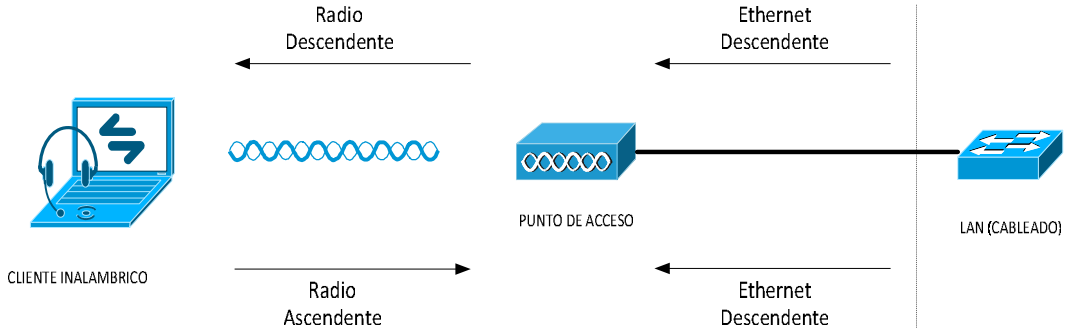


Figura 49. Sentido de flujo de tráfico de red. (Nayanajith, My CCIE Wireless Journey, 2013) .

- El flujo de radio descendente es transmitido fuera del radio del AP hacia el dispositivo cliente inalámbrico. La aplicación de QoS sobre WLAN se enfoca en este sentido de tráfico.

- El flujo de radio ascendente es el tráfico transmitido desde el dispositivo cliente inalámbrico hacia el Access Point, QoS inalámbrico no afecta a este tráfico.

- El flujo descendente Ethernet es el tráfico desde el switch o router hacia el puerto Ethernet del punto de acceso. Si QoS está habilitado en el switch o router este puede priorizar el tráfico hacia el Access Point.

- El flujo ascendente Ethernet es el tráfico enviado desde el puerto Ethernet del Access Point hacia el switch o router. El Access Point no prioriza el tráfico que se envía al segmento cableado basado en la clasificación del tráfico.

9.7. El softphone.

Un softphone, proveniente de la combinación de las palabras inglesas software y telephone, es un software que contiene todas las funcionalidades de un teléfono IP físico y utiliza los protocolos de telefonía IP para el establecimiento de llamadas a otros similares, teléfonos IP físicos o teléfonos convencionales dependiendo de la arquitectura de la red. En principio fueron desarrollados para funcionar en PCs, pero con la aparición y rápido desarrollo de los teléfonos inteligentes hoy en día existen aplicaciones para los principales sistemas operativos como son Android e IOS.

Para este proyecto se han utilizado tres aplicaciones distintas, las mismas que están en la lista de softphones más recomendados para Android (Rojano, 2013), la elección se ha realizado en base a características principales de cada uno de ellos y a la experiencia propia en implementaciones previas. A continuación se repasan breves descripciones de cada uno de ellos:

9.7.1 Bria Android Edition

De acuerdo con el portal web del fabricante: Bria Android Edition es un softphone VoIP de alta seguridad basada en estándares móvil que funciona a través de redes Wi-Fi y 3G (COUNTERPATH, 2016).

Con el uso de la lista de contactos existente en el dispositivo, el cliente Bria Android SIP facilita una fácil y eficaz de gestión de la comunicación con una interfaz de aplicación intuitiva (ver figura 50). Las funcionalidades de llamada con clase de teléfono de escritorio incluye la posibilidad de alternar entre dos llamadas, fusionar llamadas y realizar transferencias atendidas y desatendidas.

El software Bria Android edición incorpora opciones de seguridad avanzadas que permiten la señalización de llamada segura. También contiene funciones de audio mejoradas incluyendo G.711, G.722, GSM, iLBC, SILK y OPUS.

Bria Android Edition funciona perfectamente con otras soluciones de escritorio y de convergencia CounterPath, así como con equipos empresariales e infraestructuras de carrier de los principales proveedores como Alcatel-Lucent, Ericsson, BroadSoft, Metaswitch, Avaya, Cisco y NEC. Bria Android Edition también es compatible con los sistemas de telefonía basados en Asterisk.

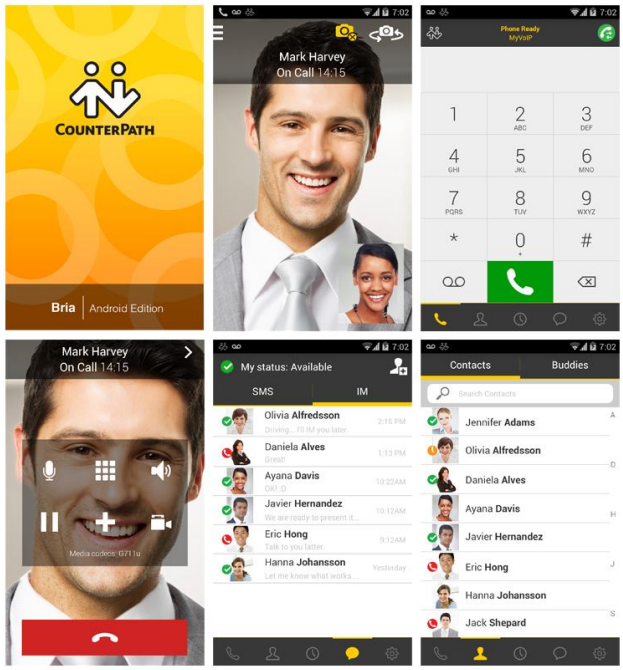


Figura 50. Capturas de pantalla del Softhphone BRIA ANDROID EDITION (COUNTERPATH, 2016)

Incluye: Compatibilidad con VPN, Grabación de llamadas, Protocolos XMPP y SIP SIMPLE, incluidos SMS, QoS (calidad del servicio): marca ToS, Seguridad y cifrado mediante TLS y SRTP, Búsquedas de registros mediante DNS SRV. Códecs G.711a/u, G.722 (HD), iLBC, GSM y SILK. También soporta G729 con el pago de la correspondiente licencia, (Rojano, 2013).

9.7.2. Zoiper IAX & SIP

Zoiper es una aplicación gratuita de softphone para protocolos IAX y SIP para llamadas de VoIP sobre redes 3G o WIFI (ZOIPER, 2015).

Zoiper es un softphone VoIP que le permite hacer chat o realizar llamadas de voz y video con sus amigos, familiares, colegas y socios de negocios. A diferencia de otros programas como Skype o Viber, es abierto y se puede utilizar con cualquier proveedor de VoIP o PBX. Permitiendo una mayor flexibilidad y la terminación más barato o mejor calidad. En la figura 51 se muestran imágenes de la aplicación.



Figura 51. Capturas de pantalla de softphone ZOIPER para Android (ZOIPER, 2015).

9.7.3. CSIP Simple.

Como indica en su descripción del Android Play Store: Proyecto OpenSource (GPL) para SIP en Android (CSipSimple, 2015). En la figura 52 aprecia la interface de la aplicación.

Entre sus principales características están:

- Alto rendimiento
- Reescritura / reglas de filtrado para la integración con Android
- SIP SIMPLE para mensajería
- Grabar llamadas

- Configuración sencilla
- UI Fancy inspirado en el tema Holo 4.x
- Muchos códecs (códecs HD, códec optimizados)
- Apoyado cifrado: TLS para SIP y SRTP / ZRTP para los medios
- Temas

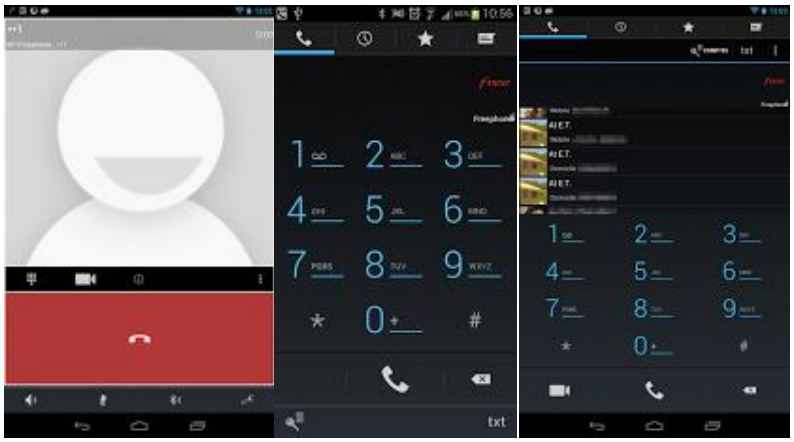


Figura 52. Capturas de pantalla de softphone CSIP SIMPLE para Android (CSipSimple, 2015)

9.8. Análisis de pruebas y resultados.

9.8.1. Configuración de la red

Los equipos pertenecientes a la red han sido configurados de la siguiente manera:

SUBREDES

En la tabla 17 se muestran los rangos de subred que se han implementado para la ejecución del proyecto.

Tabla 17. Sub direccionamiento IP

VLAN ID	Descripción	Red IP	Mascara de red
1	Red de Datos	192.168.10.0	255.255.255.0
5	Red de Telefonía IP	192.168.1.0	255.255.255.0

Nota: (Autor: José Chauca)

DIRECCIONAMIENTO IP EQUIPOS

Para los principales equipos pertenecientes a la red, se han configurado las direcciones IP de acuerdo a la tabla 18.

Tabla 18. Direccionamiento IP de equipos de telecomunicaciones.

Equipo	Dirección IP	Descripción
GATEWAY ISP	192.168.1.1	PROVEEDOR ISP
SWITCH CAPA 3	192.168.1.99	Interface VLAN 5
	192.168.10.1	Interface VLAN 1
IP-PBX Elastix	192.168.1.200	Servidor de telefonía IP
Gateway PSTN	192.168.1.210	Enlace PSTN
SERVIDOR EMPRESARIAL	192.168.10.28	Aplicaciones y base de datos
EQUIPOS VLAN 1	Cliente DHCP	
EQUIPOS VLAN 5	Cliente DHCP	

Nota: (Autor: José Chauca)

PARAMETROS QoS

De acuerdo a las recomendaciones de Asterisk, aplicación sobre la cual se basa el desarrollo de Elastix, para un servidor de telefonía basado en protocolo SIP deberá tener los valores que se detallan en la tabla 19, (Asterisk, 2014).

Gracias a la posibilidad de administración del Switch, en este se ha configurado la VLAN de voz, lo que permite marcar los paquetes de subred con el respectivo parámetro de ToS/Cos, mientras que en el Access Point, que no realiza tareas de clasificación ni marcaje de paquetes, se lo ha configurado de tal manera que permita un tratamiento especial a los paquetes de telefonía IP que ingresan a través de la interface Ethernet previamente clasificados asignado las prioridades respectivas y manejo adecuado de colas basado en el estándar 802.11e de acuerdo a la tabla 20.

Tabla 19. Parámetros QoS para Asterisk

	ToS	CoS
Señalización	Cs3	3
Audio	Ef	5
Video	Af41	4
Texto	Af41	3
Otro	Ef	

Fuente: (Asterisk, 2014).

La ranura de tiempo fija AIFS especifica el tiempo de espera para las tramas de datos, este tiempo se mide en slots y los valores admisibles están entre 1 y 255.

Tabla 20. Parámetros QoS Access Point.

Categoría de Acceso		Voz (Cos 6 – 7)
Ventana de contención mínima CWmin	AP	2
	Cliente	2
Ventana de contención máxima CWmax	AP	4
	Cliente	4
Ranura de tiempo fija AIFS	AP	1
	Cliente	2
Oportunidad para transmitir (0 – 65535	AP	0
	Cliente	0

Nota: (Autor: José Chauca).

CWmin, este parámetro es la entrada del algoritmo que determina el tiempo de espera inicial aleatorio (ventana) para reintentar una transmisión. El primer número aleatorio generado será un valor entre 0 y CWmin.

CWmax, este valor es el límite superior para el doblado del valor aleatorio de backoff cuando los tiempos de backoff han expirado antes de que se transmita datos. Cada vez que expira el backoff se dobla el backoff hasta alcanzar el CWmax.

9.8.2. Tamaño de muestra y tráfico en la red.

Tamaño de muestra.

Para considerar a los resultados obtenidos como válidos, el análisis de la información se ha basado en el tamaño de muestra obtenido estadísticamente con la formula siguiente para datos globales (Feedback Netoworks, 2013):

$$n = \frac{k^2 * p * q * N}{[e^2 * (N-1)] + k^2 * p * q}$$

N: es el tamaño de la población o universo.

k: es una constante que depende del nivel de confianza que asignemos[10]. Estos los podemos obtener de la tabla 21 (para distribución normal).

Tabla 21. Intervalos de confianza.

Confianza	Constante k
75%	1.15
80%	1.28
85%	1.44
90%	1.65
95%	1.96
95.5%	2.00
99%	2.58

Nota: (Autor: José Chauca), en base a tabla de distribución normal

e: Es el error muestral deseado. El error muestral es la diferencia que puede haber entre el resultado que obtenemos preguntando a una muestra de la población y el que obtendríamos si preguntáramos al total de ella.

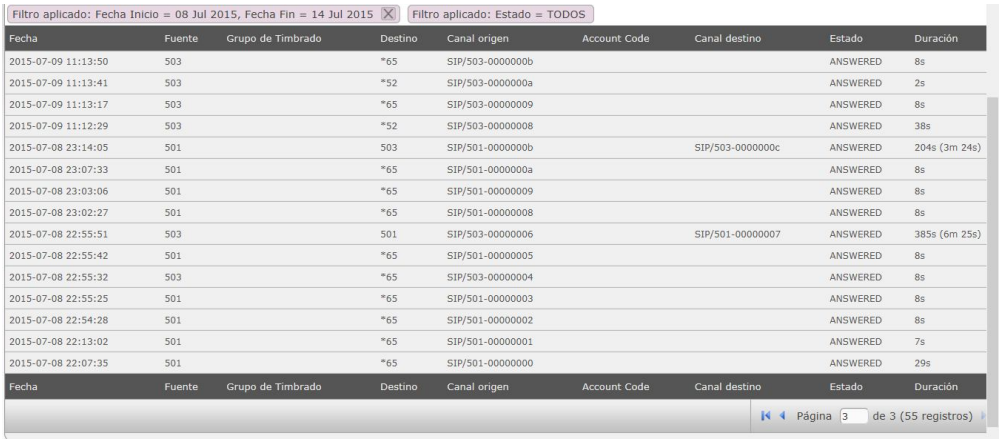
[10] Estos valores corresponden a la tabla de distribución normal, para más detalle podemos acceder al siguiente enlace: https://www.uam.es/personal_pdi/ciencias/gallardo/Tablas-normal-chi-t-F.pdf

p: Es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p=q=0.5 que es la opción más segura.

q: Es la proporción de individuos que no poseen esa característica, es decir, es 1-p.

n: Es el tamaño de la muestra (número datos a analizar).

Para nuestro caso los valores a utilizar están en la tabla 22, donde la población total a analizar es el número de llamadas de prueba que ocurrieron en el lapso de un día, este valor se puede obtener del registro de llamadas CDR de la IP-PBX (ver figura 53). Por tratarse de un ambiente controlado existe la certeza de que la comunicación se realizó entre dos dispositivos inalámbricos Android con cliente SIP instalado.



Filtro aplicado: Fecha Inicio = 08 Jul 2015, Fecha Fin = 14 Jul 2015 | Filtro aplicado: Estado = TODOS

Fecha	Fuente	Grupo de Timbrado	Destino	Canal origen	Account Code	Canal destino	Estado	Duración
2015-07-09 11:13:50	503		*65	SIP/503-0000000b			ANSWERED	8s
2015-07-09 11:13:41	503		*52	SIP/503-0000000a			ANSWERED	2s
2015-07-09 11:13:17	503		*65	SIP/503-00000009			ANSWERED	8s
2015-07-09 11:12:29	503		*52	SIP/503-00000008			ANSWERED	38s
2015-07-08 23:14:05	501		503	SIP/501-0000000b		SIP/503-0000000c	ANSWERED	204s (3m 24s)
2015-07-08 23:07:33	501		*65	SIP/501-0000000a			ANSWERED	8s
2015-07-08 23:03:06	501		*65	SIP/501-00000009			ANSWERED	8s
2015-07-08 23:02:27	501		*65	SIP/501-00000008			ANSWERED	8s
2015-07-08 22:55:51	503		501	SIP/503-00000006		SIP/501-00000007	ANSWERED	385s (6m 25s)
2015-07-08 22:55:42	501		*65	SIP/501-00000005			ANSWERED	8s
2015-07-08 22:55:32	503		*65	SIP/503-00000004			ANSWERED	8s
2015-07-08 22:55:25	501		*65	SIP/501-00000003			ANSWERED	8s
2015-07-08 22:54:28	501		*65	SIP/501-00000002			ANSWERED	8s
2015-07-08 22:13:02	501		*65	SIP/501-00000001			ANSWERED	7s
2015-07-08 22:07:35	501		*65	SIP/501-00000000			ANSWERED	29s
Fecha	Fuente	Grupo de Timbrado	Destino	Canal origen	Account Code	Canal destino	Estado	Duración

Página 3 de 3 (55 registros)

Figura 53. Registro de llamadas de la central telefónica IP. (Autor: José Chauca).

Tabla 22. Datos para cálculo de tamaño de muestra, red sin QoS.

Parámetro	**Valor**	**Observación.**
N	34	Llamadas telefónicas
K	1.95	Confianza 95 %
E	5	%
P	0.5	Probabilidad de acierto
Q	0.5	(1-p)
N	**31**	**Resultado**

(Autor: José Chauca)

Con el tamaño de la muestra establecido se procede con la evaluación de las condiciones de la llamada en cada muestra, donde se han obtenido los siguientes (más detalles en la tabla 24):

- Llamadas normales = 13.
- Llamadas con mala calidad = 18.

Con llamadas normales se hace referencia a la comunicación entre los dos dispositivos inalámbricos donde en el terminal SIP no tenemos mensajes de mala calidad de comunicación y ambos interlocutores pueden entender la conversación. Por el contrario una llamada con mala calidad presentará un mensaje en el dispositivo móvil que indica esta situación y/o uno o ambos interlocutores no entiende la conversación, típicamente percibida por cortes o retardos en la voz.

De manera similar, de los resultados obtenidos en las pruebas con calidad de servicio (ver tabla 25), se calcula el tamaño de muestra a analizar empleando las mismas fórmulas del caso anterior. Estos resultados se muestran en la tabla 23.

Tabla 23. Datos para el cálculo del tamaño de muestra, red con QoS.

Parámetro	**Valor**	**Observación.**
N	21	Llamadas telefónicas
K	1.95	Confianza 90%
E	5	%
P	0.5	
Q	0.5	
N	**20**	**Resultado**

(Autor: José Chauca)

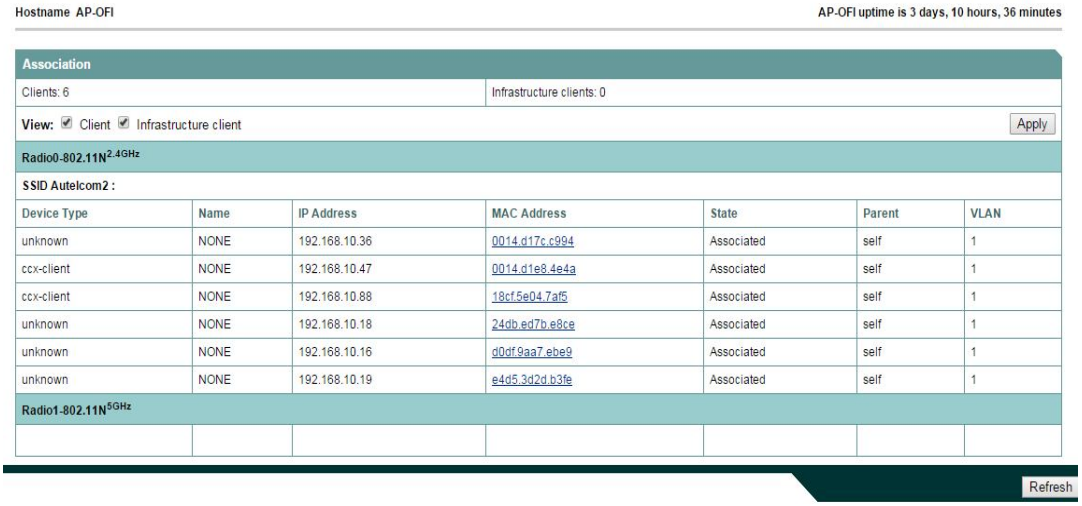
En la muestra obtenida se puede identificar los siguientes tipos de llamadas:

- Llamadas normales = 19.
- Llamadas con mala calidad = 1.

Tráfico de red.

Los resultados se han obtenido bajo las siguientes condiciones:

- Seis clientes simultáneos en la banda de 2.4 GHz (figura 54). Cuando se aplique QoS los dispositivos con capacidad de VoIP se conectaran a un SSID asignado a la VLAN de voz (figura 55).



Hostname AP-OFI — AP-OFI uptime is 3 days, 10 hours, 36 minutes

Association

Clients: 6 | Infrastructure clients: 0

View: ☑ Client ☑ Infrastructure client — Apply

Radio0-802.11N 2.4GHz

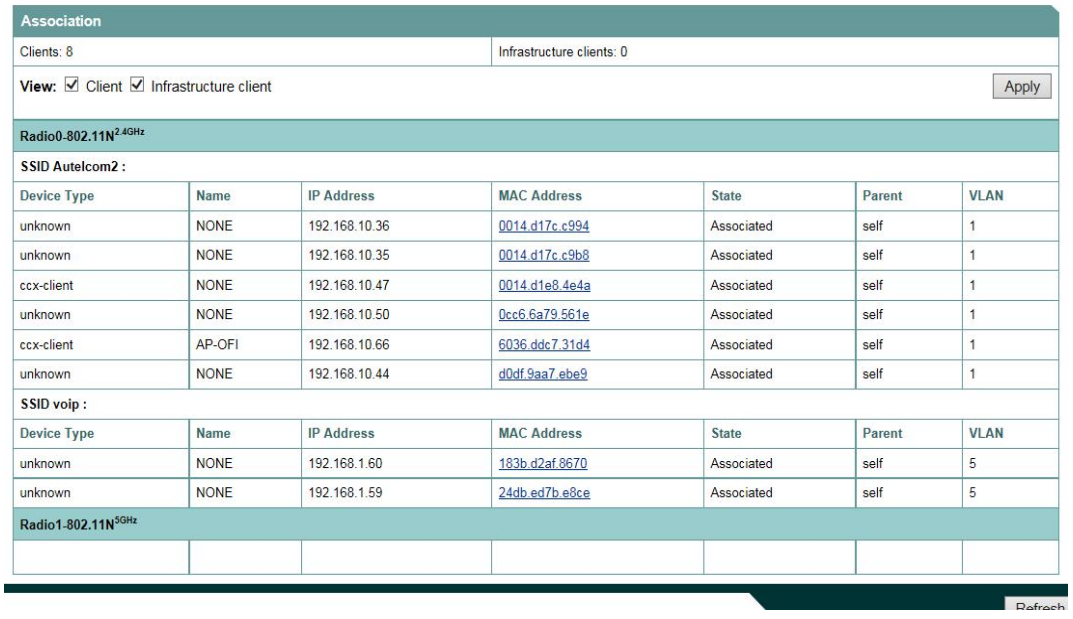
SSID Autelcom2 :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	NONE	192.168.10.36	0014.d17c.c994	Associated	self	1
ccx-client	NONE	192.168.10.47	0014.d1e8.4e4a	Associated	self	1
ccx-client	NONE	192.168.10.88	18cf.5e04.7af5	Associated	self	1
unknown	NONE	192.168.10.18	24db.ed7b.e8ce	Associated	self	1
unknown	NONE	192.168.10.16	d0df.9aa7.ebe9	Associated	self	1
unknown	NONE	192.168.10.19	e4d5.3d2d.b3fe	Associated	self	1

Radio1-802.11N 5GHz

Refresh

Figura 54. Reporte de clientes conectados al AP sin QoS. (Autor: José Chauca).



Association

Clients: 8 | Infrastructure clients: 0

View: ☑ Client ☑ Infrastructure client — Apply

Radio0-802.11N 2.4GHz

SSID Autelcom2 :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	NONE	192.168.10.36	0014.d17c.c994	Associated	self	1
unknown	NONE	192.168.10.35	0014.d17c.c9b8	Associated	self	1
ccx-client	NONE	192.168.10.47	0014.d1e8.4e4a	Associated	self	1
unknown	NONE	192.168.10.50	0cc6.6a79.561e	Associated	self	1
ccx-client	AP-OFI	192.168.10.66	6036.ddc7.31d4	Associated	self	1
unknown	NONE	192.168.10.44	d0df.9aa7.ebe9	Associated	self	1

SSID voip :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	NONE	192.168.1.60	183b.d2af.8670	Associated	self	5
unknown	NONE	192.168.1.59	24db.ed7b.e8ce	Associated	self	5

Radio1-802.11N 5GHz

Refresh

Figura 55. Reporte de clientes conectados a la red de datos y a la red de telefonía, AP con QoS. (Autor: José Chauca).

- La carga de tráfico en el aire tiene un pico máximo de 4500 (2.5 MBps) paquetes por segundo, este valor se obtiene de la figura 56, que representa el flujo de datos en el tiempo, para esto se han capturado todos los paquetes en la frecuencia de operación del Access Point con ayuda de la herramienta Newotork Monitor de Microsoft, y se han representado gráficamente utilizando la herramienta de análisis de tráfico Wireshark. Con ayuda de muestreo estadístico se ha determinado que el tamaño de muestra para conocer la carga de la red será de 380s (el cálculo se ha realizado considerando que la actividad del servicio de telefonía IP será durante 8 horas laborables)

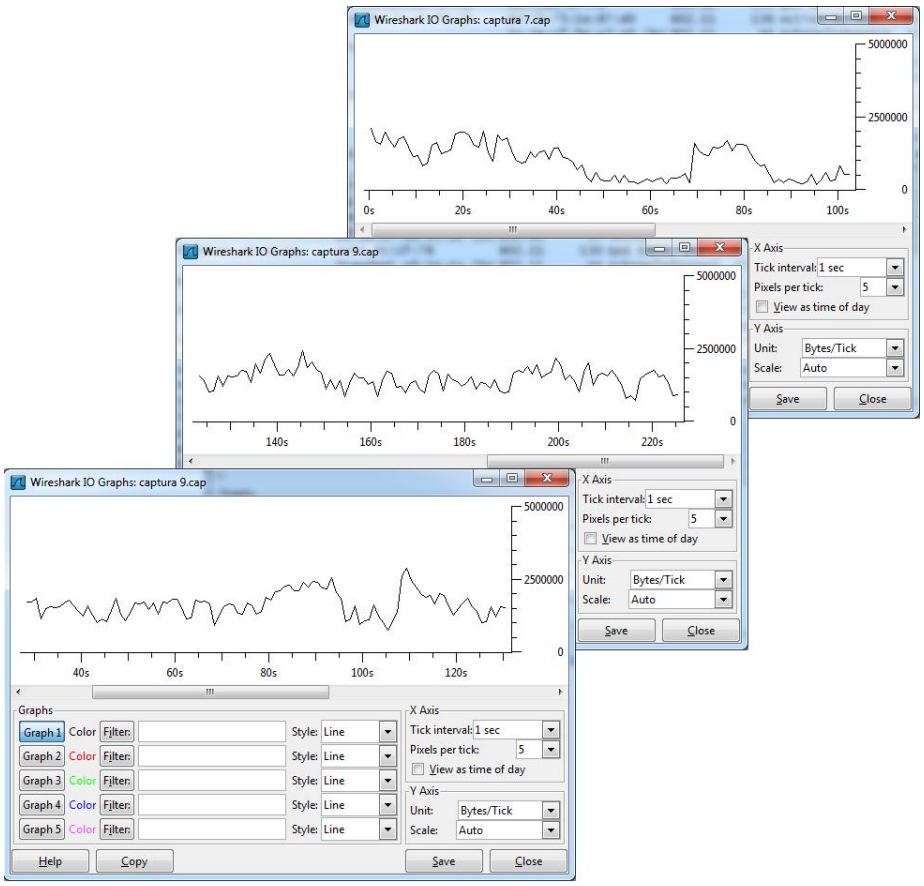


Figura 56. Tráfico inalámbrico, red sin QoS. (Autor: José Chauca).

- Para garantizar que la captura de paquetes no incluya datos de otras redes que estén trabajando en el mismo canal, con la ayuda de la herramienta Wifi Analyzer de Farproc se ha realizado un escaneo del medio, obteniendo como resultado que el SSID Autelcom2 es la única red funcionando en el canal 1 (ver figura 57)

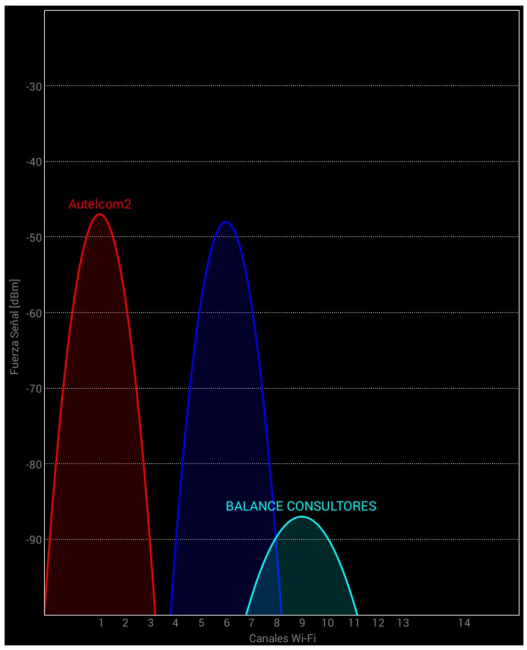


Figura 57. Resultado de Wifi Analizer, SSID Autelcom2 trabajando en canal 1. (Autor: José Chauca).

9.8.3. Resultados obtenidos.

5.8.2.1. Red Sin QoS

Percepción de la calidad de la comunicación por el usuario: mala

Las razones que llevar a tal percepción se dan por la presencia de los siguientes problemas durante una llamada voz:

- Voz entre cortada o tipo robot.
- Se escucha solo en un sentido.
- No hay voz.

Problemas atribuibles a la configuración de mecanismos de QoS no adecuados.

Apoyados en la herramienta Microsoft Network Monitor 3.4 para la captura de paquetes y representada con el software Wireshark, en la figura 58 podemos identificar que la red inalámbrica no está aplicando QoS a los paquetes de telefonía, puesto que la información de capa 2 relacionada al estándar 802.11 no contiene ningún campo de QoS a pesar que el paquete a nivel de capa 3 ha sido marcado en el campo DSCP con el valor EF (ver figura 59).

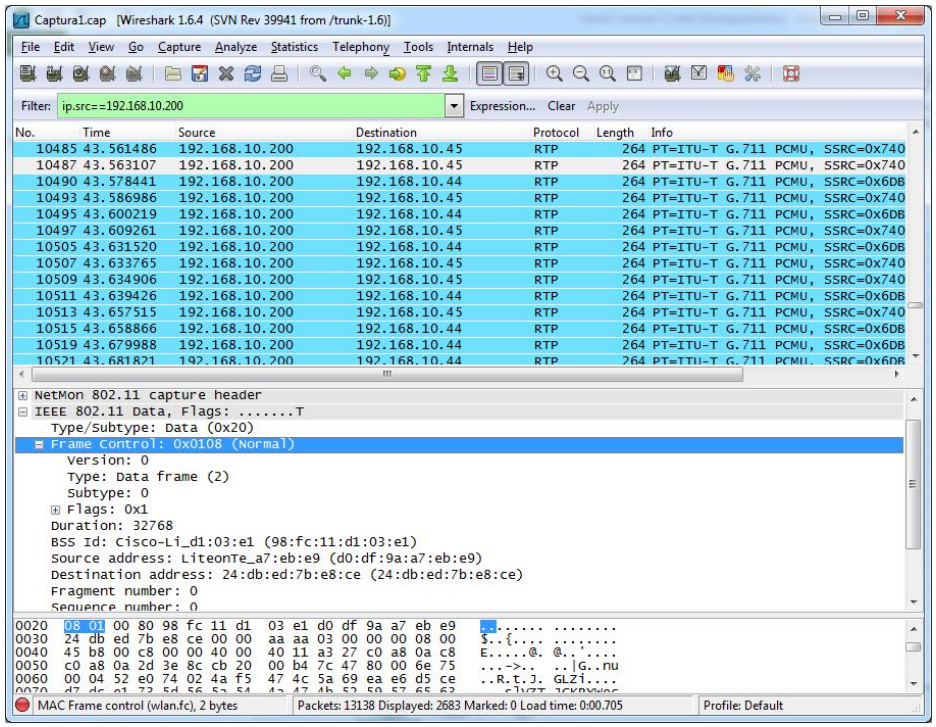


Figura 58. Trama 802.11 sin QoS. (Autor: José Chauca).

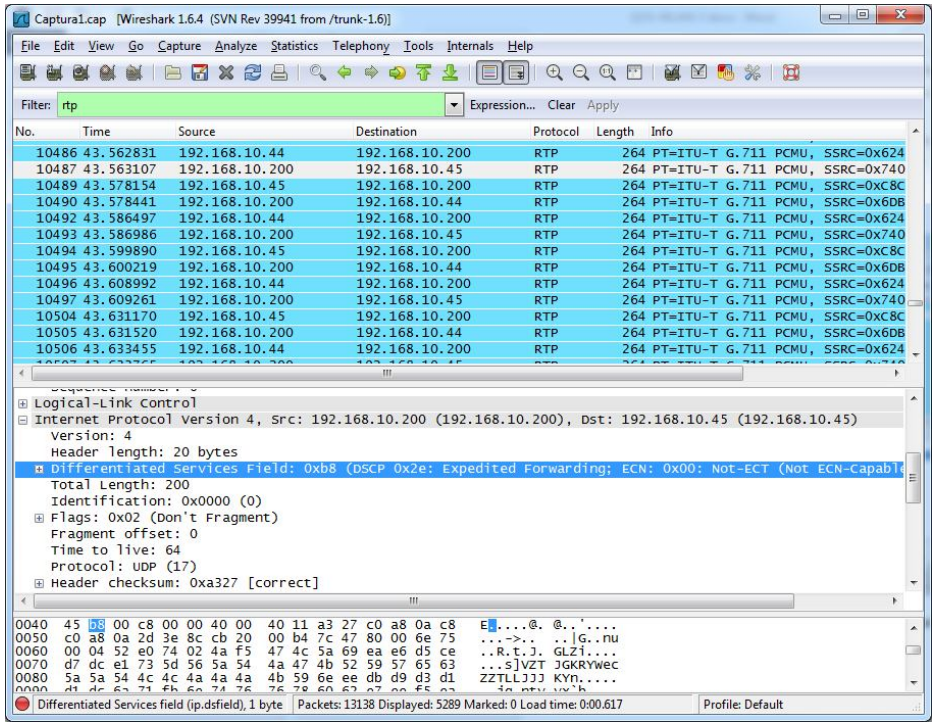


Figura 59. Paquete marcado en campo DSCP con valor EF. (Autor: José Chauca).

Resultados en Teléfono con Softphone BRIA

- El teléfono tiene asignada la extensión 501.
- Se establece una comunicación entre las extensiones 501 y 504.
- La extensión 504 es un teléfono IP físico.
- El software de Bria tiene la ventaja de poder mostrarnos estadísticas en tiempo real de la comunicación de donde podemos identificar el comportamiento de los parámetros sensibles, el sobrepasar los límites recomendables hace que la aplicación misma notifique la mala calidad de la llamada, situación que es percibida por los usuarios participantes de la comunicación (figura 60).
- Cabe indicar que los dispositivos se encuentran dentro del mismo segmento de red, donde simultáneamente existe tráfico de datos.
- En la tabla 24, tenemos los valores obtenidos de las estadísticas en uno de los dispositivos móviles, en este caso con la utilización del software BRIA (extensión 501). La imagen de cómo se muestran los valores estadísticos en la aplicación móvil los podemos apreciar en la figura 60.

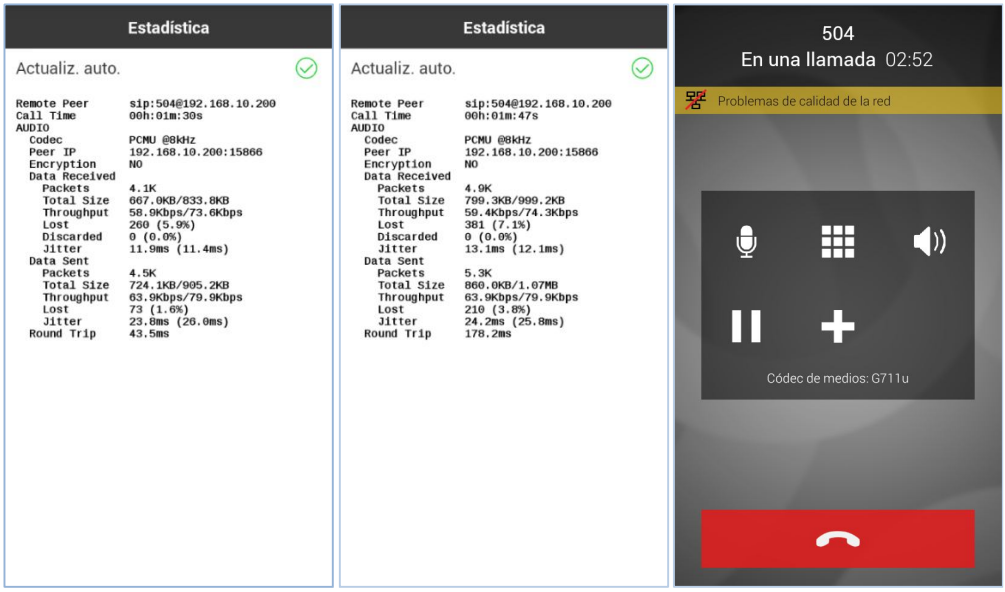


Figura 60. Estadísticas durante una llamada sin QoS, softphone BRIA.

Tabla 24. Datos obtenidos con el software BRIA en la red sin QoS.

Prueba	Jitter (ms) Max 50 ms.	Pérdida (%) Max 1%	Retardo (ms) Max 150 ms.	Calidad de llamada.
1	7.0	1.2	11.5	Mala
2	13.4	2.0	82.3	Mala
3	17.5	3.4	0.0	Mala
4	17.7	2.6	22.5	Mala
5	7.1	0.5	23.7	Buena
6	9.2	4.9	7.6	Mala
7	4.8	0.4	0.0	Buena
8	15.3	0.0	2.6	Buena
9	8	1.6	52.6	Mala
10	13.6	0.0	4.1	Buena
11	14.4	0	3.8	Buena
12	11.9	5.9	43.5	Mala
13	13.1	7.1	178.2	Mala
14	14.9	0.0	4.4	Buena
15	14.2	2.9	5.2	Mala
16	13.9	0.9	2.4	Buena
17	5.1	4.7	22.9	Mala
18	4.6	0.7	17.0	Buena

19	4.0	0.0	4.4	Buena
20	24.2	3.3	277.5	Mala
21	13.4	2.9	28.1	Mala
22	24.5	1.8	124.0	Mala
23	16.9	14.2	33.4	Mala
24	15.1	9.0	108.0	Mala
25	11.8	0.4	26.6	Buena
26	8.7	0.2	37.9	Buena
27	15.6	0.0	3.3	Buena
28	16.5	3.1	15.3	Mala
29	17.7	2.9	33.5	Mala
30	14.2	3.8	47.7	Buena
31	18.4	1.8	51.0	Mala

(Autor: José Chauca).

5.8.2.2. Red con QoS

Percepción de la calidad de la comunicación por el usuario: aceptable

Razones:

- La llamada ocurre sin mayores complicaciones, es entendible entre las partes.

Ayudados con el software de captura de paquetes en la figura 61 podemos identificar que se aplica QoS a nivel inalámbrico:

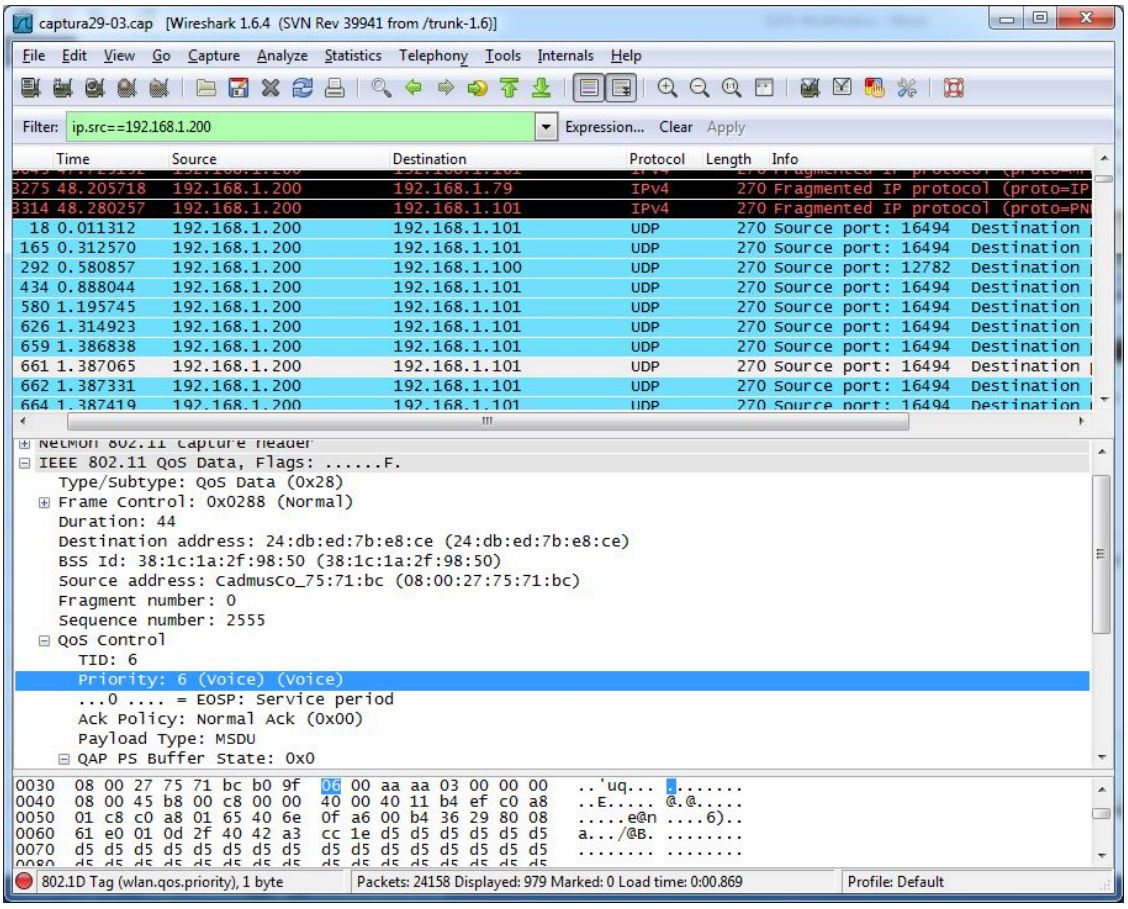


Figura 61. Trama 802.11 con QoS para voz. (Autor: José Chauca)

Pruebas con software BRIA

- Llamada desde la extensión 501 hacia la IP-PBX para escuchar la hora (*60). La imagen de la izquierda de la figura 62 contiene las estadísticas para esta llamada.

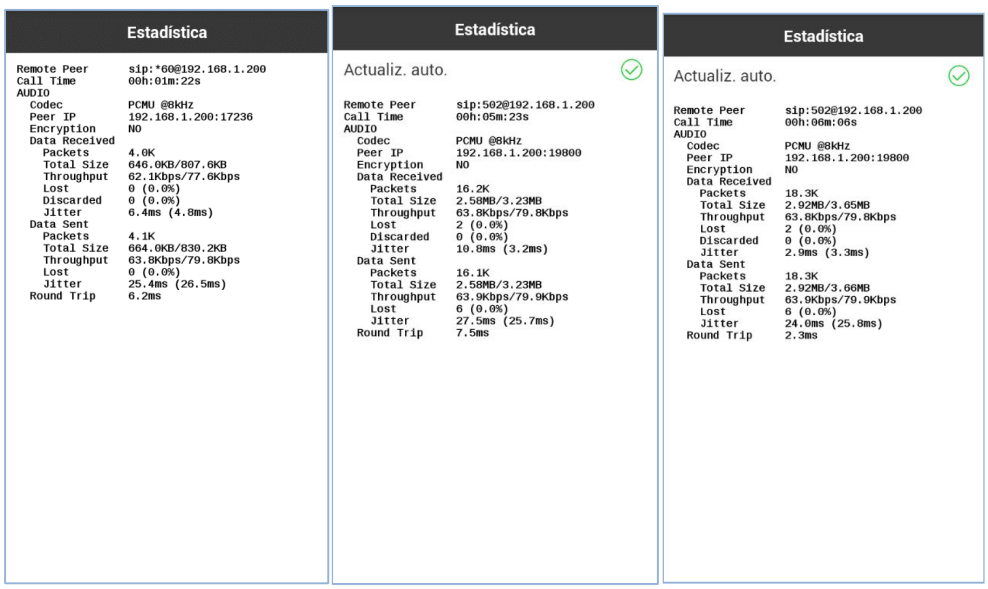


Figura 62. Estadísticas con softphone BRIA (pruebas con QoS), (Autor: José Chauca)

- Llamada entre las extensiones 501 y 502, la extensión 502 es un softphone sobre una Tablet, los resultados los tenemos en la figura 62, en las dos pantallas de la derecha.

- En la tabla 25 resumimos los valores obtenidos de las estadísticas del softphone empleado para las pruebas.

Tabla 25. Comparación valores obtenidos con QoS vs límite.

Prueba	Jitter (ms) Max 50 ms.	Pérdida (%) Max 1%	Retardo (ms) Max 150 ms.	Calidad de llamada.
1	1.5	0.0	28.0	Buena
2	14	0.0	2.8	Buena
3	14.7	0.7	1.8	Buena
4	0.8	0.4	0.0	Buena
5	14.9	0.9	5.1	Buena
6	1.0	0.0	2.9	Buena

7	14.0	0.0	3.2	Buena
8	6.4	0.0	6.2	Buena
9	10.8	0.0	7.5	Buena
10	2.9	0.0	2.3	Buena
11	14.1	0.1	3.4	Buena
12	13.6	0.0	3.1	Buena
13	15.9	0.3	4.2	Buena
14	16.6	0.5	39.8	Buena
15	28.4	0.0	21.0	Buena
16	15.9	0.0	32.7	Buena
17	3.4	0.0	13.6	Buena
18	3.5	0.3	14.5	Buena
19	18.4	0.0	76.0	Buena
20	14.8	4.5	2.3	Mala

(Autor: José Chauca).

Prueba con software ZOIPER

- Llamada entre la extensión 502 y 504, la extensión 502 corresponde al Smart-Phone, la extensión 504 es un teléfono fijo de escritorio, las estadísticas las podemos mirar en la imagen 63.



Figura 63. Estadísticas en softphone ZOIPER, (Autor: José Chauca)

9.8.4. Intervalos de confianza de las pruebas realizadas.

Red sin Calidad de Servicio.

De los datos recolectados en inalámbricas sin calidad de servicio, del total de muestras analizadas (n = 31) se obtuvo que 18 llamadas presentaban mala calidad como para mantener una conversación adecuada, en función de estos datos calculamos el intervalo de confianza para la proporción de estas llamadas (Prunosa, 2012):

- **Cálculo del parámetro (llamadas de mala calidad)**

  p = 18/31 = 0.58 (1-p = 0.42)

- **Comprobación de condiciones de aplicación.**

  P > 5/n -> 0.58 > 0.16 (cumple la condición)

- **Error estándar del parámetro.**

$$eep = \sqrt{\frac{p(1-p)}{n}}$$

  eep = 0.088

- **En base a la tabla de distribución normal se asigna al parámetro z un valor adecuado de tal forma que el grado de confianza sea del 95%**

  z = 1.96

- **El valor del intervalo de confianza con la certeza del 95% para encontrar una llamada con mala calidad en una red sin calidad de servicio está dentro del siguiente rango:**

  [p – z*epp; p + z*epp] => [41% ; 75%]

Con el último dato obtenido se puede afirmar con una confianza del 95% que en una red sin calidad de servicio se obtendrán entre el 41% al 75% de llamadas de mala calidad.

Red con Calidad de Servicio.

Para el caso de las pruebas realizadas en este tipo de red se emplearán las mismas formulas del caso anterior, de los cual obtenemos:

- **Cálculo del parámetro (llamadas de buena calidad)**

  p = 19/20 = 0.95 (1-p = 0.05)

- **Comprobación de condiciones de aplicación.**

  P > 5/n -> 0.95 > 0.25 (cumple la condición)

- **Error estándar del parámetro.**

$$eep = \sqrt{\frac{p(1-p)}{n}}$$

  eep = 0.049

- **En base a la tabla de distribución normal se asigna al parámetro z un valor adecuado de tal forma que el grado de confianza sea del 95%**

  z = 1.96

- **El valor del intervalo de confianza con la certeza del 95% para encontrar una llamada de buena calidad en una red con calidad de servicio está dentro del siguiente rango:**

  [p – z*epp; p + z*epp] => [85% ; 105%]

Con esto se puede afirmar con una confianza del 95% que en una red con calidad de servicio se obtendrán entre el 85% al 100% de llamadas de buena calidad.

9.9. Costo Total de Propiedad

En la tabla 26 se muestra el costo monetario de implementar la solución de telefonía IP con calidad de servicio inalámbrico.

Tabla 26. Precio de equipos involucrados en la solución.

Equipo	Cantidad	Precio Unitario	Precio Total
Appliance Elastix Mini UCS	1	900.00	900.00
Switch de acceso Capa 3 SG300-24	1	600.00	600.00
Access Point AIR-SAP1602	2	650.00	1300.00
Teléfono IP GXP1405	6	50.00	300.00
Softphone para Android	5	0	0
TOTAL			**3100.00**

(Autor: José Chauca).

Según el art 21 numeral 6 del reglamento de la Ley de Régimen Tributario, los equipos de computación se deprecian en 3 años o 36 meses, dando como resultado una depreciación mensual de $ 86.11 que no repercute en mayor medida en la economía de una empresa pequeña o mediana.

Todos los equipos son administrados vía web lo que hace más intuitiva su configuración

Una vez puesto en marcha el sistema, de requerirse incremento de servicios y/o funcionalidades en el servidor de comunicaciones unificadas, si no se dispone del equipo de soporte propio se podría contratar horas de servicio para funciones puntuales sin la necesidad de realizar cambios en la infraestructura LAN o WLAN.

Los usuarios con teléfonos inteligentes Android pueden disponer de una extensión en su dispositivo lo que va a permitir la movilidad dentro la red, disminución en el uso de recursos empresariales, disponibilidad de la persona. Al hablar de movilidad, se quiere decir, que el usuario no va a estar atado a su escritorio dependiendo de su conexión de red física sino que, podrá desplazarse por las ubicaciones donde tenga cobertura inalámbrica para acceso a la red empresarial. Al referirnos a la disminución del uso de recursos empresariales, se apunta a que un empleado que ocasionalmente realiza su trabajo desde la oficina no va a

requerir disponer de un teléfono físico, porque mientras trabaja desde fuera, el equipo va a quedar subutilizado, el no disponer de este dispositivo también va a evitar incurrir en gastos de consumo de energía eléctrica.

La disponibilidad de la persona (agente de ventas) en una empresa comercial es bien importante, muchas veces sucede que el operador no está en su puesto para atender la llamada de un cliente, al no ubicar al agente, como consecuencia, se puede estar perdiendo la llamada definitiva que cerrará una negociación o una orden de compra de uno de los mejores clientes, también se podría dar el caso de que simplemente el potencial cliente en la línea se cansó de esperar y molesto se va a otro proveedor. De la mano con la movilidad al disponer el empleado del servicio de telefonía institucional en su propio dispositivo va a ser contactado de manera más fácil y va a poder atender al cliente mientras se relaja caminando por la oficina, mejorando la eficiencia y productividad de los trabajadores.

10. CONCLUSIONES Y RECOMENDACIONES.

10.1. Conclusiones

Una vez llegado al término del desarrollo del presente caso podemos concluir que:

- Dentro una red inalámbrica de área local WLAN típica, el tráfico que fluye por ella no hace ninguna distinción del tipo por consiguiente no se prioriza y todos los paquetes reciben un trato igual o conocido como "best-effort", pero al implementarse el uso de comunicaciones unificas en la red, el servicio de telefonía necesita un tratamiento especial, para poder mantener una comunicación adecuada es necesario identificar los paquetes que pertenecen al tráfico de voz y asignarles un nivel de prioridad para mantener los parámetros sensibles como retardo, jitter, y pérdidas dentro de límites pre-establecidos, esto se consigue con la aplicación de políticas de calidad de servicio QoS

- Para tener un control eficiente del tráfico a nivel de la red, se ha segmentado la misma en dos redes virtuales (VLANs) a nivel de switches, la primera para el tráfico de red no sensible como web, base de datos; y la segunda para el tráfico de voz, estas mismas redes virtuales también han sido replicadas en el AP en dos SSIDs diferentes.

- Los equipos de conmutación o switches de acceso realizan la clasificación y marcado de los paquetes para toda la VLAN de voz en base a criterios de: IP Precedence = 5, DSCP = 46, el servidor de telefonía clasifica y marca los paquetes de audio como EF equivalente al DSCP = 46; en base a esta clasificación el AP asigna un valor al campo CoS = 6 para proveer una latencia < 10 ms. La clasificación y marcado de paquetes de telefonía se hace en los switches, mientras que en los APs solamente se asignan prioridades basadas en la clasificación previa.

- Para el presente proyecto en particular, debido a que mientras el usuario utiliza su dispositivo en una llamada VoIP no va a generar tráfico de datos (o va a ser mínimo) que requieran contención, será suficiente con la aplicación de QoS en el AP. La implementación de Calidad de Servicio en una red inalámbrica de área local (WLAN) se lleva a cabo solo en el sentido desde el AP hasta el dispositivo móvil, porque es el equipo que controla las conexiones de las estaciones cliente y se encarga de poner en el medio la información de acuerdo a la prioridad de categoría de acceso (CA) proveniente de la red cableada.

- De la observación de los resultados obtenidos para las muestras de la red sin QoS se puede determinar que la principal causa para que una llamada telefónica no tenga una calidad aceptable es la pérdida de paquetes cuyo valor superior al 1% dará lugar a defectos en la llamada, al mismo tiempo los parámetros como jitter o retardo se han mantenido dentro del rango permitido; en casos muy particulares se han encontrado pérdida de paquetes y retardo elevado simultáneamente como causantes de una mala calidad de voz. La percepción del usuario en una llamada con pérdidas es la de voz entre cortada. Con esto se puede asegurar con una certeza del 95% que al utilizar el servicio de telefonía IP en una red inalámbrica sin QoS la probabilidad de tener llamadas de voz de pésima calidad está en el rango de entre el 41% y 75%, haciendo a este tipo de redes inadecuado para soportar aplicaciones de tiempo real

como la telefonía IP. Para mitigar este inconveniente es necesario utilizar equipos que permitan la implementación de mecanismos de QoS inalámbrico.

- Una vez que se han aplicado los mecanismos de QoS en el Access Point, se puede afirmar con una certeza del 95% que la probabilidad de que las llamadas de voz se desarrollarán con normalidad está en el rango del 85% y 100%; en contraste con las redes inalámbricas sin QoS, las comunicaciones han mejorado significativamente. Un punto importante a considerar en una red inalámbrica con QoS, es que si bien la calidad de las comunicaciones ha mejorado, el parámetro de pérdida de paquetes en un 35% de las muestras no es nulo pero si inferior al límite del 1% que hace que las conversaciones telefónicas fluyan con normalidad.

- La aplicación de esta solución va enfocada principalmente a pequeñas y medianas empresas comerciales donde el presupuesto no les permite el despliegue de una infraestructura con equipos y personal dedicados para dar soporte a determinadas aplicaciones, con un bajo costo total de propiedad se puede mejor la productividad de los empleados, al mismo tiempo la movilidad de los usuarios hace posible que puedan utilizar sus propios dispositivos y no estar atados a puestos fijos.

- Desde el punto de vista comercial, para los integradores o vendedores de tecnología, ofrecer soluciones de acceso a la telefonía IP desde dispositivos propios del empleado y que se enmarque en los objetivos del negocio, representa una oportunidad para proveer valor agregado a los servicios que se ofertan.

10.2. Recomendaciones

- Antes de implementar este tipo de soluciones es conveniente dimensionar las capacidades de los equipos en función de los usuarios que accederán a la infraestructura, puesto que si sobrepasamos la capacidad podrían presentarse problemas a muy corto plazo que requieran de manera obligatoria inversión en nuevo equipamiento.

- La cantidad y ubicación de los puntos de acceso inalámbrico va a depender de las características físicas de la edificación, por lo tanto si esta red ofrecerá también servicio de telefonía IP se debe procurar que los niveles de señal en los dispositivos móviles sea de al menos -65 dbi, la cantidad y ubicación pueden resultar difícil de determinar a través de un “site survey” lo que hace necesario la utilización de herramientas de software que facilitan la tarea de diseño como es el caso de Ekahau Site Survey.

- Se podría analizar el comportamiento de la red de acuerdo al porcentaje de pérdida de paquetes, empleando códecs con mayor compresión de ancho de banda como G.729 o GSM, para lo cual es necesario adquirir los derechos de uso por un costo adicional. El códec utilizado en el proyecto es el G.711 que presenta mejor calidad de la voz a costa de utilizar un mayor ancho de banda; es el códec habilitado tanto en la central IP PBX como en los terminales móviles por defecto.

- Cuando se trabaja con aplicaciones de tiempo real no es suficiente con disponer del ancho de banda acorde a las necesidades. Un sistema que deba transmitir datos sensibles, como voz o video, debe implementar necesariamente QoS.

- El presente trabajo ha sido desarrollado para implementaciones donde la necesidad de acceso inalámbrico ha sido cubierto con un equipo AP, para implementaciones que requieran dos o más equipos se debería analizar la QoS de la red considerando el roaming durante la movilidad y así reducir su impacto.

11. BIBLIOGRAFÍA

Andrade, J. (2012). *ESTUDIO TÉCNICO DE UNA RED SATELITAL QUE BRINDE SOPORTE A SERVICIOS DE VOIP"*.

Asterisk. (2014, marzo). *IP Quality of Service - Asterisk Project*. Retrieved from https://wiki.asterisk.org/wiki/display/AST/IP+Quality+of+Service/

Bakin, D. (2007, mayo). *Evolution of 802.11 (physical layer)*. Retrieved from HTTPS://WWW.OKOB.NET/TEXTS/MYDOCUMENTS/80211PHYSLAYER/

Carroll, B. (2008). *CCNA Wireless Official Exam Certification Guide (CCNA IUWNE 640-721)*. Cisco Press.

CCM Benchmark. (2015, Noviembre). *WiMAX - 802.16 - Interoperabilidad mundial para acceso por micro*. Retrieved from CCM: http://es.ccm.net/contents/795-wimax-802-16-interoperabilidad-mundial-para-acceso-por-micro

Cisco Systems. (2008, mayo). *Voz : Calidad de voz*. Retrieved from Voz sobre IP - Consumo de ancho de banda por llamada.

Cisco Systems. (2010, Enero). *Voice over Wireless LAN 4.1 Desing Guide*. Retrieved from http://www.cisco.com/c/en/us/td/docs/.../vowlan/41dg/vowlan41dg-book.pdf

Cisco Systems. (2012, Octubre). *Quality of Service Networking*. Retrieved from http://docwiki.cisco.com/: http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

Cisco Systems. (2013). *802.11ac: The Fifth Generation of Wi-Fi Technical White Paper*. Retrieved from http://www.cisco.com/en/us/prod/collateral/wireless/ps5678/ps11983/white_paper_c11-713103.html

Cisco Systems. (2014, Julio). *BYOD Smart Solution*. Retrieved from www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Solution_Overview.pdf

Cisco Systems. (2015). *Cisco Aironet 1600 Series*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html

Cisco Systems. (n.d.). *FCC Regulations Update*. Retrieved from Cisco Aironet 1300 Series: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/prod_white_paper0900aecd801c4a88.html

COUNTERPATH. (2016). *The Bria Android SIP*. Retrieved from http://www.counterpath.com/bria-android-edition/

Cruz, M., & Martinez, R. (2013, marzo). *Análisis de la QoS en redes inalámbricas.* Retrieved from Revista Cubana de Ciencias Informáticas: http://scielo.sld.cu/scielo.php?pid=S2227-18992013000100010&script=sci_arttext

CSipSimple. (2015). *CSipSimple Softphone.* Retrieved from https://play.google.com/STORE/APPS/DETAILS?ID=COM.CSIPSIMPLE&HL=ES_419

Donovan, J. (2013, febrero). *Is 5 GHz the Promised Land for Embedded Wireless Applications?* Retrieved from http://www.digikey.com/en/articles/techzone/2013/feb/is-5-ghz-the-promised-land-for-embedded-wireless-applications

Elastix. (2015). *Elastix - overview.* Retrieved from http://www.elastix.org/index.php/es/informacion-del-producto/informacion.html

Elastixtech. (2013, Mayo). *Conceptos de VoIP y telefonía IP: Protocolo SIP*. Retrieved from http://elastixtech.com/protocolo-sip/

Feedback Netoworks. (2013). *Calcular la muestra correcta*. Retrieved from http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.html

Feedback Networks. (n.d.). *Calcular la muestra correcta*. Retrieved from http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.html

Felici, S. (2010, enero). *Evaluación de los mecanismos de QoS en routers para servicio multimedia.* Retrieved from http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

IEEE. (2005, Noviembre). *IEEE 802.11e - Amendment 8: Medium Access Control (MAC) Quality of Service enhancements.* Retrieved from http://ieeexplore.ieee.org/servlet/opac?punumber=10328

INEC. (2015, Agosto). *Directorio de Empresas y Establecimientos 2014.* Retrieved from http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/Empresas_2014/Principales_Resultados_DIEE_2014.pdf

Info Tech plus. (n.d.). *La couche Physique (C1).* Retrieved from http://infotechplus.free.fr/couche_ph.inc.php

Jerome, H. (2013). *CCNA Wireless 640-722 IUWNE Quick Reference.* Cisco Press.

Kioskea.net. (n.d.). *Modos de funcionamiento WIFI (802.11 o wi-fi)*. Retrieved from http://es.kioskea.net/contents/791-modos-de-funcionamiento-wifi-802-11-o-wi-fi

Kuthan, J., & Sisalem, D. (2007, Marzo). *SIP: More Than You Ever Wanted To Know About.* Retrieved from VoIP Mechanic: www.voipmechanic.com/documents/sip_tutorial.pdf

Landivar, E. (2008). *Comunicaciones Unificadas con Elastix vol. 1.* Guayaquil.

Méndez, G., & Gaviria, J. (2006). *Evaluación experimental de la capacidad de IEEE 802.11b para soporte de VoIP.* Retrieved from Universidad del Cauca.

Mérida, I. (2012, febrero). *TEOREMA DEL MUESTREO DE NYSQUIST.* Retrieved from https://2010301400isaacmerida.wordpress.com/tag/teorema-del-muestreo-de-nysquist/

Nayanajith, R. (2012, Noviembre). *My CCIE Wireless Journey & More.* Retrieved from http://mrncciew.com/2012/11/30/wireless-packet-capture-free-tool/

Nayanajith, R. (2013, Marzo). *My CCIE Wireless Journey.* Retrieved from Autonomous AP – QoS: http://mrncciew.com/2013/03/09/autonomous-ap-qos/

Nefta, A. (2013, Mayo). *Fundamentos de telefonía: VoIP – telefonía IP*. Retrieved from elastixtech.com: http://elastixtech.com/fundamentos-de-telefonia/voip-telefonia-ip/

Nóvoa, F. (2012, Noviembre). Fundamentos de telefonía IP con tecnología Cisco. Galicia, Espana.

Pham, C. (2012, mayo). *Fundamentals of Quality of Service.* Retrieved from http://cpham.perso.univ-pau.fr/ENSEIGNEMENT/UERHD/05-QoS_Scheduling.pdf

Prunosa, J. (2012, Septiembre). *Intervalos de confianza y contraste de hipotesis.* Retrieved from http://es.slideshare.net/prunogabi/intervalos-de-confianza-y-pruebas-de-hiptesis-14284291

Rajesh, S. (2006, Abril). *IEEE 802.11e WLANs / WMM.* Retrieved from http://madwifi-project.org/attachment/wiki/chipsetfeatures/wmm/qos11e.pdf

Ramos, F. (2015). *Artículo: Pérdidas en obstáculos*. Retrieved from http://www.radioenlaces.es/articulos/perdidas-en-obstaculos/

Robles, M. (2008). *QoS en redes wireless con IPv6.* Retrieved from http://sedici.unlp.edu.ar/handle/10915/4149

Rodriguez, A. (2015, Septiembre). *Standar IEEE 802.15.* Retrieved from https://prezi.com/ixprrbbvawhz/standar-ieee-80215/

Rojano, E. (2013, julio). *Los 6 softphones SIP más recomendados para Android*. Retrieved from HTTPS://WWW.SINOLOGIC.NET/BLOG/2013-07/6-SOFTPHONES-RECOMENDADOS-PARA-ANDROID.HTML

Simsek, B., & Wolter, k. (2006). *Improving the Performance of IEEE 802.11e with an Advanced Scheduling Heuristic.* Retrieved from http://page.mi.fu-berlin.de/katinkaw/.../epew06b.pdf

Smith, G., & Group, D. (2008, noviembre). *802.11 QoS Tutorial.* Retrieved from HTTP://WWW.IEEE802.ORG/1/FILES/PUBLIC/DOCS2008/AVB-GS-802-11-QOS-TUTORIAL-1108.PDF

TUTORIAL TELECOM. (2014). *Introducción al protocolo SIP*. Retrieved from http://www.tutorialtelecom.com/artic_es/sip/sip.html

Ubeda, J., & Wikipedia. (2014, Junio). *BYOD*. Retrieved from http://es.wikipedia.org/wiki/BYOD

VoIP foro. (2012, Mayo). *QoS Quality of service VOIP: Jitter, Foro de telefonía IP*. Retrieved from http://www.voipforo.com/QoS/QoS_Jitter.php

VoIP Foro. (2012, Mayo). *QoS Quality of Service VoIP: Latencia, Foro de telefonía IP*. Retrieved from http://www.voipforo.com/QoS/QoS_Latencia.php

VoIP foro. (2012, Mayo). *QoS Quality of service VOIP: Perdida de paquetes, Foro de telefonía IP*. Retrieved from http://www.voipforo.com/QoS/QoS_PacketLoss.php

VOIP-info.org. (2011, Enero). *QoS*. Retrieved from http://www.voip-info.org/wiki/view/QoS

Wi-Fi Alliance. (2008). *Voice Personal white paper,*. Retrieved from https://www.wi-fi.org/file/delivering-the-best-user-experience-with-voice-over-wi-fi-2008

Wi-fi Alliance. (2012). *Voice Enterprise White paper*. Retrieved from https://www.wi-fi.org/file/wi-fi-certified-voice-enterprise-delivering-wi-fi-voice-to-the-enterprise-2012

Yang, M.-H. (2006, octubre). *IEEE 802.11e QoS on WLANs*. Retrieved from HTTP://WWW.DOCSTOC.COM/DOCS/84960443/IEEE-80211E-QOS-ON-WLANS

Yang, R. (2012, Agosto). *802.11 standard*. Retrieved from http://www3.cs.stonybrook.edu/~jgao/CSE370-spring10/80211.pdf

ZOIPER. (2015). *Pagina principal: ZoiPer*. Retrieved from http://www.zoiper.com/

12. ACRÓNIMOS.

Access Category (AC)

Access Point (AP)

Acknowledge (ACK)

Adaptive Differential Pulse Code Modulation (ADPCM)

Algebraic Code-Excited Linear Prediction (ACELP)

American Standard Code for Information Interchange (ASCII)

Analog Telephony Adapter (ATA)

Arbitration Interframe Space (AIFS)

Basic Rate Interface (BRI)

Basic Service Set (BSS)

Basic Service Set Identifier (BSSID)

Basic Services Area (BSA)

Bring Your Own Device (BYOD)

Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)

Circuito Cerrado de Televisión (CCTV)

Class of Service (CoS)

Class-based Weighted Fair Queuing (CBWFQ)

Commited Access Rate (CAR)

Complementary Code Keying (CCK)

Complementary Code Keying (CCK)

Contention Period (CP)

Contention Window (CW)

Custom Queuing (CQ)

Destination Address (DA)

Differential Phase Shift Keying (DPSK)

Differential Quadrature Phase Keying (DQPSK)

Digital Signal proccesor (DSP)

Direct Sequense Spread Spectrum (DSSS)

Distributed Coordination Function (DCF)

Distributed coordination function (DCF)

Distributed Interframe Space (DIFS)

Distribution Sysytem (DS)

Enhanced Distributed Channel Access (EDCA)

Extended Service Set (ESS)

eXtensible Markup Language (XML)

Extensible Messaging and Presence Protocol (XMPP)

Federal Communications Commission (FCC)

First In, First out (FIFO)

Flow-based Weighted Fair Queuing (WFQ)

Foreing eXchange Office (FXO)

Foreing eXchange Subscriber (FXS)

Frame Control Sequence (FCS)

Frequecy Shift Keying (FSK)

Frequency Hop Spread Spectrum (FHSS)

Generic Traffic Shapping (GTS)

Giga bit por segundo (Gbps)

Global System for Mobile communications (GSM)

HCF Controlled Channel Access (HCCA)

High Definition (HD)

High-Level Data Link Control (HDLC)

Hybrid Coordinated Function Controlled Channel Access (HCCCA)

Hypertext Transfer Protocol (HTTP)

Independent Basic Service Set (IBSS)

Industrial, Scientific, Medical (ISM)

Institute of Electrical and Electronics Engineers (IEEE)

Inter Asterisk eXchange (IAX)

International Telecommunications Union (ITU)

Internet Engineering Task Force (IETF)

Internet Protocol (IP)

Internet Service Provider (ISP)

Level Service Agreements (LSA)

Link Fragmentation Interleaving (LFI)

Local Area Network (LAN)

Low Latency Queuing (LLQ)

MAC Service Data Unit (MSDU)

Mean Opinion Score (MOS)

Media Access Control (MAC)

Media Gateway Control Protocol (MGCP)

Mega bits por segundo (Mbps)

Multi Ratio Combining (MRC)

Multi User MIMO (MU-MIMO)

Multiple Basic Service Set Identifier (MBSSID)

Multiple Input Multiple Output (MIMO)

Multipoint Control Unit (MCU)

Network Address Translation (NAT)

Network Allocation Vector (NAV)

Oficina Central (OC)

Open System Interconnection (OSI)

Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency Division Multiplexing (OFDM)

PCF Interframe Space (PIFS)

Pequena y mediana empresa (Pyme)

Point coordination function (PCF)

Point to Point Protocol (PPP)

Primary Rate Interface (PRI)

Priority Queuing (PQ)

Pulse Code Modulation (PCM)

QoS Station (QSTA)

Quadrature Amplitude Modulation (QAM)

Quadrature Amplitude Modulation (QAM)

Quality of Service (QoS)

Radio Frequency (RF)

Random early detection (RED)

Real –Time Transport Protocol (RTP)

Receiver Address (RA)

Reduced Interframe Space (RIFS)

Request to Send/ Clear to Send (RTS/CTS)

RTP Control Protocol (RTCP)

Service Set Identifier (SSID)

Session Description Protocol (SDP)

Session Initiation Protocol (SIP)

Short Interframe Space (SIFS)

Short Inter-Frame Space (SIFS)

Short Message Service (SMS)

Simple Mail Transfer Protocol (SMTP)

Skinny Client Control Protocol (SCCP)

Small Office Home Office (SOHO)

Source Address (SA)

Station (STA)

Target Beacon Transition Time (TBTT)

Tecnologias de Información (TI)

The type of service (ToS)

Time Division Multiplexing (TDM)

Total Cost of Ownership (TCO

Traffic Especification (TSPEC)

Transmit Opportunity (TxOP)

Transmiter Address (TA)

Transport Control Protocol (TCP)

Transport Layer Security (TLS)

Unlicensed National Information Infraestructure (UNII)

Unshielded Twisted Pair (UTP)

User Agent (UA)

User Datagram protocol (UDP)

User Priority (UP)

Virtual Private Network (VPN)

Voice over Internet Protocol (VoIP)

Wi-Fi Multi Media (WMM)

Wired Equivalent Privacy (WEP)

Wireless Local Area Network (WLAN)

Wireless Metropolitan Area Network (WMAN)

Wireless Personal Area Network (WPAN)

Wireless Wide Area Network (WMAN)

Wireless Workgroup Bridege (WGB)

13. ANEXOS

13.1. Configuración de QoS en AP.

Los pasos requeridos para la configuración de QoS en un AP de la familia Aironet de Cisco (en nuestro caso se ha utilizado el modelo AIR-SAP1602I-A-K9) son los siguientes:

a. Creación de un mapa de clase utilizando el comando de **class-map** y los comandos de asociación **match**, que comprenden un conjunto de criterios de coincidencia relacionadas a clasificaciones de tráfico.

```
class-map match-all _class_AP1-QoS0
 match ip dscp ef
class-map match-all _class_AP1-QoS1
 match ip precedence 5
```

_class_AP1-QoS0 & _class_AP1-QoS1: son los nombres que hemos definido para cada clase.

***match** ip dscp ef*: asocia el tráfico marcado previamente (recordemos que el AP no lo hace) por los routers o switches, para este caso en el campo DSCP con el valor ef.

***match** ip precedence 5:* asocia el tráfico marcado previamente, para este caso en el campo CoS con el valor 5.

Si se requiere que múltiples criterios de coincidencia pertenezcan a una misma clase en lugar de la palabra clave **match-all** se debería utilizar **match-any**.

b. Creación de un mapa de política con el comando **policy-map**, que hace referencia a los mapas de clase e identifica una serie de acciones a realizar en base a los criterios de coincidencia de tráfico.

```
policy-map AP1-QoS
 class _class_AP1-QoS0
  set cos 6
```

AP1-QoS: es el nombre que le hemos dado al mapa de política.

class _class_AP1-QoS0: hacemos referencia por su nombre al mapa de clase creado anteriormente.

set cos 6, "Set CoS" es la única acción permitida en los AP, en este caso el valor 6 corresponde a la prioridad (UP) especificada en el estándar 802.11e

c. Activar el mapa de política y vincularlo a una interfaz específica con el comando **service-policy** donde se va a filtrar el tráfico.

```
interface Dot11Radio0.5
 service-policy output AP1-QoS
```

Dot11Radio0.5: es la interface de radio donde estamos aplicando el servicio.

service-policy output AP1-QoS: la palabra clave **output** indica el sentido de tráfico desde el radio del AP hasta el radio del cliente, este es el único sentido aplicable para APs Autonomos Cisco.

Los valores de categoría de acceso pueden ser modificados desde sus valores por defecto dependiendo de las necesidades QoS en el entorno, por ejemplo para la optimización de QoS con el tráfico de voz, es necesario reducir a cero el valor del parámetro de oportunidad de transmitir y reducir al máximo el umbral superior de la ventana de contención.

```
dot11 qos class voice local
  cw-max 4
  transmit-op 0
```

Debemos tener en cuenta que los valores de las categorías de acceso restantes (video, best-effort, background) deberían ser ajustadas para no degradar el rendimiento de la red.

```
dot11 qos class background local
  cw-min 6
  fixed-slot 10
!
dot11 qos class video local
  cw-max 5
   fixed-slot 3
  transmit-op 0
!
```

Los valores por defecto de las categorías de acceso (Cisco Systems, 2010) son las que se indican en la tabla 27.

Tabla 27. Valores por defecto Categorías de Acceso QoS inalámbrico.

Clase de servicio (AC)	CW min	CW max	Ranura de tiempo fija	TXOP
Background	4	10	6	0
Best effort	4	10	2	0
Video retardo < 100ms	3	2	1	3008
Voz retardo < 100ms	2	3	1	1504

Autor: Jose Chauca

13.2 Captura de paquetes en entornos inalámbricos.

Una de las herramientas bastante útiles para la solución de problemas de redes de datos es Wireshark, que nos ayuda con la captura de paquetes en determinada interface para su posterior análisis. Si se intenta capturar el tráfico inalámbrico seleccionando la interfaz inalámbrica en Wireshark, no se va a capturar con precisión los paquetes inalámbricos a través del aire. Normalmente se requiere de un adaptador inalámbrico por separado para hacer este tipo de trabajo (Nayanajith, My CCIE Wireless Journey & More, 2012).

Para este caso nos valemos de la herramienta "Microsoft Network Monitor" que ha sido desarrollado por Microsoft y se la puede descargar sin costo desde el siguiente enlace: http://www.microsoft.com/en-us/download/details.aspx?id=4865, y es soportado por la mayoría de sistemas operativos Windows.

Al utilizar esta herramienta se va a capturar todo el tráfico que el adaptador inalámbrico puede escuchar en determinado canal, no solamente en tráfico que recibe la interface; los pasos a seguir para la adecuada configuración posterior a la instalación son los siguientes:

En la pantalla inicial seleccionamos la opción "Capture Settings" para abrir la ventana de configuración (Figura 64).

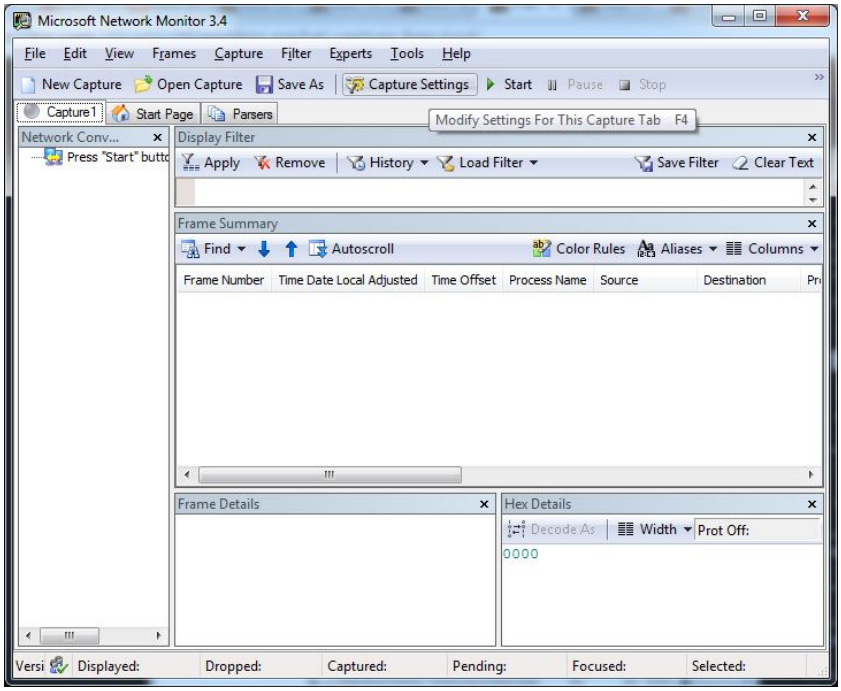


Figura 64. Seleccionar la opción "Capture Settings".

En la ventana de configuración (figura 65) nos muestra todas las interfaces disponibles en el equipo donde se ha instalado el software de captura de paquetes, debemos seleccionar el adaptador inalámbrico y abrir la ventana de propiedades.

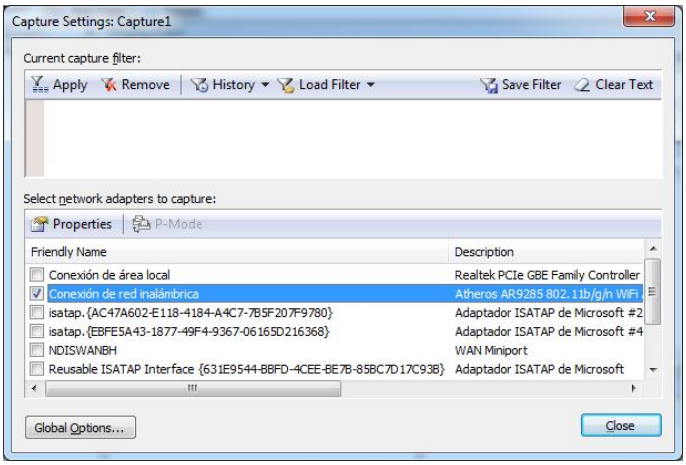


Figura 65. Seleccionar el adaptador inalámbrico. (Captura realizada por José Chauca)

En la ventana de propiedades del adaptador abrimos la ventana de opciones de escaneo para definir de manera más precisa los parámetros inalámbricos con los que se va a trabajar (figura 66).

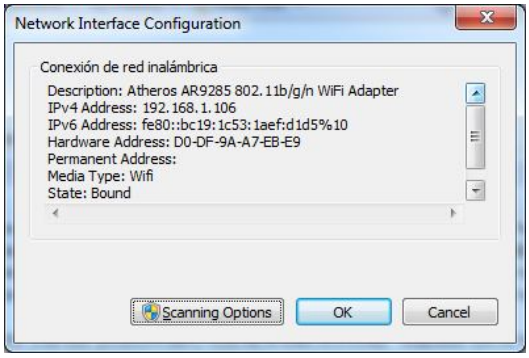


Figura 66. Propiedades del adaptador de red. (Captura realizada por José Chauca)

En las opciones de escaneo inalámbrico (figura 67) podemos seleccionar de dos posibilidades de búsqueda, la primera seleccionando el estándar y el canal, sólo uno, con el que trabajaremos y la segunda seleccionando varios estándares y canales para trabajar al mismo tiempo. La que nos interesa es la primera opción, puesto que necesitamos la captura de paquetes de un canal en particular por donde el tráfico de VoIP estará circulando, que canal elegir los podemos determinar de la configuración del AP. Al presionar el botón aplicar la interface se desconecta para el tráfico de datos de usuario y está lista para captura de paquetes. Para desactiva el modo promiscuo y habilitar el tráfico normal debemos seleccionar el botón “Cerrar y volver a modo local”

Una vez configurada la interface, haciendo clic en el botón “Start” iniciamos la captura de paquetes hasta que lo detengamos con el botón “Stop”. Con la información recogida podemos empezar nuestro análisis (figura 68). El archivo que generemos también se puede abrir con la aplicación Wireshark.

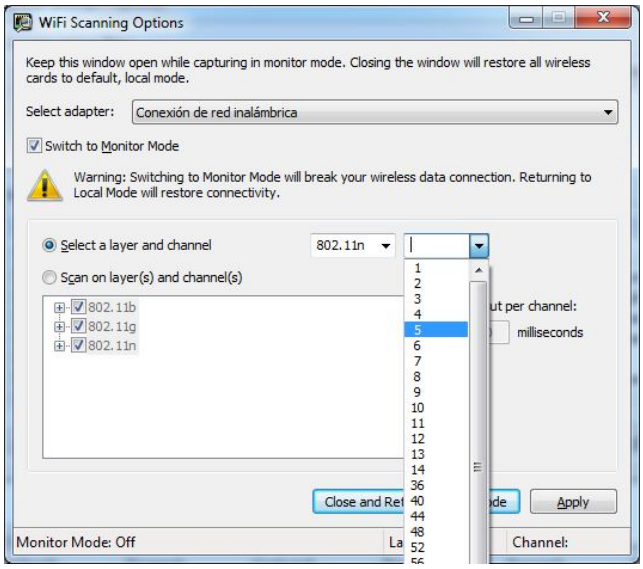


Figura 67. Selección del canal de operación de la red inalámbrica. (Captura realizada por José Chauca)

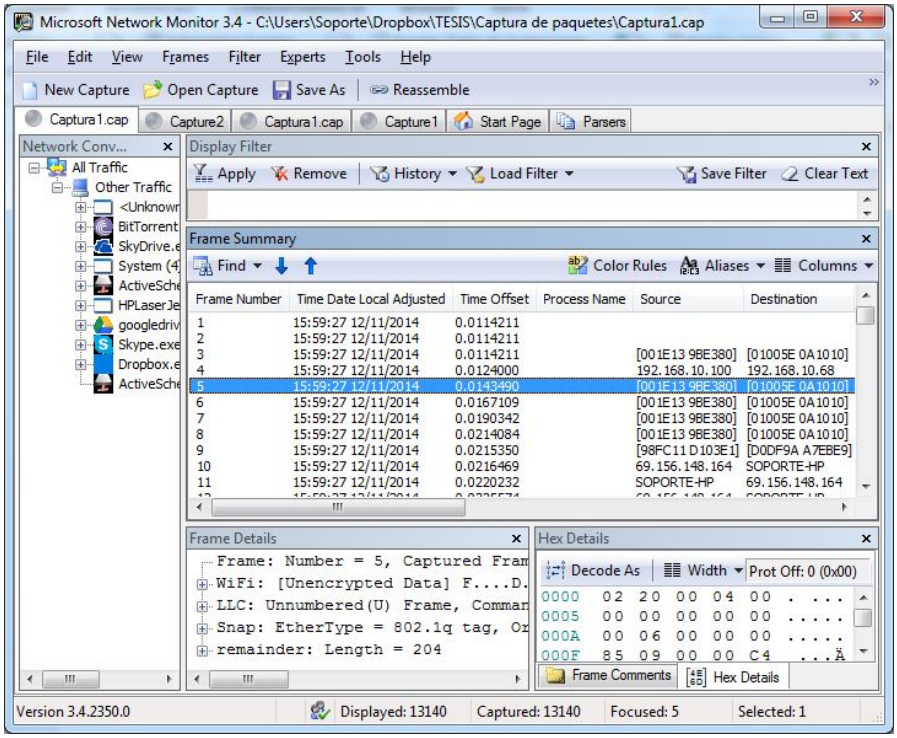


Figura 68. Datos capturados. (Captura realizada por José Chauca)

13.3. Archivo de configuración del AP utilizado en el proyecto.

```
hostname AP-OFI
!
!
logging rate-limit console 9
enable secret 5 $1$jJxF$NidOJgRA3gz2Dbi9qapHQ1
!
no aaa new-model
no ip routing
no ip cef
!
!
!
dot11 syslog
dot11 vlan-name Nativa vlan 1
 dot11 vlan-name Telefonia vlan 5
!
dot11 ssid Autelcom2
   vlan 1
   authentication open
   authentication key-management wpa version 2
   guest-mode
   mbssid guest-mode
   wpa-psk ascii 7 070A224D5B1D1A0814110A
   information-element ssidl advertisement
!
dot11 ssid voip
   vlan 5
   authentication open
   mbssid guest-mode
   information-element ssidl advertisement wps
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 062506324F41
!
 !
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
 !
 encryption vlan 1 mode ciphers aes-ccm tkip
 !
 ssid Autelcom2
 !
 ssid voip
```

```
 !
 antenna gain 0
 stbc
 beamform ofdm
 mbssid
 channel 2462
 station-role root
 !
 interface Dot11Radio0.1
  encapsulation dot1Q 1 native
  no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.5
 encapsulation dot1Q 5
 no ip route-cache
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
  encryption mode ciphers tkip
 !
 encryption vlan 1 mode ciphers aes-ccm tkip
 !
 ssid Autelcom2
 !
 antenna gain 0
 dfs band 3 block
 stbc
 channel dfs
 station-role root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.5
```

```
  encapsulation dot1Q 5
 no ip route-cache
 bridge-group 5
 bridge-group 5 subscriber-loop-control
 bridge-group 5 spanning-disabled
 bridge-group 5 block-unknown-source
 no bridge-group 5 source-learning
 no bridge-group 5 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.5
  encapsulation dot1Q 5
 no ip route-cache
 bridge-group 5
 bridge-group 5 spanning-disabled
 no bridge-group 5 source-learning
!
interface BVI1
 ip address 192.168.10.220 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.10.1
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
snmp-server view dot11view ieee802dot11 included
snmp-server community public view dot11view RO
snmp-server location OFICINA
snmp-server contact Jose Chauca
snmp-server chassis-id AP-MAIN
snmp-server enable traps dot11-qos
snmp-server enable traps syslog
 snmp-server host 192.168.10.148 public  dot11-qos syslog
bridge 1 route ip
!
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```