# CONSIDERACIONES PARA LA IMPLEMENTACION DE VOZ SOBRE IP EN REDES INALAMBRICAS

**JUAN GUILLERMO PÉREZ SARMIENTO**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER**

**ESPECIALIZACION EN TELECOMUNICACIONES**

**FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS**

**ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES**

**BUCARAMANGA**

**2008**

# CONSIDERACIONES PARA LA IMPLEMENTACION DE VOZ SOBRE IP EN REDES INALAMBRICAS

**JUAN GUILLERMO PÉREZ SARMIENTO**

**Proyecto de grado para optar el título de Especialista en Telecomunicaciones**

**DIRECTOR**

**SAMUEL GONZALO PINZON BARRIOS**

**Magíster**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER**

**ESPECIALIZACION EN TELECOMUNICACIONES**

**FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS**

**ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES**

**BUCARAMANGA**

**2008**

# LISTA DE CONTENIDO


**0. INTRODUCCIÓN ..... 1**

**1. TECNOLOGÍA VOIP Y REDES INALAMBRICAS ..... 3**

1.1 VOZ SOBRE IP - VOIP ..... 3

*1.1.1 ARQUITECTURA DE RED VoIP ..... 3*

*1.1.2 PROTOCOLOS DE VoIP ..... 6*

*1.1.3 CODECS ..... 9*

1.2 REDES INALAMBRICAS ..... 9

*1.2.1 IEEE 802.11a ..... 11*

*1.2.2 IEEE 802.11b ..... 11*

*1.2.3 IEEE 802.11g ..... 12*

*1.2.4 IEEE 802.11n ..... 12*

*1.2.5 ARQUITECTURA DE RED ..... 13*

*1.2.6 SEGURIDAD EN REDES INALAMBRICAS ..... 14*

**2. CARACTERÍSTICAS DE DESEMPEÑO PARA VOIP EN REDES INALÁMBRICAS ..... 18**

2.1 CONSIDERACIONES GENERALES ..... 18

2.2 PARÁMETROS DE RELEVANCIA PARA LA CALIDAD DEL SERVICIO EN VOIP ..... 19

*2.2.1 Disponibilidad ..... 19*

*2.2.2 Ancho de Banda y Tasa de Bits ..... 19*

*2.2.3 Retardo de Propagación ó Latencia ..... 20*

*2.2.4 Variación del Retardo ó Jitter ..... 22*

*2.2.5 Pérdida de Paquetes ..... 23*

*2.2.6 Fidelidad de voz ..... 23*

2.3 TÉCNICAS IMPLEMENTADAS PARA OBTENER QOS EN REDES IP ..... 24

*2.3.1 Marcación y clasificación del tráfico ..... 24*

*2.3.2 Virtual LAN (VLAN) ..... 26*

*2.3.3 Redes Privadas Virtuales ( Virtual Private Networks VPNs) ..... 27*

2.4 PARÁMETROS DE RELEVANCIA PARA QOS EN REDES INALÁMBRICAS ..... 28

*2.4.1 Handover o roaming ..... 28*

*2.4.2 Celda ..... 29*

*2.4.3 Cobertura de una celda ..... 29*

*2.4.4 Modelo de pérdidas de propagación ..... 29*

*2.4.5 Carga de Tráfico ofrecido ..... 29*

*2.4.6 Capacidad ..... 29*

*2.4.7 Throughput ..... 30*

*2.4.8 Interferencias ..... 30*

*2.4.9 Funcionamiento Capa MAC ..... 30*

2.5 CALIDAD DE SERVICIO EN REDES INALÁMBRICAS - 802.11E ..... 31

**3. CONSIDERACIONES PARA IMPLEMENTAR VOIP EN REDES INALÁMBRICAS ..... 33**

3.1 SELECCIÓN DEL SISTEMA INALÁMBRICO ..... 33

3.2 PLANEACIÓN DE LA RED INALÁMBRICA ..... 34
3.3 CALIDAD DE LA VOZ ..... 40
3.4 APLICACIONES DE SEGURIDAD ..... 42
3.5 SERVICIO DE VOZ SIN INTERRUPCIONES ..... 43
3.6 CONSUMO DE POTENCIA ..... 44
3.7 TERMINALES VOIP PARA WI-FI ..... 44
3.8 CASOS DE ESTUDIO ..... 45

**4. CONCLUSIONES ..... 48**

**5. BIBLIOGRAFÍA ..... 50**

# LISTA DE FIGURAS

***Figura 1*** *Funcionamiento de VoIP* ..... *3*
***Figura 2*** *Arquitectura de una red VoIP* ..... *5*
***Figura 3*** *Estándar H.323* ..... *6*
***Figura 4*** *Máximo número de canales sin interferencia cocanal* ..... *12*
***Figura 5*** *Throughput como función del número de estaciones y tasa de datos para 802.11a/g* ..... *36*
***Figura 6*** *Distribucion de Puntos de Acceso con cobertura completa.* ..... *38*

# LISTA DE TABLAS

***Tabla 1*** *Protocolos más significativos para H.323.* .....7
***Tabla 2*** *Codecs*.....9
***Tabla 3.*** *Comparación de los estándares 802.11* .....13
***Tabla 4*** *Retardo de serialización como función de la velocidad de enlace y tamaño del paquete.*.....22
***Tabla 5.*** *Número de usuarios que puede soportar un AP 802.11g como función del throughput por usuario, longitud de trama de 1500 Bytes, todas las STA trabajando a igual velocidad.* .....36

## *RESUMEN*

***TITULO.***

*CONSIDERACIONES PARA LA IMPLEMENTACION DE VOZ SOBRE IP EN REDES INALAMBRICAS* *

***AUTOR.***

*PÉREZ SARMIENTO, Juan Guillermo.* **

***PALABRAS CLAVES***

*Voz sobre IP, Redes Inalámbricas, 802.11, calidad de servicio, latencia.*

***DESCRIPCIÓN***

Este trabajo recopila información sobre protocolos de redes inalámbricas locales, mecanismos de calidad de servicio y Voz sobre IP con el fin de brindar una documentación apropiada que sirva en el momento de diseñar o implementar VoIP sobre una red inalámbrica.

El proyecto tiene por objeto la documentar los requerimientos necesarios para la implementación satisfactoria de la tecnología de Voz sobre IP en redes inalámbricas Wi-Fi.

Inicialmente se define la tecnología de Voz sobre IP, los elementos que hacen parte de su arquitectura de red y los protocolos asociados a VoIP, de igual forma se plantean las generalidades de los estándares en redes inalámbricas, como son cubrimiento de la red, disponibilidad de los canales de frecuencia a utilizar, el ancho de banda y la seguridad ofrecida en estas redes, posteriormente se presentan las características fundamentales en el desempeño de una red de VoIP que afectan la Calidad de Servicio (QoS), tales como: Latencia, Jitter, pérdida de paquetes y calidad de voz.

Una vez realizada la documentación de las dos tecnologías se realiza una recopilación de todas las consideraciones que se deben seguir al momento de implementar ambas tecnologías y que influyen en el rendimiento de la red.

Como resultado del estudio realizado al recopilar los factores determinantes en el buen diseño de una red inalámbrica que este en capacidad de prestar el servicio VoIP, se elige el estándar 802.11a como plataforma de la red inalámbrica, para asegurar una buena calidad de la voz se recomienda que los dispositivos inalámbricos cumplan con el estándar 802.11e e implementar prácticas que mejoren la seguridad de la WLAN.


---

* Proyecto de Grado

** Facultad de Ciencias Físico – Mecánicas. Ingeniería Electrónica e Ingeniería Eléctrica. Director Magister. Samuel Gonzalo Pinzón

## SUMMARY

**TITLE**

CONSIDERATIONS FOR IMPLEMENTATION OF VOICE OVER IP ON WIRELESS [*]

**AUTHOR**

PÉREZ SARMIENTO, Juan Guillermo[**].

**KEY WORDS**

Voice over IP, Wireless Network, 802.11, Quality of Service, Latency.

**DESCRIPTION**

This document compiles information about wireless LAN protocols, QoS mechanisms and voice over IP, with the purpose to present an appropriate documentation that can be used to design or implement VoIP over wireless network.

The project's objective is to define the main requirements for successfully implementation of VoIP technology over a wireless LAN network.

Initially the main elements that are part of VoIP network architecture and protocols associated with VoIP are defined. Also the wireless network standards are explained: network coverage, availability of frequency channels to use and security offered on these networks, subsequently presents the key features in the performance of a VoIP network that affect Quality of Service (QoS), such as latency, jitter, packet loss and voice quality.

After the documentation of both technologies, a compilation was made, including all the considerations that must be followed at the time of implementing both technologies and influencing the performance of the network.

As a conclusion after collecting requirements of a wireless network for providing the VoIP service, designers must choose the 802.11a standard for the wireless network platform. To ensure good quality of voice, it recommends that wireless devices have included the 802.11e standard and implemented practices that improve the security of the WLAN.


---

[*] Graduation Project

[**] Faculty of Engineering Physical-mechanics. Engineering Electronic. Dir. Mag. Samuel Gonzalo Pinzón

# 0. INTRODUCCIÓN

A raíz de la emergente necesidad de comunicación entre las personas, se ha producido un avance tecnológico en las últimas décadas que ha modificado profundamente las relaciones personales y profesionales.

Por un lado están las redes inalámbricas que surgen como una alternativa para solucionar problemas de flexibilidad, conectividad, ubicuidad, movilidad y facilidad en contraste con las redes cableadas convencionales. De otro lado y con igual importancia está la transmisión de Voz sobre IP, que como su nombre lo indica se trata de digitalizar y paquetizar la voz para transmitirla sobre la infraestructura de redes basadas en el protocolo de Internet (IP). Mediante la implementación de esta tecnología se ha logrado la prestación de más servicios sobre una misma plataforma ya que se integran voz con mejor calidad y datos en una misma red, alcanzando con ello una reducción en costos por concepto de mantenimiento de red y facturación de telefonía a larga distancia.

Hoy en día, consolidar el tráfico de voz sobre las redes inalámbricas es un reto de aplicación con gran valor para las compañías, debido a que la voz es una poderosa herramienta e implementarla sobre una plataforma móvil le da valor agregado a su funcionalidad. Por esta razón, la siguiente meta es conseguir una solución de voz inalámbrica que satisfaga los requerimientos de las empresas, para lo cual es necesario ofrecer redes con un desempeño óptimo y excelente interoperabilidad entre las tecnologías en mención.

Así, con el propósito de aprovechar satisfactoriamente los beneficios suministrados por voz sobre IP en redes inalámbricas es de imperiosa necesidad verificar que la infraestructura de red está preparada para soportar los requerimientos de dicha solución; por lo cual es importante contar con una documentación que ayude a identificar los requisitos fundamentales para lograr un diseño de red optimizado que permita la implementación sin posteriores problemas de aplicaciones de VoIP en redes inalámbricas.

Actualmente no se cuenta con un estudio que permita identificar problemas y soluciones al implantar VoIP en una red inalámbrica a fin de proteger la inversión de la compañía; por todo lo anterior, este trabajo está orientado a combinar los conocimientos sobre protocolos de redes inalámbricas locales, mecanismos de calidad de servicio y Voz sobre IP con el fin de brindar una documentación apropiada que sirva en el momento de diseñar o implementar VoIP sobre una red inalámbrica.

**Estructura del Libro**

El presente trabajo está organizado de manera que el lector pueda hacerse una visión general del estudio, para ello se dividen los temas tratados en tres capítulos descritos a continuación:

El primer capítulo define la tecnología de Voz sobre IP, los elementos que hacen parte de su arquitectura de red y los protocolos asociados a VoIP, de igual forma se plantean las generalidades de los estándares en redes inalámbricas, como son cubrimiento de la red, disponibilidad de los canales de frecuencia a utilizar, el ancho de banda y la seguridad ofrecida en estas redes.

En el segundo capítulo se presentan las características fundamentales en el desempeño de una red de VoIP que afectan la Calidad de Servicio (QoS), tales como: Latencia, Jitter, pérdida de paquetes y calidad de voz.

El tercer y último capítulo realiza una recopilación de todas las consideraciones que se deben seguir al momento de implementar ambas tecnologías y que influyen en el rendimiento de la red.

# 1. TECNOLOGÍA VOIP Y REDES INALAMBRICAS

## 1.1 VOZ SOBRE IP - VoIP

La tecnología Voz sobre IP viene del término en ingles Voice over Internet Protocol y consiste en transportar la voz sobre cualquier red basada en el protocolo IP, esto significa que para transportar voz sobre redes que emplean el protocolo de Internet, debe ser sometida a un proceso de digitalización ó conversión a señales PCM (por sus siglas en ingles Pulse Code Modulation), paquetización y encapsulamiento con el fin de enviarla sobre la misma red de datos, logrando así una red convergente que conlleva a minimizar costos de gestión y mantenimiento en la red; por ejemplo en una empresa con sedes en diferentes ciudades, la implementación de esta tecnología acarrearía un ahorro en costos de comunicaciones, puesto que las llamadas entre distintas sucursales de la empresa resultarían gratuita, pues hay que considerar que el precio del enlace se paga para transmitir datos; además, obtendría una integración de servicios y unificación de la estructura de la red empresarial que permite disminuir costos y mejorar la administración del sistema global de comunicaciones.

**Figura 1** Funcionamiento de VoIP

### 1.1.1 ARQUITECTURA DE RED VoIP

En términos generales, una topología de red VoIP está conformada por los siguientes elementos:

- ✓ Central Telefónica ó servidor: cumple funciones tales como control de admisión, autorización de llamadas, control del ancho de banda utilizado, traducción de direcciones, gestión de zona y señalización de control de llamada. Puede ser un elemento opcional en la red[1].

- ✓ Gateway: son interfaces o equipos que convierten la señalización y el canal de voz para la red IP, además de efectuar la integración de la red de voz con la red telefónica análoga, y permiten la utilización de los teléfonos analógicos o digitales existentes lo que reduce los costos de la migración para la nueva arquitectura de red. El Gateway tiene por un lado una interface LAN y por el otro dispone de una o varias de las siguientes interfaces[2]:

  - FXO: para conexión a internos de las PBXs o a la PSTN.
  - FXS: para conexión a urbanas de las PBXs o teléfonos analógicos.
  - E&M: para conexión específica a PBXs.
  - BRI: acceso básico ISDN (2B+D).
  - PRI: acceso primario ISDN (30B+D).

- ✓ Router IP: equipo encargado de encaminar los datagramas IP a una interfaz de salida, examinando la información contenida en la cabecera IP.

- ✓ Terminales IP: son el reemplazo de los actuales teléfonos, ya que pueden proporcionar cualquier combinación entre los servicios de voz, datos y video, poseen una interfaz para red Ethernet y asumen una dirección IP de la red; estos terminales se pueden implementar tanto en hardware (alámbricos ó inalámbricos), como en software; en el caso de ser terminales por software, se utiliza un computador común

---

[1] FERREIRA, Guillermo y FROCHT, Gustavo y MAYONE, Eduardo. Tecnología de Voz Sobre IP Terminal H.323 [Tesis de Grado]. (2001). 134p.
[2] Ibid.

para ejecutar el software, lo que conlleva a una solución de implementación más económica.

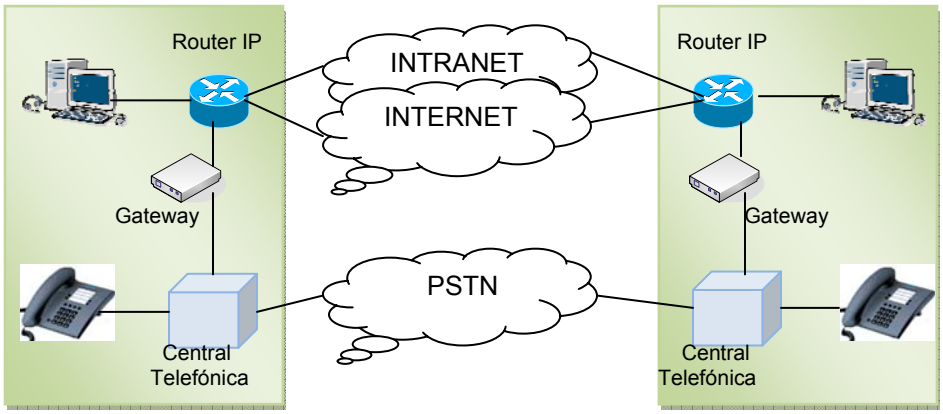
- ✓ Red IP conjunto de host y routers interconectados, los cuales emplean el protocolo de Internet para la transmisión de información, existen tres tipos de redes IP que pueden soportar la tecnología de voz sobre IP en las empresas:

•**Internet Pública**: es el conjunto más grande de redes interconectadas por todo el mundo; esta red actualmente no permite la propagación de tráfico de voz, debido a que el retardo y la pérdida de paquetes durante periodos de alto nivel de flujo degradan la calidad del tráfico altamente sensible a estos parámetros, tal como ocurre en el caso de voz en tiempo real.

•**Internet Privada**: ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que se refiere al tráfico IP. Es similar al Internet pero con mayor calidad de servicio y con mejoras en aspectos tales como seguridad. Algunos operadores que ofrecen este servicio brindan garantías para el tráfico de voz como ancho de banda adecuado y bajo retardo en las comunicaciones.

•**Intranet**: es la red IP implementada por la propia empresa. En este tipo de red la empresa tiene bajo su control todos los parámetros de la red, por lo que es ideal para transportar voz.

**Figura 2** Arquitectura de una red VoIP



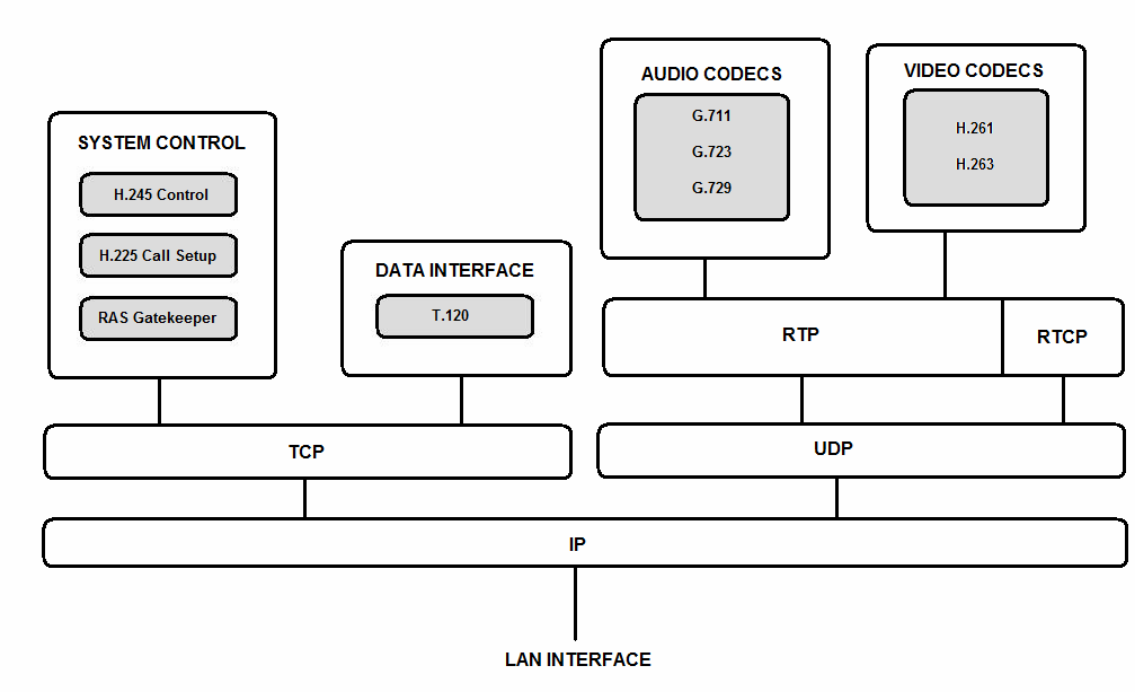
### 1.1.2 PROTOCOLOS DE VoIP

Para lograr establecer una comunicación los terminales realizan dos tipos de conexión, una orientada al tráfico de voz y la otra se encarga del control de ese proceso. Los protocolos usados para el control son H.323 y SIP.

- ✓ H.323 Protocolo definido por la Unión Internacional de las Comunicaciones para ser la base de VoIP. Este protocolo proporciona una serie de normas para administrar la señalización, el control y transporte de llamadas y aplicaciones multimedia sin importar la compatibilidad de los equipos utilizados para tal fin. H.323 define tres elementos en su arquitectura de red: Terminales, Gatekeepers y Gateways.

  El estándar H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación. La siguiente grafica muestra algunos de los protocolos más significativos para H.323.

**Figura 3** Estándar H.323




Fuente: Seminario 3COM. Editado por el autor

**Tabla 1** Protocolos más significativos para H.323.

| PROTOCOLO | DESCRIPCION |
|---|---|
| H.245 | Protocolo de control utilizado en el establecimiento y control de una llamada. |
| H.225 | Protocolo de control de llamada que permite establecer una conexión y una desconexión. |
| RAS | Sirve para registrar, control de admisión, control del ancho de banda, estado y desconexión de los participantes. |
| T.120 | Es una recomendación que define un conjunto de protocolos para conferencia de datos. |
| G.711 | Es el codec de audio obligatorio en los terminales de H.323. Usa modulación por pulsos codificados (PCM). Tasa de bits de 56Kbps y 64Kbps. |
| G.723 | Codec de audio que opera a una tasa de bits de 5.3Kbps o 6.4Kbps |
| G.729 | Codec de audio que opera a una tasa de bits de 8Kbps o 13Kbps |
| H.261 | Codec de video recomendado en H.323 |
| H.263 | Codec de video recomendado en H.323 |

- ✓ PROTOCOLO DE INICIALIZACION DE SESIONES (SIP). El protocolo SIP fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF (Internet Engineering Task Force), definiendo una arquitectura de señalización y control para VoIP. Este protocolo define como iniciar, modificar y terminar sesiones interactivas de comunicación multimedia (como video o voz) entre usuarios.

  El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP (Real Time Protocol) que se usa para transportar los datos de voz en tiempo real y SDP (Session Description Protocol) que se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.

SIP fue diseñado de acuerdo al modelo de Internet. Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos. Esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes, producto de tener que enviar toda la información entre los dispositivos finales.

SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes. Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

- ✓ PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP) El protocolo de transporte en tiempo real fue desarrollado por IETF (Internet Engineering Task Force), diseñado para transmitir información en tiempo real como su nombre lo indica. Este protocolo funciona sobre UDP e intenta hacer que los paquetes sean recibidos conforme la orden de envío.

  El RTP organiza los datos, de manera que sea posible su transmisión en tiempo real. En el caso que algún paquete llegue atrasado, el RTP causa una interpolación entre el intervalo dejado por el paquete y éste no se entrega. El atraso de paquetes puede suceder porque éstos pueden seguir caminos diferentes para llegar al destino. Eso no es un problema si se transmite un archivo, ya que sus paquetes se encajan en el destinatario. Pero eso no puede suceder con voz y vídeo, en tiempo real.

  Este protocolo proporciona información para: tipo de contenido, sincronización, información del remitente, detección de pérdidas de paquetes, segmentación y reensamble, entre otras.

  El funcionamiento de RTP está asociado al Protocolo de Control de Tiempo Real (RTCP) que es responsable por la compresión de los paquetes de los datos y

también actúa en el monitoreo de los mismos. La función principal de RTCP es informar la calidad de servicio proporcionada por RTP.

### 1.1.3 CODECS

El proceso de convertir ondas analógicas a información digital se hace con un codificador-decodificador (CODEC). La mayoría de las conversiones para una señal de voz analógica se basan en la modulación codificada mediante pulsos (PCM) o variaciones de esta.

A continuación se muestra una tabla con algunos codecs:

**Tabla 2** Codecs

| CODEC | CARGA ÚTIL | ANCHO DE BANDA CAPA 2 | ANCHO DE BANDA CAPA 3 |
|---|---|---|---|
| G.722.2 | 12.65-23.05 | 38.8 kbps | 50 kbps |
| G.722 | 32 kbps | 78.4 kbps | 89.6 kbps |
| G.711 | 64 kbps | 76 kbps | 85.3 kbps |
| G.722.2LB | 6.60 o 8.85 | 24.8 kbps | 36.0 kbps |
| G.723.1 | 5.3 o 6.3 | 16.27 o 17.07 | 25.6 o 26.4 |
| G.729A | 8 kbps | 22.4 kbps | 33.6 kbps |
| ADPCM | 32 kbps | 44 kbps | 53.3 kbps |

## 1.2 REDES INALAMBRICAS

En un comienzo las redes de datos fueron diseñadas para transporte de tráfico mediante el empleo de un canal o línea física; luego con el paso de los años, la necesidad de comunicación y transmisión de información aumentó de tal forma que fue preciso buscar un método económico y fácil de implementar a fin de ampliar las redes cableadas existentes y poner en funcionamiento redes en aquellos sitios donde es imposible una infraestructura cableada; fue entonces cuando se comenzó a estudiar la posibilidad de transferencia de ondas electromagnéticas sobre un medio no guiado como el aire y los

beneficios que se obtendrían con esto; así surgió la tecnología de redes inalámbricas con la cual se logra reducir la infraestructura física, costos de instalación y mantenimiento.

Aunque al utilizar este tipo de medio, los usuarios comparten el ancho de banda y se obtienen menores velocidades de transmisión que con una red cableada; esta tecnología ofrece ventajas a los usuarios tales como conectividad, movilidad, velocidad simétrica, buen ancho de banda, facilidad de reubicación sin incurrir en costos adicionales, adaptación de la velocidad según la intensidad de la señal para evitar errores en el desempeño de la red, gran escalabilidad y funcionamiento en la banda de 2.4GHz que no necesita licencia.

Dentro del auge de las tecnologías inalámbricas se encuentran Wi-Fi. Wi-Fi es una marca registrada de la Wireless Ethernet Compatibility Alliance, basada en el estándar IEEE 802.11 para redes inalámbricas de área local. Esta organización se encarga de certificar la interoperabilidad y compatibilidad entre productos inalámbricos de diferentes fabricantes que utilizan este estándar.

La operación tanto en capa física (DSSS Espectro Disperso de Secuencia Directa ó OFDM Modulación por División de Frecuencia Ortogonal) como en enlace de datos (adaptación de trama Ethernet + CSMA/CA)[3] para redes inalámbricas está definida por la familia de estándares IEEE 802.11, dentro de los cuales se encuentran 802.11a, 802.11b, 802.11g y 802.11n empleados por Wi-Fi.

La actual tecnología Wi-Fi que se encuentra en el mercado opera en las frecuencias de 2.4GHz y 5GHz las cuales no requieren licencia para su uso, también proporciona una cobertura de 100 metros al aire libre con altas velocidades de transmisión (54Mbps). Wi-Fi es muy utilizado dentro de empresas, hogares y universidades ya que permite movilidad para sus usuarios dentro de la red de área local.

---

[3] FERNÁNDEZ, Néstor. Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo. [Tesis Doctoral Universidad de Oviedo]. (mar, 2006). 299 p.

### 1.2.1 IEEE 802.11a

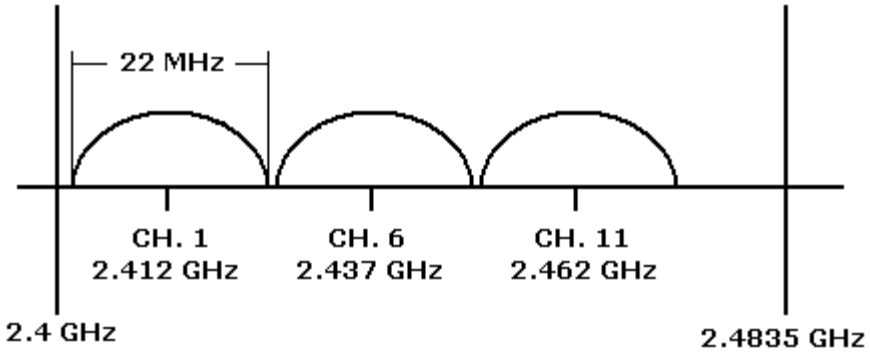
Este estándar opera en la banda de frecuencias de 5GHz y utiliza como técnica de modulación OFDM (Multiplexación por División de Frecuencia Ortogonal) lo que permite alcanzar velocidades de transmisión de 54Mbps proporcionando 8 canales sin solape. La ventaja de este protocolo es que evita interferencia con otros dispositivos inalámbricos que trabajan en la banda de frecuencias de 2.4GHz tales como teléfonos inalámbricos e incluso algunos hornos microondas, debido a que la banda en la que opera esta menos congestionada; sin embargo, su alcance se limita a 50 metros, lo cual implica que se debe instalar más puntos de acceso que si utilizase 802.11b para cubrir una misma zona.

### 1.2.2 IEEE 802.11b

Este estándar surgió por la necesidad de crear equipos de transmisión de datos de alta velocidad utilizando frecuencias del espectro radioeléctrico en bandas de uso libre tal como 2.4GHz, en la que se especificó la operación de IEEE 802.11b, a tasas de transmisión de hasta 11Mbps con un alcance de 100 m sin obstáculos, aunque puede variar dependiendo de la potencia de transmisión del dispositivo y la ganancia de la antena que está siendo utilizada para tal fin; utiliza como técnica de modulación DSSS.

Este estándar especifica 11 canales, los cuales se encuentran separados en bandas de frecuencias contiguas, cada una de 22 MHz. En la figura 2 se muestran los tres canales 1, 6 y 11 que posibilita este estándar sin solape, es decir pueden operar dentro de una misma área sin que exista interferencia cocanal, este tipo de interferencia se presenta cuando los canales comparten parte del ancho de banda que les corresponde y produce una reducción en la tasa de Throughput. Existen otros canales tales como el 2 y 7 o el 1 y 10 que tampoco presentan interferencias.

**Figura 4** Máximo número de canales sin interferencia cocanal.




### 1.2.3 IEEE 802.11g

Este protocolo opera en la misma banda de frecuencias del 802.11b, lo que permite interoperabilidad entre los dos estándares, reducción de costos y adicionalmente al utilizar la técnica de modulación OFDM, se puede obtener 54Mbps como velocidad máxima de transmisión; hecho que permite la ampliación del portafolio de servicios prestados con tecnologías inalámbricas ya que las tasas de transmisión permiten la propagación de flujos de información que requieren velocidades considerables.

Otro aspecto importante radica en que se mantiene el máximo número de canales del estándar IEEE 802.11b operando simultáneamente en una misma área sin presentar interferencia cocanal.

### 1.2.4 IEEE 802.11n

Este estándar aun esta en desarrollo, en marzo de 2007 IEEE aprobó el segundo borrador. Puede trabajar en cualquiera de las dos frecuencias empleadas actualmente, esto significa que es compatible con dispositivos que operan con los anteriores estándares. Además, combina varias antenas de radio para aumentar la capacidad de las transmisiones, llegando a alcanzar hasta 270Mbps y esta técnica permite aumentar tres veces más el rango de cobertura con respecto a 802.11g.

A continuación se hace una comparación de los estándares 802.11 en la tabla 3.

**Tabla 3.** Comparación de los estándares 802.11

| **Estándar** | **802.11a** | **802.11b** | **802.11g** | **802.11n** |
|---|---|---|---|---|
| **Aprobación IEEE** | Julio de 1999 | Julio de 1999 | Abril de 2004 | Marzo de 2007 (2° Borrador) |
| **Velocidad** | 54 Mbps | 11 Mbps | 54 Mbps | 270 Mbps |
| **Frecuencia** | 5 GHz | 2.4 GHz | 2.4 GHz | 2,4GHz y 5 GHz |
| **Cobertura** | 70 m | 100 m | 100m | 300m |
| **Tipo de Modulación** | OFDM | DSSS | OFDM y DSSS | OFDM |
| **Tasas de Transmisión*** | 5,9,12,18,24,36, 48,54 Mbps | 1,2,5.5,1 1 Mbps | 6,9,12,15,24,36,48 ,54 Mbps | 27,54,81,108,162,216,243, 270 Mbps |
| **Tasa de Datos Efectivos (Throughput Teórico)** | 32 Mbps | 5 Mbps | 32 Mbps | 124 Mbps |
| **Cifrado Disponible** | SI | SI | SI | SI |
| **Compatible con redes** | Ethernet | Ethernet | Ethernet | Ethernet |

*La tasa de transmisión depende de la distancia o del nivel de intensidad de la señal que reciba el cliente.

Fuente: PINZON, Samuel Gonzalo. Curso Redes Inalámbricas. Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones. UIS. Cohorte VII-Ciclo II, 2006. Editado por autor.

### 1.2.5 ARQUITECTURA DE RED

La arquitectura de red de 802.11 está conformada por los siguientes elementos:

- ✓ **Estación (STA):** Es el dispositivo a través del cual el cliente se conecta a la red inalámbrica.

- ✓ **Punto de Acceso (AP):** Es una estación base que administra las comunicaciones y gobiernan a la unidad de servicio básico de infraestructura.

- ✓ **Unidad de Servicio Básico de Infraestructura (BSS):** Son celdas formadas por un conjunto de STAs que se comunican unas con otras formando una configuración en modo infraestructura.

- ✓ **Unidad de Servicio Extendido (ESS):** Es una unidad lógica para presentar a los niveles superiores el conjunto de todas las redes inalámbricas, con sus correspondientes celdas y puntos de acceso.

- ✓ **Sistema de Distribución (DS):** Es una especie de backbone, por el cual los APs y BSSs se comunican.

### 1.2.6 SEGURIDAD EN REDES INALAMBRICAS

Los ataques a nivel de seguridad en redes inalámbricas trae consecuencias tales como: reducción en su ancho de banda, debido a estaciones cliente no autorizadas o a puntos de acceso ilegales que ingresan a la red y consumen parte de este recurso; por otra parte, los equipos que están conectados son vulnerables a ataques por parte de los dispositivos que han entrado de manera ilícita, estos podrían robar o destruir información de los equipos, bloquear servidores, insertar virus maliciosos en los equipos, entre otros. Por estas razones es importante tener claro que herramientas ofrecen las redes inalámbricas para brindar seguridad a las mismas.

Algunas herramientas de seguridad que se pueden utilizar son:

- ✓ **Protocolo WEP (Wired Equivalent Privacy):** Está diseñado para proteger los datos transmitidos durante una conexión inalámbrica utilizando un esquema de encriptación, este protocolo fue incluido en el estándar 802.11 y se basa en una clave simétrica, lo cual quiere decir que tanto la Estación como el Punto de Acceso deben conocer la clave que se utilizará. El protocolo WEP no tiene algún mecanismo que distribuya las claves de manera automática, lo que obliga a introducir la clave en todos los equipos de la red de forma manual. La clave

utilizada puede tener un tamaño de 40 o 104 bits, además requiere de 24 bits para el vector de inicialización. El algoritmo de encriptación utilizado es RC4, y utiliza un algoritmo de integridad CRC32 que genera un ICV (Integrity Check Value) independiente de la clave utilizada. La vulnerabilidad de este protocolo es que utiliza una longitud muy corta para el vector de inicialización, y en Internet ya se encuentran artículos acerca de cómo romper este tipo de seguridad.

- ✓ **Protocolo TKIP (Temporal Key Integrity Protocol):** Utiliza el mismo algoritmo de encriptación RC4 que el protocolo WEP, pero sus claves están construidas de forma diferente. Utiliza una clave temporal (TK) de 128 bits que es compartida entre la estación y el punto de acceso, que se actualiza cada 10.000 paquetes, y el vector de inicialización es de 48 bits, el cual se reinicia a cero cada vez que se fija una nueva clave temporal, con lo cual mejora la seguridad de la red. Para la encriptación se pueden utilizar unas claves derivadas de la TK, llamadas PPK (Per-Packet Key) que son generadas de manera dinámica por cada paquete enviado. Para la integridad de la información, TKIP implementa el algoritmo de Michael (MIC) que introduce un valor de 8 bytes antes del CRC. Este valor es encriptado utilizando una combinación de la información enviada, el vector de inicialización, la dirección origen y destino.

- ✓ **Protocolo CCMP (Counter Mode with CBC-MAC Protocol):** Es un protocolo complementario a TKIP. Su esquema de encriptación está basado en AES (Advanced Encryption Standard). Este esquema se integra en el protocolo WPA2, y utiliza claves de 128 bits con el algoritmo CBC-MAC, un vector de inicialización de 48 bits llamado PN (Packet Number) que es utilizado junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

- ✓ **Filtrado de direcciones MAC:** Este método se basa en utilizar la dirección MAC de cada estación cliente, como mecanismo de autenticación para ingresar a la red; la dirección MAC debe ser única para cada dispositivo conectado a la red

inalámbrica y viene configurada de fabrica, con lo cual se logra restringir el acceso a las direcciones que no estén autorizadas dentro de la tabla de datos creada en cada uno de los puntos de acceso. Sin embargo este método de seguridad no es muy eficiente debido a que cada vez que se quiera autorizar o denegar un equipo, es necesario editar las tablas de direcciones en todos los puntos de acceso, lo cual sería una labor tediosa en una red grande. Otra razón, es que la dirección MAC de un equipo se puede cambiar fácilmente, con lo cual un atacante podría emplear un sniffer para capturar el tráfico que circula por la red y guardar las direcciones válidas, para en el momento en que una de ellas esté disponible, asignarla a su computador e ingresar a la WLAN como un cliente autorizado.

- ✓ **Protocolo WPA (Wi-Fi Protected Access):** Fue creado para solucionar los problemas de seguridad que se tenían con el protocolo WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. El primer problema lo soluciona implementando el protocolo TKIP mencionado anteriormente. Para el segundo WPA utiliza el estándar IEEE 802.1x como mecanismo de control de acceso. Este estándar permite autenticar al usuario a través del protocolo de autenticación extensible (EAP). Existen tres tipos de elementos en 802.1x: el cliente (reside en la estación inalámbrica) que solicita acceso, el autenticador (reside en el punto de acceso) que sirve de enlace entre el cliente y el servidor de autenticación y el servidor de autenticación que se encarga de realizar la comprobación de credenciales proporcionadas por el cliente y se encuentra en un servidor AAA (Authentication, Authorization, and Accounting) servicio de usuario de acceso telefónico de autenticación remota (RADIUS). El estándar utiliza el concepto de puerto habilitado/inhablitado en el cual el autenticador crea un puerto lógico por el cliente, quien tendrá que validarse ante el servidor para tener acceso a los servicios ofrecidos por la red, de lo contrario solo se permitirá tráfico 802.1x hacia el servidor de autenticación.

- ✓ **Protocolo WPA2:** Es una mejora del protocolo WPA, cambia el esquema de encriptación a AES-CCMP, desarrollado por el NIST (National Institute of Standards and Technology).

- ✓ **Redes Privadas Virtuales VPN:** Este método emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. El servidor de autorización y autenticación de la VPN va a servir de único punto de conexión al exterior desde la red inalámbrica. Cuando un usuario se conecte a la WLAN, solo se le permite el acceso al servidor de la VPN, lo que lo obliga a autenticarse para poder conectarse.

# 2. CARACTERÍSTICAS DE DESEMPEÑO PARA VoIP EN REDES INALÁMBRICAS

En este capítulo se detalla en forma explícita, tanto los parámetros relevantes en VoIP, como las diferentes técnicas que se utilizan para asegurar calidad de servicio en redes IP y redes inalámbricas. Además, parámetros como jitter, pérdida de paquetes y retardos, entre otros, se definen y se limitan dentro de rangos de valores admisibles para que los servicios VoIP tengan un gran impacto en el usuario final. Las recomendaciones de calidad de servicio presentadas a continuación son sintetizadas de estándares y estudios realizados por la ITU[4].

## 2.1 CONSIDERACIONES GENERALES

El oído humano es poco tolerante a distorsiones de señales cuando se está desarrollando una comunicación, razón por la cual en aplicaciones que operan en tiempo real como los sistemas de telefonía, es de suma importancia controlar una serie de parámetros tales como disponibilidad del sistema, retardos de propagación, variación de dichos retardos y pérdida de paquetes, con el fin de brindar al usuario final una óptima calidad de servicio (QoS[5]).

En la telefonía convencional el control de estos parámetros se logra utilizando la conmutación de circuitos, donde se garantiza un camino fijo e invariante a la señal, logrando que todos los paquetes lleguen en el mismo orden de envió, con bajos retardos y poca probabilidad de pérdidas de información.

En sistemas VoIP no se proporciona una ruta fija puesto que operan con conmutación de paquetes, donde cada paquete toma un camino para llegar a un destino, independientemente de la ruta que tomen los demás, razón por la cual se incrementan

---

[4] ITU Unión Internacional de Telecomunicaciones.

[5] De aquí en adelante se utilizará el término QoS para hacer referencia a Calidad del Servicio.

tanto los retardos de propagación, como las pérdidas de paquetes; existiendo una mayor probabilidad de degradación en la calidad de la comunicación.

## 2.2 PARÁMETROS DE RELEVANCIA PARA LA CALIDAD DEL SERVICIO EN VOIP

A continuación se describen los factores determinantes en el proceso de entrega de un mensaje de voz al usuario final, así como sus implicaciones en QoS.

### 2.2.1 Disponibilidad

Se refiere a la probabilidad con la cual el usuario encontrará la red en las condiciones óptimas para poder hacer uso de la misma y establecer una comunicación; es decir una alta disponibilidad significa una alta probabilidad de funcionamiento del sistema, lo cual satisface al usuario ya que tiene una experiencia gratificante con el servicio.

Para garantizar este parámetro se deben tomar algunas medidas preventivas tales como disponer de redundancia en los equipos y enlaces que resultan críticos en la operación del sistema, con el propósito de tener caminos de reserva por lo cuales se pueda reenrutar el tráfico en caso de perder un equipo o enlace principal; adicionalmente es conveniente configurar los terminales de usuario de tal forma que si la llamada por algún motivo no se puede desarrollar por la red IP, se enrute hacia otra red (RDSI, PSTN) logrando de esta forma que el usuario pueda establecer la llamada cuando así lo desee.

### 2.2.2 Ancho de Banda y Tasa de Bits

El requerimiento en cuanto ancho de banda para una comunicación de voz sin comprimir empleando el protocolo de Internet, es asegurar un canal con una tasa mínima de bits constante igual a 64Kbps que se empleará mientras dure la sesión establecida, aún en caso que los dos extremos permanezcan en silencio.

En general, hay que considerar la situación en la que por la misma red circulan señales de voz, datos y video; lo cual induce a plantear la siguiente expresión para el cálculo del ancho de banda necesario en una red VoIP.

$$BW = \frac{BWvoz + BWvideo + BWdatos}{0.75}$$ [6]

Efectuando el cálculo para ancho de banda empleando la ecuación anterior, se hace un sobredimensionamiento asegurando un 25% de capacidad de reserva para ocasiones de alto tráfico en la red, esto con el fin de evitar congestión y saturación del sistema.

### 2.2.3 Retardo de Propagación ó Latencia

Teniendo en cuenta que la comunicación en mención se efectúa en tiempo real, uno de los principales objetivos es garantizar que los paquetes demoren el menor tiempo posible para ir de un extremo a otro, con el fin que el oído humano perciba correctamente el mensaje; así por ejemplo si el tiempo de latencia es igual a 25 ms, la voz del usuario que está hablando se refleja produciéndose de esta forma un eco tolerable en la comunicación, pero si la latencia supera los 30 ms es necesario implementar circuitos supresores de eco ya que la conversación se ve seriamente afectada[7].

Existen dos agentes correlacionados al retardo que son determinantes a la hora de cursar con éxito una comunicación de VoIP, por un lado está el retardo máximo aceptable para el cual la recomendación G.144 de ITU-T[8] establece que se debe encontrar dentro del rango comprendido entre 150 a 200 ms, lo que indica que retardos de propagación por encima de estos valores tornan las conversaciones inaceptables; mientras que por otro lado se encuentran los tipos de fuentes para los retardos que para este caso son dos fijo y variable, los cuales se describen a continuación.

- ✓ **Fijo:** Las fuentes de retardo fijo siempre originan la misma latencia ya que dependen del medio físico y de la velocidad de la luz; la ITU-T establece en su recomendación G.144 un valor de 6μs/Km, se relacionan tanto con los procesos a

---

[6] HUIDOBRO, José y ROLDÁN, David. Tecnología VoIP y Telefonía IP. México: Alfaomega, julio 2006. 311p.

[7] FERREIRA, Op. cit., p.11.

[8] El ITU-T es el Sector de Telecomunicaciones que desarrolla los estándares para la interconexión de equipo de telecomunicaciones.

los que se debe someter la voz para transmitirla en redes IP, como con los retardos de propagación propios de los enlaces internos de la red los cuales se suman para formar el retardo global de la conexión y corresponden a[9]:

- Retardo de Codificación: denominado también retardo de procesamiento puesto que es el tiempo que demora el procesador digital de señales en comprimir un bloque de muestras PCM (tiempo de compresión por bloque más tiempo para descomprimir un bloque más retardo del algoritmo[10]), es decir se origina al codificar las señales de audio (voz) y procesarlas con un determinado codec, razón por la cual este tiempo depende del tipo de codificador empleado y la velocidad del procesador [11].
- Retardo de Paquetización: sucede cuando las muestras de voz codificadas y comprimidas generadas cada 125 µs se almacenan hasta que se alcance la cantidad[12] necesaria para formar un paquete; este almacenamiento ocasiona un retardo proporcional al tamaño del paquete, es decir igual a 125µs*tamaño del paquete; en otras palabras se genera cuando la voz se convierte en paquetes IP. Es recomendado buscar que el retardo de paquetización no sea mayor de 30 ms[13].
- Retardo de Serialización: es el tiempo empleado para colocar tramas de voz desde la capa de aplicación hasta la interfaz de red por la cual se propagará; este retardo es directamente proporcional a la tasa de reloj en la interfaz del enlace[14], depende tanto de la velocidad de la línea como del tamaño de la trama y debe contabilizarse cada vez que un paquete pase por un router o switch[15].

---

[9] FERREIRA, Op. cit., p.11.
[10] Se genera porque el algoritmo de compresión necesita conocer algo del contenido albergado en el bloque siguiente, para lograr reproducir correctamente el bloque actual, adicionándose así una sobrecarga al bloque comprimido; la consecuencia de esto es el incremento en el retardo total del enlace debido al tiempo de procesamiento adicional necesario para la sobrecarga (5ms) [2].
[11] FERREIRA, Op. cit., p.11.
[12] "Ejemplo un paquete IP tiene 20 Bytes de encabezado, por lo cual tiene poco sentido poner menos de 20 muestras de voz de 8 bits cada una dentro del campo de datos del paquete IP" [2]
[13] FERREIRA, Op. cit., p.11.
[14] FERREIRA, Op. cit., p.11.
[15] HUIDOBRO, Op. cit., p.26.

**Tabla 4** Retardo de serialización como función de la velocidad de enlace y tamaño del paquete.

| Velocidad Enlace | Tamaño del Paquete | | | | | |
|---|---|---|---|---|---|---|
| | **64 Bytes** | **128 Bytes** | **256 Bytes** | **512 Bytes** | **1024 Bytes** | **1500 Bytes** |
| 56kbps | 9ms | 18ms | 36ms | 72ms | 144ms | 214ms |
| 64kbps | 8ms | 16ms | 32ms | 64ms | 128ms | 187ms |
| 128kbps | 4ms | 8ms | 16ms | 32ms | 64ms | 93ms |
| 256kbps | 2ms | 4ms | 8ms | 16ms | 32ms | 46ms |
| 512kbps | 1ms | 2ms | 4ms | 8ms | 16ms | 23ms |
| 768kbps | 0.64ms | 1.28ms | 2.56ms | 5.12ms | 10.24ms | 15ms |

Retardo de Conmutación: es el retardo producido por la red de interconexión.

- ✓ **Variable:** Son producidos en los switches por que los tiempos de encolamiento de los paquetes no son iguales en los buffer de salida debido a los niveles de congestión que experimentan, por lo cual se generan retardos variables a través de la red (jitter), que son manejados en el Gateway destino mediante los buffer de-jitter.

### 2.2.4 Variación del Retardo ó Jitter

Jitter se refiere a la variación que sufre el retardo en la transmisión de la información y que se ocasiona debido a la variación en los tiempos de propagación, ya que paquetes de un mismo mensaje toman caminos diferentes para llegar a su destino; ó porque los tiempos de encolamiento en los routers varían de acuerdo al estado de congestión que experimenten. En este punto hay que precisar que si dicho jitter es demasiado grande ocasiona la pérdida de paquetes con lo cual se distorsiona la fidelidad de la comunicación. Para controlar los efectos de este fenómeno, existen en el lado del receptor espacios de memoria ó buffers especiales llamados Buffer de-jitter utilizados para eliminar la variación en la latencia puesto que almacenan una cantidad ó umbral mínimo de flujo de voz para luego enviarlo controladamente a una tasa constante, de tal forma que sí han llegado paquetes en desorden nuevamente tomen la secuencia correcta y adicionalmente evitando que el flujo actual se afecte por problemas que se presenten en la red de

transporte[16]; con el empleo de este mecanismo se obtiene reproducir las conversaciones a velocidad constante lográndose que se desarrollen perfectamente.

### 2.2.5 Pérdida de Paquetes

Cuando un nodo del sistema no cuenta con la capacidad suficiente para gestionar todo el tráfico que se genera, experimenta un estado de congestión y se ve en la imperiosa necesidad de descartar paquetes, lo cual ocasiona un grave error en las comunicaciones desarrolladas en tiempo real, puesto que no es posible reconstruir correctamente el mensaje, ya que faltan ciertos tramos del mismo y el receptor no percibe la conversación de forma continua.

Ahora tomando en consideración que las redes destinadas a transmitir la voz empleando el protocolo de Internet son de paquetes, se podría pensar que un mecanismo para solucionar el problema en cuestión, seria la retransmisión de los mismos, pero esto introduciría un retardo adicional que acarrearía una mayor degradación de la voz, por lo cual no es posible implementar esta característica propia de las redes de paquetes en la tecnología de VoIP.

### 2.2.6 Fidelidad de voz

Se atribuye a la claridad con la que el usuario receptor percibe la voz del usuario transmisor, este parámetro se ve considerablemente influenciado por las distorsiones generadas por los componentes de la red en el trayecto recorrido.

En este punto es importante destacar que existen varios métodos para asegurar la calidad del servicio en los diferentes puntos de la red, sea en la periferia[17] de la red o en su núcleo[18], los cuales se describen a continuación.

---

[16] BERROCAL, Julio et al. Redes de Acceso de Banda Ancha: Arquitectura, Prestaciones, Servicios y Evolución. Madrid : 2003. 93 p

[17] Edge de la Red

[18] Core de la Red

## 2.3 TÉCNICAS IMPLEMENTADAS PARA OBTENER QOS EN REDES IP

En el extremo de la red es importante clasificar el tráfico de acuerdo al tipo de información que transporten; así mismo es primordial organizar los paquetes en colas según los requerimientos de red y políticas de administración de la misma. Mientras que en el núcleo de la red es indispensable administrar de la forma más ecuánime posible el ancho de banda; a continuación se realizará una breve descripción de los mecanismos más difundidos para lograr brindar un servicio de óptima calidad a los usuarios finales.

### 2.3.1 Marcación y clasificación del tráfico

La marcación del tráfico tiene lugar únicamente en un nodo de borde de la red Backbone, consiste en determinar el tipo de tráfico al que pertenece el paquete en uno de sus campos, para eliminar procesos de análisis dentro del sistema, ya que los demás nodos solamente procesan esta información y clasifican los flujos de información agrupándolos de acuerdo al perfil de tráfico que contengan, esto con el propósito de darle a cada paquete el tratamiento adecuado según los requerimientos que exija.

Por lo tanto la clasificación del tráfico se puede generar a diferentes niveles del modelo OSI:

| NIVEL | OPERACIÓN EN |
|---|---|
| 1 | Interfaz Física, PVC ó Puerto |
| 2 | Direcciones MAC, CoS, VLAN ID |
| 3 | IPToS, DSCP |
| 4 | Puertos TCP ó UDP |
| 7 | Identificadores de Aplicación ó URL en el contenido del paquete ó en su cabecera |

Fuente: HUIDOBRO, José y ROLDÁN, David. Tecnología VoIP y Telefonía IP. Editado por el Autor.

- ✓ **Type of Service (ToS):** La información contenida en el campo Type of Service de la cabecera IP con longitud igual a 8 bits, sirve para agrupar los paquetes según la importancia ó los recursos de red que exijan, asignando en el primer campo (bits 7-5) diferentes niveles de prioridad (7), de tal manera que el orden de envío para los flujos de bits, coincide con la disposición jerárquica a nivel de prioridad de los mismos. Por su parte el campo central (bits 4-1), denominado ToS especifica el tipo de servicio del paquete; mientras que el tercer y último campo (bit 0), corresponde a *must be zero*, que usualmente es ignorado por los enrutadores.

| PRECEDENCE | ToS | MBZ |
|---|---|---|
| 3 bits | 4 bits | 1 bit |

| DSCP | ECN |
|---|---|
| 6 bits | 2bits |

Fuentes: RFC 1349 y Juniper Networks. Editado por el Autor.

- ✓ **Servicios Diferenciados (Differenciated Services ó DiffServ):** Cuando un paquete ingresa al núcleo de la red de datos, es sometido a un proceso de clasificación y marcación con el fin de determinar el tipo de tráfico al que pertenece; dicha marcación se efectúa en el campo DSCP (Differenciated Service Code Point), últimos 6 bits del octeto Type of Service de la cabecera IP; este procedimiento se hace con el objetivo que cada flujo de información reciba el tratamiento adecuado PHB (Per Hop Behavior), especificando la cantidad de recursos, probabilidad de descarte y frecuencia de atención, en todos los enrutadores del sistema.

En este sentido es preciso explicar algo más acerca de los mecanismos PHB, definiendo los tratamientos dados a cada paquete en los enrutadores del sistema de acuerdo a los recursos de red que se empleen y prioridades que se tengan:

- Best effort: se basa en ubicar en una cola el tráfico de paquetes que han excedido la capacidad de un enlace, cuando la cola donde se están almacenando los datos

se llena, se va descartando la información entrante, es empleado para servicios que no requieren demasiados recursos ni tratamiento especial[19].

- Expedited Forwarding: fundamentada en el manejo de colas con prioridades y en el empleo de tasas de llegada a los enrutadores menores que las tasas de salida de éstos, lo cual se hace para garantizar que las colas siempre permanezcan vacías ó que la probabilidad de congestión en las mismas sea nula. Se usa para proveer a los clientes servicios Premium caracterizados por requerir retardos pequeños, bajos jitters, pocas pérdidas de paquetes, además de tasa constante de bits; en este tipo de PHB, se descartan paquetes cuando el umbral de tasa de bits que el cliente puede recibir y que está establecido en el ANS (Acuerdo de Nivel de Servicios) es superado[20].

- Assure Forwarding: se definen M clases (colas) con N niveles de descarte, la IETF[21] recomienda utilizar 4 colas con 3 niveles de descarte. Con este tipo de PHB, se estipula una cuantía mínima de recursos por clase, operando algunos mecanismos que sirven para reservar porciones de los mismos (Scheduler) y otros que ayudan a gestionar el buffer, con el fin de administrar los niveles de precedencia de descarte; se emplea para flujos de datos que requieren una tasa de bits específica, pero sin limitantes en cuanto a retardos ni jitters; entonces se emplea para asegurar la disponibilidad del servicio al usuario aún en caso de congestión de red; por lo tanto, el cliente siempre tendrá reservado una cantidad fija de ancho de banda[22]

### 2.3.2 Virtual LAN (VLAN)

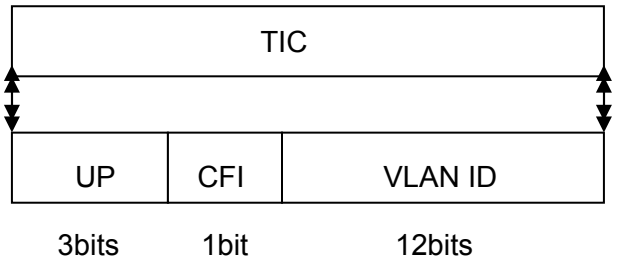
Es la técnica de software que permite crear grupos de trabajo lógicamente mediante la reunión y asignación de varios equipos terminales pertenecientes a diferentes tramos de la red LAN a un puerto del switch, de tal forma que se pueden comunicar como si todos

---

[19] RFC 2474 Definition of the differentiated services field in the IPv4 and IPv6 headers
[20] RFC 2598 An expedited forwarding PHB
[21] Grupo de Tabajo en Ingenieria de Internet
[22] RFC 2597 Assured Forwarding PHB group

pertenecieran al mismo segmento físico; el establecimiento de las VLANs se realiza ya sea estática (manualmente por el administrador) ó dinámicamente (organizando una base de datos centralizada con las direcciones MAC, de tal forma que cuando un nuevo equipo se adhiere al sistema, el switch lo incorpora automáticamente a la VLAN que corresponda), separando de esta forma los dominios de broadcast con el propósito de aislar los flujos de tráfico provenientes de cada uno de grupos lógicos; adicionalmente se obtiene un mejor rendimiento de la red ya que por lo general con este funcionamiento se logra disminuir el retardo.

Un punto que cabe resaltar es la existencia de una etiqueta de 12 bits (VLAN-ID) que se coloca después de la dirección MAC origen en la cabecera Ethernet, con el fin de identificar a qué VLAN pertenece cada trama e indicar el nivel de prioridad de la trama a nivel de capa MAC, información que va contenida en el campo User Priority de 3 bits de la etiqueta 802.1q. Para voz se asigna el valor 5 en campo UP ó prioridad.




Fuente: HUIDOBRO, José y ROLDÁN, David. Tecnología VoIP y Telefonía IP.

### 2.3.3 Redes Privadas Virtuales ( Virtual Private Networks VPNs)

Se pueden constituir caminos virtuales mediante VPN (Virtual Private Network), debido a que son sistemas que proporcionan conectividad virtual entre localizaciones geográficamente distanciadas simulando una conexión dedicada con garantía de seguridad (control de acceso, cifrado y autenticación), trabajan sobre ambientes de naturaleza pública usando los mismos enrutadores y enlaces para transportar diferentes servicios, pero brindando las mismas garantías de operación y envió de tráfico que una red privada; dichas conexiones se establecen entre dos extremos opuestos de la red llamados PE (network, service Provider Edge) y CE (Customer Edge routers).

Mediante la creación de VPN, es posible utilizar técnicas tales como, separación de flujos de tráfico de acuerdo a la clase establecida al ingreso del sistema, reserva de recursos de red, priorización de servicios y aplicación de ingeniería de tráfico para garantizar la calidad del servicio examinando la cabecera IP que la red backbone transporta hasta el destino[23].

## 2.4 PARÁMETROS DE RELEVANCIA PARA QOS EN REDES INALÁMBRICAS

Uno de los factores más relevantes a la hora de planificar una red basada en el estándar 802.11 es garantizar que la calidad de la señal transmitida no se atenué de manera considerable por motivo de interferencias, o de las características y materiales del ambiente en el cual trabajara la red.

A fin de obtener una buena relación entre la potencia de la señal recibida y el ruido interferente en una zona de cobertura dada, es necesario planificar adecuadamente el número de estaciones base[24] así como su localización en puntos estratégicos, teniendo en cuenta la cantidad de usuarios en cada zona de estudio, el tamaño del recinto y los posibles obstáculos al paso de la señal; después de haber determinado la localización de las estaciones base y su cobertura, se procede a hacer un estudio a fin de realizar una asignación eficiente de canales de acuerdo a la ubicación de estas, al número de frecuencias disponibles, la demanda de tráfico ofrecido en cada zona, el grado de servicio y la potencia recibida.

En este punto es preciso aclarar algunos conceptos estrechamente relacionados con el correcto desempeño de una red inalámbrica Wi-Fi.

### 2.4.1 Handover o roaming

Constituye un factor determinante al lograr que los usuarios se movilicen de una celda a otra sin que pierdan el servicio; para esto se conectan todos los AP a la misma subred física de tal forma que al pasar de una celda a otra se establezca conexión con la nueva estación base sin afectar la correcta transmisión de los datos.

---

[23] RFC 1349 Type of service in the Internet protocol suite
[24] Punto de acceso

El principal inconveniente radica en que para no perder la conectividad es necesario efectuar un tránsito de información que demora un lapso de tiempo entre 250 ms y 500ms lo cual conlleva pérdida de información y por ende degradación de la calidad de servicio.

### 2.4.2 Celda

La región en la cual la potencia de una estación base es lo suficientemente alta para que un receptor capture correctamente la señal se denomina celda.

### 2.4.3 Cobertura de una celda

La cobertura de una celda abarca dos aspectos principales, el primero se describe como el espacio en el cual la potencia recibida de un punto de acceso (AP) es mayor que todas las demás potencias y está por encima del umbral dado; por otro lado está el hecho que la velocidad de transmisión no se disminuye considerablemente dentro de este radio; por lo tanto dicha estación base está en capacidad de prestar servicio dentro de esa porción de área, entre mayor es la potencia del ounto de acceso mayor es el área de cobertura.

### 2.4.4 Modelo de pérdidas de propagación

Mediante este se predice la atenuación de potencia que pueden causar los obstáculos, el ruido térmico, la distancia y otros agentes que perturban el paso de la señal; se realiza un modelamiento de pérdidas a fin de calcular apropiadamente la relación señal a ruido y obtener un criterio para ubicar adecuadamente las estaciones base.

### 2.4.5 Carga de Tráfico ofrecido

Según el número de posibles usuarios en un área determinada, se estima la cantidad de datos que se pueden transmitir y se priorizan las zonas de cobertura según la cantidad de tráfico que se pueda generar en dicha área.

### 2.4.6 Capacidad

Se entiende por capacidad del sistema al mejor ancho de banda que se puede asignar a los usuarios.

### 2.4.7 Throughput

Relación existente entre la cantidad de datos transmitidos y el tiempo empleado en transferir la información.

### 2.4.8 Interferencias

Existen dos clases de interferencias provenientes de otra estación base; la primera es la denominada interferencia de canales adyacentes que se produce porque el "ancho de banda de una transmisión (22MHz) es mayor que el ancho de banda correspondiente a un canal (5MHz)" y la segunda radica en el hecho de que dos celdas contiguas trabajen sobre el mismo canal "co-canal" lo que conlleva a que se puedan producir colisiones al no detectar que otra estación está transmitiendo al mismo tiempo.

### 2.4.9 Funcionamiento Capa MAC

Entender el funcionamiento de capa MAC es de suma importancia, ya que es la encargada de controlar el acceso al medio y regular la contienda de las diferentes estaciones que para este caso serian los terminales IP.

Las tramas que se transmiten pueden ser de tres tipos: control (ACK, CTS, RTS), datos ó gestión (Beacon, TIM) y están conformadas de la siguiente forma; el primer componente de una trama radica en la cabecera MAC con longitud igual a 6Bytes, dentro del cual se albergan los campos de control, duración, direccionamiento y control de secuencia; el segundo componente principal es el cuerpo de la trama o payload de longitud variable y por último se encuentra el campo de comprobación de redundancia cíclica ó CRC de 4Bytes.

| Header | Payload | CRC |
|---|---|---|
| 6Bytes | 0-2041 Bytes | 4Bytes |

Fuente:IEEE 802.11. Editado por el Autor.

Para entender el funcionamiento de la capa MAC, es necesario aclarar que trabaja con dos protocolos de acceso al medio situados en dos subniveles de la capa MAC.

- ✓ Distributed Coordination Function (DCF) ubicado en el subnivel inferior y basado en que las estaciones contienden por el medio, así para que un terminal pueda acceder al canal existen dos mecanismos: el básico que consiste en que cuando una estación tiene un paquete para transmitir es necesario que detecte qué canal esta libre y espere un tiempo intertrama llamado DIFS igual 50 μs para estar seguros que sigue en ese estado, cuando la estación a la cual va dirigida la información la recibe satisfactoriamente, espera un tiempo intertrama llamado SIFS igual 10 μs y envía una trama ACK; pero si al terminar el DIFS el medio se encuentra ocupado, la estación debe esperar un tiempo aleatorio llamado Backoff para volver a intentar transmitir. El otro mecanismo se fundamenta en el envío de tramas CTS y RTS para reservar el canal durante cierto tiempo. Adicionalmente DCF trabaja con una variable llamada NAV que sirve para que las estaciones sepan quién controla el medio y por cuánto tiempo ya que mantiene una pronóstico de en qué momento quedara libre el canal.

- ✓ Point Coordination Protocol (PCF) ubicado en el nivel superior y el cual se fundamenta en tener periodos libres de contienda, ya que cuando esta función está habilitada, el tiempo se divide en supertramas compuestas por dos periodos uno libre de contienda (CF) y uno de contienda (CP); por lo tanto cuando se comienza en el periodo libre de contienda el AP tiene el control del acceso al medio, envía cíclicamente tramas poll para interrogar a las estaciones y autorizar la transmisión de sus datos.

## 2.5 CALIDAD DE SERVICIO EN REDES INALÁMBRICAS - 802.11e

El estándar 802.11e sirve para garantizar QoS en redes inalámbricas Wi-Fi que soportan VoIP, ya que los mecanismos habituales de capa MAC no ofrecen flexibilidad ni el grado de confiabilidad requerida. 802.11e es llamado Hybrid Coordination Function (HCF) estableciendo dos nuevas funciones de coordinación que trabajan simultáneamente en la estación base:

- ✓ Enhanced Distributed Channel Access (EDCA) que es una nueva versión de DCF, diseñado para tráfico que no tiene grandes requerimientos de ancho de banda ni

retardos pero que necesita cierto nivel de confiabilidad, tal como tráfico TCP. Con este mecanismo es posible contar con varias colas que trabajan cada una independiente de las demás, de igual forma cada cola cuenta con 8 niveles de prioridad los cuales son mapeados en 4 categorías de acceso que tienen su propio espacio intertrama (AIFS) y mantiene su propio contador de Backoff.[25]

- ✓ Control Channel Access (HCCA) creado para aplicaciones con fuertes requerimientos de ancho de banda y retardos tales como VoIP. Se emplea un elemento llamado TSPEC que contiene el conjunto de parámetros que sirven para caracterizar los flujos de tráfico que una estación desea transmitir al coordinador Hibrido (HC), éste analiza los parámetros y decide si lo admite o no.

[25] Documento OBAN

# 3. CONSIDERACIONES PARA IMPLEMENTAR VoIP EN REDES INALÁMBRICAS

Para la implementación de la tecnología VoIP en redes inalámbricas se deben superar algunos obstáculos relacionados principalmente con la baja calidad de la voz, que resultan del hecho que las características en redes cableadas e inalámbricas son muy diferentes.

Las comunicaciones en tiempo real son bastante sensibles a retardos en la entrega de paquetes de información, lo que significa una limitante más para las comunicaciones inalámbricas, debido a la naturaleza del medio de transmisión utilizado el cual puede presentar niveles significativos de interferencia ya que es compartido con otras tecnologías, que generarían retransmisiones degradando la calidad de la voz.

Por estas y otras razones a continuación se enumeran los pasos que se deben tener en cuenta a la hora de implementar VoIP en una red inalámbrica Wi-Fi, atendiendo las soluciones y recomendaciones que brindan algunos fabricantes.

## 3.1 Selección del sistema inalámbrico

En el capitulo 1, se documentaron las diferentes opciones que rigen las redes basadas en 802.11, y como cada uno de ellos ofrece diferentes tasas de transmisión y frecuencias de operación. A continuación se hará una breve explicación de los beneficios y desventajas que conlleva implementar cada una de las tecnologías definidas en 802.11 aclarando que la decisión final está en manos del diseñador acoplándose a los requerimientos y condiciones de la red.

El estándar 802.11b no es el más indicado para implementar voz sobre IP debido a que tiene una tasa máxima de transmisión de 11Mbps lo cual limita la capacidad de la red para soportar llamadas simultáneas, desventaja que se vuelve crítica al alejarse del punto de acceso (AP).

En lo concerniente a la utilización del estándar 802.11g existen algunas características que deben ser tenidas en cuenta en el momento del diseño de la red, ya que brinda una buena tasa de transmisión y cobertura pero presenta el inconveniente de operar en la banda de frecuencia de 2.4 GHz que debe ser compartida con otros dispositivos, adicionalmente solo dispone de tres canales libres de solapamiento lo cual restringe la capacidad y reduce el throughput del sistema.

Se recomienda el empleo del estándar 802.11a, puesto que opera en la frecuencia de 5GHz, la cual no está tan saturada como la banda de 2.4GHz, también ofrece una buena tasa de transmisión para la implementación de VoIP, y adicionalmente dispone de un elevado número de canales sin solaparse [12]; pero hay que tomar en consideración el hecho que es necesaria la instalación de un mayor número de APs para cubrir una determinada zona comparada con las otras tecnologías.

Por último, la tecnología 802.11n que aun esta en desarrollo podría ser los suficientemente rápida y confiable como para manejar de forma fluida servicios de VoIP en la red, debido a que triplica la capacidad de transmisión de datos de 802.11g y puede trabajar en las dos bandas de frecuencias de los estándares anteriores, es útil que trabaje en la banda de 5 GHZ, ya que esta menos congestionada y permitirá alcanzar un mejor rendimiento.

Este estándar permite interoperabilidad con los anteriores, pero si la red es utilizada por un equipo que utilice un estándar anterior, esta baja su alcance para ser compatible con los equipos más antiguos, lo cual será una desventaja de acuerdo a la planificación de la red.

## 3.2 Planeación de la red inalámbrica

Para planificar la cobertura y la capacidad de la red se recomienda realizarlo de acuerdo a las siguientes etapas: definir la conformación de celdas, la cantidad de puntos de acceso, la ubicación de los puntos de acceso y el cálculo de los niveles de potencia recibidos; teniendo presente el sistema inalámbrico seleccionado.

### 3.2.1 Conformación de las celdas

Primero se debe hacer una sectorización del lugar en el cual se instalará la red de acuerdo al tamaño de este, a la distribución de usuarios por labores, así como la demanda de tráfico que se generará en dichos lugares a fin de estimar el ancho de banda que requiere cada grupo de usuarios. De esta manera se puede definir en qué sitios hay mayor necesidad tanto de capacidad como de cubrimiento, con el fin de elegir en cuales puntos es necesario colocar un punto de acceso y las zonas criticas o posibles cuellos de botella.

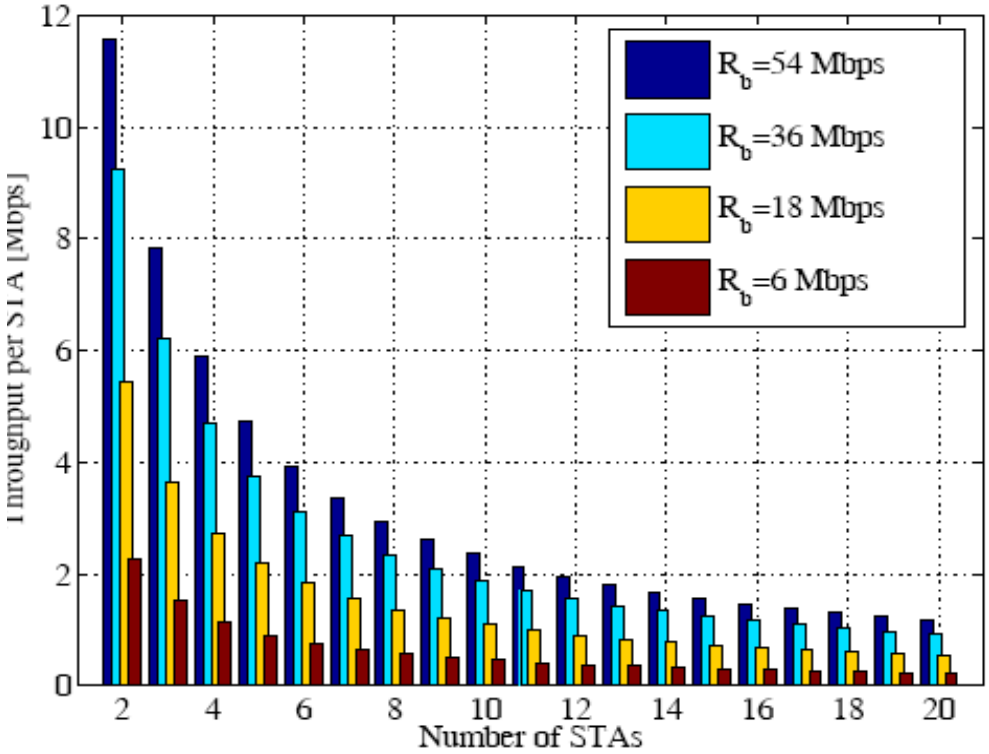
Luego, para organizar las celdas se mide la cantidad de potencia que ha sido atenuada por causa del ruido existente en el medio, si esta relación es más grande que un umbral dado, esta estación base está en capacidad de brindar el servicio en esa área, de lo contrario se deben tomar decisiones respecto a la instalación de una antena para ampliar la cobertura o colocar otra estación base como repetidor.
Por lo tanto se debe planificar muy bien la forma de distribuir los éstos puntos de acceso en la superficie de estudio para evitar interferencias.

### 3.2.2 Cantidad de puntos de acceso

Con respecto al número de puntos de acceso que se instalarán en el sistema se deben tomar en consideración parámetros como el ancho de banda, número de usuarios, utilización y velocidad para cada sector, que según el documento OBAN (Open Broadband Access Network) se determina de acuerdo, a la distancia y al tipo de recinto que se está considerando.

Los estudios y pruebas sustentados en el documento OBAN concernientes a cantidad de usuarios soportados por un Punto de Acceso para determinada tasa de transmisión, nivel de throughput y el envió de tramas de control CTS y RTS para evitar que una estación comience a transmitir cuando otra lo está haciendo, arrojan los siguientes resultados.

**Figura 5** Throughput como función del número de estaciones y tasa de datos para 802.11a/g




Fuente: Documento OBAN

**Tabla 5.** Número de usuarios que puede soportar un AP 802.11g como función del throughput por usuario, longitud de trama de 1500 Bytes, todas las STA trabajando a igual velocidad.

| | | **Tasa de Datos [Mbps]** | | | |
|---|---|---|---|---|---|
| | | **6** | **18** | **36** | **54** |
| **Throughput por usuario [Mbps]** | **0.2** | **22** | **53** | **89** | **110** |
| | **0.5** | **9** | **21** | **36** | **45** |
| | **1** | **4** | **10** | **18** | **23** |
| | **2** | **2** | **5** | **9** | **11** |

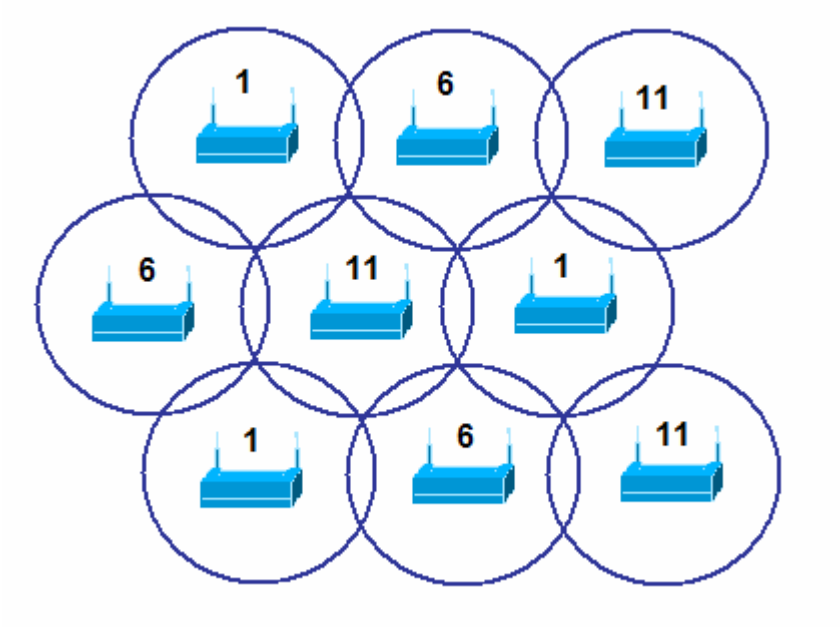
Fuente: Documento OBAN

Cabe acotar que algunas veces es mejor decisión para el diseño construir pequeñas celdas para lograr mayor capacidad y cobertura, lo cual se obtiene bajando la potencia, reduciendo el área cubierta y colocando más puntos de acceso; por lo tanto para estos casos la cantidad de APs aumentará.

Otro punto de importancia radica en que se deben realizar pruebas de medición del nivel de potencia y velocidad en toda el área que ya ha sido sectorizada y sobre la cual se ha establecido la cantidad de usuarios y el tráfico que se puede generar (necesidad de ancho de banda) para localizar las estaciones base en el punto donde se brinde mayor relación señal a interferencia al resto de zona; de igual forma es preciso determinar una altura de ubicación teniendo en cuenta las condiciones del ambiente tales como paredes, divisiones, puertas etc.

Un mecanismo para una distribución eficiente de las estaciones base es hacer que una pequeña zona este cubierta por dos AP para que de esta forma exista roaming, adicionalmente hay que tener cuidado en no fijar el mismo canal en celdas adyacentes con el fin de evitar interferencia co-canal y de igual forma tratar que una región no esté cubierta por más de tres celdas para evitar interferencia de canales adyacentes si se esta utilizando el estándar 802.11b ó g, tal como se ilustra en la siguiente gráfica.

**Figura 6** Distribucion de Puntos de Acceso con cobertura completa.




Fuente: Garcia, Nestor. Modelo de cobertura en redes inalambricas basado en radiosidad por refinamiento progresivo. Universidad de Oviedo. Tesis doctoral.

### 3.2.3 Calculo de los niveles de potencia recibidos

Es indispensable calcular los niveles de potencia recibida entre las diferentes celdas que conforman la red, para tal propósito se tiene en cuenta el modelo de pérdidas por propagación que depende de la distancia y que resulta de la sumatoria de todas las atenuaciones que sufre la potencia de la señal en la transmisión ya sea por multitrayectos, espacio libre, paredes, divisiones, ruido térmico ó cualquier otro factor que el diseñador considere.

$$Pot_{RX} = Pot_{Tx} + G_{TX} + G_{Rx} - (Per_{Lib} + Pot_{ruido} + Per_{obst})$$

Se han realizado trabajos avalados para el modelamiento de cada uno de los factores de pérdidas nombrados anteriormente, razón por la cual se tomaran estos resultados para el

cálculo de la potencia recibida. Por lo tanto las pérdidas en espacio libre se modelan de la siguiente forma[26]:

$$Per_{Lib}(d)[unidePot] = \frac{(4*\pi*d)^2}{(\lambda)^2}$$

$$Per_{Lib}(d)[dB] = 20*\log_{10}\left(\frac{4*\pi*d}{\lambda}\right)$$

La potencia del ruido se calcula así[27]:

$$Pot_{rui}[dBm] = 10*\log_{10}(KT) + 10*Log_{10}(BW) + 10dB$$

Mientras que las pérdidas debido a obstáculos tales como paredes o divisiones se modelan de la siguiente forma:

$$Per_{obst} = Per_{lib} + pAF(suav) + qAF(concre)$$

Siendo p el número de particiones suaves, q el número de paredes de concreto y AF el factor de atenuación. En algunos casos se consideran las pérdidas por multitrayectos que se hallan tomando mediciones de la potencia cada 20λ e interpolando.

Cuando el transmisor y el receptor no están en el mismo piso se tiene:

$$Per = Per_{lib} + 10*n(multipiso)*10*\log_{10}\left(\frac{d}{d_0}\right)$$

### 3.2.4 Técnicas de planeación

Con los sistemas inalámbricos es difícil predecir la propagación de las ondas de radio y detectar interferencias en la señal sin el uso de equipos de prueba, por esta razón

---

[26] Hakegard, Jan y Myhre, Bard. D8 Scenarios and Wireless Performance and Coverage. 2005

[27] Seidel, Scott y Rappaport, Theodore. *914 MHz Path Loss Prediction Models For Indoor Wireless Communications in Multifloored Buildings.* IEEE Transactions On Antennas and Propagation, Vol 4. Feb 1992.

además de las consideraciones citadas anteriormente, es necesario realizar un estudio llamado Site-survey antes de implementar la red inalámbrica.

El objetivo de un site-survey es proporcionar información suficiente para determinar la ubicación y número de puntos de acceso que proporcionan una adecuada cobertura, además de detectar interferencias de otras fuentes que pueden degradar el rendimiento de la red.

Para realizar un estudio site-survey se deben seguir los siguientes pasos:

- ✓ Obtener un plano del sitio.
- ✓ Recorrer las instalaciones para comprobar la exactitud del plano y encontrar obstáculos que puedan afectar la señal y que no figuran en el diagrama.
- ✓ Determinar la ubicación preliminar de cada punto de acceso
- ✓ Probar las ubicaciones preliminares y comprobar que se alcanzan las coberturas y rendimientos esperados
- ✓ Identificar fuentes de energía y conexiones de red para los puntos de acceso

También es posible apoyarse en técnicas por software para detectar el alcance de los puntos de acceso de acuerdo a su ubicación.

### 3.3 Calidad de la voz

Debido a que las aplicaciones VoIP son más sensibles a retardos en la transmisión que las aplicaciones de datos, es importante mantener y garantizar ciertos niveles de desempeño para implementar VoIP en la red inalámbrica de forma eficiente.

Las retransmisiones, mecanismos de seguridad, la sobrecarga de roaming, entre otros, son factores que causan latencia y jitter en la red, por estas razones se ha creado el estándar 802.11e para garantizar QoS en redes inalámbricas. Los productos que soportan 802.11e tienen certificaciones de la familia Wi-Fi Multimedia (WMM).

En este punto es importante hacer algunas recomendaciones que ayudarán al diseñador a tomar las decisiones más adecuadas en lo concerniente a calidad de servicio en la implementación de VoIP y tomando en consideración que la red inalámbrica de una empresa es una extensión de una red backbone cableada, se propone lo siguiente.

- ✓ Asegurarse que todos los equipos soporten las técnicas de calidad de servicio que se desean implementar, debido a que si algún dispositivo no habla el mismo idioma todo el diseño se dañará.

- ✓ Como se describió en el capítulo 2**,** un mecanismo muy eficiente para implementar calidad de servicio de extremo a extremo en redes IP es el llamado DiffServ, que permite clasificar y priorizar los flujos de trafico según sus requerimientos, por lo tanto se plantea la utilización de esta técnica, de tal forma que se dé el tratamiento adecuado a cada paquete en todos los nodos de la red. Así para el servicio de voz sobre IP se dará un tratamiento *Expedited Forwarding* debido a que es una aplicación en tiempo real que exige mayor prioridad y más recursos de red para garantizar bajos retardos, mínimo jitter, además de pequeña tasa de pérdida de paquetes; mientras que para servicios de correo y navegación por internet se asignará tratamiento *Best Effort*, ahora el tratamiento *Assure Forwarding* se emplearía para descartar paquetes que pertenecen a aplicaciones que no son en tiempo real y aquellas que son permisibles a retardos en tiempo real.

- ✓ Con el propósito de entregar servicios con calidad y seguridad, se propone la creación de redes privadas virtuales de tal forma que por cada túnel solamente se propague un tipo especifico de tráfico aprovechando las características de seguridad brindadas por estas conexiones virtuales; por lo cual como mínimo deben existir dos VPNs, una para datos y otra para tráfico de voz.

- ✓ En cuanto a la red inalámbrica, se debe garantizar que los dispositivos cumplan con el estándar 802.11e que incluye un número de especificaciones que mejoran el desempeño, tales como prioridad en el tráfico de flujo, la vida de la batería, reducción en el overhead del protocolo y los enlaces directos entre estaciones

inalámbricas. La prioridad del tráfico es la parte más importante de 802.11e cuando se implementa VoIP en una red inalámbrica, el acceso con prioridad al canal inalámbrico es diseñado para aplicaciones como voz y video.

Para hacer referencia a las investigaciones realizadas por los fabricantes, a continuación se nombran algunas experiencias.

En los laboratorios de la empresa Nortel Networks se ha simulado el desempeño de la implementación de VoIP en una red inalámbrica usando *Best-effort* y los resultados para que la implementación trabaje razonablemente dependen de un limitado número de usuarios, que tenga un tráfico de datos no muy grande y que las fuentes de interferencia sean bajas. El escenario de prueba fue una red inalámbrica bajo el estándar IEEE 802.11a libre de interferencias y sin tráfico de datos, la cual soportó un máximo de 30 llamadas simultáneas, dado que más llamadas incrementan el jitter considerablemente, en particular en la dirección del punto de acceso hacia el usuario. La prueba coincidió con el número de estaciones cliente para tráfico de datos que puede soportar un punto de acceso. Al final Nortel Networks recomienda implementar más puntos de acceso si se desea soportar más usuarios, teniendo la precaución de no generar interferencias co-canal entre ellos.

Por otro lado, la empresa Extricom ofrece Puntos de Acceso modelo UltraThin que no contienen buffers de paquetes entrantes y salientes, reduciendo asi la latencia y el jitter en la red. Además los APs utilizan múltiples canales que le permiten separar los paquetes de voz de los de datos a través de diferentes canales, adicionalmente soportan mejoras a los mecanismos de QoS como WMM y 802.11e.

## 3.4 Aplicaciones de seguridad

Es inaceptable considerar la implementación de voz en una red inalámbrica que no tenga algún método de seguridad en funcionamiento. Las siguientes son algunas de las pautas que debe tener una red inalámbrica para ser consideradas seguras:

- ✓ Se recomienda por lo menos, utilizar un esquema de cifrado seguro como WPA o WPA2, de ninguna manera se debe utilizar el esquema basado en WEP debido a que se ha demostrado que presenta vulnerabilidades a nivel de seguridad.
- ✓ Deshabilitar la difusión del SSID (Service Set Identifier), para no transmitir el nombre de la red.
- ✓ Para redes pequeñas se puede activar el filtrado por direcciones MAC.
- ✓ Implementar VPNs que permitan separar el flujo de tráfico de acuerdo al sistema establecido al ingreso de la red inalámbrica.

### 3.5 Servicio de voz sin interrupciones

El roaming puede ser un problema en los teléfonos Wi-Fi para VoIP. Todos los dispositivos Wi-Fi han sido diseñados para ir a través de una serie de pasos en orden para establecer una conexión con un nuevo AP cuando el actual AP alcanza un nivel de servicio demasiado bajo. Este proceso se llama roaming 802.11. El roaming ocurre sin importar que tipo de seguridad se esté utilizando, sea WEP, WPA, WPA 2 o ninguna aplicación. Con cualquiera que esté utilizando existirá un retardo en la comunicación de la red tratando de establecer una conexión con el nuevo AP.

Se necesitará un analizador de protocolos, para permitir establecer que tan a menudo un teléfono hace roaming dentro de la red estudiada. El problema es que el tiempo de roaming es variante y depende de diversos factores, tales como el tráfico de la red, la interferencia de radiofrecuencia y el desempeño del dispositivo. Estos factores pueden causar que el tiempo de roaming se incremente a niveles inaceptables que no permitirán tener una conversación aceptable.

Es importante que el diseñador de la red conozca cuál es la distancia mayor entre AP para que deje de existir servicio o pierda la conectividad dentro de la celda y ocurra roaming, sin embargo si los AP están ubicados muy cerca puede causar que algunos teléfonos realicen roaming muy seguido.

Puesto que el roaming en 802.11 es iniciado por la estación y no por el AP, los fabricantes de los teléfonos Wi-Fi tienen un alto grado de control sobre como es el comportamiento de sus móviles. Los umbrales bajos de roaming son preferibles en ambientes donde está presente VoIP inalámbrico porque esto causa que el roaming ocurra con menos frecuencia. Algunos fabricantes han creado umbrales dinámicos de roaming. Estos umbrales dinámicos aumentan cuando el teléfono está inactivo que cuando se asocia al mejor AP posible. Una vez una llamada se inicia, el umbral de roaming baja para que la llamada este menos expuesta a realizar roaming.

### 3.6 Consumo de potencia

La optimización del tiempo de vida de la batería es un factor importante, pero el ajuste más importante en la configuración cuando se implementa VoIP es la potencia de salida de los AP. Los AP permiten potencias de salida en el rango de 1 mWatt hasta 100 mWatt.

Pero los ajustes en la configuración de potencia de salida en los AP puede afectar la calidad de la llamada, puesto que los teléfonos VoIP usan generalmente niveles de potencia variables como un método para mejorar la vida de las baterías, entonces, un teléfono que deambula de un AP de alta potencia a uno de baja potencia puede ver una perdida excesiva de paquetes mientras el teléfono ajusta su nivel de potencia.

El diseñador de la red debe ajustar los niveles de potencia igual en cada AP, es necesario porque esto ayuda a mitigar la perdida de paquetes cuando existe roaming.

### 3.7 Terminales VoIP para Wi-Fi

La calidad de los terminales VoIP también es una característica importante cuando se implementa VoIP en una red inalámbrica, el teléfono debe ser capaz de reducir la potencia de transmisión de cada paquete.

El terminal debe ser configurado para que transmita datos a la más alta velocidad de transmisión y reducir el consumo de energía.

Al seleccionar el teléfono es importante tener en cuenta:

- ✓ Compatibilidad con el estándar utilizado en la red inalámbrica.
- ✓ Debe tener algún mecanismo de seguridad implementado (WEP, WPA o WPA2).
- ✓ Ofrecer calidad de servicio.
- ✓ Duración de la batería.
- ✓ Codecs que soporta el teléfono.

### 3.8 Casos de estudio

A continuación se mencionarán algunos casos de implementación de VoIP sobre redes inalámbricas:

- Cisco systems implemento una solución inalámbrica y de voz sobre IP en la empresa consorcio ALUMAR, ubicada en la ciudad de São Luís do Maranhão, Brasil. Esta empresa está dedicada a la producción de aluminio y alúmina. La línea de producción de ALUMAR está compuesta por seis "salas de cubas", con un total de 610 cubas. Para que el proceso de electrólisis de la alúmina quede bajo control, el operador de cubas necesita analizar y evaluar todas las etapas, así como tener acceso constante a las informaciones de las variables del proceso.

  Antes de la utilización de la red WLAN y de la voz sobre IP, el operador de la sala de cubas poseía como herramientas de trabajo una computadora, situada en la sala de control, un radio y un teléfono celular. En caso de observar algún fallo en el proceso de electrólisis, el operador necesitaba desplazarse hasta la sala de control más cercana que, a veces, podría estar a 600 metros de distancia de su local de trabajo, con el objeto de chequear los datos del proceso y tomar las medidas pertinentes. Al ser implantada la solución, el operador, sin necesidad de ir a la sala de control, puede tomar todas las medidas necesarias para subsanar el problema, utilizando exclusivamente un Pocket PC

  Las soluciones inalámbricas (WLAN) y de voz sobre IP se empezaron a configurar con la implantación de una red WLAN inalámbrica que comprende las tres líneas

de producción de las salas de cubas. Así, por medio de la utilización de un Pocket PC, conectado vía inalámbrica a los servidores controladores del proceso de electrólisis, los operadores consiguen actuar en forma autónoma y rápida para poner el proceso bajo control.

Después de esta etapa inicial, utilizando la solución implementada de Cisco, es posible unificar las necesidades resultantes del trabajo de los operadores de las cubas en un único equipo: el Pocket PC. Ahora, además de ejercer el control sobre los niveles de calidad del proceso de electrólisis de la alúmina, el operador puede hablar, por medio de la tecnología de voz sobre IP, con la sala de control o con el ingeniero de proceso localizado en cualquier punto de la fábrica.

La red de Telefonía IP de Alumar está compuesta por 16 Puntos de acceso, solución Cisco Call Manager, gateway de VoIP Cisco, además de teléfonos IP de Cisco y plataformas de seguridad.

- Siemens presenta otro caso en el Hotel Llao Llao, ubicado en La Patagonia, Argentina. El hotel quería implementar una red inalámbrica para brindar a sus huéspedes el servicio de internet inalámbrico y comunicaciones móviles a sus empleados dentro del hotel.

  La solución planteada por Siemens se basa en el sistema IP de comunicaciones en tiempo real HiPath 4000, con tres IPDA (estantes remotos conectados vía IP) y 906 terminales. Con 60 access points Wireless LAN se cubre toda el área brindando movilidad de voz y datos. Para garantizar la provisión de voz y datos con calidad de servicio, se incorporó un controlador Wireless LAN (HiPath Wireless Controler) que asegura la calidad en las comunicaciones telefónicas. Con 80 teléfonos IP Wireless LAN (OptiPoint WL2 Professional) los empleados pueden movilizarse cómodamente dentro del predio del hotel y dar respuesta rápida a cada pedido de los huéspedes. Dentro de las habitaciones se instalaron 111 teléfonos IP OptiPoint 410/420 para uso exclusivo de los huéspedes.

- Por último, la empresa Minera Michilla de Chile deseaba instalar vigilancia por cámaras IP y el transporte de voz y datos entre puntos distantes, como la zona de

producción y el puerto de la mina. La solución fue realizada con dispositivos Cisco y estuvo montada sobre un backbone inalámbrico, debido al terreno y geografía de la mina.

# 4. CONCLUSIONES

La transmisión de voz empleando el protocolo de internet involucra varios componentes de red, tales como central telefónica ó servidor, Gateway, terminales IP y red IP cada uno desempeñando funciones específicas y complementándose mutuamente.

Para la correcta transmisión de voz en tiempo real con el protocolo IP, son necesarios una serie de protocolos con el fin de controlar todos los aspectos pertinentes al proceso en mención.

Al recopilar los factores determinantes en el buen diseño de una red inalámbrica que este en capacidad de prestar el servicio VoIP, se elige el estándar 802.11a por sus características de tasa máxima de transmisión y su frecuencia de operación, que esta menos congestionada; adicionalmente dispone de 12 canales que no se solapan evitando la interferencia co-canal. Se debe considerar que se necesita un mayor número de puntos de acceso debido a que su alcance es más limitado que con el empleo de otra tecnología.

No se recomienda el estándar 8021.11n, por que actualmente los productos que se encuentran en el mercado son dispositivos basados en el borrador aprobado y no en el estándar final. Además, los terminales VoIP para redes inalámbricas actualmente no cubren este estándar.

Al aprobar el estándar final de 802.11n se recomienda instalar la red inalámbrica con esta tecnología para soportar VoIP, teniendo en cuenta que los teléfonos deben soportarlo.

Al implementar VoIP en una red inalámbrica es de vital importancia garantizar una adecuada cobertura, con un nivel de intensidad de la señal recibida lo suficientemente aceptable para garantizar una conversación sin interrupciones. Por esta razón, es necesario realizar un estudio site-survey para recolectar la mayor información acerca del

sitio donde se desarrolla el proyecto y determinar la ubicación de los puntos de acceso y su rango de cobertura.

Para asegurar una buena calidad de la voz se recomienda que los dispositivos inalámbricos cumplan con el estándar 802.11e, además, se plantea la técnica de Diffserv para clasificar y priorizar el trafico, y dar un tratamiento adecuado a cada paquete en todos los nodos de la red. De esta manera se dará un tratamiento *Expedited Forwarding* para las aplicaciones en tiempo real como Voz sobre IP.

Las redes inalámbricas son muy vulnerables a ataques de seguridad de la información por utilizar un medio de transmisión compartido sin control de acceso a dicho medio, por esta razón es importante tener en cuenta los estándares y las prácticas que mejoran la seguridad de la WLAN.

Los terminales VoIP para una red inalámbrica deben soportar los mecanismos de seguridad y de calidad que se van a implementar en la red. Por ultimo, es necesario ajustar la potencia de salida de los puntos de acceso para prolongar el tiempo de vida de la batería del teléfono.

# 5. BIBLIOGRAFÍA


[1] PINZON, Samuel Gonzalo. Curso Redes Inalámbricas. Escuela de Ingeniería Eléctrica, Electrónica y de Telecomunicaciones. UIS. Cohorte VII-Ciclo II, 2006.

[2] HUIDOBRO, José y ROLDÁN, David. Tecnología VoIP y Telefonía IP. México: Alfaomega, julio 2006.

[3] FERREIRA, Guillermo y FROCHT, Gustavo y MAYONE, Eduardo. Tecnología de Voz Sobre IP Terminal H.323 [Tesis de Grado]. (2001). 134p.

[4] FERNÁNDEZ, Néstor. Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo. [Tesis Doctoral Universidad de Oviedo]. (mar, 2006). 299 p.

[5] BERROCAL, Julio et al. Redes de Acceso de Banda Ancha: Arquitectura, Prestaciones, Servicios y Evolución. Madrid. ( 2003). 93 p.

[6] RFC 1349 Type of service in the Internet protocol suite

[7] RFC 2474 Definition of the differentiated services field in the IPv4 and IPv6 headers

[8] RFC 2597 Assured Forwarding PHB group

[9] RFC 2598 An expedited forwarding PHB

[10] Hakegard, Jan y Myhre, Bard. D8 Scenaries and Wireless Performance and Coverage. 2005

[11] OBAN - Open Broadband Access Network

[12] VoIP without wires, Galen Gruman. Disponible en Internet: http://www.infoworld.com

[13] Whitepaper WLANs Straight talk on voice over wireless LANs. Disponible en internet: http://www.nortelnetworks.com

[14] White paper Voice over Wi-Fi capacity planning. Disponible en Internet: http://www.proxim.com

[15] White paper Voice over wireless LAN, System Design and performance considerations. Disponible en Internet: http://www.extricom.com

[16] Is it the network? Solving VoIP problems on a wireless LAN, Benjamin Miller. Disponible en internet: http://www.globalknowledge.com

[17] www.cisco.com

[18] www.siemens.com

[19] www.3com.com

[20] www.wi-fi.org